

THE 2022 COMPENDIUM OF NPC ISSUANCES

20
22

MESSAGE



The need to raise awareness in data privacy and security remains vital in empowering our citizens and our nation. In fulfillment of its mandate, the National Privacy Commission (NPC) continues to guide and educate the Filipinos, both data subjects and personal information controllers (PICs) or personal information processors (PIPs) on data privacy and protection through the annual release of its Compendium.

The Compendium of NPC Issuances is not only a reliable source of information and guide to our citizens and stakeholders, it is also a body of work that demonstrates the Commission's commitment in ensuring that the basic human right to privacy is protected.

In 2022, we faced various privacy issues and concerns which were promptly addressed by the Commission within the purview of its mandate. Such issues and concerns ranges from health information, employment records, and requests for public officials' information up to matters concerning data subject rights, criteria for lawful processing, and penalties for privacy violators provided under the Data Privacy Act of 2012 (DPA).

With this, the 2022 Compendium of NPC Issuances is composed of 29 Advisory Opinions, 18 Decisions, 37 Resolutions, 4 Circulars, 1 Frequently Asked Questions (FAQ), and 1 Joint Administrative Order that aims to educate our citizens on various data privacy concerns.

Indeed, this Compendium also serves as the collective labor and desire of the Commission to always bring its role as partner-regulator to the next level – may it be in guiding the data subjects to know their rights or in assisting PICs and PIPs to adequately comply with the DPA.

With this, the Commission hopes that this Compendium will continue to inspire data privacy champions and allies in joining us in our vision towards a secure and world-class data privacy environment in the Philippines. Equally, may it also encourage Filipinos to remain curious and be citizens that aim to rigorously safeguard the right to privacy.

(Sgd.) ATTY. JOHN HENRY D. NAGA
Privacy Commissioner

MESSAGE



The significant increase in the processing of personal data has resulted in an intensified awareness of the Data Privacy Act of 2012 (DPA). In fact, a recent study found that people are becoming more interested in learning about data privacy and how the National Privacy Commission (NPC) can protect their personal information. The results of the study also indicate that more individuals are starting to look at data privacy as something important and relevant to them.

Building on this interest and the growing importance being given to data privacy, the NPC is pleased to present this compendium that presents a consolidated overview of its issuances in the year 2022. This material serves as an invaluable resource for those who seek to deepen their understanding of the law and its application to practical situations and experiences. In particular, the pseudonymized version of the Decisions and Resolutions of the Commission En Banc aim to provide clarity and guidance on various matters related to the application of the DPA, its IRR, and other issuances of the NPC.

The various issuances of the NPC seek to remind Personal Information Controllers (PICs), Personal Information Processors (PIPs), and data subjects about their concomitant responsibilities under the DPA. The protection of our personal information is not just the work of a single person, but it is a shared responsibility between those who process personal data and the data subjects who own that data. By reading the discussions provided herein, I hope that any misconceptions or misinterpretations of the law can be addressed and, ultimately, not only decrease the privacy risks for data subjects but also increase the level of compliance of PICs and PIPs.

Finally, I encourage everyone to not lose sight of what data privacy is all about – to protect the fundamental right to privacy of human beings – us, as data subjects. Developing a better and correct understanding of the general privacy principles and the lawful criteria for processing our personal information, among other things, is a step closer to what the NPC has always envisioned – a culture of privacy, where everyone can confidently share their information because they know that their right to privacy is protected and respected. With our collective efforts, I am confident that we can thrive, flourish, and establish an environment that fosters privacy, innovation, and growth.

(Sgd.) ATTY. LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

MESSAGE



In recent years, particularly during the COVID-19 pandemic, there has been a significant surge in the generation, storage, and transmission of personal data through digital platforms. This rise in digital platforms and services, coupled with the rapid growth of data, has raised substantial concerns regarding data privacy and protection. The extensive use of digital platforms has led to data breaches, unauthorized access, and the misuse of personal information.

Recognizing these emerging challenges, the National Privacy Commission (NPC) has proactively addressed these issues by continuously adjusting its policies and regulations, in line with the demands of this ever-evolving digital landscape. It has likewise remained true to its commitment to uphold and safeguard individuals' data privacy rights by incorporating them into its policies, plans, and programs; and empower the public with the knowledge and tools necessary to protect their data and privacy rights amidst evolving technological threats.

In line with this commitment, the Commission has compiled recent issuances into this Compendium. Through this, the NPC aims to provide a valuable platform for data subjects, privacy professionals, businesses, government agencies, and other stakeholders engaged in the processing and protection of personal data. By doing so, we seek to facilitate stakeholders' active participation in the privacy landscape, foster greater awareness, and encourage responsible handling of personal data among organizations, ultimately creating a safer and more secure digital environment for everyone.

Let's come together and recognize the vital importance of data privacy in our lives. My heartfelt hope is that this Compendium serves as a trusted companion, inspiring individuals who are dedicated to protecting and promoting the privacy rights of our fellow citizens. With each reader's involvement, let's nurture a shared commitment to data privacy.

(Sgd.) ATTY. NERISSA N. DE JESUS
Deputy Privacy Commissioner

MESSAGE



In this Fourth Industrial Revolution, data privacy has become a global priority. Technology, innovation, and rapid digital transformation challenge the traditional notions of how we perceive and use data in an increasingly complex world.

The Philippines is in a period of dynamic digital shift across all sectors. In the government, the digitalization of public services to enhance bureaucratic efficiency is an administrative priority and a part of the 8-point socioeconomic agenda of His Excellency President Ferdinand R. Marcos, Jr.

This agenda is rooted in the state policy that a secured and protected information and communications technology ecosystem will promote the free flow of information, which is vital for nation-building. This was tested no less by our lessons from the COVID-19 pandemic. Poor data privacy practices erode public trust and result in an inaccurate, delayed, and constricted flow of information that negatively impacts the fight against the novel threat. However, when data is collected in secure and protected environments, we gain access to truthful and accurate data that is crucial for informed policies, decisions, strategies, and interventions on both local and international scales.

In a similar manner, the private sector has become more open to the adoption and development of data-driven technologies, products, services, and other offerings to remain ahead of the competition. In this respect, private companies no matter the size, now appreciate the value of incorporating data privacy and security practices in their systems, processes, and policies.

Despite these developments, we should remain cognizant that building a secure and resilient digital ecosystem for the Philippines is an arduous endeavor. Many industries, even the government, are still in the infancy stages of their data protection journey. Our data privacy awareness campaigns have seen successful strides, but much work is needed to develop policies, regulations, and infostructure that can support privacy-first initiatives.

Our work now teaches future leaders and provides them with concrete examples of how to approach grey areas in the application of data privacy concepts to new ideas and concepts. It is, therefore, our solemn commitment to assure our stakeholders that their National Privacy Commission (NPC) shall continue to deliver Advisory Opinions, Advisories, and Circulars that are relevant to changing times and responsive to their needs.

We must remember that the NPC is given the distinct opportunity to witness, understand, and address the complexities faced by our stakeholders and influence the steps they take. Thus, we must remain true to our mandate, act with diligence, and work together towards the common goal of laying the foundations of data protection in the Philippines.

I wish to express my confidence and trust in the officials and employees of the NPC who, through perseverance and dedication, have demonstrated great capabilities to advance the public interest considerations inherent in data privacy protection.

This 2022 Compendium will be a guiding instrument for all our stakeholders. It is reflective of the NPC's evolving views of data privacy and protection and indicative of our strategies to enforce the Data Privacy Act through varying levels of regulatory action.

I trust that the NPC, under the Marcos Administration and in partnership with the Department of Information and Communications Technology, will continue to be instrumental on the path to recovery and nationwide transformation.

To all the officials and employees of the NPC, mabuhay!

(Sgd.) ATTY. IVIN RONALD D.M. ALZONA
Executive Director IV

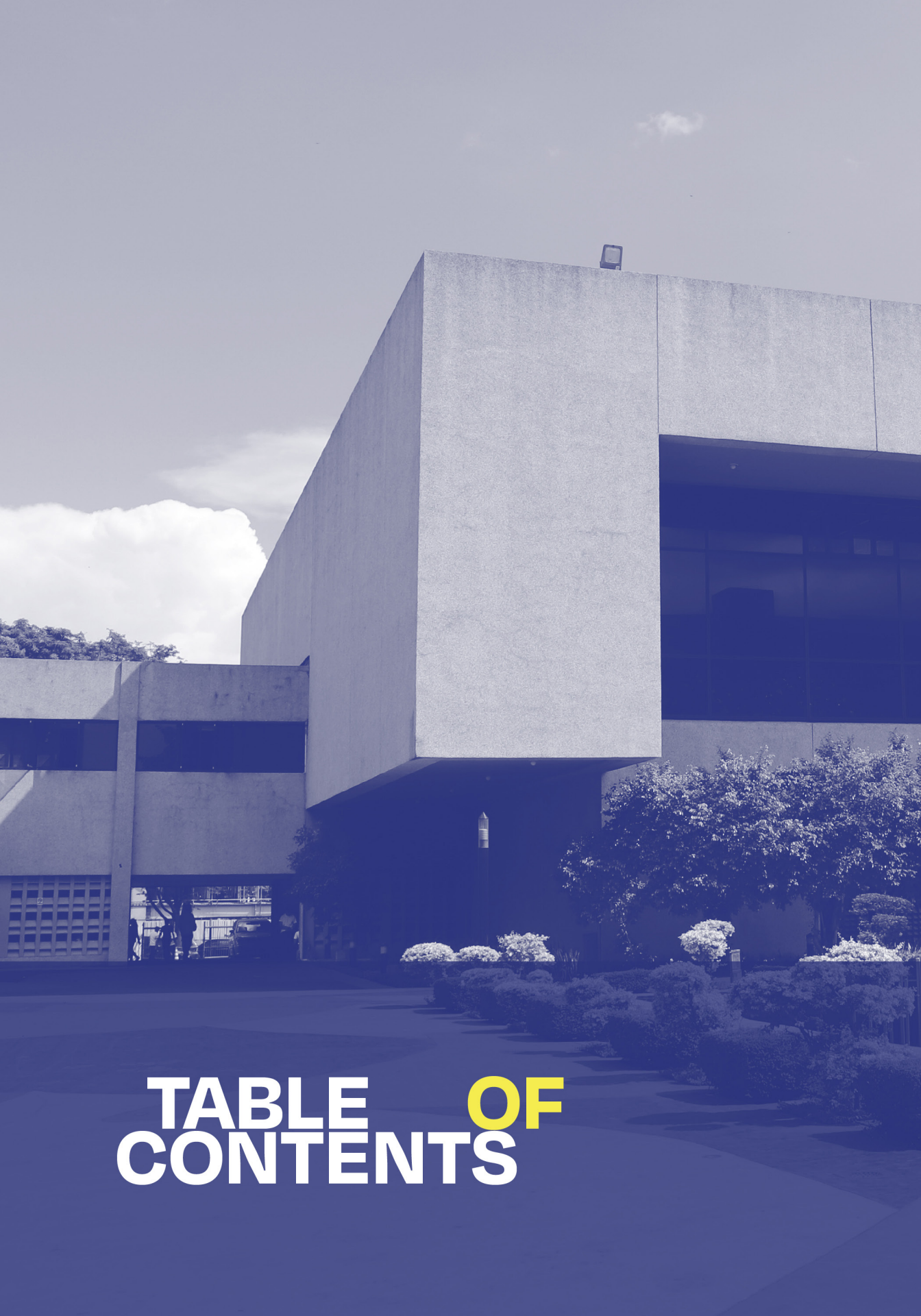


TABLE OF CONTENTS

ADVISORY OPINION

- 14 ADVISORY OPINION NO. 2022-001**
PHILHEALTH'S PUBLICATION OF THE LIST OF HEALTH CARE PROVIDERS WITH DENIED OR RETURN-TO-HOSPITAL CLAIMS

- 18 ADVISORY OPINION NO. 2022-002**
DISCLOSURE BY CAR DEALERS/AUTOMOTIVE REPAIR SHOPS OF PERSONAL DATA OF THE ABANDONED VEHICLE OWNERS

- 22 ADVISORY OPINION NO. 2022-003**
REQUEST FOR A COPY OF COMPLAINTS FILED AND RECORDS IN RELATION THERETO

- 25 ADVISORY OPINION NO. 2022-004**
DISCLOSURE OF INCAPACITATED PATIENTS AND DECEASED PATIENTS' MEDICAL INFORMATION

- 30 ADVISORY OPINION NO. 2022-005**
REQUEST FOR NAMES AND ADDRESSES OF VEHICLE OWNERS FROM THE LAND TRANSPORTATION OFFICE

- 37 ADVISORY OPINION NO. 2022-006**
REQUEST FOR CUSTOMER'S PERSONAL DATA AND TRANSACTION HISTORY WITH A PRIVATE COURIER

- 43 ADVISORY OPINION NO. 2022-007**
TRANSPORT OF PHYSICAL MEDIA CONTAINING PERSONAL DATA

- 48 ADVISORY OPINION NO. 2022-008**
OBTAINING EMPLOYMENT RECORD OR CERTIFICATION FROM THE SOCIAL SECURITY SYSTEM

- 51 ADVISORY OPINION NO. 2022-009**
PUBLICATION OF FORMER EMPLOYEES' NAMES AND
SEVERANCE FROM EMPLOYMENT
- 55 ADVISORY OPINION NO. 2022-010**
REQUEST FOR OPINION ON PRIVACY MATTERS
CONCERNING TRANSFER OF ASSETS/LIABILITIES
- 70 ADVISORY OPINION NO. 2022-011**
PERSONAL DATA RETENTION AND DELETION
- 80 ADVISORY OPINION NO. 2022-012**
REMEDIES AGAINST THE ALLEGED DATA BREACH
INVOLVING WORKABROAD.PH (WORKABROAD)
- 86 ADVISORY OPINION NO. 2022-013**
ONLINE LENDING MOBILE APPLICATION
PERMISSIONS
- 93 ADVISORY OPINION NO. 2022-014**
RECORDING AND UPLOADING OF ONLINE CLASSES
- 98 ADVISORY OPINION NO. 2022-015**
USE OF CAMERA DURING SURVEILLANCE VISITS
- 105 ADVISORY OPINION NO. 2022-016**
REQUEST FOR PERSONAL INFORMATION OF OFWs
DEPLOYED IN THE MIDDLE EAST AND OTHER
MUSLIM COUNTRIES

- 111 ADVISORY OPINION NO. 2022-017**
DISCLOSURE OF PERSONAL INFORMATION FOR
CYBERSECURITY INVESTIGATIONS
- 118 ADVISORY OPINION NO. 2022-018**
DATA SUBJECT RIGHTS IN THE PHILIPPINE
IDENTIFICATION SYSTEM
- 125 ADVISORY OPINION NO. 2022-019**
USE OF BODY-WORN CAMERA BY SECURITY
PERSONNEL
- 130 ADVISORY OPINION NO. 2022-020**
CIVIL REGISTRY DOCUMENT REQUEST BY A PERSON
OTHER THAN THE OWNER
- 135 ADVISORY OPINION NO. 2022-021**
PUBLICATION OF INFORMATION OF LIST OF
WHOLESALE ELECTRICITY SPOT MARKET (WESM)
MEMBERS AND RETAIL CUSTOMER INFORMATION
UNDER RETAIL COMPETITION AND OPEN ACCESS
(RCOA) AND GREEN ENERGY OPTION PROGRAM
(GEOP).
- 141 ADVISORY OPINION NO. 2022-022**
DISCLOSURE OF COVID-19 SWAB TEST RESULTS IN
GROUP CHAT
- 142 ADVISORY OPINION NO. 2022-023**
DISCLOSURE OF STUDENTS' PERSONAL DATA FOR
CASE BUILD-UP PURPOSES
- 151 ADVISORY OPINION NO. 2022-024**
FREE FLOW OF DATA

156 ADVISORY OPINION NO. 2022-025

201 FILES OF GOVERNMENT EMPLOYEES

162 ADVISORY OPINION NO. 2022-026

DISCLOSURE OF PERSONAL DATA THROUGH THE DATABASE OF INDIVIDUALS BARRED FROM TAKING CIVIL SERVICE EXAMINATIONS AND FROM ENTERING GOVERNMENT SERVICE (DIBAR)

168 DECISIONS

584 RESOLUTIONS

CIRCULARS

962 NPC Circular No. 2022-01

GUIDELINES ON ADMINISTRATIVE FINES

968 NPC Circular No. 2022-02

AMENDING CERTAIN PROVISIONS OF NPC CIRCULAR NO. 20-01 ON THE GUIDELINES ON THE PROCESSING OF PERSONAL DATA FOR LOAN-RELATED TRANSACTIONS

974 NPC Circular No. 2022-03

GUIDELINES FOR PRIVATE SECURITY AGENCIES ON THE PROPER HANDLING OF CUSTOMER AND VISITOR INFORMATION

981 NPC Circular No. 2022-04

REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION

**1002 FREQUENTLY ASKED QUESTIONS ON THE
GUIDELINES ON ADMINISTRATIVE FINES**

**1011 JOINT ADMINISTRATIVE ORDER NO. 22-01
Series of 2022**



ADVISORY OPINIONS

ADVISORY OPINION NO. 2022-001¹

11 February 2022



Re: **PHILHEALTH'S PUBLICATION OF THE LIST OF HEALTH CARE PROVIDERS WITH DENIED OR RETURN-TO-HOSPITAL CLAIMS**

Dear 

We write in response to your request for an Advisory Opinion received by the National Privacy Commission (NPC) seeking clarification on whether the publication of the list of health care facilities with denied or return-to-hospital (RTH) claims, including the reasons thereof, violates the provisions of the Data Privacy Act of 2012² (DPA), its Implementing Rules and Regulations³ (IRR) and other issuances of the NPC.

You stated in your letter that the Philippine Health Insurance Corporation (PhilHealth), in the interest of transparency and right to information of the public, is considering the publication of the abovementioned list. The proposed publication emanated from allegations that the PhilHealth still owes certain amounts of money when, upon verification, most of such pending claims were actually denied or RTH claims.

Claims are denied when the same are violative of existing PhilHealth laws, rules and regulations (e.g., fraudulent claims, medical condition or procedure is not compensable under the All Case Rate policy or filed beyond the prescribed period) or returned to health care facilities for correction of deficiencies (e.g., incomplete attachments, improperly filled out claim forms) and to be refiled once corrected. We further understand from your letter that the PhilHealth is mandated to establish a mechanism

¹ Tags: scope of the DPA; juridical entities; legal obligation; public authority; law or regulation; general data privacy principles; proportionality; sensitive personal information.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

³ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).

for feedback aimed at improving the quality of service and to periodically inform the public of the performance of accredited health care providers, including accreditation that has been suspended or revoked by PhilHealth.⁴

You now ask whether such publication is allowed under the DPA.

Scope of the DPA; health care providers

The DPA applies to the processing of all types of personal information and sensitive personal information (collectively, personal data) and to any natural or juridical person involved in the processing of personal data.⁵

This means that the scope of the DPA, with regard to the subject matter, is limited only to the processing of personal data or data pertaining to natural persons or individuals. Data pertaining to juridical entities (e.g., company name, address, financial information, etc.) are not covered by the DPA.

With this, we refer to the definition of health care institution under the revised IRR of the National Health Insurance Act of 2013, as amended:

Health Care Institution — refers to health facilities that are accredited with Philhealth which includes, among others, hospitals, ambulatory surgical clinics, TB-DOTS, freestanding dialysis clinics, primary care benefits facilities, and maternity care package providers.⁶

From the foregoing, health care institutions are therefore juridical persons. We wish to clarify that publications involving the details of juridical entities, do not fall within the ambit of the DPA. We emphasize that the DPA is only limited to the processing of personal data or information of natural persons.⁷

We wish to clarify further that should the terms “health care institution” or “health care facility” include health care professionals who are natural persons and there will be publications involving the details of the said natural persons, the provisions of the DPA shall apply.⁸

Lawful processing; legal obligation; functions of public authority; law or regulation

In case the publication will involve personal data as discussed above, such processing by PhilHealth may be based on the applicable criterion under Sections 12 or 13 of the DPA, for the processing of personal information and sensitive personal information, respectively.

Specifically, Section 12 (c) and (e) or Section 13 (b) may be applicable:

SECTION 12. Criteria for Lawful Processing of Personal Information. — The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: x x x

⁴ Rules and Regulations Implementing the National Health Insurance Act of 2013, Republic Act No. 7875 as amended, § 79 (2004).

⁵ Data Privacy Act of 2012, § 4.

⁶ Rules and Regulations Implementing the National Health Insurance Act of 2013, as amended, § 3 (w).

⁷ Data Privacy Act of 2012, § 4 in relation to § 3 (g) and 3 (l).

⁸ Ibid.

- (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject; x x x
- (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or x x x

SECTION 13. Sensitive Personal Information and Privileged Information. — The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: x x x

- (b) The processing of the same is provided for by existing laws and regulations: x x x.

The above is read in relation to the IRR of Republic Act (RA) No. 7875, as amended, otherwise known as the National Health Insurance Act of 2013, which mandates PhilHealth to establish a mechanism for feedback to inform the public about the performance of accredited health care providers, to wit:

SECTION 79. Mechanism for Feedback. — A mechanism aimed at improving quality of service shall be established by the Corporation to periodically inform health care providers, program administrators and the public of the performance of accredited health care providers. The Corporation shall make known to the general public information on the performance of accredited health care providers, including the release of names of those of good standing as well as those whose accreditation has been suspended or revoked by the Corporation.

In pursuit of informed choice as enunciated in the Act, feedback reports shall include information on the amount reimbursed by the Corporation vis-a-vis the actual charges billed by the accredited health care provider.⁹

The publication of personal data may be allowed since such processing is necessary for PhilHealth's compliance with its legal obligation, as the agency tasked to implement universal health coverage in the country, to inform the public about the performance of accredited health care providers which includes those with denied or RTH claims. The publication of personal data is also in recognition of PhilHealth's fulfillment of its mandate under the revised IRR of the National Health Insurance Act of 2013 to provide a mechanism for feedback to improve the quality of service.

General data privacy principles; proportionality; sensitive personal information; anonymization

But as a personal information controller (PIC), PhilHealth must still adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.¹⁰ Specific to the principle of transparency, PhilHealth should ensure that the health care providers involved are informed about the details of this type of processing (i.e., publication of the list of health care providers with denied or RTH claims).

This may be achieved through a privacy notice that will explain the purpose for posting the list (i.e., to periodically inform health care providers, program administrators and the public of the

⁹ Id. § 79.

¹⁰ Data Privacy Act of 2012. § 11. performance of accredited health care providers). The privacy notice should also

state the means for the data subjects to correct any inaccurate information and other details upon posting of the initial list which will help them exercise their rights under the DPA.

For proportionality, this requires that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.¹¹ In this regard, PhilHealth should consider indicating a specific period in its publication (e.g., “as of December 2021”) to ensure its accuracy.

Philhealth must assess what particular personal data should be published in relation to its purpose of informing the general public about health care providers with denied and RTH claims.

Sensitive personal information of doctors, nurses, midwives, dentists, pharmacists or other healthcare professionals or practitioners such as their license numbers, other government-issued identification numbers, marital status, date of birth, among others, should not be published as these may already be deemed irrelevant to the declared and specified purpose. From Philhealth’s 15 December 2021 letter, we note that the purpose for the publication or processing of personal data is to inform the public about health care providers with denied or RTH claims. This purpose can be achieved by processing only the necessary personal information (i.e., posting the list of names of health care professionals) since the names would already identify the parties concerned. Publication of the above sensitive personal information would be excessive in relation to such purpose.

Lastly, we note that the reasons for the denied or RTH claims will also be published. Philhealth must ensure that no personal data of patients shall be included in the publication. The general reasons as stated by Philhealth, e.g., fraudulent claims, medical condition or procedure is not compensable under the All Case Rate policy, filed beyond the prescribed period, should already suffice. Any other detailed disclosure of the reasons behind why certain claims are denied or returned are only relevant and necessary for the information of the health care facilities only and not the public.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC – Director IV, Privacy Policy Office

¹¹Data Privacy Act of 2012, § 11 (d).

ADVISORY OPINION NO. 2022-002¹

11 February 2022



**Re: DISCLOSURE BY CAR DEALERS/AUTOMOTIVE REPAIR
SHOPS OF PERSONAL DATA OF THE ABANDONED
VEHICLE OWNERS**

Dear 

We write in response to the request for an Advisory Opinion received by the National Privacy Commission (NPC) regarding the disclosure by car dealers/automotive repair shops of personal data of abandoned vehicle owners.

We understand that your client is engaged in the business of operating car dealerships and repair shops. In line with this, several vehicles it received for repair and/or maintenance as early as 2015 remain in its possession despite notice to the owners of the completion of service/s. This has caused prejudice to your client as the vehicles require sustained maintenance and space causing undue cost and potential legal issues in relation thereto.

We understand further that a number of these vehicles were purchased under financing arrangements with banks or financing companies. As the vehicles have been left in the repair shop for several months, if not years, there is the probability that the owners have stopped amortization payments for the abandoned vehicles.

You now ask whether informing the concerned mortgagee banks or financing companies on the status of the unclaimed vehicles that

¹ Tags: disclosure of personal data; lawful basis for processing; legitimate interest; legal claims.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission and for other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

they have financed is sanctioned under the Data Privacy Act of 2012 (DPA), particularly as a valid disclosure falling under Section 12 (f) on legitimate interest.

Lawful processing of personal information; legitimate interest of personal information controllers; Section 12 (f) of the Data Privacy Act of 2012

Under the DPA, the processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the conditions under Section 12 of the law exists. One condition under the law is processing necessary for the purposes of the legitimate interests of the personal information controller (PIC) or by a third party to whom the data is disclosed,³ to wit:

“(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.”

In the determination of legitimate interest, the following must be considered:⁴

1. Purpose test – The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve;
2. Necessity test – The processing of personal information must be necessary for the purpose of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test – The fundamental rights and freedoms of data subjects must not be overridden by the legitimate interests of the PIC or third party, considering the likely impact of the processing on the data subjects.

Indeed, legitimate interest as a ground for lawful processing of personal data is a flexible concept that may be applicable in certain instances where processing will not have unwarranted impacts on the rights and freedoms of data subjects.⁵

³ Data Privacy Act of 2012, §12 (f).

⁴ See: National Privacy Commission, Advisory Opinion Nos. 2021-10 (March 22, 2021) and 2020-50 (Nov. 26, 2020) citing Data Privacy Act of 2012, § 12 (f); United Kingdom Information Commissioner’s Office (ICO), What is the ‘Legitimate Interests’ basis?, available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>.

⁵ Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014 (available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf).

⁶ Id.

Nevertheless, PICs that consider relying on this basis should undergo a legitimate interest assessment using the aforementioned tests as guidance, and document the outcome of the assessment. This gives data subjects some guarantee that this criterion for processing will not be misused.⁶

We emphasize as well that legitimate interest is applicable only to the processing of personal information. If the disclosure will involve sensitive personal information, the PIC should determine the appropriate lawful basis under Section 13 of the DPA.

Adherence to the general data privacy principles

Nonetheless, the existence of a lawful basis for disclosure of personal or sensitive personal information (collectively, personal data) under the DPA is just one of the requirements in relation to the processing personal data. PICs are still required to adhere with the principles of transparency, legitimate purpose, and proportionality prescribed under the law.⁷

In this case, the data subjects involved must be informed that their personal data will be disclosed to the banks/financing companies in relation to the abandoned vehicles. This may be embodied through an appropriate notice sent to the vehicle owner's last known address and/or contact details stating the actions the PIC intends to make. It is suggested that a similar privacy notice be prepared and made part of the documentation with respect to future repairs and maintenance service contracts, or other similar agreements of your client.

The PIC is also reminded that the disclosure to the banks and/or financing companies should be limited to its declared and specified purpose, and that only those personal data that is adequate, relevant, suitable, necessary, and not excessive in relation to the purpose should be disclosed. Thus, personal data disclosed to the banks and financial companies should be limited to information necessary to identify the owner and the vehicle.

In addition, it is expected that the proposed disclosure will be done with accuracy – in that the details of a particular vehicle owner and abandoned vehicle should only be disclosed to the bank or financing company that financed the purchase of the vehicle and not to all possible banks or financing companies. Disclosures cannot be done in an indiscriminate manner since it would violate the principle of proportionality.

⁷ Data Privacy Act of 2012, §11.

Finally, we note that it was unclear how the banks and/or financing companies involved in the financing of specific abandoned vehicles were determined by the PIC. We highlight that in the identification of these banks and/or financing companies, it is important that PICs likewise observe compliance with the general data privacy principles and other provisions of the DPA.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2022-003¹

14 February 2022



Re: **REQUEST FOR A COPY OF COMPLAINTS FILED AND RECORDS IN RELATION THERETO**

Dear [REDACTED]

We write in response to your request for an Advisory Opinion received by the National Privacy Commission (NPC) on whether to grant the request for a copy of the complaints previously filed against a certain doctor in 2018 by five (5) medical bodies including the documents provided by the said doctor in relation to such complaints.

We understand that the documents requested will be used by the requestor in connection with a case filed by the doctor against the said requestor.

*Sensitive personal information; lawful processing;
establishment, exercise or defense of legal claims under
Section 13(f) of the Data Privacy Act of 2012*

Republic Act No. 10713, otherwise known as the Data Privacy Act of 2012 (DPA), provides a specific enumeration of personal data classified as sensitive personal information under the law, one of which involves a data subject's information pertaining to offenses and the incidence in relation thereto, to wit:

“(I) Sensitive personal information refers to personal information: x x x

¹ Tags: sensitive personal information; lawful processing; protection of lawful rights and interest of natural or legal persons in court proceedings; establishment, exercise or defense of legal claims.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10713 (2012).

(2) About all individual's health, education, genetic or sexual life of a person, or

to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings.”³ (emphasis supplied)

In fine, any (1) proceeding for any offense committed or alleged to have been committed by a data subject; (2) the disposal of the proceedings; or (3) the sentence of any court in such proceedings, are considered as sensitive personal information under the DPA.

Although there is a prohibition under the law to process sensitive personal information, the DPA also provide for exceptions to this rule. Section 13 (f) recognizes the processing which concerns the establishment, exercise, or defense of legal claims. The provision reads:

“SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: x x x

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interest of natural or legal persons in court proceedings or the establishment, exercise, or defense of legal claims, or when provided to government or public authority.”⁴

It must be noted that in the determination on whether a request based on the aforementioned provision should be granted, “the legitimacy of the purpose and the proportionality of the request shall be taken into consideration”.⁵

We understand that the request received by the Department of Health (DOH) was in the form of an email communication without any detail as to what the pending case is. To satisfy the DOH on the legitimacy of the purpose of the request, it may opt to require the requestor to provide additional information on the case. But this requirement shall still adhere to the principle of proportionality, and whatever additional information received shall be used solely for the purpose of aiding the DOH in deciding whether to release the requested documents.

³ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for other purposes [Data Privacy Act of 2012] Republic Act No. 10173, § 3 (l) (2) (2012).

⁴ Data Privacy Act of 2012, § 13 (f).

⁵ See: National Privacy Commission, NPC Advisory Opinion No. 2021-044 (Dec. 29, 2021).

It is likewise suggested that the DOH establish a system to handle such requests, to streamline the process and make it more efficient in case there will be similar requests in the future.

The DOH may also clarify with the requestor if instead of the release of the actual copies of the complaints and related documentation, an official certification from the DOH stating the details or a summary of the complaints filed, i.e., names of the medical bodies, nature of the complaints, date filed, status, etc., should suffice.

Should the request be granted, the DOH should require the requestor to sign an undertaking to the effect that the requestor recognizes that the use of the documents will be for the sole purpose of protecting his rights and interests in the case filed against him and that the use thereof beyond its declared purpose may equate to unauthorized processing penalized under the pertinent provision of the DPA. It is also important to include a clause in the undertaking whereby the requestor acknowledges that his receipt of the requested documents carries with it the obligations of a personal information controller under the DPA.⁶

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

⁶ Id

ADVISORY OPINION NO. 2022-004¹

15 February 2022

[REDACTED]

[REDACTED]

Re: **DISCLOSURE OF INCAPACITATED PATIENTS AND DECEASED PATIENTS' MEDICAL INFORMATION**

Dear [REDACTED]

We write in response to your request for an Advisory Opinion received by the National Privacy Commission (NPC) to provide guidance on the disclosure of the medical information of incapacitated patients and deceased patients.

We understand from your letter that St. Luke's Medical Center (SLMC), in providing medical and healthcare services, encounters cases wherein a patient is unconscious or otherwise unable to give consent. Furthermore, you provided that SLMC is faced with issues whenever the said patient's relatives, other than his or her spouse, common-law spouse or child who is already transacting with SLMC, ask for updates about the patient's medical condition and request for the medical records of the patient.

¹ Tags: sensitive personal information; lawful processing; protection of lawful rights and interest of natural or legal persons in court proceedings; establishment, exercise or defense of legal claims.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

You now seek guidance and clarification on the relatives who can give consent on behalf of the patient in the above scenario. Specifically, you asked the following:

1. Who has the right to receive (i) medical documents; and (ii) status updates regarding an incapacitated patient?

- a. Can any heir or relative of the patient request for medical documents and status updates from the hospital?
- b. Can other relatives be excluded by next-of-kin from receiving medical documents and status updates?
- c. Who should be our default recipient of medical documents and status updates?

2. In case relatives disagree on the issue of disclosing the status of patient's medical condition and documents, what is the hierarchy on knowing who to follow?

- a. Do we follow the spouse first, then children, then parents? What if the spouse and the children disagree?
- b. For children of legal age who disagree on a decision of sharing medical condition and documents of the patient, do we follow the eldest or do we put it to a vote? Do we have the obligation to reach out to absent children of legal age?

3. Do we have the obligation to search for an absent next-of-kin to give status updates?

4. Will the answers to queries above change if the patient expires? Does the existence of legal heirs exclude other relatives from securing medical documents from the hospital (e.g., a parent requesting medical records of a deceased son/daughter who has predeceased his or her spouse and children)?

Rights of data subjects; right to access; transmissibility of rights

Data subjects are entitled to various rights under the Data Privacy Act of 2012² (DPA) and its Implementing Rules and Regulations³ (IRR). One of the rights granted is the right of reasonable access to, upon demand, the contents of one's personal data that have been processed, among other information relating to the processing of his or her personal information and sensitive personal information (collectively, personal data).⁴

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

³ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).

⁴ Data Privacy Act of 2012, § 16 (c) (2012).

This right to access, however, may be limited in certain instances. In the current scenario, the following provision of NPC Advisory No. 2021-01 on Data Subject Rights may be taken into consideration:

“SECTION 8. Right to Access. — x x x

C. The following instances, where applicable, may limit the right to access: x x x

4. Consideration of the safety of the data subject. In exceptional cases and subject to any applicable ethical guidelines, limitations on the right to access may apply if in the professional evaluation and determination of the PIC, providing access to the requested information may cause serious harm to the physical, mental, or emotional health of the data subject.”⁵

Otherwise, the personal information controller (PIC) is obliged to grant the request of the data subject.

The right to access, along with the other rights of data subjects, must be read together with Section 17 of the DPA on transmissibility of rights. The provision states that the lawful heirs and assigns of the data subject may invoke the rights of the data subject for which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights under the DPA.⁶

Please take note that the DPA does not distinguish nor identify the persons considered to be the “lawful heirs and assigns of the data subject”. Hence, the determination of such matter may be guided by the general laws on the hierarchy of legal heirs provided under several provisions of the Civil Code of the Philippines on the laws of succession and the rules on guardianship of incompetent persons.

Incapacitated and deceased data subjects; legal heirs and assigns

As to the determination of the heir or relative who has the right to receive medical documents and status updates of an incapacitated patient, we reiterate that the DPA does not distinguish the legal heirs

⁵ National Privacy Commission, Data Subject Rights [NPC Advisory No. 2021-01], § 8 (c) (4) (29 Jan 2021).

⁶ Data Privacy Act of 2012, § 17.

⁷ SPECIAL PROCEEDINGS, Rule 92, § 2.

⁸ Id., Rule 93, § 1.

and assigns of an incapacitated data subject. The DPA may not be the appropriate law to be used as basis under this circumstance. With this, reference may be made to the general laws on the hierarchy of heirs and legal assigns identified under various provisions of the Civil Code or the rules on guardianship over incompetent persons⁷ under the Rules of Court on Special Proceedings,⁸ whichever may be applicable to the particular scenario and subject further to such other laws, regulations, and guidelines as may be applicable.

We note that this does not preclude SLMC, as a PIC, from crafting policies on the classification of relatives, the exclusion of other types of relatives and the designation of a default relative who may receive medical documents and status updates. Likewise, due regard must be given to ethical guidelines that may apply.

The above shall also apply in case of disagreement among relatives on the issue of disclosing the status of a patient's medical condition. To reiterate, SLMC may refer to the hierarchy of heirs provided by the Civil Code on the laws of succession or the rules of guardianship over incompetent persons under the Rules of Court on Special Proceedings, whichever may be applicable, in the crafting of its policies on the disclosure of a patient's medical condition and records.

With regard to SLMC's obligation to search for an absent next-of-kin, the DPA does not require PICs to do this. The NPC is also not privy to any laws or regulations which require healthcare providers to exhaust all means to search for an absentee next-of-kin. As far as the DPA is concerned, an incapacitated data subject still has the right to exercise his or her rights under the law through a legal heir or assign. If an incapacitated person does not have any other heir to whom status updates may be provided, SLMC may consider searching for the said heir through reasonable efforts.

Lastly, as to the applicability of the above discussions to deceased patients, we wish to reiterate our position. The rights of deceased data subjects, similar to incapacitated data subjects, can still be exercised through the transmissibility of rights under Section 17 of the DPA. Similarly, the DPA does not distinguish on whether a different set of rules and procedure would apply to deceased and incapacitated data subjects. The DPA may not be the appropriate law for this circumstance, and accordingly, SLMC may refer to the laws on succession, and the laws on testate succession in case the deceased left a will and designated a person to attend to his or her

medical records. Moreover, it may be more appropriate to refer to the said law with regard to the strict application of the rules on the exclusion of other relatives.

We emphasize that, as far as the DPA is concerned, the rights of data subjects including those who are deceased, incapacitated or otherwise incapable of exercising such rights, are respected. Although, the DPA does not distinguish the groups of relatives who may exercise the same, the rights of the deceased or incapacitated data subjects are still existent and may be exercised by his or her lawful heirs and assigns, subject to existing laws on succession and guardianship, whichever may be applicable. The foregoing laws referred to above may be considered, guided by applicable rules and ethical guidelines and considerations that the health sector is subject to.

It is the responsibility of the PIC to establish policies on addressing issues on disclosures to relatives, subject to the applicable laws and rules. SLMC must still implement appropriate and reasonable security measures in the disclosure of medical information to legal heirs and assigns. For example, SLMC may implement policies on properly identifying the heirs of deceased and incapacitated patients by requiring the presentation of certain documents to prove their identities. Further, the fact of disclosure to the heir must be documented (i.e., the heir may be asked to sign certain documents to record such disclosure). In the establishment of these policies, SLMC should also consider the inclusion of policies and mechanisms on ensuring that the requesting party, acting on behalf of the data subject, is clearly informed of the reason in case of the limitation or denial of the request, as required under Section 14 of NPC Advisory No. 2021-01.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2022-005¹

24 February 2022



Re: **REQUEST FOR NAMES AND ADDRESSES OF VEHICLE OWNERS FROM THE LAND TRANSPORTATION OFFICE**

Dear 

We write in response to your inquiry received by the National Privacy Commission (NPC), endorsed by the Department of the Interior and Local Government (DILG), on the Land Transportation Office's (LTO's) denial of your request for the names and addresses of the owners of some allegedly noisy vehicles in a certain locality.

We understand that you filed an email complaint with the LTO on "nuisance due to noisy vehicles" in your village. Together with the email complaint, you requested for the names and addresses of the owners of the noisy vehicles for the filing "of formal/legal charges of damages due to the pain and sufferings from the emotional distress and mental anguish cause[d] by the noisy vehicles."

We also understand that the LTO responded to your email complaint and stated that they already issued proper notices for the owners of the noisy vehicles "to show cause, as part of due process, their defense." The LTO likewise denied your request, stating that the Data Privacy Act of 2012² (DPA) prohibits disclosure of personal information without consent.

Criteria for lawful processing of personal information

The name and address of a vehicle owner are personal information, the processing of which is covered by the DPA. We wish to clarify

¹ Tags: lawful processing; consent; legitimate interest; protection of lawful rights and interest of natural or legal persons in court proceedings; establishment, exercise or defense of legal claims.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012)

that the LTO's statement that the DPA prohibits them from disclosing personal information without consent is not entirely accurate.

Consent is not the only lawful basis for processing personal information. Section 12 of the DPA provides for the various criteria for lawful processing, to wit:

SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

- (a) The data subject has given his or her consent;
- (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
- (d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
- (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
- (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.³

The LTO should determine whether the request for the disclosure of the information falls under any other criteria for lawful processing of personal information. We emphasize that consent will not always be the most appropriate lawful basis, considering the relationship of the personal information controller (PIC) with the data subject and purpose of the processing, among others.

³ Data Privacy Act of 2012, § 12.

⁴ United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimateinterests/what-is-the-legitimate-interests-basis/> [last accessed on 18 January 2022]

Legitimate interests as lawful basis for processing personal information

We understand that the purpose for the request of the names and addresses of the motor vehicle owners is for the filing of a civil action for damages “due to the pain and sufferings from the emotional distress and mental anguish cause[d] by the noisy vehicles.” It is worthy to assess whether the purpose of the request falls under Section 12 (f) of the DPA which provides for legitimate interests as a lawful basis for the processing of personal information.

‘Legitimate interests’ is different from the other criteria for lawful processing of personal information as it is not centered around a specific purpose, nor is it processing that the individual has specifically agreed to – it can, in principle, apply to any type of processing for any reasonable purpose.⁴

Since processing based on legitimate interests can apply to a wide range of circumstances, there is a need to balance legitimate interests, the necessity of the processing and the rights of the individuals while taking into consideration the circumstances.⁵

Thus, in the determination of a legitimate interest, the personal information controller (PIC) must consider the following:

1. Purpose test – The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve;
2. Necessity test – The processing of personal information must be necessary for the purpose of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test – The fundamental rights and freedoms of data subjects must not be overridden by the legitimate interests of the PIC or third party, considering the likely impact of the processing on the data subjects.⁶

The LTO should have assessed the request based on the aforementioned tests considering the specific purpose declared in the request. As a PIC who holds a repository of personal and sensitive personal information, it is expected that it should have

⁵ Id.

⁶ See generally, Data Privacy Act of 2012, § 12 (f); United Kingdom Information Commissioner’s Office (ICO), What is the ‘Legitimate Interests’ basis?, available <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-generaldata-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/> [last accessed on 18 January 2022].

⁷ 1997 Rules of Procedure, as Amended, Rule 1, § 3 (a).

⁸ National Privacy Commission, BGM vs. IPP, NPC 19-653 (Dec. 17, 2020).

policies and processes in place to evaluate whether a request for information constitutes a legitimate interest of a requesting party, among other lawful bases for processing.

*Establishment of legal claims as a legitimate interest;
Section 13 (f)*

The processing of personal information for the filing of formal/legal charges for damages is a legitimate interest. An action for the recovery of damages is characterized as a civil action. A civil action is one by which a party sues another for the enforcement or protection of a right, or the prevention or redress of a wrong.⁷

While there is an existing administrative case initiated through the email complaint, it will not address the violation of the civil rights of a complainant. Thus, an administrative case does not preclude the filing of a civil action for damages.

The Commission, in BGM vs. IPP8, had the occasion to explain that the protection of lawful rights and interests under Section 13 (f) of the DPA is considered as legitimate interest pursuant to Section 12 (f) of the DPA:

Based on the foregoing, the disclosure to be made by the Respondent of the information of the recipient of Complainant's personal information, for purposes of identification of

the person liable for the alleged fraud, sans the latter's consent, is necessary for the tprotection of the lawful rights and interests of the Complainant as contemplated by Section 13 (f) of the DPA.

Although Section 13 (f) applies to sensitive personal information while the information involved in this case is just personal information, the protection of lawful rights and interests under Section 13 (f) by the Respondent is considered as legitimate interest pursuant to Section 12 (f) of the DPA. This section provides that it is lawful to process personal information if it is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

By application in the instant case, Respondent may not be held liable for unauthorized processing should it disclose the requested information to Complainant as its disclosure would be in pursuance of the latter's legitimate interest as the same cannot be fulfilled by other means.

It should be stressed, however, that having a legitimate purpose or some other lawful criteria to process does not result in the PIC granting all request to access by the data subjects. Such requests should be evaluated on a case to case basis and must always be subject to the PIC's guidelines for the release of such information.

Thus, the processing of personal information for the establishment

of legal claims is permitted under the DPA. “Establishment” may include activities to obtain evidence by lawful means for prospective court proceedings.

General data privacy principle; proportionality; accountability

While there may be lawful basis for your request, any disclosure of personal information should still be proportional to the stated purpose.

The principle of proportionality provides that “the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.”⁹

You are requesting LTO for the names and registered addresses of the owners of noisy vehicles you have identified through photographs of their plate numbers. The purpose of which is for the filing of “formal/ legal charges of damages.” Since your request is only for the said information, LTO cannot provide more than that. The principle of proportionality necessitates that only the information requested and necessary for the purpose indicated should be processed.

While the letter request you sent to LTO is a mass request for information of several individuals, the request for each motor vehicle owners’ information should be treated as individual requests. To this effect, LTO must require further information from you, the requesting party, to ensure a comprehensive evaluation of whether to grant each request for

information and decide on a case-by-case basis. You, on the other hand, must be able to provide sufficient information to support each of the requests. In Advisory Opinion 2022-003, we opined that additional information may be required by the granting party to ascertain the validity of the purpose for the request:

To satisfy the DOH on the legitimacy of the purpose of the request, it may opt to require the requestor to provide additional information on the case. But this requirement shall still adhere to the principle of proportionality, and whatever additional information received shall be used solely for the purpose of aiding the DOH in deciding whether to release the requested documents.

⁹ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016), § 18 (c).

LTO must establish a system for handling these types of requests for information to avoid the possibility of abuse. As a request for personal information for the filing of a legal action falls under the legitimate interests of the requesting party, the system must assess the request if it satisfies the three aforementioned tests. It must also provide for a mechanism to ensure that the information to be disclosed will only be used for the purpose/s indicated.

In Advisory Opinion No. 2021-044, it was recommended that in case a request for personal information is granted, the requesting party should be required to sign an undertaking that the information will only be used for the purpose that was declared:

Should the CHMSC grant the request, it is suggested that the Requesting Party be required to sign an undertaking that the use of the documents will only be for the purpose of filing a complaint with the Ombudsman and that the proper disposal thereof is ensured if he does not push through with the filing of the complaint. Further, the undertaking must include a clause to the effect that the requestor acknowledges that he becomes a PIC by his receipt of the requested documents and therefore has the obligations of a PIC as prescribed under the DPA.

Thus, LTO should similarly require a requesting party to sign an undertaking that the information that will be acquired will only be used for the purpose which was declared and authorized.

Lastly, we wish to underscore that should the information be provided, its use is limited to the declared purpose of filing formal/legal charges by the concerned or affected individual who allegedly suffered damages. Thus, the sharing, posting or any publication of such information in any public-facing platform such as social media pages or your public Facebook group, “BF Resort Village People,” is prohibited. While you may coordinate your efforts in filing an action for damages through such platforms, you must do so in a way that will not result in the publication of the information that you might acquire from LTO.

We caution that should there be processing beyond the stated purpose, the same may be penalized under the appropriate provisions of the DPA, such as Unauthorized Processing of Personal Information, Processing of Personal Information for Unauthorized Purposes or Unauthorized Disclosure which carry penalties of “imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00)”,¹⁰ one (1) year and six (6) months to five (5) years and a fine of not less than

¹⁰ Data Privacy Act of 2012, § 25(a).

Five hundred thousand pesos (Php500,000.00) but not

more than One million pesos (Php1,000,000.00),¹¹ or “imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00),”¹² respectively.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO

OIC-Director IV, Privacy Policy Office

cc : **VIVIAN P. SUANSING**

Director III/Officer-in-Charge, Bureau of Local Government Supervision
Department of the Interior and Local Government
sarrahamosa@gmail.com

ROBERTO A. VALERA

Deputy Director, Law Enforcement Service
Land Transportation Office
ltomailbox@lto.gov.ph

JO-ANN R. ALCID, Program Director

ATTY. VERNICE C. LIWAG-PRIETO, Detailed Public Attorney
Department of Justice Action Center
dojac@doj.gov.ph

¹¹ Data Privacy Act of 2012, § 28, par.1.

¹² Id. § 32.

ADVISORY OPINION NO. 2022-006¹

28 February 2022



Re: **REQUEST FOR CUSTOMER'S PERSONAL DATA AND TRANSACTION HISTORY WITH A PRIVATE COURIER**

Dear [REDACTED],

We write in response to your request for an Advisory Opinion received by the National Privacy Commission (NPC) on whether to grant the request of the Philippine Drug Enforcement Agency (PDEA) for certain personal data including the transaction history of one of your clients.

We understand that your company is engaged in logistics delivery and e-commerce business, acting as courier of parcels of your customers for delivery to their own clients. Thus, the company processes personal information of its customers as well as the latter's clients.

We understand further that the PDEA request was made pursuant to an ongoing investigation of the individual named in the request for illegal drug trafficking by means of courier platforms.

Further, we understand that there is an existing Memorandum of Agreement (MOA) between your company and the PDEA on coordination and mutual assistance for the effective and efficient implementation of the Comprehensive Dangerous Drugs Act of 2002,² with provisions on the duties and obligations of the parties, which includes assistance in the collection, processing, and analysis of information on illegal drug activities. The pertinent provisions included in your letter reads, viz:

¹ Tags: special cases; public authority; law enforcement; constitutional and statutory mandate; proportionality.

² An Act Instituting The Comprehensive Dangerous Drugs Act Of 2002, Repealing Republic Act No. 6425, Otherwise Known As The Dangerous Drugs Act Of 1972, As Amended, Providing Funds Therefor, And For Other Purposes [Comprehensive Dangerous Drugs Act of 2002], Republic Act No. 9165 (2002)

- a. Assist the PDEA in collecting, processing, and analyzing information on illegal drug activities by promptly notifying it within (24) (sic) hours;
- b. Assist PDEA in gathering information, monitoring, and identification of suspected drug trafficking activities;
- c. Relay, deliver and report timely intelligence information or all other information obtained in the course of their business shall be brought to the PDEA for the purpose of anti-drug operations;

x x x

m. To grant access to the authorized members of the PDEA, to the merchandise/items being sold, or about to be transported from the seller and/or from their facility/warehouse to the prospective buyer/client, whenever there is an intelligence report of merchandise, item or good suspected to be containing dangerous drugs and controlled precursors and essential chemicals.”

You mentioned that your company is inclined to deny the request in view of the prohibitions of the Data Privacy Act of 2012³ (DPA) but noted the exceptions under Section ⁴ (e) of the law pertaining to information necessary in order to carry out the functions of public authorities. You now ask whether your company may grant the PDEA’s request.

Scope of the DPA; special cases under the DPA; public authority; mandate; law enforcement

The DPA and its Implementing Rules and Regulations⁴ (IRR) provide for a list of specified information which do not fall within the scope of the law.⁵ In particular, information necessary to carry out the functions of a public authority are considered special cases under the IRR, to wit:

“SECTION 5. Special Cases. The Act and these Rules shall not apply to the following specified information, only to the minimum extent of collection, access, used, disclosure or other processing necessary to the purpose, function, or authority concerned: x x x

d. Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary

³ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

⁴ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).

⁵ Id. § 4 (e) (2012). necessary to achieve the specific purpose, function or activity.”⁶ (Underscoring supplied)

authority, subject to restriction provided by law. Nothing in this Act shall be construed as having amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);

X X X

Provided, that the non-applicability if the Act or these Rules do not extend to personal information controllers or personal information processors who remain subject to the requirements of implementing security measures for personal data protection: *Provided further*, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function or activity.⁶ (Underscoring supplied)

The above special case provides for qualifications or limitations on the application of the provisions of the DPA and its IRR. This means that when the personal and/or sensitive personal information (collectively, personal data) is needed to be processed by a public authority, such as the PDEA, pursuant to its statutory mandate, the processing of such personal data may be allowed under the law, to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned.

The following should guide the company in relation to the above-quoted provision:

- a) The information is necessary in order to carry out the law enforcement functions. Where the processing activity violates the Constitution, or any other applicable law, the processing will not be considered necessary for law enforcement purposes;
- b) The processing is for the fulfillment of a constitutional or statutory mandate; and
- c) There is strict adherence to all due process requirements. Where there is a nonconformity with such processes, such processing shall not be deemed to be for a special case.⁷

Please also note that the interpretation of the aforementioned provision shall be strictly construed - only the specified information is outside the scope of the DPA, and the public authority remains

⁶ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (d) (2016).

⁷ See: National Privacy Commission, NPC Advisory Opinion No. 2021-018 (18 June 2021).

⁸ See: National Privacy Commission, NPC Advisory Opinion Nos. 2020-015 (24 Feb 2020) and 2021-028 (16 July 2021).

subject to its obligations as a personal information controller (PIC) under the DPA such as implementing security measures to protect personal data, upholding the rights of data subjects, and adhering to data privacy principles, among others.⁸

We further note that the PDEA is created under the Comprehensive Dangerous Drugs Act of 2002. Under the law, one of PDEA's powers and duties is the initiation of investigative operations related to drug related activities, to wit:

“(b) Undertake the enforcement of the provisions of Article II of this Act relative to the unlawful acts and penalties involving any dangerous drug and/or controlled precursor and essential chemical and investigate all violators and other matters involved in the commission of any crime relative to the use, abuse or trafficking of any dangerous drug and/or controlled precursor and essential chemical x x x” (Underscoring supplied)

Thus, PDEA's request for personal data and transaction history of your identified client may fall under the processing of personal data under a special case as discussed above vis-à-vis its mandate.

Data sharing; data sharing agreements

A data sharing agreement (DSA) refers to a contract, joint issuance or any similar document which sets out the obligations, responsibilities, and liabilities of the PICs involved in the transfer of personal data between or among them, including the implementation of adequate standards for data privacy and security and upholding rights of data subject.

We note that the MOA you executed with PDEA may be considered as a form of DSA as majority of its provisions deal with further processing of personal data in your possession.

Indeed, although the execution of a DSA is not mandatory, it is still considered as a best practice as provided under NPC Circular No. 2020-03⁹, to wit:

“SECTION 8. Data sharing agreement; key considerations. – Data sharing may be covered by a data sharing agreement (DSA) or a similar document containing the terms and conditions of the sharing agreement, including obligations to protect the personal data shared, the responsibilities of the parties, mechanism through which data subjects may exercise their rights, among others.

⁹ National Privacy Commission, Data Sharing Agreements [NPC Circular No. 2020-03] (23 December 2020).

The execution of a DSA is a sound recourse and demonstrates accountable personal data processing, as well as good faith in complying with the requirements of the DPA, its IRR, and issuances of the NPC. The Commission shall take this into account in case a complaint is filed pertaining to such data sharing and/or in the course of any investigation relating to, as well as in the conduct of compliance checks.”

It is also important to note that data sharing may be based on any of the criteria for lawful processing of personal data in Sections 12 and 13 of the DPA and also in pursuant to Section 4 of the law which enumerates the special cases.

As discussed above, although DSAs are not mandatory, the execution of such agreement is encouraged as the same demonstrates accountability of the involved PICs.

General data privacy principles; proportionality

However, we emphasize that while there may be a legal ground in the granting of the request, the same shall only be to the minimum extent and in proportion to the purpose declared in their request, in keeping with the general data privacy principle of proportionality.

Thus, the disclosure should be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. These qualifiers serve as the measures by which a determination can be made on whether processing is proportional and justified in relation to the declared purpose. Further, this principle requires that personal data shall only be processed if the purpose of the processing could not reasonably be fulfilled by other means.

Therefore, indiscriminate disclosure of all personal data in your possession might not be the best recourse as this could be a violation of the principle of proportionality.

For this purpose, the company should check the different categories of personal data that it processes to have an initial determination of whether the disclosure thereof is relevant to the PDEA’s investigation based on the information in the letter request as well as the other discussions between the company and PDEA. Alternatively, the company may disclose to PDEA the categories of personal data that it has and ask PDEA for feedback on the particulars of what they need and how the same relates to the investigation.

Finally, please note that the discussions above pertain to the processing of personal data as provided for under the DPA, its IRR, and issuances of the NPC and do not encompass the appropriate requirements for the validity of a search and/or seizure of the contents of the parcel/s of your clients.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2022-007¹

28 February 2022



Re: **TRANSPORT OF PHYSICAL MEDIA CONTAINING
PERSONAL DATA**

Dear [REDACTED],

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC or the Commission) on whether the act of transporting physical media that may contain personal and sensitive personal information (collectively, personal data) is considered as “processing” of the personal data that are contained therein under existing data privacy legislation such as the Data Privacy Act of 2012² (DPA), its Implementing Rules and Regulations (IRR) and applicable NPC issuances.

We understand that your company is a courier and logistics company engaged in pick-up, transport and delivery of mails, letters, pouches, cargoes and personal effects of all kinds, wherein the collection and processing of the personal data of both the shipper (sender) and of the consignee (receiver) are necessary parts of its business.

Further, we understand that among the items that are endorsed to your company for delivery are physical media such as paper documents, laptops, and other data storage devices that may contain personal data.

¹ Tags: personal information controller; personal information processor; processing; personal information; liability; damages; accountability.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

You now come to the Commission to seek clarification on the following matters:

1. Whether the act of transporting physical media that may contain personal data be considered as “processing” of the personal data that are contained therein under the DPA, IRR and applicable NPC issuances?
2. Whether a courier company is liable under existing data privacy legislation in the event of loss or damage to the shipment of a physical media that contains personal data?
3. Can the data subject claim for damages from the courier company for data privacy breach if such data subject becomes a victim of identity fraud or identity theft arising from the lost or damaged shipment of a physical media that may contain personal data?

Personal information controller and processor; personal information; processing

A personal information controller (PIC) is the person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf.³ There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.⁴

On the other hand, a personal information processor (PIP) is any natural or juridical person to whom a PIC may outsource the processing of personal data pertaining to a data subject.⁵

Based on the definitions, and as described in your letter with regard to the business of your company, it is apparent that your company is a PIC with regard to the personal data of shippers (sender) and consignees (receiver) and should therefore comply with all of its obligations under the DPA.

However, there is a need to clarify and define its role and obligations with respect to its supervision or control over physical media that are endorsed to it for pick-up, transport and or delivery.

³ Data Privacy Act of 2012, § 3 (h).

⁴ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 3 (m).

⁵ Data Privacy Act of 2012, § 3 (i).

⁶ Id. § 3 (g).

The DPA defines personal information as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.⁶

Whereas processing of personal information, refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

Considering the above, physical media being transported may or may not contain personal data. In the instance that such contains personal data, the identity of an individual may or may not be apparent and cannot be ascertained by your company.

We should distinguish between situations wherein your company has knowledge or should have knowledge on whether the physical media endorsed to it for pick-up, transport and delivery contains personal data because such is apparent on its face or due to the nature of its engagement with the other PIC/s, such as but not limited to the pick-up, transport and or delivery of credit cards, credit card statements, bills, passports, civil registry documents, and the like.

As for transactions wherein your company has no way of knowing whether the physical media endorsed to it for pick-up, transport and delivery contains personal data, it cannot be said outright that your company is engaged in personal data processing. In these cases, the company would only be acting as a PIC in relation to the personal data of the shipper (sender) and consignee (receiver).

In addition, we must emphasize that in order for the company to be considered as a PIP in this instance, the PIC-consignor has to declare that the physical media contains personal information and that there is likewise the declaration that it is acting as a PIC and the intention of the transaction is to make the company a PIP. However, in transactions wherein the consignor is an individual who holds, processes, or uses personal information in connection with one's personal, family, or household affairs, the company, cannot be considered as a PIP, as in this situation the law provides that in such an instance, the individual involved is not considered as a PIC.

Therefore, to determine the company's role in transporting physical media, the above declarations from the consignor should be made in an appropriate form provided by the company.

Determination of liability; loss or damage physical media which contains personal data

The determination of liability in the event of loss or damage to the transportation of physical media which contains personal data would generally be covered by the ordinary terms and conditions of a given service, or some other law or regulation applicable to a courier for any normal loss, damage, and or destruction to the physical media endorsed to it for pick-up, transport and delivery.

The same will not automatically constitute a data privacy violation under the DPA. Following the discussion above, this determination will depend on whether the company is acting as a PIP or not either because it knew or should have known that the physical media contains personal data or pursuant to its contract with its PIC. In the latter case, its liability may be determined based on the specific terms of its contract with its PIC and its level of compliance with its duty as a PIP.

Specific to loss or damage, we refer further to Sections 26 of the DPA on Accessing Personal Information and Sensitive Personal Information Due to Negligence. If the loss or damage resulted in allowing an unauthorized person to have access to the personal information contained in the physical media through negligence, the determination of the presence of negligence and the ensuing liability may depend on whether the company is transporting the physical media as a PIP.

Damages for personal data breach; principle of accountability

As to the claim of damages by data subjects, the determination of liability and indemnification for any damages sustained are made on a case-to-case basis.

We reiterate that pursuant to the principle of accountability under Section 21 of the DPA, each PIC is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. Whereas, the PIP has the duty to comply with the requirements of the DPA, its Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract or other legal act with a PIC.⁷

Further, the DPA IRR provides that the PIC and PIP shall implement reasonable and appropriate security measures for the protection of personal data⁸ and shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.⁹ Such measures should be implemented to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

As discussed, the liability of the company may also depend on certain factors: first, the personality of the consignor-shipper, whether the same is considered as a PIC under the DPA or not, and second, if the consignor-shipper declared to the company that the physical media contains personal data.

Lastly, it is suggested that the company consider implementing changes to its processes so that it is duly informed at the outset on whether a consignor is a PIC and that the intention of the transaction is to make the company a PIP, and whether particular items shipped contain personal data so that the appropriate safeguards can be implemented accordingly. This may be done through appropriate forms, by informing the consignor at the outset of what their role would be in the transport of the physical media, and by making it declare in the appropriate form, that it is the PIC and that the intention of the transaction is to make the company a PIP.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

⁷ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 45.

⁸ Id. § 25.

⁹ Id.

ADVISORY OPINION NO. 2022-008¹

2 March 2022



Re: **OBTAINING EMPLOYMENT RECORD OR CERTIFICATION FROM THE SOCIAL SECURITY SYSTEM**

Dear [REDACTED],

We write in response to your inquiry received by the National Privacy Commission (NPC or the Commission) to provide clarity on the permissibility of obtaining service records of individuals from the Social Security System (SSS) considering the provisions of the Data Privacy Act of 2012² (DPA).

From your email, we understand that VeritasPay Philippines, Inc. (VeritasPay) is a party to an ongoing labor case filed by its previous employees with the National Labor Relations Commission (NLRC) 1st Division. VeritasPay seeks to request a copy of records or certifications from the SSS indicating that the previous employees are now employed with another employer.

You now seek guidance from the Commission on the following queries:

1. Is it possible to request a copy of the record or certification from the SSS indicating that a previous employee is currently employed with another employer; and
2. Is the record or proof of employment classified as public record pursuant to Executive Order No. 2, Series of 2016 or Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies of Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Thereof (E.O. No. 2, s. 2016 on Freedom of Information in the Executive Branch).

¹ Tags: employee service record; protection of lawful rights and interest; court proceedings; legitimate interest.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

We further understand that the purpose for obtaining the record or proof of employment is for the company to properly pray in its next pleading for the NLRC 1st Division to provide a correct computation of monetary award and delete the period where the terminated employees are already employed with another employer, alleging it would be tantamount to double compensation and unjust enrichment enshrined in the New Civil Code.

Lawful processing; protection of lawful rights and interest in court proceedings

Any record of employment or service record may contain personal information and sensitive personal information of the employee concerned. The disclosure of such records must have legal basis under the DPA and existing laws.

In the present situation where there is a pending labor case with the NLRC, and the request for the employment records or certification is necessary for proper litigation of VeritasPay's defense, the disclosure of such records may find ground under Sections 12 and 13 of the DPA, viz:

SEC. 12. Criteria for Lawful Processing of Personal Information. The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
x x x

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

...

SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: x x x

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.³ (emphasis supplied)

However, while it appears there exists justification for the disclosure of personal data, the DPA mandates that the principle of proportionality should still be adhered to. Proportionality requires that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.⁴

³ Data Privacy Act of 2012, §§ 12 (f) & 13 (f).

⁴ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).

Given the foregoing, while there may be lawful basis for obtaining the employment records, based on the purposes stated in your inquiry, it appears that only specific facts of employment are necessary for VeritasPay's defense in the NLRC case, such as the fact of employment, name of employer and period of employment. These pieces of information may be given by the SSS through a certification. It need not provide a copy of the entire record of employment of the concerned employees.

Record or proof of employment; processing of public record under the scope of the DPA

On the question of whether the employment record is considered as public record under E.O. No. 2, s. 2016 on Freedom of Information in the Executive Branch, the NPC may not be the proper agency to determine its status as a public record since this is dependent on the law of SSS, rules and regulations, as well as E.O. No. 2. However, even if such records were classified as public records, the processing of the same is still within the scope of the DPA and its related issuances.

Likewise, the Inventory of Exceptions to EO No. 2 (S. 2016)⁵ includes information deemed confidential for the protection of the privacy of persons as an exception to the general rule of disclosure in the right of access to information. The employment records contain personal data and the disclosure of the same must be in accordance with the DPA and other existing laws and regulations.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

⁵ Office of the President, Inventory of Exceptions to Executive Order No. 2 (S. 2016), Memorandum from the Executive Secretary (Nov. 24, 2016).

ADVISORY OPINION NO. 2022-009¹

2 March 2022



Re: **PUBLICATION OF FORMER EMPLOYEES' NAMES AND SEVERANCE FROM EMPLOYMENT**

Dear [REDACTED],

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC or the Commission) on whether publishing former employees' names and the fact of severance of their employment would violate the Data Privacy Act of 2012 (DPA).

From your letter, we understand that your company, a banking institution, experienced isolated cases wherein the bank's former employees had misrepresented to existing clients (e.g., branch clients) that they were still authorized to transact on the bank's behalf. Those former employees would solicit deposits from these clients, sell bank products to extort money or do fraudulent acts such as asking clients to transfer money to their accounts which they would misappropriate for themselves.

We understand further that to curtail these incidents and to protect the interest of the bank and its clients, it is suggested that there be a publication or dissemination of a statement limited to the former employee's name and his/her severance from employment with the bank through channels of general circulation like newsletters, bank website, official social media account and or within the bank branches or premises.

¹ Tags: criteria for lawful processing; general data privacy principles; legitimate interest.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

You now come to the Commission for guidance on the following inquiries:

1. Whether the publication of employee names and the fact of severance of employment would be lawful under Section 12 (f) of the DPA; and
2. Whether it would be lawful for the bank as an alternative measure to notify its clients privately and directly, through bank authorized modes of communication, of the severance of employment of such former employee.

Public disclosure of cessation of employment; Section 12 (f); legitimate interest; fraud prevention

The DPA recognizes the processing of personal and sensitive personal information (collectively, personal data), provided the requirements of the law are complied with and subject to the adherence of the data privacy principles of transparency, legitimate purpose, and proportionality.³

Under the DPA, the names of the employee and the fact that they are no longer employed are classified as personal information, the processing of which may be based on any of the lawful bases under Section 12. Specifically in this instance, Section 12 (f) of the DPA provides that the processing of personal information is allowed if the same is necessary for the purpose of the legitimate interests pursued by the personal information controller (PIC) or by a third party:

SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
x x x

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

³ Data Privacy Act of 2012, § 11.

⁴ See: National Privacy Commission, Advisory Opinion Nos. 2022-002 (Feb. 11, 2022), 2021-10 (March 22, 2021) and 2020-50 (Nov. 26, 2020) citing Data Privacy Act of 2012, § 12 (f) and United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimateinterests/what-is-the-legitimate-interests-basis/>.

⁵ See: National Privacy Commission, Advisory Opinion Nos. 2022-002 (Feb. 11, 2022) citing Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

In the determination of legitimate interest, the following must be considered:⁴

1. Purpose test – The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve;
2. Necessity test – The processing of personal information must be necessary for the purpose of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test – The fundamental rights and freedoms of data subjects must not be overridden by the legitimate interests of the PIC or third party, considering the likely impact of the processing on the data subjects.

Indeed, legitimate interest as a ground for lawful processing of personal information is a flexible concept that may be applicable in certain instances where processing will not have unwarranted impacts on the rights and freedoms of data subjects.⁵

We note as well that although the DPA does not particularly identify matters to be considered in the PIC's determination of its legitimate interests, the EU General Data Protection Regulation (GDPR), the successor of the EU Data Protection Directive (Directive 95/46/EC) which highly influenced the DPA, provides guidance whereby the processing of personal information strictly necessary for fraud prevention purposes constitutes a legitimate interest.⁶

In this instance, the PIC must establish that the disclosure of personal information will strictly be for the resolution of previously committed frauds and the prevention of potential frauds. Further, the PIC must ensure that only personal information which are necessary and proportionate to the declared legitimate interest may be processed, considering the rights and freedoms of the data subjects.

In any case, PICs that consider relying on this basis should undergo a legitimate interest assessment using the tests as guidance and document the outcome of the assessment. This gives data subjects some guarantee that this criterion for processing will not be misused.⁷

General data privacy principles; proportionality

While there may be a lawful basis for the publication of personal information such as employee names and the fact of severance from employment with the bank (i.e., “This person is no longer connected with the bank.”), the DPA mandates that the principle of proportionality should still be adhered to. Hence, disclosing the name and the fact that the employee is no longer employed with the bank is sufficient to meet the stated purpose. Any other information beyond that may be considered disproportional.

This principle requires that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. These qualifiers serve as the measures by which a determination can be made on whether processing is proportional and justified in relation to the declared purpose. Further, this principle requires that personal data shall only be processed if the purpose of the processing could not reasonably be fulfilled by other means.

Given that the bank has determined an alternative measure of notifying its clients individually through bank authorized modes of communication, this option should also be taken into account in its assessment of whether public disclosure or publication is proportional.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2022-010¹

14 July 2022



Re: **REQUEST FOR OPINION ON PRIVACY MATTERS CONCERNING TRANSFER OF ASSETS/LIABILITIES**

Dear [REDACTED],

We respond to your request for an Advisory Opinion on whether Citibank, N.A., Philippine Branch can validly transfer the personal information of non-responsive depositors to Union Bank of the Philippines pursuant to the Share and Business Transfer Agreement (“SBTA”).

We understand that, Union Bank of the Philippines (the “Buyer”) and Citibank, N.A., Philippine Branch (the “Seller”), together with other affiliates of the Seller, entered into a Share and Business Transfer Agreement (“SBTA”) for the proposed acquisition by the Buyer of certain assets and liabilities of the Seller’s constituent business in the Philippines as well as other assets (the “Transaction”). The Transaction includes the Seller’s local credit card, unsecured lending, and deposit businesses.

We understand further, that the processing, profiling, and sharing of data and information of the Seller’s deposit customers are governed by the terms and conditions set out in its “CONSENT ON PROCESSING, PROFILING AND SHARING OF DATA AND INFORMATION” (the 2017 Data Privacy Terms) the pertinent portions of which, states:

PAR.(1): We agree that our application, enrollment, purchase, maintenance, access or continued use of any of [the Seller’s] products and services shall be deemed as our acceptance and agreement to be bound by the provisions of these terms. We hereby agree that all Personal Data (as defined under the Data Privacy Law of 2012 and its implementing rules and regulations), customer data and account or transaction information

¹ Tags: Consent

or records (collectively, the “Information”) relating to us with you from time to time may be processed, profiled or shared to, by and between [the Seller] and any of its affiliates and subsidiaries (collectively, [the “Seller”] or each of the Authority (foreign or domestic) or Data Recipients (whether in or outside the Philippines) and for the purposes as set out in [the Seller’s] Data Statement in force provided by you to us from time to time or for compliance with any law, regulation, government requirement, treaty, agreement or policy or as required by or for the purpose of any court, legal process, examination, inquiry, audit or investigation of any Authority. The aforesaid terms shall apply notwithstanding any applicable nondisclosure agreement. We acknowledge that such Information may be processed or profiled by or shared with jurisdictions which do not have strict data protection or data privacy laws. (Emphasis supplied.)

Paragraphs 5 and 6 of the customer consent section of the 2017 Data Privacy Terms also states:

PAR. (5) We consent, in connection with any proposed novation, assignment, transfer or sale of any of your rights and/or obligations with respect to or in connection with our account and any products, facilities and services available in connection with the account, to any novatee, assignee, transferee, purchaser or any other person participating or otherwise involved in such transaction, to the disclosure, to any such person, by you, of any and all Information which may be required in relation thereto.

PAR. (6) We understand and consent that the processing, profiling and sharing apply during the prospecting and application stages, as well as for the duration of and even after the rejection, termination, closure or cancellation of the account or relationship or Services (collectively “Termination”) for a period of at least ten (10) years from the Termination of our last existing account or relationship or that of the Relevant Individual as determined by you. Where you deem it necessary or are required to fulfill foreign and domestic legal, regulatory, governmental, tax, law enforcement and compliance requirements and disclosure to each of the Authority or Industry Organization, we understand and consent that the storage will be made even after a period of ten (10) years from such Termination until the final conclusion of any requirement or disclosure obligation, dispute or action. (Emphasis supplied.)

You also stated in your letter that the Seller’s deposit customers were requested to confirm their consent and adherence to the 2017 Data Privacy Terms stated above, upon the application for and availment of the Seller’s products and services. To date, 56,561 out of the Seller’s 61,986 deposit customers have accepted and expressly consented to the 2017 Data Privacy Terms. The remaining 5,425 deposit customers have not consented to the 2017 Data Privacy Terms but are covered by the “Legacy T&Cs. The relevant section of the Legacy T&Cs on sharing of customer information reads as follows:

TRANSFER AND PROCESSING OF INFORMATION

As required under Republic Act 10173 and other applicable laws and regulations, I authorize and give consent for the following: ...

- For the Bank to transfer, disclose, use and process my Personal and Account Information (including information that the Bank obtains from third parties, such as Credit Institutions and other financial or non-financial institutions), to, between and among its Authorized Third Parties (now referred to the “Receiving and Disclosing Parties”), Credit Institutions, other financial or nonfinancial institutions, or the outsourced service providers of such entities, wherever situated, or a Government Requirement, for any lawful purpose such as business development, data processing, analysis and management, surveys, product and service offers, account servicing, including rewards redemption and fulfilment, marketing activities, risk management purposes, collections purposes and reporting, use in employment checking (for financial institutions), and compliance with laws, regulations and policies or anti-money laundering, sanctions and/or the US Foreign Account Tax Compliance Act (FATCA), including withholding for purposes of the FATCA. In addition to the above, the Bank or any of the Receiving and Disclosing Parties may disclose any Information as may be required by any Government Requirement, and for compliance with any Government Requirement, or as required by or for the purposes of any audit or investigation of any authority. “Government Requirement” means any applicable law or regulation, legal, governmental or regulatory authority, or agreement entered into by the Bank and any governmental authority or between two or more governmental authorities (such law, regulation or authority may be domestic or foreign). (Emphasis supplied.)

We understand that the Seller has undertaken an information campaign and successfully sent notices (“first notice”) to its deposit customers commencing on or about 25 February 2022, through one or more of the following channels: courier, postage mail, email, SMS, branches, interactive voice response facility, recorded phone calls, the Seller’s online and mobile applications, and the Seller’s website (such notices, the “Notices to Depositors”). In the Notices to Depositors, the Seller advised its customers of the intended sale and transfer to the Buyer, and in addition to consenting to the transfer of their customer account to the Buyer, requested them to reaffirm their previous express consent to the 2017 Data Privacy Terms.

You also informed us, that the Seller sent another letter (“Second Notice”) to depositors who did not reply to the First Notice. In that letter, these depositors were advised that in the absence of any objection from the regulators:

(a) the depositors’ failure to respond or expressly object to the transfer and/or continued availment of the Seller’s products and services would be deemed their consent to the transfer of their accounts to the Buyer and a reaffirmation of their previous express consent to the 2017 Data Privacy Terms, and

(b) accordingly, the Seller will transfer their accounts and personal information to the Buyer upon the closing of the Transaction.

You further disclosed that to date, some 46,148 depositors, representing 74.4% of the Seller’s total depositors, have given their consent or signified their objection to the transfer of their accounts. For those who consented, the depositors also reaffirmed their previous express consent to transfer their personal information under the 2017 Data Privacy Terms to the Buyer. However, the remaining 15,838 depositors have not, to date, replied to the Notices to Depositors (the “Non-Responsive Depositors”).

These Non-Responsive Depositors may be further segregated as follows: Through the clarification letter you sent to us on 29 June

Classification	Number of Depositors	Description
1. Non-Responsive Depositors who have adhered to the 2017 Data Privacy Terms	11,483	Of the 15,838 Non-Responsive Depositors, 11,483 have consented to, and are bound by, the 2017 Data Privacy Terms. These Non- Responsive Depositors have been sent, on average, eleven (11) Notices to Depositors or reminders through one or more of the following channels: courier, postage mail, email, SMS, branches, interactive voice response facility, recorded phone calls, the Seller’s online and mobile applications, and the Seller’s website.

<p>2. Non-Responsive Depositors under “and/or” accounts that were originally subject to Legacy T&Cs, but where a co accountholder has expressly consented: (a) to the transfer of the account holders’ information to the Buyer, and (b) to be bound by the 2017 Data Privacy Terms</p>	<p>1,164</p>	<p>The processing, profiling and sharing of the personal information of 4,355 out of the 15,838 Non-Responsive Depositors were initially governed by the terms set out in the Seller’s August 2016 General Terms and Conditions Governing Accounts (the “Legacy T&Cs”). Of these 4,355 Non-Responsive Depositors, 1,164 depositors hold “and/or” accounts but, in response to the First Notice, at least one of the accountholders under such accounts have consented to the transfer of their accounts to the Buyer and to update their data privacy consent to the 2017 Data Privacy Terms.</p>
<p>3. Non-Responsive Depositors whose accounts are governed by the Legacy T&Cs.</p>	<p>3,191</p>	<p>Of the 4,355 Non-Responsive Depositors, 3,191 depositors continue to be governed by the Legacy T&Cs. Of this number, 2,180 are sole accountholders, while 1,011 are co-accountholders with a depositor who consented to the 2017 Data Privacy Terms.</p>

2022, we understand that the relevant sections of the T&Cs for the Seller’s Deposit and Cards/Loans products, as well as the 2017 Data Privacy Terms states:

	Cards & Loans	Deposits
General T&C's - Assignability Clause	You agree that we may assign, discount or transfer part or all of our rights and/or obligations under this Citi Card Agreement or under any Card transaction without any notice. In the event of such assignment, you agree not to assert set-off rights of any obligations we may owe you, against the assignee.	No assignability clause

	Cards & Loans	Deposits
General T&C's - Continued Use	You agree that your application, enrollment, purchase, maintenance, access or continued use of any of Citi's products and services shall be deemed as your acceptance and agreement to be bound by the provisions of these terms.	You agree that your application, enrollment, purchase, maintenance, access or continued use of any of Citi's products and services shall be deemed as your acceptance and agreement to be bound by the provisions of these terms.
General T&C's - Acceptance of updated T&Cs	We may make amendments to this Citi Card Agreement, including the fees, charges, and terms, at any time and will notify you of these changes accordingly. Your continued retention or use of the Card after we have given you notice of such changes means that you have accepted and agreed to the changes. If the amendments or changes are not acceptable to you, you may close your Card account by calling CitiPhone (8995 9999 in Metro Manila or 234 9999 in Metro Cebu).	From time to time, the Bank updates and amends its terms and conditions. The Bank will notify you of amendments to the Terms and Conditions that will not result to or pertain to fees being paid or charged on your Account through public notice such as posting the bank's official website and/or at a conspicuous place within the premises of the branch. On the other hand, the Bank will notify you of amendments to the terms and conditions that will result to or pertain to fees being paid or charged on your account through individual notice such as sending you correspondences or advisories to your last known postal or registered mail, courier delivery, electronic mail, text messages, telephone calls or other alternative modes of communication (e.g. messages for you that appears on your statement of account, etc.). If you do not agree with the revised or amendments to the terms and conditions of the Bank, you have the right to exit the contract without penalty provided that such right is exercised within thirty (30) days from receipt of

You thus seek clarification on the following:

1. Whether the Seller may validly transfer to the Buyer the personal information of the 11,483 Non-Responsive Depositors who have adhered to the 2017 Data Privacy Terms upon the completion of the Transaction, on the basis of their prior express consent to the 2017 Data Privacy Terms and the implied reaffirmation of such consent by their failure to object and continued availment of the Seller's products and services notwithstanding several Notices to Depositors/reminders sent?

2. Whether upon the completion of the Transaction, the Seller may validly transfer to the Buyer the personal information of the 1,164 Non-Responsive Depositors whose "and/or" accounts were originally subject to Legacy T&Cs, but where a coaccountholder has consented: (a) to the transfer of the account holders' personal information to the Buyer, and (b) to be bound by the 2017 Data Privacy Terms. UBP believes this is supported by the authority granted to any co-accountholder to act on behalf of the co-account holders under Deposit T&Cs, the express consent given by a co-accountholder to the updating of their data privacy consent to the 2017 Data Privacy Terms, and the provisions of paragraph 8 of the 2017 Data Privacy Terms in relation to Section 2.D of NPC Circular No. 2020-03, which grants any co-account holder the authority to update or reconfirm the data privacy consents of the accountholders?

3. Whether upon the completion of the Transaction, the Seller may validly transfer to the Buyer the personal information of the 3,191 Non-Responsive Depositors who have given their prior express consent (as set out in the Legacy T&Cs) to transfer their accounts and personal information to any other financial institution for any lawful purpose. This action is supported by their prior express consent to the Legacy T&Cs, the implied reaffirmation of such consent by their failure to object and continued availment of the Seller's products and services notwithstanding several Notices to Depositors/reminders, and, in the case of the 1,011 Non-Responsive

Depositors who are co-account holders with a depositor who consented to the 2017 Data Privacy Terms, the grounds set out in paragraphs 18 and 19?

4. Whether the seller may transfer to the buyer the personal information of its Non-Responsive Depositors with bounced notifications (wherein the seller could not confirm receipt of communications)?

5. Whether the seller may transfer to the buyer the personal information of its depositors with closed card/loan accounts?

The Seller may validly transfer to the Buyer the personal information of the 11,483 Non-Responsive Depositors who have adhered to the 2017 data privacy terms

For processing personal and sensitive personal information, this may be done pursuant to the applicable provisions of Section 12 and 13 of the DPA, to wit:

SECTION 12. Criteria for Lawful Processing of Personal Information. — The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: xxx xxx xxx

- (a) The data subject has given his or her consent;
- (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;

SECTION 13. Sensitive Personal Information and Privileged Information. — The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: xxx xxx xxx

- (a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
- (b) The processing of the same is provided for by existing laws and regulations: Provided, that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information; xxx xxx xxx.”

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and, the Private Sector, Creating for this purpose a National Privacy Commission and for other Purposes [DATA PRIVACY ACT OF 2012], Republic Act No. 10173 (2012)., §3(b).

From the foregoing, it is worthy to note that lawful processing is not always anchored or based on the presence of consent as there are other criteria which may be more appropriate and may be invoked by the personal information controller as contemplated above.

Under Section 3(b) of the DPA, consent is defined as any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so. From the definition provided above, it is clear that consent must be evidenced by written, electronic, or recorded means.²

The NPC would like to reiterate that implied or inferred consent is not recognized in this jurisdiction. The entity, as personal information controller or personal information processor must never assume the data subject's consent for any activity involving his or her personal information, most especially, sensitive personal information, unless circumstances permit the processing of personal or sensitive personal information without consent, pursuant to the DPA and the IRR.

In this instance, we understand that as far as the 11,483 Non-Responsive Depositors is concerned, the basis of processing their personal data would be based on the 2017 Data Privacy Terms of the Seller, to which they have expressed their consent and hence they are bound thereto. The pertinent provisions of which states:

PAR. (5) We consent, in connection with any proposed novation, assignment, transfer or sale of any of your rights and/or obligations with respect to or in connection with our account and any products, facilities and services available in connection with the account, to any novatee, assignee, transferee, purchaser or any other person participating or otherwise involved in such transaction, to the disclosure, to any such person, by you, of any and all Information which may be required in relation thereto.

PAR. (6) We understand and consent that the processing, profiling and sharing apply during the prospecting and application stages, as well as for the duration of and even after the rejection, termination, closure or cancellation of the account or relationship or Services (collectively "Termination") for a period of at least ten (10) years from the Termination

of our last existing account or relationship or that of the Relevant Individual as determined by you. Where you deem it necessary or are required to fulfill foreign and domestic legal, regulatory, governmental, tax, law enforcement and compliance requirements and disclosure to each of the Authority or Industry Organization, we understand and consent that the storage will be made even after a period of ten (10) years from such Termination until the final conclusion of any requirement or disclosure obligation, dispute or action. (Emphasis supplied.)

Consent should cover all processing activities carried out for the same purpose or purposes. We maintain that as long as the purpose, scope, method and extent of the processing remains to be the same as that disclosed to the data subject when consent was given,³ the consent given by the non-responsive depositors upon agreeing to the 2017 Data Privacy Terms of the Seller remains to be valid.

Additionally, the processing of the personal information of the 11,483 Non-Responsive Depositors may also be based on the existing contract that the Seller has with its depositors. We clarify that, while there is a lawful criteria for processing based on contract in section 12 of the DPA, this does not appear in section 13. Considering, however, that consent is an essential element of contracts, in the past, the Commission has applied the lawful criteria of consent under Section 13 to also include contracts as long as the contract referred still complies with the requirements for consent under the DPA.

We note that in cases where consent is not required, a privacy notice would be sufficient. However, we wish to emphasize that a privacy notice is not equivalent to consent. This document is an embodiment of the observance of the data privacy principle of transparency and upholding the right to information of data subjects.

You mentioned that the Seller has notified the affected data subjects of the proposed transfer of their personal information to the buyer by sending them eleven (11) notices as of present date. Considering the foregoing, we affirm that such notices comply with the principle of transparency adhered to by the DPA which dictates that the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised.

³ NPC Advisory Opinion No. 2018-058.

Finally, the personal information controller is not required to obtain a separate consent from the data subject as long as the purpose, scope, method and extent of the processing remains to be the same as that disclosed to the data subject through the privacy notice and the processing is still covered by the consent given or the processing does not go beyond what the applicable law or regulation requires.

The Seller may validly transfer to the Buyer the personal information of the 1,164 Non-Responsive Depositors whose “and/or” accounts were originally subject to Legacy T&Cs, but where a co-account holder has consented

As to the 1,164 Non-Responsive Depositors whose “and/or” accounts were originally subject to Legacy T&Cs but where a co-account holder has consented, we affirm that the Seller may likewise validly transfer to the buyer their personal information, considering that the processing of their personal information is based also on the Seller’s 2017 Data Privacy Terms which states:

“a co-account holder is specifically authorized to reconfirm and update their data privacy consent to the 2017 Data Privacy Terms and the consents under such terms.”

In addition, thereto, “The “Joint Account” section of the General Terms and Conditions Governing [the Seller’s] Philippines Account (“Deposit T&Cs”) applicable to the Seller’s bank accounts provides that:

“Your Joint Accounts authorize [the Seller] to accept, to pay, or to act upon the order of any of the co-account holders or signatories indicated in the Signature Card, upon written or oral instruments from any one of you, and automatically vests in any of you to do whatever is desired with the funds without the consent of the other co-account holders.”

As previously discussed, there are several criteria for processing personal and sensitive personal information under Sections 12 and 13 of the DPA. We must emphasize that the aforementioned criteria as discussed is applicable as well to these 1,164 Non-Responsive Depositors whose “and/or” accounts were originally subject to Legacy T&Cs.

Therefore, the authority granted to any co-account holder to act on behalf of the co-account holders under the Seller’s Deposit T&Cs, as well as the consent given by a coaccount holder to the updating of their data privacy consent to the 2017 Data Privacy Terms allows the seller to process and transfer the personal information of the 1,164 Non-Responsive Depositors in this case to the buyer.

The Seller may validly transfer to the Buyer the personal information of the 3,191 Non-Responsive Depositors whose accounts are governed by the Legacy T&Cs

The remaining 3,191 Non-Responsive Depositors are those whose accounts are governed by the Legacy T&Cs. As mentioned in your letter, the Legacy T&C provide that these 3,191 depositors authorize the Seller to transfer their personal information to other financial institutions for any lawful purpose.

The relevant portion of the Seller's Legacy T&C states:

As required under Republic Act 10173 and other applicable laws and regulations, I authorize and give consent for the following: ...

For the Bank to transfer, disclose, use and process my Personal and Account Information (including information that the Bank obtains from third parties, such as Credit Institutions and other financial or non-financial institutions), to, between and among its Authorized Third Parties (now referred to the "Receiving and Disclosing Parties"), Credit Institutions, other financial or nonfinancial institutions, or the outsourced service providers of such entities, wherever situated, or a Government Requirement, for any lawful purpose...

xxx

In addition, there are existing provisions in the Seller's T&C which provide:

xxx You agree that your application, enrollment, purchase, maintenance, access or continued use of any of Citi's products and services shall be deemed as your acceptance and agreement to be bound by the provisions of these terms xxx

It is evident from the prior discussions, that the transfer of the personal information of these Non-Responsive Depositors should comply with any of the of the various criteria for lawful processing under the DPA, specifically under Sections 12 or 13 of the law. Both the Seller and the Buyer may be allowed to process personal data based on the above provisions, and the consent of the Non-Responsive Depositors is no longer required in the conduct of due diligence and in the implementation of the planned transfer.

In addition, we clarify that the fact of the continuity of use by the data subject of a personal information controller's services does not automatically signify one's consent. The personal information controller should be able to prove that such act of the data subject/s constitutes their consent.

We note that in this case the data subjects herein agreed to the provisions of the T&Cs stated above. Aside from this, the Seller sent numerous notices and reminders through one or more of the following channels: courier, postage mail, email, SMS, branches, interactive voice response facility, recorded phone calls, the Seller's online and mobile applications, and the Seller's website. Notwithstanding such notices and reminders, the data subjects did not respond. Hence, the Seller sent a "Second Notice" to the data subjects wherein the depositors were advised of the intended transfer to the Buyers and that if they fail to object to the transfer and/or continue to avail of the Seller's products and services, they will be deemed to have consented to the transfer and to have full knowledge of, and acceded to, the transfer.

As such, the transfer of the personal information of the 3,191 Non-Responsive Depositors, who continued availing of the Seller's products and services, finds basis in the T&Cs previously consented to by these data subjects taking into consideration the efforts exerted by the Seller to notify and remind them.

The Seller may validly transfer to the Buyer the personal information of its Non-Responsive Depositors with bounced notifications

In your clarificatory letter dated 29 June 2022, you stated that the Seller has nonresponsive depositors with bounced notifications, whom it could not confirm their receipt of the various communications sent but who are nevertheless covered by the 2017 Data Privacy terms and/or the Legacy terms on the disclosure of information.

In this instance, the various criteria for lawful processing under the DPA, specifically under Sections 12 or 13 of the law as discussed above also applies to these non-responsive depositors with bounced notifications. We emphasize that Processing of personal information may be based on consent, contract, legal obligation, legitimate interest, among others. Similarly for sensitive personal information, the processing thereof may be based on consent, law or regulation, legal claims, among others.

Given the foregoing, we clarify that as long as the scope, method, purpose, and extent of the processing as contained in the terms and conditions, privacy policies, and policies on the processing of

information provided by the PIC to their data subjects at the time the consent was given remains the same, the consent given by the data remains to be valid as well.

Therefore, we conclude that the personal information of these data subjects (non-responsive depositors and/or card / loan accounts with bounced notifications) may be transferred by the Seller to the Buyer, as the consent given by the data subjects herein applies to this Transaction, as is clearly agreed upon by the data subjects in the 2017 Data Privacy terms and/or the Legacy terms on the disclosure of information.

The Seller may validly transfer to the Buyer the personal information of its data subjects with closed card/ loans account

There are also those data subjects who have closed card/loan accounts but who are likewise covered either by the Seller's T&C's enabling the Seller to assign its rights and obligations without any notice or the 2017 Data Privacy Terms which allows the disclosure of information to an assignee and allows the Seller to process the data subject's information up to 10 years following termination or closure of the account for various purposes, such as customer servicing, remediating customers' and/or regulatory claims/refunds as well as other compliance requirements.

In this case, the previous discussions with regard to the various criteria for lawful processing under the DPA, specifically under Sections 12 or 13 of the law as discussed also applies to these data subjects.

We note that in this case, the personal information of herein data subjects may be transferred by the Seller to the Buyer given that the data subjects have consented to the processing of their information up to 10 years following termination or closure of the card account, for various purposes, such as customer servicing, remediating customers' an/or regulatory claims/refunds and compliance to obligation as a card issuer etc. as stated in the Seller's 2017 Data Privacy Terms.

In addition, the herein data subjects have also agreed to the provisions in the Cards T&C of the Seller, which enables the Seller

to assign its rights and/or obligations without any notice. However, we note that despite such provision, the Seller still sent out notices to the herein data subjects to inform them of the Transaction with the Buyer.

Given the foregoing, the consent given by the data subjects in either of the aforementioned terms and conditions remains to be valid in this instant case, as the herein Transaction involves the transfer of the Seller's local credit card, unsecured lending, and deposit businesses to the Buyer, which means that the purpose, scope, method and extent of the processing of personal data, would remain to be the same as to what the data subjects have consented to.

As a general rule, as long as the scope, method, purpose, and extent of the processing as contained in the terms and conditions, privacy policies, and policies on the processing of information provided by the PIC to their data subjects at the time the consent was given remains the same, the consent given by the data remains to be valid as well.⁴

Please be advised that this Advisory Opinion was rendered based solely on your provided information. Any extraneous fact that may be subsequently furnished to us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)

FRANKLIN ANTHONY M. TABAQUIN IV

Director IV, Privacy Policy Office

⁴ NPC Advisory Opinion No. 2018-058.

ADVISORY OPINION NO. 2022-011¹

19 August 2022



Re: **PERSONAL DATA RETENTION AND DELETION**

Dear [REDACTED],

We respond to your inquiry regarding the request of a client of Flexi Finance Asia Inc. (FFAI) to delete his personal data from its system.

We understand that FFAI is a financing company that processes basic credit information of its clients, including their personal data as defined in the Data Privacy Act of 2012 (DPA).³ Under the Credit Information System Act (CISA),⁴ FFAI is required to retain the data of its clients for reporting to the Credit Information Corporation (CIC).

You also cite relevant provisions of FFAI's Loan Contract with the client that allows it to retain personal data, *to wit*:

b. Retain my personal information within the period as may be allowed for by law from the date of the termination of my loan contract subject to the discretion of the company. The company may use such information for any legitimate purpose but always in compliance with prevailing and to be enacted laws and regulations.

c. Retain my information in the database of the company with the latter having the right to share the same to all its affiliates and necessary third parties for any legitimate business purpose subject to the assurance by the company that proper security systems are in place to protect my information.

¹ Tags: data subject's rights; right to erasure; data retention.

³ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for other purposes [Data Privacy Act of 2012] Republic Act No. 10173 (2012).

⁴ An Act Establishing The Credit Information System And For Other Purposes [Credit Information System Act] Republic Act No. 9510 (2008).

However, the client did not substantiate his/her deletion request with any of the circumstances mentioned in Section 16 (e) of the DPA.

You thus seek guidance on the following:

1. Whether FFAI can compel the client to provide proof of the circumstances provided in Section 16 (e) of the DPA;
2. The number of years that the FFAI can retain its clients' data; and
3. If there is any violation if FFAI does not delete the client's data as requested.

Considering that your questions are interrelated, we shall discuss them jointly.

Personal Data; Basic Credit Information; Data subject rights; Right to Erasure; Limitations.

At the outset, we note that your query is silent as to the type of data involved in the client's request. Thus, we deem it prudent to discuss the difference between personal information and sensitive personal information (collectively, personal data) for proper perspective.

The DPA defines Personal Information as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.⁶

On the other hand, Sensitive Personal Information refers to personal information:

- (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
- (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
- (4) Specifically established by an executive order or an act of Congress to be kept classified.⁷

⁶ Data Privacy Act, § 3 (g)

⁷ Id., § 3 (l)

The bases for permissible processing of the two types of personal data differs. Section 12 of the DPA provides for the criteria for lawful processing of Personal Information:

SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

- (a) The data subject has given his or her consent;
- (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
- (d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
- (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
- (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

On the other hand, Section 13 of the DPA enumerates the circumstances when Sensitive Personal Information may be processed:

SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

- (a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
- (b) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are

not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing;

(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

In relation to Section 12 (c) and 13 (b) of the DPA, FFAI must additionally comply with the provisions of the CISA in processing the Sensitive Personal Information of its clients since processing based on a legal obligation requires that all conditions imposed by the legal obligation have been complied with as discussed in NPC Resolution 18-010, viz:

“Processing based on a legal obligation requires that all conditions imposed by the legal obligation have been complied with. Section 12 (c) of the DPA requires not only that the processing is “necessary” but also that it be in “compliance with a legal obligation”. Compliance with everything required by the claimed legal obligation as a condition for the processing is an essential element for any claim of valid processing under this criterion.”⁸

Under the CISA, entities providing credit facilities are required to submit credit information of its borrowers and thereafter update the same on a regular basis to the CIC.

The Implementing Rules and Regulation (IRR) of the CISA also require submitting entities to submit current, objective, factual, and basic credit data, both positive and negative, on all their data subjects.¹¹ Basic Credit Data comprises the following:

4.4. Basic Credit Data. Every participating entity shall submit to the Corporation the following basic credit data on all data subjects:

a) Individual

- i. Personal circumstances such as name (last, first, middle), date of birth, sex, civil status, present residence, employer and position or business, as the case may be;
- ii. Number of children depending for support;
- iii. TIN, SSS or GSIS No.;
- iv. Net income;
- v. Residence for the last 2 years;
- vi. Employer/s or business/es for the last 5 years;
- vii. Owners/lessee of house occupied;
- viii. Car/s owned;
- ix. Bank/s where accounts are maintained, including types of bank accounts; and
- x. Other assets, real or personal.¹²

The IRR of the CISA also provides the data that comprises Negative Information of data subjects. The IRR provides:

The IRR of the CISA also provides the data that comprises Negative Information of data subjects. The IRR provides:

4.5. Negative Information

The Corporation's credit information database shall likewise contain negative information which shall include, among others, the following:

- a) Past due;
- b) Default/s on loan/s;
- c) Details of the settlement of loans that defaulted;
- d) Foreclosures;
- e) Adverse court judgments relating to debts;
- f) Report on bankruptcy or insolvency;
- g) Petition or order on suspension of payments;
- h) Corporate rehabilitation;
- i) Other pending court cases (either as plaintiff or defendant) related to credit transactions or cases that will affect the financial capacity of the borrower;
- j) Inclusion in a bouncing check checklist;
- k) Cancelled credit cards; and
- l) Such other information that may be determined by the Corporation.¹³

⁸ National Privacy Commission, NPC Resolution 18-010

¹¹ Implementing Rules and Regulation of the Credit Information System Act (CISA) Republic Act No. 9510, § 4 (1) (2009)

¹² Id., § 4 (4)(a) (2009)

In view of the foregoing, aside from Personal Information, some of the personal data required to be submitted and/or retained by submitting entities pursuant to the CISA qualifies as Sensitive Personal Information. This can serve as guide on the type and the limits of the processing that FFAl may perform on the personal data of its clients.

Be that as it may, please note that regardless of the nature of the personal data involved, the DPA recognizes certain rights in favor of the data subject. Relevant to your query are the rights to suspend, withdraw, or order the blocking, removal, or destruction of his or her data from the personal information controller's (PIC) filing system, subject to specified conditions as stated in Section 16 (e) of the DPA.

The NPC provided further guidance on the matter through NPC Advisory No. 2021 – 01 on Data Subject Rights.¹⁵ Section 10 thereof provides:

SECTION 10. Right to Erasure or Blocking. — A data subject has the right to request for the suspension, withdrawal, blocking, removal, or destruction of his or her personal data from the PIC's filing system, in both live and back-up systems.

A. This right may be exercised upon discovery and substantial proof of any of the following:

1. The personal data is:
 - a) incomplete, outdated, false, or unlawfully obtained;
 - b) used for an unauthorized purpose;
 - c) no longer necessary for the purpose/s for which they were collected; or
 - d) concerns private information that is prejudicial to the data subject, unless justified by freedom of speech, of expression, or of the press, or otherwise authorized;
2. The data subject objects to the processing, and there are no other applicable lawful criteria for processing;
3. The processing is unlawful; or
4. The PIC or PIP violated the rights of the data subject.

Further, the same advisory provided grounds for denying requests for erasure or blocking by a Data Subject, viz:

2.Denial of Request. A request for erasure or blocking may be denied, wholly or partly, when personal data is still necessary in any of the following instances:

¹³ Id., § 4 (5) (2009)

¹⁵ National Privacy Commission, Data Subject Rights [NPC Advisory No. 2021 – 01] (January 29, 2021).

- a.) Fulfillment of the purpose/s for which data was obtained;
- b) Compliance with a legal obligation which requires personal data processing;
- c) Establishment, exercise or defense of any legal claim;
- d) Legitimate business purposes of the PIC, consistent with the applicable industry standard for personal data retention;
- e) To apprise the public on matters that have an overriding public interest or concern, taking into consideration the following factors:
 - i. Constitutionally guaranteed rights and freedoms of speech, of expression, or of the press;
 - ii. Whether or not the personal data pertains to a data subject who is a public figure; and
 - iii. Other analogous considerations where personal data are processed in circumstances where data subjects can reasonably expect further processing.
- f) As may be provided by any existing law, rules, and regulations.”

Additionally, the IRR of CISA also provides for Data Subject rights which necessarily includes the right to dispute and erasure, viz:

4.6. Rights of Data Subjects

- a) A borrower shall have the right to have ready and immediate access to credit information pertinent to him subject to the payment of a prescribed fee;
- b) He shall have the right to dispute erroneous, incomplete or misleading credit information;
- c) He shall be entitled to a simplified dispute resolution process to fast track the settlement/resolution of disputed credit information;
- d) He shall be informed of any correction or removal of any erroneous, incomplete or misleading information within 5 working days from verification or conclusion of an investigation or from deletion of the disputed information, as the case may be;
- e) He shall be entitled to indemnity in case of denial, without justification, of the aforementioned rights;
- f) He shall be notified by a submitting entity of the latter’s obligation to submit and disclose basic credit data to the Corporation; and
- g) He shall have the right to know the causes of refusal of an application for credit facilities or services from a financial institution that uses credit data as basis or ground for such refusal.¹⁸

Further, CIC Circular No. 2015-01¹⁹ lays down the obligations of a submitting entity under the CISA, viz:

4.6 The Submitting Entity shall regularly submit the Basic Credit Data of all its Borrowers contained in its data base, file or system, to the CIC not later than on the 5th day of the month and in the form/format and manner prescribed by the CIC.

4.7 The Submitting Entity shall ensure that the Basic Credit Data of all its borrowers with the CIC is accurate, complete, correct, and current up to the relevant Update Cycle Date.

4.8 The Submitting Entity shall ensure that when receiving Error Reports from the CIC, the Submitting Entity shall rectify errors in the relevant files and send the corrected files to the CIC within a period of three (3) working days. X x x”

In fine, while both the DPA and the CISA and all related issuances recognize the right of a Data Subject to request the deletion of his personal data, the exercise of such right is not absolute. PICs, such as FFAL, may request the data subject to substantiate his/her request. However, FFAL is also obliged to observe the limits imposed by law as to the type of data and the conditions for its processing.

Data retention period; CISA requirements.

It must be emphasized that the DPA requires that personal data shall only be retained for as long as necessary for the fulfillment of the purposes for which the data was obtained; for the establishment, exercise or defense of legal claims; for legitimate business purposes; or as provided by law.²⁰ Other conditions for the retention of data are also provided in Sections 12 and 13 of the DPA.

The DPA further provides that personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined. NPC Advisory Opinion No. 2017-24 is instructive on this point, viz:

“From the foregoing, it is clear that the DPA and its IRR does not provide for a specific retention period. Instead, the law sets out the general principles and guidelines for the retention of personal data. As a general rule, records containing personal data should be retained only for as long as may be necessary for the purpose or purposes for which the personal data were collected.”

¹⁸ Implementing Rules and Regulation of the Credit Information System Act (CISA) Republic Act No. 9510, § 4 (6) (2009)

¹⁹ Credit Information Corporation, Enforcement of the Credit Information System Act Pursuant to Republic Act No. 9510 and its Implementing Rules and Regulations [Circular 2015-01] § 4.2 (15 May 2015)

²⁰ Data Privacy Act of 2012, § 11 (e).

Further, Section 19(d)(1) and (2) of the IRR of the DPA provides:

“d. Personal Data shall not be retained longer than necessary.

1. Retention of personal data shall only for as long as necessary:

- a) For the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
- b) For the establishment, exercise or defense of legal claims; or
- c) For legitimate business purposes, which must be consistent with standards followed by the applicable industry or appropriate government agency.

Retention of personal data shall be allowed in cases provided by law.”

Additionally, CISA provides a period of retention if the Basic Credit Data refers to a negative credit information, viz:

“A. Retention Period for Negative Information in the Database

Any negative information on a borrower shall stay in the Corporation’s database for not more than 3 years from and after the date the negative information shall have been rectified through the following:

- i. Payment or liquidation of debt; or
- ii. Settlement of debt through compromise agreement or court decision exculpating the borrower from any liability.

Negative information shall be corrected and updated within 15 days from receipt of notice of payment, liquidation or settlement of debt in accordance with the prescribed rules of the Corporation.”²¹

Thus, although PICs cannot retain personal data in perpetuity, the continued processing thereof may be permitted if it is anchored on Sections 12 and 13 of the DPA. And, if negative information is involved, FFAI must also comply with the three-year limitation provided in the CISA. Please note that the repurposing of Personal Data retained other than for what the law prescribes may constitute as a violation of the DPA.

DPA violation for denial of data subject rights.

²¹ Rules and Regulations Implementing the Credit Information Systems Act of 2008, Rule 4 (4.5) (A). (2009).

As mentioned above, the continued processing of the Data Subjects data and, in effect, the denial of the right to delete, may be justified pursuant to Sections 12 and 13 of the DPA in relation to CISA.

On this note, the existence of a lawful ground for processing does not give PICs an unbridled power to process personal data. PICs are still required under the law to observe the data privacy principles of legitimate purpose, transparency, and proportionality. In this regard, we observed that your contract provisions appear to violate some of the data privacy principles and hence cannot serve to justify the retention of the Data Subject's personal data.

You may want to revisit the contract provisions involved as it is inconsistent with the principle of transparency which requires that the data subject should be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, his or her rights as a data subject, and how these can be exercised.²³

Also, in accordance with the principle of proportionality, the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.²⁴

We emphasize that should FFAI deny or limit the exercise of data subject rights, it should ensure that the data subject is clearly and fully informed of the reasons for the denial or limitation.²⁵

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.
Very truly yours,

Sgd.
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

²³ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §18 (2016)

²⁴ Id.

²⁵ NPC Advisory No. 2021 – 01, § 14.

ADVISORY OPINION NO. 2022-012¹

19 August 2022



Re: **REMEDIES AGAINST THE ALLEGED DATA BREACH
INVOLVING WORKABROAD.PH (WORKABROAD)**

Dear ,

We respond to your 9 December 2021 letter requesting our Advisory Opinion on the above matter.

We draw from your letter that the Philippine Overseas Employment Administration (POEA) has received numerous reports of overseas employment job seekers falling victim to the “Please Read and Understand” online scam/illegal recruitment scheme. Under the said scheme, the sender uses the name and license number of a licensed recruitment agency (LRA) in text messages or e-mails informing OFW-applicant/s that they were selected for a job abroad. The OFW-applicant/s are then instructed to pay a fee – usually labeled as reservation fee, orientation fee, or coaching fee – through money transfer and remittance platforms like Western Union, Palawan Pawnshop, and Cebuano Lhuillier Pera Padala. The scammers have also modernized to include payment platforms such as GCash, PayMaya and 7-ELEVEN.

For the period 16 June up to 13 September 2021, the POEA’s Anti-Illegal Recruitment Branch (AIRB) received complaints and inquiries from OFW-applicant/s and LRAs regarding a variation of the scheme in which they were asked to remit PhP3,000 in exchange for reservation of a slot for deployment to Canada. The AIRB noticed that, from July to August 2021, the names used in the scam e-mail ran almost alphabetically or used LRA names starting with “P” through “S”. Of the eleven (11) victims who responded to the AIRB’s inquiry on where they provided their contact information, eight (8) mentioned WorkAbroad.

¹ Tags: Special Cases; fulfillment of mandate; public authority; data sharing; data sharing agreement;

In the case of Archway International and Marketing Services, Inc. (“Archway”), they reported the use of their agency’s name in the “Please Read and Understand” online scam for supposed deployment to Canada and the United Kingdom. Archway denies any involvement, and later reported that twenty-seven (27) applicants complained about the Php3,000 training/seminar fee they paid through GCash. Archway also reported that ten (10) applicants registered with WorkAbroad.

You state further that WorkAbroad is an affiliate of JobStreet, a popular online employment website/aggregator catering to countries in Asia. WorkAbroad’s primary market is the Philippines, particularly OFWs, LRAs, and their partner foreign employers/principals.

WorkAbroad is reputed to be a legitimate job search website for OFWs, LRAs, and foreign principals. Its website includes a feature in which the applicant can upload his/her resume while additional information may be collected and stored further in their database. Some LRAs are also registered with WorkAbroad where they post job openings. While the profile of a particular LRA may include its license number, such data will not appear when a search is made using the POEA’s public database.

Thus, you seek an Advisory Opinion on the following matters:

1. Whether the POEA may request WorkAbroad to disclose who has access to the applicant’s resumes and contact information?
2. Whether the POEA may share with another government agency, in particular the DOJ, the data that it will receive from WorkAbroad after the execution of a Data Sharing Agreement (DSA).

For proper perspective, we find it necessary to discuss the salient features of the Data Privacy Act of 2012 (DPA) and its related rules and issuances –

Special Cases; fulfillment of mandate; public authority;

The Implementing Rules and Regulations (IRR) of the DPA excludes from the scope of the law certain types of processing that are considered necessary due to its purpose, function, or the activity involved. In particular, Section 5 (d) of the IRR provides:

² An Act to Strengthen the regulatory functions of the Philippine Overseas Employment Administration (POEA), Amending for this purpose Republic Act No. 8042, otherwise known as the Migrant Workers and Overseas Filipinos Act of 1995, [R.A. No. 9422, § 1]

d. Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function...subject to restrictions provided by law...

We recognize that the POEA is legally mandated to regulate private sector participation in the recruitment and overseas placement of workers. It is also tasked to formulate and implement a system for promoting and monitoring the overseas employment of Filipino workers, taking into consideration their welfare and the domestic manpower requirements.² In addition to its powers and functions, it informs migrant workers not only of their rights as workers but also of their rights as human beings, instruct and guide the workers how to assert their rights, and provide the available mechanism to redress violation of their rights.³

Premised on the foregoing, the POEA's request to access the applicants' resumes and contact information from WorkAbroad may be anchored on Section 5 (d) of the IRR of the DPA, that is, as a fulfillment of its mandate to regulate the private sector's participation in the recruitment and placement of Overseas Filipino workers.

In addition, POEA's request falls under Sections 13(b) of the DPA, to wit:

SECTION 13. Sensitive Personal Information and Privileged Information. — The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

(b) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

For processing under Section 13 (b) cited above, the government or public authority may process information pursuant to the particular agency's constitutional or statutory mandate, and subject to the requirements of the DPA. In this case, the POEA's request for information is in prosecution of its mandate to be able to provide the available mechanism to redress the violation of the rights of the migrant workers.

³ Id.

⁴ National Privacy Commission, Data Sharing Agreements [NPC Circular No. 2020-03], 2 (F) (December 23, 2020).

⁵ Id. § 2(G)

Data sharing is defined under NPC Circular No. 2020-03 as the sharing, disclosure, or transfer to a third party of personal data under the custody of a personal information controller to one or more other personal information controller/s.⁴

On the other hand, a data sharing agreement (DSA) refers to a contract, joint issuance or any similar document which sets out the obligations, responsibilities and liabilities of the PICs involved in the transfer of personal data between or among them, including the implementation of adequate standards for data privacy and security and upholding the rights of the data subjects.⁵

Please note that under Section 8 of NPC Circular No. 2020-03, the execution of a DSA is not mandatory:

SECTION 8. Data sharing agreement; key considerations. — Data sharing may be covered by a data sharing agreement (DSA) or a similar document containing the terms and conditions of the sharing arrangement, including obligations to protect the personal data shared, the responsibilities of the parties, mechanisms through which data subjects may exercise their rights, among others. The execution of a DSA is a sound recourse and demonstrates accountable personal data processing, as well as good faith in complying with the requirements of the DPA, its IRR, and issuances of the NPC. The Commission shall take this into account in case a complaint is filed pertaining to such data sharing and/or in the course of any investigation relating thereto, as well as in the conduct of compliance checks.

While the execution of a DSA is optional, we still advise that the parties execute the same as a matter of best practice and for purposes of accountability.

We recognize that the establishment of the Shared Government Information System for Migration (SGISM) is provided under the Migrant Workers and Overseas Filipinos Act of 1995 (R.A. No 8042), as amended by Republic Act 10022, to wit:

SEC. 20. Establishment of a Shared Government Information System for Migration. - An inter-agency committee composed of the Department of Foreign Affairs and its attached agency,

³ Id.

⁴ National Privacy Commission, Data Sharing Agreements [NPC Circular No. 2020-03], 2 (F) (December 23, 2020).

⁵ Id. § 2(G)

the Commission on Filipino Overseas, the Department of Labor and Employment, the Philippine Overseas Employment Administration, The Overseas Workers Welfare Administration, The Department of Tourism, the Department of Justice, the Bureau of Immigration, the National Bureau of Investigation, and the National Statistics Office shall be established to implement a shared government information system for migration. The interagency committee shall initially make available to itself the information contained in existing data bases/files. The second phase shall involve linking of computer facilities in order to allow free-flow data exchanges and sharing among concerned agencies.

The inter-agency committee shall convene to identify existing data bases which shall be declassified and shared among member agencies. These shared data bases shall initially include, but not limited to, the following information:

- (a) Masterlists of departing/arriving Filipinos;
- (b) Inventory of pending legal cases involving Filipino migrant workers and other Filipino nationals, including those serving prison terms;
- (c) Masterlists of departing/arriving Filipinos;
- (d) Statistical profile on Filipino migrant workers/overseas Filipinos/Tourists;
- (e) Blacklisted foreigners/undesirable aliens;
- (f) Basic data on legal systems, immigration policies, marriage laws and civil and criminal codes in receiving countries particularly those with the large numbers of Filipinos;
- (g) List of labor and other human rights instruments where receiving countries are signatories;
- (h) A tracking system of past and present gender disaggregated cases involving male and female migrant workers;

In the present case, the above shared government information system for migration may be used as basis for the establishment of a DSA with the DOJ for the data that it will receive from WorkAbroad. Finally, we reiterate that the DPA, its IRR and other relevant issuances of the NPC are not meant to impede the regular functions of government agencies based on their mandates. The right to access personal data is regulated by the DPA and other applicable laws on the matter.

We hope that we have sufficiently addressed your concerns. Rest assured that the NPC is your partner in good governance. Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

Sgd.

FRANKLIN ANTHONY M. TABAQUIN, IV

Director IV, Privacy Policy Office

ADVISORY OPINION

NO. 2022-013¹

31 August 2022



Re: **ONLINE LENDING MOBILE APPLICATION PERMISSIONS**

Dear ,

We respond to your request for an Advisory Opinion on the compliance of your client's microloan mobile application with the Data Privacy Act of 2012 (DPA).²

We understand that your client, AND Financing Corporation (AND-FC), is a Philippine subsidiary of AND Global Pte of Singapore. AND-FC launched LendPinoy, a mobile application that provides microloans in the Philippines.

We note that LendPinoy will use an Artificial Intelligence (AI) credit scoring process to determine the creditworthiness of individual borrowers. To do this, LendPinoy intends to utilize two processes:

- 1) obtain access to SMS data of the would-be borrowers (data subjects); and
- 2) obtain access to the bank account details of the data subjects.

You thus seek clearance from the NPC on the foregoing processing of personal information.

Advisory Opinion as guidance

At the outset, we wish to clarify that Advisory Opinions of the National Privacy Commission (NPC) do not serve as a “clearance” to the processing of personal information by personal information controllers (PICs). As stated in NPC Circular No. 18-01 (Rules of Procedure on Requests for Advisory Opinions),³

¹ Tags: lawful processing of personal information; consent; general data privacy principles; privacy impact assessment; privacy-by-design.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

the NPC’s Advisory Opinions provide guidance to the requesting party and the general public on matters relating to the interpretation of the provisions of the DPA its Implementing Rules and Regulations (IRR), and NPC issuances, compliance requirements, enforcement of data privacy laws and regulations, and other related issuances on personal data privacy, security and protection.⁴

Nevertheless, we shall discuss hereunder certain matters we observed from your request.

Application permissions; general data privacy principles; proportionality; retention; NPC Circular No. 20-01

We note from the Privacy Impact Assessment on the SMS application (SMS PIA) that the following information will be processed within the application:

The program will collect, use, retain, disclose the following personal information.

	Personal Information	Y	N
1	Name	X	
2	Home Address	X	
3	Business Address	X	
4	Email Address	X	
5	Telephone Number - Mobile Number	X	
6	Telephone Number - Work	X	
7	Telephone Number - Home	X	
8	Age	X	
9	Date of Birth	X	
10	Marital Status	X	
11	Color, Race or Ethnic Origin	X	
12	Religion (Religious beliefs or affiliations)	X	
13	Education	X	
14	Photo	X	
15	Biometrics	X	
16	Political Association	X	
17	Philosophical Beliefs, Orientation	X	
18	Health	X	
19	Sexual life/preference/practice	X	
20	Offense committed or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings	X	
21	Issued by government agencies peculiar to an individual - unique identifiers (eg TIN, UMID ID no., Driver's License no., Passport no., GSIS, SSS numbers, Voter's registration no., etc.) - previous or current health records - licenses or its denials, suspension or its revocation - tax returns	X	
22	Specifically established by an executive order or an act of Congress to be kept classified	X	

Figure 1: Threshold Analysis SMS PIA

We likewise note from Section 1 of the SMS PIA on the Description of Program, Process, or Measure involving Personal Data, that once the data subjects accept the SMS permission, all saved SMS data in the device will be transferred to the AND-FC server securely.

We further note that in Section 3.2 on the Compliance with Information Privacy Principles, particularly the answers in relation to the questions on proportionality, that AND-FC answered in the negative to the following:

³ National Privacy Commission, Rules of Procedure on Requests for Advisory Opinions [NPC Circular No. 18-01] (10 September 2018).

⁴ NPC Circular No. 18-01 Section 5 (a).

1. Is the processing of personal information adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specific purpose; and
2. Is personal information being processed because the purpose of the processing could not be reasonably fulfilled by other means?

From the foregoing, there seems to be a recognition on the part of AND-FC that the personal information to be processed is not proportional to the purpose of the processing and that there are other less intrusive means to determine creditworthiness of the data subjects.

Such processing, therefore, does not conform to the data privacy principle of proportionality which provides that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose; and personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other less intrusive means.⁵

To comply with the said principle, AND-FC should evaluate the need to access and process SMS data of the data subjects as it may be disproportionate to the purpose of granting a loan to the data subjects.

Similarly, the harvesting of all SMS data of the data subjects appears to violate the principle of proportionality because this would entail the saving and transfer of the SMS data of the borrowers from the latter's mobile phones to the cloud servers of AND-FC and storing it there for a certain period. This processing activity may be deemed excessive and unrelated to the declared and specified purpose of determining the creditworthiness of data subjects.

We note that AND-FC intends to store the SMS data in its cloud servers not only for the purpose of credit-scoring⁶ but also for the purpose of credit scoring system improvement.⁷ The SMS data will also be disclosed to authorized personnel of AND-FC's parent company, AND Solutions PTE Ltd. to study and develop its credit

⁵ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).

⁶ See Table 3 – Information Flow – SMS Permission Privacy Impact Assessment

⁷ Ibid.

⁸ Ibid.

⁹ See Part 2 – Threshold Analysis, Table 2

scoring system⁸. These are additional purposes for the benefit of AND-FC that are neither essential nor necessary to the service sought to be availed of by the data subjects. In other words, processing for these purposes should be covered by a separate lawful basis.

We also note that the purpose of the request to access and harvest SMS data is to determine the creditworthiness of the data subjects and to possibly increase their credit limit. However, we also recognize that such SMS data may contain personal information, potentially including sensitive personal information, not only of the data subjects but also of third parties who have no connection to the loan agreement between AND-FC and the data subjects. As such, the data subjects to the loan agreement with AND-FC cannot give their consent for the third parties whose personal data may be in the SMS.

We further note that AND-FC intends to process SMS data that may contain any type of information⁹, which could include personal information and sensitive personal information, about the data subjects and third parties. We wish to point out that the legitimate interest of AND-FC and the borrower cannot serve as the basis for processing the data of third parties in this scenario since the right to privacy of the latter must prevail over the legitimate interest of AND-FC and the borrower.¹⁰ Consequently, the potential borrower should not disclose the information of third parties to AND-FC.

On the other hand, we note from the Access to Online Banking Financial Information [onetime read-only access] PIA (Online Banking PIA), that two additional information will be processed, namely: online banking account details and online banking statement history.

Said collection is likewise for the purpose of determining the creditworthiness and whether to increase the credit limit of the data subjects. We reiterate our above discussions on proportionality on this matter.

We note from the Online Banking PIA that for the purpose of developing and improving the credit scoring system, products and services, information about data subjects may be anonymized.

¹⁰ Data Privacy Act of 2012, § 12 (f).

¹¹ Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, §2.1 – Definition in the EU legal context

¹² National Privacy Commission, Guidelines on the Processing of Personal Data for Loan-Related Transactions [NPC Circular No. 20-01] 14 September 2020

We reiterate the discussions above that the additional purposes (i.e., develop and improve credit-scoring systems) must have a separate lawful basis. Otherwise, AND-FC runs the risk of violating the DPA and the data privacy rights of the borrowers.

the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.¹³

This relates to the obligation of AND-FC to inform the data subjects of the nature, extent, and purpose of the processing being done in relation to the declared specific purpose, their rights under the DPA, and the security measures being implemented by to protect their personal information. AND-FC shall also inform the data subjects about the consequences of granting or not granting permissions.

In the case of JVA vs UPESO,¹⁴ the NPC ruled that:

“The test to determine if the personal information controller has complied with the general privacy principle of transparency is to examine whether an average member of the target audience could have understood the information provided to them. This does not, however, mean that the requirement to use clear and plain language necessitates using layman’s terms in place of technical words at the risk of not capturing the complex concepts they represent. Rather, this requirement means that the information required under Sections 18(a) and 34(a)(2) of the Implementing Rules and Regulations should be provided in as simple a manner as possible, avoiding sentence or language structures that are complex. The information provided should be concrete and definitive; it should not be phrased in “abstract or ambivalent terms or leave room for different interpretations. x x x ” (emphasis supplied)

Thus, a valid consent may only be obtained from the data subject if the latter had been duly informed of the abovementioned information in a manner that gives them a real choice whether to allow or deny access to their SMS data and/or online banking details.

We suggest revisiting your consent forms to ensure that consent is freely given by the data subjects and that they have been duly

¹³ Data Privacy Act of 2012, § 3 (b).

¹⁴ National Privacy Commission, JVA vs UPESO [NPC Case No. 19-498] 9 June 2020

informed of all their rights as well as consequences in giving their consent. In addition, we suggest having separate consent options for the other processing activities enumerated in the PIAs that are not essential to provide the service or product sought to be availed of by the data subject. This would give the data subjects a choice to participate in the use of their personal data for the purpose of improving the credit-scoring system of AND-FC and enable them to avoid having to sign off on the entire processing activities, particularly those activities that are not related to the purpose of securing a loan.

We reiterate, however that even if data subjects consent to the processing of their personal information, their consent does not constitute a waiver of the principle of proportionality. Thus, even if AND-FC complies with all the requisites of consent but fails to address the issues mentioned above, the processing may still be considered invalid.

Privacy by design

In addition to the conduct of the PIA, it is recommended that AND-FC incorporate privacy by design principles in the development of the mobile loan application. Privacy by design is an approach that ensures that privacy and data protection have been considered during the

design phase of a system, project, program, and process and will continue to be taken into account throughout its lifecycle and implementation.¹⁵

We note that AND-FC acknowledged in the PIA that the processing activities are not proportional to the purpose stated. This notwithstanding, AND-FC did not propose measures to address these issues and, instead, sought clearance through an Advisory Opinion to process personal information. Incorporating privacy by design in the development of a revised process and data flow system may guide AND-FC in properly addressing the privacy risks identified in the PIA.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved. Please be guided accordingly.

Very truly yours,

(SGD.) FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

¹⁵ See generally: Cavoukian, Ann Ph.D., Privacy by Design - The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices, available at <https://iapp.org/media/pdf/resource center/pbd implement 7found principles.pdf> (last accessed 21 Oct 2021).

ADVISORY OPINION NO. 2022-014¹

31 August 2022

Re: **RECORDING AND UPLOADING OF ONLINE CLASSES**

Dear [REDACTED],

We write in response to your email received by the Presidential Complaint Center, which was forwarded to the National Privacy Commission (NPC) seeking clarification on whether the recording of online classes and uploading the same to Google Classroom are a violation of privacy law.

From your inquiry, we understand that you teach in college, and it is your school's policy to require the recording of online classes and uploading the same to Google Classroom. We further understand that for not recording and uploading your online class, you are now facing a hearing in your school.

You now ask for the NPC's guidance on whether the requirement of recording online classes and uploading them is a violation of the law.

Lawful criteria for processing of online class recordings; educational framework as the contract between the school and the student.

Republic No. 10173 or the Data Privacy Act of 2012² (DPA) is the law that governs the processing of all types of personal information and provides for the rights of the data subjects. Recording of online classes and any kind of activity pertaining to the recording, be it uploading or storage, are considered as processing of personal data, considering the content of the recording involves the names, images, videos, audio or other personal data of the individuals in the online class. Thus, any activity done in relation to the online class must be in accordance with the provisions of the DPA.

¹ Tags: online classes, recording of online classes, lawful criteria for processing

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

For the lawful criteria of processing of personal information, Section 12 of the law provides the instances when personal information may be processed, while Section 13 enumerates the allowable grounds of processing of sensitive personal information.³ Should any of the grounds be present in the given scenario, there is lawful basis for the requirement of recording and uploading of online class sessions by the school.

In Non vs. Danes II,⁴ the Supreme Court clarified the relationship between the school and the students in this wise:

But it must be repeatedly emphasized that the contract between the school and the student is not an ordinary contract. It is imbued with public interest, considering the high priority given by the Constitution to education and the grant to the State of supervisory and regulatory powers over all educational institutions [See Art. XIV, secs. 1-2, 4(1)].

The above doctrine was emphasized in *Isabelo, Jr. vs. Perpetual Help College of Rizal* where the Supreme Court declared: “We have also stressed that the contract between the school and the student, imbued, as it is, with public interest, is not an ordinary contract.”⁵

Reiterating the doctrine in the *Alcuaz* and *Non* cases, the Supreme Court characterized the school-student relationship as contractual in nature.⁶

The NPC considered this characterization by the Supreme Court of the contractual relationship between the school and the student in its interpretation of the application of the DPA in a school setting. The NPC refers to this contract between the school and the student as the “educational framework,” which encompasses all activities and operations the school may perform in line with the student’s education. Any processing of personal information to fulfill the obligations of parties within the educational framework is permissible, as provided in Section 12 (b) of the DPA which states:

SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

xxx

³ See Data Privacy Act of 2012, §§ 12-13.

⁴ *Non v. Danes II*, 264 PHIL 98-131 (1990).

⁵ *Isabelo, Jr. v. Perpetual Help College of Rizal, Inc.*, 298 PHIL 382-389 (1993).

⁶ *Parents-Teachers Association of St. Mathew Christian Academy v. Metropolitan Bank and Trust Co.*, 627 PHIL 669-690 (2010).

⁷ Emphasis supplied.

(b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;⁷

On the other hand, in the case of processing of sensitive personal information within the educational framework, which includes an individual's information of his or her education such as grades, performance or awards, etc., such processing is still permitted under Section 13 (a) of the DPA, to wit:

SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

(a) The data subject has given his or her consent, specific to the purpose prior to the processing, xxx.

Although the “fulfillment of a contract” requirement is not included in the enumeration in Section 13, the NPC anchors the processing of sensitive personal information within the school's educational framework upon consent based on jurisprudence defining the contractual nature of the relationship between the school and the student. Hence, upon enrollment, the student and the school are deemed to have executed a contract imbued with public interest that necessarily carries with it the consent of both parties. A different interpretation would otherwise create an absurd situation where schools may not process or use their student's educational information for his or her own education and benefit.

Processing of personal data within the educational framework in relation to academic freedom.

At this juncture, the NPC would like to clarify that educational institutions may process personal data to achieve the purposes within its educational framework without the need for consent of the data subject. The data subject in an educational setting includes students⁸, faculty and staff. It is then of utmost importance that the school delineates all processing operations, carefully identifying those that are core to the educational framework and those outside of it (e.g. marketing or public relations purposes).

⁸ In the case of minor students, their parents or guardians.

⁹ Note 5, *supra*.

¹⁰ G.R. No. 99327, May 27, 1993.

¹¹ Isabelo Jr., 298 PHIL 382-389.

In the given facts, the NPC deems the recording of online classes, and any use, storage or any kind of processing related thereto) as permissible processing within the educational framework. The NPC, through our separate discussions with the Department of Education (DepEd) and Department of Interior and Local Government (DILG), have been informed of the necessity for these online class recordings.

Connected to this, the Supreme Court reiterated in the *Isabelo, Jr. case*,⁹ the doctrine in *Ateneo de Manila University vs. Capulong*¹⁰ that : “...this Court cited with approval the formulation made by Justice Felix Frankfurter of the essential freedoms subsumed in the term ‘academic freedom’ encompassing not only ‘the freedom to determine . . . on academic grounds who may teach, what may be taught (and) how it shall be taught’ but likewise ‘who may be admitted to study.’”¹¹

In the same vein, the NPC respects the same doctrine of Academic Freedom for the processing of personal data within the educational framework, if it is in accordance with the provisions of the DPA and other existing laws, rules and regulations. The NPC will remain neutral on the chosen methods and technology by the educational institution as long as it is within the bounds of the law.

Given the foregoing, the complained requirement of recording online classes and uploading of the same to Google Classroom is not violative of one’s data privacy. However, we take this opportunity to remind the school to uphold the principle of transparency and the data subject’s right to information, such that all data subjects within its responsibility are apprised of the school’s privacy policies.

In view of this, we take this opportunity to remind schools to create and implement policies covering the processing of online class recordings, including the specific purposes for and acceptable use of such recordings. This can be made through privacy policies that are properly disseminated to all data subjects, including school faculty and staff, the students, and their parents or guardian, if necessary. Having clear policies will not only protect the data privacy of students but the teachers’ as well.

We also advise you to check on our website Public Health Emergency Bulletin No. 17 (Bulletin), which is an Update on the Data Privacy Best Practices in Online Learning. In this Bulletin, recommendations from government agencies, teachers, learners and parents were gathered to help assess and adequately address concerns relative to online learning. This Bulletin may be helpful and applicable regarding the concern raised in your email. You may find our Bulletin at this link: NPC PHE BULLETIN No. 17: Update on the Data Privacy Best Practices in Online Learning » National Privacy Commission.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.) FRANKLIN ANTHONY M. TABAQUIN IV

Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2022-015¹

23 June 2022



Re: **USE OF CAMERA DURING SURVEILLANCE VISITS**

Dear [REDACTED],

We respond to your request for an Advisory Opinion on the taking of photos or videos by the Regulations Licensing and Enforcement Division (RLED) of the Department of Health - Metro Manila Center for Health Development (DOH-MMHCD) during its monitoring and surveillance visits.

You inform that DOH Administrative Order No.2012-0012 dated 18 July 2012 authorizes the RLED to conduct on-site visits and inspection of health facilities such as hospitals, lying-in clinics, dental clinics and clinical laboratories. To aid the exercise of RLED's visitorial function, it proposes to document its on-site visits through photos and videos to facilitate the resolution of complaints and the imposition of the appropriate penalties.

You thus seek clarification on the following:

1. Whether the RLED can take photos and videos during on-site visits for monitoring and surveillance purpose, without requesting for the consent of the authorized representatives of the health facilities or the persons whose photo or video will be taken.
2. Whether RLED can use photos and videos for purpose of presenting the same in courts and administrative bodies.
3. What data privacy laws, rules and regulations are applicable to RLED in the taking and use of photos and videos from on-site visits.

¹ Tags: lawful processing; statutory mandate; photographs; taking of videos.

Processing of audio-visual recordings for monitoring and surveillance purposes without consent allowed under the DPA under certain instances;

Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.² Accordingly, the image of an identifiable individual captured in a photograph or video is personal information about the individual and, thus, covered by the Data Privacy Act of 2012 (DPA).

The collection and use of audio-visual recordings may be justified under Section 12 of the DPA, specifically where the processing is necessary for compliance with a legal obligation,³ or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.⁴

Under Section 12 of the DPA, the processing of personal information shall be permitted only if not otherwise prohibited by law and when at least one of the following conditions exists:

- (a) The data subject has given his or her consent;
- (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
- (d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
- (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
- (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution. (emphasis ours)

² Data Privacy Act of 2012, § 20 (c)

³ Id. § 12 (c)

⁴ Id. § 12 (e)

⁵ National Privacy Commission, NPC Advisory Opinion No. 2018-053 (November 26, 2018). ⁶ Data Privacy Act of 2012, § 3 (l) (2)

Thus, in NPC Advisory Opinion No. 2018-053,⁵ we stated that the processing of personal information, which in that case involves photographs of hospital staff and doctors, can only be lawfully taken and processed when at least one of the conditions set forth in Section 12 of the DPA exists.

In addition, Section 13 of the DPA may likewise apply where a footage or image involves sensitive personal information, such as clinical photographs which necessarily contain the health information of patients.⁶ Sensitive personal information refers to personal information:

- (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
- (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
- (4) Specifically established by an executive order or an act of Congress to be kept classified.

In which case, the processing thereof is prohibited except in the following cases:

- ((a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
- (b) The processing of the same is provided for by existing laws and regulations: Provided, that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
- (c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing; (d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing;

⁷ Id. § 13 (b)

- (e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
- (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

As mentioned above, Section 13 (b) recognizes processing that is imposed by existing laws and regulations. As applied in this instance, the processing of such images is anchored on such rules and regulations mandating the RLED to conduct monitoring and surveillance of health facilities regulated by the DOH. Hence, it is permitted under the DPA to process personal data through the taking of photos or videos during on-site visits and the consent of the data subject/s is not required should their images be captured in the process.

We wish to reiterate that the consent of the data subject/s is not the only lawful criteria for processing information and that the PIC should choose the lawful basis that most closely reflect the true nature of the relationship with the data subject and the purpose of the processing.

As for photos or videos of hospital premises, the DPA will not apply if no individual or data subject is captured. This does not mean, however, that other laws, regulations and generally accepted hospital standards will not apply.⁸

Audio-visual recordings may be used as evidence by the RLED in courts and administrative bodies.

On the question of whether RLED can use photos and videos as evidence in courts and administrative bodies, Section 13 (f) states that processing of sensitive personal information is permitted if the processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or

⁸ NPC Advisory Opinion No. 2018-053.

the establishment, exercise or defense of legal claims, or when provided to government or public authority. Although Section 13(f) applies to sensitive personal information, the protection of lawful rights and interests under Section 13 (f) is considered as legitimate interest pursuant to Section 12(f) of the DPA.⁹ This section provides that it is lawful to process personal information if it is necessary for the purpose of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.¹⁰

Thus, the RLED may present in evidence photos or videos it captured during inspections as the processing of such information is pursuant to the existence of the latter's legitimate interest which is to resolve complaints filed against health facilities, and consequently, the imposition of penalties thereto.

We wish to reiterate that the law does not prohibit government agencies from processing personal data pursuant to their respective mandates, taking into consideration the applicable provisions of law, rules and regulations, and the general data privacy principles enunciated in the DPA. The DPA promotes fair, lawful, and secure processing of such information.

Adherence to the general data privacy principles when taking audio-visual recordings during on-site visit; data subjects' rights; security measures.

While there may be lawful basis for processing under the DPA, the RLED must always adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.

The principle of proportionality requires that processing of personal information shall be adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified purpose.[†] We note from your letter that the RLED intends to document its on-site visits through photos and videos to facilitate the resolution of complaints and the imposition of the appropriate penalties. The RLED must ensure that such photos and videos will only be processed in relation to such purpose.

⁹ CID Case No.17-K-003 dated 19 November 2019 ¹⁰ R.A.10173, Section 12(f); Ibid.

¹⁰ R.A.10173, Section 12(f); Ibid.

¹¹ Data Privacy Act of 2012, § 11 (c)

On the other hand, the principle of transparency requires that the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject and how these can be exercised. During the RLED's inspection, it must provide the appropriate privacy notices to apprise data subjects that it will take photos or audio-visual recordings.

A privacy notice is statement made to a data subject that describes how an organization collects, uses, retains and discloses personal information. A privacy notice may be referred to as a privacy statement, a fair processing statement or, sometimes, a privacy policy.¹² In the present case, we suggest that RLED create a privacy notice that taking of photographs or audio-visual recordings may be done during on-site visits or inspections and must include the lawful criteria on which the processing is based on. This privacy notice may be presented to the health facilities before conducting the inspection or when questions are raised on the propriety of taking photographs or videos by the RLED. By doing so, the data privacy principle of transparency is complied with.

Lastly, the RLED is required by the DPA to uphold the rights of data subjects and implement reasonable and appropriate security measures for the protection of the personal data collected against unauthorized processing. As such, the RLED must integrate privacy and data protection in all processing activities involved in the conduct of its on-site visit/s, considering the nature of the personal data that requires protection, the risks to the rights and freedoms of the patients as data subjects, current data privacy best practices, among others.¹³ We also reiterate that the audio-visual recordings, should only be used for the intended purpose thereof. You may refer to NPC Circular No. 2016-01 - Security of Personal Data in Government Agencies for further details as to which appropriate security measures are applicable to your agency.

¹² IAPP, Glossary of Privacy Terms, available at <https://iapp.org/resources/glossary/#paperwork-reduction-act-2>

¹³ Data Privacy Act of 2012, § 20

Please be advised that this Advisory Opinion was rendered based solely on your provided information. Any extraneous fact that may be subsequently furnished to us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.) FRANKLIN ANTHONY M. TABAQUIN IV

Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2022-016¹

5 July 2022



Re: **REQUEST FOR PERSONAL INFORMATION OF OFWs
DEPLOYED IN THE MIDDLE EAST AND OTHER MUSLIM
COUNTRIES**

Dear [REDACTED],

We respond to your request for an Advisory Opinion on the above matter.

You inform that the Hajj Attaché is an office attached to the National Commission on Muslim Filipinos (“NCMF”). As the current Hajj Attaché to the Kingdom of Saudi Arabia and the Philippine representative to the Office of the Islamic Conference, you have witnessed the abuses committed against Overseas Filipino Workers (“OFWs”).

To address these abuses expeditiously, you requested the Department of Foreign Affairs, Department of Labor and Employment, Overseas Workers Welfare Administration, and the Philippine Overseas Employment Administration (collectively, “Subject Departments”) for the contact details and personal information of all OFWs working in Muslim countries you deal with. It is your position that the NCMF is vested with the legitimate interest, the legal obligation, and the “public task” to obtain the requested data from the Subject Departments. However, you state that the Subject Departments are apprehensive about sharing with your office the OFWs’ personal data, citing possible violation of the Data Privacy Act of 2012 (“DPA”).

Consequently, you seek our opinion to support your request and justify the release of information by the Subject Departments.

¹ Tags: lawful processing; legitimate interest; data privacy principles.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

National Commission on Muslim Filipinos; mandate.

Under Republic Act (RA) 9997,³ the NCMF is mandated to preserve and develop the culture, tradition, institutions, and well-being of Muslim Filipinos, in conformity with the country's laws and in consonance with national unity and development.

As mentioned throughout its enabling law, the NCMF's powers and functions specifically pertain to Muslim Filipinos. However, your request to the Subject Departments states that what you are asking for is the personal information of all OFWs (i.e., Muslims and non-Muslims) in the Muslim countries within the jurisdiction of your office. It is our understanding that not all OFWs in these countries are Muslim Filipinos. Hence, the non-Muslim OFWs appear to be beyond the prescribed mandate of the NCMF. As presently worded, your request to the Subject Departments appears to encroach on their jurisdiction since the powers and mandate of the NCMF only pertain to Muslim Filipinos.

While the processing of the personal data of Muslim OFWs may fall within the mandate of the NCMF, said mandate appears to exclude the processing of the personal information of non-Muslim OFWs. Hence, there may be a need to secure the consent of non-Muslim OFWs prior to the collection and disclosure of their personal information to the NCMF.

It is worth noting further that Section 15 of RA 9997 explicitly provides for the extent of the functions of the Hajj Attaché:

Section 15. Hajj Attaché.— The President shall appoint a Hajj Attaché from among the three (3) recommendees of the Commission within fifteen (15) days from the submission of such recommendees by the Commission. The Hajj Attaché shall coordinate with the Ministry of Hajj of the Kingdom of Saudi Arabia on all matters pertaining to the conduct of the annual Hajj. He/She shall be an academic degree holder and must be able to write and speak fluently the Arabic language. He/She shall hold office in the Kingdom of Saudi Arabia and shall enjoy the same rank, salary, and privileges as those of Attachés of the national government. (Emphasis supplied).

From the foregoing, we note that the authority of the Hajj Attaché is limited to all matters pertaining to the conduct of the annual Hajj to the Kingdom of Saudi Arabia. Thus, there may be a need to

³ An Act Creating the National Commission on Muslim Filipinos Defining its Powers, Functions and Responsibilities and Appropriation Funds Therefor and for other purposes [National Commission on Muslim Filipinos Act of 2009], Republic Act No. 9997, § 4 (2009).

⁴ Data Privacy Act of 2012, § 4.

also determine whether the NCMF, through the Hajj Attaché, is the appropriate department to handle the above concerns or if it would be more legally sound to refer the concern to other agencies (i.e., the Subject Departments).

Scope; Lawful basis for processing personal information; Section 12; legal obligation; legitimate interest.

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.⁴

As discussed above, if after judicious assessment it is determined that the mandate of the NCMF and/or the Hajj Attaché may cover the processing of personal data for the purpose of reaching out to distressed Muslim OFWs, their families, and relatives, then the processing of their personal data may be justified as will be discussed below.

The collection and disclosure of personal information⁵ of Muslim OFWs constitute processing.⁶ As applied to your present concern, Section 12 (c) and (e) of the DPA appears to be the most appropriate criteria for lawful processing by the NCMF, thus:

SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
x x x

(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; xxx”

(Emphasis supplied).

Thus, the NCMF must justify to the Subject Departments that its processing falls within the ambit of the foregoing provisions.

⁵ Id. § 3 (g).

⁶ Id. § 3 (j).

⁷ Id. § 11.

Thereafter, the Subject Departments may disclose such personal information to NCMF but subject to the general data privacy principles.⁷

On the other hand, if sensitive personal information is involved, NCMF's processing thereof may be permitted under Section 13 (b) of the DPA, viz.:

SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: x x x

(b) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information; x x x

You cited in your letter Section 12 (f) of the DPA on legitimate interest as a possible basis for lawful processing of personal data:

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

It is a well-settled rule that the powers and functions of statutorily-created agencies, such as the NCMF, are measured and limited by the law creating them or granting them powers.⁸

Thus, while NCMF may rely on Section 12 (c), (e), and Section 13 (b) for the processing of personal data of Muslim OFWs, it cannot rely on legitimate interest as a criterion for the processing of the same. It has no such legitimate interest to go beyond its mandate. Any and all processing of personal information and sensitive personal information should be hinged on its legal mandate.

Adherence to the general data privacy principles; transparency; proportionality; privacy notice

⁸ Chavez v. National Housing Authority, 530 SCRA 235 (2007).

⁹ E.g., posting in their website or other appropriate platforms the NCMF or Hajj Attaché's contact details, address, updates, and announcements.

Section 11 of the DPA and Section 18 of its Implementing Rules and Regulations (“IRR”) provide that personal information controllers (“PICs”), such as the NCMF and the Subject Departments, are required to adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.

The principle of transparency refers to the awareness of the data subjects about the nature, purpose, and extent of the processing of their personal information, including recipients of their personal data. Hence, the Subject Departments must first inform the Muslim OFWs that their personal information will be shared with the NCMF, as well as the nature, purpose, and extent of the processing. If the NCMF determines that its purpose can only be fulfilled by processing the personal information of Muslim OFWs, it should not collect personal information over and beyond that which is required to achieve the declared purpose.

On the other hand, the principle of proportionality requires that the NCMF should ascertain if its purpose cannot be fulfilled by any other less intrusive means.⁹ Hence, the NCMF should specifically state the type of personal information it needs from these agencies. The request for the “names, contact details, email addresses & other personal information of all Overseas Filipino Workers deployed in the Middle East” may be too broad and excessive and, therefore, violative of the principle of proportionality.

Finally, the principle of legitimate purpose provides that the processing of personal information should be compatible with a declared and specified purpose which is not contrary to law, morals, or public policy.

Lest we be misconstrued, allow us to emphasize that we share the very laudable objective of the Honorable Hajj Attaché to assist distressed OFWs. However, any processing of personal information should be in accordance with the DPA and other existing rules and regulations.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished to us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)

FRANKLIN ANTHONY M. TABAQUIN IV

Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2022-017¹

20 September 2022



Re: **DISCLOSURE OF PERSONAL INFORMATION FOR CYBERSECURITY INVESTIGATIONS**

Dear [REDACTED],

We respond to your request for an Advisory Opinion on the application of Republic Act 10173 (or the Data Privacy Act of 2012 [DPA])² on your client's request for information from a certain corporation for investigation purposes regarding a cybersecurity incident.

We understand that your client, Corporation A, is the owner, operator, and franchise licensor of Brand B stores in the Philippines. Besides being a seller of consumer products, Brand B stores offer e-services such as bills payment, top up, cash-in, and remittance for its accredited merchant partners. One of Corporation A's largest merchant partner is Corporation C which is an e-Money Issuer.

You allege that on 1 December 2020, Corporation A discovered staggering discrepancies between the cash-ins recorded in Corporation A's System and the actual cash received by a Brand B store in Davao City. Corporation A created an investigation committee which learned that during the period 9 November – 1 December 2020, 2,516 unique Corporation C accounts successfully made cash-ins through the Corporation C application amounting to Php249,011,058.00, all without going through the Point of Sale (POS) system of the Brand B Davao Store and without the latter receiving the money from the account holders. The cashins appear to have bypassed the Corporation A's System and POS and, thus, Corporation A has no record of receiving the amounts.

¹ Tags: personal data; lawful processing; consent of data subjects; legal claims; Sec. 13 (f), DPA.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

Corporation A immediately notified Corporation C of the incident and requested the latter to block the said 2,516 accounts. Based on Corporation A's investigation, while the cash-ins involved 2,516 accounts, the incident appears to have been instigated by a syndicate of approximately 10 people by creating and using the said accounts.

In the course of Corporation A's investigations, it coordinated with Corporation C to request for information and validation of the 2,516 accounts that made the cash-ins. In particular, Corporation A requested for the following information (Requested Information):

1. Number of Corporation C accounts opened after November 2020;
2. Number of top-up transactions that were made through the Corporation C application;
3. Information regarding the accounts, including details on date of creation, manner of KYC, and other pertinent details;
4. Confirmation that the 2,516 accounts were legitimate Corporation C users;
5. Confirmation that the 2,516 accounts have been prevented from further withdrawals;
6. Confirmation that Corporation C has alerted recipient financial and non-financial institutions of the fraudulent activity in order for them to hold the funds;
7. Information regarding the recipient financial institutions that the funds were transferred or withdrawn, and the number of unique accounts in each;
8. Information regarding the withdrawals from ATM machines using the Corporation C ATM card, specifying the date, time, location, and ATM operator/bank;
9. Confirmation that the ATM operator has been notified of possible fraud and instructing them to store CCTV footage from the ATM pending further investigation;
10. Any other details that could aid Corporation A in the investigation.

However, Corporation C responded that any information to be released in relation to the incident was covered by the DPA. According to Corporation C, there must be prior consent from the data subject or a court order compelling it to disclose the information.

³ Data Privacy Act of 2012, § 3 (g).

You thus ask whether:

- a. Item nos. 1, 2, and 4 to 10 of the Requested Information are not considered as personal data, and thus not covered by the DPA; and
- b. Even assuming the above information, as well as item no. 3, are considered personal data, that the disclosure of such Requested Information does not require data subject consent prior to disclosure, as claimed by Corporation C.

It is your contention that item nos. 1, 2, and 4 to 10 are not personal data considering that the disclosure will not enable or allow the identification of persons, individuals or data subjects and are not within the purview of protected information under the DPA. In addition, it is your opinion that consent of the data subject and court order are not the only bases for disclosure of personal data.

Information excluded from the scope of the DPA.

Under the DPA, personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.³ On the other hand, sensitive personal information is clearly defined under Section 3 (I) of the law.⁴ Consequently, information that does not identify an individual are beyond the scope of the DPA.

Nevertheless, there is a need to examine the nature of the information involved item nos. 1, 2, and 4 to 10 to ascertain if they are indeed excluded from the scope of the DPA.

Item no. 1 [number of Corporation C accounts opened after November 2020] and item no. 2 [number of top-up transactions that were made through the Corporation C application] only deal with numbers of accounts and transactions, respectively.

Item no. 4 [confirmation that the 2,516 accounts were legitimate Corporation C users], item no. 5 [confirmation that the 2,516 accounts have been prevented from further withdrawals], item no. 6 [confirmation that Corporation C has alerted recipient financial and non-financial institutions of the fraudulent activity in order for

⁴ Id. § 3 (I).

⁵ See: National Privacy Commission, BGM vs. IPP, NPC 19-653 (17 December 2020), available at <https://www.privacy.gov.ph/wpcontent/uploads/2021/02/NPC-19-653-BGM-vs-IPP-Decision-FINALPseudonymized-21Dec2020.pdf> (last accessed 03 February 2022).

them to hold the funds], and item no. 9 [confirmation that the ATM operator has been notified of possible fraud and instructing them to store CCTV footage from the ATM pending further investigation] merely involve verification of the action mentioned that can be responded to by a simple “yes” or “no” answer.

Item no. 7 [information regarding the recipient financial institutions that the funds were transferred or withdrawn, and the number of unique accounts in each] deal with business information.

Item no. 8 [information regarding the withdrawals from ATM machines using the Corporation C ATM card, specifying the date, time, location, and ATM operator/bank] are information on transaction details of withdrawals using Corporation C ATM card, specifically limited to date, time, location and the ATM operator/bank.

The foregoing reveals that the nature of the information enumerated above are not personal data as these do not identify a unique individual. Thus, such items are indeed outside the scope of the DPA.

However, item no. 10 [any other details that could aid Corporation A in the investigation] is too broad for us determine if it may include personal data as defined by the DPA.

Consent or court order not required for disclosure; information necessary for the establishment, exercise or defense of legal claims

It is your contention that all of the Requested Information, including item no. 3 [information regarding the accounts, including details on date of creation, manner of KYC, and other pertinent details], are not covered by the DPA. You also contend that even if items 1, 2, and 4 to 10 are considered as personal data, such information may still be disclosed without the need for the data subject’s consent or a court order, citing Sections 12 (f) and 13 (f) of the DPA in conjunction with the National Privacy Commission’s (NPC) Decision in BGM vs. IPP.⁵

We find merit in your argument.

Sections 12 (f) and 13 (f) of the DPA state:

SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

xxx

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

xxx

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority. (Emphasis supplied)

In NPC Advisory Opinion No. 2021-036,⁶ the NPC once again discussed the application of the abovementioned provisions in relation to the processing of personal data necessary for the establishment, exercise or defense of a legal claims out of court, and likewise reiterated its ruling in BGM vs. IPP, viz:

In the interpretation of the phrase “establishment, exercise or defense of legal claims,” the Commission reiterated its stand in the case of BGM vs. IPP, viz:

In the case of NPC 17-018 dated 15 July 2019, this Commission held that “processing as necessary for the establishment of legal claims” does not require an existing court proceeding. To require a court proceeding for the application of Section 13(f) to this instance would not only be to disregard the distinction provided in the law but the clear letter of the law as well. After all, the very idea of “establishment ... of legal claims” presupposes that there is still no pending case since a case will only be filed once the required legal claims have already been established.”

...

⁶National Privacy Commission, Advisory Opinion No. 2021-036 (23 September 2021).

activities to obtain evidence by lawful means for prospective court proceedings. As such, the DPA does not require the establishment of actual or ongoing court proceedings in the application of Section 13 (f).

...

The Commission's pronouncement in the same case of BGM v. IPP may be applied in the same vein:

Although Section 13(f) applies to sensitive personal information while the information involved in this case is just personal information, the protection of lawful rights and interests under Section 13(f) by the Respondent is considered as legitimate interest pursuant to Section 12(f) of the DPA.⁷

Similar to the factual milieu of NPC Advisory Opinion No. 2021-036, it is apparent that Corporation A has a legal claim to the Php249,011,058.00 that were allegedly fraudulently withdrawn from Brand B Davao Store. In order to aid its own investigation and establish its case, Corporation A would have to gather necessary information from Corporation C as the merchant partner involved in the transactions subject of the claim.

Given the foregoing, Corporation C need not obtain consent from its data subjects or wait for a court order to provide Corporation A with the Requested Information, subject to other applicable laws or regulations.

We take this opportunity to remind that while it appears there exists justification for the disclosure of personal data, the DPA mandates that the principle of proportionality should still be adhered to. Proportionality requires that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.⁸

Please be advised that this Advisory Opinion was rendered based solely on the information you provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)

FRANKLIN ANTHONY M. TABAQUIN IV

Director IV, Privacy Policy Office

⁷ Id. Citations omitted.

⁸ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).

ADVISORY OPINION NO. 2022-018¹

20 September 2022



Re: **DATA SUBJECT RIGHTS IN THE PHILIPPINE IDENTIFICATION SYSTEM**

Dear [REDACTED],

We respond to your email inquiry on the rights of a data subject in relation to the Philippine Identification System (PhilSys) and the provisions of R.A. No. 10173, also known as the Data Privacy Act of 2012 (DPA).²

We understand that the Feedback and Grievance Division (FGD) of the PhilSys Registry Office (PRO) relayed to the Philippine Statistics Authority (PSA) Legal Service that a certain PhilSys registered person requested the deletion of his/her personal data. At the time of your inquiry, the PSA Legal Service has yet to confirm if the registered person was already issued a PhilSys Number (PSN) or PhilSys Card Number (PCN).

As context to your inquiry, you provided two scenarios. The first scenario is that the registered person is already registered in the PhilSys but has not been issued a PSN or PCN. In this scenario, you opine that the registered person has the right to withdraw consent as it is one of the rights of a data subject, and corollary thereto, the registered person has the right to request for the deletion of his/her personal data. In which case, it is your position that the registered person must execute a written request to the PRO's Data Protection Officer (DPO) stating the request for deletion is in the exercise of his/her right to erasure under the DPA. In relation to deletion, you opine that if the PRO resolves to anonymize the data then the DPO may validly deny the request for deletion of the registrant considering that anonymized data is not considered personal data.

² Tags: Philippine Identification System Act, PhilSys Act, PhilSys, national ID, identification system, rights of data subjects, right to object, right to erasure, right to deletion, lawful criteria for processing

³ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

The second scenario is that the registered person has already been issued a PSN or PCN. It is your opinion that since the PSN or PCN has already been issued, the registered person's right to erasure has already ceased. The most that the registered person can do is to request for the deactivation of her PSN or PCN pursuant to the Implementing Rules and Regulations of R.A. No. 11055.

We further understand that in two separate instances, the NPC confirmed that the processing of information under Republic Act (RA) 110554 is not based on consent. You further mentioned that in an online training conducted by an NPC representative, it was clarified that if consent is not the basis of processing, then there is nothing to withdraw.

You now ask whether a registered person is not entitled to withdraw consent as well as erase or delete his/her personal data since the processing is based on law and not consent, with no distinction as to whether the registrant has already been issued PSN/PCN.

Right to object, when applicable; processing based on law.

The DPA sets the limits of personal data processing, including the lawful bases of processing and the rights of the data subjects.

Involved in this inquiry are two (2) data subject's rights: 1) the right to object; and 2) right to erasure or blocking. The "right to withdraw consent" you mentioned, stems from the data subject's right to object as provided by Section 16 (e) of the DPA⁵ and expounded further by Section 34 (b) of the Implementing Rules and Regulations of the Data Privacy Act of 2012 (IRR),⁶ which respectively state:

SEC. 16. Rights of the Data Subject. – The data subject is entitled to:

xxx

(e) Suspend, withdraw or order the blocking, removal or destruction of his/her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected.

⁴ Philippine Identification System Act.

⁵ Data Privacy Act of 2012, § 3 (g).

⁶ Rules and Regulations Implementing the Data Privacy Act of 2012, § 34 (b) (2016).

...

Section 34. Rights of the Data Subject. The data subject is entitled to the following rights:

xxx

b. Right to object. The data subject shall have the right to object to the processing of his/her personal data, including processing for direct marketing, automated processing or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph.

When a data subject objects or withholds consent, the personal information controller shall no longer process the personal data, unless:

1. The personal data is needed pursuant to a subpoena;
2. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or
3. The information is being collected and processed as a result of a legal obligation.⁷

As with any other data subject right, the right to object to the processing of his/her personal data or to withdraw consent are not absolute and must be exercised within the parameters stated under the law. To see whether the right to object or withdraw consent will apply, another aspect to consider is the lawful basis of processing of personal data under the PhilSys.

It has been the National Privacy Commission's (NPC) stand that RA 11055 that provides the basis for the processing of personal data of Filipinos and resident aliens under the PhilSys. Section 9 of the R.A. No. 11055 which provides: "... *every citizen or resident alien shall register personally...*," embodies the legal obligation of Filipino citizens and resident aliens to register under the PhilSys thereby

⁷ Emphasis supplied.

necessitating the processing of their personal data. In connection to such requirement, Section 8 of RA 11055 lists the mandatory demographic and biometric information to be collected from registered persons.

Since it is the law and not consent that is the basis for processing under the PhilSys, the right to withdraw consent by the data subject does not apply. There is no consent to speak of since the registration to PhilSys is a legal obligation imposed upon every citizen or resident alien. To be clear, both the right to object and the right to withdraw consent do not apply in any of the scenarios mentioned above.

Right to erasure or blocking under the PhilSys.

On the other hand, the right to erasure or blocking has its own limitations as well. Section 34

(e) of the DPA's IRR enumerates the instances when the right to erasure may be exercised:

Section 34. Rights of the Data Subject. The data subject is entitled to the following rights:

xxx

e. Right to Erasure or Blocking. The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his/her personal data from the personal information controller's filing system.

1. This right may be exercised upon discovery and substantial proof of any of the following:

- (a) The personal data is incomplete, outdated, false, or unlawfully obtained;
- (b) The personal data is being used for purpose not authorized by the data subject;
- (c) The personal data is no longer necessary for the purposes for which they were collected;
- (d) The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
- (e) The personal data concerns private information that

is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;

(f) The processing is unlawful;

(g) The personal information controller or personal information processor violated the rights of the data subject.

xxx

However, R.A. 11055 and its Revised IRR do not provide for grounds for deletion or erasure of the registered person's PSN/PCN or their personal data. Instead, it provides for grounds for deactivation of the PSN, viz.:⁸

Section 9. Deactivation of PSN

A. The PSN shall be deactivated on the following grounds:

1. loss of Filipino citizenship;
2. loss of resident alien status;
3. failure to submit to initial biometric capture at age five (5) for persons who were registered at age four (4) and below;
4. failure to submit to biometric capturing at age 15 for persons who were registered at age 14 and below;
5. death of the registered person; and
6. upon the request of the registered person.

B. After due process, the PSA may deactivate the PSN on the following grounds:

1. presentation of false or fictitious supporting document/s during registration or during application for change of entries;
2. misrepresentation in any form during and after registration in the PhilSys; and
3. fraudulent application of biometric exception.

⁸ See Revised Implementing Rules and Regulations of the Philippine Identification System Act, § 9.

xxx

We emphasize that deactivation is not equivalent to deletion in the system. RA 11055 is silent on the provision for deletion. Likewise, the law and its Revised IRR do not make the distinction on instances when an individual has or has not been issued a PSN or PCN. Thus, in the absence of express provisions in the law allowing for deletion in the system, the right to erasure, or to demand for absolute deletion from the PhilSys, is not applicable to registered persons in the PhilSys.

Finally, we take this opportunity to discuss your position that if the PRO resolves to anonymize the data, the DPO may then validly deny the request for deletion of the registrant considering that anonymized data is not considered personal data. We respectfully submit that the same misapplies the concept of anonymization.

In Advisory Opinion No. 2018-068, the Commission discussed anonymization at length, viz:

Information is anonymous when such information ‘does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.’

We note also that ISO/IEC 29100 defines anonymization as a process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party.

Any information is considered anonymized if there is no possible means to identify the data subject, that is, the PIC and/or any other person are incapable of singling out an individual in a data set, from connecting two records within a data set (or between two separate data sets) and from any information in such dataset.

However, removing some identifiers, such as patient and physician names, contact information, and location, may not be enough to ensure that the PIC and/or any other person can no longer identify the data subject. Anonymization may necessitate additional measures to guarantee that the anonymity of the information is irreversible.⁹

In addition, anonymization, like any other processing activity, should be carried out with a legitimate purpose that is clear and specified. In this case, anonymization may not be utilized for the purpose of denying the deletion request.

The NPC, as the implementing agency tasked to regulate the processing of personal data, must harmonize the DPA's provisions with other laws and regulations.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)

FRANKLIN ANTHONY M. TABAQUIN IV

Director IV, Privacy Policy Office

⁹ National Privacy Commission, NPC Advisory Opinion No. 2018-068 (20 November 2018); citations omitted.

ADVISORY OPINION NO. 2022-019¹

21 September 2022



Re: **USE OF BODY-WORN CAMERA BY SECURITY PERSONNEL**

Dear [REDACTED],

We respond to your request for an advisory opinion regarding the use of body-worn cameras (BWCs) by the security personnel of ON Semiconductor Philippines, Inc., ON Semiconductor SSMP Philippines Corporation, and ON Semiconductor Cebu Philippines, Inc. (collectively, Corporations).

We gather that the Corporations are affiliate companies located in Cavite, Tarlac, and Cebu, engaged in various manufacturing, processing, and sale of semiconductors. Currently, the Corporations are exploring the possibility of requiring their security personnel to use bodyworn cameras to record their field observations and encounters, on top of the use of closedcircuit television systems (CCTVs).

You thus ask whether the Corporations' security personnel can employ BWCs without violating the provisions of the Data Privacy Act of 2012² (DPA).

*Lawful basis for processing personal information;
Section 12;*

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.³

¹ Tags: body-worn cameras, lawful processing of personal information; general data privacy principles; transparency; proportionality; privacy notice.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for r-this Purpose a National Privacy Commission, and for other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

³ Data Privacy Act of 2012, § 4.

Personal information is defined as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.⁴

Consequently, under the DPA, the images of identifiable individuals captured in a photograph or audiovisual recordings are considered personal information⁵ about the individual. Thus, the processing of which should comply with the provisions of the DPA.⁶

You mentioned that the use of the BWCs will be for a legitimate purpose, i.e., to promote the safety and protect the security of people and the manufacturing facilities of the Corporations. The use of BWCs is envisioned to:

1. Raise standards during confrontational incidents
2. Improve efficiency in incident escalation
3. Supplement opportunities for evidence capture
4. Reduce complaints
5. Assist with disciplinary and/or legal proceedings.

As justification, you cited Section 12 of the DPA, which provides for the criteria for lawful processing of personal information based on legitimate interests of the personal information controller (PIC), to wit:

SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
x x x

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

At the outset, we acknowledge that employers have legitimate standing to uphold its legitimate business interests, such as employee monitoring, security of the premises, investigations or disciplinary

⁴ Data Privacy Act of 2012, § 3 (g).

⁵ Id. § 3 (g).

⁶ Id. § 3 (j).

purposes, and other reasonable purposes which are not contrary to law, morals, or public policy.

However, we emphasize that legitimate interest in the processing activity should be linked to a specific context and that the PICs must determine the most appropriate lawful basis for processing personal information in relation to the specific purpose of the processing activity.

Hence, while the processing of personal information based on the legitimate interests of the PICs is allowed under the DPA, the Corporations must assess if the use of BWCs within the premises will pass the three-part test of Legitimate Interest, namely:

1. Purpose test - The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve.
2. Necessity test - The processing of personal information must be necessary for the purposes of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test - The fundamental rights and freedoms of data subjects must not be overridden by the legitimate interests of the PICs or third party, considering the likely impact of the processing on the data subjects.

Adherence to the general data privacy principles; transparency; proportionality; privacy notice

Aside from determining the most appropriate lawful basis for processing, the Corporations must also adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.

Particularly, the principle of proportionality requires that processing of personal information shall be adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified purpose.⁷

⁷ Data Privacy Act of 2012, § 11 (c).

⁸ National Privacy Commission, *JVA vs UPESO* [NPC Case No. 19-498] 9 June 2020

As mentioned, the Corporations have CCTVs installed in their respective facilities. Considering all attendant circumstances, the Corporations must first conduct an assessment that the use of additional BWCs is truly necessary and is the least privacy intrusive manner of processing in relation to the declared purpose.

After evaluation, if the Corporations decide to use BWCs, they must ensure that the data subjects are informed that their security personnel are equipped with BWCs. This may be done through an appropriate privacy notice which you ensure will be complied with.

The privacy notice should describe the specific processes relating to the use of BWCs. In crafting the privacy notice regarding the use of BWCs, reference can be made to Section 16 (b) of the DPA on the information that should be provided to the data subjects pursuant to their right to be informed and to demonstrate the Corporations' adherence to the data privacy principle of transparency.

Further, the Commission, in the case of JVA vs UPeso⁸, ruled that:

The test to determine if the personal information controller has complied with the general privacy principle of transparency is to examine whether an average member of the target audience could have understood the information provided to them. x x x

If the data subjects would not be able to understand the information provided in the Privacy Notice, then the Corporations should translate their Privacy Notices into the language or dialect understandable by the data subjects in their regions of operations so the latter may be fully informed of such processing.

The Corporations may also wish to review, among others, the instances when their security personnel will turn on their BWCs, the manner by which to immediately notify the data subjects on the use of BWCs, and the mechanism for data subjects to exercise their data privacy rights in relation to the BWC footages.

Privacy impact assessment

Finally, we recommend conducting a privacy impact assessment (PIA) on the use of BWCs to identify potential privacy risks to the data subjects.

A PIA is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a PIC or a personal information processor (PIP). It considers the nature of the personal data to be protected, the personal data flow, the risks to privacy and security posed by the processing, current data privacy best practices, the cost of security implementation, and, where applicable, the size of the organization, its resources, and the complexity of its operations.⁹

The PIA will help identify and provide an assessment of various privacy risks, and propose measures intended to address and mitigate the effect of these identified risks on the data subjects. We trust that after the conduct of a PIA, the Corporations would best be able to determine if the use of BWCs aligns with the basic data privacy principles.

Please be advised that this Advisory Opinion was rendered based solely on your provided information. Any extraneous fact that may be subsequently furnished to us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

Sgd.

FRANKLIN ANTHONY M. TABAQUIN IV

Director IV, Privacy Policy Office

⁹ NPC Advisory No. 2017-03, Guidelines on Privacy Impact Assessment, 31 July 2017.

ADVISORY OPINION NO. 2022-020¹

21 September 2022

[REDACTED]

Re: **CIVIL REGISTRY DOCUMENT REQUEST BY A PERSON OTHER THAN THE OWNER**

Dear [REDACTED],

We respond to your request for an Advisory Opinion on the Philippine Statistics Authority's (PSA) denial of your request for a copy of another person's civil registry documents on data privacy grounds.

You mentioned that you intend to process your deceased father's Government Service Insurance System (GSIS) benefits. You submitted your deceased father's Certificate of No Marriage (CENOMAR) which apparently lists two (2) marriages: the first to a Ms. [REDACTED] (Ms. [REDACTED]), and the second to your mother.

We understand that GSIS informed you that Ms. [REDACTED] may be disqualified from claiming your deceased father's benefits if you can submit Ms. [REDACTED]'s Death Certificate or her CENOMAR showing a subsequent marriage. Thus, you requested the PSA for a copy of Ms. [REDACTED]'s Death Certificate but was denied citing data privacy grounds.

You thus seek advice on your possible remedies to obtain the requested documents from the PSA. Further, you are also asking if you can file a complaint before the National Privacy Commission (NPC) in relation to PSA's denial of your request for Ms. [REDACTED]'s civil registry documents.

*Sensitive personal information; lawful processing;
establishment, exercise or defense of legal claims under
Section 13(f)*

¹ Tags: Philippine Identification System Act, PhilSys Act, PhilSys, national ID, identification system, rights of data subjects, right to object, right to erasure, right to deletion, lawful criteria for processing

A Death Certificate is an official document setting forth particulars relating to a deceased individual. It contains data such as (a) date and place of death, (b) full name, (c) age, (d) sex, (e) occupation or profession, (f) residence, (g) civil status, (h) nationality of the deceased, and (i) probable cause of death. Some of these items are sensitive personal information under the DPA.

The processing of sensitive personal information is generally prohibited under the DPA. However, the DPA provides for exceptions to this rule. Section 13(f) of the DPA specifically recognizes processing for the establishment, exercise, or defense of legal claims, thus:

SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: x x x

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interest of natural or legal persons in court proceedings or the establishment, exercise, or defense of legal claims, or when provided to government or public authority.

In line with the DPA's policy to protect the fundamental right of every individual to privacy, the PSA issued Memorandum Circular (MC) 2019-15 which provides for a list of people allowed to request for civil registry documents/certifications from the PSA, to wit:

6. The court or proper public official whenever absolutely necessary in administrative, judicial or other official or other proceedings to determine the identity of the person. Provided that there must be a duly issued subpoena duces tecum and ad testificandum for the production of the civil registry document.

7. Request from other government agencies pursuant to their mandate provided that the requesting government agency executed Data Sharing Agreement with PSA in accordance with NPC Circular 16-02.

Thus, the PSA is not totally precluded from providing a copy of the requested Death Certificate in the absence of the owner of the personal data or a next of kin.

However, PSA's requirement that the request should be pursuant to a pending case and that there is a duly issued subpoena directing the release of the personal data requested unduly restricts the lawful basis to process under the DPA. Moreover, not all administrative agencies have the power to issue subpoenas.

PSA's requirement is an erroneous interpretation of Section 13(f) of the DPA which was discussed in the case of BGM vs. IPP,² citing NPC 17-018 dated 15 July 2019. The NPC ruled therein that "processing as necessary for the establishment of legal claims does not require an existing court proceeding". Further, the very idea of "establishment ... of legal claims" presupposes that there is still no pending case since a case will only be filed once the required legal claims have already been established. The NPC further ruled that:

"The DPA should not be seen as curtailing the practice of law in litigation. Considering that it is almost impossible for Congress to determine beforehand what specific data is "necessary" or may or may not be collected by lawyers for purposes of building a case, applying the qualifier "necessary" to the second instance in Section 13(f) therefore, serves to limit the potentially broad concept of "establishment of legal claims" consistent with the general principles of legitimate purpose and proportionality"

Therefore, PSA's interpretation that lawful processing under Section 13 (f) requires the existence of an actual case should be reviewed and revised to properly conform to the DPA considering that it is intended to carry out the policy "to protect the fundamental right of every individual to privacy".

In line with this, the NPC also stated in the BGM case that the protection of lawful rights and interests under Section 13(f) of the DPA is considered as legitimate interest pursuant to Section 12(f) of the law. Thus, the following tests may be considered by the PIC in deciding on a request pursuant to Section 13(f), viz:

1. Purpose test – The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve;

² National Privacy Commission, NPC 19-653 (17 December 2020)

2. Necessity test - The processing of personal information must be necessary for the purpose of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test – The fundamental rights and freedoms of data subjects must not be overridden by the legitimate interest of the PIC or third party, considering the likely impact of the processing on data subjects.³

In this regard, we highlight that the appreciation of the facts and the evaluation of conditions for the release of documents under their control and custody fall primarily with the concerned agency as they are in the best position to apply their mandate⁴

In other words, even if your request for processing is supported by a lawful criteria, it does not equate to the PIC granting a blanket authority for you to access personal information and/or sensitive personal information of the data subject. Your request would still be evaluated on a case-to-case basis and must always be subject to the PIC's guidelines for the release of such information.⁵

*Data Privacy Principle of Legitimate Purpose
and Proportionality*

We take this opportunity to harmonize the restrictions in the PSA's (MC) 2019-15 vis-a-vis the recent issuances by the NPC. The grant by the PSA of access to personal data does not necessarily mean that the entire form or record requested will be disclosed. An issuance from the PSA either confirming or denying the marriage or death of the person subject of the record requested may be sufficient and aligned with the data privacy principle of proportionality.

On the other hand, the PSA also allows the disclosure of personal data through a request from another government agency pursuant to its mandate. Hence, you may want to explore the possibility of requesting GSIS to issue a formal request addressed to PSA in the confirmation of the death and/or status of marriage of Ms. [REDACTED]

³ See generally, Data Privacy Act of 2012, § 12 (f); United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/> [last accessed on 8 September 2022].

⁴ NPC Advisory Opinion 2019-037 (8 August 2019)

⁵ Id.

As to the filing of a complaint before the NPC, we suggest that you exhaust first the remedies discussed above. Although PSA's reason for not disclosing the requested information is based on an erroneous interpretation of Section 13(f) of the DPA, the mere refusal to disclose information and/or relevant documents to a data subject is not punishable under the DPA. Also, a particular agency's procedure for document requests must still be complied with even if access to the personal data has legitimate basis under the DPA.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

Sgd.
FRANKLIN ANTHONY M. TABAQUIN IV
Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2022-021¹

14 October 2022

[REDACTED]

[REDACTED]

Re: **PUBLICATION OF INFORMATION OF LIST OF WHOLESALE ELECTRICITY SPOT MARKET (WESM) MEMBERS AND RETAIL CUSTOMER INFORMATION UNDER RETAIL COMPETITION AND OPEN ACCESS (RCOA) AND GREEN ENERGY OPTION PROGRAM (GEOP).**

Dear [REDACTED]

We respond to your request for an Advisory Opinion on the Independent Electricity Market Operator of the Philippines, Inc.'s (IEMOP) data privacy concerns regarding the publication of: 1) the names of Wholesale Electricity Spot Market (WESM) members; and, 2) the names of registration applicants and the retail or contestable customers registered in the Retail Competition and Open Access (RCOA), also known as retail electricity market.

We understand that IEMOP made this inquiry as the Market Operator of WESM and the Central Registration Body (CRB) of the RCOA and Green Energy Option Program (GEOP). IEMOP cites our Advisory Opinion No. 2020-052,² which dealt with the Energy Regulatory Commission's (ERC) publication of contestable customers. IEMOP's position is that it is similarly situated to the ERC since it is also obligated by law and regulation to publish the names of WESM participants and the RCOA contestable customers. Incidentally, the RCOA contestable customers are the same contestable customers subject of the said Advisory Opinion.

¹ Tags: lawful criteria for processing; natural person; juridical person; legal obligation; publication of names.

² National Privacy Commission, NPC Advisory Opinion No. 2020-052 (20 November 2020).

We further understand that in accordance with several Department of Energy (DOE) issuances, the following are published by IEMOP on its website:

Information Owner	Information
WESM Participants	<ol style="list-style-type: none"> 1. Participant name (Name of corporation, partnership or individual) 2. Short name (short name designated by IEMOP for the participant) 3. Region (Luzon, Visayas or Mindanao) 4. Category (Generator, Private Distribution Utility, Electric Cooperative, Bulk User/Directly Connected Customer, Ancillary Service Provider, Wholesale Metering Service Provider) 5. Membership (Direct Member or Indirect Member) 6. Resource (facility name; name of power plant, if a generator) 7. Effectivity date of registration (date in which membership has become effective) 8. Registration Status (Registered, Deregistered or Ceased)
Contestable Customers (RCOA/CREM)	<ol style="list-style-type: none"> 1. Participant name (Name of corporation, partnership or individual) 2. Short name (short name designated by IEMOP for the participant) 3. Region (Luzon, Visayas or Mindanao) 4. Category (Contestable Customer, Retail Electricity Supplier, Local Retail Electricity Supplier, Supplier of Last Resort, Retail Metering Service Provider) 5. Membership (Direct Member or Indirect Member; Registered with CRB only) 6. Effectivity date of registration (date in which membership has become effective) 7. Registration Status (Registered, Deregistered or Ceased)

WESM Applicants	<ol style="list-style-type: none"> 1. Applicant name (Name of corporation, partnership or individual) 2. Short name (short name designated by IEMOP for the applicant) 3. Region (Luzon, Visayas or Mindanao) 4. Category applied for (Generator, Private Distribution Utility, Electric Cooperative, Bulk User/Directly Connected Customer, Ancillary Service Provider, Wholesale Metering Service Provider) 5. Membership type applied for (Direct Member or Indirect Member) 6. Resource (facility name; name of power plant, if a generator) 7. Application Type (New registration or additional facility) 8. Status (For completion)
------------------------	---

Furthermore, we understand that WESM members and applicants may be juridical entities or individual persons. Currently, however, the registered members are all juridical entities. In addition, contestable customers may likewise be juridical entities or individuals who are operating as sole proprietorships.

Thus, you seek guidance on the following:

- 1) Whether IEMOP may publish the names of WESM members and names of applicants for WESM registration by virtue of the WESM Rules promulgated by the DOE pursuant to Republic Act No. 9136, otherwise known as the Electric Power Industry Reform Act (EPIRA); and
- 2) Whether IEMOP may publish the names of retail or contestable customers that are registered to participate in the Retail Competition and Open Access (RCOA) or the retail electricity market on the basis of The Retail Market Manual on Disclosure and Confidentiality of Retail Customer Information (Retail Manual - DCRCI) likewise promulgated by the DOE.

Lawful criteria for processing; compliance with a legal obligation

Section 3 of the EPIRA defines the responsibilities of the various government agencies and private entities in relation to the electric power industry. The WESM and the RCOA are part of the electric market industry framework.

Pursuant to DOE Department Circular No. DC2018-01-0002,³ IEMOP was established to be the independent market operator of the WESM. Thus, it is evident that IEMOP is obligated to comply with the EPIRA and is regulated by the DOE through applicable issuances.

Under the WESM Rules promulgated by the DOE, IEMOP is required to publish the following:

- a) A list of registered WESM members, including the names and categories in which they are registered; and
- b) A list of applicants for WESM registration, including the name of the applicant and the status of its application.⁴

On the other hand, the Retail Manual on Disclosure and Confidentiality of Retail Customer Information (Retail Manual – DCRCI)⁵ designates the IEMOP to be the Central Registration Body that is required to publish “Retail Customer Information” of contestable customers, including their names and short names.⁶

The abovementioned information published by IEOMP is based on the nonconfidential information enumerated in Clause 5.4 of the Retail Manual – DCRCI, which are:

1. Service address of the registered facility
2. Contact details
3. Supply details
 - a. incumbent supplier
 - b. past supplier/s
 - c. duration of supply contract
 - d. names of counterparties
4. Details contained in the ERC’s Certificates of Contestability, as applicable.

³ Department of Energy, Department Circular No. DC-2018-01-002, “Adopting Policies for the Effective and Efficient Transition to the Independent Market Operator for the Wholesale Electricity Spot Market” (17 January 2018).

⁴ Wholesale Electricity Spot Market Rules (WSEM Rule), available at <https://www.wesm.ph/downloads/download/TWFya2V0lFJlcG9ydHM=/MTkyMg==> (last accessed 10 June 2022).

⁵ Promulgated by the DOE through Department Circular Nos. DC2013-07-0014, DC2021-06-005, and DC2021-06-0012.

⁶ Ibid.

The Data Privacy Act of 2012⁷ (DPA) governs the processing of personal data. Under the DPA, the processing of personal data shall only be allowed under certain conditions provided in Sections 12 and 13 depending on whether the information involved is classified as personal information or sensitive personal information.

In this regard, we reiterate the discussion in Advisory Opinion No. 2020-052 where we stated that information on juridical entities is outside the scope of the DPA. Thus, the publication of WESM members or applicants for registration and contestable customers in the RCOA that are juridical entities may be done in accordance with applicable laws, rules, and regulations without violating the DPA.

We also discussed in Advisory Opinion No. 2020-052 that the publication of personal information of an individual or a sole proprietorship who may qualify as a WESM member or as a contestable customer is allowed subject to Section 12 of the DPA, thus:

In the event where the contestable customer is an individual or a sole proprietorship whose name and generic location would be subject to publication, Section 12 of the DPA states that that the processing of personal information shall be permitted if necessary for compliance with a legal obligation to which the personal information controller is subject or when necessary in order to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.

In this instance, the ERC may cite the pertinent provisions of the Electric Power Industry Reform Act of 2001 (EPIRA) and/or other applicable laws and regulations to justify the publication of names and generic locations of individuals identified as qualified contestable customers as a legal obligation of the ERC and/or part of the fulfillment of its mandate.

Under the DPA, the processing of personal data is allowed when it is necessary for compliance with a legal obligation. In *RLA v. PLDT*

⁷ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

Enterprise,⁸ the National Privacy Commission (NPC) discussed the elements that should exist for valid processing based on a legal obligation : “(1) if the legal obligation the PIC cites as lawful criteria exists and applies to the PIC; (2) if the processing that the PIC performs is necessary to comply with the legal obligation; and (3) if all the conditions imposed by the legal obligation for the processing of the personal information have been complied with.”⁸

A survey of the relevant DOE regulations cited clearly show that the IEMOP has a legal obligation to publish the information provided above. As such, as long as the elements mentioned above are complied with, -IEMOP can publish the names of WESM members and the names of applicants for WESM registration, by virtue of the WESM Rules. Similarly, the names of retail or contestable customers that are registered to participate in the RCOA may also be published on the basis of the Retail Manual – DCRCI.

Nevertheless, IEMOP, as a PIC, is still mandated to adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. It also has the obligation to implement reasonable and appropriate organizational, physical, and technical security measures for protection of personal data, and ensure that it processes information in a manner that upholds the data privacy rights of its data subjects.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)

FRANKLIN ANTHONY M. TABAQUIN IV

Director IV, Privacy Policy Office

⁸ National Privacy Commission, *RLA v. PLDT Enterprise* [NPC Resolution No. 2018-010] (10 December 2021).

ADVISORY OPINION NO. 2022-022¹

19 October 2022



Re: **DISCLOSURE OF COVID-19 SWAB TEST RESULTS IN
GROUP CHAT**

Dear [REDACTED],

We respond to your request for clarification on the data privacy implication of a proposed internal practice of disclosing COVID-19 test results in your office's group chat.

We understand that the Davao Center for Health Development (DCHD) wishes to enhance its contact tracing of COVID-19 positive cases within its office. The intended purpose is to improve infection control and minimize the spread of positive cases to ensure unhampered operations.

You further inform that in a survey conducted among DCHD's employees, a majority voted to have the complete list of COVID-19 positive employees posted in the group chat composed of 250 members, while a minority opposed the measure. The purpose of posting in the group chat is to let everyone be aware if they are possible close contacts and, thus, enable them to take the necessary precautions to avoid infection.

Thus, you seek guidance on the following:

1. Due to the majority voting in favor of the posting COVID-19 swab test results in the group chat, is DCHD allowed to post the complete list in the group chat despite a minority signifying to the contrary?
2. Is written consent still necessary for those who agreed to have their names posted in the group chat once they have positive results?

¹Tags: COVID-19, swab test results, contact tracing, sensitive personal information, disclosure.

Lawful criteria for processing of COVID-19 test results, provided by law and regulation; limitations on disclosure

Under the Data Privacy Act of 2012 (DPA)² the processing of personal data shall only be allowed under certain conditions provided in Sections 12 and 13 depending on whether the information involved is classified as personal information or sensitive personal information. In addition, the Section 18 (b) of the Implementing Rules and Regulations (IRR) of the DPA also requires that the processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality. Transparency requires that the data subjects are informed of the details of the processing of their personal data, such as the nature, purpose and extent of processing as well as their rights as data subjects. The principle of legitimate purpose, on the other hand, states that the processing of personal information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. Finally, proportionality calls for the processing of personal information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

In the case of COVID-19 contact tracing, we stated in Advisory-Opinion-No.-2020-022³ that the processing of any personal data, including the test results, is based on law and regulation, viz.:

Accordingly, contact tracing would inevitably involve the processing of personal and sensitive personal information (collectively, personal data) of COVID-19 suspected, probable, and confirmed cases by the DOH and other government agencies engaged in the COVID-19 response.

Such processing for contact tracing is expected to be in accordance with existing laws and regulations on the matter, i.e., Republic Act No. 11332 or the Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act, the DPA, as well as applicable issuances of the DOH and the NPC.

The DOH Updated Guidelines on Contact Tracing provides for the specific guidelines for the identification of contacts of suspect cases, case investigation and contact tracing for probable and confirmed cases, contact tracing in areas with community transmission, among others. These guidelines also provide for the use of standard forms, i.e., Case Investigation Form, Travel History Form, Close Contact Line List Form, Profile of the COVID-19 Close Contacts, etc.

All these measures ensure that only the necessary personal data are collected in a standard and appropriate manner and disclosed only to the proper authorities.

In the same Advisory Opinion, we further stated that the disclosure of personal data related to COVID-19 shall be made pursuant to Annex A of the DOH Updated Guidelines on Contact Tracing, thus:

6. Disclosure of Patient Identifiers or Patient Data shall be limited to authorized entities, officers, personnel and concerned individuals only. The said disclosure is allowed if the same will serve a public purpose or function during the COVID-19 pandemic.

Disclosure to the public, the media, or any other public-facing platforms without the written consent of the patient or his/her authorized representative or next of kin, shall be strictly prohibited.

The above policy is further reinforced in the DOH-NPC Joint Memorandum Circular on the Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response, which contains a similar provision under Section VI (D) (2) thereof on the Specific Guidelines on Use and Disclosure of Health Information.

We also stated in NPC Circular No. 2021-02 that the disclosure of personal data in cases of contact tracing “shall be limited to public health authorities, such as the DOH and its authorized partner agencies, LGUs, or other lawfully authorized entities, officers, or personnel, and must only be for the purpose of responding to the public health emergency.”⁴

Thus, we do not suggest posting in a group chat the names of employees who are COVID-19 positive. Through Department Memorandum No. 2020-0189, the Department of Health (DOH) already laid down the procedure which a Personal Information Controller (PIC), such as your office, must observe in relation to contact tracing.⁵ As such, we recommend that the guidelines be strictly observed since it provides the lawful basis which justifies the processing of personal data of employees under the circumstances. Consent not the appropriate basis for disclosure of COVID-19 swab test results

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

³ See National Privacy Commission, NPC Advisory Opinion No. 2020-022 (8 June 2022).

Under the DPA, consent of the data subject that is freely given, specific, and informed, is recognized as one of the lawful criteria for processing.⁶ In the present case, however, the parties do not stand on equal footing. In the field of data protection and privacy, it has been recognized that there is a clear imbalance of power between the employer and the employee because by the very nature of the relationship, employees may not have genuine free choice and may not subsequently be able to withdraw their consent without adverse consequences.⁷ As such, consent is not the most appropriate basis for processing since it can be tricky to ascertain if the employees concerned freely gave their consent.

Instead, the appropriate lawful basis for processing relative to contact tracing purposes is provided and limited by law and regulation, that is, DOH Department Memorandum No. 2020-0189. Given this, it would be inconsistent with the basis for processing to ask employees to consent to such additional processing since it already goes beyond the prescribed procedure under the regulation. Mere participation in the survey in the group chat cannot be recognized as a positive indication of valid consent since the elements of consent under the DPA are not present. Moreover, asking the employees' consent for processing in addition to what is provided by the law and regulation would be unjust and improper as the data subject may not be able to distinguish the basis for which their personal data is being processed. In present situation, the employees may feel the need to give their consent for all things related to contact tracing.

Proper procedures already exist to address the demands of the COVID-19 public health emergency while ensuring the protection of the individual's data privacy. As the PIC and employer, DCHD should adhere with the requirements of the law as well as implement strategies that are least intrusive to the rights and freedoms of its employees. Even though the proposed disclosure in the group chat is made with good intentions, this strategy may run afoul with the employee's data privacy.

⁴ See National Privacy Commission, Guidelines on the Processing of Personal Data During Public Health Emergencies for Public Health Measures, NPC Circular No. 2021-02 [NPC Circular 21-02] (08 November 2021).

⁵ Department of Health, Update Guidelines on Contact Tracing of Close Contacts of Confirmed Coronavirus Disease (COVID19) Cases, Department Memorandum No. 2020-0189 (17 April 2020).

⁶ Data Privacy Act of 2012, § 3 (b).

⁷ See Article 29 Working Party, Opinion 8/2001 on the processing at work (13 September 2001) available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf (last accessed 31 March 2022).

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)

FRANKLIN ANTHONY M. TABAQUIN IV

Director IV, Privacy Policy Office

ADVISORY OPINION NO. 2022-023¹



11 November 2022



Re: **DISCLOSURE OF STUDENTS' PERSONAL DATA FOR
CASE BUILD-UP PURPOSES**

Dear 

We respond to your request for an Advisory Opinion on whether the University of the Philippines Diliman (University) may disclose its students' personal data in connection with an “on-going case build-up” preparatory to the filing of a case for violation of Republic Act No. 11053 or the Anti-Hazing Act of 2018.²

As you have narrated, a 
 The lawyer of wrote the University's Office of the Vice Chancellor for Student Affairs asking for a list of the subject fraternity's: 1) alleged current members, 2) student and alumni members, and 3) new recruits. The following specific information pertaining to the listed individuals were also requested:

- Full name;
- Address;
- Phone number and/or email address;
- Enrolment, course, degree, and campus; and
- For new recruits, in addition to the above, their parents' name, addresses, phone number and/or email address.

The lawyer's request for the forgoing is purportedly intended for a

¹ Tags: disclosure of student personal information and sensitive personal information; Section 12 (f); Section 13 (f); proportionality.

² An Act Prohibiting Hazing and Regulating Other Forms of Initiation Rites of Fraternities, Sororities, and Other Organizations, and Providing Penalties for Violations thereof, Amending for the Purpose Republic Act No. 8049, Entitled “An Act Regulating Hazing and Other Forms of Initiation Rites in Fraternities, Sororities, and Organizations and Providing Penalties therefor [Anti-Hazing Act of 2018], Republic Act No. 11053 (2018).

case build-up, and to invite or summon potential witnesses and/or co-complainants or co-plaintiffs.

You are thus concerned if the disclosure of such information is in line with the Data Privacy Act of 2012 (DPA).³

Information requested are personal information and sensitive personal information

The requested information are classified as personal information and sensitive personal information (collectively, personal data) under the DPA.

Specifically, names and contact details (addresses, phone numbers, and email addresses) of the students and their parents are considered as personal information under the DPA. On the other hand, the requested information on enrolment, course, degree, and campus may be considered as sensitive personal information since it pertains to an individual's education.

Lawful basis for processing under Section 13; establishment of legal claims.

The disclosure of personal and sensitive information is considered as processing under the DPA. Consequently, the same should be based on the most appropriate lawful criterion for processing under Sections 12 and 13, respectively.

In the present case, the avowed purpose for the request for information is to build-up a case and invite or summon potential witnesses and/or co-complainants for the filing of a case for violation of the Anti-Hazing Act of 2018.

For the sensitive personal information requested, the disclosure may find basis under Section 13 (f), viz.:

SECTION 13. Sensitive Personal Information and Privileged Information. –
The processing of sensitive personal information and privileged information

³ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

⁴ Data Privacy Act of 2012, § 13 (f).

⁵ National Privacy Commission, NPC Advisory Opinion No. 2021-36 (Sept. 23, 2021) citing National Privacy Commission, NPC 19-653 (Dec. 17, 2020).

shall be prohibited, except in the following cases: x x x

- (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.⁴ (emphasis supplied)

The term “establishment” may include activities to obtain evidence by lawful means for prospective court proceedings.⁵

On the other hand, the disclosure of personal information may be justified as falling under legitimate interest criterion in Section 12 (f):

SECTION 12. Criteria for Lawful Processing of Personal Information. The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
x x x

- (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution. (emphasis supplied)

In the case of *BGM vs. IPP*,⁶ the Commission articulated that the protection of lawful rights and interests under Section 13(f) is considered as legitimate interest pursuant to Section 12(f):

Although Section 13(f) applies to sensitive personal information, the protection of lawful rights and interests under Section 13(f) by the Respondent is considered as legitimate interest pursuant to Section 12(f) of the DPA. This section provides that it is lawful to process personal information if it is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

By application in the instant case, Respondent may not be held liable for unauthorized processing should it disclose the requested information

⁶ National Privacy Commission, NPC 19-653 (17 December 2020)

⁷ National Privacy Commission, NPC Case No. 17-018 (15 July 2019).

⁸ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).

to Complainant as its disclosure would be in pursuance of the latter's legitimate interest as the same cannot be fulfilled by other means.

Thus, the disclosure of the requested personal data for the declared purpose finds support under the DPA. We emphasize that the DPA is neither a tool to prevent the discovery of a crime nor a means to hinder legitimate proceedings.⁷

Proportionality of processing; necessity of personal data requested vis-à-vis the specified and declared purposes

Nonetheless, utmost consideration must also be given to the general data privacy principle of proportionality. The University should evaluate whether the personal data requested is relevant and is not excessive to the purpose. Note that while the law may allow processing when there is a lawful basis for the same, the processing of personal data remains to be subject to the proportionality principle which requires that the processing shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.⁸

As such, the University should determine whether to disclose all requested information taking into consideration the information stated in the request letter and its necessity and relevance to the declared purposes.

Should the University deem it proper to grant the request, it is recommended that the requesting party be made to sign an undertaking that the use of the requested information will only be for the purpose for which it is requested (i.e., filing a complaint for violation of the Anti-Hazing Act of 2018). Further, the proper disposal of such personal data should be ensured should the parties decide not to pursue the filing of the case. Likewise, the undertaking must include a clause to the effect that the requesting party acknowledges that he or she becomes a personal information controller (PIC) upon receipt of the requested documents and, therefore, is bound to observe the obligations of a PIC under the DPA.⁹

Lastly, should the information be provided, its use should be limited to the declared purpose of filing formal/legal charges by the

concerned or affected individual who allegedly suffered damages. Thus, the sharing, posting or any publication of such information in any public-facing platform such as social media pages or public groups is prohibited. We caution that should there be processing beyond the stated purpose, the same may be penalized under the appropriate provisions of the DPA, such as Unauthorized Processing of Personal Information, Processing of Personal Information for Unauthorized Purposes or Unauthorized Disclosure.¹⁰

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

SGD.
FRANKLIN ANTHONY M. TABAQUIN IV
Director IV, Privacy Policy Office

⁹ National Privacy Commission, NPC Advisory Opinion No. 2021-044 (29 December 2021).

¹⁰ See: National Privacy Commission, NPC Advisory Opinion No. 2022-005 (24 February 2022).

ADVISORY OPINION NO. 2022-024¹

21 November 2022



Re: **FREE FLOW OF DATA**

Dear [REDACTED]

We respond to your inquiry regarding the concept of the free flow of data. You cited in your letter the discussions on the concept of “free flow of data” in high-level statements of the APEC,² and G20.³ Likewise, in the WTO Joint Statement Initiative on e-commerce, the relevant working text refers to the “flow of information” as well as “cross-border transfer of information by electronic means” or “cross-border data flows.”

You further inform that trade agreements have also evolved to meet changing digital realities, with provisions relating to enabling trusted data flows by developing mechanisms to protect personal data being transferred across borders and allow businesses to transfer information across borders regardless of where they are located.

It is in this context that the Bureau of International Trade Relations (BITR) of the Department of Trade and Industry (DTI) is inquiring

¹ Tags: free flow of data; data transfer; cross-border data transfer; accountability.

² APEC Internet and Digital Economy Roadmap: Key focus area of “Facilitating the free flow of information and data for the development of the Internet and Digital Economy, while respecting applicable domestic laws and regulations”; APEC Putrajaya Vision 2040: Innovation and Digitalization pillar, wherein members have committed to “strengthen digital infrastructure, accelerate digital transformation, narrow the digital divide, as well as cooperate on facilitating the flow of data and strengthening consumer and business trust in digital transactions; APEC Cross-Border Privacy Rules (CBPR) System and APEC Privacy Framework: Preamble states that “a key part of efforts to improve consumer confidence and ensure the growth of electronic commerce must be cooperation to balance and promote both effective information privacy protection and the free flow of information in the Asia Pacific region.”

³ At the G20, Japan launched the Osaka Track based on the concept of “data free flow with trust” (DFFT) as an organizing principle for a global approach to data governance. It should be noted that DFFT has been pushed by Japan in APEC, although with resistance among the developing economy members. A few APEC economies have openly expressed reservations on the use of “free” in relation to data flows.

whether the concept of the free flow of data falls under the purview of the Data Privacy Act of 2012⁴ (DPA) or in other related law or policy, and if the National Privacy Commission (NPC) foresees any future implications on data localization, data sovereignty, and data protection. The BITR likewise requests for any information, views, or insights to inform and guide the BITR on the stage of the Philippines' work in terms of establishing a framework to govern cross-border e-commerce and data flows.

Free flow of data and the Data Privacy Act of 2012

Section 2 on the Declaration of Policy of the Data Privacy Act of 2012⁵ (DPA) states that:

It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

The DPA indeed concerns itself with the free flow of data but limited to the specific context of personal data processing⁶ only. The law has the twin task of protecting the right to privacy while ensuring the free flow of information.

This means recognizing the fundamental right of individuals to the protection of the privacy of their personal data, and at the same time, recognizing interests of the government and the private sector in the processing of personal data which is vital in the implementation of constitutional and statutory mandates and in lawful business operations, respectively.

⁴ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012)

⁵ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

⁶ Id. § 3 (j): Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

⁷ See generally: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119, Recital 53 (4 May 2016) and Organisation for Economic Co-operation and Development (OECD) Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data, Paragraphs 17-18 (Amended on 11/07/2013).

The use of the term “free” in relation to “flow of information” is not intended to denote absoluteness in the use and/or transfer of information by personal information controllers (PICs) whether locally or across transnational borders. Any processing of personal data is still regulated and subject to the requirements of the DPA and issuances of the NPC.

We note that this interpretation is similar and consistent with other international instruments and laws on data privacy. There is a recognition that free flow of data should be facilitated but subject to the implementation of sufficient safeguards and where appropriate, conditions, limitations, or restrictions on the flow of data should be proportionate to the risks of the personal data processing activity.⁷

Likewise, the NPC is cognizant that cross-border data flows can have significant benefits for economic growth and that data governance is essential in the context of rapid digitalization.

The DPA does not serve as a barrier to the free flow of data across borders so long as appropriate safeguards on personal data protection are in place. This means that transfer of personal data must adhere to general privacy principles of proportionality, transparency, and legitimate purpose.⁸ PICs must also ensure that recipients of personal data outside the Philippines process data in a manner consistent with requirements of the DPA and must put in place contractual or other reasonable safeguards to guarantee a comparable level of protection for data transferred.

Relevant policies on data transfers

Related to the concept of free flow of data is the principle on secure and trusted transfer of personal data. Section 21 of the DPA states that:

Section 21. Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

⁸ Data Privacy Act of 2012, §11.

⁹ National Privacy Commission, NPC 19-910 (17 December 2020).

¹⁰ National Privacy Commission, Data Sharing Agreements [NPC Circular No. 2020-03], (December 23, 2020).

- a. The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. x x x

In the case of *In Re: FLI Operating ABC Online Lending Application*,⁹ the NPC expounded that the PIC cannot surrender its accountability and responsibility to prevent any unauthorized processing under the DPA to the Personal Information Processor (PIP). The NPC ruled therein that the respondent cannot be absolved of its violations of the DPA on the argument that the processing for purposes of collections was subcontracted. The NPC explained that the respondent cannot escape the fact that it was in the position to control and exercise discretion over what personal information it processed and the extent of its processing.

In connection with the principle of accountability on transfers of personal data in Section 21 of the DPA, the NPC also issued NPC Circular No. 2020-03¹⁰ on Data Sharing Agreements. In essence, the NPC explained that data sharing requires that the sharing, disclosure, or transfer to a third party of personal data should adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. Likewise, organizations should implement reasonable and appropriate organizational, physical, and technical security measures intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.

Mechanisms to facilitate cross-border transfers of personal data that comply with privacy and data protection requirements and principles are likewise an area of importance. Thus, the NPC issued NPC Advisory No. 2021-02 on the Guidance for the use of the ASEAN Model Contract Clauses and ASEAN Data Management Framework. This Advisory recognizes the value of these initiatives to data privacy protection and trustworthy cross-border data flows and hence, promotes the adoption and use in its domestic legal framework. This Advisory also aims to provide additional guidance to supplement the ASEAN Model Contractual Clauses and ASEAN Data Management Framework as to how personal information controllers (PICs) and processors (PIPs) in the Philippines may use these in their respective personal data processing activities.

Further, the NPC continues to foster collaboration with like-minded jurisdictions in supporting privacy-respecting cross-border data flows through the APEC Cross Border Privacy Rules (CBPR) System and the Global CBPR Forum. This is in line with NPC's mission of establishing a regulatory environment that ensures accountability in the processing of personal data and promotes global standards for data privacy and protection.

Future implications on data localization, data sovereignty, and data protection

At this juncture, it would be speculative for the NPC to provide an answer to the posited question of whether the NPC foresees any future implications on data localization, data sovereignty, and data protection vis-à-vis the concept of the free flow of data.¹¹ Nevertheless, the NPC remains proactive in fulfilling its mandate and will respond and adapt appropriately according to the call of the times.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished to us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)

FRANKLIN ANTHONY M. TABAQUIN IV

Director IV, Privacy Policy Office

¹¹ National Privacy Commission, Rules of Procedure on Requests for Advisory Opinions [NPC Circular 18-01], § 5 (b) (4) (September 10, 2018).

ADVISORY OPINION NO. 2022-025¹

22 November 2022

[REDACTED]

Re: **201 FILES OF GOVERNMENT EMPLOYEES**

Dear [REDACTED],

We respond to your inquiry concerning the rights of government employees to their 201 files and other information processed by a government agency.

You inform that you have been an employee of the Department of Agriculture [REDACTED]

[REDACTED] In September 2020, you received a Special Order reassigning you to a remote province. You filed an appeal before the Civil Service Commission (CSC) to assail your reassignment. Pending your appeal, you requested to be reinstated at your original station but was denied. Months later, you were dropped from the rolls without notice. As a result, you filed another petition before the CSC for being dropped from the rolls.

To support your petition, you requested for a copy of your 201 file which is in the custody of the Human Resources Office of DA- [REDACTED] In your letters to the Officer-in-Charge Regional Director (OIC-RD), you insisted that government employees are entitled to copies of Director (OIC-RD), you insisted that government employees are entitled to copies of their 201 files citing relevant CSC rules and the Data Privacy Act of 2012.

Through a 31 March 2022 letter, the OIC-RD denied your request for copies of your 201 Files stating that:

¹ Tags: 201 files; government employee; Civil Service Commission; right to access; data subject rights; legal claims.

“... as an employee that is deemed Dropped from the Rolls, the Office has no more recourse left but to turn-over his/her 201 files. However, MC Number 1, series of 2011, of the Civil Service Commission, generally instructed the NGAs, GOCCs and SUC to undertake the turning over of 201 files to all those applicable former employees perhaps in batches, as the procedure provided in the mentioned MC entails coordination with several offices and requires the necessary clearances from affected former employees.”

In addition, the OIC-RD reasoned that, “as a former government employee, the provisions of the Data Privacy Act of 2012 do not apply to you.” He cited Section 4 (a) of the Data Privacy Act of 2012² (DPA) and stated that the provisions of the DPA should be read together with the necessary Civil Service Rules and Issuances.

201 files; government employees are data subjects with data privacy rights; the establishment, exercise or defense of legal claims

We refer to CSC Memorandum Circular No. 8, series of 2007 (MC 08-2007)³ which states that government employee’s 201/120 file consist of copies of the following documents:

- a) Appointments [CSC Form 33]
- b) Assumption to Duty
- c) Certification of Leave Balances (for transferees)
- d) Clearance from Property and Money Accountabilities (for transferees)
- e) Contracts of Services (if applicable)
- f) Copies of Certificates of Eligibilities
- g) Copies of Diplomas, Commendations and Awards
- h) Copies of Disciplinary Actions (if any)
- i) Copy of Marriage Contract (if applicable)
- j) Designations
- k) Medical Certificate [CSC Form 211]
- l) NBI Clearance
- m) Notice of Salary Adjustments/Step Increments
- n) Oath of Office
- o) Personal Data Sheet [CSC Form 212]
- p) Position Description Forms

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

³ Civil Service Commission, “Management of 201/120 Files” [CSC Memorandum Circular No. 8, series of 2007], 17 May 2007 (available at [http://www.csc.gov.ph/2014-02-21-08-28-23/pdf-files/category/32-mc-2007.html?download=321 mc8s2007](http://www.csc.gov.ph/2014-02-21-08-28-23/pdf-files/category/32-mc-2007.html?download=321%20mc8s2007))

⁴ National Privacy Commission, NPC Advisory Opinion No. 2018-028 (16 May 2018).

In Advisory Opinion No. 2018-028,⁴ we had the occasion to discuss that an employee, being a data subject, is entitled to have reasonable access to the personal information in his/her 201 file:

Accordingly, Employee A, being a data subject, is entitled to have reasonable access to the personal information in her 201 file. She may exercise her right to access in the manner provided under the DPA but she must still abide by company protocols in accessing her 201 file.

Under the law, the company is obligated to respond and grant reasonable access to subject request. Should the request be ignored or denied, a complaint with the NPC may be initiated following the procedure laid down in NPC Circular No. 2016-04, as one of NPC's functions is to enforce and effectively implement the provisions of the DPA, including those pertaining to the rights of data subjects.

In addition, the National Privacy Commission (NPC) issued NPC Advisory No. 2022-01, "Guidelines on Requests for Personal Data of Public Officers"⁵ to provide guidance in dealing with personal and sensitive personal information (collectively, personal data) of government employees. The said Advisory unequivocally states that public officers and employees are recognized as data subjects with all the concomitant rights and available redresses, viz.:

C. Public officers are data subjects within the purview of the Act, with all the concomitant rights and available redresses under the same.

However, certain personal data relating to their positions and functions is subject to certain exceptions provided in the Act and disclosures required under other applicable laws.

In these exceptional cases, these information relating to their position and official functions are not covered by the DPA. However, the exemption is not absolute. The exclusion of such information from the scope of the law is interpreted as an exemption from complying with the requirements of Sections 12 or 13 on lawful criteria for processing; and the collection, access, use, disclosure, or other processing is limited to the minimum extent necessary to achieve the purpose, function, or activity concerned. Personal information controllers (PICs) undertaking the processing of such information remain to be subject to the other requirements of the DPA, including implementing security measures to protect personal data and upholding the rights of the public officers as data subjects.⁶

⁵ National Privacy Commission, Guidelines on Requests for Personal Data of Public Officers [NPC Advisory No. 2022-01], (4 February 2022), available at: <https://www.privacy.gov.ph/wp-content/uploads/2022/02/NPC-Advisory-No.-2022-01-Request-for-Personal-Data-of-Public-Officers.pdf>.

⁶ Id., at §3(C). (Emphasis supplied.)

Consequently, the unequivocal statement of the OIC-RD that the provisions of the DPA do not apply to government employees is misplaced. As a data subject, you have data privacy rights to your own personal data, including the right to access such information. A PIC must have policies to facilitate the exercise of a data subject's right to access. These policies must include, among others, the procedure to acquire the information, the retention period of the data and the mode of disposal or deletion. Thus, you should be provided with the information you requested in accordance with the policies of DA- [REDACTED] on a data subject's right to access information and the retention period for personal and sensitive personal information, as well as other existing policies related to government employment records.

In addition, you mentioned that your request for a copy of your 201 files is to support your petition before the CSC to question your reassignment and your eventual dropping from the rolls. Thus, the request is made for the establishment, exercise or defense of legal claims which is a lawful criterion for processing under Section 13 (f) of the DPA, to wit:

SECTION 13. Sensitive Personal Information and Privileged Information. — The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: x x x

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

In EA and TA vs. EJ, EE and HC the Commission emphasized that:

“...processing as necessary for the establishment of legal claims” does not require an existing court proceeding. To require a court proceeding for the application of Section 13(f) to this instance would not only be to disregard the distinction provided in the law but the clear letter of the law as well. After all, the very idea of “establishment ... of legal claims” presupposes that there is still no pending case since a case will only be filed once the required legal claims have already been established.

7 EA and TA vs. EJ, EE and HC, NPC 17-018, Decision dated 15 July 2019, at page 8.
8 Civil Service Commission, “Addendum to CSC Memorandum Circular No. 8, s. 2007 on Management of 201/120 Files” [CSC Memorandum Circular No. 1, series of 2011], 17 January 2011 (available at <http://www.csc.gov.ph/phocadownload/userupload/itduser/mc01s2011.pdf>).

The turnover of 201 files under CSC Memorandum 1, Series of 2011 is separate from a government employees' exercise of his right to access.

The OIC-RD referred to CSC Memorandum Circular No. 1, Series of 2011 (MC 01-2011)⁸ in refusing to provide you with your 201 files. MC 01-2011, which is an addendum to MC 08-2007 on the Management of 201/120 files of government employees, provides for guidelines on how the turnover of 201/120 files should be done in case personnel resigns, retires or is separated.

Since you are requesting for your 201 file to support your petition against what you perceive to be an unjust personnel action, going through the processes described under MC 01-2011 might be against your interest. Thus, the NPC takes this opportunity to state that the exercise of your right to access your personal data is separate from the processes that a government employee needs to undergo for the turnover of 201 files in cases of separation, retirement, or resignation.

The NPC subscribes to the harmonization of existing laws and relevant government issuances. However, it must be noted that in this situation, you are contesting your separation from the service. This should not hinder your right to access your own personal data. Neither should your right to access your information be detrimental to your petition.

Moreover, it is evident that you are not requesting for the turnover of your 201 files but only for copies of the files to support your petition. On this note, MC 08-2007 provides that the head of office in charge of Human Resource Management shall “provide the personnel concerned with original copies of the agency and approved appointment as well as duplicate/machine copies of document in the 201/120 file for their own record.”⁹

This means that access to such information should be allowed even without the need to go through the process of turning over of 201 files. Further, MC 08-2007 provides that that the head of office in charge of Human Resource Management shall also be responsible for the establishment, maintenance and disposal of 201/120 files.¹⁰ Thus, in accordance with MC 08-2007 and NPC Advisory No. 2022-01, the Department of Agriculture should have a mechanism to enable

the exercise of the right to access personal and sensitive personal information, including its employees' 201 files, without stringent and excessive requirements.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished to us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved. Please be guided accordingly.

Very truly yours,

(Sgd.)

FRANKLIN ANTHONY M. TABAQUIN IV

Director IV, Privacy Policy Office

¹⁰ Id.

Ref No.: PDD-22-00301

ADVISORY OPINION

NO. 2022-026¹

23 November 2022



Re: **DISCLOSURE OF PERSONAL DATA THROUGH THE DATABASE OF INDIVIDUALS BARRED FROM TAKING CIVIL SERVICE EXAMINATIONS AND FROM ENTERING GOVERNMENT SERVICE (DIBAR)**

Dear [REDACTED],

We respond to your request for clarification on whether the online disclosure of personal data of dismissed officials/ employees through the Database of Individuals Barred from Taking Civil Service Examinations and from Entering Government Service (DIBAR), would violate the Data Privacy Act of 2012 (DPA),² considering that the posting of such personal data is part of the constitutional mandate of the Civil Service Commission (CSC).

We understand that the CSC, through the Integrated Records Management Office, developed the DIBAR which is an electronic database of government officials and employees who have been dismissed and precluded from being re-hired in the government service. The DIBAR contains information on the administrative decision against the concerned officials/ employees, which includes the offense committed and penalty imposed. It also contains the following: name, agency, civil service eligibility, date and place of exam, exam rating, gender, date and place of birth, occupation category, and position of the employee. This information is necessary for identity verification of a dismissed official/ employee to ensure that he/ she will neither be re-hired in the government service nor be able to retake any civil service examination.

¹ Tags: Civil Service Commission, constitutional mandate, exemption, disclosure, database, security measures, privacy impact assessment, proportionality, rights of data subjects, right to rectification.

² Republic Act (R.A.) No. 10173.

You further mentioned that the DIBAR was previously posted in the CSC Website accessible to all government agencies but was subsequently removed in 2018 as a form of self-regulation by the CSC in observance of the DPA.

Processing of personal data pursuant to a constitutional or statutory mandate; extent of exemption from the DPA

Section 4 of the DPA states that the law applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. Likewise, it provides for certain exemptions, including those personal data necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law.³

Such exemption, however, is only to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned.⁴ The non-applicability of the DPA or its Implementing Rules and Regulations (IRR) do not extend to personal information controllers (PICs) or personal information processors (PIPs), who remain subject to the requirements of implementing security measures for personal data protection.⁵ Thus, for the exemption to apply, the personal data processed by public authorities must be necessary to carry out their function as a law enforcement agency or regulatory body, and that such processing is in accordance with their constitutional or statutory mandate.

The CSC, as the central personnel agency of the government, is constitutionally mandated to establish a career service and adopt measures to promote morale, efficiency, integrity, responsiveness, progressiveness, and courtesy in the civil service. It shall strengthen the merit and rewards system, integrate all human resources development programs for all levels and ranks, and institutionalize a management climate conducive to public accountability.⁶

³ Data Privacy Act of 2012, § 4 (e); Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016), § 5 (d).

⁴ Rules and Regulations Implementing the Data Privacy Act of 2012, § 5.

⁵ Ibid.

⁶ PHIL. CONST. art. 9 (B) § 3; See also Executive Order No. 292, Book V, Title I, Subtitle A, Chapter 1, § 1.

We recognize that in order to uphold the principle of merit and fitness in the government service, the CSC has to establish a system for the selection and retention of those who are found to be qualified and the exclusion of those who have been adjudged unfit to hold government office due to having been dismissed for cause from the government service. Hence, it is within the CSC's mandate to develop and utilize the DIBAR for the purpose of identity verification of dismissed officials/employees for the use of all government agencies, and the same is treated as a special case under Section 5 (d) of the IRR of the DPA.

Implementation of security measures

We nonetheless underscore that as a PIC, the CSC is still required under the DPA to implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data within its custody.⁷ The security measures shall maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any unlawful processing.⁸

This obligates the CSC to ensure that any natural person acting under their authority and who has access to personal data in the DIBAR, processes the data contained therein only upon proper instruction or as required by law.⁹ The CSC should limit the access to DIBAR only to specific authorized users whose functions necessitate such access, such as the designated personnel from the Human Resource (HR) department/division of government agencies.

It is also incumbent upon the CSC to establish and implement data protection policies specific for the DIBAR, taking into account the nature, scope, context, and purposes of the processing, as well as the risks posed to the rights and freedoms of the dismissed officials/employees who are the data subjects.¹⁰ For further information on security measures for the protection of personal data, please refer to Sections 25-29 and 30-33 of the IRR of R.A. No. 10173.

Privacy impact assessment

⁷ Rules and Regulations Implementing the Data Privacy Act of 2012, § 25.

⁸ Ibid.

⁹ Ibid.

¹⁰ Rules and Regulations Implementing the Data Privacy Act of 2012, § 26 (b). ¹¹ Id. § 30-33.

We also highlight that all sensitive personal information in the DIBAR should be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, subject to the IRR and other issuances of the National Privacy Commission (NPC).¹¹ CSC should conduct a Privacy Impact Assessment (PIA) prior to the adoption of the DIBAR. In CID Case No. 17-K-003, we discussed the following:

“A PIA should be conducted prior to the deployment of a project, product, or service that involves the collection of personal information. When there are new or revised industry standards, organization policy, law or regulation, or when there are changes to methods in which personal information is handled, a personal information controller should conduct a PIA again on the pertinent process.

To emphasize, it should not only identify the existing controls and risks a project, product, or service may have upon personal data privacy, but it should lead to the identification of remedial actions or mitigation measures necessary to avoid or reduce those risks. These remedial actions and mitigation measures may be incorporated in the organization’s Privacy Management Program (PMP).”

For further guidelines, please refer to NPC Circular No. 2016-01 - Security of Personal Data in Government Agencies and NPC Advisory No. 2017-03 - Guidelines on Privacy Impact Assessments.

*Adherence to general data privacy principles;
proportionality*

In the implementation of the DIBAR, the CSC should also adhere to the general data privacy principles provided under the DPA and its IRR, particularly the principle of proportionality.

The CSC must ensure that the disclosure of personal data to the government agencies, through the DIBAR, is limited to the declared and specified purpose. Similarly, only those personal data that are adequate, relevant, suitable, necessary, and not excessive in relation to the purpose should be disclosed.

As such, personal data disclosed to the authorized users should be limited to information necessary to verify the identity of the dismissed officials/employees. The CSC should determine and evaluate whether all the personal data indicated are indispensable for the purpose of ascertaining the identity of those included in the DIBAR. Likewise, the DIBAR should not be publicly accessible online, considering that the information stated therein may be considered

sensitive personal information, particularly those involving the offense committed by the concerned officials/employees and the penalty imposed.

Fair and accurate processing; limitations on data subject rights

In addition, the CSC has the obligation to ensure that all personal data are processed fairly and lawfully, and are accurate, relevant and, kept up to date.¹² In case of inaccurate or incomplete personal data in the DIBAR, the same must be rectified, supplemented, destroyed or their further processing restricted by the CSC.¹³

The CSC should also provide means for the exercise of data subject rights. However, we emphasize that these rights are not absolute and may be duly restricted when necessary for public interest, protection of other fundamental rights, or when the processing of personal data is for investigations in relation to any criminal, administrative, or tax liabilities of a data subject, among others.

Considering the foregoing, we clarify the minimum requirements and recommend the following:

- Since the DIBAR was developed only for the use of all government agencies, CSC shall not provide access to the public, even though it is made available on its website. For this purpose, the CSC may update the DIBAR by incorporating an identity verification of the authorized users, such as requiring a username and password and other Multi-Factor Authentication (MFA) methods.
- Only authorized HR personnel from government agencies shall be given access to the DIBAR.
- There should be adequate safeguards to protect CSC's computer network against accidental, unlawful or unauthorized usage, or any interference which will affect data integrity or hinder the functioning or availability of the DIBAR.
- Prior to the adoption of the DIBAR, CSC should conduct a PIA.
- The CSC should have available mechanisms for the exercise of the rights of the data subjects where applicable, such as the right to rectification.

¹² Data Privacy Act of 2012, § 11 (b) (c).

¹³ Ibid.

We trust that the CSC is aware of its obligations under the DPA, its IRR, and issuances of the NPC, such as NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies and NPC Circular No. 16-03 on Personal Data Breach Management, among others.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

FRANKLIN ANTHONY M. TABAQUIN IV

Director IV, Privacy Policy Office



DECISIONS

ECV,
Complainant,

-versus-

NPC 18-074

For: Violation of the Data Privacy Act of 2012

CVF,

Respondents.

X-----X

DECISION

NAGA, P.C.;

Before this Commission is a Complaint filed by ECV against CVF for violating Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA).¹

Facts

ECV, in her Complaints-Assisted Form dated 23 July 2018, alleged that CVF obtained a copy of her Marriage Certificate “without any authority.”²

ECV narrated that on 30 November 2017, CVF humiliated her when the latter alleged that she was a mistress.³ When confronted by ECV’s son about her proof of such claim, CVF allegedly responded that she was able to get a copy of the Marriage Certificate of “the first family of UD from the [National Statistics Office].”⁴ The National Statistics Office (NSO) was the previous name of the Philippine

¹ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes, [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

² Complaints-Assisted Form dated 23 July 2018 of ECV, at page 2.

³ Id.

⁴ Id., at pages 2-3.

Statistics Authority (PSA).⁵

In a subsequent email to the Commission sent on 06 August 2018, ECV stated that CVF was able to acquire her Marriage Contract from the PSA without her knowledge and permission.⁶ ECV attached scanned copies of two (2) Philippine National Police (PNP) Incident Record Forms in the email to support her complaint.⁷ ECV narrated that CVF confronted her and said in the vernacular that she was a mistress.⁸ As evidence of the claim, CVF uttered that she had her NSO Marriage Certificate.⁹

Subsequently, ECV informed the Commission, through an email sent on 07 August 2018 at 1:46 AM, that she received a copy of CVF's administrative complaint against her for misconduct.¹⁰ She claimed that:

There are two Marriage Contract[s] from Philippine Statistics Authority attached in the last part of the affidavit that they have submitted to the Department of Education, Region X - Northern Mindanao, Cagayan de Oro City. The Marriage Contract belongs to RV & ECV and RV & EI. I know this is an opportunity to file a complaint and protect my rights.¹¹

In the email, ECV attached a Complaint dated 09 May 2018 filed before the Department of Education (DepEd) for Misconduct (DepEd Complaint), which included, as an attachment, ECV's Marriage Contract with RV dated 10 July 1987.¹² In a succeeding email sent at 1:47 AM of the same day, ECV attached a letter in response to the DepEd Complaint.¹³ In the letter, she claimed that CVF is in violation of Section 25 of the DPA.¹⁴

⁵ See An Act Reorganizing the Philippine Statistical System, Repealing for the Purpose Executive Order Numbered One Hundred Twenty-One, Entitled "Reorganizing and Strengthening the Philippine Statistical System and for Other Purposes", [Philippine Statistical Act of 2013], Republic Act No. 10625, § 28 (2013).

⁶ Email of ECV sent on 06 August 2018.

⁷ Id. PNP Incident Record Form Entry No. XXX-1 and PNP Incident Record Form Entry No. XXX-2, both dated 04 December 2017.

⁸ Id. at PNP Incident Record Form Entry No. XXX-2 dated 04 December 2017.

⁹ Id.

¹⁰ Email of ECV sent on 07 August 2018, 1:46 AM.

¹¹ Id.

¹² Id., See Complaint dated 09 May 2018 of CVF.

¹³ Email of ECV sent on 07 August 2018, 1:47 AM. See Letter dated 12 July 2018 of ECV.

¹⁴ Id. at page 1.

The Commission, through the Complaints and Investigation Division (CID), issued an Order to Confer for Discovery, which directed the parties to appear before the Commission on 18 October 2018.¹⁵

During the discovery conference, both parties appeared and manifested that they were willing to enter into a settlement.¹⁶ In an email sent on 09 November 2018, ECV manifested that the “agreed Amicable Settlement did not prosper”, and attached further evidence for the proceedings, including a Supplemental Complaint Affidavit dated 07 November 2018 (Supplemental Affidavit).¹⁷

The Supplemental Affidavit stated the following allegations, among others:

1. That I am the Complainant in the CID Case No. 18-5-074 xxx
2. That the Respondent is CVF xxx
3. That on November 30, 2017, while supervising the repair of our fence, she confronted me and uttered defamatory statements;
4. That the utterance expressed that I am only a mistress;
5. That my son JCV was agitated and immediately asked her if she has evidence regarding her allegations and the Respondent said that they obtained Marriage Contracts from the NSO. xxx

xxx

7. That the respondent answered that they have obtained from the NSO a Marriage Contract from another wife and our own Marriage Contract;
8. That on December 3, 2017, another incident occurred and I personally saw CF mother of the respondent waving a pieces of paper (sic) which happens to be my Marriage Contract and the Marriage Contract of my husband to his first wife while the respondent is uttering the same defamatory remarks;

xxx

¹⁵ Order to Confer for Discovery, undated, at page 1.

¹⁶ See Order dated 13 April 2019, at page 1.

¹⁷ Email of ECV sent on 09 November 2018.

10. That aside from the defamatory remarks uttered against me, she also filed a malicious complaint before Department of Education, Region X, charging me of Misconduct;

11. That some of the pieces of evidence attached are my Marriage Contract and the Marriage Contract of my husband to his other wife;¹⁸ (Emphases supplied)

In an Order dated 13 April 2019, the CID directed the parties to submit their Compromise Agreement within fifteen (15) days from receipt thereof. Should the parties fail to do so, CVF was ordered to file her Comment within ten (10) days from conclusion of the proceedings, ECV was given ten (10) days from their receipt of the comment to file her Reply, and CVF was given ten (10) days from receipt of the Reply to file her Rejoinder.¹⁹

CVF submitted a Manifestation of Compliance dated 07 June 2019.²⁰ She manifested that no compromise agreement was reached and attached her Responsive Comment to the Complaint.²¹

In her Responsive Comment dated 07 June 2019,²² CVF: 1) denied the allegation that she obtained ECV's Marriage Certificate, or that she made any processing in relation to said Marriage Certificate;²³ 2) claimed that ECV has long harassed CVF and her family, which led the latter to file the DepEd Complaint for Misconduct, docketed as Admin Case No. 10-18-027;²⁴ and 3) raised the defense that the Complaint should be dismissed outright for being filed beyond the reglementary period under Section 4(c), Rule II,²⁵ and Section 12 (b), (c), and (d), Rule III,²⁶ of NPC Circular No. 16-04 (2016 NPC Rules of Procedure).

ECV filed a Comment and Opposition dated 25 November 2019.²⁷ She reiterated the contents anchoring her complaint,²⁸ narrated various cases between the parties,²⁹ and alleged that the complaint

¹⁸ Supplemental Complaint Affidavit dated 07 November 2018 ECV, at pages 1-2.

¹⁹ Order dated 13 April 2019, at page 3.

²⁰ Manifestation of Compliance dated 07 June 2019 of CVF.

²¹ *Id.*, at page 1.

²² Responsive Comment dated 07 June 2019 of CVF.

²³ *Id.*, ¶¶ 1-4, at pages 3-4.

²⁴ *Id.*, ¶¶ 5-6, at page 4.

²⁵ *Id.*, ¶9, at page 5.

²⁶ *Id.*, ¶11, at pages 5-6.

²⁷ Comment and Opposition dated 25 November 2019 of ECV.

²⁸ *Id.*, ¶¶ 1-16, at pages 1-3.

before the Commission was timely filed.³⁰

In an Order dated 16 September 2021, the CID ordered the DepEd to submit a certified true copy of the case file for the DepEd Complaint docketed as Admin Case No. 10-18-XXX.³¹

In a Compliance dated 22 September 2021, the DepEd submitted certified true copies of various documents constituting the case file of the DepEd Complaint.³²

On 04 January 2022, the CID acknowledged receipt of the case files.³³ In relation to the Marriage Contract of RV and ECV (herein Complainant), the CID asked for confirmation whether the said document was originally filed by CVF, or the circumstance of how the document formed part of the case file.³⁴

In a Certification dated 12 January 2022, the DepEd certified “that a photocopy of the Marriage Contract between RV and ECV dated July 10, 1987, was attached, and included by CF when she filed the complaint against ECV before the Department of Education, Regional Office 10.”³⁵

Issues

- I. Whether the Complaint should be dismissed for being filed beyond the reglementary period.
- II. Whether Respondent violated Section 25(b) of the DPA.

Discussion

The Commission dismisses the Complaint for lack of merit.

I. The Commission exercises its authority to resolve the case on the merits.

²⁹ Id., at pages 4-9.

³⁰ Id., at page 10.

³¹ Order dated 16 September 2021, at page 1.

³² Compliance dated 22 September 2021 of the Department of Education- Region X, Northern Mindanao.

³³ Order dated 04 January 202[2], at page 1.

³⁴ Id.

³⁵ Certification dated 12 January 2022 of the Department of Education- Region X, Northern Mindanao.

ECV filed her complaint against CVF on 23 July 2018.³⁶ The first event to have allegedly violated her privacy rights happened on 30 November 2017, when CVF stated that she obtained ECV's Marriage Contract from the NSO.³⁷ The second relevant event was narrated in her Supplemental Affidavit dated 07 November 2018, when she stated that CVF attached her Marriage Contract in the DepEd Complaint.³⁸

NPC Circular No. 16-04, or the 2016 NPC Rules of Procedure, was the applicable procedural rules at the time of the filing of the complaint. Section 12(c) of the NPC Circular No. 16-04 allows for the outright dismissal of a complaint when it "is filed beyond the period for filing."³⁹

Further, this Commission refers to the last paragraph of the aforementioned Circular, viz:

SECTION 4. Exhaustion of remedies. – No complaint shall be entertained unless:

a. the complainant has informed, in writing, the personal information controller or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same;

b. the personal information controller or concerned entity did not take timely or appropriate action on the claimed privacy violation or personal data breach, or there is no response from the personal information controller within fifteen (15) days from receipt of information from the complaint;

c. and the complaint is filed within six (6) months from the occurrence of the claimed privacy violation or personal data breach, or thirty (30) days from the last communiqué with the personal information controller or concerned entity, whichever is earlier.

³⁶ Complaints-Assisted Form dated 23 July 2018 of ECV.

³⁷ *Id.*, at pages 2-3.

³⁸ Supplemental Complaint Affidavit dated 07 November 2018 of ECV, ¶11, at page 2.

³⁹ National Privacy Commission, Rules of Procedure, NPC Circular No. 16-04, §12(c) (15 December 2016) (NPC Circular 16-04).

The failure to comply with the requirements of this Section shall cause the matter to be evaluated as a request to the National Privacy Commission for an advisory opinion, and for the National Privacy Commission to take such further action, as necessary. The National Privacy Commission may waive any or all of the requirements of this Section, at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to the affected data subject.⁴⁰ (Emphasis supplied)

On its face, the complaint was filed beyond the six-month period, counted from November 2017. Nevertheless, the last paragraph of Section 4 of the 2016 Rules of Procedure allows the Commission to “waive any or all of the requirements of this Section, at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to the affected data subject.”⁴¹

The Commission exercises its authority to waive the requirement under Section 4(c) of the 2016 Rules of Procedure. ECV’s allegations, if substantially proven, may lead the Commission to conclude that there was a serious violation of the DPA. ECV may also have been seriously harmed due to the processing of her Marriage Contract, which was exposed to her employer, the DepEd.

Thus, the Commission finds it appropriate to exercise its authority to resolve the case on the merits.

II. CVF cannot be held liable for the violation of Section 25(b) or Unauthorized Processing of Sensitive Personal Information.

⁴⁰ Id., § 4.

⁴¹ Id.

The controversy essentially revolves around the processing of ECV's Marriage Contract.

The DPA defines processing as “any operation or any set of operations performed upon personal information including, but not limited to, the retrieval...storage, [and] use...of data.”⁴²

ECV narrated that on 30 November 2017, CVF said that she was able to obtain ECV's Marriage Contract from the NSO.⁴³ The Marriage Contract was later attached by ECV to the DepEd Complaint.⁴⁴

CVF denies these allegations. She reasons that, as stated by ECV herself, she would have no authority to obtain the document from the PSA, and “[t]hus, without such authority, it is legally impossible for the PSA to release the Complainant's Marriage Certificate or any personal information to Respondent.”⁴⁵

There are two instances of processing of personal data involved in this case: 1) the acquisition of ECV's Marriage Certificate; and 2) the submission of her Marriage Certificate as part of the DepEd Complaint.

a. There is no substantial evidence to show that the acquisition of ECV's Marriage Certificate was unauthorized.

In relation to the first processing, CVF “vehemently denies” that she obtained the Marriage Certificate of ECV and her husband.⁴⁶ However, it is not disputed that CVF, as the complainant in the DepEd Complaint, submitted ECV's Marriage Certificate to the government agency. This was affirmed by the DepEd itself when it certified that the Marriage Certificate “was attached, and included by CVF when she filed the complaint against ECV before the Department of Education, Regional Office 10.”⁴⁷

⁴² Data Privacy Act of 2012, § 3(j).

⁴³ Supplemental Complaint Affidavit dated 07 November 2018 of ECV, ¶7, at page 1.

⁴⁴ Id., ¶11, at page 2.

⁴⁵ Responsive Comment dated 07 June 2019 of CVF, ¶3, at pages 1-2.

⁴⁶ Id., ¶1, at page 1.

⁴⁷ Certification dated 12 January 2022 of the Department of Education- Region X, Northern Mindanao.

Thus, it can be reasonably concluded that CVF was able to obtain ECV's Marriage Certificate from the fact that she submitted it to the DepEd.

Under PSA Memorandum Circular No. 2017-09, dated 19 June 2017 (PSA Circular), the PSA enumerated the parties who may request an original and certified true copy of a Certificate of Live Birth, Certificate of Marriage, and Certificate of Death.⁴⁸ Pursuant to the Circular, the PSA may only release the Certificates to the following persons or entities:

1. The owner himself or through a duly authorized representative;
2. His/her spouse, parent, direct descendants, guardian or institution legally in-charge of him/her, if minor;
3. The court or proper public official whenever absolutely necessary in administrative, judicial or other official proceedings to determine the identity of a person;
4. In case of the person's death, the nearest of kin.⁴⁹

The evidence on record does not contain adequate information on when CVF actually acquired the Marriage Certificate. ECV, in her sworn statements, merely recounts CVF's alleged utterances of securing ECV's Marriage Certificate.⁵⁰ ECV only provided her own narrations, without any sufficient corroborating or equivalent proof, that establishes the period of CVF's acquisition of the document. If CVF obtained the Marriage Certificate after the issuance of the PSA Circular, there would be reasonable grounds for unauthorized processing since she is not one of the entities authorized to receive the Marriage Certificate.

48 Philippine Statistics Authority, Issuance of Original and Certified True Copy of Certificate of Live Birth, Certificate of Marriage and Certificate of Death, Memorandum Circular No. 2017-09, ¶ 2 (19 June 2017).

49 *Id.*

50 See Complaints-Assisted Form dated 23 July 2018 of ECV, at pages 2-3; Supplemental Complaint Affidavit dated 07 November 2018 of ECV, ¶¶ 5 & 8, at pages 1-2; PNP Incident Record Form Entry No. XXX-2 dated 04 December 2017, at page 2.

Since there is no substantial proof to show that CVF obtained the Marriage Certificate in violation of the PSA Circular, the Commission cannot conclude that CVF committed unauthorized processing in relation to the acquisition of the Marriage Certificate.

b. The use of ECV's Marriage

Certificate falls within processing that is necessary for the establishment, exercise or defense of legal claims.

There is no violation of Section 25(b) of the DPA.

The second processing relates to CVF's submission of ECV's Marriage Certificate to the DepEd as attachment to her complaint. To reiterate, DepEd certified that ECV's Marriage Contract "was attached, and included by CVF when she filed the complaint against ECV before the Department of Education, Regional Office 10."⁵¹

In ECV's Supplemental Affidavit, she prays that CVF be held liable for Section 25 of the DPA.⁵² This provision penalizes the unauthorized processing of personal information under Section 25(a), and sensitive personal information under Section 25(b).⁵³

The Commission finds it relevant to focus on Section 25(b) of the DPA. The unauthorized processing of sensitive personal information has three (3) elements, namely:

1. The accused processed information of the data subject;
2. The information processed is classified as sensitive personal information; and
3. The processing was done without the consent of the data subject or without authority under the DPA or any existing law.⁵⁴

The Commission finds the first element present. There is substantial evidence to show that CVF submitted ECV's Marriage Contract for the DepEd Complaint. As discussed, the DepEd issued a certification

⁵¹Certification dated 12 January 2022 of the Department of Education- Region X, Northern Mindanao.

⁵² Supplemental Complaint Affidavit dated 07 November 2018 of ECV, ¶ 22, at page 3.

⁵³ Data Privacy Act of 2012, § 25.

⁵⁴ NPC 18-077, Decision dated 15 April 2021, at page 6.

stating that CVF attached and included the Marriage Contract for her DepEd Complaint against ECV.⁵⁵ These actions squarely fall within the definition of processing, which includes the use of a data subject's personal information.⁵⁶

The second element of Section 25(b) of the DPA is also present. Under the DPA, sensitive personal information includes a person's marital race, status, and age.⁵⁷ ECV's Marriage Contract contains these pieces of information.

The last element of the crime requires that the processing be without the consent of the data subject or without authority under the DPA or any existing law.⁵⁸ This element, however, is absent. The Commission finds that the processing of ECV's sensitive personal information was anchored on Section 13(f) of the DPA, which provides:

SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

xxx

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.⁵⁹ (Emphasis supplied)

There are three (3) instances wherein Section 13(f) of the DPA is applicable: “(a) the proceeding is necessary for the protection of lawful rights and interests of natural persons in court proceedings; (b) the processing is necessary for the establishment, exercise or defense of legal claims; or (c) the processing concerns personal

⁵⁵ Certification dated 12 January 2022 of the Department of Education- Region X, Northern Mindanao.

⁵⁶ See Data Privacy Act of 2012, § 3j.

⁵⁷ Id., § 3(l).

⁵⁸ NPC 18-077, Decision dated 15 April 2021, at page 6.

⁵⁹ Data Privacy Act of 2012, § 13(f).

information that is provided to government or public authority.”⁶⁰

CVF’s submission of ECV’s Marriage Contract to the DepEd falls within processing that is necessary for the “establishment, exercise or defense of legal claims.”⁶¹

As stated in EA and TA vs. EJ, EE and HC:

The DPA should not be seen as curtailing the practice of law in litigation. Considering that it is almost impossible for Congress to determine beforehand what specific data is “necessary” or may or may not be collected by lawyers for purposes of building a case, applying the qualifier “necessary” to the second instance in Section 13(f) therefore, serves to limit the potentially broad concept of “establishment of legal claims” consistent with the general principles of legitimate purpose and proportionality.⁶²

In her DepEd Complaint, CVF alleged that ECV made malicious utterances against her and her family.⁶³ CVF also asked the DepEd “to conduct an investigation and consequently penalize the respondent for such misconduct.”⁶⁴

CVF submitted various pieces of evidence to support her DepEd Complaint, namely: 1) affidavits from her witnesses;⁶⁵ 2) Tax Declarations of Real Property;⁶⁶ 3) Joint Special Power of Attorney;⁶⁷ 4) Marriage Certificate of RV and EI;⁶⁸ 5) Marriage Certificate of RV and ECV;⁶⁹ and 6) pictures of CVF’s window showing the alleged actions done by ECV.⁷⁰

⁶⁰ EA and TA vs. EJ, EE and HC, NPC 17-018, Decision dated 15 July 2019, at page 8.

⁶¹ Data Privacy Act of 2012, §13(f).

⁶² EA and TA vs. EJ, EE and HC, NPC 17-018, Decision dated 15 July 2019, at pages 8-9.

⁶³ Complaint dated 09 May 2018 of CVF, ¶¶ 5-9, at pages 2-3.

⁶⁴ Id., ¶11, at page 3.

⁶⁵ Id., Annex “A” – Affidavit of RBF, and unmarked Annexes- Affidavits of CF, Gilbert Sanchez Jr., and HOR, all dated 20 April 2018.

⁶⁶ Id., unmarked Annexes – Tax Declaration of Property No. 14-XXX-XXXX, and Tax Declaration of Property No. 02-XXX-XXXX.

⁶⁷ Id., unmarked Annex – Joint Special Power of Attorney.

⁶⁸ Id., unmarked Annex – Marriage Certificate of RV and EI.

⁶⁹ Id., unmarked Annex – Marriage Certificate of RV and ECV.

⁷⁰ Id., unmarked Annex – various pictures.

To be clear, the Commission is not the proper body to determine the merits of the legal claims that are sought to be established, exercised, or defended by parties, pursuant to Section 13(f) of the DPA.⁷¹ It cannot rule on whether the Marriage Contract helps or detracts from CVF's complaint. Rather, the Commission's task is to determine whether the processing of personal information complies with the DPA, and other related issuances of the Commission.

Further, in relation to compliance with the DPA, the Commission emphasizes that though there may be lawful basis in processing personal or sensitive personal information, such as anchoring the processing in Section 13(f) of the DPA, the said processing must still adhere and be consistent with Section 11 of the DPA, which provides for the General Data Privacy Principles of transparency, legitimate purpose, and proportionality.⁷²

The DepEd Complaint relates to ECV's misconduct.⁷³ CVF contextualizes the "strained relationship" between the parties as a result of a boundary dispute,⁷⁴ and ECV's various gossips that tainted CVF and her family's reputation.⁷⁵ She argues that "[a] teacher's duty is not limited to being an agent of knowledge but, above all else, an agent of morals... A teacher, both in her official and personal conduct, must display exemplary behavior."⁷⁶

Given the context and allegations, the Commission finds that CVF's submission of ECV's Marriage Certificate was necessary for the establishment, exercise or defense of her legal claims against ECV. It should be emphasized that the processing of ECV's Marriage Certificate was not done in a vacuum but was in relation to the DepEd Complaint in order for CVF to support her allegations and to provide better context. In its Decision dated 23 April 2021, the DepEd used the "facts established and the evidence presented [to] support the findings of ECV's guilt".⁷⁷ The processing, given the surrounding context,

⁷¹ See EA and TA vs. EJ, EE and HC, NPC 17-018, Resolution dated 05 November 2020, at page 3.

⁷² Data Privacy Act of 2012, § 11.

⁷³ Complaint dated 09 May 2018 of CVF.

⁷⁴ Id., ¶ 1, at page 1.

⁷⁵ Id., ¶¶ 7-9, at pages 2-3.

⁷⁶ Id., ¶ 13, at page 3.

⁷⁷ Decision of the Department of Education- Region X, Northern Mindanao dated 23 April 2021, at page 3.

cannot be considered unlawful or illegal. It squarely falls within “the establishment, exercise or defense of legal claims” under Section 13(f) of the DPA.

Additionally, the processing is valid since the sensitive personal information was “provided to government or public authority.”⁷⁸ The nature of the information and the party’s purpose in providing it to the public authority should be connected to the latter’s mandate and in relation to the legal claims of the party.

As part of DepEd’s mandate, it is tasked to hear administrative charges against public school teachers, especially when they allegedly violate the Code of Professional Conduct for Teachers.⁷⁹ Here, the processing was in the context of ECV’s position as a public school teacher,⁸⁰ and her alleged violations of specific provisions of the “Philippine Code of Ethics for Professional Teachers”.⁸¹ The processing of sensitive personal information, which was provided to the DepEd for the necessary establishment of CVF’s legal claims, falls within Section 13(f) of the DPA.

Moreover, ECV failed to provide substantial evidence that CVF had no basis to process her Marriage Contract. The Commission emphasizes that the data subject’s consent is not the only basis for lawful processing of personal or sensitive personal information since Sections 12 and 13 of the DPA provide for other lawful bases for processing to be authorized.⁸² While ECV may not have consented to the processing of her Marriage Contract, such act may still be allowed if it is anchored on other bases provided in Section 13 of the DPA.

The Commission finds that there was a valid basis for processing ECV’s sensitive personal information through Section 13(f) of the DPA. Consequently, CVF has not violated Section 25(b) of the law since the processing was in relation to the establishment, exercise or defense of legal claims, and provided to a government body.

⁷⁸ Data Privacy Act of 2012, § 13(f).

⁷⁹ See The Magna Carta for Public School Teachers, Republic Act No. 4670, §§ 7-9 (1966); Department of Education, Revised Rules of Procedure of the Department of Education in Administrative Cases, DepEd Order No. 49, series of 2006, §§ 1, 8-10, 46 (12 December 2006).

⁸⁰ Complaint dated 09 May 2018 of CVF, ¶ 2, at page 1.

⁸¹ *Id.*, ¶¶ 14-15, at pages 3-4.

⁸² See Data Privacy Act of 2012, §§ 12 & 13.

WHEREFORE, premises considered, the Complaint is hereby **DISMISSED** for lack of merit.

SO ORDERED.

City of Pasay, Philippines.
17 March 2022.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

ECV

Complainant

CVF

Respondent

MB
Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

MLF,
Complainant,

-versus-

NPC 19-C-142

For: Violation of the Data Privacy Act of 2012

MYTAXI.PH CORPORATION
(GRAB PHILIPPINES),

Respondents.

X-----X

DECISION

AGUIRRE, D.P.C.;

Before this Commission is a complaint filed by MLF against MyTaxi. PH Corporation, doing business under the name of “Grab Philippines” (Grab Philippines), for an alleged violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

MLF, in his Complaints-Assisted Form, claimed that Grab Philippines committed violations of the DPA.¹

On 6 February 2019, he booked a car ride from UP Town Center² and was assigned to Grab driver ADB with Booking ID No. IOS-141-99938-8-345.³ As stated by MLF:

Within the Grab System[,], my Name [and] Mobile Number is [sic] made available to the driver. There is also an in[-]app chat function. Both Mobile Number and Chat function are made available with my consent under their terms and condition for the purpose of transacting a ride. So that driver and rider can communicate to meet each other.⁴

¹ Complaints-Assisted Form, 2 March 2019, at 1, in MLF v. MyTaxi.Ph Corporation, NPC Case No. 19- 142 (NPC 2019).

² Id. at 4.

³ Id. at 2.

MSH,
Complainant,
-versus-

NPC 18-142

For: Violation of the Data Privacy Act of 2012
BB, JA, AA

RSF & TCC,

Respondents.

X-----X

DECISION

NAGA, P.C.;

Before this Commission is a Complaint filed by MSH (MSH) against TCC (TCC), and its president, RSF (RSF) for the alleged violation of Republic Act No. 10173, or the Data Privacy Act of 2012 (DPA).

Facts

MSH filed a Complaint dated 25 September 2018 (Complaint) against respondents due to the discrepancies in her Transcript of Records (TOR), particularly the course and the Commission on Higher Education (CHED) Special Order Number (S.O. No.) indicated in the TOR.¹

MSH is a graduate of TCC, with a degree of Bachelor of Elementary Education (BEE), based on CHED's S.O. No. 50-140101-0126 s. 2008.²

From the records of the case, TCC issued two (2) TORs in the name of MSM. In the first TOR, dated 23 May 2008, the course stated was Bachelor of Secondary Education (BSE), instead of BEE. Meanwhile, the CHED S.O. No. found in the "remarks" portion was CHED S.O. No. 50-140102-0100 s. 2008.³ TCC issued a corrected TOR, dated

¹ Complaint Assisted Form dated 25 September 2018 filed by Complainant MSH.

² See Id; Transcript of Records dated 19 June 2018.

³ Transcript of Records dated 23 May 2008. Discrepancy underlined.

22 January 2018, which stated that MSH's course was "Bachelor of Elementary Education", however, there was still an error in the CHED S.O. number, by stating "CHED S.O. No. 50-140102-0126 s. 2008".⁴

MSH alleged that due to these discrepancies, her employer, San Francisco Parish School (SFPS), conducted a background check and concluded that her credentials were fake, to her "grave shame and public humiliation".⁵ Further, she is asking for "monetary settlement".⁶

The parties failed to reach an amicable settlement during the course of the proceedings.⁷ Thus, the Commission, through the Complaints and Investigation Division (CID), issued an Order dated 02 September 2021, directing the respondents to file a verified comment within fifteen (15) days from receipt of the Order.⁸

The respondents subsequently filed a Verified Comment dated 22 September 2021 (Verified Comment).⁹ In the Verified Comment, the respondents prayed for the dismissal of the Complaint for lack of cause of action and utter lack of merit.¹⁰

The respondents reasoned that upon learning of the discrepancies from MSH, the Registrar undertook the following actions: 1) an Affidavit of Discrepancy dated 18 June 2018 stating the correct information, and explaining that the discrepancies were "obviously caused by typographical error or pure excusable inadvertence xxx";¹¹ 2) a Certification dated 08 May 2018 stating the correct information, and further certifying that MSH was of "good moral character and has shown exemplary conduct during her stay in this institution";¹² and 3) another Certification dated 08 May 2018, explaining that the discrepancies were "misprinted", and attaching the corrected TOR and certified true copy of the diploma.¹³

Further, the respondents explained that they did not issue the

⁴ Transcript of Records dated 22 January 2018. Discrepancy underlined.

⁵ Complaint Assisted Form dated 25 September 2018 filed by Complainant MSH, at page 2.

⁶ Id., at page 3.

⁷ Undated Letter of Complainant MSH, transmitted through e-mail, on 20 November 2018.

⁸ Order (To File Verified Comment) dated 02 September 2021.

⁹ Verified Comment dated 22 September 2021 filed by RSF and TCC.

¹⁰ Id., at page 3.

¹¹ Id., at unmarked Annexes.

¹² Id.

¹³ Id.

incorrect TORs to SFPS, even though the latter requested the TORs as part of the background check, since there was no written authorization from MSH.¹⁴ Thus, there was no improper disclosure.

Issue

Whether the respondents violated the Data Privacy Act of 2012.

Discussion

The Commission deems it necessary to summarize the undisputed facts for a proper discussion of the case.

From the records, it is clear that there were two (2) TORs containing discrepancies, namely: the stated course and the CHED S.O. number of MSH.¹⁵ These discrepancies were subsequently rectified through an Affidavit of Discrepancy and two Certifications, both dated 08 May 2018, and both signed by the Registrar, providing the correct details and explaining the reasons for the discrepancies.¹⁶ Nevertheless, due to the incorrect TORs, MSH's employer, SFPS, conducted a background check and concluded that her credentials were fake.¹⁷

This Commission finds it undisputed that TCC is a personal information controller (PIC), since it “controls the collection, holding, processing or use of personal information.”¹⁸ MSH is the data subject for she is “an individual whose personal information is processed.”¹⁹ The personal information involved are the course and CHED S.O. number given that the data “when put together with other information would directly and certainly identify an individual”.²⁰ Here, TCC processed the personal information of MSH (course and CHED S.O. No) for the

¹⁴ *Id.*, at 2.

¹⁵ See Transcript of Record dated 23 May 2008, and Transcript of Record dated 22 January 2018.

¹⁶ Verified Comment dated 22 September 2021 filed by RSF and TCC.

¹⁷ Complaint Assisted Form dated 25 September 2018 filed by Complainant MSH.

¹⁸ Republic Act No. 10173, or the Data Privacy Act of 2012, Section 3(h).

¹⁹ Republic Act No. 10173, or the Data Privacy Act of 2012, Section 3(c).

²⁰ Republic Act No. 10173, or the Data Privacy Act of 2012, Section 3(g).

issuance of her TOR.

While TCC endeavored to rectify the discrepancies of MSH's personal information, the Commission finds that the respondent should indemnify MSH for the damages sustained due to the inaccurate and false information found in her previous TORs.

A PIC is obligated to ensure compliance, among others, with Section 11 of the DPA, providing for the General Data Privacy Principles. Particularly, Section 11(c) states:

SEC. 11. General Data Privacy Principles. – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

Personal information must be:

XXX

(c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted; xxx²¹ (Emphasis supplied)

In this regard, Section 19(c) of the Implementing Rules and Regulations of the DPA (IRR) requires PICs to ensure data quality, to quote:

SECTION 19. General Principles in Collection, Processing and Retention. — The processing of personal data shall adhere to the following general principles in the collection, processing, and retention of personal data:

xxx

c. Processing should ensure data quality.

1. Personal data should be accurate and where necessary for declared, specified and legitimate purpose, kept up to date.

2. Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.²² (Emphases supplied)

Meanwhile, a data subject has the right to rectification under Section

²¹ Republic Act No. 10173, or the Data Privacy Act of 2012,, Section 11(c).

34 of the IRR:

SECTION 34. Rights of the Data Subject. — The data subject is entitled to the following rights:

XXX

d. Right to rectification. The data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: Provided, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.²³ (Emphasis supplied)

Separate from the data subject's right to rectification is the right of a data subject to damages anchored on Section 16(f) of the DPA, which provides:

SEC. 16. Rights of the Data Subject. – The data subject is entitled to:

xxx

(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.²⁴

Based on Section 11(c) of the DPA, and Section 19(d) of the IRR of the DPA, the respondent, being a PIC, had the obligation to ensure that MSH's personal information was accurate and up to date. Yet, the fact that TCC separately issued two (2) inaccurate TORs reveals a clear lapse in ensuring diligent compliance with the DPA. MSH acted in the exercise of her right to rectification due to the inaccurate and false information stated in the two (2) TORs.

The Commission notes that TCC subsequently undertook to correct and update the TORs.²⁵ Nevertheless, the issuance of

²² Implementing Rules and Regulations of Republic Act No. 10173, Section 19(c).

²³ Implementing Rules and Regulations of Republic Act No. 10173, Section 34(d).

²⁴ Republic Act No. 10173, or the Data Privacy Act of 2012, Section 16(f).

inaccurate information, in itself, caused damage to MSH. Due to the discrepancies, SFPS found it necessary to conduct a background check to verify the authenticity of the credentials and integrity of MSH.²⁶ This would have been avoided if TCC had more stringent measures in place to ensure data quality.

Section 16(f) of the DPA allows for indemnification in favor of the data subject when it is shown that there were damages sustained, and the cause of the injury was due to “inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.”²⁷ As discussed, the Commission finds that damages were sustained by MSH, despite TCC’s subsequent rectification of the inaccurate personal information. Thus, Section 16(f) of the DPA is applicable.

The Commission finds that Section 16(f) of the DPA is applicable since: 1) there was inaccurate and false information contained in two (2) TORs issued by TCC; and 2) there was damage because these discrepancies cast doubt on MSH’s credentials and employment. TCC’s subsequent rectification of the TORs does not prohibit indemnification in favor of MSH.

As to the type and amount of damages to be awarded, it is appropriate to award MSH nominal damages. The award for nominal damages is proper when “a legal right is technically violated and must be vindicated against an invasion that has produced no actual present loss of any kind or where there has been a breach of contract and no substantial injury or actual damages whatsoever have been or can be shown.”²⁸

It has been ruled that “[t]he assessment of nominal damages is left to the discretion of the court/tribunal, according to the circumstances of the case.”²⁹

²⁵ See Verified Comment dated 22 September 2021 filed by RSF and TCC.

²⁶ See Complaint Assisted Form dated 25 September 2018 filed by Complainant MSH, at page 2; and Verified Comment dated 22 September 2021 filed by RSF and TCC, at page 2.

²⁷ Republic Act No. 10173, or the Data Privacy Act of 2021, Section 16(f).

²⁸ MCC Industrial Sales Corp. v. Ssangyong Corp., G.R. No. 170633, 17 October 2007.

Taking into consideration the circumstances of the case, the Commission finds that damages in the amount of ten thousand pesos (Php 10,000.00) is proper.

While MSH impleaded RSF, TCC's president, as a respondent in the case, only TCC is the proper party to indemnify her given that TCC is the PIC. Further, MSH has not proven that RSF had any intentional or direct involvement with the discrepancies.

The Commission notes that TCC subsequently rectified the discrepancies found in the two (2) separate TORs, thus honoring her right to rectification. Nevertheless, the issuance of the incorrect TORs affected MSH's employment, and led to her employer conducting background checks on her credentials. Worse, it concluded that her credentials were fake. This would have all been avoided if TCC was zealous in ensuring data quality. It committed lapses in this obligation by issuing two incorrect TORs. Hence, the propriety of the award.

WHEREFORE, premises considered, this Commission ORDERS Respondent, TCC, to:

1. INDEMNIFY the Complainant, MSH, in the amount of ten thousand pesos (Php 10,000.00) for the damages sustained due to Respondent's issuance of inaccurate and false information, pursuant to Section 16(f) of the Data Privacy Act of 2012; and
2. SUBMIT proof of compliance by Respondent with the abovementioned award within fifteen (15) days upon receipt of this Decision.

SO ORDERED.

City of Pasay, Philippines.

03 February 2022.

Sgd.

²⁹ EA v. Q2 88, Inc., NPC 18-103, 23 July 2020, at page 7.

JOHN HENRY D. NAGA

Privacy Commissioner

I CONCUR:

Sgd.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

Copy furnished:

MSH

Complainant

RSF and TCC

Respondents

COMPLAINTS AND INVESTIGATION DIVISION

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

CL,
Complainant,

-versus-

NPC No. 19-030
(formerly CID Case No. 19-A-030)
For: Violation of the Data Privacy Act of 2012

CL, DDZ,
Respondents.

X-----X

DM,
Complainant,

-versus-

NPC No. 19-132
(formerly CID Case No. 19-B-132)
For: Violation of the Data Privacy Act of 2012

DDZ,
Respondents.

X-----X

DECISION

NAGA, P.C.;

Before this Commission are the complaints separately filed by Mr. CL and Mr. DM against Mr. DDZ for alleged violations of the Data Privacy Act (DPA) of 2012.

Facts

CL, DM, and DDZ were personnel of MVP, a company located at Clark Freeport Zone. On 22 November 2018, DDZ was terminated by MVP as Accounts Executive Officer.

On 28 November 2018, DDZ filed a case before the Office of the City Prosecutor of Mabalacat, Pampanga against DM, a member of the

MVP Board of Directors, and IP, an Executive Assistant to the CEO, for theft.

On 28 December 2018, DDZ moved to amend his original complaint to include CL and alleged grave coercion and light threats. Attached to DDZ's complaint-affidavit to the Office of the City Prosecutor is a letter to the Department of Labor and Employment (DOLE) attaching copies of CL's and DM'S passports as evidence.¹ As indicated in his complaint-affidavit, DDZ also sent copies of the passports in his letters to the Clark Development Corporation (CDC) and the Bureau of Immigration (BI).

On 16 and 25 January 2019, CL and DM filed a complaint before the Commission, respectively. Both Complaints alleged that DDZ violated the DPA for revealing their passport without their consent, and that DDZ, may have broken into MVP's database where the scanned copies of the passports are stored. Complainants also stated that the attachment of their passports in the complaint filed before the Office of the Prosecutor, DOLE, CDC, and BI was for the purpose of harassing the Complainants.²

CL prayed that DDZ be held liable for the violations of Section 29 of the DPA. He also prayed for DDZ to be deported for the aforementioned violation. While DM prayed that DDZ be held liable for the violation of Sections 29 and 31 of the DPA.

DDZ filed an Answer to CL dated 07 June 2019 and to DM dated 16 August 2019. In his separate Answers, he argued that the Complaints before the NPC is a form of retaliation from Complainants since they are in danger of being deported for working in the Philippines without the necessary working VISA.

He also argued that the Commission should not have entertained the complaints for failing to exhaust all remedies as provided in Section 4 of the NPC Circular No. 16-04. Further he stated that, assuming that the complaint is valid, the passports are excluded from the coverage of Section 4(e) of the DPA and that the processing of such information is permitted under Section 12 (e) and (f) and 13 (f) of the DPA.³ In addition, he stated that he was able to obtain the passports upon legitimate request from SM (former Operations Manager) and

¹ Records (NPC Case No. 19-030) at 1 to 31, and Records (NPC Case No. 19-132) at 1-19.

² Records (NPC Case No. 19-030) at 1 to 9, and Records (NPC Case No. 19-132) at 1 to 6.

³ Records (NPC Case no. 19-030) at p. 89 to 90, and Records (NPC Case no. 19-132) at p. 45 to 46 and 78.

DMV (former President and CEO), fully disclosing the purpose of where the passports are going to be used.⁴

On 01 July 2019 and 12 September 2019, CL and DM filed their Reply, respectively.⁵ Complainants maintain that DDZ failed to explain how he was able to obtain his sensitive personal information and that DDZ illegally obtained their passports and used it without their consent. They also argued that the use of their passports is not covered in the exceptions mentioned in Section 4(e) and Section 12(e) and (f) of the DPA. Further, CL reiterated his arguments in his previous complaint that DDZ has no authority/access to his sensitive personal information and therefore, has violated the DPA.

In his Rejoinder⁶, DDZ reiterated his arguments in his Answer. He also stated that he was dismissed on November 27, 2018, and his letter to DOLE was received on December 18, 2018 which shows that he can no way enter the premises of MVP earlier than the date of his dismissal. He then prays for the Complaints to be dismissed for failure to exhaust remedies under Section 4 of the DPA and for the lack of merit.

Issues

1. Whether the Complaints are exempted from Section 4 of the NPC Circular No. 16-04.
2. Whether the Respondent violated the Data Privacy Act.
3. Whether Respondent committed unauthorized access or intentional breach in processing Complainants' passports.

Discussion

The Complaints for the violation of the DPA lack merit.

- I. The Complaints are exempted from Section 4 of the NPC Circular 16-04

⁴ Id. at p. 51 to 58, and p. 41 to 49.

⁵ Id. at p. 71 to 78, and p. 62 to 70.

⁶ Records (NPC Case no. 19-030) at 88 to 93, and Records (NPC Case no. 19-132) at 72 to 79.

In his Answer and Rejoinder, Respondent argues that the Commission should not have entertained the Complaints for failing to exhaust all remedies under Section 4 of NPC Circular No. 16-04. This Commission refers to the last paragraph of the aforementioned Circular, viz:

SECTION 4. Exhaustion of remedies. – No complaint shall be entertained unless:

- a. the complainant has informed, in writing, the personal information controller or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same;
- b. the personal information controller or concerned entity did not take timely or appropriate action on the claimed privacy violation or personal data breach, or there is no response from the personal information controller within fifteen (15) days from receipt of information from the complaint ;
- c. and the complaint is filed within six (6) months from the occurrence of the claimed privacy violation or personal data breach, or thirty (30) days from the last communiqué with the personal information controller or concerned entity, whichever is earlier.

The failure to comply with the requirements of this Section shall cause the matter to be evaluated as a request to the National Privacy Commission for an advisory opinion, and for the National Privacy Commission to take such further action, as necessary. **The National Privacy Commission may waive any or all of the requirements of this Section, at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to the affected data subject.⁷ (Emphasis supplied)**

Further, Rule II, Section 2 of the NPC Circular No. 2021-01 provides:

The NPC may waive any or all of the requirements of this Section at its discretion upon (a) good cause shown, properly alleged and proved by the complainant; or (b) if the allegations in the complaint involve a serious violation or breach of the Data Privacy Act of 2012, taking into account the risk of harm to the affected data subject, including but not limited to:

- i. when there is grave and irreparable damage which can only be prevented or mitigated by action of the NPC;
- ii. when the respondent cannot provide any plain, speedy or adequate remedy to the alleged violation;
- iii. or the action of the respondent is patently illegal. (Emphasis supplied)

⁷ Section 4 of NPC Circular 16-04

This Commission recognizes that it is afforded with a broad range of powers to implement its mandate such as the power to waive the requirements of its Rules of Procedure. However, there are two alternate factors to be taken into account should it decide to waive the requirements of the aforementioned section: (a) good cause shown, properly alleged and proved by the complainant; or (b) if the complaint involves a serious violation or breach of the DPA, taking into account the risk of harm to affected data subjects.

Moreover, this Commission takes this opportunity to remind its previous ruling in NPC Case No. 19-528, which states that the purpose of Section 4 of NPC Circular No. 16-04 is to prevent the unduly clogging of the Commission's docket and avoid instances wherein a case shall be dismissed despite the good cause shown by the Complainant or the case involves a serious violation of the DPA. This Commission also reminds that the Rule is meant to prohibit instances of deciding cases based on mere technicalities.⁸

Additionally, it shall be emphasized that the personal information of Complainants were already processed by the Respondent when he requested and accessed the passports and included it to his Complaint-Affidavit. In this case, the Rule can no longer apply given that the Respondent cannot take any appropriate action to remedy the situation since the passports were already included in the Complaint-Affidavit filed before the Office of the Prosecutor and cannot be withdrawn.

The Commission also finds that the Complaints involve a possible violation of the DPA given the alleged unauthorized processing of passports by the Respondent since the passports processed contain sensitive personal information, and the processing of such information is generally prohibited subject only to a few exceptions. In addition, the processing of sensitive personal information involved may pose a risk of serious harm to the affected data subjects since the personal information involved may be used to enable identity fraud, theft, crimes, and other harm.

Further, as the Complainants allege the violation of Criteria for Lawful Processing of Personal Information, Sensitive Personal Information, and Unauthorized Access or Intentional Breach⁹ due to the processing

⁸ Resolution, NPC Case No. 19-528. Dated 23 February 2021.

of their passports without their consent and unauthorized access to their personal information, this Commission then finds that it is but proper to waive the requirement under Section 4 of NPC Circular No. 16-04. This is in consideration of the possible risk of harm to the affected data subjects and that the Complaints involve a serious violation or breach of the DPA.

II. Respondent's processing of passports

is permissible under the Data Privacy Act of 2012

Respondent stated that he was able to obtain a copy of CL and DM's passports through a legitimate request from the Human Resources (HR) of MVP, SM (former Operations Manager), and DMV (former President and CEO) wherein he fully disclosed the purpose of his request of attaching the information in his complaint-affidavit. In his Rejoinder to CL's Reply, Respondent stated:

11. Respondent upon his legitimate request with the HR of MVP, with full complete statements of the purpose for which such Information was needed, was provided with the copy of complainant's passport. There is no way can the respondent enter the premises of MVP since he was dismissed, albeit illegally, from his employment and prevented to enter the MVP;¹⁰

In his Answer to DM's Complaint, which he then also reiterated in his Rejoinder for this case, Respondent stated:

20. Respondent, upon his legitimate request with the employees of MVP, particularly SM, the former Operations Manager, and DMV, the former President and CEO, with full complete statements of purpose for which such Information was needed, was provided with the copy of complainant's passport. There is no way the respondent can enter the premises of MVP since he was dismissed, albeit illegally, from his employment and prevented to enter MVP;¹¹

At the outset, it shall be emphasized that in this case, there are two forms of processing involved. Section 3(j) of the DPA defined processing as:

- (j) Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection,

⁹ Sections 12, 13 and 29, DPA.

¹⁰ Records (NPC Case No. 19-030) at p. 91.

¹¹ Records (NPC Case No. 19-132) at p. 46.

recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.¹²

The first processing conducted by DDZ was when he requested for CL and DM's passports from MVP's officer and successfully collected such information. The second processing was when DDZ used the copy of Complainants' passports as attachment to his complaint-affidavit before the Office of the Prosecutor of Mabalacat, Pampanga, Letter to DOLE, CDC, and BI.

As previously discussed, passports contain sensitive personal information wherein its processing is generally prohibited subject only to a few exceptions. Such exceptions are provided in Section 13(f) of the DPA, thus:

SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

- (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.¹³ (Emphasis Supplied)

This Commission then finds that Respondent's request and access to the copies of CL and DM's passports fall under the exception as stated in Section 13(f) of the DPA, specifically, the processing is necessary for the establishment, exercise or defense of legal claims. As previously ruled by the Commission in NPC Case No. 17-018, "the relationship of the parties during the processing and judicial ties between them are being considered in determining valid reliance to Section 13(f) of the DPA."¹⁴ In this case, Respondent's attachment of CL and DM's passports to his DOLE letter attached in his complaint-affidavit to the Office of the Prosecutor is to show factual antecedent for his allegations of theft and grave coercion against Complainants. It also alleges that both CL and DM are Australian citizens without valid working visas in the Philippines.

Likewise, the second processing by Respondent wherein he submitted the copies of passports as attachment to his letter to

¹² Section 3(j) of the Data Privacy Act of 2012.

¹³ Section 13(f) of the DPA.

DOLE, CDC and BI which were attached to his complaint-affidavit to the Office of the Prosecutor, also falls under the same exception stated in the aforementioned section.

It must be noted that DDZ's allegations of CL and DM's grave threats and illegal stay in the Philippines are under the investigative powers of these government agencies. The Office of the Prosecutor has the investigative powers on all charge of crimes, misdemeanors, and violations of penal laws and ordinances within their respective jurisdictions.¹⁵ While, the Secretary of Labor has the visitorial power to inspect the premises, books of accounts and records of any person or entity covered by the Labor Code, require it to submit reports regularly on prescribed forms, and act on violation of any provisions of the Labor Code.¹⁶

CDC as the operating and implementing arm of the Bases Conversion and Development Authority (BCDA), is authorized to manage the Clark Special Economic Zone (CSEZ).¹⁷ And finally, the functions of the Bureau of Investigation primarily include the administration and enforcement of immigration, citizenship and alien admission and registration laws in accordance with the provisions of the Philippine Immigration Act of 1940, as amended (C.A. No. 613, as amended).¹⁸

Moreover, this Commission takes this opportunity to reiterate its ruling in a previous case¹⁹, that the processing of personal and sensitive personal information relying in Section 13(f) must still adhere and be consistent with Section 11 of the DPA or the General Data Privacy Principles of transparency, legitimate purpose, and proportionality. Further, Section 13(f) requires that the processing activities shall be done within the limits of the law, such entails the obligations of the controller to comply with the requirements of the DPA.

III. Respondent cannot be held liable
for the violation of Section 29 of the DPA
or Unauthorized Access or Intentional Breach

CL and DM alleged that DDZ may have broken into the MVP's database where the scanned copies of their passports are stored.

¹⁴ Resolution, NPC Case No. 17-018. Dated 05 November 2020.

¹⁵ Section 9(b) of the Republic Act No. 10071.

¹⁶ Article 37 of the Labor Code of the Philippines.

¹⁷ Section 1 of Executive Order No. 80, Series of 1993

¹⁸ Section 31 of the Administrative Code of 1987

However, Complainants failed to provide substantial proof to support their allegations and prove that a violation of Section 29 or Unauthorized Access or Intentional Breach were committed by the Respondent. Section 29 of the DPA states:

SEC. 29. Unauthorized Access or Intentional Breach. – The penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.²⁰ (Emphasis Supplied)

Complainants were not able to demonstrate by substantial evidence the very corpus delicti of the crime which is the instance that the Respondent breaks into the data system where personal or sensitive personal information of the MVP is stored. Section 22 of NPC Circular No. 16-04 provides, “the Decision of the Commission shall adjudicate the issues raised in the complaint on the basis of all the evidence presented and its own consideration of the law.” (Emphasis Supplied)

Further, as the Supreme Court held in *Florencio Morales, Jr. v. Ombudsman Conchita Carpio-Morales, et. al.*, “The basic rule is that mere allegation is not evidence and is not equivalent to proof. Charges based on mere suspicion and speculation likewise cannot be given credence. When the complainant relies on mere conjectures and suppositions, and fails to substantiate his allegations, the complaint must be dismissed for lack of merit.”²¹

With only mere allegations and absent the supporting evidence to prove that Respondent indeed broke into the database of MVP to obtain the copies of their passports, such allegations cannot be given credence by the Commission. Thus, this Commission finds that Respondent cannot be found to have committed a violation of Section 29 of the DPA or Unauthorized Access or Intentional Breach. WHEREFORE, all premises considered, this Commission resolves that the instant Complaints filed by CL and DM are hereby DISMISSED for lack of merit.

¹⁹ Resolution, NPC Case No. 17-018. Dated 5 November 2020.

²⁰ Section 29 of the Data Privacy Act of 2012.

SO ORDERED.

City of Pasay, Philippines.
10 June 2021.

SGD.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

SGD.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner
SGD.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

CL
Complainant

DM
Complainant

MJRVLO
Counsel for Complainants

DDZ
Respondent

PMB
Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

JRO,
Complainant,

-versus-

NPC No. 19-278

For: Violation of the Data Privacy Act of 2012

MSMI,
Respondent.

X-----X

DECISION

NAGA, P.C.;

Before this Commission is a Complaint filed by JRO (JRO) against MSMI (MSMI) for an alleged violation of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA).¹

Facts

JRO, in his Complaints-Assisted Form dated 27 March 2019 (Complaint), alleged that he had resigned from his employer, MSMI, on 31 December 2018.² He was formerly MSMI's Philippine Overseas Employment Administration (POEA) liaison officer/processing officer.³ Despite his resignation, his personal account, including his name and POEA Code SB-003621, was still used to process MSMI's seafarer transactions through Oller's email address.⁴ He learned about this upon verification from the POEA and when he received documents from concerned seafarers.⁵

JRO alleges that he is "suffering from extreme anxiety, sleepless nights, and mental anguish" due to these actions.⁶ He seeks for

¹ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes, [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

² Complaints-Assisted Form dated 27 March 2019 of JRO, at page 3.

³ Id.

⁴ Id.

⁵ Id.

reasonable damages and permanent revocation of MSMI's POEA license.⁷ JRO also seeks for a ban on the processing of personal data due to “unlawful acts which constitute estafa, cybercrime infringements and other criminal, civil and administrative violations.”⁸

As proof, JRO attached an image of his POEA ID, Certificate of Employment, and screenshots of various emails allegedly from POEA eServices.⁹

Two screenshots showed the following entries supposedly from POEA eServices:

[Sent by POEA eServices on 12 Mar, 17:00]

Dear XXXX,

Your Application status has is (sic) now Completed by SB-003621: JRO from MSMI agency

xxx

[Sent by POEA eServices on 12 Mar, 16:38]

Dear XXXX,

Your Application status has is (sic) now For Printing by SB-003621: JRO from MSMI agency ¹⁰

Forwarded messages from “MA” to JRO contained various messages from the alleged email of POEA eServices (eservices@poea.gov.ph) that relates to the status of the POEA application, containing the following entries:

⁶ Id., at page 4.

⁷ Id.

⁸ Id.

⁹ Id.

¹⁰ Id., see unmarked Annexes.

Dear XXXX,

Your Application status has is (sic) now For Payment by SB-003621: JRO from MSMI agency

xxx

Dear MA,

Your Application status has is (sic) now For Printing by SB-003621: JRO from MSMI agency

xxx

Dear MA,

Your Application status has is (sic) now Completed by SB-003621: JRO from MSMI agency

xxx

Dear MA,

Your Application status has is (sic) now For Contract by SB-003621: JRO from MSMI agency¹¹

Another screenshot from “TE” also contains a forwarded message from POEA eServices relating to the status of a POEA Application:

Dear XXXX,

Your Application status has is (sic) now Completed by SB-003621: JRO from MSM agency¹²

Through the Complaints and Investigation Division (CID), the parties were ordered to appear before the Commission to confer for discovery on 18 June 2019.¹³ In the discovery conference, both parties appeared.¹⁴ MSMI, through counsel, manifested that it will be filing a Motion to Dismiss.¹⁵ Thus, it was given fifteen (15) days from the discovery conference to submit the same. Meanwhile, JRO was given fifteen (15) days from receipt of the Motion to Dismiss to file a Comment, with another five (5) days from receipt of the Comment for MSMI to file a Reply.¹⁶

¹¹ Id.

¹² Id.

¹³ Order to Confer for Discovery dated 24 April 2019, at page 1.

¹⁴ Order dated 18 June 2019, at page 1.

¹⁵ Id.

¹⁶ Id.

MSMI, through counsel, filed its Motion to Dismiss dated 02 July 2019 (Motion to Dismiss).¹⁷ In the Motion to Dismiss, MSMI stated the following context as part of its defenses:

1. MSMI is a duly licensed manning agency (LMA) which is “engaged in the provision of quality crew manning services to ship owners, ship operators and ship managers engaged in international maritime business.”¹⁸ As part of its primary business as an LMA, it “is required by the POEA under Memorandum Circular No. 06-2018...to register with the latter’s web-based in-house contract processing system known as the Sea-based e-Contracts System (“SBECS”) online in order to have the standard employment contracts of its prospective seafarers processed and approved prior to deployment.”¹⁹
2. In the SBECS registration procedure, an LMA, like MSMI, is mandated to submit to the POEA a Request for Enrollment and Availment of POEA e-Services (REAPS) which contains the complete names and emails of a maximum of three users.²⁰ Once the registration requirements are met, POEA will enroll and finalize the credentials and machine of the submitted users, and when authenticated, the “SBECS will only recognize that machine and the duly-registered access credentials.”²¹
3. The SBECS enables the LMA “to upload scanned copies of their standard employment contracts with prospective seafarers for POEA’s processing and approval. Once processing has been completed, notification is sent to the registered e-mail addresses of the LMA-nominated user.”²²

MSMI claims that JRO was employed as its POEA liaison officer from 16 November 2012 up to 31 December 2018, and had the obligation of liaising with POEA, which included processing documents, managing MSMI’s accounts, and using the company-supplied computers.²³ Part of JRO’s responsibilities was the processing of documents in POEA’s system, namely, the Sea-based e-Contracts System (SBECS).²⁴

¹⁷ Motion to Dismiss dated 02 July 2019 of MSMI

¹⁸ *Id.*, ¶ 1.

¹⁹ *Id.*, ¶ 2.

²⁰ *Id.*, ¶ 3.

²¹ *Id.*

²² *Id.*, ¶ 4.

²³ *Id.*, ¶¶ 5-6.

²⁴ *Id.*, ¶ 6(a).

The SBECS was established by the POEA as a “secured web-based facility” developed for licensed manning agencies (LMAs) in order to “submit online 24/7 their request for processing (RFP), pay online the POEA processing and [Overseas Workers Welfare Administration] membership fees, submit online the seafarer’s contract and print the electronic Overseas Employment Certificate (OEC) of the seafarers in the comfort of the agency’s office.”²⁵

During JRO’s employment, he was nominated as an authorized user of the SBECS through the company-issued email: jr.o@msm.com.ph, “which was specifically provided for purposes of accessing Respondent’s SBECS account.”²⁶ At the time of his resignation, MSMI alleges that JRO “was the only SBECS user officially registered to the system on behalf of Respondent.”²⁷

When JRO resigned, MSMI submitted a letter to POEA informing them about the resignation, and that its new liaison officer was RDR.²⁸ This letter was duly acknowledged by POEA. However, according to MSMI, it was only on 05 April 2019 that MSMI received POEA’s confirmation that it may now use its company account for its new liaison officer to process seafarer contracts in the SBECS.²⁹

Before POEA’s confirmation, MSMI “was not able to receive the access credentials for its new POEA Liaison Officer in time to address [JRO’s] departure.”³⁰ Thus, MSMI alleges that it was “compelled by the legitimate need to maintain its business operations which requires, among others, the ongoing processing of its seafarers’ POEA contracts, [and] continued to access its SBECS account using the credentials registered with the company e-mail address jr.o@msm.com.ph until 04 April 2019.”³¹

²⁵ Id., See Annex “C”, citing Philippine Overseas Employment Administration, Memorandum Circular No. 06, series of 2018, New Procedure for Online Registration of Seafarers and Seabased e-Contracts System (SBECS), ¶ 1, ¶ 2 (POEA Memorandum Circular No. 06-2018).

²⁶ Id., ¶¶ 7-8.

²⁷ Id., ¶ 7.

²⁸ Id., ¶ 9.

²⁹ Id., ¶¶ 9-10.

³⁰ Id., ¶ 9.

³¹ Id.

MSMI contends that the POEA-registered account is not personally registered or owned by JRO, especially since only LMAs are allowed to register in the SBECs.³²

Even assuming that MSMI was processing JRO's personal information, the processing was lawful pursuant to MSMI's legitimate interest based on Section 12(f) of the DPA.³³ MSMI claims that JRO's resignation placed the company in a "dire situation considering that POEA had yet to approve the access credentials of its new POEA Liaison Officer."³⁴ If MSMI did not use the POEA account, "it would've experienced debilitating work stoppage for a period of four (4) months because of its inability to process seafarer contracts."³⁵

MSMI claims that it did not get any complaints from JRO about the company's use of the "access credentials for purely business-related purposes", and so was shocked when it received JRO's Complaint through the Order to Confer Discovery dated 24 April 2019.³⁶

Thus, MSMI prays for the Complaint's dismissal based on the following reasons: 1) the Complaint is not a violation of the DPA or does not involve a privacy violation, meriting outright dismissal;³⁷ and 2) Oller failed to follow the exhaustion of remedies since it did not inform MSMI, in writing, about the alleged privacy violation.³⁸

In response, Oller filed a Comment and Opposition to the Motion to Dismiss dated 02 July 2019 with Prayer for the Issuance of Cease and Desist Orders as Provided for Under Chapter II, Section 7(a)(b) (c)(d) AND (i) of R.A. 10173, dated 10 June 2019 (sic) (Comment).³⁹ In his Comment, JRO countered that "he immediately informed and pleaded [with] the company officers and employees to refrain from accessing his personal information and to subsequently dispose of

³² *Id.*, ¶ 18.

³³ *Id.*, ¶ 24.

³⁴ *Id.*, ¶ 25.

³⁵ *Id.*

³⁶ *Id.*, ¶ 11.

³⁷ *Id.*, ¶ 15.

³⁸ *Id.*, ¶ 29.

³⁹ Comment and Opposition to the Motion to Dismiss dated July 2, 2019 with Prayer for the Issuance of Cease and Desist Orders as Provided for Under Chapter II, Section 7(a)(b)(c)(d) AND (i) of R.A. 10173, dated 10 June 2019 (sic) of JRO.

any of his personal information.”⁴⁰ JRO alleges that he informed ATN “to withdraw, block, remove and destroy” his personal information given that there were two (2) other remaining employees, RDR and ATN, who had access to SBECS.⁴¹ Oller attached a scanned copy of a POEA e-Services Enrollment and Availment Form (REAPS), signed by MSMI’s president, showing the nomination of three (3) users with their corresponding email addresses.⁴²

MSMI filed a Motion for Extension dated 22 July 2019, seeking an additional period of five (5) days, or until 27 July 2019, within which to file a Reply to JRO’s Comment.⁴³ Subsequently, MSMI filed a Reply (to the Complainant’s 10 June 2019 Comment and Opposition), dated 26 July 2019 (Reply).⁴⁴

In its Reply, MSMI claims that JRO only “provides self-serving and unsubstantiated declarations” regarding his allegation that he immediately informed the company about refraining from using his personal information,⁴⁵ or that he informed the company in writing.⁴⁶ MSMI reiterated its arguments in its Motion to Dismiss, particularly that the alleged personal account was actually owned by the company,⁴⁷ and that it had legitimate interests in using the same.⁴⁸

Thereafter, JRO filed a Manifestation with Prayer to Expunge from the Record of the Case the Respondents’ Reply (dated 26 July 2019) and Penalized Respondents (sic) Under Sec. 33 of R.A. 10173, dated 05 August 2019 (Manifestation).⁴⁹ JRO contends that his narration is truthful, and that there should be no reason for an outright dismissal, since the Complaint showed good cause to be decided on the merits.⁵⁰ Further, since the Commission did not grant MSMI’s Motion for Extension, the Reply was not filed on time.⁵¹

⁴⁰ Id., ¶ 3.

⁴¹ Id.

⁴² Id., Annex “A”.

⁴³ Motion for Extension dated 22 July 2019 of MSMI.

⁴⁴ Reply dated 26 July 2019 of MSMI.

⁴⁵ Id., ¶¶ 9-10.

⁴⁶ Id., ¶¶ 11-15.

⁴⁷ Id., ¶ 25.

⁴⁸ Id., ¶ 30.

⁴⁹ Manifestation with Prayer to Expunge from the Record of the Case the Respondents’ Reply (dated July 26, 2019) and Penalized Respondents (sic) Under Sec. 33 of R.A. 10173, dated 05 August 2019 of JRO.

⁵⁰ Id., ¶ 2.

⁵¹ Id., ¶ 1.

of his personal information.”⁴⁰ JRO alleges that he informed ATN “to withdraw, block, remove and destroy” his personal information given that there were two (2) other remaining employees, RDR and ATN, who had access to SBECS.⁴¹ Oller attached a scanned copy of a POEA e-Services Enrollment and Availment Form (REAPS), signed by MSMI’s president, showing the nomination of three (3) users with their corresponding email addresses.⁴²

MSMI filed a Motion for Extension dated 22 July 2019, seeking an additional period of five (5) days, or until 27 July 2019, within which to file a Reply to JRO’s Comment.⁴³ Subsequently, MSMI filed a Reply (to the Complainant’s 10 June 2019 Comment and Opposition), dated 26 July 2019 (Reply).⁴⁴

In its Reply, MSMI claims that JRO only “provides self-serving and unsubstantiated declarations” regarding his allegation that he immediately informed the company about refraining from using his personal information,⁴⁵ or that he informed the company in writing.⁴⁶ MSMI reiterated its arguments in its Motion to Dismiss, particularly that the alleged personal account was actually owned by the company,⁴⁷ and that it had legitimate interests in using the same.⁴⁸

Thereafter, JRO filed a Manifestation with Prayer to Expunge from the Record of the Case the Respondents’ Reply (dated 26 July 2019) and Penalized Respondents (sic) Under Sec. 33 of R.A. 10173, dated 05 August 2019 (Manifestation).⁴⁹ JRO contends that his narration is truthful, and that there should be no reason for an outright dismissal, since the Complaint showed good cause to be decided on the merits.⁵⁰ Further, since the Commission did not grant MSMI’s Motion for Extension, the Reply was not filed on time.⁵¹

⁴⁰ *Id.*, ¶ 3.

⁴¹ *Id.*

⁴² *Id.*, Annex “A”.

⁴³ Motion for Extension dated 22 July 2019 of MSMI.

⁴⁴ Reply dated 26 July 2019 of MSMI.

⁴⁵ *Id.*, ¶¶ 9-10.

⁴⁶ *Id.*, ¶¶ 11-15.

⁴⁷ *Id.*, ¶ 25.

⁴⁸ *Id.*, ¶ 30.

⁴⁹ Manifestation with Prayer to Expunge from the Record of the Case the Respondents’ Reply (dated July 26, 2019) and Penalized Respondents (sic) Under Sec. 33 of R.A. 10173, dated 05 August 2019 of JRO.

⁵⁰ *Id.*, ¶ 2.

⁵¹ *Id.*, ¶ 1.

MSMI filed a Motion to Expunge with Ex Abudanti Ad Cautelam (to Complainant's 05 August 2019 Manifestation) dated 28 August 2019.⁵² Aside from reiterating its previous arguments, in the said Motion, MSMI prayed that the Manifestation be expunged from the records since the final pleading was its Reply, based on the Commission's Order dated 18 June 2019.⁵³ Further, MSI averred that Oller has not proven that there were three (3) authorized users to use the SBECS since the REAPS that Oller attached to his Comment was merely a request, not the actual approval from POEA.⁵⁴

MSMI thereafter filed an Ex-Parte Motion to Resolve (Respondent's Motion to Dismiss dated 02 July 2019), dated 26 November 2019, where the Respondent prayed that the Complaint be dismissed.⁵⁵ JRO also filed a Motion for Early Resolution and to Declare Respondents in Default, dated 01 December 2019, also praying for the resolution of the case.⁵⁶

In a Resolution dated 12 January 2021, the CID resolved to deny JRO's request to expunge MSMI's Reply; it also denied MSMI's motion to expunge JRO's Manifestation, both based on due process considerations.⁵⁷

Issues

- I. Whether the Complaint should be dismissed for failing to follow the rule on exhaustion of administrative remedies.
- II. Whether MSMI committed a violation of the DPA.

Discussion

The Commission dismisses the Complaint for lack of merit.

I. The Commission exercises its authority to resolve the case on the merits.

⁵² Motion to Expunge with Ex Abudanti Ad Cautelam (to Complainant's 05 August 2019 Manifestation) dated 28 August 2019 of MSMI.

⁵³ *Id.*, ¶ 10.

⁵⁴ *Id.*, ¶ 31.

⁵⁵ Ex-Parte Motion to Resolve (Respondent's Motion to Dismiss dated 02 July 2019), dated 26 November 2019 of MSMI., ¶ 10.

⁵⁶ Motion for Early Resolution and to Declare Respondents in Default, dated 01 December 2019 of JRO, Prayer.

⁵⁷ Resolution dated 12 January 2021, at pages 2-3.

MSMI contends that the case should be dismissed since JRO did not prove that he complied with Section 4(a) of NPC Circular No. 16-04, also known as the 2016 NPC Rules of Procedure.⁵⁸

In response, JRO claims that after resigning, he immediately informed the company to refrain from accessing his personal information.⁵⁹ NPC Circular No. 16-04 was the applicable procedural rules at the time of the filing of the complaint. Section 4 of the aforementioned Circular states:

SECTION 4. Exhaustion of remedies. – No complaint shall be entertained unless:

- a. the complainant has informed, in writing, the personal information controller or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same;
- b. the personal information controller or concerned entity did not take timely or appropriate action on the claimed privacy violation or personal data breach, or there is no response from the personal information controller within fifteen (15) days from receipt of information from the complaint ;
- c. and the complaint is filed within six (6) months from the occurrence of the claimed privacy violation or personal data breach, or thirty (30) days from the last communiqué with the personal information controller or concerned entity, whichever is earlier.

The failure to comply with the requirements of this Section shall cause the matter to be evaluated as a request to the National Privacy Commission for an advisory opinion, and for the National Privacy Commission to take such further action, as necessary. The National Privacy Commission may waive any or all of the requirements of this Section, at its discretion, upon good

⁵⁸ Motion to Dismiss dated 02 July 2019 of MSMI, ¶ 29.

⁵⁹ Comment and Opposition to the Motion to Dismiss dated July 2, 2019 with Prayer for the Issuance of Cease and Desist Orders as Provided for Under Chapter II, Section 7(a)(b)(c)(d) AND (i) of R.A. 10173, dated 10 June 2019 (sic) of John Raeman R. Oller, ¶ 3.

cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to the affected data subject.⁶⁰ (Emphases supplied)

Based on the record, JRO has not concretely provided evidence that it has complied with Section 4(a) of NPC Circular No. 16-04, since there is no proof that he informed MSMI, in writing, about the alleged privacy violation. Other than his allegations stated in his various pleadings before the Commission,⁶¹ JRO did not attach any letter or other written correspondence to MSMI relating to the alleged privacy violation. Thus, he did not provide substantial evidence that will lead the Commission to conclude that he complied with Section 4(a) of NPC Circular No. 16-04.

Nevertheless, the Commission exercises its authority to waive the requirement of exhaustion of administrative remedies, based on the last paragraph of Section 4 of the 2016 Rules of Procedure.

JRO's allegations, if substantially proven, may lead the Commission to conclude that there was a serious violation of the DPA. The allegations also show that there may be serious risk of harm to JRO, given that the emails he provided allegedly show acts which he did not do, but may be liable for.

Thus, the Commission finds it appropriate to exercise its authority to resolve the case on the merits.

II. MSMI did not commit a violation of the DPA.

JRO claims that there was a violation of the DPA since MSMI continually utilized his "POEA account" to process its seafarer clients' transactions.⁶²

⁶⁰ National Privacy Commission, Rules of Procedure, NPC Circular No. 16-04, § 4 (15 December 2016).

⁶¹ See Comment and Opposition to the Motion to Dismiss dated July 2, 2019 with Prayer for the Issuance of Cease and Desist Orders as Provided for Under Chapter II, Section 7(a)(b)(c)(d) AND (i) of R.A. 10173, dated 10 June 2019 (sic) of JRO, ¶ 3.

⁶² Complaints-Assisted Form dated 27 March 2019 of JRO, at page 3.

There are three pieces of information that JRO claims to be part of his personal information: 1) his email account, 2) his name, and 3) the POEA Code.⁶³

At the outset, the Commission finds that JRO did not actually own the “POEA account” that enabled MSMI to use the SBECS. The company-issued email and POEA Code, which are both needed to register and use the SBECS, are part of MSMI’s assets.

There is substantial evidence on record to show that MSMI has ownership over the company-issued email and POEA Code. Particularly, the contract processing fees to use the POEA system was paid by MSMI.⁶⁴

The email, jr.o@msm.com.ph, is also reasonably seen to be a company-issued email, with the email identifier itself linked to the company. The signed REAPS provided by JRO himself shows that the request to enroll into the SBECS was made by MSMI.⁶⁵

Further, under POEA Memorandum Circular No. 06, series of 2018, (POEA Circular) which has for its subject the “New Procedure for Online Registration of Seafarers and Seabased e-Contracts System (SBECS)”, it is the LMA who requests or nominates the users to the POEA.⁶⁶

Thus, given that these are company-owned assets, the corresponding credentials for the use of the SBECS are not owned by JRO. The “POEA account” is for the company’s transactions, and not for his personal use. In other words, the company was authorized to use the POEA credentials since this was company-owned.

The POEA Code, in this instance, cannot be considered personal information given that the said code is owned by MSMI. Meanwhile,

⁶³ Id.

⁶⁴ Motion to Dismiss dated 02 July 2019 of MSMI, Annex “I” and “I-1”.

⁶⁵ See Comment and Opposition to the Motion to Dismiss dated July 2, 2019 with Prayer for the Issuance of Cease and Desist Orders as Provided for Under Chapter II, Section 7(a)(b)(c)(d) AND (i) of R.A. 10173, dated 10 June 2019 (sic) of JRO, Annex “A”.

⁶⁶ POEA Memorandum Circular No. 06-2018, § 2, ¶ 1.

though the email is company-issued, it may fall under the definition of personal information since JRO's name is stated therein.⁶⁷

Nevertheless, the fact that MSMI used JRO's company-issued email even after his resignation does not immediately equate to a violation of the DPA.

Section 12 of the DPA provides for the criteria for lawful processing of personal information. Aside from consent, the DPA has other bases for lawful processing, including processing which is anchored on legitimate interests, to quote:

SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

xxx

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.⁶⁸

Thus, a Personal Information Controller (PIC) may still lawfully process personal information, even without a data subject's consent, if it is based on other criteria found in the DPA, such as Section 12(f).

The Commission finds that MSMI had a legitimate interest in continuing to use its POEA account even after JRO's resignation, given the mandate of the POEA Circular, and MSMI's required business processes.

To reiterate, the POEA Circular which provides for SBECS, includes agencies like MSMI.⁶⁹ Through the SBECS, an LMA is able to use

⁶⁷ See Data Privacy Act of 2012, § 3(g): Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

⁶⁸ *Id.*, § 12(f).

⁶⁹ POEA Memorandum Circular No. 06-2018, § 1, ¶ 1.

“a secured web-based facility developed for active LMAs to submit online 24/7 their request for processing (RFP), pay online the POEA processing and OWWA membership fees, submit online the seafarer’s contract and print the electronic Overseas Employment Certificate (OEC) of the seafarers in the comfort of the agency’s office.”⁷⁰ Otherwise, agencies that fail to register to the SBECS “will be reverted to regular counter processing.”⁷¹

In order to use the SBECS, the agency had to provide a list of names and email addresses to the POEA, which shall serve as the agency’s request or nomination for enrollment or availment of the POEA’s system.⁷² The SBECS also could only be accessed by “authorized users”,⁷³ which means that the account had to be specific to a person. Thus, MSMI needed to provide JRO’s name and email address to comply with the said Circular. After complying, MSMI had the authority to use the POEA account given that it owned the POEA Code and issued Oller’s company email.

The account or credentials which is authorized to use the SBECS, including the name registered in its system, cannot be immediately changed by the company. SBECS is managed by the POEA. As discussed, the LMA has to nominate its authorized users for the POEA’s approval,⁷⁴ and POEA is the one who authorizes the nominated users of the LMA, to quote from the Circular:

xxx

If the SBECS requirements mentioned above are met by the agency, the POEA ICT Branch shall enroll the user credentials in the system. Authorized users shall receive their username and system link through the email address indicated in the agency REAPS.⁷⁵

Through a letter dated 18 December 2018, MSMI undertook to inform the POEA about JRO’s resignation and that its new liaison officer

⁷⁰ Id.

⁷¹ Id., § 5.

⁷² Id., § 2, ¶ 1.

⁷³ Id., see also § 3, ¶ 1.2.

⁷⁴ Id., § 2, ¶ 1.

⁷⁵ Id., § 3, ¶ 1.2.

was RDR.⁷⁶ POEA acknowledged the same through a letter dated 03 January 2019.⁷⁷

The Commission emphasizes that access to the SBECS had to be allowed by POEA.⁷⁸ However, the evidence shows that MSMI only gained access from POEA for RDR on April 2019.⁷⁹ Thus, even though JRO resigned as of 31 December 2018, MSMI could not immediately use the POEA account via RDR's credentials since this was dependent on POEA enrolling the user's credential in its system.

Relatedly, JRO alleges that the MSMI should not have used his email after his resignation, given that there were two other people that had access to the SBECS.⁸⁰ As proof of this claim, JRO submitted a signed Request for Enrollment and Availment of POEA e-Services (REAPS).⁸¹

However, as the form itself states, the REAPS is a request form, and does not indicate the action done by POEA regarding MSMI's request. Thus, at best, the REAPS only shows that MSMI requested three users to be authorized to use the SBECS. It does not prove, however, that POEA actually approved all three (3) nominated names to use the SBECS.

JRO has not proven, with substantial evidence, that MSMI had two (2) other authorized users that could have accessed the SBECS. In comparison, MSMI was able to adequately prove that it only had access for Dela Rosa on April 2019.⁸²

As the REAPS also shows, RDR was one of the persons cited in the request form to be authorized to use the SBECS.⁸³ The Commission notes that MSMI had to request the POEA to register RDR as the new POEA liaison officer after JRO's resignation.⁸⁴ This new position

⁷⁶ Motion to Dismiss dated 02 July 2019 of MSMI, Annex "F".

⁷⁷ Id., Annex "G".

⁷⁸ See POEA Memorandum Circular No. 06-2018, § 3, ¶ 1.2.

⁷⁹ Motion to Dismiss dated 02 July 2019 of MSMI, Annex "H".

⁸⁰ Comment and Opposition to the Motion to Dismiss dated July 2, 2019 with Prayer for the Issuance of Cease and Desist Orders as Provided for Under Chapter II, Section 7(a)(b)(c)(d) AND (i) of R.A. 10173, dated 10 June 2019 (sic) of JRO, ¶ 3.

⁸¹ Id., Annex "A".

⁸² Motion to Dismiss dated 02 July 2019 of MSMI, Annex "H".

⁸³ Comment and Opposition to the Motion to Dismiss dated July 2, 2019 with Prayer for the Issuance of Cease and Desist Orders as Provided for Under Chapter II, Section 7(a)(b)(c)(d) AND (i) of R.A. 10173, dated 10 June 2019 (sic) of JRO, Annex "A".

⁸⁴ Motion to Dismiss dated 02 July 2019 of MSMI, Annex "F".

was duly acknowledged by the POEA in its letter dated 03 January 2019.⁸⁵ These circumstances discredit JRO's claim that the other requested names in the REAPS were ultimately authorized by the POEA since MSMI had to request access for Dela Rosa as its new liaison officer.

Given the circumstances, MSMI's processing was valid considering that it used the company-linked POEA Code through a company-issued email to use the POEA account owned by MSMI. It also adequately established that its new liaison officer, Dela Rosa, only had access to SBECS months after JRO's resignation, even though the company already informed POEA about these facts.

Under Section 12(f) of the DPA, the PIC's legitimate interest may be "overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution."⁸⁶ In this case, JRO has not sufficiently alleged, or proven, that he has fundamental rights enshrined in the Constitution that would override MSMI's legitimate interests.

In sum, the Commission finds that MSMI's processing is considered as "necessary for the purposes of the legitimate interests" since the use of the SBECS is provided by POEA, validly authorized given the circumstances, and is integral to its business processes as an LMA.

WHEREFORE, premises considered, the Complaint is hereby DISMISSED for lack of merit.

SO ORDERED.

City of Pasay, Philippines.
31 March 2022.

⁸⁵ Id., Annex "G".

⁸⁶ Data Privacy Act of 2012, § 12(f).

Sgd.

JOHN HENRY D. NAGA

Privacy Commissioner

WE CONCUR:

Sgd.

DUG CHRISTOPER B. MAH

Deputy Privacy Commissioner

(Inhibited)

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

Copy furnished:

JRO

Complainant

MSMI

Respondent

AML

Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

**IN RE: ORIENTE EXPRESS TECHSYSTEM
CORPORATION (CASHALO)
AND ITS RESPONSIBLE OFFICERS**

NPC SS 21-005

For: Violation of the Data Privacy Act of 2012

X-----X

DECISION

NAGA, P.C.;

Before this Commission is the Fact-Finding Report (FFR) with Application for the Issuance of a Temporary Ban on processing of personal data filed by the Complaints and Investigation Division (CID) of the National Privacy Commission (NPC) dated 09 June 2021, which serves as its Complaint (Complaint) pursuant to the NPC's power to conduct a sua sponte investigation.¹ The Complaint alleged violations of Republic Act No. 10173, or the Data Privacy Act of 2012 (DPA), by Oriente Express Techsystem Corporation (OETC) which operates the Cashalo online lending application (Cashalo).

Facts

On 09 June 2021, the CID submitted its FFR with Application for the Issuance of a Temporary Ban against OETC. The CID alleged that OETC violated Sections 11, 16, and 25 of the DPA and Section 3(D)(4) of NPC Circular No. 20-01 (Guidelines on the Processing of Personal Data for Loan-related Transactions).²

The CID, in its Complaint, alleged the following:

¹ See National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission, NPC Circular No. 2021-01, rule I, § 4(p); rule X, §§ 4-5 (28 January 2021) (2021 NPC Rules of Procedure).

² Fact-Finding Report (with Application for Issuance of Temporary Ban on the Processing of Personal Data) dated 09 June 2021 of the Complaints and Investigation Division, at p. 18. (Fact-Finding Report)

Cashalo is a loan-related application available at the Google Play Store, with SEC Registration No. CSC201800209 and Certificate of Authority No. 1162. All loans under the Cashalo Platform are financed by Paloo Financing Inc.

On 14 May 2021, the CID simulated the app installation and registration process for loan application with the Cashalo App.

xxx

Upon installation, a consent screen on the application appeared requiring access to Phone, Messaging, Contacts, Location, and external data from other applications. When the downloaded application was opened, a notification asking access to the contacts appeared. The CID tried to decline the asked permission, but the application asked again for the permission to access the contacts.

In providing character references, there was no separate interface in the App. There was no manual way of entering a phone number and that it must be through giving access to the contacts list. The loan application will not proceed to the next step without the character reference's phone number.

The CID noticed that the Cashalo application utilized the Cordova plugin to fetch the contact information on the test device.³ (citations omitted)

In the CID's Technical Report dated 14 May 2021, it further alleged:

10. As part of Android's programming capability, the Android SDK provides coding for Contacts retrieval wherein an application will have the ability to collect data from contacts. That being said, Android supports user privacy through App permissions. The user has control over the data that they share with apps, the user understands what data an app uses, and why the app accesses this data and an app accesses and uses only the data that's required for a specific task or action that the user invokes.⁴

³ Id., at pp. 1-2.

⁴ Technical Report dated 14 May 2021 of the Complaints and Investigation Division, ¶ 10. The Technical Report is cited in the Fact-Finding Report.

In its Complaint, the CID stated that OETC failed to adhere to the requirements of the DPA, specifically Section 11 which deals with the General Data Privacy Principles (transparency, legitimate purpose, proportionality).⁵

For the principle of transparency, the CID explained that this is related to the data subject's right to information under Section 16 of the DPA.⁶ The CID claimed that OETC failed to uphold the principle of transparency since it "failed to provide the purpose for the storage of the personal information accessed, and such cannot be seen in the App's Privacy Notice nor can be deduced from the permission it requires."⁷

In terms of the legitimate purpose principle, the CID argued that it is upheld when one of the criteria for lawful processing, as provided in Sections 12 and 13 of the DPA, is met.⁸ According to the CID, OETC does not have a legitimate purpose in processing personal information of its users since it was done without valid consent.⁹ The CID stated that in Cashalo's Privacy Policy, the data subjects have no opportunity to make an informed choice since in order for the users to avail of Cashalo's services, they have no choice but to accept the terms and conditions it provided.¹⁰ CID further stated that such act of OETC is "misleading and inherently unfair."¹¹

The CID argued that Cashalo can access and store the personal information of the data subjects including their phone contacts, which is not relevant to the purpose of a loan transaction.¹²

Moreover, the CID stated that "the respondent is without a valid consent or authority under the DPA and other existing laws, to process and store the phone contacts of the borrowers. As such it

⁵ Fact-Finding Report of the Complaints and Investigation Division, pp. 8-15.

⁶ *Id.*, at pp. 9-10.

⁷ *Id.*, at p. 10.

⁸ *Id.*, at p. 11.

⁹ Fact-Finding Report of the Complaints and Investigation Division, at p. 12.

¹⁰ *Id.*, at p. 12.

¹¹ *Id.*

¹² *Id.*, at p. 13.

should be deemed to be unauthorized and in violation of Section 25 of the DPA.”¹³

The CID alleged that in terms of proportionality, OETC failed to clearly indicate in Cashalo’s Privacy Notice the purpose and extent of accessing the personal information of its clients, including their phone contacts.¹⁴ The CID also referred to the portion of Cashalo’s Privacy Notice which states that OETC, with its subsidiaries and affiliates, “may share any and all information relating to User to each other for any legitimate business purposes [such as]...credit collection, outsourcing of collections to third parties, remedial measure for collection (i.e. referral to agents and lawyers for collection).”¹⁵ Further, in the Privacy Notice’s “Use/Purpose of Personal Data”, the CID cited that one of Cashalo’s enumerated use/purpose is “to facilitate loan processing from application, review, monitoring, payment, collection and other remedial measures.”¹⁶

The CID concluded that OETC “intends to process any and all information about the data subject, including phone contacts, for purposes of debt collection.”¹⁷

Accordingly, the CID alleged that the processing of the data subject’s information for debt collection violated Section 3(D)(4) of the NPC Circular No. 20-01.¹⁸ It faulted OETC for having a Privacy Policy that was vague and ambiguous since it declared that any and all information of the data subject may be used for purposes, which included debt collection.¹⁹ The CID stated that the consent given by Cashalo’s users cannot be considered free, voluntary, and informed because data subjects have no choice but to allow access to its phone contact list to avail of OETC’s loan service.²⁰

¹³ Fact-Finding Report of the Complaints and Investigation Division, at p. 14.

¹⁴ *Id.*

¹⁵ *Id.*, at p.14. See Supplemental Report dated 31 May 2021, Annex “A”.

¹⁶ *Id.*

¹⁷ Fact-Finding Report of the Complaints and Investigation Division, at p. 14.

¹⁸ *Id.*

¹⁹ *Id.*, at p. 15.

²⁰ *Id.*

The CID further argued that OETC is liable for Section 25 of the DPA that deals with the unauthorized processing of personal information and sensitive personal information.²¹ It contended that:

[M]ere permissions before installation of the mobile application and during the launch of the application itself does not suffice as a valid consent, as consent cannot be said to be made in an informed, free, and voluntary manner. Respondent's clients were left with no choice but to allow permissions, whose purposes were vaguely provided in its Privacy Policy, in order to use the application and apply for a loan.²²

OETC's Board of Directors (BOD) were the responsible officers liable for Section 25 of the DPA since the BOD was the one "who decides [for the corporation] and should have the duty of diligence. The violation of the corporation is a violation of the person behind it which are its officers or board."²³

The CID also prayed for the issuance of temporary ban on the processing of personal information in relation to the Cashalo app.²⁴ It stated that there was substantial evidence to warrant the temporary ban's issuance given that "[OETC's] processing of personal data [was] without adherence to the Data Privacy Principles enshrined in the DPA", and since it was violative of NPC Circular 20-01, Section 3 (D)(4) since "there [was] sufficient information to support that [OETC] has the ability to access, store, and copy phone contact lists of its borrowers and utilizes that stored data for use in debt collection or to harass its borrowers".²⁵ Further, the CID claimed that the temporary ban's issuance was crucial for the preservation and protection of the data subjects' rights.²⁶ The CID concluded that all of the grounds for the issuance of a temporary ban were present.²⁷

²¹ Fact-Finding Report of the Complaints and Investigation Division, at p. 16.

²² *Id.*

²³ *Id.*, at p. 17.

²⁴ *Id.*

²⁵ Fact-Finding Report of the Complaints and Investigation Division, at p. 17.

²⁶ *Id.*

²⁷ *Id.*, at p. 18.

On 16 June 2021, the Commission issued an Order directing OETC to submit its Position Paper in lieu of a summary hearing within ten (10) days from receipt of said Order.²⁸

On 09 July 2021, OETC's legal counsel filed its Entry of Appearance and an Urgent Manifestation with Motion for Leave and Time to File Position Paper (Re: Order dated 16 June 2021).²⁹ OETC prayed for an extension of at least fifteen (15) days to submit its Position Paper.³⁰

On 15 July 2021, the Commission granted OETC's request for extension to file its Position Paper.³¹

On 23 July 2021, OETC submitted its Position Paper Ad Cautelam (Position Paper).³²

In its Position Paper, OETC argued that: 1) the CID's Complaint did not establish all the requisites for the issuance of a temporary ban,³³ 2) it did not violate the DPA and NPC Circular No. 20-01 since the processing and collecting of personal data of Cashalo users was valid, had legitimate purposes, and done in accordance with the Philippine's data privacy laws;³⁴ and 3) OETC's officers or BOD were not liable for violations of the DPA.³⁵

OETC argued that the CID failed to establish that a temporary ban was needed to protect public interest since its Complaint lacked any specific allegation that OETC was engaging in unscrupulous debt collection methods.³⁶ Rather, it only alleged numerous complaints

28 In re: Oriente Express Techsystem Corporation (Cashalo), NPC SS 21-005, Order dated 16 June 2021, at p. 2.

29 Entry of Appearance and Urgent Manifestation with Motion for Leave and Time to File Position Paper (Re: Order dated 16 June 2021) dated 09 July 2021 of Oriente Express Techsystem Corporation.

30 Id., at p. 4.

31 In re: Oriente Express Techsystem Corporation (Cashalo), NPC SS 21-005, Resolution dated 15 July 2021, at p. 2.

32 Position Paper Ad Cautelam dated 23 July 2021 of Oriente Express Techsystem Corporation.

33 Id., ¶¶ 43-61.

34 Id., ¶¶ 62-147.

35 Id., ¶¶ 148-152.

36 Position Paper Ad Cautelam dated 23 July 2021 of Oriente Express Techsystem Corporation, ¶¶ 44-50.

against unnamed online lending applications (OLAs), without proving that OETC was actually the cause of these complaints.³⁷

OETC argued further that the CID failed to prove that there were facts entitling the issuance of a temporary ban since its allegations to warrant the issuance of a temporary ban were “clearly unfounded”.³⁸ In disproving the CID’s argument that it failed to inform the data subjects of the extent of its processing, OETC claimed that the Cashalo app “notifies the user multiple times of the purpose(s) for data collection” through its Privacy Policy and “simplified pop-up boxes”.³⁹ As to the CID’s allegation that the Cashalo app “has the ability to access, store, and copy phone contact lists”,⁴⁰ OETC explained that its access to phone contacts was only for “Know Your Customer” (KYC) measure, fraud prevention and credit scoring purpose.⁴¹

OETC claimed that it did not violate Section 11 (with regard to legitimate purpose) and Section 16 (in relation to a data subject’s right to information) of the DPA since “there are legitimate purpose(s) for the processing of personal information and the same were fully disclosed to Cashalo app users.”⁴²

OETC also averred that it did not violate Section 25 of the DPA because “all instances of processing done by [OETC], through the Cashalo app, have the free, specific and informed consent of the data subjects who have been sufficiently informed in a concise, transparent, and intelligible manner as to which information are being processed, as well as the purposes for such processing.”⁴³

OETC emphasized that its users enter private loan contracts with the company akin to contracts of adhesion, which are not contracts

37 Id.

38 Id., ¶ 52.

39 Id., ¶ 53.

40 See Fact-Finding Report of the Complaints and Investigation Division, at p. 17.

41 Position Paper Ad Cautelam dated 23 July 2021 of Oriente Express Techsystem Corporation, ¶ 57.

42 Id., ¶ 73.

43 Id., ¶ 90.

automatically considered illegal, unfair, or vitiates the user's consent.⁴⁴

For its processing of phone contacts, OETC claimed that the processing was valid, and once the user completes the loan application, the Cashalo app notifies users that they may already remove access to their phone contact lists.⁴⁵

OETC disputed the CID's claim that the Cashalo app does not provide a separate interface for users to provide character references, since there was an interface that allows its users to freely select their preferred character references, with corresponding details.⁴⁶

Nevertheless, OETC stated that it will be implementing the following developments: 1) "all instances of references selection in the Cashalo app will no longer trigger or require permission to access phone contacts",⁴⁷ 2) while there is an existing in-app messaging platform to inform users that they may remove device permissions, there will also be an identical pop-up notice having the same function,⁴⁸ 3) update of its Privacy Policy to further clarify its personal data processing,⁴⁹ and 4) allowing users to apply for a loan even if the permission to access their location is denied.⁵⁰

OETC manifested that it would be implementing the developments via an updated Cashalo app which will be submitted to Google Play Store for review and approval.⁵¹

Thus, OETC prayed for the Commission to deny the issuance of a temporary ban on the processing of personal data with respect to

⁴⁴ Id., ¶¶ 95-97.

⁴⁵ Position Paper Ad Cautelam dated 23 July 2021 of Oriente Express Techsystem Corporation, ¶¶ 101-102.

⁴⁶ Id., ¶¶ 135-139.

⁴⁷ Id., ¶ 156.

⁴⁸ Id., ¶ 157.

⁴⁹ Position Paper Ad Cautelam dated 23 July 2021 of Oriente Express Techsystem Corporation, ¶ 158.

⁵⁰ Id., ¶ 159.

⁵¹ Id., ¶ 155.

the Cashalo app and dismiss the sua sponte investigation for lack of merit.⁵²

On 29 July 2021, the Commission issued an Order directing CID to submit its comment on OETC's Position Paper.⁵³ In the same Order, the Commission also set a virtual Clarificatory Hearing to be held on 19 August 2021.⁵⁴

The CID thereafter submitted its Comment/Opposition (to Respondent's Position Paper dated 23 July 2021) dated 13 August 2021 (Comment).⁵⁵

In its Comment, the CID claimed that it made an investigation on the revised Cashalo app.⁵⁶ Particularly, the CID alleged that OETC "tried to remedy the issue regarding the access and storing of the data subject's contacts by removing the permissions and asking them to manually input contacts of their own preference to be designated as reference contacts."⁵⁷ Nevertheless, the CID argued:

However, even though this update was made, the respondent failed to rebut the fact that the application does not have the ability to store the data of the data subject's using their application.⁵⁸

The CID also raised the problem that OETC allegedly already had access to the data of those data subjects who applied for loan before the update was made.⁵⁹ Further, the CID argued that data subjects who applied for a loan before the update would still be able to access the old version of the application since the update applies prospectively.⁶⁰

52 Id., at p. 59.

53 In re: Oriente Express Techsystem Corporation (Cashalo), NPC SS 21-005, Order dated 29 July 2021, at p. 4.

54 Id.

55 Comment/Opposition (to the Respondent's Position Paper dated 23 July 2021) dated 13 August 2021 of the Complaints and Investigation Division.

56 Id., ¶ 4.

57 Id., ¶ 5.

58 Id., ¶ 6.

59 Id., ¶ 7.

60 Id., ¶¶ 7-8, ¶ 11.

In support of its allegation that OETC violated Section 3(D)(4) of NPC Circular No. 20-01, the CID pointed out that since OETC hurriedly revised the Cashalo app after the sua sponte investigation, this act was already an admission that it has the capacity to access the contacts of its clients through their mobile phones.⁶¹

The CID maintained that there was substantial evidence to warrant the issuance of a temporary ban on the processing of personal data against OETC in relation to its Cashalo app.⁶²

Through an Order dated 17 August 2021, the Commission rescheduled the clarificatory hearing to 26 August 2021 instead of 19 August 2021,⁶³ after OETC submitted an Urgent Motion to Reset the Clarificatory Hearing Scheduled on 19 August 2021, dated 16 August 2021, due to the Enhanced Community Quarantine implemented in Metro Manila.⁶⁴

On 26 August 2021, the Commission conducted a clarificatory hearing. In an Order dated 26 August 2021, OETC was ordered to submit the following documents to the Commission:

1. Evidence showing its implementation of the representations made to the Commission during the hearing, specifically on the removal of access to the contact list and location data;
2. Copy of a certificate of deletion of the data when the data subject has requested for the deletion of their data or proof of confirmation of deletion of data when the data subject has furnished the request via electronic mail; and
3. Copy of the Platform Services Agreement between Oriente Express Techsystem Corporation and Paloo Financing Inc.⁶⁵

⁶¹ Id., ¶ 23.

⁶² Comment/Opposition (to the Respondent's Position Paper dated 23 July 2021) dated 13 August 2021 of the Complaints and Investigation Division, ¶ 25.

⁶³ In re: Oriente Express Techsystem Corporation (Cashalo), NPC SS 21-005, Order dated 17 August 2021, at p. 3.

⁶⁴ Urgent Motion to Reset the Clarificatory Hearing Scheduled on 19 August 2021 dated 16 August 2021 of Oriente Express Techsystem Corporation.

⁶⁵ In re: Oriente Express Techsystem Corporation (Cashalo), NPC SS 21-005, Order dated 26 August 2021, at pp. 1-2.

OETC thereafter submitted its Compliance [Re: Order dated 26 August 2021] dated 03 September 2021.⁶⁶ OETC manifested that it no longer requests access to contacts even for KYC, fraud prevention and credit scoring.⁶⁷ OETC supported this claim by submitting a video which shows the installation of the Cashalo app and the permissions required.⁶⁸ OETC also provided the following proof:

- 1) Photos/screenshots of Manual Entry of References, with separate interface;⁶⁹
- 2) Photos/screenshots of Optional Location Permission Access;⁷⁰
- 3) Proof of Request for the Deletion of Data Subject/s' Data furnished via electronic mail and its corresponding Proof of Confirmation of Deletion of Data;⁷¹ and
- 4) Copy of the Platform Service Agreement between OETC and Paloo Financing Inc.⁷²

On 17 September 2021, the Commission issued an Order which denied the CID's application for a temporary ban, with the following dispositive portion, to wit:

WHEREFORE, premises considered, this Commission DENIES the Application for Temporary Ban on the processing of personal data filed by the Complaints and Investigation Division of the National Privacy Commission for failure to satisfy the requisites for the issuance of Temporary Ban specifically, Section 3(1) and (2), Rule IX of the NPC Circular

66 Compliance [Re: Order dated 26 August 2021] dated 03 September 2021 of Oriente Express Techsystem Corporation.

67 Id., ¶ 2.

68 Id., ¶ 2.1; See video file of Oriente Express Techsystem Corporation.

69 Id., ¶ 2.2; Annex "1".

70 Compliance [Re: Order dated 26 August 2021] dated 03 September 2021 of Oriente Express Techsystem Corporation, ¶¶ 4-6; Annex "2" and video file of Oriente Express Techsystem Corporation.

71 Id., ¶ 7; Annexes "3" & "4".

72 Compliance dated 26 August 2021.

No. 20-01. The Commission hereby ORDERS Respondent Oriente Express Techsystem Corporation and its Responsible Officers within a non-extendible period of FIFTEEN (15) days from receipt of this ORDER to:

1. Revise its Privacy Policy and processes to conform with Republic Act No. 10173, known as the Data Privacy Act of 2012, as its Privacy Policy should match its representations and admissions discussed during the Clarificatory Hearing held last 26 August 2021; and
2. Submit proof of compliance of its revised Privacy Policy and processes.⁷³

With the issuance of the Order denying the CID's Application for Temporary Ban, the proceedings before the Commission based on the CID's Complaint against OETC resumed, pursuant to Rule IX, Section 2 of NPC Circular 2021-01, or the 2021 NPC Rules of Procedure.⁷⁴

On 10 December 2021, OETC submitted: 1) its revised Privacy Policy in compliance with the Order dated 17 September 2021,⁷⁵ and 2) proof of revisions made in the Cashalo app.⁷⁶

On 31 March 2022, the Commission ordered both the CID and OETC to submit their respective Memoranda within fifteen (15) days from receipt of the Order.⁷⁷

On 16 May 2022, the CID submitted its Memorandum.⁷⁸ CID maintained that OETC violated Sections 11, 12, 13, and 16, all of the DPA, since it failed to adhere to the principles of transparency, legitimate purpose, and proportionality.⁷⁹

⁷³ In re: Oriente Express Techsystem Corporation (Cashalo), NPC SS 21-005, Order dated 17 September 2021, at pp 26-27.

⁷⁴ Id., at p. 27. See NPC Circular No. 2021-01, rule VIII, § 4.

⁷⁵ Compliance dated 10 December 2021 of Oriente Express Techsystem Corporation, ¶ 2. Annex "1".

⁷⁶ Id., ¶ 3. See video files of Oriente Express Techsystem Corporation.

⁷⁷ In re: Oriente Express Techsystem Corporation (Cashalo), NPC SS 21-005, Order dated 31 March 2022

⁷⁸ Memorandum dated 16 May 2022 of the Complaints and Investigation Division, at pp. 3-7.

⁷⁹ Id., at p. 3.

The CID argued that OETC violated the transparency principle since “[it] failed to provide clearly in their privacy policy what is the purpose/s why they access and store the personal information of their clients.”⁸⁰

The CID also alleged that OETC violated the principle of legitimate purpose, reasoning thus:

The Respondent however, failed to provide any proof that its data subjects consented to the processing of their personal information and sensitive personal information through written, electronic, recorded means, before or even after they entered their information in the application. This is particularly evident in the processing (collection and retention) of borrower’s phone contact list that is not germane to the purpose of the loan transaction entered into with the Respondent.⁸¹

The CID further argued that OETC violated the proportionality principle by using dangerous permissions to access a user’s Phone, Location, Storage, and Camera.⁸²

According to the CID, OETC violated Section 25 of the DPA.⁸³ It contended that OETC’s processing of the phone contact lists of its clients may be considered as unauthorized processing since the “information [was] used for purposes without the data subject’s [clear] consent or otherwise authorized by law.”⁸⁴ The CID also pointed out that during the clarificatory hearing, OETC allegedly admitted that “[it is] using the personal information of the clients that [it] accessed and stored for marketing purposes.”⁸⁵

The CID also faulted OETC for accessing its data subjects’ contacts since this was allegedly excessive in relation to the loan application.⁸⁶

⁸⁰ Id.

⁸¹ Id., at p. 5.

⁸² Memorandum dated 16 May 2022 of the Complaints and Investigation Division, at p.5.

⁸³ Id., at pp. 7-8.

⁸⁴ Id., at p. 7.

⁸⁵ Id., at pp. 7-8.

⁸⁶ Memorandum dated 16 May 2022 of the Complaints and Investigation Division, at p.8.

Moreover, the CID stated that if OETC is found liable, the penalty should be imposed upon its BOD being the responsible officers who, by their gross negligence, allowed the commission of the violations.⁸⁷

On 17 May 2022, OETC submitted its Memorandum.⁸⁸ OETC emphasized that it did not violate Sections 11 and 16 of the DPA since there were “legitimate purpose/s for the processing of personal information and the same were fully disclosed to the Cashalo app users” in the Privacy Policy and pop-up notification boxes.⁸⁹ These purposes are “to conduct and perform fraud monitoring, detection, analysis, and prevention; to develop, enhance and maintain a risk assessment process and model, offline and online; and to develop and generate a credit score, credit model and user, model among others.”⁹⁰ OETC further claimed that Cashalo’s Privacy Policy was also clear, unambiguous, concise, and simple.⁹¹

OETC likewise argued that it did not violate Section 25 of the DPA since it has been able to procure the free, specific, and informed consent of the Cashalo app users.⁹² It submitted that the CID’s Complaint failed to prove by substantial evidence that the purposes for the processing of Cashalo app users’ personal data was actually vague.⁹³

OETC claimed that it was able to obtain its users valid consent even if the contracts may be considered as contracts of adhesion, since the users are free to reject the permissions asked for by the Cashalo app.⁹⁴ OETC further argued that consent was validly obtained from its users since they were “sufficiently informed, multiple times, in a concise, transparent, and intelligible manner as to which information are being processed, as well as the purposes for such processing.”⁹⁵

87 Id.

88 Memorandum dated 17 May 2022 of Oriente Express Techsystem Corporation.

89 Id., ¶¶ 85-86.

90 Id., ¶ 30.

91 Id., ¶¶ 90-91.

92 Memorandum dated 17 May 2022 of Oriente Express Techsystem Corporation, ¶¶ 98-129.

93 Id., ¶ 104.

94 Id., ¶¶ 106-110.

95 Id., ¶ 123.

Further, OETC averred that it did not violate Section 3(D)(4) of NPC Circular No. 20-01.⁹⁶ Aside from CID's alleged failure to substantiate the violation,⁹⁷ the updated Cashalo app also no longer triggers or requires permission to access phone contacts since this was completely replaced with a manual entry field.⁹⁸ Even in previous versions of the Cashalo app, OETC claimed that it never processed the user's phone contact list for debt collection or harassment, but did so only for legitimate reasons such as KYC.⁹⁹

Finally, OETC concluded that considering that it did not violate the DPA and NPC Circular No. 20-01, there was no basis for holding its officers or Board of Directors liable.¹⁰⁰

Issues

- I. Whether OETC did not adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.
- II. Whether OETC violated Section 25 of the DPA.
- III. Whether OETC violated the provisions under Section 3(D)(4) of NPC Circular No. 20-01.

Discussion

Under the DPA, the NPC has the obligation to ensure a personal information controller's compliance with the law¹⁰¹ and institute investigations when necessary.¹⁰²

96 Memorandum dated 17 May 2022 of Oriente Express Techsystem Corporation, ¶¶ 130-171.

97 Id., ¶¶ 130-138.

98 Id., ¶ 139.

99 Id., ¶ 140.

100 Memorandum dated 17 May 2022 of Oriente Express Techsystem Corporation, ¶¶ 172-176.

101 An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter II, § 7(a) (2012).

102 Id. § 7(b).

The NPC's mandate is supported by the NPC Circular No. 2021-01, which allows the procedure for sua sponte investigations of circumstances surrounding possible privacy violations or personal data breaches.¹⁰³

The NPC's CID is the division tasked to, among others, “[institute] investigations regarding violations of the Act, these Rules, and other issuances of the Commission, including violations of the rights of data subjects and other matters affecting personal data.”¹⁰⁴

The FFR of the CID serves as the complaint in the sua sponte investigation.¹⁰⁵ An FFR is submitted to the Commission en banc “for its perusal to determine whether violations of the Data Privacy Act of 2012 (DPA) were committed. Considering that the FFR contains all the findings of the investigating division of the NPC, such document is the complaint initiating the administrative proceedings in cases of sua sponte investigation.”¹⁰⁶ The term sua sponte, when translated, means “of one’s own accord”.¹⁰⁷ Consequently, the NPC, through the CID, initiated of its own accord a complaint against OETC by filing the FFR. In effect, the CID serves as the complainant in the proceedings against the respondent. Meanwhile, the NPC’s Commission en banc acts as a collegial body to adjudicate the case.¹⁰⁸ It shall review the evidence presented, including the FFR and supporting documents.¹⁰⁹

In administrative proceedings like this case, complainants “carry the burden of proving their allegations with substantial evidence.”¹¹⁰ As further explained by the Supreme Court in *De Jesus v. Guerrero III*:

¹⁰³ NPC Circular No. 2021-01, rule X, §§ 5-6.

¹⁰⁴ National Privacy Commission, Implementing Rules and Regulations of the Data Privacy Act of 2012, rule III, § (e) (1) (2016) (IRR of the DPA) .

¹⁰⁵ NPC Circular No. 2021-01, rule X, §§ 3-5. See *In re: FCash Global Lending Inc., Operating FastCash Online Lending Application*, NPC 19-909, Resolution dated 28 April 2022.

¹⁰⁶ *In re: FCash Global Lending Inc., Operating FastCash Online Lending Application*, NPC 19-909, Resolution dated 28 April 2022., at pp. 3-4.

¹⁰⁷ *Id.*, at p. 4.

¹⁰⁸ See Data Privacy Act of 2012, , chapter II, § 7(b).

¹⁰⁹ NPC Circular No. 2021-01, rule VIII, § 1.

¹¹⁰ *Office of the Ombudsman v. Fetalvero, Jr.*, G.R. No. 211450, 23 July 2018.

In administrative proceedings, the quantum of proof necessary for a finding of guilt is substantial evidence, i.e., that amount of relevant evidence that a reasonable mind might accept as adequate to support a conclusion. Further, the complainant has the burden of proving by substantial evidence the allegations in his complaint. The basic rule is that mere allegation is not evidence and is not equivalent to proof. Charges based on mere suspicion and speculation likewise cannot be given credence. Hence, when the complainant relies on mere conjectures and suppositions, and fails to substantiate his allegations, the administrative complaint must be dismissed for lack of merit.¹¹¹

Guided by these pronouncements and after carefully considering the evidence and claims of both parties, the Commission dismisses the complaint for lack of substantial evidence to warrant a finding of a privacy violation.

I. Substantial evidence is lacking to conclude that OETC failed to adhere to the general data privacy principles under the DPA.

The CID posited that OETC “failed to provide the purpose for the storage of the personal information accessed, and such cannot be seen in the App’s Privacy Notice nor can be deduced from the permission it requires”, thus failing to adhere to the principle of transparency.¹¹² OETC countered that the purposes for processing personal data are found in Cashalo’s Privacy Policy,¹¹³ in its pop-up boxes informing users of the permissions required,¹¹⁴ and through clear and unambiguous language.¹¹⁵

After weighing both claims, the Commission finds that the CID did not sufficiently prove that OETC failed to adhere to the transparency principle.

¹¹¹ G.R. No. 171491, 04 September 2009.

¹¹² Fact-Finding Report of the Complaints and Investigation Division, at p. 10.

¹¹³ Memorandum dated 17 May 2022 of Oriente Express Techsystem Corporation, ¶ 86.

¹¹⁴ Id.

¹¹⁵ Id., ¶ 90.

Under Rule IV, Section 18 of the Implementing Rules and Regulations of the DPA (IRR), transparency is explained as follows:

a. Transparency. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.¹¹⁶

From the foregoing, OETC has adequately shown that the Cashalo app users are informed of the purposes of the processing of their personal information through its Privacy Policy and pop-up notification boxes in the Cashalo app.¹¹⁷

In its Privacy Policy, the user is notified of the purposes for collection of personal data which include the conduct and performance of fraud monitoring, detection, analysis, and prevention.¹¹⁸ The pop-up boxes inform the users of the purposes for each application permissions in a way that is specific, plain, and unambiguous.¹¹⁹

In its Compliance dated 03 September 2021, OETC updated the Cashalo app with the access to contacts and location permission no longer requested even for KYC, fraud prevention, and credit scoring.¹²⁰ In inputting character references, the user can manually input the contact number of his or her character reference.¹²¹ Also, for location data, even if the user denies the permission, the application would still proceed to function.¹²² However, the user has the option

¹¹⁶ National Privacy Commission, Implementing Rules and Regulations of the Data Privacy Act of 2012, rule IV, § 18(a) (2016).

¹¹⁷ See Position Paper dated 23 July 2021 of Oriente Express Techsystem Corporation, Annexes "2"- Privacy Policy dated 25 May 2021, "2-A"- Privacy Policy dated 27 October 2020, "3-A"- screenshot of pop-up notices.

¹¹⁸ Id., ¶ 10.

¹¹⁹ Id., Annex "3-A".

¹²⁰ Compliance [Re: Order dated 26 August 2021] dated 03 September 2021 of Oriente Express Techsystem Corporation, ¶ 2; See also Annex "1" and Annex "2".

¹²¹ Id., ¶ 2.2.

¹²² Id., ¶ 4.

to allow access to location data to avail of services such as locating the nearest payment center.¹²³

Through the exchange of pleadings and clarificatory hearing, OETC addressed the issues found in its Privacy Policy and clarified its provisions, namely:

1. The Privacy Policy has already been revised and clarified to remove any mention of data being shared by OETC to third parties for marketing purposes.¹²⁴
2. With regard to the provision which states that, “once information is provided, changes may no longer be allowed x x x,” Cashalo app users are now allowed to initiate requests to rectify or erase their personal data in the Cashalo app itself. Users can exercise these rights either via email or in the app, which is also made clear in the Privacy Policy.¹²⁵
3. With respect to the provision stating that “the applications and all supporting documents and any other information obtained relative to this application shall be used by and communicated to OETC and shall remain its property whether or not my credit score is determined, or the loan is granted,” OETC has already removed it since OETC’s ownership of personal data was never the intention of the afore-stated statement.¹²⁶
4. The Privacy Policy has also expressly stated that third-party individuals shall not be considered co-makers of loans and no payment will be collected from them. Further, it also states that there shall be no attempt to collect from or enforce against third-party individuals for payment collection or remedial measures.¹²⁷

¹²³ Id., ¶ 6.

¹²⁴ Compliance by OETC dated 10 December 2021, ¶ 2.1.

¹²⁵ Id., ¶ 2.2.

¹²⁶ Id., ¶ 2.3.

¹²⁷ Id., ¶ 2.5.

The Commission notes OETC's efforts in implementing its remediation measures for Cashalo's Privacy Policy, and in complying with the Commission's orders to enhance how Cashalo app users know the nature, purpose, and extent of the processing of their personal data. To be clear, remediation measures do not cure liabilities under the DPA that have already incurred. Nevertheless, the Commission finds that Cashalo has adequately shown that it informed its users of the processing through its Privacy Policy and pop-up notifications. Thus, in totality, OETC has provided sufficient evidence that it upholds the transparency principle.

In terms of legitimate purpose, the CID argued that OETC did not uphold this principle since the Privacy Policy was presented without an opportunity for data subjects to make an informed choice.¹²⁸ The CID reasoned that "[f]or data subjects to avail of [OETC's] services, they have no choice but to accept the terms and conditions provided by [OETC]. Otherwise, data subjects cannot proceed with the processing to obtain a loan. This act of [OETC] is misleading and inherently unfair."¹²⁹

Further, the CID also claimed that the Cashalo app can access and store personal information of the data subjects including their phone contacts. CID argued that such storing of phone contacts is not related to the fulfillment of the loan transaction with the borrower,¹³⁰ thus, violating Sections 11, 12, 13, and 16 of the DPA.

OETC disputed the CID's characterization and claims that consent was validly acquired, and that there were legitimate purposes for the processing of its users' personal data.¹³¹ The processing of the personal data of the users were based on legitimate purpose, i.e., for anti-fraud assessment, credit assessment, risk underwriting and assessment, transaction processing, and regulatory reporting, among others.¹³²

¹²⁸ Fact-Finding Report of the Complaints and Investigation Division, at p. 12.

¹²⁹ *Id.*

¹³⁰ *Id.*, at p.13.

¹³¹ Position Paper dated 23 July 2021 of Oriente Express Techsystem Corporation, pp. 2-3.

¹³² *Id.*

Section 11 of the DPA provides for the General Data Privacy Principles and specifically states that:

SEC. 11. General Data Privacy Principles. – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

Personal information must be:

(a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only; (Emphasis supplied)¹³³

Moreover, Section 18 (b) of the IRR provides that in adhering with the principle of legitimate purpose, “the processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.”¹³⁴

To reiterate, OETC’s stated purpose for processing information is for anti-fraud assessment, credit assessment, risk underwriting and assessment, transaction processing, and regulatory reporting, among others.¹³⁵ The CID itself, in its FFR, noted OETC’s purposes found in the Privacy Policy:

While the term ‘legitimate business purpose’ is too general, the Privacy Policy provided the examples of determining credit score and providing a loan. But in the ‘Use/Purpose of Personal Data’ portion of the Privacy Policy, it further provides that borrower’s Personal Data shall be processed, collected, used, disclosed, stored and retained for the following purposes, including to facilitate loan processing from application, review, monitoring, payment, collection and other remedial measures.¹³⁶

¹³³ Data Privacy Act of 2012, chapter II, § 11(a).

¹³⁴ IRR of the DPA, § 18(b). 2

¹³⁵ Position Paper dated 23 July 2021 of Oriente Express Techsystem Corporation, p. 3.

¹³⁶ Fact-Finding Report of the Complaints and Investigation Division, at p. 13.

A lending or financing company, like OETC, is not prohibited from processing information for purposes such as preventing fraud, determining credit worthiness, or collecting debt, provided that it be within the bounds of law and related issuances of the DPA.¹³⁷

Further, OETC purposes for processing were determined and declared from the outset. When users click the “Sign Up” button in the Cashalo app, they cannot proceed without scrolling through the Privacy Policy and Cashalo’s Terms of Service.¹³⁸ Thus, the “Accept” button remains to be greyed-out and unclickable “unless and until the users have scrolled to the bottom of the [Privacy Policy]”.¹³⁹

OETC clarified in its updated Privacy Policy that the “contact number/s” it collects is that of the users, with the phone book of the user’s device never used for collection and other remedial measures.¹⁴⁰ Further, access to contacts is no longer requested in the Cashalo app even for KYC, fraud prevention, and credit scoring.¹⁴¹

The CID characterized Cashalo’s Privacy Policy as being “misleading and inherently unfair” since users have no choice but to accept it to use the app.¹⁴² The CID points to this as a badge of vitiated consent. The Commission is not persuaded by CID’s reasoning. Cashalo’s Privacy Policy may be considered a contract of adhesion. When “one party imposes a ready-made form of contract on the other, [this] is not strictly against the law.”¹⁴³ The Supreme Court has stated that “[a] contract of adhesion is as binding as ordinary contracts, the reason being that the party who adheres to the contract is free to reject it entirely.”¹⁴⁴ In other words, users are free to accept or reject the terms of the Privacy Policy. Users who accept are deemed to have given their consent freely. The CID failed to provide other proof or adequate reasoning of the users’ lack or impairment of consent.

137 See National Privacy Commission, Guidelines on the Processing of Personal Data for Loan-related Transactions, NPC Circular 20-01 (14 September 2020).

138 Memorandum dated 17 May 2022 of Oriente Express Techsystem Corporation, ¶ 29.

139 Id.

140 Id., ¶ 23.3.

141 Id., ¶ 41.

142 Fact-Finding Report of the Complaints and Investigation Division, at p. 12.

143 Cabanting v. BPI Family Savings Bank, Inc., G.R. No. 201927, 17 February 2016.

144 Id. (Emphases supplied.)

From the records, the Commission finds that OETC has sufficiently shown that its Privacy Policy and pop-up notices adequately informed its users on the purposes for collection of personal data and that the stated purposes are not contrary to law, morals, or public policy.¹⁴⁵ Further, since OETC has sufficiently proven that consent was validly obtained and the purposes for processing were not illegal, OETC did not violate the principle of legitimate purpose.

Lastly, in terms of proportionality, the CID submitted that the “use of the following dangerous permissions to access the Phone, Location, Storage, and Camera, in its application, violates the principle of proportionality, as it is excessive and unnecessary in fulfilling its purpose of collecting on the data subject’s account or collecting the delinquent account.”¹⁴⁶

OETC countered that the Cashalo app requires user-granted permission to access the phone’s contact list only for valid legitimate purposes, such as fraud prevention.¹⁴⁷ As “[OETC] is involved in the online lending business, its continued existence heavily depends on the calculated trust they can extend to its users/borrowers.”¹⁴⁸

Rule IV, Section 18(c) of the DPA’s IRR states:

Proportionality. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.¹⁴⁹

145 Memorandum dated 17 May 2022 of Oriente Express Techsystem Corporation, ¶ 30.

146 Memorandum dated 16 May 2022 of the Complaints and Investigation Division, at p. 5.

147 Memorandum dated 17 May 2022 of Oriente Express Techsystem Corporation, ¶ 141.

148 Position Paper dated 23 July 2021 of Oriente Express Techsystem Corporation, ¶ 126.

149 Implementing Rules and Regulations of the Data Privacy Act of 2012, rule IV, § 18(c).

The proportionality principle is adhered to “when the processing is the least intrusive measure to achieve its purported aims.”¹⁵⁰

The Commission finds that OETC has sufficiently proven that the permission and processing of personal data are adequate, necessary, suitable and not excessive to its declared purpose.

When users apply for a loan through the Cashalo app by clicking the “Apply Now” button, users are prompted with pop-up boxes to allow the app “access to the mobile phone’s camera, photos, and location”, with separate pop-up boxes per request.¹⁵¹ The Cashalo app requires the camera and media permissions as part of KYC processes.¹⁵² The camera permission is used for identity verification and the media gallery is accessed for the user to upload supporting documents such as proofs of billing, certificates of employment, and the like.¹⁵³ The Commission finds that the processing is relevant and necessary to OETC’s declared and specified purpose. Based on the records, there was also no substantial evidence to show that the processing was excessive, or that it could reasonably be fulfilled through other means.

Other than its allegations that the permissions are dangerous and excessive, the CID has not provided substantial evidence that OETC’s processing is outside the purposes stated or that the processing was unnecessary. Thus, weighing the two parties’ respective allegations and evidence, the Commission rules that there is no substantial evidence to find that OETC violated the proportionality principle.

II. OETC cannot be held liable for the violation of Section 25 or Unauthorized Processing of Personal Information and Sensitive Personal Information.

¹⁵⁰ MNL vs PXXX Corporation, Decision dated 29 October 2020, at p. 22.

¹⁵¹ Memorandum dated 17 May 2022 of Oriente Express Techsystem Corporation, ¶ 45.

¹⁵² Id., ¶ 45.

¹⁵³ Id.

In determining whether a violation of Section 25 of the DPA occurred, three elements must be established with substantial evidence:

1. The accused processed the information of the data subject;
2. The information processed was personal information or sensitive personal information;
3. That the processing was done without the consent of the data subject, or without being authorized under this act or any existing law.¹⁵⁴

The CID argued that OETC violated Section 25 of the DPA since “[OETC] indeed processed the personal information and sensitive personal information of all of its borrowers without consent being validly acquired, and the processing not validly authorized under the DPA and other existing laws, processing will be unauthorized (sic).”¹⁵⁵ The CID particularly points to OETC’s processing of the user’s phone contact list as unauthorized.¹⁵⁶ According to the CID, Cashalo users did not validly consent in allowing the application’s permissions, and they were left with no choice but to accept these permissions to use the application.¹⁵⁷ Lastly, CID argued that the access to the users’ contact lists is excessive for the loan application.¹⁵⁸

OETC emphasized that “the fact that consent was given by Cashalo app users is beyond question since...users would not have been able to proceed with submitting their user profile without providing the necessary consent to access the user’s phone contacts for purposes of KYC, fraud prevention, and credit scoring.”¹⁵⁹ It also argued that the CID failed to prove by substantial evidence that the purposes for the processing of personal data of the Cashalo app users were

154 In Re: FLI Operating ABC Online Lending Application, NPC 19-910, Decision dated 17 December 2020 at p. 17.

155 Memorandum dated 16 May 2022 of the Complaints and Investigation Division, at p.7.

156 Id.

157 Id.

158 Id.

159 Memorandum dated 17 May 2022 of Oriente Express Techsystem Corporation, ¶ 107.

actually vague.¹⁶⁰ The users validly gave their consent by being sufficiently informed multiple times of the purposes for processing.¹⁶¹

Here, while the first and second requisites are present, the Commission finds that the third requisite is lacking.

The first element is present since OETC is a personal information controller (PIC) that processes the personal data of its users through its Cashalo app.¹⁶²

The second element is also present since OETC collects a user's full name, permanent and residential address, contact number/s, email address, birth date and/or age, gender, employment information, financial capacity information bank account details, credit card and/or financial account information, financial history and details of government-issued identifications, among other personal data.¹⁶³ The personal data collected from Cashalo's users are considered personal information and sensitive personal information.

The third and last element requires that the processing was done without the consent of the data subject or without authority under the DPA or any existing law.¹⁶⁴ The CID failed to prove the presence of this element.

To recall, consent is one of the bases for lawful processing. Sections 12 and 13 of the DPA provide that:

SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

¹⁶⁰ Id., ¶ 104.

¹⁶¹ Id., ¶ 123.

¹⁶² See Data Privacy Act of 2012, § 3(h).

¹⁶³ Position Paper dated 23 July 2021 of Oriente Express Techsystem Corporation, Annexes "2"- Privacy Policy dated 25 May 2021, "2-A"- Privacy Policy dated 27 October 2020.

¹⁶⁴ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter II, § 7 (2012).

(a) The data subject has given his or her consent;

xxx

SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;¹⁶⁵

As discussed, the Privacy Policy may be considered a contract of adhesion, which is not illegal in this jurisdiction. The case of *Encarnacion Construction & Industrial Corp. v. Phoenix Ready Mix Concrete Development & Construction, Inc.* explains the concept of a contract of adhesion:

A contract of adhesion is one wherein one party imposes a ready-made form of contract on the other. It is a contract whereby almost all of its provisions are drafted by one party, with the participation of the other party being limited to affixing his or her signature or “adhesion” to the contract. However, contracts of adhesion are not invalid per se as they are binding as ordinary contracts. While the Court has occasionally struck down contracts of adhesion as void, it did so when the weaker party has been imposed upon in dealing with the dominant bargaining party and reduced to the alternative of taking it or leaving it, completely deprived of the opportunity to bargain on equal footing. Thus, the validity or enforceability of the impugned contracts will have to be determined by the peculiar circumstances obtained in each case and the situation of the parties concerned.¹⁶⁶(Emphasis supplied)

For the Commission to find that the users’ consent to Cashalo’s Privacy Policy was not validly obtained, the CID must not just allege, but provide substantial evidence, that the users who consented to

¹⁶⁵ Data Privacy Act of 2012, chapter II, §§ 12-13.

¹⁶⁶ *Encarnacion Construction & Industrial Corp. v. Phoenix Ready Mix Concrete Development & Construction, Inc.*, G.R. No. 225402, 04 September 4, 2017.

the Privacy Policy were “completely deprived of the opportunity to bargain on equal footing.”¹⁶⁷

On the contrary, OETC has provided adequate proof that users have already been notified twice of what particular data shall be processed and the purposes for their processing.¹⁶⁸ These notifications are given at the earliest stage and even prior to the commencement of any processing.¹⁶⁹ In relation to consent, there is a natural presumption that “one does not sign a document without first informing himself of its contents and consequences.”¹⁷⁰ The CID failed to refute this presumption. Moreso, the CID also failed to prove that there was unauthorized processing that would warrant a violation under Section 25 of the DPA.

The CID also failed to prove that the OETC’s processing of personal data was violative of the DPA or any other law. As discussed, the Commission cannot find that OETC particularly violated the general data privacy principles of transparency, legitimate purpose, and proportionality found in the DPA. The CID has also not sufficiently argued that OETC violated any other provision in the DPA or other laws.

Further, the Commission finds that the CID failed to prove, with substantial evidence, that the Cashalo app has accessed data stored in the mobile phone of its users, particularly the user’s contact list, and that this processing was particularly unauthorized under the DPA or any other law. As the Supreme Court emphasized in *Government Service Insurance System v. Prudential Guarantee*, “it is basic in the rule of evidence that bare allegations, unsubstantiated by evidence, are not equivalent to proof. In short, mere allegations are not evidence.”¹⁷¹

¹⁶⁷ Id.

¹⁶⁸ Position Paper Ad Cautelam dated 23 July 2021 of Oriente Express Techsystem Corporation, ¶¶ 7-13.

¹⁶⁹ Id., ¶ 9.

¹⁷⁰ *Encarnacion Construction & Industrial Corp. v. Phoenix Ready Mix Concrete Development & Construction, Inc.*, G.R. No. 225402, 04 September 4, 2017.

¹⁷¹ G.R. No. 165585, 20 November 2013.

Thus, OETC and its responsible officers cannot be held liable for Section 25 of the DPA.

III. There is no substantial evidence to find that OETC violated Section 3(D)(4) of NPC Circular No. 20-01.

Section 3(D)(4) of NPC Circular No. 20-01 states:

SECTION 3. Guidelines. — The processing of personal data for evaluating loan applications, granting loans, collection of loans, and closure of loan accounts shall be subject to the following general guidelines:

xxx

D. Where online apps are used for loan processing activities, LCs, FCs, and other persons acting as such shall be prohibited from requiring unnecessary permissions that involve personal and sensitive personal information.

xxx

4. Access to contact details in whatever form, such as but not limited to phone contact list or e-mail lists, the harvesting of social media contacts, and/or copying or otherwise saving these contacts for use in debt collection or to harass in any way the borrower or his/her contacts, are prohibited. In all instances, online lending apps must have a separate interface where borrowers can provide character references and/or co-makers of their own choosing.¹⁷²

The CID argued that OETC violated NPC Circular No. 20-01 since there were dangerous permissions in the Cashalo app (Phone, Location, Storage, and Camera).¹⁷³ Further, with regard to OETC's alleged processing of the user's phone contact list for debt collection, the CID claimed that this was a prohibited activity that violated the Circular.¹⁷⁴

¹⁷² NPC Circular 20-01, § 3(D)(4) (14 September 2020).

¹⁷³ Memorandum dated 16 May 2022 of the Complaints and Investigation Division, at p.5.

¹⁷⁴ *Id.*, at p. 7.

OETC countered that the CID's allegations were unsubstantiated by evidence. Further, the access to contact lists were for fraud prevention, credit assessment, and KYC.¹⁷⁵ This can be proven by the various pop-up boxes notifying the user about the purposes for data processing.¹⁷⁶

After weighing the claims and proof of both parties, the Commission finds that there is a lack of substantial evidence to conclude that OETC violated Section 3(D)(4) of NPC Circular No. 20-01.

In CID's Supplemental Technical Report dated 14 May 2021, the CID admitted that "since data transmissions using API are secured, it is difficult to determine if the Cashalo application actually transmits the data to a remote database."¹⁷⁷ The CID explained that "what the phrase means is that it is difficult to determine what data the application is transmitting."¹⁷⁸ Thus, there is insufficient evidence on record for CID to support its claims about dangerous permissions. On the other hand, as discussed, OETC has provided adequate proof that it has not been accessing its users' contact lists for debt collection or harassment. It has also shown that it has made relevant changes in its Privacy Policy, and application, to better align with NPC Circular 20-01.¹⁷⁹

The CID has not proven that OETC accessed the contact list for unlawful purposes. In any event, OETC has provided proof that its latest version already removed access to a user's contact list, even for KYC, and there is a separate interface for users to input their character reference.¹⁸⁰

In summary, the CID has failed to prove with substantial evidence that OETC and its responsible officers: 1) failed to adhere to the

175 Memorandum dated 17 May 2022 of Oriente Express Techsystem Corporation, ¶ 145.

176 Id.

177 Supplemental Technical Report dated 14 May 2021 of the Complaints and Investigation Division, ¶ 15.

178 Comment/Opposition (to Respondent's Position Paper dated 23 July 2021) dated 13 August 2021 of the Complaints and Investigation Division, ¶ 10. (Emphasis supplied)

179 Memorandum dated 17 May 2022 of Oriente Express Techsystem Corporation, ¶ 139.

180 Id., ¶ 170.

general data privacy principles, 2) violated Section 25 of the DPA, and 3) violated Section 3(D)(4) of NPC Circular 20-01.

WHEREFORE, premises considered, the Fact-Finding Report with Application for the Issuance of a Temporary Ban against **Oriente Express Techsystem Corporation (Cashalo)** is hereby **DISMISSED**.

SO ORDERED.

City of Pasay, Philippines.
16 June 2022.

Sgd.

JOHN HENRY D. NAGA

Privacy Commissioner

WE CONCUR:

Sgd.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

Sgd.

DUG CHRISTOPHER B. MAH

Deputy Privacy Commissioner

Copy furnished:

CMT

Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

KRL,

Complainant,

-versus-

CID Case No. 17-K-003

*For: Violation of the
Data Privacy Act
of 2012*

**UNIVERSITY, AA, MC, NCB, RG
GV, GCT, RR, MR, PB**

Respondents.

X-----X

DECISION

AGUIRRE, *D.P.C.*

For consideration before this Commission is a complaint filed by KRL against University, **AA, MC, NCB, RG GV, GCT, RR, MR, and PB**, for an indeterminate violation of the Data Privacy Act (DPA).¹

These Proceedings

On 19 April 2018, this Commission, through the Complaints and Investigation Division, conducted a Discovery Conference. At the Conference, the respondents were directed to submit a responsive Comment within ten (10) days from receipt of the Order dated 26 April 2018.²

On 30 April 2018, the respondent university, through counsel, filed a Notice of Entry of Appearance with Motion for Clarification of Procedure. The respondent university raised an issue regarding the propriety of the Commission's act of taking immediate action on the complaint without having the complainant exhaust all the administrative remedies available to him. The respondent university also argued that the complaint should have been referred to a

¹ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [DATA PRIVACY ACT].

² Records, p. 46; see NPC Circular No. 16-04, Rule III, Section 15.

Mediation Officer to explore the possibility of first reaching an amicable settlement.

On 18 May 2018, the respondent university filed a Motion to Admit Comment with Partial Compliance, citing the “amount of documentary evidence being required from the respondent University.”³ The individual respondents, AA, MC, NCB, RG, GV, GCT, RR, MR, and PB have not submitted their individual comments. The Comment of the respondent university contained a narration of the incidents and arguments against the complainant’s allegation, and attached as annexes a Privacy Impact Assessment (PIA), DTR and Payroll processes, attendance records of the complainant, as well as affidavits from the Human Resources and Development Unit (HRDU) Director, the Clerk of the College of Business Management and Accountancy (CBMA), the Secretary of the CBMA, a part-time faculty member of the CBMA, the Department Head of the Real Estate Management (REM) of CBMA, and the Finance Director.

Facts

On the basis of these, the following facts were established:

The complainant was a part-time faculty member in the University. He was named in a letter-complaint written by the respondents, who are all faculty members of the University, informing WUT, president of the university, about alleged unreasonable and oppressive practices of the newly-appointed dean of the College of Business Management and Accountancy (CBMA), CS. Dean CS was the one who informed the complainant about the letter-complaint on 10 November 2017.

Copies of the letter-complaint were also furnished to the Chairman of the Board, the Commission on Higher Education (CHED), and the Regional Director of the Department of Labor and Employment (DOLE).

The pertinent portion of the letter-complaint stated as follows:

Gross ignorance of labor management

She called HR office and asked if [respondent university] follows the principle “no work, no pay.” She received an affirmative answer. She did not further inquire as to other details. She has no knowledge that holidays and those

³ *Id.*, p. 76

declared no classes for reason of fortuitous events and force majeure shall be paid to the employees as provided for by Labor Code provisions. She deducted all the hours/period for the holiday and no classes to the prejudice of the faculty members, and erased the total number of days we reported. But for one of her recruited faculty, by the name of **KRL, this dean, favorably endorsed the former's DTR**. The dates (August 21 and 28) included are the same dates for the other faculty members who were deducted from them but no deduction for Mr. Legaspi. Is she at liberty to make a mockery of the provisions of the Labor Code? To apply the law negatively to those employees, she doesn't like and to apply the same provisions positively to those employees, she likes? Are we changing now the core values of [respondent university]?⁴

Based on those statements, complainant concludes that the respondents were able to access his DTR and pay slip because they are specific about the deductions and have a strong conviction that he was paid for the dated holidays.⁵ The letter-complaint did not, however, attach copies of the complainant's daily time record (DTR) or pay slips.

The respondents do not deny having accessed the complainant's DTR. In fact, one of the respondents, RR, a Department Head of Real Estate Management and faculty member, admits that he chanced upon it when he was scanning the bundled DTRs of the entire CBMA for the month of August 2017.⁶ According to him, as a Department Head, he is sometimes asked to turn over accomplished DTRs of the faculty to the College Clerk or "attendance-in-charge" from the College Secretary when the latter is not present to personally receive it.⁷ He was looking for his DTR in a pile that was alphabetically-arranged when he caught sight of the complainant's DTR.⁸

Complainant wrote a letter-complaint to the NPC to hold the respondents liable for the damages caused to him personally and professionally.⁹ He stated that he intentionally did not file the complaint with University as he already lost trust and confidence in the institution.¹⁰

Arguments of the Parties

⁴ *Id.*, at p. 6-7. Emphasis in the original.

⁵ *Id.* at p. 1.

⁶ *Id.* at p. 117.

⁷ *Id.* at p.118.

⁸ *Ibid.*

⁹ *Id.*, at p.2.

¹⁰ *Id.*, at p. 2.

The complainant now comes to the Commission saying that he feels his right to privacy has been violated.¹¹ According to him, the respondents' act of copy furnishing CHED with their letter-complaint caused his personal information to be exposed to a more severe extent which caused him dismay.¹² He asserts that as a human resource management professor and someone who has been working in the industry for quite some time, he is fully aware that such information should be confidential.¹³ He states that he has experienced sleepless nights from the time he knew about the incident and feels threatened that all the personal information he submitted to the institution is at risk of exposure.¹⁴

The respondent university, in their Notice of Entry of Appearance with Motion for Clarification of Procedure, argues that the complainant failed to allege that he has exhausted all remedies available to him.¹⁵ Citing the Commission's Rules on the Alternative Modes of Dispute Resolution,¹⁶ it likewise raises that the complaint should have been referred to a Mediation Officer for assistance in reaching an amicable settlement¹⁷ since the complaint is devoid of any serious allegations that would warrant immediate conduct of investigation by the Commission.¹⁸

In their comment, the respondent university allege that they have substantially complied with the requirements of Republic Act No. 10173 or the Data Privacy Act of 2012 ("DPA"), having completed phases 1 and 2 of the registration process of the Commission. While it has already completed privacy impact assessments for most of its processes, the DTR system is not one of them. The respondent university conducted a privacy impact assessment on the DTR system after the Discovery Conference.¹⁹

The respondent university asserts that consent of data subjects is not required for the processing of the DTRs, because it is an administrative matter inherent in the operation and legitimate

¹¹ *Id.*, at p.1.

¹² *Ibid.*

¹³ *Id.*, at p.1.

¹⁴ *Id.*, at p.2.

¹⁵ *Id.*, at p.52.

¹⁶ NPC Circular 16-04, Sections 25-27.

¹⁷ Records, p. 55.

¹⁸ *Id.*, at p.55-56.

¹⁹ *Id.*, At p. 92-103.

purpose of the university.²⁰ It vehemently denies that there was unauthorized processing of complainant's personal data, as DTRs contain no personal or sensitive personal information, nor are the DTRs considered confidential by the University and its faculty members.

According to them, the DTRs are processed in the following manner:

1. The full time faculty members with overload, and part-time faculty members fill up the DTRs regularly and turn them over to the designated Attendance-in-Charge (usually, the Secretary/Clerk of the College).
2. On every cut-off date (the 15th and 20th of the month), the designated Attendance-in-Charge will check the DTRs for completeness and accuracy. They will forward the same to the office of the Dean for checking, signature, and endorsement to the HRDU.
3. The HRDU staff will check the data in the DTRs and will determine whether the DTR data match the data gathered from the biometrics. Once confirmed, the HRDU staff concerned forwards the attendance records to the HRDU Director for approval.
4. The HRDU forwards the DTR to Finance Unit for payroll processing.²¹

There are instances when the College Clerk or "attendance-in-charge" in the Office of the College Secretary is not around to personally receive the DTRs, particularly for the part-time faculty members who have limited time in the University and who rarely chance upon the College Clerk.²² For purposes of meeting the cut-off date for submission of the DTRs, as a matter of practice, faculty members transmit the DTRs to the College Secretary through the following methods: (a) by posting it in the corkboard inside the Dean's Office; (b) by asking a co-faculty to submit it to the College Clerk; (c) by asking their respective personal staff to submit the DTR to the

²⁰ *Id.*, At p. 85.

²¹ *Id.*, At p.107.

²² *Id.*, At p.109.

College Clerk; (d) by submitting it through the Department Head, and the latter will transmit the DTR to the College Clerk; (e) by asking the class beadle/president to submit the DTR of the faculty concerned to the College Clerk; or (f) course it through the Student Apprentice available.²³

The respondent university denies that the professors illegally accessed complainant's pay slip. According to them, the payroll system of the University is web-based and can only be accessed through the internet by the employee concerned. The pay slips are downloaded by the Payroll Master for viewing and printing by the concerned employee using his/her unique Employee ID code and password.²⁴

Issues

The issues to be resolved in this case are:

1. Whether the Commission erred in taking immediate cognizance of the complaint;
2. Whether the Commission erred in not requiring the parties to submit the complaint to alternative dispute resolution;
3. Whether the complainant's DTR contains personal information; and
4. Whether the respondents committed a violation in relation to the complainant's DTR, warranting a recommendation for prosecution under the Data Privacy Act of 2012.
5. Whether the respondents committed a violation in relation to the complainant's pay slip, warranting a recommendation for prosecution under the Data Privacy Act of 2012.

Discussion

The NPC committed no error in taking immediate cognizance of the complaint.

Section 4 of NPC Circular No. 16-04 provides that no complaint shall be entertained unless it has been shown that the complainant has informed, in writing, the concerned entity of the privacy violation or personal data breach and if there was no response within 15 days or

²³ *Id.*, at p.109.

²⁴ *Id.*, at p.124.

timely and appropriate action on the claimed privacy violation or personal data breach.

In his complaint filed on 28 November 2017, the complainant admitted the following:

I intentionally did not file the complaint to [respondent university] as I already lost my trust and confidence to the institution knowing that such information was given and exposed to and by the faculty members.²⁵

Nevertheless, the following exchange during the discovery conference shows that there was an attempt to comply with the requirement of exhaustion of administrative remedies:

KRL: Your honor just to answer that, I approach NPC on November 28, 2017 and they advised me to write a letter first to University, so I was advised correctly of what the process is all about and then they ask me to wait for 15 days if there will be no action, that's the time that we will pursue it and I informed them that "after 15 days there was no response from the Human Resource Department regarding my complaint, they weren't able to reach out to me: so that's the time I pursued it."²⁶

The respondent university indeed received a copy of the complaint on the same day it was received by Commission. The complainant stated for the record that when he submitted his complaint with the Commission, he had been advised to wait at least 15 days to afford the respondent university the opportunity to take appropriate action. However, no action was taken on his complaint.

At any rate, the same Section in Circular 16-04 provides that the Commission may waive any or all of the requirements for exhaustion of remedies, at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to the affected data subject. Considering the allegations on the face of the complaint that the complainant's DTR and pay slips may have been illegally accessed and disclosed by the respondents, it is well within the authority of the Commission to take action on this serious allegation of a violation of the DPA.

²⁵ *Id.*, At p.2.

²⁶ *Id.*, at p.32.

The decision to submit a case for alternative dispute resolution lies with the parties.

The Alternative Dispute Resolution Act of 2004 (the ADR Act of 2004) embodies the policy of the state to actively promote party autonomy in the resolution of disputes, or the freedom of the parties to make their own arrangements to resolve their disputes.²⁷ Mediation, in particular, is an alternative dispute resolution mechanism characterized by the principles of voluntariness, integrity of determination, and the policy that the decision-making authority in the mediation process rests with the parties.²⁸

At the onset of the Discovery Conference, Atty. Francis Acero, Chief of the Complaints and Investigation Division, asked the complainant if he was willing to compromise and settle amicably.²⁹ To this, the complainant answered in the negative.³⁰ To insist on the conduct of a mediation at this point would have been a violation of not only the ADR Act of 2004 but of the Commission's own alternative dispute mechanisms at that time as well.

The DTR contains personal information.

In their Comment with Partial Compliance, the respondent university attached a Privacy Impact Assessment (PIA) report on the DTR System of University.³¹ In the submitted PIA, the threshold analysis contained several questions, including: "(a) Will the project or system involve the collection of new information about individuals?"³² To this, the respondent answered "no."³³

A perusal of the complainant's DTRs, however, would show that the DTR document contains the complainant's handwritten name, the college or unit where he teaches, and the month covered.³⁴ The majority of the document is a table of dates with filled-out "time in" and "time out" fields. At the bottom of the document, there is a

²⁷ R.A. 9285, Section 2.

²⁸ *Ibid.*, at Section 8.

²⁹ Records, p. 27-28.

³⁰ *Id.*, at p.28.

³¹ Records, p. 92.

³² Records, p. 93.

³³ *Ibid.*

³⁴ Records, p. 125-129.

“prepared by” field with the complainant’s handwritten name and signature.³⁵

The DPA provides that personal information is any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.³⁶

In this case, the complainant’s name, college/unit, and signature are information from which his identity can be directly ascertained. The DTRs of the complainant, then, are considered to contain personal information.

The failure of the respondent university to treat the information collected in the monthly DTRs as personal information resulted in the lack of clearly documented and implemented policies regarding its processing. In conducting a PIA, the personal information controller – the respondent University, in this case - must refer to the law to determine what it should consider as personal information. If such collected information meets the definition or enumeration provided by the DPA for personal or sensitive personal information, then the obligations provided by law should be complied with: its processing must be based on any of the lawful criteria under the law, and it must be accorded the adequate organizational, technical, and physical security measures, to name a few. Hence, even if the personal information controller views certain information as “public knowledge,” it should still be properly classified according based on the definition provided by the law in the PIA and treated and protected accordingly.

It should be stressed that a PIA, however, is not an end in itself. In conducting a PIA, a personal information controller is tasked to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a personal information controller.³⁷ When no PIA has been conducted yet, it should be done on a per-process basis across all the processes of the of the organization in order to assess the current situation, the existing controls in place, the compliance gaps that have been overlooked, the

³⁵ *Ibid.*

³⁶ R.A. 10173, Section 3(g).

³⁷ NPC Advisory 2017-03.

privacy risks associated with them, and identify the measures needed to address them.

In order to specifically assess these risks, the personal information controllers should carry out their organization's data inventory and data map since both will help in classifying different categories and uses of personal data, and how they flow across the organization.

A PIA should be conducted prior to the deployment of a project, product, or service that involves the collection of personal information. When there are new or revised industry standards, organization policy, law or regulation, or when there are changes to methods in which personal information is handled, a personal information controller should conduct a PIA again on the pertinent process.

To emphasize, it should not only identify the existing controls and risks a project, product, or service may have upon personal data privacy, but it should lead to the identification of remedial actions or mitigation measures necessary to avoid or reduce those risks. These remedial actions and mitigation measures may be incorporated in the organization's Privacy Management Program (PMP).

In this case, the submitted PIA by the respondent university stated the existence of organizational, physical, and technical measures in place for the DTR system. After this, however, the respondent university did not provide details on these or how it intended to address what the Comment referred to as "long-standing practices" of the faculty regarding their submission of DTRs.³⁸ The affidavits of the College Clerk,³⁹ the Secretary of CBMA,⁴⁰ one of the part-time faculty,⁴¹ and a Department Head from the CBMA,⁴² admitted as well that there are several long-standing practices where the DTRs are transmitted through different routes⁴³ that deviate from the official process in handling the employees' DTR.⁴⁴

³⁸ Records, p. 86.

³⁹ *Id.*, at p. 109.

⁴⁰ *Id.*, at p.112.

⁴¹ *Id.*, at p.114.

⁴² *Id.*, at p. 116.

⁴³ *Supra* note 24.

⁴⁴ *Supra* note 22.

Nowhere in the respondent university's submitted PIA were these practices even mentioned, despite the fact that these should been considered as compliance gaps resulting in privacy risks that needed to be mitigated by reasonable and appropriate organizational, physical, and technical measures. By simply treating it as a checklist, the respondent university treated the PIA as the ultimate result, when it should have considered it as a tool to improve its processes and systems for the protection of its stakeholder's privacy.

It is incumbent upon the respondent university to revise its PIA in general and on the DTR system in particular to reflect and address the gaps brought about by actual, current practices and as identified in the letter-complaint.

Respondents did not commit a violation in relation to the complainant's DTR to warrant a recommendation for prosecution.

In analyzing whether there are possible violations by the respondent faculty members of the DPA that warrant a recommendation for prosecution, we primarily look into the different stages of processing that the personal information undergoes, and determine whether each one is supported by one or more lawful basis for processing enumerated in the DPA.

The lack of either a uniform policy or process that covers the actual practices in the handling of the employees' DTR, including the ones identified by the aforementioned affiants, cannot by itself give rise to a cause of action for unauthorized or illegal access to personal information as provided by the DPA.⁴⁵ It was admitted by respondent RR that as a Department Head, he is sometimes asked to turn over accomplished DTRs of the faculty to the attendance-in-charge from the College Secretary when the latter is not present to personally receive it.⁴⁶ This color of authority to access the DTRs, with the acquiescence of the faculty members over time, cannot be overlooked.

⁴⁵ SEC. 26. *Accessing Personal Information and Sensitive Personal Information Due to Negligence.* – (a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

⁴⁶ *Supra* note 8.

Indeed, the interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.⁴⁷ That cannot be said to be the case here, as the complainant and other faculty members could have reasonably expected the further access of their DTRs by different persons in the college upon submission thereof based on the existing practice of the school.

This Commission has previously decided that this concept of “reasonable expectation” is considered in determining the legitimacy of the additional processing by examining whether such further processing is compatible with the original business purpose communicated to the data subject and not beyond what the data subject may reasonably expect as to the purpose, scope, manner, and extent of the processing of their personal data.⁴⁸

Having discussed respondent professors’ initial access, the next stage of processing in this case was the use of the information in the DTR to support their claim of “gross ignorance of labor management” in their letter-complaint about Dean CS.

The individual respondents used the complainant’s name to give a specific case of “gross ignorance of labor management,” which was one of the allegations against Dean CS. The letter-complaint questioned the Dean’s alleged unequal treatment regarding holidays and suspended class days due to fortuitous events in the DTRs of faculty members, in relation to the provisions of the Labor Code on holiday pay. To the respondent professors’ personal knowledge, the complainant was the only faculty member who did not receive deductions on the holidays of August 21 and 28 of 2017. The use of the complainant’s name, therefore, was necessary for the protection of the respondents’ lawful rights and interests as contemplated by Section 13(f) of the DPA. The fact that the respondents copy-furnished both the CHED and DOLE does not veer away from that lawful criteria, considering the allegations of the letter-complaint may possibly be the concern of these agencies as well.

⁴⁷ NPC Advisory Opinion 2018-20.

⁴⁸ See, *Villegas v. Revilles*, NPC Case 17-047, *citing* EU General Data Protection Regulation, Recital 47.

Although Section 13(f) applies to sensitive personal information while the information involved in this case is just personal information, the protection of lawful rights and interests under Section 13(f) by the respondent faculty members in this case is considered as legitimate interest pursuant to Section 12(f) of the DPA. This section provides that it is lawful to process personal information if it is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.⁴⁹

The DPA is not intended to cover every possible infraction in the workplace or even society. While the complainant may feel aggrieved with the mention of his name in the letter-complaint, it cannot be said, however, that the complainant incurred actual damage, considering the objective of that letter-complaint was to inform the President of University of their concerns about the Dean and not the complainant. In the event that the circumstances stated in the letter-complaint about the complainant are untrue, there are other remedies available to him under existing laws, although not the DPA. The merits of the letter-complaint and the truth of their claims are irrelevant to our determination whether there was a violation of the DPA in the processing of complainant's DTR.

The respondents did not commit a violation in relation to the complainants pay slip to warrant a recommendation for prosecution under the Data Privacy Act of 2012.

In the complaint, the complainant alleges that "based on [the statements in the respondents' letter], they were able to access [his] pay slip."⁵⁰

In cases filed before administrative or quasi-judicial bodies such as the Commission, a fact may be deemed established if it is supported by substantial evidence, or that amount of relevant evidence which a reasonable mind might accept as adequate to justify a conclusion.⁵¹

⁴⁹ R.A. 10173, Section 12(f).

⁵⁰ Records, p. 1.

⁵¹ Rules of Court, Rule 133, Section 5.

The complainant's allegation in relation to his pay slip remains unsubstantiated. This is all the more true considering the affidavit of the Finance Director that stated "any figures or computation in determining one's payroll is done within the department's office and the finance personnel are the only ones who are authorized to view and do the computation" and that "no other department computes the figure, the HRD only provides the supplementary documents in order to arrive with the figure."⁵² There is nothing in the allegations of the complainant that explain how the respondent faculty members could have circumvented the university process on the processing of pay slip to access the same aside from his mere speculation. Notice must also be made that there was no mention of the complainant's salary in the subject letter-complaint to WUT

WHEREFORE, premises considered, the Commission finds no violation of the Data Privacy Act on the part of the respondents University, **AA, MC, NCB, RG GV, GCT, RR, MR, PB**, to warrant a recommendation for prosecution. The complaint filed by complainant KRL is hereby **DISMISSED**.

SO ORDERED.

Pasay City, 19 November 2019.

(SGD.)

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

Concurring:

(SGD.)

IVY D. PATDU

Deputy Privacy Commissioner

(SGD.)

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

⁵² Records, p. 177

COPY FURNISHED

KRL

Complainant

Quezon City, Metro Manila

ABAD ABAD & ASSOCIATES

Counsel for Respondent

Unit 215 Buma Building, 1012 Metropolitan Avenue
San Antonio Village, Makati City, Metro Manila

COMPLIANCE AND MONITORING DIVISION

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

JLB,

Complainant,

CID-18-D-009

*For: Violation of the
Data Privacy Act of
2012*

-versus-

SECURITY BANK CORPORATION,

Respondents.

X-----X

DECISION

**NAGA,
D.P.C.:**

This case involves an alleged unauthorized disclosure by the Respondent of the Cash Advance Personal Identification Number (CA PIN) and other personal information of the Complainant to unknown persons.

The Facts

JLB (Complainant) is a Security Bank Mastercard credit card holder since 16 January 2018. Security Bank Corporation (Respondent) is a universal banking corporation duly organized and existing under the laws of the Philippines.

On 29 January 2018, Complainant requested the CA PIN of his credit card through the Customer Service Hotline of the Respondent.

On 03 February 2018, Respondent, through Safefreight Services, Inc. (Safefreight), delivered the requested CA PIN to the billing address of the Complainant, which was received by a certain LA who identified herself as the Complainant's maid/caretaker. However, in a phone call with the Respondent's representative, the Complainant denies knowing LA. The Complainant then conveyed

to the representative of the Respondent to deliver the subsequent requested CA PIN to CB, MNB, and JPB only.

Respondent then delivered the second CA PIN to the Complainant's billing address, which was received by CB on 23 February 2018.¹

On 26 February 2018, the courier service provider, Safefreight, investigated the complaint of the Complainant in relation with the first CA PIN. Safefreight visited Complainant's residence and was able to speak with LA. LA confirmed the receipt of the first CA PIN, which according to her was forwarded to the Complainant.²

On 04 April 2018, Respondent's Customer Contact Group received an email from Complainant alleging that the bank exposed his personal and banking information to unknown individuals.

On 07 April 2018 a regenerated third CA PIN was delivered to the billing address of the Complainant, which was received by CB.

On even date, the Commission, through its Complaints and Investigation Division (CID), received the Letter of Complaint dated 06 April 2018 from the Complainant.

The Complainant alleged that the Respondent exposed his personal and sensitive personal information (i.e., full name, address, CA PIN, and name of bank) to persons unknown to him and that it may bring potential risk to his finances and safety. Complainant thus, charges Respondent with violations of Sections 32 and 33 of the Data Privacy Act of 2012 (DPA).³

Respondent filed its Comment in compliance with the Commission's Order dated 04 July 2018. Respondent argues the following:

¹ Note that the Respondent's agent erroneously reported to the Complainant that it was delivered to a certain MC. Nevertheless, the Complainant acknowledged in his Reply to the Respondent's Comment that the second CA PIN was received by CB.

² Annex 3 of Respondent's Comment

³ Complaint dated 06 April 2018

1. The CA PIN documents were properly sealed and endorsed to the courier services and it was delivered to the billing address indicated in the Complainant's credit card application.
2. Upon the investigation of Safefreight, they were able to validate that LA is the Complainant's maid and that she was able to forward the CA PIN to the Complainant.
3. That the properly sealed second and third CA PIN was received by the Complainant's father, CB in the indicated billing address.⁴

In the Order dated 20 June 2018, the case was called for Discovery Conference on 04 July 2018.

On 04 July 2018, the Complainant and Respondent's counsel appeared before the Commission and signified that there is no need to secure evidence from each other to further their case.

Complainant filed his Reply to the Respondent's Comment on 05 August 2018. In the Reply, the Complainant restated the allegations in his Complaint. He also maintained that the proof of delivery signed by LA should not be considered proof of delivery to the correct address or that it was received by an authorized recipient. Further, he emphasized that he does not know LA.

On 19 February 2020, this Commission ordered the Respondent to submit Supplemental Comment with reference to item number 25 of their submitted Comment.⁵ Specifically, the Commission wants the Respondent to submit details on utilization of the three CA PINs that were issued to the Complainant herein. However, up to date, the Commission did not receive any submissions from the Respondent.

Issue

⁴ Respondent's Comment dated 04 July 2018

⁵ 25. Lastly, it should also be noted that Complainant JLB has already used the CA PIN he requested when he successfully availed a cash advance through his credit card on 09 April 2018. Prior to this, there were two (2) CA PIN transactions involving attempts to avail cash advance made on 03 April 2018 with reference to the credit card of Complainant JLB. This only goes to show that Complainant JLB received his CA PIN.

Whether the Respondent violated Sections 32 and 33 of the DPA.

Discussion

The Complaint lacks merit. The Commission finds that the Complainant herein failed to prove by substantial evidence violations of Section 32 and Section 33 of the DPA by the Respondent herein.

As already established in past rulings, in administrative proceedings such as in this Commission, the burden is on the Complainant to prove by substantial evidence the allegations in his Complaint are true.⁶ “Substantial evidence is more than a mere scintilla of evidence. It means such relevant evidence as a reasonable mind might accept as adequate to support a conclusion, even if other minds equally reasonable might conceivably opine otherwise.”⁷

Section 32 (Unauthorized Disclosure) and Section 33 (Combination or Series of Acts) of the DPA provide, *thus*:

SEC. 32. *Unauthorized Disclosure.* – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one (1) year to three

(3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

(b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos

⁶ Montemayor v. Bundalian, 453 Phil. 158 167

⁷ *Ibid*

(Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

SEC. 33. *Combination or Series of Acts.* – Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

Complainant alleges that unauthorized disclosure of personal and sensitive personal information was committed when the Respondent delivered the first CA PIN to LA, a person that the Complainant does not know. In the Comment provided by the Respondent, it was stated that the three (3) CA PINs were delivered in the billing address provided by the Complainant to the Respondent in his credit card application. The first CA PIN was received by LA, who upon the Courier Troubleshoot Investigation Report conducted by Safefreight,⁸ revealed that she was the Complainant's maid. It was later found out that the second and third CA PINs were received by CB, the father of the Complainant, in the same billing address. In fact, the second and third CA PINs were eventually used by the Complainant in two (2) instances on 03 April 2018 and on 09 April 2018.

Instead of presenting an evidence to counter the Respondent's contentions, the Complainant herein just reiterated in his Reply his allegation that LA is not known to him, viz:

"I can no longer count how many times I have advised Security Bank Corporation (SBC) that I do not know any person name LA."⁹

Section 1, Rule 131, of the Revised Rules on Evidence provides, viz:

Burden of proof and burden of evidence. – Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim or defense by the amount of evidence required by law. Burden of proof never shifts.

⁸ Annex 3 of Respondent's Comment

⁹ Reply of the Complainant to the Respondent's Comments

Burden of evidence is the duty of a party to present evidence sufficient to establish or rebut a fact in issue to establish a prima facie case. **Burden of evidence may shift from one party to the other in the course of the proceedings, depending on the exigencies of the case.** (Emphasis supplied)

At this point, the Complainant has now the burden of evidence to prove in his Reply that LA is not known to him and that there was improper delivery of the CA PIN despite the delivery of the Respondent in the billing address as stated in the Complainant's credit card application. However, in this case, the Complainant just reiterated and relied on his allegations to counter the defenses provided by the Respondent. Basic is the rule that mere allegation is not evidence and is not equivalent to proof.¹⁰

Having failed to prove the factual allegations contained in the Complaint by substantial evidence, the allegations for violation of Section 32 and Section 33 of the DPA should likewise fail.

On another matter, this Commission would like to respond to the Respondent's assumption that it already established reasonable and appropriate measures intended for the protection of personal information just because it sent to its clients a properly sealed document, viz:

"There is also no unauthorized disclosure of Complainant JLB's CA PIN. We invite the attention of the Honorable Commission that when a CA PIN requested by a certain client is delivered, **the same is contained in a properly sealed document which can only be opened by tearing the sides of perforated paper....** Thus, even if the properly sealed document containing the CA PIN was handed to LA by the courier, delivery alone to the latter of the same is not equivalent to unauthorized disclosure of his CA PIN."

This Commission does not agree with Respondent's assertion that properly sealing of the documents is all it takes to comply with the DPA in this case. Section 20 of the DPA provides:

¹⁰ Morales, Jr. v. Ombudsman Carpio-Morales, et. al., G.R. No. 20808627, July 2016

SEC. 20. Security of Personal Information. – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

To fully comply with the DPA, delivery procedure must include the policy that a document shall only be given to authorized persons if the primary recipient is not present to receive such document and other policies that will ensure the proper disclosure of documents containing personal and sensitive personal information.

Further, even if the Respondent subcontracts its courier service, the DPA still puts the responsibility of complying with the requirements of said law on the Personal Information Controllers (PICs), viz:

SEC. 14. Subcontract of Personal Information. – A personal information controller may subcontract the processing of personal information: Provided, That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws.

Thus, even if the Complainant failed to establish his case by substantial evidence, this Commission would not be precluded to conduct Compliance Check to the Respondent herein as provided by NPC Circular No. 18-02. This is to ensure that its processes and procedures are compliant with the DPA and other issuances of the Commission.

WHEREFORE, all premises considered, this Commission resolves to **DISMISS** the instant Complaint filed by JLB against Security Bank Corporation for lack of merit.

SO ORDERED.

Pasay City, Philippines;
18 March 2021.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

JLB
Complainant

LPMMDAF
Counsel for the Respondent

SECURITY BANK CORPORATION

Respondent

COMPLAINTS AND INVESTIGATION DIVISION

COMPLIANCE AND MONITORING DIVISION

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

KGR,

Complainant,

-versus-

CID Case No. 18-E-040

*For: Violations of Sections
27, 28,
31, and 32 of the Data
Privacy Act of 2012*

BB, JA, AA

Respondents.

X-----X

DECISION

AGUIRRE, D.P.C.

Before this Commission is a complaint by KGR (“Complainant”) against BB, JA, and AA (“Respondents”) for violation of several provisions of the Data Privacy Act.

The Facts

Complainant was at Rans C Computer Repair Services (“Ran C”) sometime in the morning of 07 March 2018 to print a copy of her resume. She was assisted by Respondent BB, a staff member of Ran C. After several attempts of printing her resume, she was given one copy for which she paid P8.00. Upon checking her resume, she noticed a straight white line on her picture. She called the attention of Respondent BB, who told her that it was fine and that is how the machine prints. Complainant stated that she will not pay for that kind of printing.

Thereafter, on 11 March 2018, Complainant and her mother went to Ran C and she saw copy of her resume posted on one of the CPUs in the shop.¹ Complainant and her mother called the attention of the present staff member, Respondent JA. Respondent JA asked Respondent BB about the resume over the phone and the latter replied,

¹Records, p. 2.

*“Sorry po talaga Ma’am nainis po kasi ako.”*² Respondent AA, the owner of Ran C, claims she was not aware of the incident as she was not in the shop for the past few days. Complainant filed an Incident Report, Blotter, and sent two (2) Memoranda to Respondents requesting for a letter of apology and damages under the Data Privacy Act of 2012,³ which Respondents never replied to.

On 22 May, Complainant filed a Complaint-Affidavit with the National Privacy Commission (“Commission”). The case was called for Discovery Conference on 19 July 2018 and was reset to 11 September 2018 due to work suspension on the original schedule.

During the Discovery Conference, the parties manifested that they were not willing to enter into a settlement. Complainant was given ten

(10) days to submit additional evidence to substantiate her allegations. Respondent was given ten (10) days from receipt of such additional evidence to file their Responsive Comment. Complainant was given ten (10) days after her receipt of this to file her Reply.⁴

On 24 September 2018, Complainant sent an email to the Commission stating thus:

As I want to practice and fight for my rights, I feel and am already very exhausted mentally and emotionally. I and my uncle have been trying to have a reasonable and fair settlement with them out of court witnessed by the Circle C Mall admin staff and security officers but they still won’t cooperate. I have decided to stop and not pursue this anymore. Again, thank you to you all. I do appreciate your noble servitude in protecting the privacy rights of your fellow Filipino/s. May God bless you always!⁵

Respondents later filed a Motion to Waive Presentation of Additional Evidence (with attached Joint Counter Affidavit) dated 26 September 2018, stating that the Complainant failed to provide additional evidence and must be deemed to have waived her right to submit the same.⁶

² *Ibid.*

³ *Id.*, pp. 9-10; 17.

⁴ *Id.*, p. 38.

⁵ *Id.*, p. 48.

⁶ *Id.*, p. 39.

Arguments of the Parties

Complainant alleges that the resume contained her sensitive personal information. In her Complaint, she states that “everyone who entered the shop can easily see her resume.”⁷ She filed a criminal complaint for violation of Sections 27, 28, 31, and 32 of the Data Privacy Act arising from Improper Disposal, Unauthorized Purposes, Malicious and Unauthorized Disclosure of her sensitive personal information without her prior consent and knowledge.⁸

In their Joint Affidavit, Respondents admit that BB cut the portion of Complainant’s resume where her photo, address, contact nos. and e- mail were printed. They state that he pasted this on the side of the CPU inside the cashier’s counter for purpose of identifying the Complainant in case she returns. He did it because he does not want to transact anymore with Complainant.⁹

They dispute the Complainant’s allegations, thus:

It must be emphasized that the size of the CPU where the resume portion was posted is not fronting a customer or the customer area. Ergo, a customer cannot see what was pasted on the CPU side unless the customer will get [sic] inside the counter or overreach the desk. To conclude, Complainant noticed her photo on the side of the CPU because she is the very person in the photo. She is familiar with herself and her own resume. Be it noted that Complainant’s personal information are not readable from the customer area because the font is too small. In short, there is no public accessibility of the information which R.A. 10173 intends to penalize.

Issue

The issue to be resolved in this case is whether Respondents committed acts in violation of Complainant’s privacy rights under the Data Privacy Act.

⁷ Ibid.

⁸ *Id.*, p. 1.

⁹ *Id.*, at p. 42.

Discussion

At the outset, it should be noted that the email sent by Complainant on 24 September 2018 to the Commission expressing her intention not to pursue the case cannot be considered an affidavit of desistance for purposes of terminating the case. The Commission thus resolves this Complaint on the basis of the evidence on record.

Respondents misunderstand the concept of personal information controllers, processing, and disposal.

In their Joint Affidavit, Respondents argue:

None of the Respondents is a personal information controller nor a personal information processor. Respondents are not engaged to (sic) any of those acts that would define them as personal information controller or processor. Respondents are engaged in the lease of computer units and printing of paper works. They are not engaged in the act of “processing” as defined in R.A. 10173.¹⁰

There is nothing in the law that requires entities to be engaged in the primary business of processing information before they are considered personal information controllers. By having the control of and discretion in the use of personal information of individuals, they are already considered the controller. They are thus accountable for the protection of the information and for the observation of the obligations under the law. These persons and entities must be able to justify their processing of personal data under any of the lawful criteria provided in the law.¹¹ They have an obligation to provide mechanisms for the access, correction, and removal of personal data upon request, as well as the filing of a complaint. They are further required to secure the processing of any personal data by documenting and implementing organizational, technical, and physical measures to respect the abovementioned rights.¹² At the core of these obligations are the general data privacy principles¹³ of transparency, legitimate purpose, and proportionality. Following this, any person or entity that

¹⁰ Records, p. 45.

¹¹ R.A. 10173, §§ 12-13.

¹² *Id.*, at § 20.

¹³ *Id.*, at § 11.

processes information should process information only for legitimate purposes that have been made known to the data subject. They should only process as much information as is needed to achieve their clearly defined and stated business purposes or to comply with the provisions of law or regulation.

Respondents also argue that:

The act prohibits (sic) by Sec. 28 is “processing.” Sec. 3 (j) of R.A. 10173 defined processing as “any operation any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

Respondents did not conduct any kind of operation or any set of operation. The personal information in the resume portion was not collected, recorded, organized, stored nor updated. Neither was there modification, retrieval, consultation, use, consolidation, blocking, erasure nor destruction of data. The personal information in the resume portion remained as is.¹⁴

It must be clarified that “processing” under the Data Privacy Act is *any* use of personal and sensitive personal information for the duration of its entire data life cycle – from its collection, processing, and retention, up to the disposal or erasure of personal data. A data life cycle begins and ends taking into consideration the purpose for processing that information in the first place.

Despite Respondents’ assertion that they are engaged in the lease of units and printing of paper works,¹⁵ they nevertheless still handle personal information in the course of their operations. Respondents must bear in mind that their processing of such personal information should only be for the purpose of delivering the services they provide.

In addition, Respondents’ appreciation of the term “disposal” is also misplaced. In their Joint Affidavit, they state:

Disposal means “throwing away.” To set the record straight, Respondents did not dispose the resume portion bearing the photo, contact number, address and e-mail of Complainant.

¹⁴ Records, p. 44.

¹⁵ *Supra* at note 10.

Respondent BB pasted the resume portion on the CPU and not “disposed.”¹⁶

Contrary to what Respondents assert, “disposal” is not limited to the physical act of throwing away. Simply recycling the backside of a document containing personal or sensitive personal information can be considered “improper disposal” since it allows the further processing of the personal data despite its purpose having already been fulfilled. As stated above, personal data should only be processed for as long as necessary to achieve the stated purpose. Once that purpose is achieved, the personal data should be disposed of in a way that makes further processing no longer possible.

Respondent and all other personal information controllers should be aware of the obligations imposed by the Data Privacy Act. These misconceptions, though not enough to merit a recommendation for prosecution in this case, nevertheless pose very real risks to data subjects.

The Complaint must be dismissed for lack of merit.

It is a disputed fact whether the posted resume is indeed viewable by the general public. While the Complainant alleges that “it can be easily seen by anyone who will enter their shop,” the Respondents claim that “the side of the CPU where the resume portion was posted is not fronting a customer or customer area... a customer cannot see what was pasted on the CPU side unless the customer will get (sic) inside the counter or overreach the desk.”¹⁷

Such fact is crucial in determining whether such posting was pursuant to a legitimate business interest – that is, choosing whom to transact with – and whether such was done in a manner that is mindful of the general privacy principle of proportionality.

In administrative proceedings such as this case, it is the complainant who carries the burden of proving their allegations with substantial

¹⁶ Records., p. 43.

¹⁷ Records, p. 43.

evidence or such “relevant evidence that a reasonable mind might accept as adequate to support a conclusion.”¹⁸

Instead of providing the additional evidence as directed during the Discovery Conference,¹⁹ Complainant sent an email to the Commission stating that she will no longer pursue the case.²⁰

The Commission is bound to adjudicate complaints following its Rules of Procedure, which provides:

Section 22. Rendition of decision. – The Decision of the Commission shall adjudicate the issues raised in the complaint **on the basis of all the evidence presented** and its own consideration of the law.²¹

As such, on the basis of all the evidence presented, the Commission finds that there is insufficient evidence to support the claims of Complainant for Respondents’ violation of the Data Privacy Act.

The Commission therefore resolves to dismiss the complaint for lack of substantial evidence required in establishing cases before quasi-judicial bodies.

WHEREFORE, on the basis of this Complaint, the Commission hereby resolves to **DISMISS** the Complaint of KGR against Respondents BB, JA, and AA.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against the Respondent before any other forum or tribunal, if any.

SO ORDERED.

Pasay City, 12 May 2020.

¹⁸ Ombudsman v. Fetalvero, G.R. No. 211450, 23 July 2018.

¹⁹ Records, p. 38.

²⁰ *Supra* at note 5.

²¹ NPC Circular No. 16-04 dated 15 December 2016 (“NPC Rules of Procedure”), Sec. 22, Emphasis supplied.

(sgd)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

(sgd)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(sgd)
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED

KGR
Complainant

**BB,
JA,
AA**
Respondents

AMM
Counsel for Respondents

**COMPLAINTS AND INVESTIGATIONS DIVISION;
ENFORCEMENT DIVISION;
GENERAL RECORDS UNIT**
National Privacy Commission

JRG,

Complainant,

-versus-

NPC Case No. 19-450

(Formerly CID Case No. 19-450))

*For: Violation of the Data
Privacy Act of 2012*

**CXXX LENDING CORPORATION
(EP),**

Respondent.

X-----X

DECISION

AGUIRRE, D.P.C.:

Before this Commission is a Complaint by JRG (Complainant) against CXXX Lending Corporation (Respondent) for a violation of the Data Privacy Act of 2012.

Facts of the Case

Complainant, using the Complaints-Assisted Form, described her complaint as follows “*harassment & invasion of privacy; text blasting to all my contacts.*”¹ She stated that she has suffered depression and trauma from Respondent’s acts.² She alleged that she found out about this incident when her contacts forwarded to her the text message.³ Complainant indicates that she is seeking a temporary ban on Respondent’s processing.⁴

The parties were initially scheduled for Discovery Conference on 12 August 2019, but this was rescheduled after a Presidential Proclamation declared this as a regular holiday in observance of the Muslim feast of Eid’l Adha.⁵ The Discovery Conference was reset to 19 August 2019.

¹ Complaints-Assisted Form received on 28 June 2019.

² *Id.*, at 3.

³ *Id.*, at 5.

⁴ *Id.*, at 7.

⁵ Presidential Proclamation No. 555.

At the Discovery Conference, Respondent was present but Complainant failed to appear. The Investigating Officer issued an Order resetting the Discovery Conference to 18 September 2019⁶ but Complainant again failed to appear on the said date.⁷ Thereafter, the Investigating Officer issued an Order requiring Respondent to file a Responsive Comment within ten (10) days from receipt of that Order.⁸

In their Comment, Respondent confirmed that Complainant was a borrower whose account was overdue for one hundred thirty two (132) days. As to the allegations of “text blasting” to all the Complainant’s contacts, Respondent stated thus:

We are not tolerating any indecent moves of our employee/agent... The original term is only 14 days and the purpose of which is being explained by our review team “as it is for emergency use only.” It is also disclosed that we are asking for at least two to five (2-5) character references in the event that we cannot contact her.⁹

Respondent alleges that Complainant has given her consent for the access of her contact lists. Their Comment stated thus:

Based on Republic Act No. 3765, otherwise known as Truth in Lending Act, the company observes the disclosure requirements as it is being read by the clients/customers by clicking “agree” prior to claiming the loan proceeds at our accredited merchant partners branch of her choice. As it is operated online, systems generated loan Agreement is provided herein...[a]pplication procedures are also attached herein... the said procedures will best answer her queries. **Therefore, she allows us to access her contact lists.** She may review the said procedures to help her clarify her complaint, as we cannot access her contacts without her permission.¹⁰

Issue

1. Whether Respondent committed a violation of the Data Privacy Act that warrants a recommendation for prosecution; and

⁶ Order dated 19 August 2019.

⁷ Attendance Sheet for Discovery Conference dated 18 September 2019.

⁸ Order dated 18 September 2019.

⁹ Comment dated 08 October 2019. Emphasis supplied.

¹⁰ *Ibid.*

2. Whether a temporary ban should be issued against Respondent's processing of personal data.

Discussion

The Complaint does not warrant a recommendation for prosecution of a violation under the Data Privacy Act

The Complaint alluded to certain messages sent by Respondent to her contacts. The Complaint, however, did not specify the content of these forwarded text messages. Aside from allegations that she learned about the incident from messages forwarded by her contacts, Complainant has not offered any proof of the existence of these messages supposedly sent by Respondent to third parties. She has also not identified the contacts she was referring to.

Despite several opportunities given to Complainant to substantiate her allegations at the two (2) Discovery Conferences scheduled on 19 August 2019 and 18 September 2019, Complainant failed to appear without notice or justification.

Given all these, the Commission is left without any basis to recommend Respondent for prosecution under the Data Privacy Act, considering it is bound to adjudicate following the NPC Rules of Procedure, which provides:

Section 22. Rendition of decision. – The Decision of the Commission shall adjudicate the issues raised in the complaint **on the basis of all the evidence presented** and its own consideration of the law.¹¹

As the Supreme Court held in *Government Service Insurance System v. Prudential Guarantee*, “it is basic in the rule of evidence that bare allegations, unsubstantiated by evidence, are not equivalent to proof. In short, mere allegations are not evidence.”¹²

As such, in the absence of sufficient evidence to support Complainant's allegations that Respondent disclosed her personal

¹¹ NPC Circular No. 16-04 dated 15 December 2016 (“NPC Rules of Procedure”), Section 22. Emphasis supplied.

¹² G.R. No. 165585, 20 November 2013, *citing* Real v. Belo, 542 Phil. 109 (2007).

information to her contacts, it cannot be said that Respondent committed an act that would constitute the prohibited acts of unauthorized processing¹³ or processing for an unauthorized purpose.¹⁴

The Complaint does not warrant the issuance of a temporary ban

Complainant stated in the Complaints-Assisted form that she is applying for a temporary ban on Respondent's processing of her personal data based on the ground of "legal & hearing."¹⁵ The issuance of this is governed by the NPC Rules of Procedure which provide:

Section 19. *Temporary Ban on Processing Personal Data.* – At the commencement of the complaint or at any time before the decision of the National Privacy Commission becomes final, a complainant or any proper party may have the National Privacy Commission, acting through the investigating officer, impose a temporary ban on the processing of personal data, if on the basis of the evidence on record, such a ban is necessary in order to preserve the rights of the complainant or to protect national security or public interest.

a. A temporary ban on processing personal data may be granted only when: (1) the application in the complaint is verified and shows facts entitling the complainant to the relief demanded, or the respondent or respondents fail to appear or submit a responsive pleading within the time specified for within these Rules; xxx¹⁶

Considering the findings above on the Complaint's lack of substantial evidence, Complainant's application for the issuance of a temporary ban is denied.

Respondent misunderstands the concept of consent

Nevertheless, the Commission notes that Respondent misunderstands the Data Privacy Act (DPA) in asserting that they obtained Complainant's consent to access her contacts.¹⁷

¹³ Republic Act No. 10173, Section 25.

¹⁴ *Id.*, at Section 28.

¹⁵ Complaints-Assisted Form, p. 7.

¹⁶ *Supra* Note 11, at Section 19.

¹⁷ *Supra* Note 9.

The Loan Agreement, attached to their Responsive Comment, contains this provision:

VIII. Waivers

xxx

The Borrower hereby willingly, voluntarily, and with full knowledge of his right under the law, waives the right to confidentiality of information and authorize the Lender to disclose, divulge, and reveal any such information relating to Borrower's loan availment, including events of default, for the purpose of, among others, client evaluation, credit reporting or verification and recovery of the obligation due and payable to the Lender under this Loan Agreement.

In view of the foregoing, the Lender may disclose, divulge and reveal the aforementioned information to third parties, including but not limited to the Borrower's employer, credit bureaus, the Lender's affiliate, subsidiaries, agents, service providers, as well as any prospective assignee or transferee, rating agency, insurer, and any such person, entity or regulatory body that may be required by law or competent authority.¹⁸

Personal information controllers who rely on consent as basis to process their information must ensure that such consent is "freely given, specific, and an informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her."¹⁹

In its waiver provision, Respondent combines various purposes for disclosure and various parties to be given access of Complainant's information. This does not meet the requirement for consent to be specific. Having an enumeration of each and every purpose of the processing in a single paragraph still fails to provide the data subject with a genuine choice as he or she will be bound to sign off on the entire provision in toto.²⁰

Provisions that use vague and overbroad language, as in this case, cannot be said to comply with the general privacy principle of

¹⁸ *Id.*, at Annex A.

¹⁹ Republic Act No. 10173, Section 3(b).

²⁰ NPC Advisory Opinion 2018-063. 23 October 2018.

transparency. As the DPA's Implementing Rules and Regulations explain:

The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

While the Commission finds that the allegations of Complainant are not sufficiently substantiated to warrant a recommendation for prosecution, it finds it necessary to emphasize the need for personal information controllers, such as Respondent, to inform their data subjects of the purpose of the processing of their personal information in "clear and plain language." The requirement to use clear and plain language does not mean using layman's terms to substitute technical words at the risk of not capturing the complex concepts they represent. Rather, this requirement means that information should be provided in as simple a manner as possible, avoiding sentence or language structures that are complex.²¹ The information provided should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations²² such as in the above-cited provision which uses the word "any" several times, as well as wordings like "including but not limited to".

WHEREFORE, all the above premises considered, the Complaint by JRG against CXXX Lending Corporation is hereby **DISMISSED**.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against the Respondent before any other forum or tribunal, if any.

SO ORDERED.

Pasay City, Philippines;
09 June 2020.

²¹ See, Guidelines on transparency under Regulation 2016/679 of the Article 29 Working Party (2017).

²² *Ibid.*

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

Copy furnished:

JRG
Complainant

CXXX LENDING CORPORATION (EP)
Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

MNLC, INC. represented by
IKP,
Complainant,

-versus-

NPC Case No. 19-528
(Formerly CID Case No. 19-G-528) *For: Violation of Section 13, in relation to Section 25(b) of the Data Privacy Act*

PXXX CORPORATION, RCM
and AD,
Respondent.

X-----X

DECISION

AGUIRRE, D.P.C.:

Before this Commission is a Complaint filed by Complainant MNLC, Inc. (MNLCI) against Respondents PXXX Corporation, RCCM, and AD, for an alleged violation of Republic Act No. 10173 (“Data Privacy Act”).

The Facts

Complainant MNLC, Inc. (MNLCI), represented by its Head Elder IKP, is a religious corporation composed mostly of Koreans and their families who practice Christianity in the Philippines. The religious officers and church members of the Complainant regularly gather during Sundays in its place of worship located at the 3rd Floor of MXXX Building being managed by Respondents. For the past nine (9) years, Complainant has owned all the units on the third floor of the building.¹

Sometime in March 2019, Respondent PXXX Corporation (Respondent Corporation) started implementing security measures in the building that required the Complainant to submit Philippine

¹ Records, pp. 1-7 dated 19 July 2019.

government-issued identification cards (IDs) of their church members.²

Respondent RCM, OIC-Administration Department and Marketing Manager of MNLCI, sent a letter to Complainant, through PMH, reminding the latter that the implementation of such security measures will start on 05 May 2019.³ He also sent a letter dated 06 May 2019 to all tenants and unit owners of the building informing them about the strict enforcement of “No ID, No Entry” policy in the building.⁴

On 16 May 2019, the Complainant, through its counsel, reached out to the Respondents to clarify matters concerning the implementation of said new policy. However, Complainant’s counsel and Respondents failed to meet and talk about the issues on the newly implemented security measures.⁵

On the same day, Respondent AD, Legal and Corporate External Affairs Head of MNLCI, sent a letter to Complainant reiterating the submission of original Philippine government-issued or any valid IDs from its church members on weekdays from 10:00A.M. to 12:00P.M. supposedly for validation purposes. Respondent also stated that the IDs provided by Complainant to its church members are denied and are not to be acknowledged by the security personnel of the building.⁶

Complainant sent more letters to the Respondents requesting for the basis in requiring the Complainant’s church members to submit their IDs. Specifically, the Complainant asked for the following: (1) a copy of the House Rules and Regulations of the Respondent Corporation; (2) reports of the crimes allegedly committed in the building; and (3) reports to the police concerning these crimes.⁷

RCM insisted in a letter dated 26 May 2019 that the church members of Complainant should submit their original passports, valid IDs bearing their Philippine residence addresses, and colored ID pictures for the production of their respective IDs to be used in

² Fact-Finding Report dated 14 October 2020, at p. 1.

³ *Supra* note 1, at 29 dated 30 April 2019.

⁴ *Id.*, at 30 dated 06 May 2019.

⁵ *Id.*, at 3.

⁶ *Id.*, at 33 to 35 dated 16 May 2019.

⁷ *Id.*, at 42 dated 26 May 2019.

entering the premises of the building.⁸ However, Complainant received another letter dated 31 May 2019 from the counsel of Respondent Corporation stating that the Complainant will be the one to provide the IDs for its members.⁹

Since the letter of RCM contradicts the statements in the letter of Respondent Corporation's counsel, Complainant tried to secure a copy of the building rules where the implemented security measures are based upon.¹⁰ Up to the filing of the Complaint, Complainant was unable to secure a copy of the same.¹¹

Upon the surrender of the passports and valid IDs of the Complainant's church members, employees of the Respondent Corporation took photos of their passports and valid IDs using their mobile phones.¹² The employees utilized these identification documents to produce another ID to be paid by the church members.¹³

Complainant's church members had no recourse but to submit their IDs containing their addresses and other personal data in order to avoid being harassed during frisking. Some of these members were forced to give their passports and IDs in order to practice their religion peacefully.¹⁴

Proceedings

The case was called for a summary hearing on 02 August 2019 for Complainant's application for a temporary ban where the parties were also required to submit the judicial affidavits of their witnesses in accordance with Sections 3 and 4 of A.M. No. 12-8-8- SC dated 4 September 2012 (Judicial Affidavit Rule).¹⁵

⁸ *Id.*, at 42 dated 26 May 2019.

⁹ *Id.*, at 40 to 41 dated 31 May 2019.

¹⁰ *Id.*, at 51 to 53 dated 03 June 2019.

¹¹ *Supra* note 2, at p. 2.

¹² *Supra* note 1, at 61.

¹³ *Id.*, at 5.

¹⁴ *Supra* note 2, at p. 2.

¹⁵ *Supra* note 1, at 64 and 65.

Respondent's counsel of record filed a Formal Entry of Appearance with Motion for Resetting and Extension of Time to File Responsive Pleading, asking for the resetting of the summary hearing to 16 August 2019 in order to have additional time to prepare the necessary pleadings for the summary hearing.¹⁶

Both parties and their respective counsels appeared during the scheduled summary hearing on 02 August 2019. However, Respondents' representative and counsel, by way of special appearance, only arrived after the hearing was already adjourned. Complainant submitted the judicial affidavits of its witnesses, namely, IKP, HCM, GSP, and HHJ. Considering that it was the first setting for the summary hearing and the reasons of the Respondents' counsel in the motion were reasonable, the motion for resetting was granted. The parties were ordered to appear on 09 and 16 August 2019.¹⁷

The counsels of both parties appeared for the summary hearing on 09 August 2019. The parties identified the witnesses to be presented for the summary hearing. Complainant's counsel manifested that there was a failure on its part to attach the Secretary's Certificate mentioned and to attach as Annex "A-1" in the judicial affidavit of its witness IKP due to inadvertence. Respondents were given a period of five (5) days to make the necessary changes on the judicial affidavits of their witnesses considering that they raised the issue of Complainant's lack of legal personality.¹⁸

Parties presented their testimonial and documentary evidence during the last scheduled summary hearing on 16 August 2019. Complainant presented its witnesses, namely, IKP, HCM, GSP, and HHJ. Meanwhile, Respondents presented their witness, AD. All the witnesses identified their judicial affidavits and adopted the same as their direct testimonies. The presentation of evidence for both parties was then terminated. Respondents were required to submit within four (4) days the building's rules and regulations and the incident reports mentioned during the presentation of witnesses. Respondents asked for five (5) days to submit written

¹⁶ *Id.*, at 66 to 68.

¹⁷ *Id.*, at 69, 157 and 158.

¹⁸ *Id.*, at 159, 179 and 180.

manifestation. Complainant also asked for the same period to file a comment to the manifestation of the Respondents.¹⁹

On 20 August 2019, Respondents filed a Memorandum as an answer to Complainant's application for a temporary ban on the processing of its church members' personal information. Respondents discussed the issues they believed were for resolution. First, Respondents submitted the issue that the Commission should rule on which legal authority between the Data Privacy Act and the NPC Rules of Procedure should be relied upon. Second, Respondents also raised the issue whether the alleged violation in the complaint is detrimental to national security and public interest. Third, Respondents questioned the legal personality of Complainant because it cannot be considered as data subject whose personal information is being processed. Lastly, Respondents claimed that Complainant failed to exhaust administrative remedies because the correspondences sent by the latter's counsel lacked the required special power of attorney or the Secretary's Certificate.²⁰

The Commission, through the investigating officer, issued an Order dated 11 September 2019 granting the temporary ban on the processing of personal data against Respondent Corporation. The ban covered: (1) the processing of personal data of Complainant's church members who have not yet provided their identification documents to Respondents for validation; and (2) the requirement for the use of Respondent corporation-issued IDs for the Complainant's church members who have already submitted their passports and IDs.²¹

In the same Order, Respondent Corporation was also directed to

(1) return to Complainant's church members all the copies of their passports and valid IDs; (2) delete or dispose all copies of the passports and valid IDs, digital or otherwise; and (3) to allow Complainant to provide IDs for their church members and officers bearing only their photos and English names. Further, Respondents were also required to submit an affidavit of compliance stating that the personal data of Complainant's church

¹⁹ *Supra* note 2, at p. 3.

²⁰ *Supra* note 1, at 244 to 253.

²¹ *Id.*, at 276 to 279.

members are no longer kept independently in any of Respondent Corporation's records.²²

On 25 September 2019, Respondents filed a Motion for Reconsideration of the Order imposing a temporary ban on its processing of personal data of Complainant's church members. The motion is premised on the ground that the complaint is not imbued with public interest supposedly because Complainant's church members belong to a particular and specified class composed mostly of foreign individuals. As such, according to Respondents, "they cannot be considered public in general for the protection against public interest to apply."²³ Respondents further argued that the temporary ban should not have been issued in the first place because the acts complained of are not considered imbued with public interest.²⁴

Respondents also filed an Addendum to the Motion for Reconsideration. The Addendum discussed that Complainant provided a clear, explicit and emphatic consent in using the Respondent corporation-issued ID.²⁵

On 11 October 2019, both parties and their counsels attended the discovery conference. Both parties manifested that they were not seeking any additional information or documents from each other. The Complainant and Respondents also filed a Manifestation and Counter-Manifestation, respectively, as to whether the directives in the Order dated 11 September 2019 were stayed by the Respondents' Motion for Reconsideration. Respondents were ordered to file their Responsive Comment to the complaint. Complainant was also ordered to file its reply to the comment.²⁶

On 28 October 2019, Respondents filed a Responsive Comment to the Complaint. They raised similar issues discussed in the memorandum they previously submitted. First, Respondents assailed the legal personality of Complainant as it is not considered a data subject because it is a corporate or artificial being only existing in contemplation of law. They pointed out that the individual members of Complainant have not executed any

²² *Ibid.*

²³ *Id.*, at 287.

²⁴ *Id.*, at 285 to 292.

²⁵ *Id.*, at 293 to 298.

²⁶ *Id.*, at 332 to 333.

authorization designating Complainant or any of its witnesses to represent them in the proceedings before the Commission. Second, Respondents also allege that Complainant failed to exhaust administrative remedies. They argue that, although there were several correspondences between Complainant's counsel, Abellera and Calica Law Offices, and Respondents, there was no special power of attorney or Secretary's Certificate showing that Complainant's counsel is also authorized to represent the individual members of Complainant. Third, Respondents claim that they have observed the general data privacy principles of transparency, legal purpose, and proportionality in processing the personal information of complainant's church members.²⁷

Respondents also filed an Addendum to the Responsive Comment. They added that processing the personal information of Complainant's church members was necessary to achieve lawful and non-commercial objectives considering that Respondent Corporation undertook heightened security measures in view of the crimes against properties committed to their tenants inside the building.²⁸

On 14 November 2019, Complainant manifested that the contents of Respondents' Comment are a mere rehash of their previous arguments as discussed during the proceedings on the issuance of a temporary ban. Complainant also prayed for indemnification, destruction of its church members' personal data processed by Respondents, and a recommendation to prosecute Respondents for violation of Section 13 in relation to Section 25(b) of the Data Privacy Act.²⁹

On 18 November 2019, the Commission issued a Resolution denying the Motion for Reconsideration of the Order dated 11 September 2019 issuing a temporary ban on processing against Respondents. The Commission also required Respondents to submit an affidavit of compliance showing that they have complied with the Commission's order to: (1) return to complainant's church members all the copies of their passports and valid IDs; (2) delete or dispose all copies of the passports and valid IDs, digital or otherwise; and (3) to allow complainant to

²⁷ *Id.*, at 335 to 351.

²⁸ *Id.*, at 352 to 359.

²⁹ *Id.*, at 361 to 362.

provide IDs for their church members and officers bearing only their photos and English names.³⁰

Thereafter, Complainant filed a Manifestation and Motion dated 03 February 2020 stating that Respondent Corporation continues to require Complainant to use only the Respondent Corporation- issued IDs to gain entrance to the building, and claimed that such act was in defiance of this Commission's Order dated 11 September 2019 and Resolution dated 18 November 2019. Complainant also manifested that Respondent has not yet submitted an affidavit of compliance.

Given this, Respondents were ordered to show cause and explain why it should not be held in contempt for disregarding this Commission's Order.³¹

On 27 February 2020, Respondents filed a Manifestation and Motion (with notice of change of office address). Respondents moved that the pending show cause Order's resolution be deferred considering that the parties were on the verge of signing a compromise agreement.³²

This Commission denied the Motion seeking to defer its compliance with the show cause order explaining that the possible signing of a compromise agreement and the issue of failing to comply with this Commission's Order are completely different matters. Respondents were given a final opportunity to submit their explanation to the show cause order.³³

On 03 June 2020, Complainant manifested that it sent a letter dated 06 March 2020 to the Respondents, terminating all efforts for settlement. As such, it urged the Commission to seek Respondents' compliance with the Orders dated 11 September 2019 and 18 November 2019.³⁴

On 09 June 2020, the Respondents filed their Compliance *ad Cautelam*. In the Joint Affidavit of Compliance executed by Respondents AD and RCM, they claim that Respondent Corporation had ceased from processing the personal information

³⁰ *Id.*, at 369 to 376.

³¹ Order dated 14 February 2020.

³² *Supra* note 2, at pp. 5-6.

³³ Order dated 03 March 2020.

³⁴ Manifestation dated 09 March 2020.

of Complainant's church members by stopping the issuance of IDs to them. They also mentioned that all copies of passports, other valid IDs and personal data digitally stored or otherwise from Complainant's church members were completely deleted and disposed. They also stated that the Respondent Corporation no longer required Complainant's church members to use the Respondent Corporation's-issued IDs.³⁵

On 17 August 2020, Complainant filed a Motion to Resolve asking that the case already be considered submitted for resolution.³⁶

Issues

The issues in this case are:

1. Whether this Commission validly acquired jurisdiction over this case;
2. Whether the Complaint should be dismissed on the ground of non-exhaustion of remedies under NPC Circular 16-04;
3. Whether Respondent obtained valid consent from Complainant to collect and process personal and sensitive personal information from their members;
4. Whether Respondent had a legitimate interest to collect and process personal and sensitive personal information from Complainant's members;
5. Whether Respondent complied with the principle of proportionality in collecting and processing personal and sensitive personal information from Complainant's members;
6. Whether Respondent is liable for unauthorized processing of personal and sensitive personal information of Complainant's members;
7. Whether the Complainant is entitled to damages; and
8. Whether the Compliance Ad Cautelam submitted by Respondents is sufficient in relation to the Order dated 03 March 2020.

Discussion

This Commission validly acquired jurisdiction over this case

³⁵ Joint Affidavit of Compliance dated 08 June 2020.

³⁶ Motion to Resolve dated 26 June 2020.

Respondents argue that this Commission has not validly acquired jurisdiction over this case because Complainant has no personality to file the complaint supposedly because the real party in interest, the individual members of MNLCI, “have not executed any authorization authorizing MNLC or IKP, GSP and HCM to represent them in this proceedings (sic).”³⁷ On the basis of this, Respondents further argue that “IKP, GSP and HCM are testifying as mere representatives/witnesses and not as complainants. It is therefore submitted that, for this Commission to have jurisdiction, a formal complaint must be filed by a data subject.”³⁸

The important consideration in determining whether this Commission validly acquired jurisdiction over a case is whether the allegations, assuming they were true, show that a privacy violation was committed against a data subject.

In this case, IKP, the Head Elder of MNLC, Inc., alleged in his Complaint-Affidavit that Respondents committed acts violative of his privacy rights. The fact that he and the other church members, who executed affidavits in support of the Complaint-Affidavit, also sought to represent the other members of MNLCI does not change their status as affected data subjects.

Whether IKP and the others were testifying as mere representatives or witnesses and not as complainants or whether each and every single member of MNLCI should have issued individual authorizations is of no moment. Strict adherence to the technicalities of NPC Circular No. 16-04 or the NPC Rules of Procedure (“Rules”) may be dispensed with following Section 33 of the same Rules which provide for a liberal interpretation “in a manner mindful of the rights and interests of the person about whom personal data is processed.”³⁹ As the Supreme Court held in *Heirs of Amada Zaulda v. Zaulda*,⁴⁰ technicalities may be dispensed with if it impedes the attainment of justice, thus:

What should guide judicial action is the principle that a party- litigant should be given the fullest opportunity to establish the merits of his complaint or defense rather than for him to lose

³⁷ Memorandum dated 20 August 2019.

³⁸ *Id.*

³⁹ *FGP v. Maersk*, NPC Case No. 18-038, 21 May 2020.

⁴⁰ G.R. No. 201234, March 17, 2014.

life, liberty, honor, or property on technicalities. The rules of procedure should be viewed as mere tools designed to facilitate the attainment of justice. Their strict and rigid application, which would result in technicalities that tend to frustrate rather than promote substantial justice, must always be eschewed.⁴¹

As to the supposed privacy violations, it should also be noted that Respondents themselves admitted that the processing at issue in this case involved the personal data of all the members of MNLCI. In their Addendum to the Motion for Reconsideration, Respondents argue that the emails of IKP and the other members of MNLCI supposedly show that they can validly process the personal data of the entire MNLCI congregation on the basis of consent, thus:

1. MNLC (MNLC) by means of electronic message or Email dated June 26, 2019 personally and knowledgeably notified and confirmed herein respondents that MNLC's (sic) **including all MNLCI members pastors and elders** will use MXXX ID thus **manifesting a clear, explicit and emphatic consent of the entire congregation...**
2. ... Also, as it can be garnered from the letter is unequivocal consent to **scan MNLCI Members government issued identification...**⁴²

Having admitted the allegations in the Complaint relating to the processing of the personal data of all the members of MNLCI's congregation, albeit supposedly on the basis of consent, Respondents cannot now claim that this Commission did not acquire jurisdiction. The determination of the validity of the processing carried out by Respondents, including whether the basis relied upon to process is proper, is precisely within the mandate of this Commission.

In addition, Respondents mistakenly assume that the Commission can only acquire jurisdiction on a matter affecting any personal information if a formal complaint is filed by a data subject. Respondents fail to consider, however, that the Commission is fully empowered to investigate, on its own initiative,

⁴¹ *Ibid.*

⁴² *Supra* note 1, at 311-312. Emphasis supplied.

circumstances surrounding a possibly serious privacy violation or personal data breach.⁴³ The allegations in the Complaint raise potentially serious privacy violations that require this Commission to take such further action on the matter as may be necessary, after having been informed of the same.

The Complaint should not be dismissed on the basis of non-exhaustion of remedies

Respondents claim that Complainant failed to exhaust administrative remedies because the correspondences sent by the latter's counsel lacked the required special power of attorney or the Secretary's Certificate.⁴⁴

NPC Circular No. 16-04 provide for the rule on exhaustion of remedies, thus:

Section 4. Exhaustion of remedies. No complaint shall be entertained unless:

xxx

- a. the complainant has informed, in writing, the personal information controller or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same;⁴⁵

As this Commission has ruled in a previous Decision,⁴⁶ this rule was intended to prevent a deluge of vexatious complaints from those who waited for a long period of time to pass before deciding to lodge a complaint with the NPC, unduly clogging its dockets. Notably, however, the same Section provides that the Commission has the discretion to waive any of the requirements upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to Complainant.

⁴³ *Supra* note 2, at p. 6.

⁴⁴ *Supra*, note 20.

⁴⁵ Section 4, Rule II, NPC Circular 16-04. Dated 15 December 2016.

⁴⁶ NPC Case No. 18-083, dated 21 May 2020.

That Decision cited the Supreme Court in stating thus:

The Court has allowed some meritorious cases to proceed despite inherent procedural defects and lapses. This is in keeping with the principle that rules of procedure are mere tools designed to facilitate the attainment of justice and that strict and rigid application of rules which would result in technicalities that tend to frustrate rather than promote substantial justice must always be avoided. It is a far better and more prudent course of action for the court to excuse a technical lapse and afford the parties a review of the case to attain the ends of justice, rather than dispose of the case on technicality and cause grave injustice to the parties, giving a false impression of speedy disposal of cases while actually resulting in more delay, if not a miscarriage of justice.⁴⁷

The Rules include, as a ground for the Commission to waive any of the requirements, instances when the complaint involves a serious violation or breach of the Data Privacy Act. In this case, the Complaint-Affidavit contains allegations such as:

23. The series of acts of harassment by PXXX to force MNLCI's members to comply and submit their passports and ID's is a violation of Section 13. There could never be consent if the MNLCI member is harassed or, at the very least, inconvenienced by long lines or body frisking to force him to submit his passport, which would then be photographed by PXXX. Coerced consent is no consent at all.

This serves as sufficient basis for the Commission to waive the technicalities cited by Respondents in the absence of a Special Power of Attorney or Secretary's Certificate, which they claim to be their basis for not entertaining the letters.

*Respondent did not obtain
valid consent from
Complainant to collect and
process personal and
sensitive*

⁴⁷ PNB v. Court of Appeals, G.R. No. 218901, 15 February 2017.

*personal information from
their members*

The Complaint pertains to Respondent Corporation's requirement that Complainant's church members submit their original passports, valid government IDs bearing their residence addresses in the Philippines, and colored ID pictures. The employees of Respondent Corporation then took photos of the church members' passports and valid IDs using their personal mobile phones.⁴⁸ The employees used those identification documents to produce another ID to be paid for by Complainant's church members.⁴⁹ The IDs issued by Respondent Corporation, with the bearers' addresses prominently displayed in front,⁵⁰ would have to be used by the church members in entering the building.⁵¹

The passports and government-issued IDs of the Complainant's church members contain both personal information and sensitive personal information as defined under the Data Privacy Act.⁵²

Under the Data Privacy Act, the processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

- (a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
- (b) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
- (c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

⁴⁸ *Supra* note 1, at 61.

⁴⁹ *Id.*, at 5.

⁵⁰ *Id.*, at 145.

⁵¹ *Id.*, at 42 dated 26 May 2019.

⁵² Data Privacy Act, §3.

(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing;

(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.”⁵³

Respondents anchor the processing of such information on the supposed consent given by Complainant’s church members, through its church elders, and on the legitimate interest of maintaining security inside the building.

In both their Responsive Comment⁵⁴ and Addendum to the Motion for Reconsideration,⁵⁵ Respondents relied on the e-mail dated 25 June 2019 from one of Complainant’s church elders, PMH, to show that consent was given to allow them to process the information of all the church members:

To: RCM
OIC-Admin. Dept

Cc: AD

Re: Our MNLC willing to use your I.D.

Dear Gentlemen,

We are willing to use the I.D. cards that are provided by you. We request you to increase the number of manpower on Sunday to facilitate smoother distribution of ID cards as large number of people gather at the same time.

⁵³ *Id.*, §13.

⁵⁴ *Supra* note 1, at 341.

⁵⁵ *Id.*, at 294-295

Our Church will cover the extra cost of the reinforcement of manpower on Sunday (June 30th).

And, we would like to request you to set up separate table for those people who were not able to scan I.D. because they could not attend the worship service three weeks ago.

We hope to continue maintenance good relationship your PXXX Corp.

Thanks and very truly your's

Mr. PMH
Head, Admin of MNC⁵⁶

Further, Respondents cited another email dated 26 June 2019 from IKP to Respondent RCM. They claimed that this email is the affirmation of Complainant's willingness to use Respondent Corporation-issued IDs. The said e-mail states:

Hi RCM!

This is Elder IKP of MNLC and Good morning !

Regarding MXXX ID,

Our MNLC's Chief Administration Officer PMH already submitted yesterday our letter to confirm to use MXXX ID from coming Sunday (June/30~~~)

And happy to solve this hectic pending issue each other under the love of same God and Jesus Christ.⁵⁷

The Data Privacy Act provides that the consent of a data subject must be a "freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her... It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so."⁵⁸ The Data Privacy Act also requires that "[c]onsent shall be evidenced by written, electronic or recorded means."⁵⁹

⁵⁶ *Id.*, at. 341 and 348.

⁵⁷ *Id.*, at 340 and 347.

⁵⁸ Data Privacy Act, §3(b).

⁵⁹ *Id.*

In determining whether consent was freely given, the data subject must be given a real choice where there is no risk of deception, intimidation, coercion or significant negative consequences if he or she does not consent. If the consequences of giving consent undermine the individual's freedom of choice, consent would not be free.⁶⁰ For instance, a “bundled” consent will generally not suffice as the data subject is not empowered to make a true choice.⁶¹

The e-mails quoted in both the Responsive Comment⁶² and Addendum to the Motion for Reconsideration⁶³ of Respondents, supposedly an indication of consent as a lawful basis for processing, must be contextualized. It must be noted that said e-mails were sent after several events have already transpired involving Complainants' church members and Respondents. Two

(2) respected church members were banned from entering the premises and exercising their religion, an event that frightened most of the church members.⁶⁴ Guard dogs were posted at the entrance of the building. Churchgoers were delayed for over an hour and a half before they can enter the building leaving most seats still vacant by the time their worship started.⁶⁵ These allegations in the Complaint-Affidavit remain to be unrefuted by Respondents, thus:

On 12 May 2019, tempers flared resulting in exchange of words between MNLCI members and PXXX's guards. In a letter dated 15 May 2019, PXXX banned two (2) respected church members, MH and LSB, from entering the Building from 14 to 19 May 2019.

Guard dogs are posted at the entrance and churchgoers are delayed for as long as an hour and a half before they can enter the Building. They attach pictures of the long line at the entrance endured by MNLCI's members on 23 June 2019, thereby leaving mostly vacant seats by 11:00AM, which is the start of our time of worship during Sundays. Such form of harassment was implemented by PXXX by significantly reducing the entrance line to one, intended to force churchgoers to surrender their passports and valid ID's for

⁶⁰ National Privacy Commission. Advisory Opinion 2019-034 Re: Consent and Its Withdrawal for Employment Purposes. 02 September 2019, *citing* European Commission, Article 29, Data Protection Working Party, Opinion 15/2011.

⁶¹ National Privacy Commission. Advisory Opinion No. 2018-013 Re: Privacy Policy and Consent of Data Subjects. 18 April 2018.

⁶² *Supra* note 1, at 341.

⁶³ *Id.*, at 294-295.

⁶⁴ *Id.*, at 73.

⁶⁵ *Id.*, at 3.

processing by PXXX's employees, supposedly for the production of PXXX-issued ID's that shall be paid for by MNLCI's members.⁶⁶

Clearly, the supposed consent of Complainant's church members relied upon by Respondents cannot be considered freely given as required by the Data Privacy Act. An imbalance already exists between the controller and the data subject. Respondents not only controlled the MNLC members' access to their place of worship, which they describe as the "really most important and worthy matter in their whole life,"⁶⁷ but they have already demonstrated their willingness to assert this control by banning church members and posting guard dogs.

Taking all the circumstances of this case into consideration, it can be seen that the e-mails from church elders of complainants relied upon by Respondents were written in light of the growing tension between Respondents or the personal information controller on the one hand, and Complainant's church members or the data subjects on the other. In fact, in the email of IKP dated 28 June 2019, cited by Respondents in their Motion for Reconsideration, he categorically stated that their use of the MXXX ID was purely for the purpose of smooth and quick entrance process for normal and spiritual worship, especially for the church members who did not submit yet their copies of Government IDs.⁶⁸ From this it can be seen that the supposed consent was given only so that the church members can attend worship services peacefully. Given all the pressure exerted on them, including being forced to choose between giving up their privacy or the exercise of their religion, it cannot be said that the church members were empowered to make a true and free choice.⁶⁹ Clearly, this kind of consent is invalid.

This Commission also notes that Complainant, in its letter to Respondents dated 04 June 2019, already categorically stated that the latter's act in collecting passports, residential data, and photographs from Complainant's church members was not voluntary and that while some of their members may have submitted these documents it was just for the purpose of gaining access to their place of worship.⁷⁰ This not only reinforces the fact

⁶⁶ *Id.*, at 3 to 5.

⁶⁷ *Supra* note 2, at p. 10.

⁶⁸ *Supra* note 1, at 343 and 350.

⁶⁹ National Privacy Commission. NPC Advisory Opinion 2018-063 Re: Review of Consent Form. 23 October 2018.

⁷⁰ *Supra* note 1, at 44.

that no consent was validly given by Complainant's church members, but more importantly, Respondents were aware of such fact.

This awareness is borne out in the cross-examination of Respondent AD where he admitted that no written consent was obtained from Complainant's church members prior, during or after the processing of their personal data. Clearly, the supposed consent relied upon by Respondents is entirely based on the emails of some Complainant's members and not the written, electronic, or recorded consent of the individual church members as required by the Data Privacy Act.

Given all these, Respondents processed the personal data of the Complainant's church members without the consent of the data subjects as defined under the Data Privacy Act.

This Commission also notes the inconsistent manner in which Respondents deal with MNLCI and its representatives – questioning the authority of Complainant's representatives to file this case for the entire congregation while relying on practically the same representatives and claiming that they consented for everyone else. Respondents cannot have it both ways.

Respondent cannot rely on legitimate interest to collect and process personal and sensitive personal information from Complainant's members

Previously, Respondent Corporation only required that the church members of the Complainant wear insignias or stickers during Sundays.⁷¹ Thereafter, Respondents required the Complainant to produce IDs for their church members to be used in entering the building every Sunday.⁷² Witnesses for Complainant testified that MNLCI produced IDs for their church members for their worship

⁷¹ *Id.*, at 29.

⁷² *Id.*, at 30.

days within the building.⁷³ Respondent AD admitted this fact in his 16 May 2019 letter to Complainants where he said:

[W]e appreciate that the MNLC, thorough the indomitable will and persistence of PMH, have at long last abided by the requirement of providing ID's to the members of MNLC, however after much review of your Identification Cards, our security and safety consultants have observed that the archetype of MNLC Identification Cards are without a doubt susceptible to security breach, which may include but not limited to, meagre (sic) identification control system and counterfeit.⁷⁴

During the summary hearings, however, Respondent AD, while acknowledging that Complainant already provided IDs to its members, gave a different reason why Respondents rejected these IDs. He explained that while the MNLC-issued IDs showed both the Korean and English names of the church members, the Korean characters were bigger and more prominent. He stated that this was a security threat to the other tenants of the building, because only the church members can read and understand the Korean characters.

Despite their compliance with Respondents' requirements of producing the IDs for its church members, for the reasons stated above these were disallowed and Complainant's church members were required to submit their passports and valid IDs bearing their Philippine residence address in order to enter the building for their Sunday worship.⁷⁵ Respondents' employees took photos of the passport and IDs of Complainant's church members using their personal mobile phones and used the gathered personal data to produce and issue its own ID for which it charged a fee.

Respondents justified the processing of these personal data supposedly for purposes of their legitimate interest to enforce building security rules and regulations in light of the reported recent incidents. The relevant portions of the Respondents' buildings and regulations with regard to the "No ID, No Entry" policy provide:

3.4 Office visitors and clients maybe allowed entry when properly identified and acknowledged by person/s to be visited and prior

⁷³ *Id.*, at 76.

⁷⁴ *Id.*, at 34.

processing by building security. Person/s not properly identified or owned by an authorization from unit owners or tenants shall not be allowed entry beyond regular hours.

Office visitors and clients must present and deposit a valid Identification Card with their picture, in exchange for a visitor's card. Valid IDs shall be current issues of the following:

3.4.1 Passport

3.4.2 Driver's license

3.4.3 PRC ID

3.4.5 Voter's ID, TIN, SSS

3.5 Visitors shall complete the registration form with information regarding their visit and shall be provided a building pass for security purposes. It is understood that PXXX Corp. protects the data and information collected through the registration form using technical, physical and administrative security measures to reduce the risk of loss, misuse, unauthorized access, disclosure or modification of the given information and will only retain the information collected as long as it is reasonably needed for each purpose.⁷⁶

Despite Complainant's compliance in producing the IDs for its church members and the clarifications sought from Respondent to produce its own IDs, Complainant was unable to prevent the copying of their church members' identification documents and the production of IDs displaying their Philippine residence.⁷⁷ These were suddenly required in order to enter the building for their Sunday worship. In disallowing the use of Complainant- issued IDs, Respondents decided to provide IDs for a fee after gathering the identification documents from Complainant's church members.

Respondents argued that these strengthened security measures are necessary to protect the safety, health, and life of the church members following several incidents of breaking and entering, theft, vandalism, and other occurrences that causes fright to the tenants.⁷⁸

⁷⁶ *Id.*, at 190 and 191.

⁷⁷ *Id.*, at 136.

⁷⁸ *Id.*, at 343.

While the security of the premises and tenants of the building is a legitimate interest, the fact remains that these stricter security measures are only applied to Complainant's church members and not to the other tenants of the building.

There is nothing on record that would remotely show that the church members were suspected to be behind any of the security incidents mentioned by Respondents. In one incident report, a church member of the Complainant was even the one who witnessed a certain individual posting decals on the building premises.⁷⁹ In another incident where fire hose nozzles were stolen, a non-resident was identified as a suspect.⁸⁰

Respondent did not observe the principle of proportionality in collecting and processing personal and sensitive personal information from Complainant's members

Respondents insisted that the collection and processing of Complainant's church members personal data from passports and government-issued IDs is proportional to their legitimate interest to ensure safety and order within the premises of the building.⁸¹ However, the principle of proportionality requires that the processing of personal information must be relevant to, and must not exceed, the declared purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.⁸² Hence, proportionality is met when the processing is the least intrusive measure to achieve its purported aims.⁸³

⁷⁹ *Id.*, at 219-220.

⁸⁰ *Id.*, at 239-240.

⁸¹ *Id.*, at 344.

⁸² Implementing Rules and Regulations (IRR) of R.A. 10173. §18(c).

⁸³ ICCPR, Art. 19; General Comment 34, par. 34; UNHRC, 'General Comment No. 22: Article 18 (Freedom of Thought, Conscience or Religion)', (30 July 1993) UN Doc CCPR/c/21/Rev.1/Add.4 ('General Comment 22'), par. 8; Shelton v. Tucker, 364 US 479

In this case, the requirement of submission of passports, government-issued IDs, and colored ID pictures is not the least intrusive means to achieve the desired purpose. The IDs issued by Complainant to its church members should suffice as an exhibit of the authorization as required under the building rules.⁸⁴

This fact was recognized by Respondents when they alleged in both their Motion for Reconsideration⁸⁵ and Responsive Comment⁸⁶ that they have been constantly reminding Complainant to provide even just an emblem, insignia or even as simple as stickers, where security guards on duty can positively identify their church members. They claim, however, that the security measures they implemented as against Complainant and its members were justified “because of MNLC’s delay and unjustified refusal.”⁸⁷

Respondents seem to have forgotten their previous statements and admissions in making this claim. As discussed above, Respondent AD acknowledged in his 16 May 2019 letter and during the summary hearing that Complainants already issued ID cards to its members. In both those instances, Respondent AD gave inconsistent reasons why Respondents disallowed the ID cards issued by Complainants: susceptible to security breach on the one hand, and the Korean names were bigger and prominently than the English names on the other. Apparently, Respondents’ claim that all they are asking Complainant to provide is “just an emblem, insignia or even as simple as stickers so that the security guards on duty can identify their church members,”⁸⁸ is clearly not true.

Setting aside for a moment the validity and veracity of those reasons, including whether Respondents have the necessary security measures and systems in place such that their own issued IDs are not susceptible to the same security issues they claim in relation to the IDs issued by Complainant, their previous assertions belie Respondents’ current claim on the necessity and proportionality of the measures it adopted.

(1960); *Thorgeirson v. Iceland* App No. 13778/88 (ECTHR, 25 June 1992).

⁸⁴ *Supra* note 1, at 190 and 191.

⁸⁵ *Id.*, at 291.

⁸⁶ *Id.*, at 344.

⁸⁷ *Ibid.*

⁸⁸ *Ibid.*

The fact that none of Respondents' alleged reasons for disallowing the IDs Complainant issued to its members find basis in any of its documented policies also argues against the proportionality of these measures. As this Commission noted in its Resolution denying Respondents' Motion for Reconsideration:

In determining what information can be collected for and displayed on the ID card, the respondents must consider the purpose for such ID. The above-cited House Rules and Regulations signifies that the ID is an exhibit of such authorization to enter from the building tenant. There is no documented policy which declares that the ID card should serve other purposes, nor is there anything that requires the tenant to be supported by 201 file records or to have specific security measures.⁸⁹

The availability of a far less intrusive measure demonstrates that the measures employed by Respondents are disproportionate to the aim they seek to achieve. Inasmuch as Respondents recognized the issued IDs of the other tenants in the building, the same standard should have been applied to the church members of Complainant. The subject measure cannot be considered proportionate to the claim of increased security in the premises of MXXX Building.

This is all the more true considering Respondent AD's letter to the Bureau of Immigration (BI) and copy-furnishing the Embassy of the Republic of Korea, the Department of Foreign Affairs, and the Mayor of the City of Makati, dated 24 June 2019. The letter stated thus:

[W]e ardently request your office to look into this matter as there might be Korean Nationals members of the MNLC who have expired VISA or undesirable aliens or fugitives from other countries.

xxx

Thank you very much and in the highest interest of justice
and
peace, we fervently seek your office's intervention
on the

⁸⁹ *Id.*, at. 374-375.

legality and validity of the immigration and alien admission of the members, pastors and elders of the MNLC.⁹⁰

By no stretch of reasoning can the involvement of the BI be considered as necessary to fulfill the declared purpose of security measures in the building. The request for the BI's intervention in investigating the validity of the Korean nationals' visas only strengthens the conclusion that the application of strict security measures were specifically targeted to the Complainants' members and hence excessive to the declared purpose of building security measures.

The previous Order⁹¹ of this Commission granting the request for Temporary Ban discussed this matter, thus:

PXXX cites security measures as the declared purpose for requiring the validation of passports and government-issued IDs of MNLCI's church members. However, **the fact that the stricter security measures applied only to MNLCI's church members, and not the other tenants of the building, cannot be justified as proportional.** The recognition of validly-issued MNLCI IDs should be considered as sufficient to meet the authorization requirements for entrance to the building, in as much as PXXX recognizes the company-issued IDs of its other tenants. The negative effects that these security measures have caused cannot be overlooked.⁹²

The Compliance ad Cautelam is not sufficient

At the outset, the Commission wishes to clarify a misconception by the Respondent Corporation with regard to the public's compliance to the Orders issued by the Commission. In their Counter-Manifestation dated 03 October 2019, they state:

6. [C]onsidering that the filing of a motion for reconsideration is regarded as part of "due process of law" respondents cannot be barred from filing the same. To proceed with the implementation of the Order dated 11 September 2019 notwithstanding the timely filing of the motion for reconsideration would be tantamount to disregarding respondent's right to due process of

⁹⁰ *Id.*, at 62-63.

⁹¹ Order dated 11 September 2019.

⁹² Emphasis supplied.

law as it would render naught the latter's right to question the propriety of the assailed order of this Honorable Commission.⁹³

Aside from the lack of support in law or in regulations, Respondents failed to consider that the NPC Rules of Procedure clearly indicate the period of effectivity of a Temporary Ban on Processing Personal Data, thus:

SECTION 19. Temporary Ban on Processing Personal Data – At the commencement of the complaint or at any time before the decision of the National Privacy Commission becomes final, a complainant or any proper party may have the National Privacy Commission, acting through the investigating officer, impose a temporary ban on the processing of personal data, if on the basis of the evidence on record, such ban is necessary in order to preserve the rights of the complainant or to protect national security or public interest...

XXX

d. If so issued, the temporary ban on processing personal data shall remain in effect until the final resolution of the case or upon lawful orders of the Commission or lawful authority.⁹⁴

In the Respondents' eventual submission of its Compliance *Ad Cautelam*, the Commission notes that other than bare allegations, Respondents failed to provide proof that they no longer require the Complainant's members to use PXXX-issued IDs. Notably, two (2) months after the Commission's denial of the Motion for Reconsideration of the Respondents, Complainants filed a Manifestation that Respondents still refused to allow Complainant's members to enter with MNLCI-issued IDs.⁹⁵

In an e-mail to the Commission on 06 November 2020, Mr. GSP, a member and deacon of MNLCI, detailed the security measures implemented by PXXX in relation to Complainant's members:

NPC has requested to confirm, if the Peaceland (sic) (Building owner; "PL") do not require PL issued ID for entrance?

⁹³ *Supra* note 1 at 327-329.

⁹⁴ Section 19, NPC Circular No. 16-04. Rules of Procedure of the National Privacy Commission. Dated 15 December 2016. Emphasis supplied.

⁹⁵ Manifestation and Motion by Complainant, dated 3 February 2020.

1. Officially, PL do not make it (*sic*) a requirement to present PL ID.

PL, however, before lock-down, have allowed those with PL ID to enter without difficulties.

Those without PL ID, had to (1) queue (*sic*) up in long lines, (2) present PH gov't issued ID (any other ID denied), (3) register all names of family, just to enter for worship services.

This practically made it impossible for those who have no PH gov't ID at hand.

More important, PL did not apply such strict restrictions to those of other tenants on other floors, as they simply entered with their own tenant IDs.

With no grounds, PL did not allow MNLCI ID. It is even more unjust, as MNLCI is owner of our two floors, and we are not even tenants.⁹⁶

While the Respondent Corporation no longer officially requires the Complainant's members to use their building ID, the Commission finds that their practices of requiring additional documents and information only from Complainant's members and not its other tenants effectively continue to defy the Order of the Commission dated 11 September 2019⁹⁷ which: 1) imposed a temporary ban on the processing of the personal data of Complainant's church members who have not yet provided their identification documents to Respondents, and 2) required Respondent to allow Complainant to provide IDs for their church members and officers bearing only their photos and English names.

Respondents are liable for unauthorized processing of personal and sensitive personal information of Complainant's members

⁹⁶ Email dated 6 November 2020 by GSP.

⁹⁷ *Supra* note 21.

In determining whether a violation of Section 25(b) of the Data Privacy Act occurred, three elements must be established with substantial evidence:

1. The accused processed the information of the data subject;
2. The information processed was personal information or sensitive personal information;
3. That the processing was done without the consent of the data subject, or without being authorized under this act or any existing law.⁹⁸

As to the first element, the Data Privacy Act provides a definition of processing as “any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.”⁹⁹ Simply stated, processing refers to any use of personal data at any stage of the data life cycle.

In this case, it has been established that Respondents processed the information of Complainant’s members through the required collection of original passports, valid IDs bearing their Philippine residence addresses, and colored ID pictures, which were later on stored.

As to the second element, the information subject of this case is sensitive personal information. Under the Data Privacy Act, sensitive personal information refers to information:

1. About an individual’s **race, ethnic origin**, marital status, **age**, color, and religious, philosophical or political affiliations;
2. About an individual’s health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

⁹⁸ NPC Case No. 17-018, Decision dated 15 July 2019.

⁹⁹ Data Privacy Act, §3(j).

3. **Issued by government agencies** peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4. Specifically established by an executive order or an act of Congress to be kept classified.¹⁰⁰

Considering the collection of government IDs and passports, the exposure of the Complaint's members race, ethnic origin, age, and government-issued identifiers is inevitable.

With regard to the third element, the Commission has extensively discussed that the Respondents failed to present any valid criteria for the lawful processing of the church members' personal data. The Commission has also found an inability by Respondent to show adherence with the data privacy principles of transparency, legitimacy, and proportionality.

Following this, the Commission finds that Respondents' processing of the personal information of the Complainant's members meets all the elements of Section 25(b) of the Data Privacy Act.

Considering that Respondent PXXX is a Corporation, Section 34 of the Data Privacy Act applies, thus:

Section 34. Extent of Liability. If the offender is a corporation, partnership, or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime.

The Commission notes the direct involvement of Respondent AD, as the Head of the Legal & Corporate External Affairs Department, and Respondent RCM, as the Office in Charge of the Administration Department, in the Respondent Corporation's collection of sensitive personal information from Complainant's members. The Commission also notes the communications made by Complainant's counsel to the Respondents' Board of Directors

¹⁰⁰ *Id.*, at § 3(l). Emphasis supplied.

that repeatedly raised this concern. Despite being apprised of the issues, the Board of Directors nevertheless allowed such unauthorized practices to persist.

In addition, the actions of Respondents in continuing to process the information of Complainant's church members in a manner inconsistent with how it treats its other tenants in defiance of this Commission's Order demonstrates not just gross negligence but bad faith on their part.

Complainant's members are entitled to damages

The Data Privacy Act provides that every data subject has the right to be indemnified for "any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information."¹⁰¹ Indeed, it is part of the Commission's mandate to award indemnity on matters affecting any personal information.¹⁰²

It is worth noting that the Data Privacy Act does not require actual or monetary damages for data subjects to exercise the right to damages. As provided in the law, the consequences of processing inaccurate information is enough for the right to arise.¹⁰³

The Data Privacy Act provides that restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.¹⁰⁴ The relevant provision in this Code states:

Art. 2221. Nominal damages are adjudicated in order that a right of the plaintiff, which has been violated or invaded by the defendant, may be vindicated or recognized, and not for the purpose of indemnifying the plaintiff for any loss suffered by him.

¹⁰¹ *Id.*, at §16(f).

¹⁰² *Id.*, at §7(b).

¹⁰³ *Ibid.*

¹⁰⁴ *Id.*, §37.

The Data Privacy Act gives individuals the right to receive indemnification from personal information controllers and personal information processors for both material and non-material damages.¹⁰⁵ The Supreme Court has also clarified that no actual present loss is required to warrant the award of nominal damages, thus:

Nominal damages are recoverable where a legal right is technically violated and must be vindicated against an invasion that has produced no actual present loss of any kind or where there has been a breach of contract and no substantial injury or actual damages whatsoever have been or can be shown.¹⁰⁶

Pursuant to the New Civil Code and following the aforementioned findings that Respondents not only unlawfully processed the subject sensitive personal information but also failed to observe the general privacy principle of proportionality, the Commission finds that the award of nominal damages to Complainant is warranted.

WHEREFORE, all premises considered, this Commission hereby:

1. **FINDS** that Respondent AD, Respondent RCM, and the Board of Directors of PXXX Corporation, namely EPA, CAS, RCM, HAB, and JRB, as its responsible officers, have violated Section 25(b) of the Data Privacy Act;
2. **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice, recommending the prosecution of respondents for the crime of Unauthorized Processing under Section 25 of the Data Privacy Act, and for its further actions;
3. **AWARDS** damages, in the amount of P1,000.00, to each member of Complainant MNLC as of the date of filing of the Complaint Affidavit on 23 July 2019 for Respondent's

¹⁰⁵ See, Handbook on European Data Protection Law, p. 246.

¹⁰⁶ Seven Brothers Shipping Corporation v. DMC-Construction Resources, Inc. G.R. No. 193914. November 26 2014.

unlawful collection of their sensitive personal information, pursuant to Section 16 (f) of the Data Privacy Act; and

4. **ORDERS** the submission of proof of compliance by Respondents' with abovementioned award within thirty (30) days of receipt of this Decision.

SO ORDERED.

Pasay City, Philippines;

29 October 2020.

Sgd.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

WE CONCUR:

Sgd.

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

Sgd.

JOHN HENRY D. NAGA

Deputy Privacy Commissioner

COPY FURNISHED:

AAC LAW OFFICES

Counsel for the Complainant

MP LAW OFFICE

Counsel for the Respondents

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

AMP

Complainant,

-versus-

NPC Case No. 19-621

(Formerly CID Case No. 19-G-621)

*For: Violation of the Data
Privac Act of 2012*

**HXXX LENDING TECHNOLOGY,
INC (CM)**

Respondent.

X-----X

DECISION

AGUIRRE, D.P.C.:

Before this Commission is a Complaint filed by AMP (Complainant) against Creditable Lending Corporation (Respondent) for a violation of the Data Privacy Act of 2012 (DPA).

Facts of the Case

Complainant, using the Complaints-Assisted Form, described his complaint as “*threatening or all contacts will receive message (sic) regarding unsettled amount.*”¹ He stated that his credibility was affected and that all his co-workers, family members complained about the calls and text messages they have received.² He alleges that he was humiliated and embarrassed.³ Complainant indicated that he is seeking a temporary ban on Respondent’s processing.⁴

The parties were ordered to appear for discovery conference on 13 September 2019.⁵ Both parties failed to appear on the said date, causing the discovery conference to be reset on 12 December 2019.⁶

¹ Complaints-Assisted Form received on 26 July 2019.

² *Ibid.*

³ *Ibid.*

⁴ *Ibid.*

⁵ Order dated 26 July 2019.

⁶ Order dated 17 December 2019.

On the second discovery conference, Complainant failed to appear while Respondent was present. The Respondent was then ordered to submit its Responsive Comment.⁷

In its Responsive Comment, Respondent contended that Complainant willingly and knowingly gave his consent to them, thus:

12. It is worthy to note that Complainant AMP willingly and knowingly gave his consent to Respondent HXXX through its Mobile App to make and manage phone calls, to access photos, media and files on his device as can be shown in Annex “C” and “C-1”. Consent is acquired before any customer-borrower may start processing the loan application. It was also clear in the Privacy Policy of what kind of information needs to be collected, one of which is the communication information containing call history, sms (sic), CONTACTS and more.

xxx

14. Moreover, the Authorization Letter of Information of Information (sic) found at the end of the process of the loan application expressly stated that borrower-customer is granting Respondent HXXX to use the contacts and addresses provided for collection purposes when the applicant’s loan becomes overdue.

15. Assuming arguendo that messages were sent by Respondent HXXX pending presentation of those messages, there was no violation committed as there was a proper consent obtained from Complainant AMP to use other ways, such as contacts and addresses, for collection purposes when Complainant AMP defaulted in his loan as provided in the Authorization Letter of Information which Complainant AMP agreed upon during his loan application. xxx⁸

Issues

1. Whether Respondent committed a violation of the Data Privacy Act that warrants a recommendation for prosecution; and
2. Whether a temporary ban should be issued against Respondent’s processing of personal data.

⁷ Order dated 12 December 2019

⁸ Responsive Comments dated 20 December 2019.

Discussion

The Complaint does not warrant a recommendation for prosecution of a violation under the Data Privacy Act

The Complaint alleged that certain messages were sent by Respondent to his contacts. The Complaint, however, did not specify the content of these forwarded text messages. Aside from allegations that his co-workers and family members complained about the calls and text messages they received from Respondent, Complainant has not offered any proof of the existence of the messages supposedly sent by Respondent to these third parties.

Despite the opportunities given to Complainant to substantiate his allegations during the two (2) discovery conferences scheduled on 13 September 2019 and 12 December 2019, Complainant failed to appear without notice or justification.

Given all these, the Commission is left without any basis to recommend Respondent for prosecution under the Data Privacy Act, considering it is bound to adjudicate following the NPC Rules of Procedure, which provides:

Section 22. Rendition of decision. – The Decision of the Commission shall adjudicate the issues raised in the complaint **on the basis of all the evidence presented** and its own consideration of the law.⁹

As the Supreme Court held in *Government Service Insurance System v. Prudential Guarantee*, “it is basic in the rule of evidence that bare allegations, unsubstantiated by evidence, are not equivalent to proof. In short, mere allegations are not evidence.”¹⁰

As such, in the absence of sufficient evidence to support Complainant’s allegations that Respondent disclosed his personal information to his contacts, it cannot be said that Respondent committed an act that would constitute the prohibited acts of

⁹ NPC Circular No. 16-04 dated 15 December 2016 (“NPC Rules of Procedure”), Section 22. Emphasis supplied.

¹⁰ G.R. No. 165585, 20 November 2013, *citing* Real v. Belo, 542 Phil. 109 (2007).

unauthorized processing¹¹ or processing for an unauthorized purpose.¹²

The Complaint does not warrant the issuance of a temporary ban

In his Complaints-Assisted form, Complainant applied for a temporary ban on Respondent's processing of his personal data based on the ground of "privacy invasion."¹³ This is governed by NPC Circular 16-04 (NPC Rules of Procedure) which provides:

Section 19. *Temporary Ban on Processing Personal Data.* – At the commencement of the complaint or at any time before the decision of the National Privacy Commission becomes final, a complainant or any proper party may have the National Privacy Commission, acting through the investigating officer, impose a temporary ban on the processing of personal data, if on the basis of the evidence on record, such a ban is necessary in order to preserve the rights of the complainant or to protect national security or public interest.

a. A temporary ban on processing personal data may be granted only when: (1) the application in the complaint is verified and shows facts entitling the complainant to the relief demanded, or the respondent or respondents fail to appear or submit a responsive pleading within the time specified for within these Rules; xxx¹⁴

Not having presented any evidence, much less substantial evidence, Complainant's application for the issuance of a temporary ban is denied.

Respondent misunderstands the concept of consent

Nevertheless, the Commission notes that Respondent misunderstands the DPA in asserting that they obtained Complainant's consent to access his contacts.¹⁵

¹¹ Republic Act No. 10173, Section 25.

¹² *Id.*, at Section 28.

¹³ *Supra*, Note 1.

¹⁴ NPC Circular No. 16-04 dated 15 December 2016 ("NPC Rules of Procedure"), Section 19.

¹⁵ *Supra*, Note 9.

Notably, the “consent” form that appears on the screen of the customer-borrowers upon download of the application merely asks:

Allow cm to make and manage phone calls? (Deny, Allow)¹⁶

xxx

Allow cm to access photos, media and files on your device?
(Deny / Allow)¹⁷

The Privacy Policy attached by Respondent only states “anti-fraud services” as the purpose for obtaining the customer-borrower’s communication information, thus:

1. What kind of information needs to be collected? xxx
 - Communication information. Call history, sms, contacts and more.

xxx

2. How to use customer information? xxx
 - Communication information. Based on the consent of the customer, the data reported to the server, the information will be used for anti-fraud services. xxx¹⁸

Respondent likewise asserts in its Responsive Comment that the Authorization Letter of Information should also serve as a justification of consent from Complainant.

A look at the Authorization Letter of Information, however, would show that it only refers to emergency contacts and not the entirety of the contacts in Complainant’s phone book:

Important
Note:

xxx

The applicant has already clearly understand and accept the Cash Lending service from HXXX Lending Technology Inc the person will provide the **emergency contact** to objectively evaluate the credit level and lending amount and supply the good service for the applicant.

¹⁶ *Supra*, Note 8 at Annex C.

¹⁷ *Ibid*, at Annex C-1.

¹⁸ *Ibid*, at Annex D.

The applicant will agree and grant that HXXX Lending Technology Inc can use the other contact ways and address provided for collection when the applicant is overdue for repayment.¹⁹

Personal information controllers who rely on consent as basis to process their information must ensure that such consent is “freely given, specific, and an informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her.”²⁰

The data subject must be informed of all the personal information intended to be collected. In this case, the Commission notes that the Privacy Policy and Authorization Letter of Information did not adequately inform the customer borrowers of the full extent of the intended processing. It only stated that it will process the customer- borrower’s emergency contacts, which the Complainant may easily accept as an industry practice. This notice to the customer-borrower, however, is inconsistent with the allegations in the Complaint that all of Complainant’s co-workers and family members received messages of his unsettled loan.²¹

Uninformed consent cannot be considered as valid consent.

The Commission likewise notes that the Authorization Letter of Information contains ambiguous statements such as how “HXXX Lending Technology Inc. can use the other contact ways and address provided for collection when the applicant is overdue for repayment.”²² The broad statement of purpose for processing cannot be considered as compliant with the general privacy principle of transparency.

The DPA’s Implementing Rules and Regulations explain the principle of transparency, thus:

The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data

¹⁹ *Ibid*, at Annex F. Emphasis supplied.

²⁰ Republic Act No. 10173, Section 3(b). Emphasis supplied.

²¹ *Supra*, Note 1.

²² *Supra*, Note 8 at Annex F.

should be easy to access and understand, using clear and plain language.

While the Commission finds that the allegations of Complainant are not sufficiently substantiated to warrant a recommendation for prosecution, it finds it necessary to emphasize the need for personal information controllers, such as Respondent, to inform their data subjects of the nature and purpose of the processing of their personal information in “clear and plain language.” The requirement to use clear and plain language does not mean using layman’s terms to substitute technical words at the risk of not capturing the complex concepts they represent. Rather, this requirement means that information should be provided in as simple a manner as possible, avoiding sentence or language structures that are complex.²³ The information provided should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations²⁴ such as in the above-cited provision which states that “HXXX Lending Technology Inc. can use the other contact ways and address provided for collection when the applicant is overdue for repayment.”

WHEREFORE, all the above premises considered, the Complaint by AMP against HXXX Lending Technology Inc. (CM) is hereby **DISMISSED**.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against the Respondent before any other forum or tribunal, if any.

SO ORDERED.

Pasay City, Philippines;
19 November 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

²³ See, Guidelines on transparency under Regulation 2016/679 of the Article 29 Working Party (2017).

²⁴ *Ibid.*

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

AMP
Complainant

ACA
Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

RABD

Complainant,

-
versus-

NPC Case No. 19-1221
*For: Violation of the
Data Privacy Act of
2012*

FXXX GLOBAL LENDING, INC.

Respondent.

X-----X

DECISION

AGUIRRE, D.P.C.

Before this Commission is a complaint filed by RABD (“Complainant”) against FXXX Global Lending, Inc. (“Respondent”) for a violation of the Data Privacy Act.

The Facts

In the Complaint, Complainant alleged that Respondent sent mass text messages (“text blasts”) to her phone contacts to inform them of her unpaid loan. She further alleges that Respondent sent text messages threatening her using information they collected from her phone.¹ She claimed that Respondent was able to hack her contacts, inbox, and images.²

On 13 September 2019, Complainant sent a letter to the Commission stating thus:

I am writing this letter to request your good office for withdrawal of my filed complaint against FXXX online lending company. After careful consideration, I decided not to take any action against them in order to have peace on both sides.³

¹ Records, p. 3.

² *Id.*, at 5.

³ *Id.*, at 9.

She was informed by the Complaints and Investigation Division that she needed to submit a notarized Affidavit of Desistance.⁴ On 3 March 2020, Complainant submitted her Affidavit of Desistance which stated the following:

1. I am the Complainant in the above-titled complaint filed and pending before the National Privacy Commission against FXXX Global Lending, an online lending mobile application;
2. I realize that I am no longer interested in pursuing this case because I already settled my obligation to (sic) them;
3. I also believe that it is best to end the proceedings in this case.

Premises considered, I am permanently withdrawing my complaint against respondent in the above-titled case. I am no longer interested, and hereby desist, in prosecuting this case.

I am executing this Affidavit of Desistance to have the complaint immediately dismissed and deemed closed.⁵

Complainant personally appeared before the Commission's resident notary public to swear to the due execution of her Affidavit of Desistance. The notary public explained to her the implications and consequences if she desists from proceeding further.

Discussion

Given Complainant's personal appearance before the Commission's resident notary public to attest to her execution of the Affidavit of Desistance, the Commission finds the document to have been willingly and voluntarily executed, without any indication of fraud, deception, or misrepresentation.

The Commission wishes to emphasize that Complainant's Affidavit of Desistance does not *ipso facto* result in the termination of the case nor does it divest the Commission of its jurisdiction to investigate further, *sua sponte*, on the possible criminal liabilities that may result from the alleged violations of the Data Privacy Act.

⁴ *Id.*, at 10.

⁵ *Id.*, at 11.

In this case, however, the Commission is constrained to dismiss the Complaint considering that the allegations cannot be proven without the evidence to be provided by Complainant.

This is consistent with NPC Circular 16-04 (“Rules of Procedure”) which provides:

Section 22. Rendition of decision. – The Decision of the Commission shall adjudicate the issues raised in the complaint on the basis of all the evidence presented and its own consideration of the law.⁶

WHEREFORE, all premises considered, the Commission hereby resolves to **DISMISS** the Complaint of RABD against Respondent FXXX Global Lending Inc.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against the Respondent before any other forum or tribunal, if any.

SO ORDERED.

Pasay City, 25 June 2020.

Sgd.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

WE CONCUR:

Sgd.

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

⁶ NPC Circular No. 16-04 dated 15 December 2016 (“NPC Rules of Procedure”), Sec. 22.

Sgd.
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED

RABD
Complainant

FXXX GLOBAL LENDING, INC.
Respondent

COMPLAINTS AND INVESTIGATIONS DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

MHH,

Complainant,

-versus-

NPC Case No. 18-141

(Formerly NPC Case No. 18-I-141) *For: Violation of the Data Privacy Act of 2012*

VCF and SFPS,

Respondents.

X-----X

DECISION

AGUIRRE, D.P.C.:

For this Commission's Resolution is the Complaint¹ filed by Complainant MHH against Respondents VCF and SFPS, involving an alleged violation of R.A. No. 10173 (Data Privacy Act).

The Facts

The Complainant alleges that she has been a private school teacher in SFPS for ten (10) years. She states that on 18 October 2017, the School Director of SFPS, Respondent VCF, sent a letter² to the Registrar of Tomas Claudio Colleges (TCC) requesting a copy of Complainant's Official Transcript of Records and Diploma without her consent. The letter was premised on his intention to ensure that the teachers working in the institution were well-equipped with the necessary units and seminars needed to effectively teach the students.

On 28 April 2018, while Complainant was processing her master's degree enrolment in TCC, she was informed about Respondent VCF's letter-request and that TCC did not respond to the same.³ Complainant then called JPS, the SFPS Secretary, to clarify the matter. He answered, "*Ma'am, tapos na po iyon. Dala lang po ng galit, magpapaliwanag po kami ni A.*"⁴

¹ Complaint via online complaints-assisted portal dated 25 September 2018.

² Letter-Request dated 18 October 2017.

³ *Supra* note 1.

⁴ *Ibid.*

The Complainant replied and said, “*Ok na iyon, sige tapos na. Sana tama na.*”⁵

After the call was disconnected, Complainant received a text message⁶ stating that:

Madam, lipas na yun, sorry kung nawalan talaga kami ng tiwala noon, alam mo naman ang tension dati kaya siguro dala ng galit ay nakasama kami sa ganun sitwasyon, papaliwanag kami ni A sayo as soon as possible, isa ka sa advisers ko pero nagawa ko yun kaya sorry ulit, my second mom!⁷

After that, Complainant thought that the issue was already settled.⁸ However, the SFPS Management Committee sent a letter to the Registrar of TCC dated 02 May 2018 informing them that they were in the process of reviewing the documents of their old and new teacher applicants and following up on their 18 October 2017 letter:

In connection to this, please provide us a written explanation on the letter submitted to your office last October 18, 2017 of the documents of MHH for verification veracity (sic) of the papers submitted.⁹

On 09 May 2018, Complainant wrote a letter to Respondent VCF informing him that she will file criminal and administrative cases against SFPS and all the persons whose signatures appeared on the letter dated 02 May 2018, which included Respondent VCF. Complainant enumerated the violations they have allegedly committed against her, namely, Section 2, Bill of Rights of the Philippines Constitution; Sections 25 and 26 of R.A. No. 10173 (Data Privacy Act of 2012); Section 1 of Article V, Section 2 of Article VI, and Sections 1, 2 and 3 of Article XI of Code of Ethics for Professional Teachers.

On 25 September 2018, the Complaints and Investigation Division (CID) of this Commission received a Complaint¹⁰ from

⁵ *Ibid.*

⁶ *Ibid.*

⁷ Screenshot of a text message dated April 28.

⁸ *Supra* note 1.

⁹ *Ibid.*

¹⁰ *Supra* note 1.

Complainant via its online complaints-assisted portal alleging that Respondent VCF, requested from TCC her Official Transcript of Records and Diploma without her consent and knowledge.

On 14 November 2018, the CID ordered the parties to appear before this Commission to Confer for Discovery to discuss whether discovery of information and of electronically-stored information will be sought; the issues relating to preservation of information, the period to produce the information, the method of asserting and preserving claims of privilege information, confidentiality and proprietary status of information, the appropriateness of allocating expenses of production of information, and any other issues relating thereto.¹¹ Both parties were present.¹²

On 03 December 2018, Respondents filed their Answer.¹³ Respondent VCF alleged that on 01 May 2017, he became the School Director of SFPS and he discovered that the school was laden with debts due to qualified theft, unpaid tuition fees, low number of enrolees, and unqualified personnel. In the course of the investigation and evaluation of the problem, SFPS was able to get hold of two (2) transcripts of records of Complainant, namely, (1) Transcript of Records dated 23 May 2008 with the course of Bachelor of Secondary Education with Special Order No. [Redacted] S. 2008; and (2) Transcript of Records dated 22 January 2018 with the course of Bachelor of Elementary Education with Special Order No. [Redacted] S. 2008.

Since Respondent VCF was unable to solicit a convincing explanation from the Complainant, he sent the letter dated 18 October 2017 to TCC requesting for a copy of the Official Transcript of Records and Diploma of Complainant, which was ignored. After seven (7) months, the SFPS Management Committee sent the 02 May 2018 letter to TCC asking for a written explanation on status of their first letter, which was also ignored.¹⁴

Respondents denied Complainant's allegations that SFPS was making a background check on her and claimed that the inquiry

¹¹ Order to Confer for Discovery scheduled on 14 November 2018.

¹² Fact-Finding Report dated 28 April 2020.

¹³ Answer dated 28 November 2018.

¹⁴ *Supra* note 12.

was for the legitimate interest of the school to protect it from unqualified personnel.¹⁵

Respondents also stated that prior to the filing of the instant complaint, Complainant also filed a complaint against LOC, a public school principal.¹⁶ On the other hand, Complainant's son filed complaints against IR, MD, PO, TS, LL, and BD,¹⁷ for allegedly taking part in the background checking of the authenticity and validity of Complainant's credentials.

Respondents also refuted Complainant's claim that she had submitted her Transcript of Records when she applied at SFPS, asserting that Complainant was suspended in 2012 for her failure to submit the same.

It was only during the discovery conference on 14 November 2018 that Complainant submitted the following documents:

1. Official Transcript of Records dated 19 June 2008;
2. Diploma for Bachelor of Elementary Education; and
3. Affidavit of Discrepancy of MSD.¹⁸

Respondents maintained that the Affidavit of Discrepancy by TCC's School Registrar is not reliable since it did not explain the discrepancies in the two (2) different official transcript of records. Furthermore, the submissions made by the Complainant only prove that there were indeed different courses and different special order numbers in complainant's transcripts of records.¹⁹

In Complainant's Reply,²⁰ she argued that the signatories of the letter dated 02 May 2018 were not legitimate members of the SFPS Management Team since most of them were just volunteer parishioners. Thus, she asserted that they have no right to meddle with school issues in the absence of an employer-employee relationship with SFPS or any board resolution, constitution or other document granting them authority.

¹⁵ *Ibid.*

¹⁶ Letter -Complaint dated 15 May 2018.

¹⁷ Letter-Complaint received on 14 June 2018.

¹⁸ *Supra* note 12.

¹⁹ *Supra* note 13.

²⁰ Reply dated 02 December 2018.

Complainant also stressed that her credentials were allegedly disclosed by ECP, Respondents' counsel, during a non-related case conference before the Department of Labor and Employment Mediation Board in Cainta, Rizal.²¹

Complainant maintained that the discrepancy in her transcripts of records is not her fault and any accountability should be shouldered by TCC.²²

In Respondents' Rejoinder,²³ they reiterated the failure of Complainant to submit her transcript of records in 2012. Despite being given a three (3)-day suspension in the Memorandum dated 2 April 2012 and promising to submit her Transcript of Records in a letter dated 03 August 2012, Complainant was again given a warning in a subsequent Memorandum dated 21 September 2012 but she still failed to submit her Transcript of Records. Respondents maintained that it has the right to protect SFPS and to be clarified as to the truth or falsity of the two sets of Transcripts of Records, which was the reason why the letter- requests were sent to TCC.

Issue

The sole issue in this case is whether Complainant was able to prove that Respondent committed a violation of the Data Privacy Act.

Discussion

This Commission hereby finds no substantial evidence to support the Complaint for a violation under the Data Privacy Act.

Complainant's allegation of a data privacy violation is centered on Respondents' letter-requests to TCC for a copy of her official Transcript of Records and Diploma after it found that her personnel file contains discrepancies.

²¹ *Ibid.*

²² *Ibid.*

²³ Rejoinder received by General Records Unit on 22 January 2019.

The documentary evidence submitted by the parties show that TCC did not release any of Complainant's records despite the repeated requests of Respondents. It was only during the discovery conference that the Complainant submitted her records when required by the investigating officer.²⁴

Respondents cannot be held liable for a data privacy violation for merely requesting from TCC the Transcript of Records and Diploma of Complainant. The unheeded request for documents containing personal information cannot be considered as processing of personal information. The processing of personal information is an essential element of any data privacy violation.

Section 3(j) of the Data Privacy Act defines *Processing* as follows:

Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the **collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.**²⁵

While there were requests from Respondents for a copy of Complainant's Transcript of Records and Diploma, TCC did not grant such requests. Intent to process is not a violation under the Data Privacy Act, as it defines processing as a "set of operations performed upon personal information."²⁶ Without any of these acts performed upon Complainants' Transcript of Records and Diploma coming from TCC, there was no processing of the personal information contained in those documents.

Moreover, as to the two (2) sets of Transcripts of Records of Complainant that were already in the possession of Respondents during their alleged investigation regarding unqualified personnel, there is nothing on record to show that they were obtained by Respondents through unlawful or unauthorized means.

Transcripts of Records are part of the usual pre-employment documents that need to be submitted during the recruitment process. The record also shows that SFPS followed up several times with Complainant for her to submit her Transcript of

²⁴ *Supra* note 12.

²⁵ Emphasis supplied.

²⁶ Data Privacy Act, Section 3(j).

Records back in 2012. Complainant even stated in her Reply that she would not be in service with SFPS for 10 years if the matter were not resolved.²⁷ In fact it was Complainant who stated that the Transcript of Records dated 23 May 2008, the Transcript of Records dated 22 January 2018, and her Diploma were already in the possession of Respondents as part of her 201 files.²⁸

Complainant also alleged in her Reply that her credentials were disclosed to unauthorized persons, such as the SFPS management committee, the PTA president of SFPS, the president of TCC, and the volunteer parishioners of SFPS.²⁹ While the 02 May 2018 letter Complainant referred to states that it was attaching the “papers submitted by the said person,” there is no evidence on record, however, showing the exact nature of those papers or that they contained personal information.

It is a basic rule of evidence that mere allegations are not equivalent to proof.³⁰ As this Commission held in *JV v. JR*:³¹

The complaint shall only be recommended for prosecution if it is supported with relevant evidence which a reasonable mind might accept as adequate to justify a conclusion. The allegations in the complaint must be based on substantial evidence that there is a clear and real violation of the law.

As to Complainant’s claim that her credentials were disclosed by Respondents’ counsel, ECP, during a non-related case conference before the Department of Labor and Employment Mediation Board in Cainta, Rizal, suffice it to say that aside from the fact that no proof of said disclosure has been proffered, Respondents’ counsel is not a respondent in this case.

This Commission takes this opportunity to clarify that educational records are considered sensitive personal information, the lawful processing of which should conform to Section 13 of the Data Privacy Act. Given this, Respondents’ justification for requesting the educational records of Complainant from TCC without her

²⁷ *Supra* note 20, at par. 4(o).

²⁸ *Ibid.*, at par. 4(q).

²⁹ *Ibid.*, at par. 4(f), (g), and (i).

³⁰ *See*, *Morales v. Ombudsman*, 798 SCRA 609, 17 July 2016.

³¹ NPC. Case No. 17-047, 13 August 2019, *available at* <https://www.privacy.gov.ph/wp-content/uploads/2020/10/CID-17-047-JV-v.-JR-Decision-PSD-10Aug2020.pdf>.

consent on the basis of its legitimate interest as an employer holds no merit.

This Commission's Advisory Opinion No. 2018-006 provides that:

First and foremost, LPU, as an educational institution, is considered as a personal information controller (PIC), processing personal information of its students, employees, and alumni, thus, is covered by the law and under the jurisdiction of the NPC.

X X X

As a PIC, LPU is bound to **implement reasonable and appropriate organizational, physical, and technical measures to protect the personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.** It is accountable for any personal information under its control and custody, including those transferred to a third party. Given the responsibility of LPU to secure personal information, its **denial of your request for information may be justified due to the lack of consent of the data subject.** Although consent is not the only condition for lawful disclosure or processing, in general, of personal information, it may be the most appropriate criterion in this scenario. Likewise, LPU as the **PIC is mandated to recognize and enforce the rights of the data subject, including the right to be informed regarding the recipients to whom data will be disclosed.**³²

Be that as it may, since the allegations for unauthorized processing, accessing personal information due to negligence, and unauthorized disclosure have not been proven by Complainant, her Complaint must be dismissed.

WHEREFORE, premises considered, the instant complaint is hereby **DISMISSED** for lack of merit.

SO ORDERED.

Pasay City, Philippines
09 June 2020.

³² Emphasis supplied.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

MHH
Complainant

VCF
Respondent

SFPS
Respondent

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION**

GENERAL RECORDS UNIT
National Privacy Commission

ECB,

Complainant,

NPC 17-005a

For: Violation of the
Data Privacy Act

-versus-

SSMSM,

Respondent,

X-----X

DECISION

NAGA, D.P.C.:

This refers to the complaint filed by ECB (Complainant) against SSMSM (Respondents), regarding the processing, access to and disclosure of the detailed record of the Complainant's calls to a certain mobile user.

The Facts

Complainant alleges that Ms. IM, an agent of the Respondents, has disclosed to her colleague the detailed records of the Complainant's calls to a certain mobile user.

On 29 November 2017, Complainant filed a formal complaint to this Commission. In the complaint, the Complainant attached a letter dated 28 October 2017 addressed to the branch head of SC – SM Manila as part of her evidence. In said letter, Complainant reiterated that the disclosure of confidential information to IM's colleague was made without her consent. She also attached a summary of information that was disclosed by IM.

Complainant also attached in her complaint another letter wherein Respondents apologized for the incident caused by the latter's agent. In the said letter, Respondents also informed

Complainant that IM was placed on hold status, pending a disciplinary action against her.

On 03 May 2018, the parties were ordered to appear for a discovery conference, however, both parties failed to appear. Hence, another discovery conference was set on 13 August 2018.

On 13 July 2019, Respondents submitted a Motion to Dismiss with an attached receipt, release, waiver, and quitclaim ("Quitclaim") dated 31 January 2019. Respondents claim that the attached acknowledgement receipt of Php 150,000.00 from SCI was executed by the Complainant herself. Thus, Respondents prayed for dismissal of the case due to the amicable settlement between the parties.

However, the Complaints and Investigation Division (CID) noted that the documents were unsworn and no competent proof of identity of Complainant was attached. The CID then ordered the Complainant to appear before this Commission to verify whether she voluntarily, willingly, and knowingly executed said Quitclaim.

On 13 November 2019, Complainant personally appeared before the CID and attested as to the fact of the due execution of the Quitclaim. She also submitted her identification cards and the specimen of her signature.

On 13 December 2019, Respondents submitted the original copy of the notarized Quitclaim of the Complainant.

On 06 March 2020, the CID submitted the case to the Commission for its resolution.

Discussion

This Commission finds that CID is correct in confirming the authenticity of the submitted Quitclaim by ordering the Complainant to appear before it in order to confirm and acknowledge the authenticity of said document. She also confirmed

with CID that she received Php150,000.00 as settlement consideration.

Further, seeing that the Quitclaim has no badges of fraud and deception; and that it was done in consideration of a sufficient settlement consideration; and its provisions are not contrary to law, public order, public policy, morals or good customs, or prejudicial to a third person then the Quitclaim shall be treated as a voluntary agreement between the parties to settle the instant case.

As ruled by the Supreme Court in *Arlo Aluminum Inc., v. Vicente Pinon, et. al.*¹, “But where it is shown that the person making the waiver did so **voluntarily, with full understanding of what he was doing**, and the **consideration for the quitclaim is sufficient and reasonable**, the transaction must be recognized as a valid and binding undertaking.” (Emphasis Supplied)

WHEREFORE, premises considered, this Commission resolves that the instant Complaint filed by ECB be **DISMISSED**.

SO ORDERED.

Pasay City, Philippines.
02 July 2020.

(Sgd.)

JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

(Sgd.)

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

¹G.R. No. 215874, 05 July 2017

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

ECB
Complainant

AACR&C
Counsel for SSMSM

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

ID Y.S.

Complainant,

—versus—

DS BANK,

Respondent.

NPC 17-015

(For violation of
Data Privacy Act of
2012)

X-----X

DECISION

LIBORO, P.C.:

Before this Commission is a complaint filed by ID Y.S. (Complainant) against DS Bank (Respondent) for the violation of Data Privacy Act of 2012 (DPA).

Facts

Sometime in June 2016, Complainant called Respondent’s hotline and its Collection Department to complain about the demand letters she had been receiving since March to July 2016 addressed to a certain ID L.S. with account number 0000xxxxxxxxxxxxx. One of the agents verified that the account number belonged to Complainant while another agent told her that it was a case of mistaken identity. Hence, Complainant requested that Respondent’s fraud department investigate her concern.

On 16 August 2016, Complainant filed a letter-complaint with Bangko Sentral ng Pilipinas (BSP) against Respondent regarding the issue. In reply, Respondent apologized for sending erroneous demand letters to her email address idys@yahoo.com. Further, Respondent’s agent I.J.C. informed Complainant that her email account had been removed from the account of ID L.S.

On 24 May 2017, Complainant filed the instant complaint before the Commission and alleged that she never received feedback on the internal investigation of Respondent regarding her concern.

On 30 August 2017, both parties appeared and expressed their willingness to explore the possibility of an amicable settlement. However, both parties were unable to agree on the terms and conditions of the settlement during the Discovery Conference dated 27 September and 25 October 2017.

Discussion

This case before the Commission warrants dismissal.

The crux of the complaint is the allegation by Complainant that her data privacy rights in accordance with the DPA was violated by Respondent when she received several demand letters for a credit card payment.

Justice Alicia Austria-Martinez penned that he who alleges a fact has the burden of proving it and a mere allegation is not evidence¹. Hence, the burden lies on Complainant to prove whether or not Respondent committed a violation of the DPA.

Section 3 (f), Rule 1 of NPC Circular 16-03 (Personal Data Breach Management) provides that:

Personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of: An availability breach resulting from loss, accidental or unlawful destruction of personal data; Integrity breach resulting from alteration of personal data; and/or A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.

Upon careful examination of the case, Respondent sent several demand letters containing the personal data of ID L.S. (“Data Subject”)

¹ Luxuria Homes Inc. vs. CA, GR No. 125986, Jan 28, 1999

to Complainant. Accordingly, the personal data of the Data Subject was breached or compromised due to the unauthorized disclosure by Respondent. However, Complainant as a mere recipient of the demand letter was not personally affected by the unauthorized disclosure committed by Respondent to the Data Subject.

Settling the existence of breach in this case, the Commission now tackles the crux of the complaint. Section 3 of NPC Circular 16-04 (NPC Rules of Procedure) provides for who may file a complaint:

SECTION 3. Who may file complaints. – The National Privacy Commission, sua sponte, or persons who are the subject of a privacy violation or personal data breach, or who are otherwise personally affected by a violation of the Data Privacy Act, may file complaints for violations of the Act. The person who is the subject of the privacy violation or personal data breach, or his or her duly authorized representative may file the complaint, Provided, that the circumstances of the authority must be established. Any person who is not personally affected by the privacy violation or personal data breach may: (a) request for an advisory opinion on matters affecting protection of personal data; or (b) inform the National Privacy Commission of the data protection concern, which may in its discretion, conduct monitoring activities on the organization or take such further action as may be necessary.

In this case, the Commission observed that there was no allegation that Complainant's personal information was breached and resulted to loss, accidental, or unlawful destruction of her personal data. Further, there was no allegation that Complainant's personal information was disclosed to the Data Subject or to any other person. What was alleged in the Complaint is that Complainant was personally affected when she became the recipient of the demand letters belonging to the Data Subject.

The clear provision of the law then clearly implies that being a recipient alone of someone else's personal information does not entitle the recipient, which is the Complainant in this case, the right to file a complaint or claim for damages. Hence, Complainant's allegation that she was personally affected cannot be admitted by the Commission for her failure to show that her personal information was breached or compromised. Complainant's stand-alone allegation is not sufficient

to file a complaint before the Commission because she is neither the subject of a privacy violation or personal data breach, or who is otherwise personally affected by a violation of the DPA. Put simply, Complainant does not have a legal standing to sue Respondent since she is not the affected data subject or was personally affected by a violation of the DPA.

The pronouncement however of the Commission in this case does not bar the people who are not personally affected to call the attention of the Commission on matters affecting protection of personal data.

The law also extends help to any person who is not personally affected by the privacy violation or personal data breach. Whereas, the person not personally affected, like Complainant in this case, can request for an advisory opinion on matters affecting protection of personal data. As to data protection concern, they can inform the National Privacy Commission, which may in its discretion, conduct monitoring activities on the organization or take such further action as may be necessary.

In view of the foregoing, the Commission finds that the case must be dismissed for the reason that Complainant does not have a legal standing to sue Respondent for a violation of the DPA.

WHEREFORE, premises considered, the case NPC 17-015- ID Y.S. vs. DS Bank is hereby **DISMISSED** for lack of merit.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against the Respondent before any other forum or tribunal, if any.

SO ORDERED.

Pasay City, Philippines;
31 January 2020.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy

Commissioner Copy furnished:

ID Y.S.
Complainant

DS BANK
Respondent

**LEGAL DIVISION ENFORCEMENT
DIVISION GENERAL RECORDS
UNIT**
National Privacy Commission

EA and TA,

Complainant,

-versus-

NPC Case No. 17-018

*For: Violation of Section 25 (b)
of the Data Privacy Act of
2012*

EJ, EE and HC,

Respondents.

X ----- X

DECISION

For consideration of the Commission is the complaint filed by Complainants EA and TA against Respondents EJ, EE and HC for Violation of Section 25(b) of the Data Privacy Act of 2012 (DPA).¹

Relevant Facts

Complainants allege that:

1. On 07 April 2017, Respondents EJ and HC filed a case against Complainant TA for Falsification of Public Documents docketed as NPS No. VI- 10-INV-17D-00915 before the Office of the City Prosecutor of Iloilo City;
 - a. The case involved the alleged falsification of the two birth certificates of CEA and CTA, the sons of TA.

¹ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012]

- b. EJ alleged that TA falsified the entries in the certificates of live birth stating that the Complainants were married on December in California, USA.
 - c. EJ also submitted before the Office of the City Prosecutor of Iloilo City the Certificate of Marriage² between Complainant EA and a certain MS and Certificates of No Marriage (CENOMAR)³ of both complainants.
- 2. Respondents were neither authorized to obtain nor access any of the mentioned documents, as well as the personal information contained therein.
 - 3. Respondent EE obtained said documents containing sensitive personal information under the order of her employer, EJ. They resorted to underhanded means in obtaining these documents.
 - 4. The acts of Respondents endanger the sanctity and privacy of the Complainants and the public at large.⁴

Complainants allege that Respondents committed unauthorized processing of sensitive personal information prohibited under the DPA. Complainants argue that the documents containing sensitive personal information were obtained without their consent and without authority under the DPA or any existing law.

On 31 August 2017, Complainants submitted their Supplemental Complaint reiterating the points already raised in their Complaint- Affidavit.⁵

On 18 September 2017, Respondents EJ and EE, filed their Comment, where they raised the following arguments:

² Records, p. 40.

³ *Id.*, at pp. 12 and 15.

⁴ *Id.*, at pp. 1-3.

⁵ *Id.*, at pp. 56-58.

1. The Data Privacy Act of 2012 does not apply to them because it only covers natural and juridical persons involved in data processing;

2. The act of reporting the matter as to the true and factual marital status of the complainants to the proper authorities is not considered within the definition of “processing of personal sensitive [sic] information” no matter how expansive the definition of the term;

3. The marital status of Complainants are not personal or sensitive personal information because they are there for everybody to know. They are to be considered as “public records” as they are readily available from the public registry. Complainants are even fostering in all their complaints, pleadings and allegations that they are married, and they have legitimate children; and

4. Assuming that processing was done with the sensitive personal information of Complainants, it was made for a legitimate purpose of filing a criminal complaint of falsification.⁶

Respondents EJ and EE submitted their Supplemental Comment containing substantially the points they previously raised in their Comment.

On 17 November 2017, Complainants personally filed before the Commission their Reply refuting the arguments of Respondents stating that:

1. Personal sensitive information, as defined under the Data Privacy Act, is privileged and confidential and prohibits its processing except in certain circumstances, under Section 13 of R.A. 10173. Complainants allege that the act of respondents does not fall within the exceptions in processing sensitive personal information.

2. Neither EJ, EE, nor their authorized agents were the data subjects concerned in the documents requested. Therefore, they have no authority to access or use the personal sensitive information in the subject documents

⁶ *Id.*, at pp. 186-193.

pertaining to the Complainants and their children. It is clear from the Data Privacy Act that these can only be obtained by the data subject themselves or their authorized representatives.⁷

On 10 January 2018, a Discovery Conference was held⁸ where all the parties appeared except for Espinosa. During the conference, it was made known to the Commission that Respondent HC is the sister of Complainant TA.

According to EJ, they requested the subject documents from Philippine Statistics Authority (PSA) because TA filed a petition for guardianship proceedings over her mother who was EJ's client. EJ explained that the documents were obtained to determine the moral fitness of TA as the guardian of his client.⁹

Further, he also said that the documents were obtained sometime in September 2016, before PSA issued in 2017 the guidelines limiting the release of those kinds of documents only to specified authorized persons.¹⁰ He alleged that after obtaining the documents, he learned of the marital circumstances of TA. This incident prompted him to file a complaint for falsification against her.

Based on the documents submitted and the proceedings held, it appears that there were other pending cases between the parties and that the conflict between them started when HC, by virtue of a Special Power of Attorney, sold some of the properties of their mother. EJ was the one who notarized all the legal documents pertaining to the sale. When Complainants discovered those transactions, the parties started filing different cases against each other, including the present complaint. Respondents used the subject documents in the guardianship proceedings and in the criminal complaint against Complainants.

¹¹

ISSUE

⁷ *Id.*, at pp. 266-275

⁸ *Id.*, p. 304.

⁹ *Id.*, p. 310. Transcript of Discovery Hearing on 10 January 2018.

¹⁰ *Id.*

¹¹ *Id.*, at pp. 4-20. Annex of the Complaint-Affidavit.

The sole issue to be determined in this case is whether the Respondents violated Section 25 (b) of the DPA in processing the Complainant's personal data for the purposes described above.

DISCUSSION

In determining whether a violation of Section 25(b) of the DPA occurred, three elements must be established with substantial evidence:

1. The accused processed the information of the data subject;
2. The information processed was personal information or sensitive personal information;
3. That the processing was done without the consent of the data subject, or without being authorized under this act or any existing law.

As to the first element, the DPA provides a definition of processing as “any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.”¹² Simply stated, processing refers to any use of personal data at any stage of the data life cycle.

In this case, Respondents requested and consequently obtained the subject documents from PSA in order to look into the personal circumstances of Complainant TA and, in view of the petition for guardianship proceedings she filed for their mother , to oppose to TA's moral fitness as such guardian.

Respondent EJ also used the same documents in filing the criminal complaint docketed as NPS No. VI-10-INV-17D-00915 before the Office of the City Prosecutor of Iloilo City. The documents, containing the personal and sensitive personal information of Complainants were annexed to the criminal complaint to support his allegations in that case.

Given these, Respondents' actions of collecting, storing, and using the sensitive personal information of Complainants as evidence

¹² Data Privacy Act of 2012, § 3(j).

to support their allegations in the criminal complaint in NPS No. VI- 10-INV-17D-00915 is considered processing of sensitive personal information.

Any misconception about “processing” being limited to digital means should be dispelled. The DPA covers not just the processing of digital data but any processing of personal information whether it is in a digital or paper form. The DPA does not distinguish.

As to the second element, the information subject of this case is sensitive personal information. Under the DPA, sensitive personal information refers to information:

1. About an individual’s race, ethnic origin, **marital status**, age, color, and religious, philosophical or political affiliations;
2. About an individual’s health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4. Specifically established by an executive order or an act of Congress to be kept classified.¹³

Contrary to the allegations of Respondents that “[t]he information as to the marital status of Complainants are there for everybody to know, it is not personal nor sensitive, since marital status of a person is public information,”¹⁴ marital status is specifically included in the enumeration of what is considered sensitive personal information under the DPA.

¹³ Data Privacy Act of 2012, § 3(l). Emphasis supplied.

¹⁴ Records, p. 251.

It is a misconception that publicly available personal data can be further used or disclosed for any purpose whatsoever without regulation. Personal data does not lose the protection afforded by the DPA simply because it has been made public or is publicly accessible.¹⁵

In this case, the fact that Complainants announce their status in public does not change the nature of this information as sensitive personal information. The law specifically enumerates what can be considered as sensitive personal information based on the potential risk posed by its processing to the data subject, and the enhanced protection needed to avert it. Under the Act, the rule is that the processing of the enumerated sensitive personal information is prohibited unless one of the grounds for lawful processing of such sensitive personal information is present.¹⁶

With regard to the third element, Section 13 of the Act expressly prohibits the processing of sensitive personal information, except in the following cases:

“xxx

- f. The processing concerns such personal information as is **necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims**, or when provided to government or public authority (Emphasis supplied).”

During the Discovery Conference, it was repeatedly brought to the attention of the Commission that the Complainants and Respondents were already opposing parties in a guardianship proceeding even before Respondents filed the criminal complaint for Falsification against Complainants. In the guardianship proceeding, TA is the petitioner while EJ is the counsel of the ward subject of the proceedings.

EJ insists that the relevant documents were obtained while there was a pending case between them. He allegedly processed the sensitive personal information of Complainants to protect the interest of his client in the guardianship proceeding before the Regional Trial

¹⁵ See, Data Privacy Act of 2012, § 4; IRR §§ 4 & 5.

¹⁶ Data Privacy Act of 2012, § 13.

Court of Roxas City, Iloilo, Branch 14.¹⁷ The Respondents, however, failed to substantiate this allegation.

On this matter, it must be clarified that the Data Privacy Act makes a distinction between the three instances where Section 13(f) is applicable, namely: (a) The processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings; (b) The processing is necessary for the establishment, exercise or defense of legal claims; or (c) The processing concerns personal information that is provided to government or public authority.

In this case, while no evidence was submitted to establish that the subject documents were presented in the guardianship proceedings, it is not, however, disputed that the Respondents used the subject documents to build a case for falsification of public documents against Complainants. This falls squarely under the instance of “processing as necessary for the establishment of legal claims” which does not require an existing court proceeding. To require a court proceeding for the application of Section 13(f) to this instance would not only be to disregard the distinction provided in the law but the clear letter of the law as well. After all, the very idea of “establishment ... of legal claims” presupposes that there is still no pending case since a case will only be filed once the required legal claims have already been established.

In addition, the use of the qualifier “necessary” in the law should be understood to apply not just to the “protection of lawful rights and interests of...persons in court proceedings” but also to the “establishment... of legal claims.”

The DPA should not be seen as curtailing the practice of law in litigation. Considering that it is almost impossible for Congress to determine beforehand what specific data is “necessary” or may or may not be collected by lawyers for purposes of building a case, applying the qualifier “necessary” to the second instance in Section 13(f) therefore, serves to limit the potentially broad concept of “establishment of legal claims” consistent with the general principles of legitimate purpose and proportionality.

¹⁷ Records, p. 6.

As regards legitimate purpose, the Implementing Rules and Regulations (IRR) of the Data Privacy Act provides that the processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.¹⁸ This means that the processing done for the establishment of a legal claim should not in any manner be outside the limitations provided by law. The DPA is neither a tool to prevent the discovery of a crime nor a means to hinder legitimate proceedings.

In this case, the collection of the subject documents was in view of the falsification case that was eventually filed with the Regional Trial Court of Roxas City, Iloilo. The processing of the documents for this cannot be considered as wrongful or illegal.

This is all the more true since the subject documents were obtained by the respondents from the Philippine Statistics Authority (PSA) before the PSA limited the authorized persons who can request for copies of Certificates of Birth, Certificates of Marriage and Certificates of Death when it issued Office Memorandum No. 2017- 050¹⁹ on 17 April 2017 and the Memorandum Circular No. 2017-09 ²⁰ on 19 June 2017, thus:

1. 28 October 2016 - Certificate of Live Birth of CEA;
2. 25 October 2016 - Certificate of Live Birth of CTA;
3. 25 October 2016 - The Marriage Certificate of EA and MS with annotation of Final Judgment of Nullity of Marriage under Article 36 of the Family Code;
4. 30 October 2016 - Certificate of No Marriage (CENOMAR) of TA; and
5. 30 September 2016 - CENOMAR of EA.

¹⁸ Implementing Rules and Regulations of the Data Privacy Act of 2012 (hereinafter, "IRR"), § 18(b).

¹⁹ Records, p. 270.

²⁰ Records, p. 276.

It should be stressed, however, that having a legitimate purpose or some other lawful criteria to process does not result in PSA being legally obliged to grant such request. A person requesting for certain information from an administrative agency remains to be subject to that agency's guidelines for the release of such information. In this case, had Respondents requested for the abovementioned certificates after the PSA issued its guidelines, they would have been obliged to comply with such despite having complied with the requirements of the DPA on lawful criteria for processing.

Aside from legitimate purpose, the qualifier "necessary" also pertains to the general privacy principle of proportionality. Under the IRR, the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed **only if the purpose of the processing could not reasonably be fulfilled by other means.**²¹

The proportionality principle, as manifested in the qualifier "necessary" serves as a sufficient test in determining whether the processing is justified in relation to the declared purpose.

In this case, considering that the documents were used in the falsification case and absent any showing that its use was unjustified, it cannot therefore be said that the processing done by Respondents was not necessary.

While the processing of sensitive personal information is expressly prohibited under Section 13 of the Act, the processing made on the sensitive personal information of Complainants falls under one of the exceptions thereto. The Commission finds that the third element is not present in this case. Respondents did not commit unauthorized processing of sensitive personal information under Section 25 (b) of the Data Privacy Act of 2012.

While we find that the Respondent did not violate Section 25 (b) of the Data Privacy Act of 2012, this does not, however, preclude any civil, criminal or administrative liability, if any, on the part of the Respondents arising from other laws.

²¹ IRR, § 18(c), emphasis supplied.

DISPOSITIVE

WHEREFORE, the foregoing considered, this Commission finds that Respondent did not violate Section 25(b) of the Data Privacy Act of 2012 on unauthorized access of sensitive personal information.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against the respondents before any other forum or tribunal, if any.

SO ORDERED.

Pasay City, 15 July 2019.

(SGD.)

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

Concurring:

(SGD.)

IVY D. PATDU

Deputy Privacy Commissioner

(SGD.)

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

EA

5802 Capiz

TA

5802 Capiz

EJ

5000 Iloilo City

EE

5000 Iloilo City

HC

Oton, 5020 Iloilo

ENFORCEMENT DIVISION

Legal and Enforcement Office

National Privacy Commission

5th Floor West Banquet Hall, Delegation

Bldg. PICC Complex, 1307 Manila

B.Q.N.,

Complainant,

—versus—

NPC 18-066

NUQ INC., *doing the business
under the name and style of HQ,
N.S., N.U., D.B.L.
and S.K.D.,*

*(For violation of Data
Privacy Act of 2012)*

Respondents.

X-----X

DECISION

LIBORO, P.C.:

Before this Commission is a case filed by B.Q.N. (Complainant) against NUQ INC., *doing the business under the name and style of HQ, N.S., N.U., D.B.L. And S.K.D. (Respondents)* for the violation of Data Privacy Act of 2012 (DPA).

Facts

On 06 July 2018, Complainant filed a complaint before the National Privacy Commission and alleged the following:

A court order¹ has been issued to Respondents requiring the release of K.H.Q.'s (K.H.Q.) income as Complainant's HQ driver. The income information was offered as evidence in a case against K.H.Q.. However, Respondents allegedly submitted a certification disclosing information pertaining to Complainant's income and not that of K.H.Q.'s. The

¹ Order of the Regional Trial Court, Branch 94 of Quezon City, dated 06 February 2018:
As prayed for by Atty. S, let subpoena duces tecum ad testificandum be issued to Winston Beltran, Security and Safety Head, HQ, xxxxxxxx, for him to bring a Certification as to the date of accreditation as HQ driver of the accused and his number of trips and monthly earnings from January 2017 up to January 2018 and to testify thereon on the said date.

certification includes the name of the driver, vehicle type and plate number driven by K.H.Q., date of accreditation of K.H.Q. as HQ driver; name of complainant as operator; and breakdown of the number of rides, fares and incentives earned by K.H.Q. from January 2017 to January 2018.

On 11 September 2018, parties were ordered to confer for discovery. However, through email, Respondents asked for its postponement. Complainant manifested that she was not willing to enter into an amicable settlement. Thus, Respondents were ordered to submit their responsive Comment instead.

On 01 August 2018, Respondents filed their responsive Comment together with their supporting documents. In their Comment, Respondents explained that the disclosure of personal information indicated in the certification is legitimate. It was made in the performance of a legal obligation imposed upon Respondents through a validly issued court order². The compliance thereto will necessarily involve the processing and disclosure of personal information of K.H.Q. and Complainant to comply with a legally issued and served *subpoena*. Hence, the Respondents further stated that since the processing and disclosure of the personal information of Complainant and K.H.Q. are explicitly allowed under the law then the disclosure of the personal information included in the certification is not contrary to the DPA, its implementing rules and regulations, and other issuances of the Commission.

On 18 October 2018, Complainant submitted her Reply. She argued that Respondents made inconsistent statements in its Comment when it claimed that HQ is not privy to any arrangement between the peer/operator and the driver regarding how they split their earnings, while also stating in the same pleading that both the driver and the peer/operator share the same summary of earnings. Complainant questioned respondent HQ's argument that the information which it processes regarding fare and incentive earnings solely belong to the driver when in fact the certification it issued in the name of Complainant also bears the same exact earnings as that issued to K.H.Q..

² Ibid.

Issue

Whether Respondents committed a violation of the DPA in submitting the subject certification to the court in compliance to a *subpoena*.

Discussion

This complaint lacks merit and hence, the Commission adjudged its dismissal.

Upon careful consideration of the submissions of both parties, the Commission observed that Complainant is the car operator of Toyota Vios that is registered on a HQ platform while K.H.Q. is the registered driver. Due to a criminal case filed against K.H.Q., the court issued a *subpoena* against Respondents. The *subpoena* obliged Respondents to release a Certification as to the date of accreditation as HQ driver of K.H.Q., his number of trips, and monthly earnings from January 2017 up to January 2018. Hence, Respondents as the personal information controller (PIC) processed the information of K.H.Q. to comply with the *subpoena*. However, Complainant alleged that Respondents issuance of the Certificate containing her information instead of K.H.Q.'s information violated her data privacy rights against unlawful processing and unauthorized disclosure because the personal information was processed and disclosed without her consent.

Not all processing and disclosure of personal information, like Complainant's information in this case, are violations of the DPA. It allows lawful circumstances where personal information can be validly processed and disclosed notwithstanding the absence of consent.

Section 12 of the DPA provides the criteria for lawful processing of personal information:

SEC. 12. The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

(a) The data subject has given his or her consent;

(b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;

(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;

(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

The processing of personal information shall be permitted only if not otherwise prohibited by law. Among the criteria for lawful processing of personal information provided above, it provided that processing of information is permissible if the processing is necessary for compliance with a legal obligation to which the personal information controller is subject.

In this case, the legal obligation of Respondents arose from the *subpoena* issued by the court. Rule 21, Rules of Court, provided the rules regarding *subpoena* and the effect of non-compliance therewith:

Section 1. Subpoena is a process directed to a person requiring him to attend and to testify at the hearing or the trial of an action, or at any investigation conducted by competent authority, or for the taking of his deposition. It may also require him to bring with him any books, documents, or other things under his control, in which case it is called a subpoena duces tecum.

xxxx

Section 9. Failure by any person without adequate cause to obey a subpoena served upon him shall be deemed a contempt of the court from which the subpoena is issued. If the subpoena was not issued by a court, the disobedience thereto shall be punished in accordance with the applicable law or Rule.

The *subpoena* being required by the court and issued within its powers, created an obligation arising from law³ on the part of Respondents in this case. The *subpoena duces tecum* is, in all respects, like the ordinary *subpoena ad testificandum* which mandates the witness to bring with him and produce at the examination the books, documents, or things described in the subpoena.⁴ Like in this case, Respondents were required to submit a Certification⁵ containing all the details required in the *subpoena*. Ergo, Respondents cannot be faulted in processing the information because of its compliance with the aforementioned.

Section 17 of the Implementing Rules and Regulations of the Data Privacy Act of 2012 (Rules) provides that:

The processing of personal data shall be allowed, subject to compliance with the requirements of the Act and other laws allowing disclosure of information to the public, and adherence to the principles of transparency, legitimate purpose, and proportionality.

The Rules⁶ then subjects the processing of data with DPA compliance and other laws allowing disclosure of information to the public. It further states that it should adhere to the principles of transparency, legitimate purpose, and proportionality. In the principle of proportionality⁷, it provides that:

The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared

³ New Civil Code, Article 1157.

⁴ G.R. No. L-13463, H. C. LIEBENOW vs. THE PHILIPPINE VEGETABLE OIL COMPANY, November 9, 1918

⁵ Respondent HQ's certification, which was submitted to the court, enumerates the following:

- a. Name of the driver: K.H.Q.
- b. Vehicle type and plate number driven by K.H.Q.;
- c. Date of accreditation of K.H.Q. as HQ driver;
- d. Name of complainant as operator; and
- e. Breakdown of the number of rides, fares and incentives earned by K.H.Q. from January 2017 to January 2018.

⁶ Section 18 of the Implementing Rules and Regulations of the Data Privacy Act of 2012

⁷ Section 18 (c) of the Implementing Rules and Regulations of the Data Privacy Act of 2012

and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

The aforesaid principle then states that when assessing the processing of personal data, proportionality requires that only the personal data which is adequate and relevant for the purposes of the processing is collected and processed. In this case before the Commission, Respondents only processed and collected the information required in the *subpoena*.

More so, due to the nature of *subpoena*, Respondent's cannot be faulted as failure to comply to the foregoing shall be deemed contempt of court with its corresponding liability.

Respondent HQ does not distinguish between the earnings of the driver and the operator, considering that its records only indicate the number of rides, fares, and incentives that are indicated in the mobile application. Considering that Respondent HQ is not a privy to the arrangement between the driver and the car owner, the grievance submitted by Complainant is not a matter that can be addressed before the Commission.

In a nutshell, the information contained in the certification under the name of K.H.Q., including the information on the number of rides, fares, and incentives, relates to K.H.Q. and not to Complainant. The processing of Complainant's name as the operator was pursuant to a legal obligation by virtue of a subpoena issued to Respondents and in accordance with the principle of proportionality.

With the foregoing, it is prudent for the Commission to dismiss the case since the processing and disclosure of the personal information included in the Certification is not contrary to the DPA, its rules and regulations, and other issuances of the Commission.

Moving forward, the Commission takes this opportunity to remind the Respondents as a PIC to abide by the general privacy principles of transparency, legitimacy, and proportionality as it processes information even when responding to a legal obligation. Respondents

should always be mindful of the rights and interests of the individual about whom personal information is processed⁸.

WHEREFORE, premises considered, the case NPC 18-066 “ B.Q.N. vs. NUQ INC., *doing the business under the name and style of HQ, N.S., N.U., D.B.L. and S.K.D.*” is hereby **DISMISSED** for lack of merit.

SO ORDERED.

Pasay City, Philippines;
21 May 2020.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

B.Q.N.
Complainant
XXXXXXXXXX
XXXXXXXXXX

HQ, NUQ INC,
N.S., N.U., D.B.L. AND S.K.D.
Respondent

⁸ NPC 17-047, Decision, National Privacy Commission.

XXXX

X

XXXX

X

**LEGAL DIVISION ENFORCEMENT
DIVISION GENERAL RECORDS
UNIT**

National Privacy Commission

ECV

Complainant,

NPC 18-074

-versus-

CVF,

Respondent.

For: Violation of
the Data Privacy
Act of 2012

X-----X

DECISION

NAGA, P.C.;

Before this Commission is a Complaint filed by ECV against CVF for violating Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA).¹

Facts

ECV, in her Complaints-Assisted Form dated 23 July 2018, alleged that CVF obtained a copy of her Marriage Certificate “without any authority.”²

ECV narrated that on 30 November 2017, CVF humiliated her when the latter alleged that she was a mistress.³ When confronted by ECV’s son about her proof of such claim, CVF allegedly responded that she was able to get a copy of the Marriage Certificate of “the first family of UD from the [National Statistics Office].”⁴ The National Statistics

¹ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes, [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

² Complaints-Assisted Form dated 23 July 2018 of ECV, at page 2.

³ *Id.*

⁴ *Id.*, at pages 2-3.

Office (NSO) was the previous name of the Philippine Statistics Authority (PSA).⁵

In a subsequent email to the Commission sent on 06 August 2018, ECV stated that CVF was able to acquire her Marriage Contract from the PSA without her knowledge and permission.⁶ ECV attached scanned copies of two (2) Philippine National Police (PNP) Incident Record Forms in the email to support her complaint.⁷ ECV narrated that CVF confronted her and said in the vernacular that she was a mistress.⁸ As evidence of the claim, CVF uttered that she had her NSO Marriage Certificate.⁹

Subsequently, ECV informed the Commission, through an email sent on 07 August 2018 at 1:46 AM, that she received a copy of CVF's administrative complaint against her for misconduct.¹⁰ She claimed that:

There are two Marriage Contract[s] from Philippine Statistics Authority attached in the last part of the affidavit that they have submitted to the Department of Education, Region X - Northern Mindanao, Cagayan de Oro City. The Marriage Contract belongs to RV & ECV and RV & El. I know this is an opportunity to file a complaint and protect my rights.¹¹

In the email, ECV attached a Complaint dated 09 May 2018 filed before the Department of Education (DepEd) for Misconduct (DepEd Complaint), which included, as an attachment, ECV's Marriage Contract with RV dated 10 July 1987.¹² In a succeeding email sent at 1:47 AM of the same day, ECV attached a letter in response to the DepEd Complaint.¹³ In the letter, she claimed that CVF is in violation of Section 25 of the DPA.¹⁴

⁵ See An Act Reorganizing the Philippine Statistical System, Repealing for the Purpose Executive Order Numbered One Hundred Twenty-One, Entitled "Reorganizing and Strengthening the Philippine Statistical System and for Other Purposes", [Philippine Statistical Act of 2013], Republic Act No. 10625, § 28 (2013).

⁶ Email of ECV sent on 06 August 2018.

⁷ *Id.* PNP Incident Record Form Entry No. XXX-1 and PNP Incident Record Form Entry No. XXX- 2, both dated 04 December 2017.

⁸ *Id.* at PNP Incident Record Form Entry No. XXX-2 dated 04 December 2017.

⁹ *Id.*

¹⁰ Email of ECV sent on 07 August 2018, 1:46 AM.

¹¹ *Id.*

¹² *Id.*, See Complaint dated 09 May 2018 of CVF.

¹³ Email of ECV sent on 07 August 2018, 1:47 AM. See Letter dated 12 July 2018 of ECV.

¹⁴ *Id.* at page 1.

The Commission, through the Complaints and Investigation Division (CID), issued an Order to Confer for Discovery, which directed the parties to appear before the Commission on 18 October 2018.¹⁵

During the discovery conference, both parties appeared and manifested that they were willing to enter into a settlement.¹⁶ In an email sent on 09 November 2018, ECV manifested that the “agreed Amicable Settlement did not prosper”, and attached further evidence for the proceedings, including a Supplemental Complaint Affidavit dated 07 November 2018 (Supplemental Affidavit).¹⁷

The Supplemental Affidavit stated the following allegations, among others:

1. That I am the Complainant in the CID Case No. 18-5-074 xxx
2. That the Respondent is CVF xxx
3. That on November 30, 2017, while supervising the repair of our fence, she confronted me and uttered defamatory statements;
4. That the utterance expressed that I am only a mistress;
5. That my son JCV was agitated and immediately asked her if she has evidence regarding her allegations and the Respondent said that they obtained Marriage Contracts from the NSO. xxx

xxx

7. That the respondent answered that they have obtained from the NSO a Marriage Contract from another wife and our own Marriage Contract;
8. That on December 3, 2017, another incident occurred and I personally saw CF mother of the respondent waving a pieces of paper (*sic*) which happens to be my Marriage Contract and the Marriage Contract of my husband to his first wife while the respondent is uttering the same defamatory remarks;

xxx

¹⁵ Order to Confer for Discovery, undated, at page 1.

¹⁶ See Order dated 13 April 2019, at page 1.

¹⁷ Email of ECV sent on 09 November 2018.

10. That aside from the defamatory remarks uttered against me, she also filed a malicious complaint before Department of Education, Region X, charging me of Misconduct;

11. That some of the pieces of evidence attached are my Marriage Contract and the Marriage Contract of my husband to his other wife;¹⁸ (Emphases supplied)

In an Order dated 13 April 2019, the CID directed the parties to submit their Compromise Agreement within fifteen (15) days from receipt thereof. Should the parties fail to do so, CVF was ordered to file her Comment within ten (10) days from conclusion of the proceedings, ECV was given ten (10) days from their receipt of the comment to file her Reply, and CVF was given ten (10) days from receipt of the Reply to file her Rejoinder.¹⁹

CVF submitted a Manifestation of Compliance dated 07 June 2019.²⁰ She manifested that no compromise agreement was reached and attached her Responsive Comment to the Complaint.²¹

In her Responsive Comment dated 07 June 2019,²² CVF: 1) denied the allegation that she obtained ECV's Marriage Certificate, or that she made any processing in relation to said Marriage Certificate;²³ 2) claimed that ECV has long harassed CVF and her family, which led the latter to file the DepEd Complaint for Misconduct, docketed as Admin Case No. 10-18-027;²⁴ and 3) raised the defense that the Complaint should be dismissed outright for being filed beyond the reglementary period under Section 4(c), Rule II,²⁵ and Section 12 (b), (c), and (d), Rule III,²⁶ of NPC Circular No. 16-04 (2016 NPC Rules of Procedure).

ECV filed a Comment and Opposition dated 25 November 2019.²⁷ She reiterated the contents anchoring her complaint,²⁸ narrated various

¹⁸ Supplemental Complaint Affidavit dated 07 November 2018 ECV, at pages 1-2.

¹⁹ Order dated 13 April 2019, at page 3.

²⁰ Manifestation of Compliance dated 07 June 2019 of CVF.

²¹ *Id.*, at page 1.

²² Responsive Comment dated 07 June 2019 of CVF.

²³ *Id.*, ¶¶ 1-4, at pages 3-4.

²⁴ *Id.*, ¶¶ 5-6, at page 4.

²⁵ *Id.*, ¶9, at page 5.

²⁶ *Id.*, ¶11, at pages 5-6.

²⁷ Comment and Opposition dated 25 November 2019 of ECV.

²⁸ *Id.*, ¶¶ 1-16, at pages 1-3.

cases between the parties,²⁹ and alleged that the complaint before the Commission was timely filed.³⁰

In an Order dated 16 September 2021, the CID ordered the DepEd to submit a certified true copy of the case file for the DepEd Complaint docketed as Admin Case No. 10-18-XXX.³¹

In a Compliance dated 22 September 2021, the DepEd submitted certified true copies of various documents constituting the case file of the DepEd Complaint.³²

On 04 January 2022, the CID acknowledged receipt of the case files.³³ In relation to the Marriage Contract of RV and ECV (herein Complainant), the CID asked for confirmation whether the said document was originally filed by CVF, or the circumstance of how the document formed part of the case file.³⁴

In a Certification dated 12 January 2022, the DepEd certified “that a photocopy of the Marriage Contract between RV and ECV dated July 10, 1987, was attached, and included by CF when she filed the complaint against ECV before the Department of Education, Regional Office 10.”³⁵

Issues

I. Whether the Complaint should be dismissed for being filed beyond the reglementary period.

II. Whether Respondent violated Section 25(b) of the DPA.

Discussion

²⁹ *Id.*, at pages 4-9.

³⁰ *Id.*, at page 10.

³¹ Order dated 16 September 2021, at page 1.

³² Compliance dated 22 September 2021 of the Department of Education- Region X, Northern Mindanao.

³³ Order dated 04 January 202[2], at page 1.

³⁴ *Id.*

³⁵ Certification dated 12 January 2022 of the Department of Education- Region X, Northern Mindanao.

The Commission dismisses the Complaint for lack of merit.

I. The Commission exercises its authority to resolve the case on the merits.

ECV filed her complaint against CVF on 23 July 2018.³⁶ The first event to have allegedly violated her privacy rights happened on 30 November 2017, when CVF stated that she obtained ECV's Marriage Contract from the NSO.³⁷ The second relevant event was narrated in her Supplemental Affidavit dated 07 November 2018, when she stated that CVF attached her Marriage Contract in the DepEd Complaint.³⁸

NPC Circular No. 16-04, or the 2016 NPC Rules of Procedure, was the applicable procedural rules at the time of the filing of the complaint. Section 12(c) of the NPC Circular No. 16-04 allows for the outright dismissal of a complaint when it "is filed beyond the period for filing."³⁹

Further, this Commission refers to the last paragraph of the aforementioned Circular, *viz*:

SECTION 4. Exhaustion of remedies. – No complaint shall be entertained unless:

- a. the complainant has informed, in writing, the personal information controller or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same;
- b. the personal information controller or concerned entity did not take timely or appropriate action on the claimed privacy violation or personal data breach, or there is no response from the personal information controller within fifteen (15) days from receipt of information from the complaint;

³⁶ Complaints-Assisted Form dated 23 July 2018 of ECV.

³⁷ *Id.*, at pages 2-3.

³⁸ Supplemental Complaint Affidavit dated 07 November 2018 of ECV, ¶11, at page 2.

³⁹ National Privacy Commission, Rules of Procedure, NPC Circular No. 16-04, §12(c) (15 December 2016) (NPC Circular 16-04).

c. and the complaint is filed within six (6) months from the occurrence of the claimed privacy violation or personal data breach, or thirty (30) days from the last communiqué with the personal information controller or concerned entity, whichever is earlier.

The failure to comply with the requirements of this Section shall cause the matter to be evaluated as a request to the National Privacy Commission for an advisory opinion, and for the National Privacy Commission to take such further action, as necessary. **The National Privacy Commission may waive any or all of the requirements of this Section, at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to the affected data subject.**⁴⁰ (Emphasis supplied)

On its face, the complaint was filed beyond the six-month period, counted from November 2017. Nevertheless, the last paragraph of Section 4 of the 2016 Rules of Procedure allows the Commission to “waive any or all of the requirements of this Section, at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to the affected data subject.”⁴¹

The Commission exercises its authority to waive the requirement under Section 4(c) of the 2016 Rules of Procedure. ECV’s allegations, if substantially proven, may lead the Commission to conclude that there was a serious violation of the DPA. ECV may also have been seriously harmed due to the processing of her Marriage Contract, which was exposed to her employer, the DepEd.

Thus, the Commission finds it appropriate to exercise its authority to resolve the case on the merits.

II. CVF cannot be held liable for the violation of Section 25(b) or Unauthorized Processing of Sensitive Personal Information.

⁴⁰ *Id.*, § 4.

⁴¹ *Id.*

The controversy essentially revolves around the processing of ECV's Marriage Contract.

The DPA defines processing as “any operation or any set of operations performed upon personal information including, but not limited to, the retrieval...storage, [and] use...of data.”⁴²

ECV narrated that on 30 November 2017, CVF said that she was able to obtain ECV's Marriage Contract from the NSO.⁴³ The Marriage Contract was later attached by ECV to the DepEd Complaint.⁴⁴

CVF denies these allegations. She reasons that, as stated by ECV herself, she would have no authority to obtain the document from the PSA, and “[t]hus, without such authority, it is legally impossible for the PSA to release the Complainant's Marriage Certificate or any personal information to Respondent.”⁴⁵

There are two instances of processing of personal data involved in this case: 1) the acquisition of ECV's Marriage Certificate; and 2) the submission of her Marriage Certificate as part of the DepEd Complaint.

a. There is no substantial evidence to show that the acquisition of ECV's Marriage Certificate was unauthorized.

In relation to the first processing, CVF “vehemently denies” that she obtained the Marriage Certificate of ECV and her husband.⁴⁶ However, it is not disputed that CVF, as the complainant in the DepEd Complaint, submitted ECV's Marriage Certificate to the government agency. This was affirmed by the DepEd itself when it certified that the Marriage Certificate “was attached, and included by CVF when she filed the complaint against ECV before the Department of Education, Regional Office 10.”⁴⁷

⁴² Data Privacy Act of 2012, § 3(j).

⁴³ Supplemental Complaint Affidavit dated 07 November 2018 of ECV, ¶17, at page 1.

⁴⁴ *Id.*, ¶11, at page 2.

⁴⁵ Responsive Comment dated 07 June 2019 of CVF, ¶13, at pages 1-2.

⁴⁶ *Id.*, ¶1, at page 1.

⁴⁷ Certification dated 12 January 2022 of the Department of Education- Region X, Northern Mindanao.

Thus, it can be reasonably concluded that CVF was able to obtain ECV's Marriage Certificate from the fact that she submitted it to the DepEd.

Under PSA Memorandum Circular No. 2017-09, dated 19 June 2017 (PSA Circular), the PSA enumerated the parties who may request an original and certified true copy of a Certificate of Live Birth, Certificate of Marriage, and Certificate of Death.⁴⁸ Pursuant to the Circular, the PSA may only release the Certificates to the following persons or entities:

1. The owner himself or through a duly authorized representative;
2. His/her spouse, parent, direct descendants, guardian or institution legally in-charge of him/her, if minor;
3. The court or proper public official whenever absolutely necessary in administrative, judicial or other official proceedings to determine the identity of a person;
4. In case of the person's death, the nearest of kin.⁴⁹

The evidence on record does not contain adequate information on when CVF actually acquired the Marriage Certificate. ECV, in her sworn statements, merely recounts CVF's alleged utterances of securing ECV's Marriage Certificate.⁵⁰ ECV only provided her own narrations, without any sufficient corroborating or equivalent proof, that establishes the period of CVF's acquisition of the document. If CVF obtained the Marriage Certificate after the issuance of the PSA Circular, there would be reasonable grounds for unauthorized processing since she is not one of the entities authorized to receive the Marriage Certificate.

⁴⁸ Philippine Statistics Authority, Issuance of Original and Certified True Copy of Certificate of Live Birth, Certificate of Marriage and Certificate of Death, Memorandum Circular No. 2017-09, ¶ 2 (19 June 2017).

⁴⁹ *Id.*

⁵⁰ See Complaints-Assisted Form dated 23 July 2018 of ECV, at pages 2-3; Supplemental Complaint Affidavit dated 07 November 2018 of ECV, ¶¶ 5 & 8, at pages 1-2; PNP Incident Record Form Entry No. XXX-2 dated 04 December 2017, at page 2.

Since there is no substantial proof to show that CVF obtained the Marriage Certificate in violation of the PSA Circular, the Commission cannot conclude that CVF committed unauthorized processing in relation to the acquisition of the Marriage Certificate.

b. The use of ECV's Marriage Certificate falls within processing that is necessary for the establishment, exercise or defense of legal claims. There is no violation of Section 25(b) of the DPA.

The second processing relates to CVF's submission of ECV's Marriage Certificate to the DepEd as attachment to her complaint. To reiterate, DepEd certified that ECV's Marriage Contract "was attached, and included by CVF when she filed the complaint against ECV before the Department of Education, Regional Office 10."⁵¹

In ECV's Supplemental Affidavit, she prays that CVF be held liable for Section 25 of the DPA.⁵² This provision penalizes the unauthorized processing of personal information under Section 25(a), and sensitive personal information under Section 25(b).⁵³

The Commission finds it relevant to focus on Section 25(b) of the DPA. The unauthorized processing of sensitive personal information has three (3) elements, namely:

1. The accused processed information of the data subject;
2. The information processed is classified as sensitive personal information; and
3. The processing was done without the consent of the data subject or without authority under the DPA or any existing law.⁵⁴

The Commission finds the first element present. There is substantial evidence to show that CVF submitted ECV's Marriage Contract for the

⁵¹Certification dated 12 January 2022 of the Department of Education- Region X, Northern Mindanao.

⁵² Supplemental Complaint Affidavit dated 07 November 2018 of ECV, ¶ 22, at page 3.

⁵³ Data Privacy Act of 2012, § 25.

⁵⁴ NPC 18-077, Decision dated 15 April 2021, at page 6.

DepEd Complaint. As discussed, the DepEd issued a certification stating that CVF attached and included the Marriage Contract for her DepEd Complaint against ECV.⁵⁵ These actions squarely fall within the definition of processing, which includes the use of a data subject's personal information.⁵⁶

The second element of Section 25(b) of the DPA is also present. Under the DPA, sensitive personal information includes a person's marital race, status, and age.⁵⁷ ECV's Marriage Contract contains these pieces of information.

The last element of the crime requires that the processing be without the consent of the data subject or without authority under the DPA or any existing law.⁵⁸ This element, however, is absent. The Commission finds that the processing of ECV's sensitive personal information was anchored on Section 13(f) of the DPA, which provides:

SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

XXX

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.⁵⁹
(Emphasis supplied)

There are three (3) instances wherein Section 13(f) of the DPA is applicable: “(a) the proceeding is necessary for the protection of lawful rights and interests of natural persons in court proceedings; (b) the processing is necessary for the establishment, exercise or defense of

⁵⁵ Certification dated 12 January 2022 of the Department of Education- Region X, Northern Mindanao.

⁵⁶ See Data Privacy Act of 2012, § 3j.

⁵⁷ *Id.*, § 3(l).

⁵⁸ NPC 18-077, Decision dated 15 April 2021, at page 6.

⁵⁹ Data Privacy Act of 2012, § 13(f).

legal claims; or (c) the processing concerns personal information that is provided to government or public authority.”⁶⁰

CVF’s submission of ECV’s Marriage Contract to the DepEd falls within processing that is necessary for the “establishment, exercise or defense of legal claims.”⁶¹

As stated in *EA and TA vs. EJ, EE and HC*:

The DPA should not be seen as curtailing the practice of law in litigation. Considering that it is almost impossible for Congress to determine beforehand what specific data is “necessary” or may or may not be collected by lawyers for purposes of building a case, applying the qualifier “necessary” to the second instance in Section 13(f) therefore, serves to limit the potentially broad concept of “establishment of legal claims” consistent with the general principles of legitimate purpose and proportionality.⁶²

In her DepEd Complaint, CVF alleged that ECV made malicious utterances against her and her family.⁶³ CVF also asked the DepEd “to conduct an investigation and consequently penalize the respondent for such misconduct.”⁶⁴

CVF submitted various pieces of evidence to support her DepEd Complaint, namely: 1) affidavits from her witnesses;⁶⁵ 2) Tax Declarations of Real Property;⁶⁶ 3) Joint Special Power of Attorney;⁶⁷ 4) Marriage Certificate of RV and EI;⁶⁸ 5) Marriage Certificate of RV and ECV;⁶⁹ and 6) pictures of CVF’s window showing the alleged actions done by ECV.⁷⁰

⁶⁰ *EA and TA vs. EJ, EE and HC*, NPC 17-018, Decision dated 15 July 2019, at page 8.

⁶¹ Data Privacy Act of 2012, §13(f).

⁶² *EA and TA vs. EJ, EE and HC*, NPC 17-018, Decision dated 15 July 2019, at pages 8-9.

⁶³ Complaint dated 09 May 2018 of CVF, ¶¶ 5-9, at pages 2-3.

⁶⁴ *Id.*, ¶11, at page 3.

⁶⁵ *Id.*, Annex “A” – Affidavit of RBF, and unmarked Annexes- Affidavits of CF, Gilbert Sanchez Jr., and HOR, all dated 20 April 2018.

⁶⁶ *Id.*, unmarked Annexes – Tax Declaration of Property No. 14-XXX-XXXX, and Tax Declaration of Property No. 02-XXX-XXXX.

⁶⁷ *Id.*, unmarked Annex – Joint Special Power of Attorney.

⁶⁸ *Id.*, unmarked Annex – Marriage Certificate of RV and EI.

⁶⁹ *Id.*, unmarked Annex – Marriage Certificate of RV and ECV.

⁷⁰ *Id.*, unmarked Annex – various pictures.

To be clear, the Commission is not the proper body to determine the merits of the legal claims that are sought to be established, exercised, or defended by parties, pursuant to Section 13(f) of the DPA.⁷¹ It cannot rule on whether the Marriage Contract helps or detracts from CVF's complaint. Rather, the Commission's task is to determine whether the processing of personal information complies with the DPA, and other related issuances of the Commission.

Further, in relation to compliance with the DPA, the Commission emphasizes that though there may be lawful basis in processing personal or sensitive personal information, such as anchoring the processing in Section 13(f) of the DPA, the said processing must still adhere and be consistent with Section 11 of the DPA, which provides for the General Data Privacy Principles of transparency, legitimate purpose, and proportionality.⁷²

The DepEd Complaint relates to ECV's misconduct.⁷³ CVF contextualizes the "strained relationship" between the parties as a result of a boundary dispute,⁷⁴ and ECV's various gossips that tainted CVF and her family's reputation.⁷⁵ She argues that "[a] teacher's duty is not limited to being an agent of knowledge but, above all else, an agent of morals... A teacher, both in her official and personal conduct, must display exemplary behavior."⁷⁶

Given the context and allegations, the Commission finds that CVF's submission of ECV's Marriage Certificate was necessary for the establishment, exercise or defense of her legal claims against ECV.

It should be emphasized that the processing of ECV's Marriage Certificate was not done in a vacuum but was in relation to the DepEd Complaint in order for CVF to support her allegations and to provide better context. In its Decision dated 23 April 2021, the DepEd used the "facts established and the evidence presented [to] support the findings of ECV's guilt".⁷⁷ The processing, given the surrounding context,

⁷¹ See *EA and TA vs. EJ, EE and HC*, NPC 17-018, Resolution dated 05 November 2020, at page 3.

⁷² Data Privacy Act of 2012, § 11.

⁷³ Complaint dated 09 May 2018 of CVF.

⁷⁴ *Id.*, ¶ 1, at page 1.

⁷⁵ *Id.*, ¶¶ 7-9, at pages 2-3.

⁷⁶ *Id.*, ¶ 13, at page 3.

⁷⁷ Decision of the Department of Education- Region X, Northern Mindanao dated 23 April 2021, at page 3.

cannot be considered unlawful or illegal. It squarely falls within “the establishment, exercise or defense of legal claims” under Section 13(f) of the DPA.

Additionally, the processing is valid since the sensitive personal information was “provided to government or public authority.”⁷⁸ The nature of the information and the party’s purpose in providing it to the public authority should be connected to the latter’s mandate and in relation to the legal claims of the party.

As part of DepEd’s mandate, it is tasked to hear administrative charges against public school teachers, especially when they allegedly violate the Code of Professional Conduct for Teachers.⁷⁹

Here, the processing was in the context of ECV’s position as a public school teacher,⁸⁰ and her alleged violations of specific provisions of the “Philippine Code of Ethics for Professional Teachers”.⁸¹ The processing of sensitive personal information, which was provided to the DepEd for the necessary establishment of CVF’s legal claims, falls within Section 13(f) of the DPA.

Moreover, ECV failed to provide substantial evidence that CVF had no basis to process her Marriage Contract. The Commission emphasizes that the data subject’s consent is not the only basis for lawful processing of personal or sensitive personal information since Sections 12 and 13 of the DPA provide for other lawful bases for processing to be authorized.⁸² While ECV may not have consented to the processing of her Marriage Contract, such act may still be allowed if it is anchored on other bases provided in Section 13 of the DPA.

The Commission finds that there was a valid basis for processing ECV’s sensitive personal information through Section 13(f) of the DPA. Consequently, CVF has not violated Section 25(b) of the law since the

⁷⁸ Data Privacy Act of 2012, § 13(f).

⁷⁹ See The Magna Carta for Public School Teachers, Republic Act No. 4670, §§ 7-9 (1966); Department of Education, Revised Rules of Procedure of the Department of Education in Administrative Cases, DepEd Order No. 49, series of 2006, §§ 1, 8-10, 46 (12 December 2006).

⁸⁰ Complaint dated 09 May 2018 of CVF, ¶ 2, at page 1.

⁸¹ *Id.*, ¶¶ 14-15, at pages 3-4.

⁸² See Data Privacy Act of 2012, §§ 12 & 13.

processing was in relation to the establishment, exercise or defense of legal claims, and provided to a government body.

WHEREFORE, premises considered, the Complaint is hereby **DISMISSED** for lack of merit.

SO ORDERED.

City of Pasay, Philippines.
17 March 2022.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

ECV
Complainant

CVF
Respondent

MB

Counsel for Respondent

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION**

GENERAL RECORDS UNIT

National Privacy Commission

GJ,

Complainant,

-versus-

NPC 19-0048

*For: Violation of the Data
Priva Act of 2012*

VMJ AND MTP,

Respondents.

X-----X

DECISION

NAGA, D.P.C.:

Before this Commission is a Complaint filed by GJ (Complainant) against VMJ and MTP (Respondents) for a violation of the Data Privacy Act of 2012 (DPA).

Facts of the Case

The parties are employees of DFX. Complainant is an Insurance Section Supervisor of the International Department under the Finance Division, while Respondent VMJ is the Officer-in-Charge (OIC) of the Management Information Services Division (MSD) and concurrent Manager of the Manpower Development Department (MDD), and Respondent MTP is the OIC of the Human Resource Division (HRD).

On 24 April 2018, Complainant was allegedly requested by Respondent VMJ for an immediate meeting to inquire details regarding her notice of disallowance that she, along with her co- employee refused to submit a reply to considering their previous submission.¹

¹ Complaint-Assisted Form (CAF), received on 01 February 2019.

On the same week, Complainant came to know from an unnamed concerned employee that copies of her training certificates were allegedly collected by Respondent VMJ from the training section without proper endorsement and request filed with the Human Resource Information Section (HRIS).

On 07 May 2018, Complainant sent a letter to Respondents stating that the DPA requires that all personal information must be collected for reasons that are specified, legitimate, and reasonable.²

On 15 May 2018, Complainant received Respondent VMJ's reply wherein the latter explained that her function includes the evaluation and ascertainment of the completeness of documents to accomplish the docketing process. Further, Respondent VMJ alleged that no breach of data privacy was committed as the information or document collected was specific, the circumstances for requesting it were legitimate and reasonable and for internal use only.³

Complainant responded to both Respondents by sending her own reply.⁴ The reply mainly refuted Respondents' claim and maintained that there was a violation of data privacy. Further, she allegedly requested for a certified true copy of the memorandum (HRMD-MDD- 20XX-XX) from HRD on 06 July 2018. The request was denied.⁵

On 31 January 2019, Complainant filed the instant Complaint before the Commission. She alleged that Respondent VMJ's collection of the copies of her training certificates from Training Section-MDD without properly endorsing his request to the HRIS is a violation of her data privacy rights. Complainant manifests that her training certificates and 201 file are the personal information affected by the act of Respondents. Thus, she prayed for all the reliefs allowed by law and that the Commission impose the corresponding penalty for violation of the DPA. Likewise, a prayer to order Respondents to cease and desist from performing any act prohibited under the said law.⁶

² Memorandum re: Training Certificates dated 07 May 2018

³ Memorandum (HRMD-MDD)-29XX-XX dated 15 May 2018

⁴ Memorandum re: Training Certificates dated 04 June 2018

⁵ Complaint-Assisted Form (CAF), received on 01 February 2019

⁶ Id.

The parties were ordered to appear before the Commission to confer for discovery on 17 April 2019.⁷ Acting on a request from Respondents to reschedule the discovery conference, an Order dated 10 April 2019 was issued rescheduling the discovery conference to 30 April 2019.⁸

During the discovery conference, both parties were present⁹ and signified their willingness to enter into amicable settlement through an application for mediation. Correspondingly, an Order¹⁰ to mediate was issued for the parties to appear at the preliminary mediation conference which was scheduled on 07 June 2019.¹¹

On 07 June 2019, there being no settlement reached by the parties,¹² they were ordered to appear before the Commission for the resumption of complaint proceedings on 02 July 2019.¹³

During the second discovery conference, both parties were present.¹⁴ Considering the manifestation of the parties, Respondents were given ten (10) days to file their Responsive Comment while Complainant was also given ten (10) days from receipt of the Responsive Comment to file her Reply. In addition, Respondents were given an option to file their Rejoinder within ten (10) days from receipt of the Reply.¹⁵

On 15 July 2019, a Responsive Comment was jointly filed by Respondents and prayed that the instant Complaint be dismissed for lack of cause of action.¹⁶

As alleged by Respondents, during an examination of documents forwarded to the office for the liquidation of a training attended to by Complainant, it was discovered that the training directive was not part of the documentation. Respondents clarified that what was retrieved from the Training Section-MDD was a training directive and not a training certificate. Respondents manifest that the retrieval of the said training directive was necessary as it is part of the documentation

⁷ Order to Confer for Discovery dated 23 March 2019

⁸ Order 10 April 2019

⁹ Attendance Sheet for Discovery Conference dated 30 April 2019

¹⁰ Order to Mediate dated 30 April 2019

¹¹ Order dated 30 April 2019

¹² Notice of Non-Settlement of Dispute dated 07 June 2019

¹³ Order for Resumption of Complaint Proceedings dated 07 June 2019

¹⁴ Attendance Sheet for Discovery Conference dated 02 July 2019

¹⁵ Order dated 02 July 2019

¹⁶ Responsive Comment received on 15 July 2019

requirement needed to be attached for liquidation purposes and the intention in retrieving the training directive is to attest to the fact that the said training passed through proper procedure.¹⁷

In the memorandum-reply dated 15 May 2018 of Complainant, Respondent VMJ alleged that he replied to the same on 07 May 2018. He explained that as part of the functions of his office, he has the authority to retrieve the training directive from the Training Section– MDD department. Respondent VMJ further explained that the retrieval of the training certificate was intended to establish a fact that Complainant attended the required training and that any issues on the said training will be settled.¹⁸

Respondents claimed that no breach of data privacy was committed as the information collected was specific, circumstances were legitimate, reasonable and for internal use only, which is intended to settle the liquidation of funds used for a particular training. Further, Complainant did not indicate in the Complaint when and how the Complainant's 201 file was retrieved.¹⁹

In addition, Respondents argued that the Complaint should not have been entertained. They claim that the Complaint was filed in 31 January 2019, seven (7) months and twenty-four (24) days after Complainant's last communication was transmitted to Respondents. Such act failed to conform to exhaustion of remedies under Section 4 (c) of NPC Circular No. 16-04.²⁰

Respondents stressed that the training directive is evidence that the training to be attended has been authorized by the office and obligates the employee to attend. It contains the name and position of the personnel, details of the training and the required submission. Respondents claims that it does not contain sensitive personal information as defined by Section 3 (l) of the DPA.²¹

On 23 July 2019, Complainant filed her Reply dated 18 July 2019 wherein she prayed that such Reply be given due credence and consideration and the reliefs prayed for in the Complaint be granted.

¹⁷ Id.

¹⁸ Memorandum re: Training Certificates dated 07 May 2018

¹⁹ Responsive Comment received on 15 July 2019

²⁰ Id.

²¹ Id.

Complainant contended that she strongly disagree with the position of the Respondents as there are conflicting statements in Respondents' Responsive Comment.²²

First, Complainant alleged that it is highly impossible that there is a liquidation of training attended by her because the training was from 25-27 April 2017 and the liquidation was done allegedly on the latter part of 2018 for which a clearance was issued to her indicating that liquidation was already completed.²³

Second, Complainant claims that Respondents' clarification for retrieving a training directive and not a training certificate is against what was clearly indicated in the Memorandum 15 May 2018. In the Memorandum, Respondents stated that a training certificate was retrieved. Such admission was made to justify that the retrieval of the certificate was intended to establish a fact where an issue on a training was being settled.²⁴

Third, Complainant refutes that the validation and verification if a training passed through the proper procedure is Respondents' function. Their duty only includes receiving the documents submitted to them and not the one who complete it. Complainant further allege that Respondents are incorrect in saying that there was no breach of data privacy as the information was specific, the circumstances for obtaining the copy was legitimate, reasonable and for internal use only. However, the purpose for which the information was taken, without her consent, is malicious.²⁵

Fourth, Complainant stressed that the Commission may accept complaints even after the lapse of six (6) months period from the occurrence of the claimed privacy violation or personal data breach, at its discretion and expounded that the violation of DPA applies to all types of personal information.²⁶

²² Reply dated 18 July 2019, received 23 July 2019.

²³ Id.

²⁴ Id.

²⁵ Id.

²⁶ Id.

Fifth, Complainant argued that violation of the DPA does not only involve sensitive personal information. The law applies to all types of personal information as provided by Section 4 of the DPA.²⁷

On 05 August 2019, the Commission received Respondents' Rejoinder to the Reply of the Complainant wherein Respondents' reiterated its prayer for dismissal for lack of cause of action.²⁸

In the said Rejoinder, Respondents denied Complainant's claim that their statements are conflicting in relation to the supposed liquidation that was done during the latter part of 2018 which, according to them, Complainant's claim has no basis, as no such statement was made and said date of liquidation is immaterial.²⁹

Respondents reiterated their allegations that what was retrieved is a training directive and not a training certificate. Nonetheless, whether it was a directive or certificate, MDD has a file of all company-funded trainings by reason of its function. Should a document relative to a training is lacking, furnishing a copy of the required document for the purpose of completing it is acted upon. The submissions are intended to fully account for expenses disbursed in relation to company-funded trainings and the retrieval and use of a training document can neither be malicious since it is for a legitimate purpose, which is to account for a disbursement of government funds.³⁰

Respondents countered Complainant's fourth point by admitting that the Commission may waive the timeliness of the filing of the complaint but contended that the seriousness of the damage or risk of harm was not shown and likewise does not correspond with Complainant's procrastinated move.³¹

Finally, Respondents states that there was no processing of personal information made in the instant case. Retrieval of an official training document of a government employee using government funds for an officially sanctioned activity neither constitute processing nor a disclosure of personal information protected by the DPA.³²

²⁷ Id.

²⁸ Rejoinder of Respondents (to the Reply of Complainant) received on 05 August 2019.

²⁹ Id.

³⁰ Paragraphs 3-4, Id.

³¹ Paragraph 5, Id.

³² Id.

Issues

1. Whether the Complaint should be dismissed for being filed out of time as provided under Section 4 (c) of the NPC Circular No. 16-04; and
2. Whether Complainant was able to prove that Respondents committed a violation of the DPA.

Discussion

The instant Complaint lacks merit.

Complainant is exempted from Section 4 of the NPC Circular No. 16-04.

As provided by Section 4 of NPC Circular No. 16-04 or the NPC Rules of Procedure, the Commission has the sole discretion to waive the rule on period of filing upon good cause shown, or if the complaint involves a serious violation or breach of the DPA, taking into account the risk of harm to complainant, *to wit*:

SECTION 4. Exhaustion of remedies. – No complaint shall be entertained unless:

- a. the complainant has informed, in writing, the personal information controller or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same;
- b. the personal information controller or concerned entity did not take timely or appropriate action on the claimed privacy violation or personal data breach, or there is no response from the personal information controller within fifteen (15) days from receipt of information from the complaint ; and
- c. the complaint is filed within six (6) months from the occurrence of the claimed privacy violation or personal data breach, or thirty (30) days from the last communiqué with the personal information controller or concerned entity, whichever is earlier.

The failure to comply with the requirements of this Section shall cause the matter to be evaluated as a request to the National Privacy Commission for an advisory opinion, and for the National Privacy Commission to take such further action, as necessary. **The National Privacy Commission may waive any or all of the requirements of this Section, at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to the affected data subject.** (Emphasis Supplied)

Likewise, Section 2, Rule II of the NPC Circular No. 2021-01 or the NPC 2021 Rules of Procedure, has further provided circumstances wherein the Commission should take into consideration if it wishes to exercise such waiver, viz:

SECTION 2. Exhaustion of remedies. – No complaint shall be given due course unless it has been sufficiently established and proven that:

xxx

The NPC may waive any or all of the requirements of this Section at its discretion upon (a) good cause shown, properly alleged and proved by the complainant; or (b) if the allegations in the complaint involve a serious violation or breach of the Data Privacy Act of 2012, taking into account the risk of harm to the affected data subject, including but not limited to:

- i. when there is grave and irreparable damage which can only be prevented or mitigated by action of the NPC;
- ii. when the respondent cannot provide any plain, speedy or adequate remedy to the alleged violation; or
- iii. the action of the respondent is patently illegal.

In addition, as held by the Commission in the case of NPC 19-030 and NPC 19-132,³³ it has been emphasized that despite the failure to exhaust all remedies under Section 4 of NPC Circular No. 16-04, the Commission has its discretionary power to waive the requirements under the said Section grounded on good cause shown, or if the complaint involves a serious violation or breach of the DPA, taking into account the risk of harm to complainant.

³³ Resolution, NPC CN 19-030 and NPC 19-132 dated 10 June 2021

Moreover, in NPC Case No. 19-528, the Commission states the purpose of Section 4 of NPC Circular No. 16-04 which is to prevent the unduly clogging of the Commission's docket and avoid instances of dismissing a case based on mere technicalities.³⁴

In consideration of the Rules and preceding decisions, the Commission weighed and found that herein Complainant was able to file a complaint which demonstrated good cause to justify the waiver of the procedural requirement.

In contrary with Respondents' contention that the seriousness of the damage or the risk of harm towards Complainant was not shown and does not correspond with Complainant's belated filing, the allegations in the instant Complaint posed a serious risk or harm committed by Respondents that if proven and not acted upon, may lead to grave injustice to Complainant since it involves the processing of Complainant's training certificates without proper endorsement and request from the HRIS. In addition, Complainant likewise manifests that her 201 files were affected by the act of Respondents. Hence, the Commission deems it proper to waive the requirement under Section 4 of NPC Circular No. 16-04.

*Complainant failed to prove
that Respondents violated
the DPA.*

It has been numerously held by the Commission that unsubstantiated allegations by either the complainant, respondent or both, cannot merit a favorable decision from the Commission and would warrant a dismissal of the case.

As previously held by the Commission in NPC Case No. 19-569, a complaint bearing only allegations without any corresponding pieces of evidence to support complainant's claim cannot merit a favorable decision from this Commission, *to wit*:

As the Supreme Court held in *Government Service Insurance System v. Prudential Guarantee*, "it is basic in the rule of evidence that bare allegations, unsubstantiated by evidence, are not

³⁴ Resolution, NPC Case No. 19-528 dated 23 February 2021.

equivalent to proof. In short, mere allegations are not evidence.”³⁵

Further, as held by the Supreme Court in the case of *Wong v. Wong*, “The rule is well-settled that he who alleges a fact has the burden of proving it and a mere allegation is not evidence. Thus, his self-serving assertion cannot be given credence.”³⁶

Hence, bearing only allegations without any corresponding pieces of evidence to support Complainant’s claim that Respondent disclosed her personal information which includes the details about her unsettled obligation to her contact list, from which caused her sleepless night and embarrassment, cannot merit a favorable decision from this Commission.³⁷

Moreover, in NPC Case No. 19-612, the Commission likewise dismissed the case for lack of merit as the complainant in the case did not attached any evidence to support her claim, viz:

In this case, Complainant alleged that Respondent contacted Complainant’s manager, superior and other people in her contact list which allegedly were not registered as contact reference in her loan application and informed them about her unpaid loan. Records show that Complainant have not attached any evidence to support her claim. In addition, Complainant was given a chance to substantiate her allegations during the discovery conference. However, Complainant was absent on both dates scheduled for the said discovery conference. More so, she failed to justify her absence. Accordingly, Complainant failed to substantiate the allegations she leveled against Respondent with proof required by law despite being given the opportunity to do so. Other than her bare allegations there is nothing in the records that would indicate that Respondent indeed violated the DPA.

With the foregoing, Complainant’s unsubstantiated allegations remain as mere allegations which cannot be accepted as proof. Hence, the Commission so hold that if a complaint against a corporation holds no basis whatsoever in fact or in law, the Commission will not hesitate to dismiss the case due to a groundless allegation³⁸

³⁵ G.R. No. 165585, 20 November 2013, *citing* Real v. Belo, 542 Phil. 109 (2007).

³⁶ G.R No. 180364, 03 December 2014.

³⁷ Decision, NPC Case No. 19-569 dated 19 November 2020.

³⁸ Decision, NPC Case No. 19-612 dated 13 November 2020

In addition, NPC Case No. 18-135 was dismissed as the Commission cannot rely on mere allegations that is not supported by substantial evidence, to wit:

In this case, the Complainant was not able to provide substantial evidence to prove the alleged recording of his phone calls without his consent. He did not adduce any evidence that could substantiate the existence thereof. Bare allegations, unsubstantiated by evidence, are not equivalent to proof.³⁹

The Commission is bound to adjudicate complaints following Section 22 of NPC Circular 16-04, which provides:

Section 22. Rendition of decision. – The Decision of the Commission shall adjudicate the issues raised in the complaint **on the basis of all the evidence presented** and its own consideration of the law. (Emphasis supplied)

In view of the foregoing, this Commission finds that there is insufficient information to substantiate the allegations of Complainant in the instant complaint against Respondents. Therefore, the Complaint must be dismissed for lack of merit. The Commission cannot rely on mere allegations that is not supported by substantial evidence.⁴⁰

In the present case, Complainant neither specified the particularity of the certificates nor presented pieces of evidence that would substantiate her claim of unauthorized collection. Despite having discovered the alleged violation through a concerned employee, Complainant did not include such material testimony or documentary evidence to support and justify her claim. In addition, Complainant failed to provide an evidence that her training certificate were actually retrieved. She merely anchored her allegations on Respondents' reply which was the memorandum (HRMD-MDD)-20XX-XX dated 15 May 2018 which mentions the retrieval of a training certificate. This memorandum was the reply to Complainant's 07 May 2018 Memorandum.

³⁹ Florencio Morales, Jr., v Ombudsman, G.R. No. 208086. July 27, 2016.

⁴⁰ Decision, NPC Case No 18-135 dated 06 August 2020

Moreover, Complainant alleged in her Complaint that her 201 files were affected. However, no discussion were made in her Complaint on how such files were affected and violated the DPA.

In consideration of the foregoing, the Commission cannot merely rely on the allegations of Complainant in order to decide in her favor. Hence, the Commission finds to dismiss this case.

Respondents were acting within the bounds of their official function

Consent is not the only lawful basis for processing of personal information.⁴¹ As provided by Section 12 (f) of the DPA, one of the criteria to lawful processing of personal information is if the processing is necessary for the purposed of the legitimate interests pursued by the personal information controller, viz:

SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

xxx

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.⁴²

Based on records ⁴³, one of the functional statements of MDD is managing training programs and maintaining employees' records of trainings and seminars attended, among others. Hence, the retrieval of the training certificates or training directive, by reason of Respondents' function, is within their authority.

Further, as government employees performing an official act, Respondents have in their favor the presumption of regularity in the

⁴¹ Section 12 and 13 of the DPA.

⁴² Section 12 (f) of R.A. No. 10173

⁴³DFXX Functional Statement Manpower Development Department, page 35

performance of official duties.⁴⁴ However, Complainant failed to refute this presumption by clear and convincing evidence. Hence, such presumption stands.

WHEREFORE, all the above premises considered, this Commission resolves that the instant complaint filed by GJ against VMJ and MTP is hereby **DISMISSED** for lack of merit.

SO ORDERED.

Pasay City, Philippines;
17 September 2021.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

GJ
Complainant

⁴⁴ *Yap vs Lagtapon*, GR No. 196347, 23 January 2017 citing *Gatmaitan v. Gonzales*, 525 Phil. 658, 671 (2006)

VMJ

Respondent

MTP

Respondent

**COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION**

GENERAL RECORDS UNIT

National Privacy Commission

MLF,

Complainant,

-versus-

**MYTAXI.PH CORPORATION (GRAB
PHILIPPINES),**

Respondent.

X-----X

NPC 19-142

(Formerly CID
Case No. 19-C-
142)

For: Violation of
the Data Privacy
Act of 2012

DECISION

AGUIRRE, D.P.C.;

Before this Commission is a complaint filed by MLF against MyTaxi.PH Corporation, doing business under the name of “Grab Philippines” (Grab Philippines), for an alleged violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

MLF, in his Complaints-Assisted Form, claimed that Grab Philippines committed violations of the DPA.¹

On 6 February 2019, he booked a car ride from UP Town Center² and was assigned to Grab driver ADB with Booking ID No. IOS-141- 99938-8-345.³ As stated by MLF:

Within the Grab System[,] my Name [and] Mobile Number is [sic] made available to the driver. There is also an in[-]app chat function. Both Mobile Number and Chat function are made available with my consent under their terms and condition **for**

¹ Complaints-Assisted Form, 2 March 2019, at 1, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19- 142 (NPC 2019).

² *Id.* at 4.

³ *Id.* at 2.

the purpose of transacting a ride. So that driver and rider can communicate to meet each other.⁴

MLF alleged that, after approximately three to ten (3-10) minutes from booking the ride,⁵ ADB told him that “it’s traffic and asked [him] to cancel the trip.”⁶ He further claimed in his Complaints- Assisted Form that “[t]his is not allowed. In fact[,] Grab Philippines penalizes riders who cancels [sic] trips. So[,] I responded to the driver that I will not cancel the trip but he can if he wants. After which the driver cursed me with the words ‘*tang inamo*’. Then cancelled the trip.”⁷

MLF escalated the matter to Grab Philippines as a privacy violation under Section 28 of the DPA.⁸ In turn, the Data Protection Officer (DPO) replied that “[r]egarding your concern with misuse of personal data, we would like to let you know that the conversation stayed within the app thus it does not breach you [sic] privacy.”⁹ As for Customer Support, it relayed that the driver had sent a handwritten apology letter explaining that the text message was not intended for MLF.¹⁰ MLF opined, however, that Grab Philippines’ responses are mere excuses and that it is not properly using his personal data.¹¹

On 06 June 2019, the Commission ordered the parties to confer for a discovery conference.¹² Only MLF appeared.¹³ The Commission, therefore, issued an Order requiring Grab Philippines to file its responsive comment within ten (10) days from receipt of the Order¹⁴ and an Order requiring MLF to file his reply to the responsive comment within ten (10) days from receipt of the responsive comment.¹⁵

⁴ *Id.* at 2-3. Emphasis supplied.

⁵ *Id.* at 4.

⁶ *Id.* at 3.

⁷ Complaints-Assisted Form, 02 March 2019, at 3, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019). Emphasis supplied.

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*

¹² Order to Confer for Discovery, 13 April 2019, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19- 142 (NPC 2019).

¹³ Attendance Sheet for Discovery Conference, 06 June 2019, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

¹⁴ Order, 14 June 2019, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

¹⁵ *Id.*

On 24 June 2019, Grab Philippines, through counsel, filed its Entry of Appearance and Motion for Resetting of Discovery Conference.¹⁶ It alleged that it belatedly received the Order to Confer for Discovery, hence it respectfully prayed for resetting.¹⁷

On 05 July 2019, Grab Philippines filed a Manifestation and Motion to Defer Submission of Responsive Comment and asked that the filing of its responsive comment be deferred until its prior Motion for Resetting be resolved.¹⁸

On 15 July 2019, the Commission issued a Resolution granting Grab Philippines' Motions.¹⁹ With MLF's conformity, the discovery conference was reset to 13 August 2019.²⁰

During the Discovery Conference on 13 August 2019, both parties appeared.²¹ Grab Philippines manifested that it was not willing to undergo mediation proceedings.²² MLF requested from Grab Philippines the discovery of the following information:

- (1) his e-mail trail with the customer service and data protection officer of respondent from February to March 2019;
- (2) his complaints with the customer service department of respondent;
- (3) his chat logs with respondent's partner from January to May 2019; and
- (4) a copy of respondent's privacy impact assessment for 2018 and 2019.²³

MLF also manifested that he would submit a supplemental complaint. The Commission ordered Grab Philippines to submit the required documents and MLF to submit his supplemental affidavit within fifteen (15) days from receipt of the Order.²⁴

¹⁶ Entry of Appearance and Motion for Resetting of Discovery Conference, 24 June 2019, at 1, *in*. MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

¹⁷ *Id.* at 2.

¹⁸ Manifestation and Motion to Defer Submission of Responsive Comment, 05 July 2019, at 2, *in*. MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

¹⁹ Resolution, 15 July 2019, at 2, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

²⁰ *Id.*

²¹ Order, 13 August 2019, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

²² *Id.*

²³ *Id.*

²⁴ *Id.*

On 27 August 2019, MLF submitted his Affidavit Addendum.²⁵ He attached the email thread between him and Grab Philippines' DPO to show that "[the DPO] replied one time to the email."²⁶ Furthermore, he narrated another incident that occurred on 31 March 2019 wherein the Grab driver asked him to cancel the trip.²⁷ The driver, however, did not cancel the trip and "held [MLF] hostage from using the service."²⁸ MLF had to call Customer Support to cancel the trip and book another one.²⁹ He similarly escalated the incident to Grab Support.³⁰ MLF claimed that "[i]n this incident the Driver has misused my Personal Data (Grab Account) to deny me of Grab Service. A driver is not allowed to ask a Rider to Cancel a ride [...]."³¹ He argued that:

Grab being the Personal Information Controller of my Data (Name, Mobile Number, Grab Account) is responsible in [sic] ensuring [that] my Data is only used for authorized purposes. Based on their Terms and Condition, I am providing Grab Consent to process and share my Personal Data to their partners (Driver) **for the purpose of transacting a trip/ride**. Grab is not a social media/chat app. I do not choose the drivers who will process my data. Grab is the one who assigns them to me. **I do not intend to have chat, call and sms with these assigned drivers outside of transacting a ride**. In my case the Grab App was used by one of their driver [sic] for unjust vexation (original complaint). And in the complaint number 2 my Grab Account was held hostage by the driver who was forcing me to cancel the ride. **In both cases, this is not the consent that I approved Grab to allow my Personal Data to be used for.** [...] Despite their claims of penalizing these erring partners (Drivers), misuse of my personal data still happened again. There is negligence in [sic] Grab's part of handling my personal data based on Terms and Condition that I agreed on [sic].³²

On 28 August 2019, Grab Philippines submitted the following documents requested during the Discovery Conference:

²⁵ Affidavit Addendum to CID Case No. 19-C-142, 27 August 2019, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

²⁶ *Id.* Annex A.

²⁷ Affidavit Addendum to CID Case No. 19-C-142, 27 August 2019, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Id.*

³¹ *Id.*

³² *Id.* Emphasis supplied.

1. Copy of email exchanges between MLF and Grab Philippines' DPO containing a copy of the Complaint sent on 09 February 2019;³³
2. Copy of email thread of Grab Philippines' customer service department with MLF;³⁴ and
3. Copy of MLF's chat logs with Grab Philippines' partner, *i.e.*, ADB.³⁵

As for the 2018 and 2019 Privacy Impact Assessment (PIA) reports, Grab Philippines argued that it is too burdensome on its part to submit these documents because MLF has no legal right to request copies of its entire PIA results, which contain privileged, confidential, and other protected information.³⁶

On 09 September 2019, Grab Philippines filed its Comment to MLF's Complaint and Affidavit Addendum.³⁷ Grab Philippines admitted the facts as alleged by MLF and added that he demanded its DPO to come up with a comprehensive and definitive report within forty- eight (48) hours; otherwise, he would report the case to this Commission.³⁸ Grab Philippines alleged that it properly managed MLF's complaint and escalated it to the proper team.³⁹ It even caused the suspension of ADB.⁴⁰ Grab Philippines, however, claimed that MLF's demand to terminate ADB cannot be done because it will interfere with the contract between Grab Philippines and its "partners/drivers" (drivers).⁴¹

Grab Philippines argued that it should not be held liable for the subject acts committed by its drivers because there is no employee- employer relationship existing between them.⁴² Instead, the Land Transportation Franchising and Regulatory Board (LTFRB) Memorandum Circular No. 2015-15 ruled that drivers accredited by Transportation Network Companies, such as Grab Philippines, are independent contractors.⁴³ Furthermore, Grab Philippines

³³ Compliance to Order dated 13 August 2019, 28 August 2019, Annex A, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

³⁴ *Id.* Annex B.

³⁵ *Id.* Annex C.

³⁶ *Id.* at 2.

³⁷ Comment to Complaint dated 02 March 2019 and Affidavit Addendum dated 27 August 2019, 09 September 2019, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

³⁸ *Id.* at 2.

³⁹ *Id.* at 2-3.

⁴⁰ *Id.* at 3.

⁴¹ *Id.* at 12.

⁴² *Id.* at 5.

⁴³ Comment to Complaint dated 02 March 2019 and Affidavit Addendum dated 27 August 2019, 09 September 2019, at 5, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

maintained that, as provided in its GrabPeer Service Agreement with its drivers, it “shall have no right to, and shall not, control the manner or prescribe the method the [drivers] use to perform accepted bookings.”⁴⁴ In conjunction, its Terms and Conditions for GrabCar Philippines Drivers “expressly states that it shall not be responsible or liable for acts and/or omissions of any services offered by its [drivers] to its passengers, and for any illegal action committed by them.”⁴⁵

Considering the foregoing, Grab Philippines averred that it is not the Personal Information Controller (PIC) in the complained incidents, therefore, it should not be held liable.⁴⁶ It maintained that under its Terms and Conditions for Drivers and Terms of Use for Passengers, its service is limited to linking passengers with third party transportation providers.⁴⁷ It does not provide transportation services or any act that can be construed in any way as an act of a transportation provider especially since it has “no right to, and shall not, control the manner or prescribe the method the [drivers] use to perform accepted bookings.”⁴⁸ Thus, “the fact that the alleged unauthorized communications between the [drivers] and [MLF] happened using [its] mobile application, *i.e., in-app chat feature*, does not make [it] liable for the alleged violation of [MLF’s] privacy rights.”⁴⁹

Alternatively, Grab Philippines posited that assuming it was the PIC, there was no unauthorized processing of personal data.⁵⁰ MLF consented to its collection and use of his personal data.⁵¹ Additionally, Grab Philippines’ Privacy Policy states that these personal data may be used to “enable communications between users, *i.e., [drivers]*.”⁵² Through Grab Philippines’ Terms of Use for Passengers, MLF also agreed that his personal data may be shared with third party providers who “may communicate with him for any reasons whatsoever.”⁵³ Thus, though it does not tolerate unruly and unprofessional behavior of its drivers and frowns upon the cancellation of trips, it may not be held liable for the sharing of

⁴⁴ *Id.* at 5-6.

⁴⁵ *Id.* at 6.

⁴⁶ *Id.* at 7.

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ Comment to Complaint dated 02 March 2019 and Affidavit Addendum dated 27 August 2019, 09 September 2019, at 8, in *MLF v. MyTaxi.Ph Corporation*, NPC Case No. 19-142 (NPC 2019).

⁵⁰ *Id.* at 8.

⁵¹ *Id.*

⁵² *Id.*

⁵³ *Id.* at 9. Emphasis omitted.

MLF's personal data which enables communication between him and its drivers.⁵⁴

Issues

- I. Whether the case should be dismissed outright; and
- II. Whether Grab Philippines violated Section 28 or Processing of Personal or Sensitive Personal Information for Unauthorized Purposes of the DPA.

Discussion

I. The case should be dismissed outright pursuant to Section 12 (b), Rule III, of NPC Circular No. 16-04 (2016 NPC Rules of Procedure).

Given that MLF filed his complaint on 02 March 2019, prior to the effectivity of NPC Circular No. 2021-01 (2021 NPC Rules of Procedure), the applicable rule is the 2016 NPC Rules of Procedure, which provides that:

Rule III. Procedure in Complaints

...

Section 12. Outright Dismissal. – The Commission may dismiss outright any complaint on the following grounds:

...

- b. The complaint is not a violation of the Data Privacy Act or does not involve a privacy violation or personal data breach[.]⁵⁵

There is no privacy violation in this case. The foul statement from the Grab driver in this situation, no matter how offensive, does not in itself constitute a violation of the DPA.

⁵⁴ *Id.*

⁵⁵ National Privacy Commission, Rules on Procedure of the National Privacy Commission, Circular No. 04, Series of 2016 [NPC Circular No. 16-04], § 12 (b) (15 December 2016).

In this case, ADB asked MLF to cancel the trip.⁵⁶ When MLF refused, the driver sent him a message through the in-app chat, stating “*tang inamo*.”⁵⁷ MLF opined that these types of communication from drivers are “outside of transacting a ride”⁵⁸ and are no longer for the purpose of coordinating a ride.⁵⁹

The Commission finds MLF’s interpretation of Grab Philippines’ purpose of the processing of his personal information to be erroneous and narrow. The legitimate purpose principle requires that: (1) the purpose of the processing must be specified and declared to the data subject; and (2) the purpose must not be contrary to law, morals, or public policy.⁶⁰ The first requisite should be understood in relation to the principle of transparency in that the data subject must be informed of the specific legitimate purpose behind the processing of his personal information. The second requisite requires the purpose to be within the limitations of the law, which should be understood to include the entire body of laws, rules, and regulations. Additionally, the purpose of the processing should not go against prevailing morals or run counter to public policy.

Both requisites of legitimate purpose are satisfied in this case. The processing of MLF’s information was done in pursuance of a legitimate purpose, which is to allow the communication between the driver and the passenger to facilitate the transaction of a Grab ride. This purpose was adequately communicated to MLF through Grab Philippines’ Privacy Policy and Terms of Use for Philippines GrabCar Passengers.⁶¹

Grab Philippines is a technology company that “enables and facilitates the matching and booking of transportation solutions [...] between independent third-party service providers and independent customers through its online application software.”⁶²

MLF claimed that he allowed Grab Philippines to share his personal data to its drivers since he “registered to [sic] [G]rab with

⁵⁶ Complaints-Assisted Form, 02 March 2019, at 3, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

⁵⁷ *Id.* Emphasis supplied.

⁵⁸ Affidavit Addendum to CID Case No. 19-C-142, 27 August 2019, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019). Emphasis supplied.

⁵⁹ Compliance to Order dated 13 August 2019, 28 August 2019, Annex B, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019). Emphasis supplied.

⁶⁰ National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (2016).

⁶¹ Comment to Complaint dated 2 March 2019 and Affidavit Addendum dated 27 August 2019, 09 September 2019, Annex J, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019); *Id.* Annex K.

⁶² *Id.* at 1. Emphasis omitted.

the intent of transacting a ride.”⁶³ He, however, opined that the driver contacted him “for purposes that [he] did not provide consent on [sic] based on [Grab Philippines’] terms and conditions.”⁶⁴ He further stressed that:

Under the Data Privacy laws in the Philippines my rights as a data subject wherein my contact [i]nformation (mobile number and grab account) is collected for the purpose of transact[ing] a grab transaction. This rude and unacceptable behavior by your partner is clearly in violation of what constitutes as official business.⁶⁵

Certainly the [c]ommunication of the partner does not cons[t]itute as official business [sic] or consent of me as a data subject. [...] As per the data privacy act my personal [i]nformation and contact should only be used for the consent that [I] allowed grab[.]⁶⁶

This is definately [sic] not authorize[d] use of my personal information and contact. I did not consent grab or your partners to harass me.⁶⁷

MLF argued that:

The issue here is the driver was able to use [Grab Philippines’] platform to message me with messages that are obviously **not for official use**. I did not register or used [sic] grab to be harassed by your partner. [...] Under the data privacy act this constitutes as unauthorized use of my personal data. This includes the facility and consent for your driver to be able to communicate to [sic] me.

...

The issue here is [Grab Philippines’] system allowed an unfit partner to harass a rider. This includes providing the partner or driver access to the chat, call and sms facility which [...] I provided consent to for official business.⁶⁸

If [Grab Philippines is] not aware as per the data privacy law my [i]nformation as a data subject is to be used **only for official**

⁶³ Complaints-Assisted Form, 02 March 2019, at 4, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

⁶⁴ *Id.* Emphasis supplied.

⁶⁵ Affidavit Addendum to CID Case No. 19-C-142, 27 August 2019, Annex A, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

⁶⁶ *Id.* at Annex A.

⁶⁷ *Id.* at Annex A.

⁶⁸ Compliance to Order dated 13 August 2019, 28 August 2019, Annex B, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019). Emphasis supplied.

business. In the case of your platform[,] my name, mobile number, facility to call/sms/message me is disclosed to you and your partners in good faith **for the purpose of coordinating a ride. This has been violated when your partner began using that [i]nformation and that access outside of what would constitute as official business.**⁶⁹

It is clearly enumerated in his contract with Grab Philippines, however, that aside from providing services to MLF, Grab Philippines may share his personal data to other users to enable the communication between them, for any reason whatsoever. Grab Philippines specifically declared this legitimate purpose to MLF. It provides in its Terms of Use for Philippines GrabCar Passengers that:

The Company may use and process your Personal Data for business and activities of the Company which shall include, without limitation[,] the following (the “Purpose”):

- To perform the Company’s obligations in respect of any contract entered with you;
- To provide you with any services pursuant to the Terms of Use herein;

...

- **To share your Personal Data [...] with the Company’s and Group’s agents, third party providers, developers, advertisers, partners, even companies or sponsors who may communicate with you for any reasons whatsoever.**⁷⁰

Grab Philippines’ Privacy Policy similarly states that:

Use of Personal Data

Grab may use, combine and process your Personal Data for the following purposes (“Purposes”).

...

- provide you with Services across our various business verticals;

...

⁶⁹ *Id.* Annex B. Emphasis supplied.

⁷⁰ Comment to Complaint dated 02 March 2019 and Affidavit Addendum dated 27 August 2019, 09 September 2019, Annex J, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019). Emphasis supplied.

- **enable communications between our users[.]**⁷¹

In the absence of any law or regulation prohibiting the same and considering further that it does not go against prevailing morals or run counter to public policy, Grab Philippines' purpose of enabling communication between drivers and passengers through the in-app chat module to facilitate the matching and booking of transportation solutions is considered legitimate.

While it is true that purpose is confined to official business use, MLF's interpretation of what constitutes official business use is inaccurate. He correctly stated that official use should mean "for the purpose of coordinating a ride."⁷² Coordinating a ride, however, is not strictly limited to messages that involve only transportation or booking a ride.

The Commission limits its disposition of the case to the issues raised against Grab Philippines and Grab Philippines' obligations under the DPA. Therefore, it shall not discuss violations of laws that are beyond its jurisdiction. Thus, from a privacy perspective, despite the foul and improper language used by the Grab Philippines driver, the processing of MLF's information by Grab Philippines in this case, adheres to the general privacy principle of legitimate purpose precisely because the communication between the driver and the passenger remains to be in relation to the desired transportation transaction. The incidents complained of by MLF all occurred within the in-app chat module of Grab Philippines⁷³ and the exchange between the parties took place in the process of negotiating and eventually carrying out a Grab ride transaction.

Grab Philippines, as the platform that facilitates and enables the matching and booking of transportation solutions between independent third party service providers and independent customers, has no control over the manner in which the drivers communicate or correspond with their passengers for the purpose of booking or transacting a ride. Nevertheless, the exchange of messages between the passengers and the drivers, though related to

⁷¹ *Id.* at Annex K. Emphasis supplied.

⁷² Compliance to Order dated 13 August 2019, 28 August 2019, at Annex B, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

⁷³ Complaints-Assisted Form, 02 March 2019, at 2-4, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019); Affidavit Addendum to CID Case No. 19-C-142, 27 August 2019, Annex A, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019); Affidavit Addendum to CID Case No. 19-C-142, 27 August 2019, Annex B, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

cancellation or inappropriate statements, do not remove the situation from its legitimate purpose of transacting or booking a ride.

While the driver's use of profanity may result in violations of other laws as against him, given its jurisdiction, the Commission limits its disposition of the case to the issues raised by MLF against Grab Philippines and its obligations under the DPA.

The Commission finds that, in relation to the obligations of Grab Philippines under the DPA, Grab Philippines did not commit any privacy violation because these exchanges remain within the legitimate purpose consented to by MLF. As such, the driver's profanity continues to be within the context of the whole general purpose of the communication to fulfill a Grab ride transaction, especially since the exchanges were made only within Grab Philippines' app and in the process of discussing the details of the booking. The utterance of a foul statement does not, by itself, place it outside of the original legitimate purpose from which it stemmed. In effect, contrary to MLF's claim, the in-app chat and the messages exchanged therein never ceased to be for the purpose of coordinating a ride. Therefore, the exchanges continue to be for the legitimate purpose of transacting official business.

Given that the exchanges in the in-app chat module relating to foul language and cancellations are still within Grab Philippines' legitimate purpose, there is no privacy violation in this case. As such, it should be dismissed pursuant to Section 12 (b), Rule III of NPC Circular No. 16-04.

II. There is no violation of Section 28 or the Processing of Personal or Sensitive Personal Information for Unauthorized Purposes.

MLF roots his complaint in Section 28 of the DPA.⁷⁴ Section 28 or the Processing of Personal or Sensitive Personal Information for Unauthorized Purposes requires the concurrence of the following elements:

1. a person processed information of the data subject;
2. the information processed is classified as personal or sensitive personal information;

⁷⁴ Complaints-Assisted Form, 02 March 2019, at 3, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

3. the person processing the information obtained consent of the data subject or is granted authority under the DPA or existing laws; and
4. the processing of personal or sensitive personal information is for a **purpose that is neither covered by the authority given by the data subject and could not have been reasonably foreseen by the data subject nor otherwise authorized** by the DPA or existing laws.⁷⁵

The first three (3) requisites are present in this case.

Section 3 of the DPA defines personal information and processing as follows:

Section 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

...

(g) Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

...

(j) Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.⁷⁶

Given the foregoing, the first and second requisites are met.

The DPA defines a Personal Information Controller (PIC) as a “person or organization who **controls the collection, holding, processing or use** of personal information, including a person or organization who instructs another person or organization to collect,

⁷⁵ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 28 (2012). Emphasis supplied.

⁷⁶ *Id.* § 3 (g) & (j).

hold, process, use, transfer or disclose personal information on his or her behalf.”⁷⁷

The Terms of Use for Philippines GrabCar Passengers specifically provides the following:

10. Personal Data Protection

You agree and consent to the **Company using and processing your Personal Data** for the Purpose and in the manner as identified hereunder.

...

The **Company may use and process your Personal Data** for business and activities of the Company which shall include, without limitation[,] the following (the “Purpose”):

- To perform the Company’s obligations in respect of any contract entered with you;
- To provide you with any services pursuant to the Terms of Use herein;

...

- Process, manage or verify your application for the Service pursuant to the Terms of Use herein;
- To validate and/or process payments pursuant to the Terms of Use herein;

...

- To communicate with you for any of the purposes listed herein;

...

- To share your Personal Data amongst the companies within the Company’s group of companies comprising the subsidiaries, associate companies and or jointly controlled entities of the holding company of the group (the “Group”) and with the Company’s and Group’s agents, third party providers, developers, advertisers, partners, event companies or sponsors who may communicate with you for any reasons whatsoever.⁷⁸

⁷⁷ *Id.* § 3 (h). Emphasis supplied.

⁷⁸ Comment to Complaint dated 02 March 2019 and Affidavit Addendum dated 27 August 2019, 09 September 2019, Annex J, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019). Emphasis supplied.

Based on the foregoing, Grab Philippines is a PIC because it collects, processes, and retains personal data of the passenger before and after booking a ride. Prior to booking a ride transaction, the passenger uses a “mobile application supplied to [him] by the [Grab Philippines] Company[.]”⁷⁹ In the course of booking a ride, it processes personal information in order to “perform the Company’s obligation” and provide the passenger “with any services.”⁸⁰ It also determines what information will be shared to its drivers and provides the means to allow the passenger to coordinate with the driver through its in-app chat module.⁸¹

Thus, Grab Philippines, as the PIC, processed the personal information of MLF, particularly his mobile number and name, in order to connect him to its drivers.

As for the third requisite, it is fulfilled pursuant to the following admissions of MLF stating that he consented to Grab Philippines’ Terms and Conditions for the purpose of transacting a ride so that he and the driver can communicate with each other:

Both Mobile Number and Chat function are made **available with my consent** under their terms and condition for the purpose of transacting a ride. So that driver and rider can communicate to meet each other.⁸²

Based on their Terms and Condition, **I am providing Grab [c]onsent** to process and share my Personal Data to their partners (Driver) for the purpose of transacting a trip/ride. [...] There is negligence in [sic] Grab’s part of handling my personal data based on Terms and Condition **that I agreed on** [sic].⁸³

This includes providing the partner or driver access to the chat, call and sms facility **which [...] I provided consent to for official business.**⁸⁴

The fourth requisite, however, is lacking.

⁷⁹ *Id.* Annex J.

⁸⁰ *Id.* Annex J.

⁸¹ Complaints-Assisted Form, 02 March 2019, at 2-3, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019).

⁸² *Id.* Emphasis supplied.

⁸³ Affidavit Addendum to CID Case No. 19-C-142, 27 August 2019, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019). Emphasis supplied.

⁸⁴ Compliance to Order dated 13 August 2019, 28 August 2019, Annex B, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019). Emphasis supplied.

In processing of personal information for unauthorized purposes, the person processing the information either obtained the data subject's consent or is authorized for a declared and specific purpose under the DPA or any existing laws. The processing becomes unlawful, however, when the information is processed for a different purpose that is neither covered by the authority obtained from the data subject or could not have been reasonably foreseen by the data subject or otherwise authorized under the DPA or any existing law.

As mentioned in MLF's Affidavit Addendum, he himself admitted that he is "providing Grab [c]onsent to process and share [his] Personal Data to their partners (Driver) for the purpose of transacting a trip/ride."⁸⁵ To reiterate the above discussion, the conversation between MLF and the driver continues to be within the context of transacting for a Grab ride. Therefore, the exchanges, in relation to Grab Philippines' obligations under the DPA, are still within official business and legitimate purpose consented to by MLF.

Grab Philippines did not process MLF's personal information for a different purpose that is neither covered by the authority given by him nor otherwise authorized by the DPA or existing laws. The processing of MLF's information remains in accordance with Grab Philippines' legitimate purpose of enabling communications between the driver and the passenger to facilitate the transaction of a Grab ride.

Given that the processing of MLF's personal information did not go beyond what he consented, it being within the ambit of the declared and specified purpose, the Commission finds that Grab Philippines did not violate Section 28 of the DPA.

WHEREFORE, premises considered, this Commission resolves that the case filed by MLF against MyTaxi.Ph Corporation is hereby **DISMISSED**.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases before any other forum or tribunal, if any.

SO ORDERED.

⁸⁵ Affidavit Addendum to CID Case No. 19-C-142, 27 August 2019, *in* MLF v. MyTaxi.Ph Corporation, NPC Case No. 19-142 (NPC 2019). Emphasis supplied.

City of Pasay,
Philippines. 31 March
2022.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

MLF
Complainant

MYTAXI.PH CORPORATION
Respondent

QUISUMBING TORRES
Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

JGO,

Complainant,

-versus-

**FYNAMICS LENDING, INC.,
(PONDO PESO)**

Respondents.

NPC 19-187

For: Violation of the
Data
Privacy Act

X-----X

DECISION

NAGA, D.P.C.:

This refers to the complaint filed by JGO (Complainant) against Fynamics Lending, Inc. operating PondoPeso lending application (Respondent), regarding the unlawful processing, access to and disclosure of personal information of the Complainant.

Facts

Complainant alleged in his complaint that he was unable to pay on time his loan with the Respondent due to a personal financial crisis. Complainant also alleged that three (3) days after he defaulted on his payment, the Respondent's agents informed the contacts in the Complainant's phonebook that he has an outstanding loan with the Respondent. Further, Respondent's agents also threatened one of his friends over his unpaid loan and insinuated that the Complainant appointed him to be his reference, even if such appointment was never been made.

On 21 May 2019, parties were ordered to appear for a summary hearing in view of the temporary ban sought by the Complainant. The Respondent asked for continuance of summary hearing due to lack of material time.

On 07 June 2019, the next summary hearing was conducted. Only the counsel for Respondent appeared. During the hearing, Respondent manifested that they were able to amicably settle the case with the Complainant. As such, they were ordered by the Complaints and Investigation Division (CID) to submit the necessary pleadings to recognize and verify the settlement between the parties.

On 10 June 2019, this Commission received the notice of appearance and omnibus motion of the Respondent with copy of waiver, quitclaim and release (Quitclaim) signed by the Complainant. However, no competent proof of identity of the Complainant was attached to the Quitclaim.

On 30 July 2019, the parties were ordered to appear to confirm the submission. Unfortunately, both parties failed to appear on the said date.

On 11 September 2019, the parties were ordered to appear to confer for discovery. Only the Complainant appeared, and he then attested to the investigating officer that he voluntarily and knowingly executed the subject Quitclaim.

On 03 March 2020, the CID submitted the case to the Commission for its resolution.

Discussion

This Commission finds that the submitted Quitclaim was sufficiently and diligently confirmed by the investigating officer. Complainant personally appeared before the investigating officer to confirm that he knowingly, voluntarily, and willingly signed the Quitclaim.

In addition, Complainant submitted to this Commission a video file¹ on 12 March 2020, which shows that the Complainant, accompanied by the counsel for the Respondent, is reading the

¹ NPC 19-187 JGO v Fynamics Lending Inc (PondoPeso) Annex A

Quitclaim and stating that he is fully aware of the terms and consequences of entering into the agreement.

Further, seeing that the Quitclaim has no badges of fraud and deception; and that it was done in consideration of a sufficient settlement consideration; and its provisions are not contrary to law, public order, public policy, morals or good customs, or prejudicial to a third person then the Quitclaim shall be treated as a voluntary agreement between the parties to settle the instant case.

As ruled by the Supreme Court in *Arlo Aluminum Inc., v. Vicente Pinon, et. al.*², “But where it is shown that the person making the waiver did so **voluntarily, with full understanding of what he was doing**, and the **consideration for the quitclaim is sufficient and reasonable**, the transaction must be recognized as a valid and binding undertaking.” (Emphasis Supplied)

WHEREFORE, premises considered, this Commission resolves that the instant Complaint filed by JGO case be **DISMISSED**.

SO ORDERED.

Pasay City, Philippines;
18 June 2020.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

JGO
Complainant

GQLO
Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

GJJ,

Complainant,

-versus-

**CREDITABLE LENDING
CORPORATION (EASY PESO),**
Respondent.

X-----X

NPC 19-465

(Formerly CID
Case No. 19-G-
465)

For: Violation of
the Data Privacy
Act of 2012

DECISION

AGUIRRE, D.P.C.;

Before this Commission is a Complaint filed by GJJ against Creditable Lending Corporation (Easy Peso) for an alleged violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

On 23 July 2019, GJJ, in her Complaints-Assisted Form, alleged that Easy Peso committed violations of the DPA.¹ She described that, “they are hacker, they are scammer, they violate the civil law (shaming/threatening) they are lending sharks, they are not registered in SEC/or any gov’t agency.”² She was made aware of Easy Peso’s acts involving her “personal data, contacts, social media, [and] phone data” through “friends/relatives” and, as a result, she felt “shamed and threatened.”³

On 20 August 2019, the parties were ordered to appear for discovery conference.⁴ GJJ, however, failed to appear.⁵ The discovery conference, therefore, was rescheduled to 26 September 2019.⁶

¹ Complaints-Assisted Form, 23 July 2019, at 3, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

² *Id.*

³ *Id.* at 5-6.

⁴ Order to Confer For Discovery, 23 July 2019, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

⁵ Attendance Sheet for Discovery Conference, 20 August 2019, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19- 465 (NPC 2019).

⁶ Order, 20 August 2019, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

At the discovery conference, Easy Peso manifested that “the contents of the text messages sent to complainant and her phone book contacts; [and] the numbers of the senders” be produced to determine if the mobile numbers used were traceable to itself.⁷

On 07 October 2019, the Commission received an email from GJJ containing screenshots of text messages from Easy Peso that were allegedly sent to her contacts.⁸ It is comprised of five (5) screenshots, four (4) of which were sent to the number “0923 082 0350,” and another to a certain “NN.”⁹ The messages sent to “0923 082 0350” are all related to debt collection and, from the contents of the messages themselves, appear to have been sent to the mobile number of GJJ:¹⁰

[...] naman po ang iyong ginagawa. Dahil dito kami ay nagbibigay sa iyo ng huling paalala na bayaran mo ang iyong overdue, dahil kung hindi ay magsasampa kami ng small claim at amin ng kokontakin and iyong kompanyang pinagtratrabahuhan na magresulta sa mas malaking alalahanin sa darating na araw. EASY-PESO LENDING CORPORATION.¹¹

Sa kabila ng aming patuloy na paalala sa iyo na bayaran ang iyong overdue, ay wala pa rin kaming natatanggap na anumang kabayaran sa iyong pagkaka utang. Kung paano namin pinapahalagahan ang aming relasyon sa iyo bilang aming kliyente ay kabaliktaran naman po ang iyong ginagawa. Dahil dito kami ay nagbibigay sa iyo ng huling paalala na bayaran mo ang iyong overdue, dahil kung hindi ay magsasampa kami ng small claim at amin ng kokontaking ang iyong kompanyang pinagtratrabahuhan na magresulta sa mas malaking alalahanin sa darating na araw. EASY-PESO LENDING CORPORATION.¹²

Attention!!! Wala kaming nakikitang payment sa iyong Easypeso Lending account. Wala na din kaming magagawa kundi humingi ng tulong at iakyat sa iyong Barangay ang iyong kaso. Kayo din ang mahihirapan sa laki ng abala dahil lang sa hindi mo pagbabayad ng maayos. As a result, mahihirapan ka ng mag loan sa ibang Credit and Lending companies at possible na magka-record ka pa sa NBI. Contact us if you wish to clear your name. Easypeso Collection.¹³

⁷ Order, 26 September 2019, in GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

⁸ Bill of Particulars, 07 October 2019, at 1-5, in GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

⁹ *Id.*

¹⁰ Fact-Finding Report, 09 February 2022, at 6, in GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

¹¹ Bill of Particulars, 07 October 2019, at 1, in GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

¹² *Id.*

¹³ *Id.* at 1-3.

MAGANDANG GABI!! TAPOS NA ANG PALUGIT NA IBINIGAY SAYO NI EASY PESO! PANAHOON NA PARA KAMI NAMAN ANG GUMAWA NG HAKBANG PARA MAKABAYAD KAYO!¹⁴

SA ANIM NA ARAW NA PAGSASAWALANGBAHALA NINYO SA INYONG PAGKAKAUTANG KAY EASY PESO! HIHINGE NA KAMI NG TULONG SA INYONG MGA KAKILALA UPANG KAYO AY MAKABAYAD! MARAMING SALAMAT PO!¹⁵

The screenshot of the message supposedly sent to a certain NN, which she forwarded to GJJ, states:

Good day! Kindly inform Ms. GJJ regarding her loan in EASYPESO to settle the account immediately. If she keeps on refusing to repay her obligation in the company we will file a civil case against her from [sic] running away from her loan. Thank you.¹⁶

As a response, GJJ told NN to block Easy Peso and stressed that she had done the same, stating, “*Pablock nyan ta. Nareport ko na yan. Hack phone ko na isa.*”¹⁷

On 15 October 2019, Easy Peso submitted its Responsive Comment.¹⁸ It alleged that according to its investigation, GJJ’s account has been overdue for one hundred forty-four (144) days.¹⁹ Hence, it argued that “what she have [sic] attached is what we think reasonable to collect the repayment. We are not tolerating any indecent moves of our employee collector/agent.”²⁰ More importantly, Easy Peso alleged that GJJ gave consent to access her contact lists:

It is also disclosed that we asked for two to five (2-5) character references in the event that we cannot contact her. Based on Republic Act No. 3765, otherwise known as Truth in Lending Act, the company observes the disclosure requirements as it being read by the clients/customers by **clicking “agree” prior to claiming the loan proceeds** at our accredited merchant partners branch of her choice. As it is operated online, systems generated loan [a]greement is provided, copy attached herein [...]. The said procedures will best answer her queries as **she allowed us to**

¹⁴ *Id.* at 4.

¹⁵ *Id.* at 5.

¹⁶ *Id.* at 2.

¹⁷ Bill of Particulars, 07 October 2019, at 2, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

¹⁸ Answer to Complaint, 15 October 2019, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

¹⁹ *Id.*

²⁰ *Id.* OPC_ADJU_DCSN-V1.0,R0.0, 05 May 2021

access her contact lists. The complainant is advised to review the said procedures to help her clarify her complaint, as **we cannot access her contacts without her permission.**²¹

Lastly, Easy Peso interposed that, “[h]ad she reached our customer service mobile number at 09664171884 which is known to her, we should had [sic] addressed her problem without involving your good office[.]”²²

On 15 November 2021, the Commission mandated the responsible officers of Easy Peso to file a Verified Comment within fifteen (15) calendar days from receipt of the Order.²³

On 03 December 2021, Easy Peso, in its Reply with Motion to Dismiss, argued that the Complaint should be dismissed on the following grounds:

1. The Complainant, failed to establish the proof of authenticity of the evidence during the conference.
2. That it is against Respondent company’s policy to establish any other person other than those that the complainant consented to.
3. That there is insufficient information to substantiate the allegations in the complaint, and that evidence showing that the Respondent did contact all in her contact list, other than those voluntary provided, should have been presented.
4. That a condition precedent for filing the claim has not been complied with.
5. That the National Privacy Commission’s [C]ircular no. 16-04 Rules of Procedure of the National Privacy Commission Rule II, sec. 4 a, b, and c, states in pertinent parts that:
 - a. the complainant has informed in writing, the personal information controller or concerned entity of the privacy violation or personal data breach to allow the appropriate action on the same;

. . .

The National Privacy Commission may waive any or all the requirements of this Section, as [sic] its discretion upon good cause shown, or if the complainant involves a serious violation or breach of the Data Privacy Act, taking into account the risk or harm to the affected data subject.

²¹ *Id.* Emphasis supplied.

²² *Id.*

²³ Order to Comment, 15 November 2021, in *GJJ v. Creditable Lending Corporation*, NPC Case No. 19-465 (NPC 2019).

6. Additionally, complainant failed to provide supporting documents that show the violation of Data Privacy Act or related issuances; or the acts or omissions allegedly committed by the respondent amounting to a privacy violation or personal data breach as stated in the circular no. 16-04 Rules of Procedure of the National Privacy Commission Rule !! [sic] Section 10.
7. The Complainant has not communicated to us prior to filing of this complaint.

...

9. The respondent has no data on file, beginning last quarter of 2020, the company has decided to temporary stop the operations due to severe losses and condoned all the debts outstanding on all clients.²⁴

Issues

- I. Whether the case should be dismissed on procedural grounds for GJJ's failure to give Easy Peso an opportunity to address the Complaint; and
- II. Whether Easy Peso committed a violation of the Data Privacy Act that warrants recommendation for prosecution.

Discussion

- I. **The case should not be dismissed outright despite GJJ's failure to afford Easy Peso the opportunity to address the Complaint.**

Easy Peso alleged that GJJ did not provide it with an opportunity to address her Complaint.²⁵ As a result, it argued that the Commission should dismiss the case pursuant to Rule II, Section 4 of NPC Circular No. 16-04 (Rules of Procedure),²⁶ which provides that:

Section 4. Exhaustion of remedies – No complaint shall be entertained unless:

²⁴ Reply with Motion to Dismiss, 03 December 2021, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

²⁵ Answer to Complaint, 15 October 2019, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

²⁶ Reply with Motion to Dismiss, 03 December 2021, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

- a. The complainant has informed, in writing, the personal information controller or concerned entity of the privacy violation or personal data breach appropriate action on the same[.]²⁷

The same section, however, gives the Commission the discretion to waive any conditions precedent enumerated therein:

Section 4. Exhaustion of remedies –

. . .

The **National Privacy Commission may waive any or all of the requirements of this Section, at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act**, taking into account the risk of harm to the affected data subject.²⁸

In this case, the Complaint contains allegations regarding Easy Peso’s purported unauthorized processing of GJJ’s personal data,²⁹ through the sending of unwarranted texts that disclose details of her unpaid loan obligation to members of her contact list. The allegations, assuming they are true, directly contravene specific portions of the DPA and its related laws. Further, it exposes the data subject herein, as well as other data subjects whose personal information is processed by Easy Peso, to a real risk of serious harm. These allegations, therefore, serve as sufficient basis to give the Complaint due course and not dismiss it on its face.

II. Easy Peso did not commit a violation of the DPA that warrants a recommendation for prosecution.

A. GJJ did not overcome the burden of proof necessary to shift the burden of evidence to Easy Peso.

In administrative proceedings, such as this case, it is the complainant who carries the burden of proving her allegations in the complaint with substantial evidence or such “relevant evidence that a reasonable mind might accept as adequate to support a conclusion.”³⁰

²⁷ National Privacy Commission, Rules on Procedure of the National Privacy Commission, Circular No. 04, Series of 2016 [NPC Circular No. 16-04], § 4 (a) (15 December 2016).

²⁸ *Id.* Emphasis supplied.

²⁹ Complaints-Assisted Form, 23 July 2019, at 5, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

³⁰ Office of the Ombudsman v. Loving F. Fetalvero, Jr., G.R. No. 211450 (2018).

Section 1, Rule 131 of the 2019 Amendments to the Revised Rules on Evidence distinguishes between burden of proof and burden of evidence:

Section 1. *Burden of proof and burden of evidence.* - Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim or defense by the amount of evidence required by law. **Burden of proof never shifts.**

Burden of evidence is the duty of a party to present evidence sufficient to establish or rebut a fact in issue to establish a *prima facie* case. **Burden of evidence may shift** from one party to the other in the course of the proceedings, depending on the exigencies of the case.³¹

Thus, it is the party who alleges a fact that has the burden of proving it. Allegations alone do not constitute evidence since “self-serving assertion[s] cannot be given credence.”³²

Accordingly, the screenshots used by GJJ to substantiate her claims are insufficient. She alleges that she learned of the incident from her “friends/relatives,”³³ and alluded to certain messages sent by Easy Peso to her contacts. She did not, however, provide copies of these alleged messages. Nor did she submit any form of supporting evidence, such as affidavits from her friends and relatives, attesting to the fact that they received messages from Easy Peso. Instead, GJJ only provided four (4) screenshots containing text messages sent to a number that, based on the contents of the messages themselves, is seemingly hers.³⁴

She also attached the screenshot of a message supposedly forwarded to her by NN without showing the actual message supposedly received by NN from Easy Peso. She merely submitted these screenshots without the slightest explanation of the surrounding circumstances. GJJ also failed to categorically state that these people supposedly contacted are not included in the list of two (2) to five (5) character references she was supposedly required to provide Easy

³¹ 2019 AMENDMENT TO THE 1989 REVISED RULES ON EVIDENCE, A.M. No. 19-08-15-SC, Rule 131, §1 (1 May 2020). Emphasis supplied.

³² Tze Sun Wong v. Kenny Wong, G.R. No. 180364 (2014).

³³ Complaints-Assisted Form, 23 July 2019, at 5, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

³⁴ See Bill of Particulars, 07 October 2019, at 1 & 3-5, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

Peso in case she can no longer be reached such that the act of Easy Peso in contacting them already went beyond the consent she gave.³⁵

In effect, she was not able to create a *prima facie* case, since she did not

(1) identify the recipients of the messages and have those recipients affirm that they actually received the messages; (2) disclose the mobile number that sent the messages; (3) and, as regards, “NN,” establish with certainty that NN actually received a message from Easy Peso.

GJJ failed to categorically show that the mobile number used to contact the recipients belongs to Easy Peso. Nor did she offer any other proof of the existence of messages supposedly sent by Easy Peso to third parties outside her nominated character references. She also failed to refute Easy Peso’s allegation that she nominated two (2) to five (5) character references.³⁶ By the same token, she was not able to establish that the recipients of the alleged messages were not her character references.

Aside from these unsubstantiated screenshots, the Commission stresses that the message NN sent to GJJ cannot be validated as coming from Easy Peso. It does not show from whom the message originated since it is a mere forwarded text. Essentially, she failed to show proof of the actual message allegedly sent by Easy Peso to “NN.”

The Rules on Electronic Evidence, which applies to administrative proceedings,³⁷ states that:

Section 1. Audio, video and similar evidence. – Audio, photographic and video evidence of events, acts or transactions shall be admissible provided is shall be shown, presented or displayed to the court and shall be **identified, explained or authenticated by the person who made the recording or by some other person competent to testify on the accuracy** thereof.

Section. 2. Ephemeral electronic communication. – Ephemeral electronic communications shall be proven by the testimony of a person who was a party to the same or has personal knowledge thereof. In the absence or unavailability of such witnesses, other competent evidence may be admitted.

³⁵See Answer to Complaint, 15 October 2019, in *GJJ v. Creditable Lending Corporation*, NPC Case No. 19-465 (NPC 2019).

³⁶ *Id.*

³⁷ RULES ON ELECTRONIC EVIDENCE, A.M. No. 01-7-01-SC, Rule 1, §2 (July 2001).

A **recording of the telephone conversation or ephemeral electronic communication shall be covered by the immediately preceding section.**³⁸

It further provides for the method of proof:

Section 1. Affidavit of evidence. – All matters relating to the admissibility and evidentiary weight of an electronic document may be **established by an affidavit** stating facts of direct personal knowledge of the affiant or based on authentic records. The affidavit must affirmatively show the competence of the affiant to testify on the matters contained therein.³⁹

Given the foregoing, it is clear that the submission of screenshots alone, without an affidavit authenticating and explaining its contents as well as the competence of the affiant to testify on such matters, does not pass the requirement of admissibility.

Moreover, the Supreme Court has held that “to satisfy the substantial evidence requirement for administrative cases, **hearsay evidence should necessarily be supplemented and corroborated by other evidence that are not hearsay.**”⁴⁰ Evidently, GJJ’s act of attaching the unsubstantiated screenshots in and of itself, without any supporting affidavits attesting to its contents, is not enough to discharge the burden of proof. To establish her claim, it is necessary for the friends and relatives who allegedly received messages from Easy Peso to give statements corroborating any screenshot she presents. Thus, even assuming that GJJ presented the actual message received by “NN,” it is still necessary that it be authenticated in an affidavit in order to be given evidentiary weight.

Therefore, absent any other supplementing evidence, the screenshots continue to be hearsay.

The Commission notes, however, that Easy Peso could have conveniently disclosed and presented GJJ’s alleged chosen character references which could have sufficiently established that the mobile numbers contacted were only those that were validly nominated.

³⁸ *Id.* Rule 11, §1-2 (July 2001). Emphasis supplied.

³⁹ *Id.* Rule 9, §1 (July 2001). Emphasis supplied.

⁴⁰ Re: Letter of Lucena Ofendo Reyes Alleging Illicit Activities Of A Certain Atty. Cajayon Involving Cases In The Court Of Appeals, Cagayan De Oro City, A.M. No. 16-12-03-CA (2017). Emphasis supplied.

Nevertheless, as previously discussed, the burden of evidence did not shift to it and the Commission cannot recommend the criminal prosecution of the responsible officers of Easy Peso based on the weakness of their defense.⁴¹

Ultimately, it is GJJ that bears the burden of proving the allegations in her Complaint with substantial evidence. Jurisprudence is settled that if she “fail[s] to show in a satisfactory manner the facts upon which [her] claims are based, the [respondent is] **not obliged** to prove [its] exception or defense.”⁴²

The Commission, therefore, is left without any basis to recommend Easy Peso for prosecution under the DPA considering it is bound to adjudicate based on the following:

Section 22. *Rendition of decision.* – The Decision of the Commission shall adjudicate the issues raised in the complaint **on the basis of all the evidence presented** and its own consideration of the law.⁴³

As such, the Commission finds that the evidence presented is insufficient to support the claims of GJJ that Easy Peso violated the DPA.

B. Easy Peso did not violate Section 25 of the DPA.

Section 25 of the DPA or Unauthorized Processing of Personal or Sensitive Personal Information is committed when the following requisites concur:

1. The perpetrator processed the information of the data subject;
2. The information processed was personal information or sensitive personal information; and
3. The processing was done without the consent of the data subject, or without being authorized under the DPA or any existing law.⁴⁴

Section 3 of the DPA defines personal information and processing as follows:

⁴¹ See *People of the Philippines v. Sangcajo, Jr.*, G.R. No. 229204 (2018).

⁴² Re: Letter of Lucena Ofendo Reyes Alleging Illicit Activities Of A Certain Atty. Cajayon Involving Cases In The Court Of Appeals, Cagayan De Oro City, A.M. No. 16-12-03-CA (2017). Emphasis supplied.

⁴³ NPC Circular No. 16-04, § 22. Emphasis supplied.

⁴⁴ NPC 19-134, 10 December 2021, at 12 (NPC 2021) (unreported).

(g). Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

...

(j) Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.⁴⁵

Given the foregoing, the first and second requisites are met. Easy Peso processed the personal information of GJJ, particularly her name and number, when it allegedly collected, stored, and sent text messages to the people in her contact list regarding her loan.

The third requisite, however, is absent.

Personal information may be processed when it is for a legitimate interest. Section 12(f) of the DPA provides:

Section. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

...

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

⁴⁵ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (g) & (j) (2012).

Here, Easy Peso alleged in its Responsive Comment that GJJ's account, which had an original term of only fourteen (14) days, was already one hundred forty-four (144) days overdue.⁴⁶ Moreover, it argued that it "asked for two to five (2-5) character references in the event that we cannot contact her."⁴⁷ GJJ did not refute these allegations. Additionally, her submitted screenshots show that she had blocked all the collection messages sent to her.⁴⁸

As previously discussed, Easy Peso requires its clients to click "Agree" before claiming the loan proceeds at accredited merchant partner branches.⁴⁹ With this, the Privacy Policy submitted by Easy Peso in its Responsive Comment explicitly states:

In order to assess your loan credit, we will obtain your following information for approval of your application or getting a higher loan amount and longer terms. We commit that the data will be saved and encrypted, and only be used for borrowing money from our platform

. . .

Communication information: **contacts, just in case you can't be reached for credit investigation for applying a loan or other situations.**⁵⁰

It is clear from Easy Peso's Privacy Policy that it may process a client's contacts if she cannot be reached or located. This fact was never refuted by GJJ.

The screenshots of the messages contain the "restore to messages," "add to whitelist," and "delete" options, which clearly demonstrate that GJJ has already blocked the number and messages from Easy Peso.⁵¹ She even instructed her NN to block the same and admitted that she has done so, claiming that, "[n]areport ko na yan."⁵² Furthermore, the screenshots reveal that she has not replied, even once, to Easy Peso's collection reminders.⁵³ Additionally, a perusal of

⁴⁶ Answer to Complaint, 15 October 2019, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

⁴⁷ *Id.*; See also Reply with Motion to Dismiss, 03 December 2021, Annex "A" at 1, 3-4, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

⁴⁸ Bill of Particulars, 07 October 2019, at 3-5, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

⁴⁹ Answer to Complaint, 15 October 2019, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).
⁵⁰ Answer to Complaint, 15 October 2019, Annex "D", *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019). Emphasis supplied.

⁵¹ Bill of Particulars, 07 October 2019, at 3-5, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

⁵² *Id.* at 2 Emphasis supplied.

⁵³ *Id.* at 1.

these same screenshots confirm that Easy Peso was merely following up on her outstanding loan obligation:

*[K]ami ay nagbibigay sa iyo ng huling paalala na bayaran mo ang iyong overdue [...]*⁵⁴

*Sa kabila ng aming patuloy na paalala sa iyo na bayaran ang iyong overdue [...]*⁵⁵

Kindly inform GJJ regarding her loan in EASYPESO to settle the account immediately.⁵⁶

The totality of GJJ's actions demonstrates that she is, in fact, avoiding Easy Peso. Given that the clause in the Privacy Policy states that it may use contacts when the client cannot be reached,⁵⁷ Easy Peso merely enforced the obligations stipulated in the contract it entered into with GJJ. Thus, it has a legitimate reason to undertake the processing of her contacts. A lending company has legitimate interests in collecting outstanding obligations due to it. Considering that GJJ failed to refute the defenses raised by Easy Peso despite being given the opportunity to do so, it can be said that Easy Peso's act of getting in touch with presumably valid character references that GJJ herself nominated is necessary for its legitimate interest.

Also, it should be taken into consideration that, during this time, NPC Circular No. 20-01 (Guidelines on the Processing of Personal Data for Loan-Related Transactions) stating that, "[a]ccess to contact details in whatever form, such as but not limited to phone contact list [...] and/or copying or otherwise saving these contacts for use in debt collection or to harass in any way the borrower or his/her contacts, are prohibited,"⁵⁸ had not yet taken effect. In the absence of the Circular, it cannot be said that Easy Peso's act of reaching out to GJJ's contacts is violative of the DPA. Easy Peso did not go beyond what it informed GJJ it would do since its actions merely executed what was purportedly in the Privacy Policy.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.* at 2.

⁵⁷ Answer to Complaint, 15 October 2019, Annex "D", in *GJJ v. Creditable Lending Corporation*, NPC Case No. 19-465 (NPC 2019).

⁵⁸ National Privacy Commission, Guidelines on the Processing of Personal Data for Loan-Related Transactions, Circular No. 01, Series of 2020 [NPC Circ. No. 20-01], § 3 (D)(4) (28 January 2021).

GJJ was not able to sufficiently establish that Easy Peso went beyond the terms disclosed to her when she availed herself of the loan. Consequently, absent the third requisite, it cannot be said that Easy Peso committed an act that would constitute unauthorized processing.

Jurisprudence reiterates that “contracts of adhesion are not invalid *per se*; they are not entirely prohibited. The one who adheres to the contract is in reality free to reject it entirely; if he adheres, he gives his consent.”⁵⁹ Thus, “a contract duly executed is the law between the parties, and they are obliged to comply fully and not selectively with its terms. A **contract of adhesion is no exception.**”⁶⁰

As regards contracts, the Supreme Court has also stressed that:

[I]t must be emphasized that a **party to a contract cannot deny its validity after enjoying its benefits** without outrage to one's sense of justice and fairness. Where parties have entered into a well- defined contractual relationship, it is imperative that they should honor and adhere to their rights and obligations as stated in their contracts because obligations arising from it have the force of law between the contracting parties and should be complied with in good faith.

As a rule, a court in such a case has no alternative but to enforce the contractual stipulations in the manner they have been agreed upon and written. **Courts, whether trial or appellate, generally have no power to relieve parties from obligations voluntarily assumed simply because their contract turned out to be disastrous or unwise investments.**⁶¹

Subject to the rights and obligations provided under the DPA, the Commission emphasizes that the DPA cannot be used to escape obligations validly and voluntarily entered into by the data subject. As such, Easy Peso did not commit unauthorized processing when it enforced its contractual obligations.

C. Given that no DPA violation exists, it is not necessary to discuss and establish participation or gross negligence of Easy Peso's officers.

⁵⁹ RCBC v. Court of Appeals, G.R. No. 133107 (1999).

⁶⁰ Avon Cosmetics, Inc. v. Luna, G.R. No. 153674 (2006). Emphasis supplied.

⁶¹ Development Bank of the Philippines. v. Court of Appeals, G.R. No. 13870 (2006). Emphasis supplied.

Easy Peso is incorporated and duly authorized by the Securities and Exchange Commission to operate as a lending company.⁶² As such, Section 34 of the DPA applies, which provides:

Section 34. *Extent of Liability.* – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, **who participated in, or by their gross negligence,** allowed the commission of the crime.⁶³

In this case, however, there is no DPA violation that has been established. Hence, it is not necessary to discuss whether Easy Peso's officers participated in the violation or are grossly negligent.

Taking into account the totality of the foregoing reasons, the Commission cannot recommend the prosecution of Easy Peso.

WHEREFORE, premises considered, this Commission resolves that the case filed by GJJ against Creditable Lending Corporation (Easy Peso) is hereby **DISMISSED** for lack of substantial evidence.

This is without prejudice to the filing of appropriate civil, criminal, or administrative cases, if any, against Creditable Lending Corporation (Easy Peso) before any other forum or tribunal.

SO ORDERED.

City of Pasay, Philippines.
03 March 2022.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

⁶² Certificate of Incorporation and Authority to Operate as a Lending Company, *in* GJJ v. Creditable Lending Corporation, NPC Case No. 19-465 (NPC 2019).

⁶³ Data Privacy Act of 2012, § 34 (2012). Emphasis supplied.

JOHN HENRY D. NAGA
Privacy Commissioner

Copy furnished:

GJJ
Complainant

CREDITABLE LENDING CORPORATION (EASY PESO)
Respondent

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

MPM ,

Complainant,

-versus-

NPC Case No. 19-569

(Formerly CID Case No. 19-G-569) For: Violation of the Data Privacy Act of 2012

PERA4U,

Respondent.

X-----X

DECISION

NAGA, D.P.C.:

Before this Commission is a Complaint by MPM (Complainant) against Pera4U (Respondent) for a violation of the Data Privacy Act of 2012 (DPA).

Facts of the Case

Complainant alleged that Respondent made several offensive calls to her to demand payment of her loan. She likewise alleged that Respondent called and sent text messages to her contact list disclosing her personal information, including the details about her unsettled obligation, viz:

“Tawag ng tawag para mangaway at maningil. Turuan ka pa nila na manghiram sa iba para mabayaran sila.¹

xxx

Sinabi po nila about my loan and kung magkano²”

As a result, Complainant’s colleagues knew of her unpaid loan with Respondent causing her embarrassment and to have sleepless

¹ Complaint-Assisted Form, page 3.

² Id. Page 4.

nights. The Complainant also applied for a temporary ban on the processing of personal data against the Respondent.

At the Discovery Conference set on 06 September 2019, both parties failed to appear. Hence, the Discovery Conference was reset on 03 December 2019.³

On 08 October 2019, the parties were ordered to appear for a Summary Hearing.⁴ On 15 October 2019, Complainant failed to appear. This prompted the Respondent to manifest to reset the Summary Hearing to another date.⁵ The request was granted, and the parties were ordered to appear for another summary hearing on 15 November 2019. However, Complainant still failed to appear.⁶

During the second Discovery Conference on 03 December 2019, both parties failed to appear.⁷ Respondent was then ordered to submit its Responsive Comment.

In Respondent's Responsive Comment, it contended that there is no good cause shown neither is there any violation or breach present in the instant case. It argued that Complainant merely alleged that they unlawfully accessed his contacts where in fact the Complainant consented to the same when he applied for his loan with Pera4U.⁸

Respondent further asserts that Complainant has given consent for them to access her contacts especially the reference contacts. It was even Complainant who provided the contact references to them. This information would be helpful to make sure that Complainant can be contacted in case of default on the obligation and if she refuses to answer their calls or reminders.⁹

Respondent denies the allegation of harassment and threat claiming that they have Quality Assurance in place to help prevent such incidents of harassment and threats from happening and Respondent has issued certain guidelines as to how each collecting agent must collect from its customers.¹⁰ Respondents also contended

³ Order dated 10 September 2019

⁴ Order for Summary Hearing dated 08 October 2019.

⁵ Order dated 15 October 2019.

⁶ Attendance Sheet for Summary Hearing dated 15 November 2019.

⁷ Attendance Sheet for Discovery Conference dated 03 December 2019.

⁸ Pera4u Comment, page 4 (18)

⁹ Id., page 7 (27)

¹⁰ Id., page 7 (30)

that the Complainant only made allegations that the Respondent threatened and harassed her and her contacts asking the Complainant to pay her obligations. No proof as to these allegations were presented.¹¹

Issue

Whether Respondent committed a violation of the Data Privacy Act.

Discussion

The Complaint lacks merit.

In the Complaint filed by Complainant, she plainly alleged the violations committed against her by Respondent. As Complainant described it, “*Tawag ng tawag para mangaway at maningil. Turuan ka pa nila na manghiram sa iba para mabayaran sila.*” However, nowhere in the said Complaint did Complainant stated the content of the message that caused her sleepless nights and embarrassment. She likewise failed to identify the receivers of the alleged text message that were sent by Respondent. Further, no proof was submitted to substantiate her claim. Lastly, Complainant failed to cite or refer to a specific provision of the DPA that was allegedly violated by the Respondent.

Despite several opportunities given to Complainant to prove her allegations at the two (2) Discovery Conferences scheduled on 06 September 2019 and 03 December 2019, Complainant still failed to appear without prior notice nor justification.

In consideration of the circumstances of this case, the Commission is bound to adjudicate in accordance with the provision of the NPC Circular 16-04 or the NPC Rules of Procedure, viz:

Section 22. Rendition of decision. – The Decision of the Commission shall adjudicate the issues raised in the

complaint **on the basis of all the evidence presented** and its own consideration of the law.¹²

As the Supreme Court held in *Government Service Insurance System v. Prudential Guarantee*, “it is basic in the rule of evidence that bare allegations, unsubstantiated by evidence, are not equivalent to proof. In short, mere allegations are not evidence.”¹³

Further, as held by the Supreme Court in the case of *Wong v. Wong*, “The rule is well-settled that he who alleges a fact has the burden of proving it and a mere allegation is not evidence. Thus, his self-serving assertion cannot be given credence.”¹⁴

Hence, bearing only allegations without any corresponding pieces of evidence to support Complainant’s claim that Respondent disclosed her personal information which includes the details about her unsettled obligation to her contact list, from which caused her sleepless night and embarrassment, cannot merit a favorable decision from this Commission.

The Complainant herein also prayed for the temporary ban on the processing of her personal data against the Respondent.¹⁵ The issuance of this is governed by the NPC Rules of Procedure which provides:

Section 19. *Temporary Ban on Processing Personal Data.* – At the commencement of the complaint or at any time before the decision of the National Privacy Commission becomes final, a complainant or any proper party may have the National Privacy Commission, acting through the investigating officer, impose a temporary ban on the processing of personal data, if on the basis of the evidence on record, such a ban is necessary in order to preserve the rights of the complainant or to protect national security or public interest.

a. A temporary ban on processing personal data may be granted only when: (1) the application in the complaint is verified and shows facts entitling the complainant to the relief demanded, or the respondent or respondents fail to appear or submit a responsive pleading within the time specified for within these Rules; xxx¹⁶

¹² NPC Circular No. 16-04 dated 15 December 2016 (“NPC Rules of Procedure”), Section 22. Emphasis supplied.

¹³ G.R. No. 165585, 20 November 2013, *citing* Real v. Belo, 542 Phil. 109 (2007).

¹⁴ G.R No. 180364, 03 December 2014.

¹⁵ Complaints-Assisted Form, p. 7.

¹⁶ *Supra* Note 11, at Section 19.

Considering that the Complainant failed to substantiate her allegations as already provided above, the application for temporary ban should likewise be denied by this Commission for lack of substantial evidence.

WHEREFORE, premises considered, the Complaint is hereby **DISMISSED** for lack of merit. This Commission also resolves to **DENY** the application for temporary ban on processing personal data filed by Complainant MPM.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against Respondent before any other forum or tribunal, if any.

SO ORDERED.

Pasay City, Philippines;
19 November 2020.

Sgd.

JOHN HENRY D. NAGA

Deputy Privacy Commissioner

WE CONCUR:

Sgd.

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

Sgd.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

COPY FURNISHED:

MPM

Complainant

PERA4U LENDING

Respondent

COMPLAINTS AND INVESTIGATION DIVISION

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

**IN RE: WEFUND LENDING
CORPORATION (JUANHAND) AND
ITS RESPONSIBLE OFFICERS**

NPC SS 21-006

For: Violation of
the Data Privacy
Act of 2012

INITIATED AS A *SUA SPONTE* NPC
INVESTIGATION ON THE
POSSIBLE DATA PRIVACY
VIOLATIONS COMMITTED BY
WEFUND LENDING CORPORATION
(JUANHAND)

X-----X

DECISION

AGUIRRE, D.P.C.;

Before this Commission is a Fact-Finding Report with Application for the Issuance of a Temporary Ban on the Processing of Personal Data (FFR) dated 09 June 2021 against Wefund Lending Corporation (JuanHand), the operator of the online lending application, JuanHand, and its responsible officers.

The Complaints and Investigation Division (CID) of the National Privacy Commission, pursuant to its power to conduct *sua sponte* investigations, filed an FFR against JuanHand. The FFR alleged that JuanHand committed violations of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) and the Commission's issuances. This concludes the *sua sponte* investigation conducted by the Commission.

Facts

On 09 June 2021, the CID submitted its FFR against JuanHand following numerous reports of continuing privacy violations committed by several online lending applications (OLAs).¹ The CID

¹ Fact-Finding Report, 09 June 2021, at 1, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

initiated a *sua sponte* investigation against JuanHand² pursuant to Section 7 of the DPA that mandates the Commission to institute investigations in cases it deems appropriate³ and NPC Circular 21-01 (2021 Rules of Procedure) that permits the NPC to initiate *sua sponte* investigations and file complaints for DPA violations.⁴ The FFR serves as the complaint, with the CID as the Nominal Complainant, in *sua sponte* investigations.⁵

In the CID's technical investigation, it downloaded JuanHand installer version v.3.7.1 from Google Play Store and simulated JuanHand's registration and loan application processes.⁶

The permissions required by the application (app) were outlined in Google Play Store prior to its download and installation:⁷

- read calendar events plus confidential information;
- add or modify calendar events and send email to guests without owner's knowledge;
- read your contacts;
- approximate location (network-based); and
- precise location (GPS and network-based).⁸

Upon the installation and opening of the app, it immediately asked for permission to access contacts, thus, the CID stressed that "the permission to access contacts was required upon installation of the application, even without a loan being applied for."⁹

During the CID's simulation, when the loan application form required character references, the app prompted the CID to: "[p]lease allow access to your contacts. This authorization will allow us to speed up your application process and prevent criminals from stealing your money."¹⁰ Thus, the notification for permission to access contacts appeared when the app was opened and when inputting of character references were asked in the loan application process.¹¹ The CID found

² *Id.*

³ *Id.* at 5.

⁴ *Id.*

⁵ *Id.*

⁶ *Id.* at 1.

⁷ Fact-Finding Report, 09 June 2021, at 2, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

⁸ Technical Report, 17 May 2021, at 5 (Annex B), *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

⁹ Fact-Finding Report, 09 June 2021, at 2, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022). Emphasis removed.

¹⁰ *Id.* Emphasis removed.

¹¹ *Id.*

that there was no manual way of entering a phone number and it must be done through giving access to the contact list.¹² Corollary, the loan application would not have progressed to the next step if the character references' phone numbers were not given.¹³

When the CID examined the source code of the app, it showed that the app utilized the Android software development kit (SDK) that provides coding for contacts retrieval, wherein an app will have the ability to collect data from contacts.¹⁴ The "AndroidManifest.xml" file explicitly contained a contacts permissions line as seen in the code "android.permissions.READ_CONTACTS".¹⁵ The CID explained that, when this is enabled, it gives an app the ability to read the user's phone contacts data.¹⁶

The CID also disclosed that "no Privacy Policy was found on both JuanHand's website and mobile application."¹⁷ It searched for JuanHand's Privacy Policy and instead found a link to the Service Agreement, which is "found only during the signup process in the [app] and the user will not be able to see or read the [S]ervice [A]greement again as there is no link of this agreement inside the application and no visible link on [JuanHand's] website."¹⁸

The Service Agreement provided for the following pertinent provisions:

[B. Limitation of Use]

[4. You agree to register with a username that does not to [sic] violate the laws and social ethics and provide your real information, and comply with the following requirements:]

[b].You must provide true, up-to-date, valid and complete information, and **grant Juanhand a permanent right to use the information you provide free-of-charge for the purpose of using Juanhand service.**

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ Fact-Finding Report, 09 June 2021, at 2, *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹⁶ *Id.*

¹⁷ *Id.* at 3.

¹⁸ *Id.*

[K. Privacy]

[2. Source of Information]

[b]. In addition to the information provided to Juanhand by the User voluntarily, User agrees that Juanhand and its partners to collect and verify the User's information, including, but not limited to the following manner:

iv. **information related to personal communication (including, but not limited to, contact list, geographical location, device identification number, social networking profiles)** provided or authorized by the User, or communication information relating to the activities and logging in by the User provided to Juanhand by other Users or third party, Juanhand can collect this information in the User's file.

[vi.] Juanhand will collect your Facebook platform information through your authorization. Including but not limited to: username, user ID, registered email, gender, etc.

[3. Use of Information]

[g]. I authorize the disclosure to and collection of my personal data from Third Party Entities ('Partners') engaged by Juanhand for the purposes stated under the heading Use of Personal Data. These Partners shall refer to my employer (for auto-debit or other auto-deduction mechanism) whether private or government, telecommunication companies (e.g., Globe Telecom, Inc., PLDT, Smart, Sun Cellular), utility companies (e.g., Meralco, Maynilad), government agencies (e.g., SSS, GSIS, NSO, BIR), credit bureaus (e.g., CIC, NFIS), remittance companies (e.g., Palawan Express, Cebuana Lhuillier, etc.), insurance providers (e.g., Sun Life Grepa Financial Inc., Insular Life, etc.), financial service providers (e.g., CC Mobile Financial Services Philippines, etc.), and other service providers. (2) I authorize Lending Company Inc. to share my personal data with Lending Company Inc.'s parent, affiliate, subsidiaries even after my loan with Lending Company Inc. is sold or assigned by it to another creditor for data analytics, determination of insurable interest and amount insured, statistical analysis and demographics, and business development purposes, and fraud detection and investigation.

[h.] I authorize Juanhand to process Mobile device data (e.g., mobile phone number/s, mobile phone message data, SIM, IMEI, or other device identifiers, type of device, device operating system, device settings, user account information for your mobile device or Google PlayStore account, information about mobile network provider, device specifications), **Location data (e.g., mobile device location, time zone setting); Phone data (e.g., contact lists, SMS metadata, types and nature of mobile**

applications found on your mobile device); mobile app usage data (e.g., traffic volume, mobile app usage) and telecommunications usage data or ‘telco usage score’.

[4. Disclosure of User’s Information by JuanHand]

[d.] When the Borrower is overdue for payment, Juanhand may publish the personal information of such user for the purpose of collecting debt. Juanhand shall not be held liable.

The Data Privacy Act (DPA) establishes that you have the following rights as a data subject:

- You have the right to indicate your refusal to the collection and processing of your personal data. You also have the right to be informed and to withhold your consent to further processing in case there are any changes or amendments to information given to you. Once you have notified us of the withholding of your consent, further processing of your personal data will no longer be done, unless (i) the processing is required pursuant to a subpoena, lawful order, or as required by law; or (ii) the collection and processing is pursuant to any lawful criteria indicated under the terms of this Policy.
- You have the right to reasonable access to your personal data. Furthermore, you have the right to limit and prevent disclosure of your personal data and to receive notification of any possible breaches of your personal data.
- You may also correct or remove any information that you think is inaccurate. You have the right to dispute any inaccuracy or error in your personal data. You may request for the correction or removal of any inaccuracy or error in your personal data by logging into your account or making a formal request with our Data Privacy Officer.
- You have the right to the destruction of your personal data;
- You have the right to damages; and
- You have the right to lodge a complaint with the National Privacy Commission (NPC).

If you would like to make any request in relation to your rights as a data subject, please contact our Data Protection Officer (‘DPO’) with the contact details listed below. **Please note that the exercise of some of your rights as a data subject is subject to review and may result in the denial of any application currently pending.**¹⁹

¹⁹ *Id.* at 3-4. Emphasis supplied; See Supplemental Report, 31 May 2021, Annex A (JuanHand User Agreement Web), *in re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

The CID, however, found through “JuanHand’s Permission Information,” that JuanHand’s system can do the following:

1. read the borrower’s calendar events plus confidential information;
2. add or modify calendar events;
3. send email to guests without the owner’s knowledge;
4. read borrower’s contacts;
5. collect data from contacts; and
6. pinpoint the borrower’s approximate and precise location through its network and GPS.²⁰

As can be gleaned from the Service Agreement and the permissions that CID discovered in its technical investigation, there are certain permissions that were not disclosed at all in the Service Agreement, particularly the ability to read and modify a borrower’s calendar events and confidential information.

Based on the foregoing, the CID argued that JuanHand violated the DPA and the Commission’s issuances.

First, the CID opined that the undisclosed permissions in JuanHand’s app violated Section 16 of the DPA.²¹ It found that:

The capabilities of JuanHand’s system to read the borrower’s calendar events plus confidential information, add or modify calendar events, send email to guests without the owner’s knowledge, read borrower’s contacts, collect data from contacts and pinpoint the borrower’s approximate and precise location through its network and GPS are all unknown to the prospective borrower. The **permission information [...] is not shown to the users thru [sic] prompts or permissions when applying for a loan but was discovered by the CID Technical Team from the Google Play Store and not from the application itself.**²²

Since JuanHand’s data subjects were not informed that their personal information have been processed, the CID argued that JuanHand violated Section 16 of the DPA, which states that a data subject is

²⁰ *Id.* at 4-5.

²¹ Fact-Finding Report, 09 June 2021, at 5, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

²² *Id.* Emphasis supplied.

entitled to “[b]e informed whether personal information pertaining to him or her shall be, are being or have been processed[.]”²³

Second, the CID asserted that JuanHand’s undisclosed permissions violated the general privacy principles of transparency, legitimate purpose, and proportionality.²⁴

The CID elaborated that pursuant to the transparency principle, a data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks involved.²⁵ It argued that JuanHand “has the duty to inform its data subjects, by clearly indicating in its privacy notice, the purpose/s for storage of the personal information they access.”²⁶ Related to this, the CID elucidated that “under NPC Circular 20-01, access is allowed for [OLA] provided [it] will use such information for [Know Your Customer (KYC)] purposes, after accomplishing such purpose, the OLA should have removed their access on the personal information it stored.”²⁷ Thus, the CID claimed that JuanHand violated the principle of transparency because the borrowers were not aware of the nature, extent, and risks involved in granting access to his contacts.²⁸ The app “failed to provide the purpose for the storage of the personal information accessed, and such cannot be seen in the [a]pp’s Privacy Notice nor can [it] be deduced from the permission it requires.”²⁹

As to the principles of proportionality and legitimate purpose, the CID contended that JuanHand violated these general privacy principles when it required access to borrowers’ contacts.³⁰

Legitimate purpose provides that “the processing of information shall be compatible with a declared and specified purpose, which must not be contrary to law, morals, or public policy.”³¹

²³ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 16 (2012).

²⁴ Fact-Finding Report, 09 June 2021, at 6, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

²⁵ *Id.*

²⁶ *Id.* at 7.

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.*

³⁰ Fact-Finding Report, 09 June 2021, at 7, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

³¹ National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (2016).

According to the CID's technical investigation, when the permission to access contacts is denied, a prompt is shown, stating: "Please allow access to your contacts. This authorization will allow us to speed up your application process and prevent criminals from stealing your money."³² Thus, it argued that, "[h]arvesting contacts and data of contacts are irrelevant, unnecessary and excessive in its declared purpose of speeding up the processing of loan applications and prevention of criminals from stealing money."³³

The CID further opined that "the legitimate purpose principle requires that the processing or [sic] personal information should meet one of the criteria for the lawful processing of information as provided in Sections 12 and 13 of the DPA[.]"³⁴ Valid consent or authority under the DPA and other existing laws is necessary for the processing to be authorized.³⁵ Given this, the CID alleged that JuanHand is without valid consent or authority under the DPA to process and store the borrowers' phone contacts, which is in violation of the abovementioned general privacy principles.³⁶

Third, the CID asserted that "Juan[H]and's requirement of having access to phone book contacts even before the processing of the loan clearly violates NPC Circular No. 20-01" or the Guidelines on the Processing of Personal Data for Loan-Related Transactions (Loan-Related Transactions Circular).³⁷ This is because, according to the CID, the Loan-Related Transactions Circular "prohibits access to contact details in whatever form, such as but not limited to phone contact list, the harvesting of social media contacts, and/or copying or otherwise saving these contacts."³⁸ Further, it argued that "[i]n all instances, online lending apps must have a separate interface where borrowers can provide character references and/or co-makers of their own choosing."³⁹ Thus, the CID maintained that:

As discussed, JuanHand did not limit itself to a number of character references of the borrower's own choosing but required access to all phone and social media contacts. It also failed to

³² Fact-Finding Report, 09 June 2021, at 8, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

³³ *Id.* at 7.

³⁴ *Id.* at 8.

³⁵ *Id.* at 9.

³⁶ *Id.* at 10.

³⁷ *Id.*

³⁸ Fact-Finding Report, 09 June 2021, at 10, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

³⁹ *Id.* at 11.

comply with the required separate interface where borrowers can provide character references and/or co-makers of their own choosing. The availability of far less intrusive measures, such as reliance on a limited number of reference contacts provided by the borrower, demonstrates that the measures employed by JuanHand were disproportionate to the aim of evaluation of the loan application and/or loan collection purposes.⁴⁰

Fourth, the CID stated that the Privacy Policy violated the DPA and its issuances:

JuanHand's Privacy Policy, imbedded in the Service Agreement, not only violates the general data privacy principles of transparency, legitimate purpose and proportionality but makes a mockery of the Data Privacy Act when it says that the exercise of the privacy rights by the users is subject to review by JuanHand and may result in the denial of any pending application in violation of Section 16 of the DPA. The borrowers are made to choose between their privacy and the much-needed funds. The consent, therefore, that the borrowers granted to JuanHand was not by will but thru [sic] coercion.⁴¹

In addition, the CID pointed out irregularities in JuanHand's Service Agreement:

The Service Agreement of JuanHand provides that the borrower must provide true, up-to-date, valid and complete information, and grant JuanHand a permanent right to use the information the borrower provided free-of-charge for the purpose of using Juanhand service. The permanent right to use the information provided by the borrower free-of-charge for the purpose of using JuanHand service is in violation of Rule IV of the Implementing Rules and Regulations of the Data Privacy Act of 2012 which states that the personal data should not be retained longer than necessary. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

The provision in the Service Agreement which provides that: 'When the Borrower is overdue for payment, Juanhand may publish the personal information of such user for the purpose of collecting debt. Juanhand shall not be held liable.' violates NPC Circular No. 20-01 specifically Section 3, paragraph D4 of the Circular which states:

⁴⁰ *Id.*

⁴¹ *Id.*

‘Access to contact details in whatever form, such as but not limited to phone contact list or e-mail lists, the harvesting of social media contacts, and/or copying or otherwise saving these contacts for use in debt collection or to harass in any way the borrower or his/her contacts, are prohibited. In all instances, online lending apps must have a separate interface where borrowers can provide character references and/or co-makers of their own choosing.’⁴²

Again, the CID reiterated that undisclosed permissions in the app exist, and that JuanHand did not acquire the consent of the data subjects to process personal information arising from these undisclosed permissions.⁴³ The CID considered these acts to be unauthorized processing of personal information in violation of Section 25 of the DPA since JuanHand processed personal information without valid consent or authority under the DPA and other existing laws.⁴⁴

After having alleged violations of the DPA, the CID argued that JuanHand’s responsible officers should be held liable pursuant to Section 34 of the DPA.⁴⁵

Lastly, the CID interposed that:

Based on the initial results of the investigation conducted by the CID, there is sufficient ground to warrant for the issuance of a Temporary Ban on the processing of personal data against WEFUND Lending Corporation, in relation to its online lending application, JuanHand. A review of its privacy policy shows that JuanHand’s nature, purpose, and extent of accessing and processing user’s personal information failed to adhere to the principles of transparency, legitimate purpose and proportionality. The simulation of the installation of JuanHand’s application and analysis of its source code show that its use of dangerous permissions, is in direct violation of the prohibition against the access of contacts, as provided in NPC Circular 20-01.⁴⁶

⁴² *Id.* at 13.

⁴³ *Id.* at 12.

⁴⁴ Fact-Finding Report, 09 June 2021, at 12, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

⁴⁵ *Id.* at 13.

⁴⁶ *Id.* at 15-16.

As such, it argued that substantial evidence had been established for the issuance of a temporary ban against JuanHand.⁴⁷

On 16 June 2021, the Commission issued an Order suspending the complaint proceedings until the resolution of the application for the issuance of a temporary ban.⁴⁸ JuanHand was ordered to submit a position paper on the application for the issuance of a temporary ban within ten (10) days from its receipt of the Order.⁴⁹

On 05 July 2021, the CID submitted a Supplemental Fact-Finding Report with Application for Issuance of Temporary Ban on the Processing of Personal Data, impleading specific responsible officers of JuanHand in their official capacities as corporate officers and members of the Board of Directors (Corporate Officers and Directors), in line with Section 34 of the DPA.⁵⁰

In a letter dated 02 August 2021, JuanHand acknowledged receipt of the 16 June 2021 Order issued by the Commission and requested an extension to submit its position paper since its change in physical office caused its belated receipt of the Order.⁵¹

On 12 August 2021, JuanHand submitted a Motion to Properly Serve Order with Motion to Admit Position Paper *Ad Cautelam*⁵² and its Position Paper on the application of the issuance of a temporary ban.⁵³ It attached to the Position Paper a “standalone and rectified Privacy Policy independent from the Service Agreement.”⁵⁴ JuanHand claimed that the new Privacy Policy shall be shown and given consent to by the borrowers upon registration and loan application.⁵⁵

Further, JuanHand clarified that it has not published any image or information of its users for purposes of loan collection or harassment.⁵⁶

⁴⁷ *Id.* at 16.

⁴⁸ Order, 16 June 2021, at 1, *in re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

⁴⁹ *Id.* at 2.

⁵⁰ Supplemental Fact-Finding Report, 05 July 2021, at 2, *in re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

⁵¹ JuanHand Letter, 02 August 2021, *in re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

⁵² Motion to Properly Serve Order with Motion to Admit Position Paper *Ad Cautelam*, 12 August 2021, *in re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

⁵³ Position Paper, 12 August 2021, *in re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

⁵⁴ *Id.* at 2.

⁵⁵ *Id.*

⁵⁶ *Id.* at 3.

It will, however, continue to publish personal information of delinquent users to the Credit Information Corporation for purposes of creating a centralized credit information system.⁵⁷

As regards the undisclosed permissions in its app, JuanHand explained that “[d]espite the embedded privacy policy in the Service Agreement, which we undertake to rectify immediately, we would like to clarify the corresponding consent sought and granted by our users in relation to the permission information”:

<ul style="list-style-type: none">• send email to guests	Users are manually fill in his/her email address. There is no way a user become unaware of providing email address. Under section 3(d) of the Service Agreement, we stated clearly that Juanhand may use the User's information to communicate with the User and deliver information via SMS messages, email and phone calls with respect to communications relating to the use of Juanhand by the User.
<ul style="list-style-type: none">• read borrower's contacts,• collect data from contacts	Under section 2(b)(iv) and 3(h) of the Service Agreement, we stated clearly that Juanhand will collect and process contact list. More explanation about accessing contact list later.
<ul style="list-style-type: none">• pinpoint the borrower's approximate and precise location through its network and GPS	Under section 2(b)(iv) and 3(h) of the Service Agreement, we stated clearly that Juanhand will collect and process geographical location (e.g., mobile device location, time zone setting). ⁵⁸

...

Further, **we do also read the borrower’s calendar events and add or modify calendar events. We consider that accessing and modifying user’s calendar is legitimate and proportional to the purpose stated in the Service Agreement** for two reasons:

- (i) Credit Analysis and Scoring: by accessing the calendar, we seek to identify due dates of other loans or payment obligations of the users to determine whether or not to provide loan services, and if so, his/her credit limits;

⁵⁷ *Id.* at 3-4.
⁵⁸ *Id.* at 4.

(ii) Due Day Reminder: by adding due date to the users' calendar, it would be easier for the users to apprehend the due date and, thus, repayment obligation.

Therefore, we consider that when users give consent to the Service Agreement, users are materially informed the kind of personal information shall be processed in compliance with section 16(a) of the DPA and have given consent to the above functions.⁵⁹

Nevertheless, JuanHand acknowledged that it shall “enhance the transparency and timeliness of obtaining user’s consent by incorporating” certain prompts upon registering as a user in its app.⁶⁰

Lastly, JuanHand stressed that it does not use its users’ contact lists for purposes of collection or harassment but only for purposes of identity verification, credit scoring, and fraud prevention.⁶¹ It argued that accessing the borrower’s contact list is necessary since, in certain situations, it is the only means available to verify its users.⁶² Thus, “[v]erification by accessing users’ contact lists [...] is a less-intrusive and more reliable way for [JuanHand] to assess credit level and risks.”⁶³

JuanHand prayed for the dismissal of the application for the issuance of a temporary ban on its processing of personal data.⁶⁴

On 12 August 2021, the Commission issued an Order granting the application for the issuance of a temporary ban against JuanHand because all the requisites for granting a temporary ban were satisfied.⁶⁵ The temporary ban would remain in effect until the final resolution of the *sua sponte* investigation against JuanHand and its Corporate Officers and Directors.⁶⁶ Further, it ordered the following:

Further, pursuant to the **TEMPORARY BAN**, Respondent Wefund Lending Corporation shall:

⁵⁹ Position Paper, 12 August 2021, at 5, *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022). Emphasis supplied.

⁶⁰ *Id.*

⁶¹ *Id.* at 7.

⁶² *Id.*

⁶³ *Id.* at 8.

⁶⁴ *Id.* at 10.

⁶⁵ Order, 12 August 2021, at 6-15, *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

⁶⁶ *Id.* at 16.

1. Immediately take down its online lending application, JuanHand, to ensure that it is no longer available for download, installation or use by data subjects; and
2. Stop personal data processing activities, including those activities outsourced to third parties, where the processing operations involves use of information from the phonebook, directory, and contact list of data subjects, disclosure of false or unwarranted information, and other unduly intrusive personal data processing methods.⁶⁷

The Commission also ordered JuanHand to file its comment on the allegations in the FFR within ten (10) days from receipt of the Order.⁶⁸

On 02 September 2021, JuanHand took down the app and submitted its Comment to the Order and Temporary Ban dated 12 August 2021.⁶⁹

It emphasized that, pursuant to the 12 August 2021 Order, it has taken down the JuanHand app from Google Play, Apple's AppStore, Huawei's AppGallery, and Vivo Market, thereby making the app unavailable for download by the public in any official platform.⁷⁰ It also attached as annexes its revised Privacy Policy and Service Agreement, as well as their respective correct hyperlinks.⁷¹ Aside from producing a separate Privacy Policy, JuanHand also began incorporating the Privacy Policy in its user registration process.⁷² Users can now view the entire document and choose whether to agree to the Privacy Policy before completing the registration.⁷³

As regards the permissions, JuanHand alleged that it deleted from its app the access to its users' calendar, location, contact list, and social networking profile.⁷⁴ It also removed from its revised Privacy Policy the permissions to access calendar, location, contact list, and social networking profile.⁷⁵ In order to make the prompts for these permissions more "eye-catching," it has shifted from using system prompts to providing more intuitive and visible pop-up prompts

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ Comment to the Order and Temporary Ban dated 12 August 2021, 01 September 2021, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

⁷⁰ *Id.* at 1.

⁷¹ *Id.* at 2.

⁷² *Id.*

⁷³ *Id.*

⁷⁴ *Id.* at 3.

⁷⁵ Comment to the Order and Temporary Ban dated 12 August 2021, 01 September 2021, at 3, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

when the app attempts to access user's personal information, wherein the users may accept or deny such access.⁷⁶ Effectively, JuanHand explained that these new alterations would ensure that:

[E]very time the data of a user is being accessed, such pop-up prompt will trigger and will halt the entire process. This pop-up prompt is now effective and live in JuanHand App during user registration and loan application. We guarantee to the Commission that there will be no hidden permissions in JuanHand App and that we have implemented a more intuitive design geared towards to providing actionable knowledge to our users and protection of the user's data.⁷⁷

JuanHand also included the "What's New" feature in the app itself and not merely in the download interface of platforms.⁷⁸ Any material changes, such as the amendment of the Privacy Policy and Service Agreement and other new functionalities, among other things, will be shown in the "What's New" interface.⁷⁹

Seeing, however, as the app is not available for the public market, JuanHand explained that it re-created its app in a sandbox mode to ensure that the app fully complies with all the requirements imposed by law and by the Commission.⁸⁰ It attached a quick response (QR) code for the Commission to download the testing version 4.1.1 of the app since JuanHand strives to ensure full alignment with the Commission's regulations prior to the final re-deployment of its app to the public.⁸¹

Lastly, JuanHand attached as annexes its (1) Personal Privacy Information Management Policy which serves as its comprehensive corporate data protection policy and (2) Information Security Emergency Response Management Directive which serves as its structured approach in responding to incidents wherein the users' data privacy may be breached or in any way compromised.⁸² Thus, it prayed that the Commission lift its temporary ban on the app and allow its re-deployment to the public.⁸³

⁷⁶ *Id.*

⁷⁷ *Id.* at 3-4.

⁷⁸ *Id.* at 4.

⁷⁹ *Id.*

⁸⁰ *Id.*

⁸¹ Comment to the Order and Temporary Ban dated 12 August 2021, 01 September 2021, at 4, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

⁸² *Id.* at 5.

⁸³ *Id.* at 7.

On 10 September 2021, it filed both the Entry of Appearance with Motion to Admit [Supplemental Comment with Motion for Lifting of Temporary Ban]⁸⁴ and the Supplemental Comment with Motion for Lifting of Temporary Ban⁸⁵.

Meanwhile, the Enforcement Division (EnD) of the Commission continuously monitored the availability of the app pursuant to the temporary ban.⁸⁶ It received, however, an email complaint which included a link provided by the JuanHand Collection Department for the downloading of the app.⁸⁷ Upon investigation, it found that the direct download link (DDL) was for JuanHand app version 4.2.0:⁸⁸

To note, this version of the JuanHand APK file (v4.2.0) is different from the one investigated by the Complaints and Investigation Division (CID) which is v3.7.1 and the one [JuanHand] sent in an email [...], which is v.4.1.1, for compliance checking and investigation.⁸⁹

Thus, on 16 September 2021, the EnD issued a Letter to JuanHand regarding its compliance with the Commission's 12 August 2021 Order.⁹⁰ The EnD confirmed that, as of 06 September 2021, the JuanHand app was no longer available for download on different platforms.⁹¹ The EnD, however, relayed that:

[T]he Commission received several reports from Juanhand's users. According to the reports, **JuanHand's Collection Department sent them various links leading to the Direct Download Links to the JuanHand application. Upon investigation, the EnD was able to download the JuanHand application through the Direct Download Links after following the links provided in the reports.**

As the Order dated 12 August 2021 directs JuanHand to 'immediately take down its online lending application,

⁸⁴ Entry of Appearance with Motion to Admit Supplemental Comment with Motion for Lifting of Temporary Ban, 10 September 2021, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

⁸⁵ Supplemental Comment with Motion for Lifting of Temporary Ban, 10 September 2021, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

⁸⁶ Enforcement Division Memorandum, 14 September 2021, at 1, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ *Id.* at 3.

⁹⁰ Enforcement Division Letter of Compliance with Order dated 12 August 2021 in NPC SS 21-006 entitled "*In re: Wefund Lending Corporation (JuanHand)*", 16 September 2021, at 1, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

⁹¹ *Id.* at 2.

JuanHand, to ensure that it is no longer available for download, installation or use by data subjects,' JuanHand is instructed to **EXPLAIN** the foregoing incident within **FIVE DAYS (5)** from receipt of this letter. Such incident could be construed as a violation of the Temporary Ban.⁹²

On 17 September 2021, the Commission issued an Order noting JuanHand's Comment and submissions.⁹³ In the Commission's Order, it emphasized that JuanHand was previously ordered to comment on the FFR dated 09 June 2021 and not the issuance of the temporary ban.⁹⁴ Nevertheless, it reiterated its order for JuanHand and its Corporate Officers and Directors to comment on the FFR within a non- extendible period of ten (10) days from receipt of the Order.⁹⁵

On 08 October 2021, JuanHand submitted its Reply and Explanation to the National Privacy Commission Enforcement Division Letter dated 16 September 2021.⁹⁶ It countered that prior to the commencement of the *sua sponte* investigation, it already prepared a template for the repayment reminder Short Message Service (SMS) and emails it will send out to its users that have availed themselves of loans.⁹⁷ The template includes, among other things, a hyperlink to the JuanHand app.⁹⁸ It explained that:

The sending of SMS and emails is an **automatic process sent by the JuanHand system, without human intervention**, which transmits repayment reminders to the Borrowers[.]

...

Based on the abovementioned template, the hyperlink or DDL has always been part of the messages, both SMS and email, sent to JuanHand users even before the issuance of the Temporary Ban.

...

⁹² *Id.* Emphasis supplied.

⁹³ Order, 17 September 2021, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

⁹⁴ *Id.* at 3.

⁹⁵ *Id.* at 3-4.

⁹⁶ Reply and Explanation to the National Privacy Commission Enforcement Division Letter dated 16 September 2021, 08 October 2021, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

⁹⁷ *Id.* at 2.

⁹⁸ *Id.* at 3.

Unfortunately, after the removal or unavailability of the JuanHand application on the Platforms for download, the standardized or template repayment reminder SMS and emails, which were **inadvertently retained, automatically sent out, without human intervention**, to the JuanHand users, which still contained the hyperlink or DDL to the JuanHand application.⁹⁹

JuanHand stressed that it only became aware of the situation on 17 September 2021, after which it conducted an internal investigation to rectify the situation.¹⁰⁰ Apparently, the “template repayment reminders were not updated or revised—the same unintentionally retained the hyperlink or DDL” since the reminders were “system-generated and automatically sent” to its users following certain timelines or outstanding milestones.¹⁰¹ After being made aware of the situation, JuanHand immediately ordered the removal of the DDLs from its repayment reminders and instructed its designated personnel to ensure that the DDLs that were sent out to users be inaccessible and deactivated.¹⁰² JuanHand posited that since its focus was solely to take down its app from downloading platforms and prepare responses to the orders of the Commission, it committed a “complete and unfortunate oversight” when the DDL to its app continued to be included in its repayment reminder.¹⁰³

Nevertheless, despite the inadvertent sending of SMS and emails containing the DDLs, JuanHand stressed that it never meant to circumvent the prohibition under the temporary ban and that it immediately took actions to rectify the matter.¹⁰⁴ Lastly, as a sign of good faith and in immediate response to the EnD’s letter, JuanHand sent messages to its six hundred thirty-two (632) users that were able to use, access, or download the app during the period of the temporary ban’s effectivity:

Dear Valued Client. We apologize to inform [you] that Juan[H]and application is currently unavailable for downloading in compliance to National Privacy Commission’s order. If you have received Juan[H]and download links before, please do not access it anymore. We would like to express our sincere gratitude to every Juan. Thank you.¹⁰⁵

⁹⁹ *Id.* Emphasis supplied.

¹⁰⁰ *Id.* at 4.

¹⁰¹ *Id.*

¹⁰² Reply and Explanation to the National Privacy Commission Enforcement Division Letter dated 16 September 2021, 08 October 2021, at 4, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21- 006 (NPC 2022).

¹⁰³ *Id.* at 5.

¹⁰⁴ *Id.*

¹⁰⁵ *Id.* at 6. Emphasis removed.

On 11 October 2021, JuanHand submitted to the Commission its Comment (on the Fact-Finding Report dated 09 June 2021) addressing the allegations of the CID in its FFR.¹⁰⁶

JuanHand stressed that there is more than one allowable basis for processing in this case: (1) data subject's consent; (2) contract of loan; and (3) legitimate interests pursued as lender.¹⁰⁷ Thereafter, it stated that JuanHand has "already rectified any perceived violation" of the DPA and that it has pursued "legitimate interests and purposes" in processing the personal information of its users.¹⁰⁸ Moreover, it asserted that the data it processed is only "personal information, which can be collected for specified and legitimate purposes determined and declared before, **or as soon as reasonably practicable after collection**, and later processed in a way compatible with such declared, specified and legitimate purposes only."¹⁰⁹ JuanHand argued that, aside from the user's acceptance of the terms and conditions in the pop-up permissions, it considered, in good faith, the continuous use of its app as the user's express consent to the collection of personal information.¹¹⁰

JuanHand countered the contentions of the CID by alleging, first, that it has already corrected the undisclosed permissions.¹¹¹ JuanHand opined that, as regards the permission information claimed by the CID to have been discovered through the Google Play Store and not the JuanHand app itself, the "point of contention [...] boils down to the propriety of the format/manner upon which such permissions are to be disclosed" since the "[p]ermission [i]nformation has already previously existed, albeit in the Google Play Store and not in the OLA itself."¹¹² In any case, JuanHand emphasized that it has already revised and addressed this particular issue by making the following changes:

33.1. Access to users' calendar, location, contact list and social networking profile have been removed and deleted from the JuanHand OLA.

¹⁰⁶ Comment on the Fact-Finding Report dated 09 June 2021, 11 October 2021, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹⁰⁷ *Id.* at 5.

¹⁰⁸ *Id.* at 6.

¹⁰⁹ *Id.* at 7. Emphasis supplied.

¹¹⁰ *Id.*

¹¹¹ *Id.* at 8.

¹¹² Comment on the Fact-Finding Report dated 09 June 2021, 11 October 2021, at 8-9, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

33.2. The Privacy Policy has been further revised, removing any perceived Undisclosed Permissions to access users' calendar, location, contact list and social networking.

33.3. [JuanHand] reconfigured JuanHand OLA by providing more visible pop-up prompts when there is an attempt to access users' personal information, subject to the user's acceptance or denial of such access. In case of the latter, no access or collection will take place. These pop-up prompts effective even during user registration and loan application.¹¹³

In relation to this, JuanHand asserted that it similarly corrected and revised the app to comply with the principles of transparency, legitimate purpose, and proportionality.¹¹⁴

Pertaining to the principle of transparency, JuanHand took into consideration the findings of the CID and “[excluded] access to calendar, location, contact list and social networking accounts of the data subject” in its latest Privacy Policy.¹¹⁵ Moreover, it reiterated that it improved the prompts that will enable data subjects to modify their permission or consent and ensured that the users can easily be informed of the changes to the JuanHand app through the “What’s New” feature.¹¹⁶

As to the general privacy principle of legitimate purpose, JuanHand argued that its processing of information was compatible with the declared and specified purposes indicated for access to the user's contact list, which is: “(1) to speed up the application process, and (2) to prevent criminals from stealing user's money.”¹¹⁷

In addition, JuanHand interposed that since the information is personal information and not sensitive personal information, its collection may still be subject to subsequent consent from the users.¹¹⁸

JuanHand, however, “[conceded] that there were issues in the operation and coding of its application, which failed to provide a means to continue a loan application in cases where a user disagrees

¹¹³ *Id.* at 9.

¹¹⁴ *Id.*

¹¹⁵ *Id.* at 12.

¹¹⁶ *Id.*

¹¹⁷ *Id.* at 13.

¹¹⁸ Comment on the Fact-Finding Report dated 09 June 2021, 11 October 2021, at 14, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

to provide access to their contacts.”¹¹⁹ Thus, to address the concerns of the CID, it no longer requested access to the user’s contact list in its latest update of the app.¹²⁰

As for the proportionality principle, JuanHand explained that:

[JuanHand], in good faith, [was] of the belief that their questioned action of requesting for the access of a user’s contact list was in proportion to the purpose it declared.

[JuanHand], in requesting for the access to the contact list of its users, [was] hinged on the belief that it was a necessary means to protect legitimate business interests and to serve the interests of the user for credit approval.

Admitting that the purpose for which [JuanHand] requested for the contact list may have been fulfilled by other means in a more ideal scenario, the realities of the situation in the Philippines do not make other options a reasonable means to achieve the purpose sought to be addressed by [JuanHand].¹²¹

. . .

[T]he target market of the JuanHand application consists of the individuals in the lower economic brackets. As such, these realities were taken into consideration by [JuanHand] in its decision to request for access to the user’s contact data.¹²²

Nevertheless, JuanHand acknowledged the concerns raised by the CID and reiterated that it no longer requests for or uses the contact list of its users.¹²³

Regarding the Loan-Related Transactions Circular, JuanHand stressed that it interpreted the prohibition to access contacts as being qualified by the statement “for use in debt collection or to harass in any way the borrower or his/her contacts.”¹²⁴ It stated that it has never made use of a user’s contact information to harass for debt collection.¹²⁵ Instead, the information was merely used for purposes of identity verification,

¹¹⁹ *Id.*

¹²⁰ *Id.* at 15.

¹²¹ *Id.*

¹²² *Id.* at 16.

¹²³ *Id.*

¹²⁴ Comment on the Fact-Finding Report dated 09 June 2021, 11 October 2021, at 16, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹²⁵ *Id.*

credit scoring, and fraud prevention, and it was simply stored in its system as a potential reference source.¹²⁶ In any case, it has now removed its request to access and use its borrowers' contacts.¹²⁷ The supposed violations and concerns of the Commission, therefore, have already been addressed.¹²⁸

JuanHand similarly revised its Service Agreement and removed the contentious provisions raised by the CID to improve compliance with the DPA and its issuances.¹²⁹

Lastly, JuanHand argued that its Corporate Officers and Directors should not be held personally liable because they did not actively participate in, nor by their own gross negligence, allow for the commission of the crime.¹³⁰ As to the first category, it opined that it always acted in good faith when it executed the purported erroneous acts.¹³¹ It even acquired the advice of legal professionals to review the legality of its documents and the process flows of the app since it admits that its own interpretation of the DPA and its issuances, particularly on OLAs, are inadequate.¹³² As to the second category, it asserted that assuming there was negligence, it did not amount to "gross negligence" since JuanHand made efforts to comply with the DPA and its issuances.¹³³

JuanHand prayed that the temporary ban be lifted and that it be allowed to re-deploy the app to the public.¹³⁴

On 17 December 2021, JuanHand filed a Motion to Resolve the imposition of the Temporary Ban on the Processing of Personal Data.¹³⁵ On 10 January 2022, it filed a Supplemental Motion to Resolve the imposition of the Temporary Ban.¹³⁶

¹²⁶ *Id.* at 17.

¹²⁷ *Id.*

¹²⁸ *Id.*

¹²⁹ *Id.*

¹³⁰ Comment on the Fact-Finding Report dated 09 June 2021, 11 October 2021, at 22, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

¹³¹ *Id.*

¹³² *Id.*

¹³³ *Id.*

¹³⁴ *Id.* at 23.

¹³⁵ Motion to Resolve, 17 December 2021, *in* In re: Wefund Lending Corporation and its Responsible Officers, NPC SS 21- 006, (NPC 2022).

¹³⁶ Supplemental Motion to Resolve, 10 January 2022, *in* In re: Wefund Lending Corporation and its Responsible Officers, NPC SS 21-006, (NPC 2022).

On 13 January 2022, the Commission issued a Resolution lifting the Temporary Ban issued against JuanHand.¹³⁷ Despite lifting the ban, the Commission, in an Order dated 13 January 2022, enjoined JuanHand to address the issues it raised regarding the version 4.1.1, version 4.2.0, its Privacy Manual, and its Security Incident Management Policy so that it may fully comply with the DPA and the other issuances of the Commission.¹³⁸ Thus, the Commission ordered the parties to submit their respective Memoranda within ten (10) days from the submission of JuanHand's proof of compliance to the mandated changes.¹³⁹

On 28 February 2022, JuanHand filed its Compliance.¹⁴⁰ JuanHand claimed that it only accesses its borrowers' camera or photo gallery for KYC, credit assessment, and fraud prevention at the beginning of loan application processes.¹⁴¹ It specified that both version 4.1.1 and version 4.2.0 of its app have been duly rectified to comply with Section 3(D)(3) of the Loan-Related Transactions Circular on camera permissions.¹⁴² Particularly, the app now contains prompts through its "Close Camera Permission" feature informing its users when they may already turn off or disallow permission to access their cameras or photo galleries.¹⁴³ Thus, upon uploading photos and successfully submitting their loan applications, users may now deny camera access for the app.¹⁴⁴

Additionally, JuanHand submitted its rectified Privacy Manual that includes organizational, physical, and technical measures.¹⁴⁵ It provides for the procedure for appointing data privacy and compliance officers, the conduct of annual privacy trainings, privacy impact assessments, and review of data protection policies.¹⁴⁶ Physical security measures such as storage, limitation of access, and modes of transfer of personal data are included as well as technical security measures involving encryption and authentication processes.¹⁴⁷ Lastly, its submitted Privacy Manual discusses mechanisms in determining the basis for lawful processing of personal data and

¹³⁷ Resolution, 13 January 2022, at 6-7, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹³⁸ Order, 13 January 2022, at 9, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹³⁹ *Id.* at 10.

¹⁴⁰ Memorandum (for Respondents), 10 March 2022, at 5, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹⁴¹ Compliance, 28 February 2022, at 3, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹⁴² *Id.* at 2.

¹⁴³ *Id.*

¹⁴⁴ *Id.* at 3.

¹⁴⁵ *Id.*

¹⁴⁶ *Id.*

¹⁴⁷ Compliance, 28 February 2022, at 3, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

mirrors the rights of data subjects in accordance with Sections 12, 13, and 16 of the DPA.¹⁴⁸ It also submitted its rectified Security Incident Management Policy that complies with NPC Circular No. 16-03 (Personal Data Breach Management) in order to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident.¹⁴⁹ It provides for an incident response procedure in case of security incidents or breaches¹⁵⁰ and for a procedure that complies with the requirements of personal data breach notification.¹⁵¹

On 10 March 2022, JuanHand filed its Memorandum.¹⁵² The CID filed its Memorandum on 16 March 2022.¹⁵³ Both parties reiterated the arguments found in their respective pleadings.

Issue

Whether JuanHand and its Corporate Officers and Directors committed violations of the DPA and the Commission's issuances that warrant a recommendation for prosecution.

Discussion

JuanHand's position mainly asserted that it is no longer liable for violations of the DPA and the Commission's issuances since it already incorporated and made changes to the app to align with the results of the CID's investigation on undisclosed permissions:

There are no longer any 'Undisclosed Permissions' in the JuanHand OLA. Section 16 of the Data Privacy Act is not violated.¹⁵⁴

. . .

¹⁴⁸ *Id.* at 4.

¹⁴⁹ *Id.*

¹⁵⁰ *Id.*

¹⁵¹ *Id.* at 5.

¹⁵² Memorandum (for Respondents), 10 March 2022, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

¹⁵³ Memorandum, 16 March 2022, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

¹⁵⁴ Memorandum (for Respondents), 10 March 2022, at 8, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

[JuanHand has] already rectified and revised the [JuanHand] OLA to comply with the principles of transparency, legitimate purpose, and proportionality.¹⁵⁵

...

Thus, as it currently stands, the supposed violations by [JuanHand] and the concerns of the Honorable Commission have already been addressed.¹⁵⁶

...

In any case, [JuanHand's] willingness to abide by all the directives of this Honorable Commission is evident in the rectifications made in the Service Agreement, the JuanHand OLA itself, and the privacy policies.¹⁵⁷

...

Further, in [its] Compliance dated 28 February 2022, [JuanHand] made the following rectifications pursuant to the Honorable Commission's Order dated 13 January 2022[.]¹⁵⁸

This argument is flawed. Rectification after the fact does not cure violations that arose prior to the changes made. This was made clear even in the Commission's 13 January 2022 Order when it stated that:

Compliance with this Order **shall not excuse [JuanHand] and its responsible officers from any violations** of the Data Privacy Act of 2012 and its Implementing Rules and Regulations **that may have resulted from their previous actions before and during the time the Temporary Ban** was in place.¹⁵⁹

The Commission finds that JuanHand committed lapses in its actions before and during the effectivity of the temporary ban. Nevertheless, these lapses, even if taken together, are not sufficient to warrant a recommendation for prosecution.

I. JuanHand's lapses in its actions resulted in a violation of Section 25 of the DPA.

¹⁵⁵ *Id.* at 10.

¹⁵⁶ *Id.* at 17.

¹⁵⁷ *Id.*

¹⁵⁸ *Id.* at 20.

¹⁵⁹ Order, 13 January 2022, at 10, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022). Emphasis supplied.

The root of the CID's contentions stemmed from the alleged undisclosed permissions:

The capabilities of JuanHand's system to read the borrower's calendar events plus confidential information, add or modify calendar events, send email to guests without the owner's knowledge, read borrower's contacts, collect data from contacts and pinpoint the borrower's approximate and precise location through its network and GPS are all unknown to the prospective borrower. The permission information for these capabilities is not shown to the users thru [sic] prompts or permissions when applying for a loan but was discovered by the Technical Team from the google play store and not from the application itself. Thus, the data subjects are uninformed that his or her confidential personal information including that of his or her contacts have been processed in violation of Section 16 of the DPA.¹⁶⁰

...

In the Fact-finding Report, the CID said that the undisclosed permissions in JuanHand's Application also violated the principles of transparency, legitimate purpose, and proportionality, as described in Rule IV, Sections 17 and 18 of the Implementing Rules and Regulations of the DPA[.]¹⁶¹

...

JuanHand's processing of personal information is in violation of Sections 12 and 13 of the Data Privacy Act which requires consent of the data subject prior to the processing. An undisclosed permission did not acquire the consent of the data subject. Thus, the processing of personal data by JuanHand did not adhere to Sections 12 and 13 of the DPA, violating therefore Section 25 of the DPA being unauthorized processing of personal information.¹⁶²

...

Moreover, without a valid consent, or authority under the DPA and other existing laws, processing will be unauthorized in violation of Section 25 of the Data Privacy Act of 2012. Where information is used for purposes other than what the data subject clearly agreed to, or otherwise authorized by law, the further

¹⁶⁰ Memorandum, 16 March 2022, at 2, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022). Emphasis removed.

¹⁶¹ *Id.* at 3.

¹⁶² *Id.* at 7.

processing of the information may be considered processing for unauthorized purpose.¹⁶³

JuanHand did not refute the results of the CID's investigation regarding its undisclosed permissions. Rather, to address this point, it admitted that its app does "read the borrower's calendar events and add or modify calendar events."¹⁶⁴ JuanHand's arguments instead attempted to address the conclusions the CID sought to derive from these findings of fact by arguing that it considers the accessing and modifying of its borrower's calendar as "legitimate and proportional to the purpose stated in the Service Agreement. [...] [t]herefore, [it] consider[s] that when users give consent to the Service Agreement, users are materially informed [of] the kind of personal information [that] shall be processed in compliance with [S]ection 16(a) of the DPA and have given consent to the above functions."¹⁶⁵

Considering the foregoing, it is evident that JuanHand committed lapses.

The results of the CID's investigation on JuanHand's Permission Information demonstrated that the system can do the following:

1. read the borrower's calendar events plus confidential information;
2. add or modify calendar events;
3. send email to guests without the owner's knowledge;
4. read borrower's contacts;
5. collect data from contacts; and
6. pinpoint the borrower's approximate and precise location through its network and GPS.¹⁶⁶

Not all permissions, however, were indicated in the Service Agreement, particularly the permission to access a borrower's calendar events and confidential information as well as read and modify the calendar events.¹⁶⁷ This is an erroneous oversight because "it is the Service Agreement that potential borrowers are asked to

¹⁶³ *Id.*

¹⁶⁴ Position Paper, 12 August 2021, at 5, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹⁶⁵ *Id.*

¹⁶⁶ Fact-Finding Report, 09 June 2021, at 4-5, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹⁶⁷ See Supplemental Report, 31 May 2021, Annex A (JuanHand User Agreement Web), *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

consent to and is the one that governs the relationship between the borrower and JuanHand.”¹⁶⁸ Moreover, as emphasized by the Commission in its 12 August 2021 Order:

JuanHand does not have a clear understanding of the lawful criteria for processing under the DPA that it is relying on. As reflected in its Position Paper, JuanHand considers access to and modification of a user’s calendar as legitimate and proportional to the purpose stated in the Service Agreement. However, JuanHand is unclear on which specific purpose it pertains to. JuanHand subsequently states that ‘when users give consent to the Service Agreement, users are materially informed [of] the kind of personal information [that] shall be processed in compliance with [S]ection 16(a) of the DPA and [users] have given consent to the above functions.’ This statement is, at best, confusing.

The primary contract entered into by JuanHand and its users is a loan. When entering a loan, the borrower signifies consent to the purposes necessary to deliver the services contemplated in the contract, this necessarily includes the processing of relevant personal information. JuanHand, in including the privacy policies in its Service Agreement and in creating the revised Privacy Policy, acknowledges that its main basis for processing personal information is consent. **In this case, however, for matters where it did not request consent from its data subjects, JuanHand erroneously attempts to fill in the gaps by conveniently citing legitimate interest as its basis in processing their personal information.**

According to JuanHand, it considers accessing and modifying a user’s calendar as legitimate and proportional to the purpose in the Service Agreement[.]

...

In the next provision, JuanHand declares that users are ‘materially informed’ of the kind of personal information it processes when users give consent[.]

...

The privacy provisions in the Service Agreement, however, do not mention access to the user’s phone calendar. In fact, the request for permission to access and modify the calendar is not included among the disclosed permissions JuanHand requests from its users, as presented in Annex 2 of the Position Paper. The access and modification of the calendar that JuanHand claims to

¹⁶⁸ Order, 12 August 2021, at 9, *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

be covered under its legitimate interest is not included in the categories of personal information that will be collected and processed, as set out in the Service Agreement. As a result, the access and modification of the calendar could not have been disclosed to the data subjects. JuanHand neither informed its borrowers of the additional personal information that will be processed nor acquired their consent to such processing. **Having failed to inform its borrowers of such processing, much less acquired their consent, JuanHand cannot belatedly use legitimate interest to cure this defect especially since its borrowers could not have expected this at the time they gave their consent.**¹⁶⁹

Aside from this, the CID also pointed out that the clause in the Service Agreement regarding publication is violative of the DPA and its issuances.¹⁷⁰ Sections K(4)(c) and (d) of the Service Agreement provide:

c. After the repayment is overdue, [JuanHand] as the Facilitator is entitled to disclose to the Investor the personal information of the Borrower, and to or obtain by the Facilitator through this Agreement and other lawful means and include the personal information submitted by the Borrower or collected by [JuanHand] into the blacklist of the [JuanHand] Website and the national and local personal credit information systems. The Facilitator is also entitled to share with any third parties the personal information of the Borrower, which was submitted by the Borrower or collected by the Facilitator in public domain, so that the Facilitator and the third parties can collect the overdue amount and such personal information can be used for the approval of other loan applications made by the Borrower. All the legal liabilities shall be borne by the Borrower and [JuanHand] shall not take any responsibilities.

d. When the Borrower is overdue for payment, [JuanHand] may publish the personal information of such user for the purpose of collecting debt. [JuanHand] shall not be held liable.¹⁷¹

JuanHand contended that the limitation of liability does not pertain to the DPA, but it is only connected to its publication in case of delinquent users and where payment is overdue.¹⁷² It argued that the contentious provision should be read in conjunction with the provision of the

¹⁶⁹ *Id.* at 9-11. Emphasis supplied.

¹⁷⁰ Fact-Finding Report, 09 June 2021, at 11 & 13, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹⁷¹ Supplemental Report, 31 May 2021, Annex A (JuanHand User Agreement Web) at 9, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022). Emphasis supplied.

¹⁷² Memorandum (for Respondents), 10 March 2022, at 19, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

Service Agreement pertaining to disclosure in relation to credit information systems.¹⁷³ The Commission previously pointed out that the publication is accompanied by a categorical statement, thereby putting into question its alleged non-limitation of liability:

The Commission understands that JuanHand’s disclosure of the personal information of delinquent users to the [Credit Information Corporation] is pursuant to Section K(4)(c) of the Service Agreement[.]

. . .

However, Section K(4)(d) of the Service Agreement allows JuanHand to ‘publish the personal information of such user for the purpose of collecting debt’. Further, JuanHand categorically states that it ‘shall not be held liable’ for such publication.¹⁷⁴

Lastly, while the temporary ban was in effect, the Commission received several reports from JuanHand users who received various messages from its Collection Department containing the DDL of the app.¹⁷⁵ Upon investigation, the EnD was able to download the JuanHand app through the provided DDL.¹⁷⁶ Thus, on 17 September 2021, the EnD sent a letter to JuanHand requiring it to explain the foregoing incident.¹⁷⁷

On 08 October 2021, JuanHand responded to the EnD’s letter.¹⁷⁸ It explained that the DDLs were inadvertently sent in an SMS and email as part of an automatic process which transmits repayment reminders to existing JuanHand users.¹⁷⁹ It reiterated this in its Memorandum, stating that:

100.1. The dissemination of the DDL was done through **automatic, system-generated repayment reminder SMS and emails**, and therefore was done inadvertently, with no intention to violate the Temporary Ban. The DDLs were inadvertently sent through system-generated repayment reminders containing a single hyperlink or DDL [...], which automatically redirects users

¹⁷³ *Id.*

¹⁷⁴ Order, 12 August 2021, at 11, *in re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹⁷⁵ Enforcement Division Letter of Compliance with Order dated 12 August 2021 in NPC SS 21-006 entitled “*In re: Wefund Lending Corporation (JuanHand)*”, 16 September 2021, at 2, *in re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹⁷⁶ *Id.*

¹⁷⁷ *Id.*

¹⁷⁸ Reply and Explanation to the National Privacy Commission Enforcement Division Letter dated 16 September 2021, 08 October 2021, *in re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹⁷⁹ *Id.* at 3.

to the latest version of the JuanHand OLA, regardless of changes and updates to the same.

100.2. Upon becoming aware of the incident, [JuanHand] immediately made efforts to rectify the same.¹⁸⁰

Thus, the Commission finds that JuanHand violated Section 25 of the DPA or Unauthorized Processing of Personal or Sensitive Personal Information.

Unauthorized Processing of Personal or Sensitive Personal Information is committed when:

1. The perpetrator processed the information of the data subject;
2. The information processed was personal information or sensitive personal information; and
3. The processing was done without the consent of the data subject, or without being authorized under the DPA or any existing law.¹⁸¹

All three (3) requisites are present here. The circumstances when taken together substantially demonstrate that JuanHand processed the personal information of its data subjects, particularly their calendar events, without their consent.

On the first requisite, JuanHand processed information of its data subjects. Section 3 of the DPA defines processing as follows:

(j) Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.¹⁸²

In its Position Paper dated 12 August 2021, JuanHand stated that it “[does] also **read** the borrower’s calendar events and **add** or **modify**

¹⁸⁰ Memorandum (for Respondents), 10 March 2022, at 23, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022). Emphasis supplied.

¹⁸¹ NPC 19-134, 10 December 2021, at 12 (NPC 2021) (unreported).

¹⁸² Data Privacy Act of 2012, § 3 (j).

calendar events.”¹⁸³ The first requisite of processing was admitted by JuanHand.

As for the second requisite, the information that JuanHand processed is personal information. Section 3 of the DPA defines personal information:

(g) Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.¹⁸⁴

In its Position Paper dated 12 August 2021, JuanHand admitted that it considered the user’s calendar as a “kind of personal information.”¹⁸⁵ Further, it stated that:

We consider that accessing and modifying user’s calendar is legitimate and proportional to the purpose stated in the Service Agreement for two reasons:

- (i) Credit Analysis and Scoring: by accessing the calendar, we seek to identify due dates of other loans or payment obligations of the users to determine whether or not to provide loan services, and if so, his/her credit limits;
- (ii) Due Day Reminder: by adding due date to the users’ calendar, it would be easier for the users to apprehend the due date and, thus, repayment obligation.

Therefore, we consider that when users give consent to the Service Agreement, users are materially informed the kind of personal information shall be processed in compliance with section 16(a) of the DPA and have given consent to the above functions.¹⁸⁶

As mentioned, JuanHand accessed and used the user’s calendar for credit analysis and scoring and payment reminders. These information allow it to “identify due dates of other loans or payment obligations of the users.”¹⁸⁷ Clearly, the identity of the borrower can be reasonably

¹⁸³ Position Paper, 12 August 2021, at 5, *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022). Emphasis supplied.

¹⁸⁴ Data Privacy Act of 2012, § 3 (g).

¹⁸⁵ Position Paper, 12 August 2021, at 5, *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹⁸⁶ *Id.*

¹⁸⁷ *Id.*

and directly ascertained through the information contained in the calendar. The calendar information, thus, is personal information under the DPA.

As for the third requisite, JuanHand processed personal information without the consent of the data subjects or without lawful basis under the DPA or any existing law.

The CID discussed in its FFR that:

After a thorough search, the CID Technical Team found ‘JuanHand’s Permission Information’ (Annex ‘B’) revealing that JuanHand’s system, **can do** the following:

1. read the borrower’s calendar events plus confidential information;
2. add or modify calendar events;
3. send email to guests without the owner’s knowledge;
4. read borrower’s contacts;
5. collect data from contacts; and
6. pinpoint the borrower’s approximate and precise location through its network and GPS.¹⁸⁸

The CID, through its technical investigation, discovered that during the time it conducted the investigation, JuanHand’s app was able to utilize the abovementioned permissions. Apart from that, prior to the CID’s downloading and installation of the app, the permissions required by the app were outlined in the Google Play Store:¹⁸⁹

- read calendar events plus confidential information;
- add or modify calendar events and send email to guests without owner’s knowledge;
- read your contacts;
- approximate location (network-based); and
- precise location (GPS and network-based).¹⁹⁰

¹⁸⁸ Fact-Finding Report, 09 June 2021, at 4-5, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022). Emphasis supplied.

¹⁸⁹ *Id.* at 2.

¹⁹⁰ Technical Report, 17 May 2021, at 5 (Annex B), *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

As previously discussed, however, JuanHand's Service Agreement does not indicate all of the abovementioned permissions outlined in the Google Play Store and those discovered by the CID during its technical investigation.¹⁹¹ The Service Agreement did not inform the data subjects that it can and does access, read, and modify their calendar events and other confidential information.¹⁹²

Thus, the Commission finds that JuanHand's processing of personal information was without consent of the data subjects.

The CID was able to prove, through its technical investigation, that there were undisclosed permissions not mentioned in the Service Agreement. This is a violation of the general privacy principle of transparency, which requires the Personal Information Controller (PIC) to ensure that the data subject is aware of the nature, purpose, and extent of the processing of his or her personal data.¹⁹³ The principle of transparency similarly requires that these materials be easily accessible and understandable by the data subjects and should be in clear and plain language.¹⁹⁴ The requirement to use clear and plain language means that information should be provided in as simple a manner as possible.¹⁹⁵ In NPC 19-450, the Commission emphasized the "clear and plain language" requirement:

The requirement to use clear and plain language does not mean using layman's terms to substitute technical words at the risk of not capturing the complex concepts they represent. Rather, this requirement means that information should be provided in as simple a manner as possible, avoiding sentence or language structures that are complex. **The information provided should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations** such as in the above-cited provision which uses the word 'any' several times, as well as wordings like 'including but not limited to'.¹⁹⁶

In NPC 19-498, the Commission held that "vague, overbroad, and confusing language cannot be said to comply with the requirements of

¹⁹¹ See Supplemental Report, 31 May 2021, Annex A (JuanHand User Agreement Web), *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

¹⁹² See *id.*

¹⁹³ Rules and Regulations Implementing the Data Privacy Act of 2012, § 18.

¹⁹⁴ *Id.*

¹⁹⁵ See *JRG v. CXXX Lending Corporation*, NPC Case No. 19-450, 09 June 2020, at 6, *available at* https://www.privacy.gov.ph/wp-content/uploads/2022/01/Decision_NPC-19-450-JRG-v.-CXXX.pdf (last accessed 30 May 2022).

¹⁹⁶ *Id.* Emphasis supplied.

the transparency principle.”¹⁹⁷ Statements fail to satisfy the transparency principle if data subjects are not informed of the nature, purpose, and extent of the processing that the PIC is permitted to undertake.¹⁹⁸ The Commission explained as follows:

This vague, overbroad, and confusing language cannot be said to comply with the requirements of the transparency principle and its **objective of providing meaningful information to data subjects to enable them to understand the purpose, scope, nature, and extent of processing of their personal information**. Taken plainly, what Respondent obtained was blanket consent to process the information they acquired from Complainant and not **informed consent to process specific information for a specified and limited purpose**.¹⁹⁹

A PIC, therefore, should inform the data subjects that it will process particular personal information for a specific and limited purpose.²⁰⁰

With these, it can be seen that JuanHand violated the principle of transparency. To recall, “it is the Service Agreement that potential borrowers are asked to consent to and is the one that governs the relationship between the borrower and JuanHand.”²⁰¹ In failing to include certain employed permissions in the Service Agreement, JuanHand did not sufficiently inform its data subjects of its processing pertaining to the undisclosed permissions in a manner that enables them to understand the purpose, scope, nature, and extent of processing of their personal information.²⁰²

In effect, this violation of the general privacy principle of transparency resulted in a violation of Section 25 of the DPA. Since the data subjects were not informed in a way that they can properly understand the specific nature, purpose, and extent of the processing the PIC is permitted to undertake, they were not able to make an informed decision regarding the processing of their personal information. Thus, there can be no valid consent in JuanHand’s processing of their personal information relating to the undisclosed permissions.

¹⁹⁷ NPC Case No 19-498, 09 June 2020, at 8 (NPC 2020) (unreported).

¹⁹⁸ *Id.*

¹⁹⁹ *Id.* Emphasis supplied.

²⁰⁰ *See id.*

²⁰¹ Order, 12 August 2021, at 9, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

²⁰² *See* NPC Case No 19-498, 09 June 2020, at 8 (NPC 2020) (unreported).

JuanHand, in its Position Paper, admitted that the undisclosed permissions were being executed despite its glaring absence in the Service Agreement:

[W]e do also read the borrower's calendar events and add or modify calendar events. We consider that accessing and modifying user's calendar is legitimate and proportional to the purpose stated in the Service Agreement[.]

...

Therefore, we consider that when users give consent to the Service Agreement, users are materially informed the kind of personal information shall be processed in compliance with section 16(a) of the DPA and have given consent to the above functions.²⁰³

As previously discussed, JuanHand should have informed its data subjects that it will process their personal information for a specific and limited purpose. It cannot argue that its borrowers are materially informed since it did not validly acquire its data subjects' consent specific to the nature, purpose, and extent of the particular processing activity.

The Commission reminds PICs that regardless of the basis of processing, the principle of transparency dictates that information regarding the nature, purpose, and extent of the processing of personal information still has to be provided to the data subject.

Moreover, a perusal of JuanHand's argument above shows that it relied on consent and contract for its processing. Nevertheless, it attempted to argue that "accessing and modifying user's calendar is **legitimate and proportional to the purpose** stated in the Service Agreement."²⁰⁴ To recall, it stressed that there is more than one allowable basis for processing in this case, such as consent, contract of loan, and legitimate interest pursued as a lender.²⁰⁵ Therefore, it alleged that it has pursued "legitimate interests and purposes" in processing the personal information of its users.²⁰⁶

²⁰³ Position Paper, 12 August 2021, at 5, *in re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022). Emphasis supplied.

²⁰⁴ *Id.* Emphasis supplied.

²⁰⁵ Comment on the Fact-Finding Report dated 09 June 2021, at 5, 11 October 2021, *in re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

²⁰⁶ *Id.* at 6.

The Commission stresses that legitimate interest cannot be used to circumvent data subject rights. It cannot justify improper processing that has already occurred on the basis of the lawful criteria of consent or contract. Given that JuanHand relied on consent as its lawful criteria for processing, then it must show and prove that it obtained proper and specific consent.

This is not to say that legitimate interest cannot apply alongside consent or contract. Legitimate interest can apply in a contract or in a processing related to consent if it can justify the processing of things already agreed upon by the parties, which can be determined by the type of contract entered into, the relationship of the parties, and other similar circumstances. Thus, legitimate interest can be used to fill in gaps in the contract only if the processing involves something that the data subject can reasonably expect from the terms stated in the contract.

This is not the case for JuanHand since access and modification of a borrower's calendar is not something that a user would reasonably expect to fall under the terms stated in JuanHand's Service Agreement, particularly:

K. Privacy

...

2. Source of information

...

b. In addition to the information provided to JuanHand by the User voluntarily, User agrees that Juanhand and its partners to collect and verify the User's information, including, but not limited to the following manner:

- i. User's information collected by Juanhand and its cooperating party.
- ii. User's information authenticated by the third party.
- iii. information relevant to such User collected by automatically tracking by Juanhand based on the User's behavior on this Website.
- iv. information related to personal communication (including, but not limited to, contact list, geographical location, device identification number, social networking profiles) provided or

authorized by the User, or communication information relating to the activities and logging in by the User provided to Juanhand by other User or third party, Juanhand can collect this information in the User's file.

v. Other information related to the use of Juanhand services by the User.

vi. Juanhand will collect your Facebook platform information through your authorization. Including but not limited to: username, user ID, registered email, gender, etc.²⁰⁷

To do something entirely different and not covered by the Service Agreement is problematic and unfair since data subjects will be made to believe that the processing will not go beyond the terms to which they agreed; but in reality, the PIC crosses the boundary in processing personal information. Thus, JuanHand cannot use legitimate interest in the alternative to fill in the gaps of its contract.

Given the foregoing, JuanHand has no lawful basis under the DPA or any existing laws to process the personal information of its data subjects in relation to the undisclosed permissions.

Taking all the foregoing into consideration, JuanHand violated Section 25 of the DPA.

II. Liability of responsible officers based on Section 34 of the DPA.

The DPA imposes criminal penalties on specific acts, which are imposed by courts of law after the conduct of a criminal trial.²⁰⁸ Upon a finding of a violation, the Commission may recommend to the Department of Justice the prosecution and imposition of penalties on the violations enumerated under the DPA.²⁰⁹ These unlawful acts provided in Sections 25 to 32 are unauthorized processing of personal or sensitive personal information, processing personal or sensitive personal information for unauthorized purposes, accessing of personal or sensitive personal information, unauthorized access or intentional breach, improper disposal of personal or sensitive personal information, concealment of security breaches involving sensitive personal information, malicious disclosure, and unauthorized

²⁰⁷ Supplemental Report, 31 May 2021, Annex A (JuanHand User Agreement Web) at 7-11, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

²⁰⁸ Data Privacy Act of 2012, chapter VIII.

²⁰⁹ *Id.* § 7 (i).

disclosure.²¹⁰ If the PIC or Personal Information Processor (PIP) is a juridical person, then the penalties are imposed on its responsible officers.²¹¹

Corporations and other juridical entities cannot be prosecuted for crimes under Philippine law.²¹² It is an established principle in criminal law that:

Only natural persons can be the active subject [the criminal] because of the highly personal nature of the criminal responsibility.

Since a felony is a punishable act or omission which produces or tends to produce a change in the external world, it follows that **only a natural person can be the active subject [the criminal] of a crime, because he alone by his act can set in motion a cause or by his inaction can make possible the completion of a developing modification in the external world.**²¹³

Specific to violations committed by a corporation, the Revised Corporation Code provides that:

Section 171. *Liability of Directors, Trustees, Officers, or Other Employees.* If the offender is a corporation, the penalty may, at the discretion of the court, be imposed upon such corporation and/or upon its directors, trustees, stockholders, members, officers, or employees **responsible for the violation or indispensable to its commission.**²¹⁴

Jurisprudence provides that corporations have a separate and distinct personality from its officers:

Bicol Gas is a corporation. As such, it is an entity separate and distinct from the persons of its officers, directors, and stockholders. It has been held, however, that **corporate officers or employees, through whose act, default or omission the**

²¹⁰ *Id.* §§ 25-32.

²¹¹ *Id.* § 34.

²¹² See *People v. Tan Boon Kong*, G.R. L-35262 (1930).

²¹³ LUIS B. REYES, *THE REVISED PENAL CODE, CRIMINAL LAW*, BOOK 1 ARTICLES 1-113 505 (2012). Emphasis removed. Emphasis supplied.

²¹⁴ An Act Providing for the Revised Corporation Code of the Philippines [REVISED CORPORATION CODE], Republic Act No. 11232, § 171 (2019). Emphasis supplied.

corporation commits a crime, may themselves be individually held answerable for the crime.²¹⁵

Thus, as held by the Supreme Court, “[a] corporation can act only through its officers and agents, and where the business itself involves a violation of the law, the correct rule is that all who participate in it are liable.”²¹⁶ Certain special laws provide for the particular officers who shall be held responsible for corporate crimes.²¹⁷ In the DPA, this is specified in Section 34.

Therefore, Section 34 supplies the gap in Sections 25 to 32 of the DPA by specifying that the officers of erring corporations are the natural persons that will be held responsible for such violations and will be the accused in the criminal case that will be filed.

The Commission emphasizes that, for juridical entities, a violation of Section 25 does not automatically result in a recommendation for prosecution. Rather, there is a need to identify the proper responsible officers that shall be the accused in the criminal case. With this, the standard for the identification of responsible officers is provided by Section 34 of the DPA. Section 34, therefore, adds another layer for violations of Sections 25 to 32 when juridical entities are involved.

Section 34 of the DPA explicitly states that a responsible officer can be subject to the imposable penalties in two instances: (1) participation in the commission of the crime, or (2) allowing the commission of the violation through gross negligence:

Section 34. *Extent of Liability.* If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, **who participated in, or by their gross negligence,** allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer

²¹⁵ *Espiritu Jr. v. Petron Corporation*, G.R. No. 170891 (2009). Emphasis supplied.

²¹⁶ *People v. Tan Boon Kong*, G.R. L-35262 (1930).

²¹⁷ JOSE R. SUNDIANG, SR. & TIMOTEO B. AQUINO, REVIEWER ON COMMERCIAL LAW 60 (2019).

perpetual or temporary absolute disqualification from office, as the case may be.²¹⁸

The Commission has previously expounded on an officer's liability:

The DPA is clear, however, that the liability of the responsible officers in cases where the offender is a corporation does not rely on active participation alone. Gross negligence is explicitly stated in the DPA as a ground for criminal liability.²¹⁹

In relation to this, the Commission stresses that the clause “who participated in, or by their gross negligence” should be viewed in relation to the acts of the responsible officers that reasonably caused the violation, without which the violation would not have occurred. Ultimately, however, this shall be applied on a case-to-case basis.

Thus, the Commission takes this opportunity to draw a distinction between the different sections in Chapter VIII (Penalties) of the DPA, namely Sections 25 to 32 and Section 34.

The evidence required for Sections 25 to 32 of the DPA is substantial evidence demonstrating that all the elements of the respective violations are present. Meanwhile, the evidence necessary to establish Section 34 of the DPA is substantial evidence proving that the specific responsible officers reasonably caused the violation by their participation or allowed the commission of the violation through their gross negligence.

III. The case should be dismissed for lack of substantial evidence supporting a recommendation for prosecution based on Section 34 of the DPA.

The CID argued that the undisclosed permissions show that “there is sufficient legal and factual basis” for the Commission to hold

²¹⁸ Data Privacy Act of 2012, § 34. Emphasis supplied.

²¹⁹ In Re: FLI Operating ABC Online Lending Application, NPC 19-910, 17 December 2020, at 35, available at <https://www.privacy.gov.ph/wp-content/uploads/2021/02/NPC-19-910-In-re-FLI-Decision-LYA-Final-pseudonymized-17Dec2020-.pdf> (last accessed 30 May 2022).

JuanHand's Corporate Officers and Directors, as the responsible officers, liable.²²⁰ To further bolster its claim, it posited that:

First, Respondent Wefund admitted all the allegations in the Fact-finding Report. It in fact offered to rectify its shortcomings identified in the Order and FFR and undertook to implement immediate rectification and remedial actions. Finally, Wefund warranted that it shall also remain fully cooperative and supportive with the NPC in the further investigation and will be open to promptly rectify any issues and adopt any recommendation made by the NPC.

Second, the responsible officers did not file any comment to the Fact-Finding Report as ordered by the Commission. In Wefund's Position Paper, no defense was interposed as to why the responsible officers should not be penalized if found guilty of the violations of the DPA.²²¹

In arguing that the Corporate Officers and Directors of JuanHand are liable, the CID discussed the abovementioned arguments to harp on Section 34 which states that "liability shall be imposed upon the Board of Directors, as responsible officers, who participated in, or by their gross negligence, allowed the commission of the crime[.]"²²²

In administrative proceedings, however, jurisprudence consistently maintains that: "The burden to establish the charges rests upon the complainant. [...] **The respondent is not even obliged to prove his exception or defense.**"²²³

In line with this, the Commission held in NPC 19-465 that:

[T]he Commission cannot recommend the criminal prosecution of the responsible officers of [Respondent] based on the weakness of their defense.

Ultimately, it is [Complainant] that bears the burden of proving the allegations in her Complaint with substantial evidence. Jurisprudence is settled that **if she 'fail[s] to show in a satisfactory manner the facts upon which [her] claims are**

²²⁰ Memorandum, 16 March 2022, at 9, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022); See Supplementary Fact-Finding Report (with Application for Issuance of Temporary Ban on the Processing of Personal Data), 05 July 2021, at 2-3, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

²²¹ Memorandum, 16 March 2022, at 9, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

²²² *Id.*

²²³ *National Bureau of Investigation v. Conrado M. Najera*, G.R. No. 237522 (2020). Emphasis supplied.

based, the [respondent is] not obliged to prove [its] exception or defense.’²²⁴

Thus, the Commission stresses that, contrary to the CID’s argument, the lack of any defense presented by JuanHand on possible violations committed by its Corporate Officers and Directors is not enough basis to recommend them for prosecution.

In any case, there is no evidence on record, despite the investigation conducted and allegations made by the CID, that sufficiently establishes in any way that JuanHand’s Corporate Officers and Directors (1) participated in or (2) exercised gross negligence in allowing the commission of the crime.

To reiterate, a recommendation for prosecution under Section 34 requires substantial evidence showing that the responsible officers committed acts that reasonably caused the violation, without which the violation would not have occurred, or allowed its commission through their gross negligence.

In this case, there is nothing on record demonstrating that JuanHand’s Corporate Officers and Directors either (1) participated in the violation or (2) by their gross negligence, allowed the commission of the crime in order to hold them liable based on Section 34 of the DPA. The lapses pointed out are sufficient to demonstrate that JuanHand violated Section 25 of the DPA. The lapses themselves do not, however, automatically prove that the elements necessary to hold Corporate Officers and Directors liable based on Section 34 of the DPA are present. Given this, the Commission finds that the lapses in this case are not tantamount to substantial evidence required to warrant a recommendation for prosecution under Section 34 of the DPA.

There is no substantial evidence to prove that JuanHand’s Corporate Officers and Directors participated in the violation. The term “participated in,” as found in Section 34 of the DPA, requires that the responsible officers committed acts that reasonably caused the violation, without which the violation would not have occurred. As such, the instance of “participated in” contemplates a situation wherein the officers and employees that will be recommended for

²²⁴ NPC 19-465, 03 March 2022, at 10 (NPC 2022) (unreported). Emphasis supplied.

prosecution are “responsible” for and the root cause of the violation of the DPA in such a way that if they had not committed certain acts, then the violation would not have transpired. Examples of this instance cover situations wherein the responsible officer directs the execution of the act resulting in the violation or through his acts, reasonably caused the commission of the violation without which such violation would not have occurred. Thus, a sense of causation is essential when determining if the responsible officers may be held liable based on participation.

Given the foregoing, the Commission finds that there is no substantial evidence proving that JuanHand’s Corporate Officers and Directors committed any acts that reasonably caused its violation of Section 25 of the DPA. In the absence of substantial evidence, JuanHand’s Corporate Officers and Directors cannot be held liable based on participation in Section 34 of the DPA.

As for gross negligence, the Commission finds that the second instance of Section 34 is similarly not present in this case. It is settled that “he who alleges has the burden of proving his allegation with the requisite quantum of evidence.”²²⁵ Absent substantial proof, an allegation of gross negligence cannot be presumed. Here, there is no substantial evidence on record demonstrating that JuanHand’s Corporate Officers and Directors by their gross negligence, allowed the commission of the crime.

The Supreme Court defines gross negligence as follows:

[G]ross negligence [...] refers to negligence characterized by the want of even slight care, or by acting or omitting to act in a situation where there is a duty to act, **not inadvertently but wilfully and intentionally, with a conscious indifference** to the consequences, insofar as other persons may be affected. It is the omission of that care that even inattentive and thoughtless men never fail to give to their own property. It denotes a flagrant and culpable refusal or unwillingness of a person to perform a duty.²²⁶

The oversights committed by JuanHand do not demonstrate that its Corporate Officers and Directors refused to perform their necessary duties under the DPA. Moreover, the acts of JuanHand to rectify its

²²⁵ *Tacis v. Shields Security Services, Inc.*, G.R. No. 234575 (2021).

²²⁶ *Securities and Exchange Commissioner v. Commission on Audit*, G.R. No. 252198 (2021). Emphasis supplied.

mistakes upon notification by the Commission show its willingness to comply with its mandated duties.

Pertaining to the DDLs, after being alerted of the incident, JuanHand immediately removed the DDLs from its repayment reminders and ordered that the sent DDLs be inaccessible and deactivated.²²⁷ Furthermore, it sent messages to its users that were able to use, access, or download the app during the period of the temporary ban's effectivity, particularly stating that the app is "currently unavailable for downloading in compliance [with the] National Privacy Commission's order. If you have received Juan[H]and download links before, please do not access it anymore."²²⁸

This was verified by the EnD when it declared that:

The alleged accessible links mentioned in the reports to the CID included in the automated messages through the following links are also no longer working, meaning, the **mobile app is no longer accessible through these links there were reported after the effectivity of the temporary ban[.]**²²⁹

As for the app itself, JuanHand has revised it by (1) removing access to users' calendar, location, contact list and social networking profiles; (2) incorporating more visible pop-up prompts during the registration and loan application procedure when there is an attempt to access or use its users' personal information that would allow users to ask for or modify the permissions that they have granted; and (3) adding a "What's New" feature that allows data subjects to be easily informed of the changes in the app.²³⁰

These were confirmed by the EnD in its assessment. It found that versions 4.1.1 and 4.2.0 of the app are no longer functional and are now unusable; rather, old users are prompted to update to the app's latest version 5.0.0.²³¹ Particularly, as regards the iOS version:

²²⁷ Reply and Explanation to the National Privacy Commission Enforcement Division Letter dated 16 September 2021, 08 October 2021, at 4, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21- 006 (NPC 2022).

²²⁸ *Id.* at 6. Emphasis removed.

²²⁹ Enforcement Division Memorandum, 03 November 2021, at 3, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022). Emphasis supplied.

²³⁰ Memorandum (for Respondents), 10 March 2022, at 9 & 13, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

²³¹ Enforcement Division Enforcement Assessment Report, 28 April 2022, at 3, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

[W]hile there are still no prompts giving the user permission to allow the application to access the phone's contact list, it has an option for manual entry of references. The iOS version now has two options wherein users can input their contact references. First, users can manually enter their contact references. Second, users can choose their contact references from their contact list. According to [JuanHand], this is solely for the purpose of convenience of the users and the application cannot "read" the entire contact lists of users.

...

[T]his claim was verified by EnD. In the generated iOS Privacy Report, it was **confirmed that the JuanHand OLA does not have permission to access the users' contacts**.²³²

Further, it created a separate Privacy Policy excluding access to calendar, location, contact list and social networking accounts of the data subject.²³³ Its Service Agreement, on the other hand, removed all the alleged contentious provisions pointed out by the CID in order to improve compliance with the DPA and its issuances.²³⁴

As regards the alleged violations of the Loan-Related Transactions Circular pointed out by the CID, JuanHand asserted that:

[I]n no instance has it ever used the contact information acquired from the users' contact list as a means of harassment in the process of debt collection.

...

That said, in order to cooperate, comply, and address the concerns of the CID, Respondent WeFund no longer requests for access to the user's contacts list.²³⁵

The Commission takes this opportunity to clarify the Loan-Related Transactions Circular, specifically Section 3(D)(4), which states that:

Access to contact details in whatever form, such as but not limited to phone contact list or e-mail lists, the harvesting of

²³² *Id.* Emphasis supplied.

²³³ Memorandum (for Respondents), 10 March 2022, at 12, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

²³⁴ *Id.* at 17.

²³⁵ *Id.* at 15.

social media contacts, and/or copying or otherwise saving these contacts for use in debt collection or to harass in any way the borrower or his/her contacts, are prohibited. In all instances, online lending apps must have a separate interface where borrowers can provide character references and/or co-makers of their own choosing.²³⁶

The Commission emphasizes that the phrase “access to contact details in whatever form” should be read in the context of the qualifying phrase contained within the same paragraph, “for use in debt collection or to harass in any way [...] are prohibited.”²³⁷ Thus, it is not the collection of contacts nor its access *per se* that is prohibited, especially since there are instances when the collection or processing of contacts falls under lawful processing. Rather, what the Circular strictly prohibits is the utilization of these contacts to unduly burden borrowers when they are used for purposes of debt collection and harassment.

The Loan-Related Transactions Circular similarly contains rules on camera permissions. JuanHand has addressed the issues surrounding camera permissions of both version 4.1.1 and version 4.2.0.²³⁸ Through the “Close Camera Permission” feature, users are now prompted that they may turn off or disallow permission to access their cameras or photo galleries upon uploading their pictures successfully and submitting their loan application.²³⁹ The EnD has validated that this feature is present and functioning.²⁴⁰

Lastly, it has now provided for organizational, physical, and technical measures in both its revised Privacy Policy and Security Incident Management Policy.²⁴¹ As confirmed by the EnD in its assessment, these now align with the DPA and the Commission’s issuances.²⁴²

The Commission notes that, in addition to JuanHand’s willingness to comply with its Orders, its voluntary acts of changing key members of

²³⁶ National Privacy Commission, Guidelines on the Processing of Personal Data for Loan-Related Transactions, Circular No. 01, Series of 2020 [NPC Circ. No. 20-01], § 3 (D)(4) (28 January 2021).

²³⁷ *Id.*

²³⁸ Memorandum (for Respondents), 10 March 2022, at 20, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

²³⁹ *Id.* at 20-21.

²⁴⁰ Enforcement Division Enforcement Assessment Report, 28 April 2022, at 4, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

²⁴¹ Memorandum (for Respondents), 10 March 2022, at 21, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

²⁴² Enforcement Division Enforcement Assessment Report, 28 April 2022, at 2, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

its management team and legal counsel are inconsistent with gross negligence.

JuanHand, in its Supplemental Motion to Resolve, stated that it has now “initiated the appointment of a more senior and experienced legal and compliance manager in the management team as the new data privacy officer in due course, to better oversee the compliance and protection of its users’ data privacy.”²⁴³ The Commission considers the efforts of JuanHand in diligently complying with its obligations as a PIC by appointing more experienced members to its managerial team in order to better protect the rights of its data subjects.

Moreover, the Commission recognizes its change in counsel as a badge of its willingness to comply with the DPA and the Commission’s issuances. JuanHand, through its former counsel,²⁴⁴ attempted to rectify the alleged errors pointed out by the CID by preparing and attaching to its Position Paper a standalone Privacy Policy that was independent from the Service Agreement and that complied with the DPA.²⁴⁵ Despite the rectifications made, the Commission was unconvinced that there is no potential danger to data subjects, thus an Order granting the temporary ban to preserve and protect the rights of the data subjects was issued:

An analysis of JuanHand’s Position Paper, Service Agreement, and revised Privacy Policy shows that the issuance of the temporary ban is necessary to protect the rights of data subjects for the following reasons: (1) JuanHand’s preparation and submission of a ‘standalone and rectified Privacy Policy independent from the Service Agreement’ does not necessarily change the manner it processes personal data; (2) JuanHand’s understanding and application of the criteria of lawful processing personal data, as gleaned from its revised Privacy Policy, is ambiguous; (3) JuanHand’s allegations in the Position Paper are inconsistent with its Service Agreement and revised Privacy Policy.²⁴⁶

On 10 September 2021, JuanHand’s new counsel entered its appearance.²⁴⁷ Evidently, JuanHand, through its new counsel, was

²⁴³ Supplemental Motion to Resolve, 10 January 2022, at 5, *in* *In re: Wefund Lending Corporation and its Responsible Officers*, NPC SS 21-006, (NPC 2022).

²⁴⁴ Entry of Appearance of the Former Counsel was on 10 August 2021.

²⁴⁵ Position Paper, 12 August 2021, at 2, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No 21-006 (NPC 2022).

²⁴⁶ Order, 12 August 2021, at 7, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

²⁴⁷ Entry of Appearance with Motion to Admit [Supplemental Comment with Motion for Lifting of Temporary Ban], at 1, *in* *In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers*, NPC SS Case No. 21-006 (NPC 2022).

able to properly address, to the satisfaction of the Commission, the initial lapses discovered by the CID that resulted in the imposition of the temporary ban. As a result, the Commission issued a Resolution lifting the temporary ban.²⁴⁸

Thus, taking into account the totality of the evidence and circumstances, JuanHand clearly demonstrated that its dedication to swiftly and substantially rectify its errors contradict the presence of willful and conscious indifference. Thus, despite the lapses present in this case, it does not amount to gross negligence sufficient to recommend JuanHand's Corporate Officers and Directors for prosecution based on Section 34 of the DPA.

Moreover, the Commission notes that the imposition of a temporary ban against JuanHand would not automatically result in an eventual recommendation for prosecution based on Section 34 of the DPA.

To recall, a temporary ban against JuanHand was granted on 12 August 2021 since all the requisites for its issuance were satisfied.²⁴⁹ Nevertheless, the Commission eventually issued a Resolution on 13 January 2022 lifting the temporary ban.²⁵⁰

The threshold for the issuance of a temporary ban is different from that of a recommendation for prosecution. A temporary ban, being a provisional remedy, is granted in order to prevent any potential harm from arising as well as to deter any further harm to data subjects from proliferating. Thus, the existence of a clear and present potential harm may result in the granting of a temporary ban. Its issuance, however, is not definitive proof that warrants a recommendation for prosecution. The Commission, in determining recommendations for prosecution, must still decide based on the totality of evidence presented, since it is bound to adjudicate based on the following:

²⁴⁸ Resolution, 13 January 2022, at 6, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

²⁴⁹ Order, 12 August 2021, at 6-15, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

²⁵⁰ Resolution, 13 January 2022, at 6, *in* In re: Wefund Lending Corporation (JuanHand) and its Responsible Officers, NPC SS Case No. 21-006 (NPC 2022).

Section 3. *Rendition of decision.* The Decision of the Commission shall resolve the issues **on the basis of all the evidence presented** and its own consideration of the law.²⁵¹

Despite its investigation, the CID failed to present substantial evidence with respect to the Corporate Officers and Directors of JuanHand to support the allegations pertaining to Section 34 of the DPA. It cannot be assumed that JuanHand's Corporate Officers and Directors can be held liable based on Section 34 of the DPA simply because of their position. Given the foregoing, the Commission is constrained to find that there is no showing that JuanHand's Corporate Officers and Directors participated in the violation nor allowed its commission by their gross negligence. Without proof, JuanHand's Corporate Officers and Directors cannot be recommended for prosecution under the DPA.

WHEREFORE, premises considered, this Commission resolves that the case filed against Wefund Lending Corporation and its Corporate Officers and Directors is hereby **DISMISSED**.

This is without prejudice to the filing of appropriate civil, criminal, or administrative cases, if any, against Wefund Lending Corporation and its Responsible Officers.

SO ORDERED.

City of Pasay, Philippines.
16 May 2022.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

²⁵¹ National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC 2021 Rules of Procedure], rule VIII, § 3 (28 January 2021). Emphasis supplied.

JOHN HENRY D. NAGA
Privacy Commissioner

DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

VASIG ABARQUEZ LUMAUIG ABARQUEZ PUNO
Counsel for Respondents

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION**
GENERAL RECORDS UNIT
National Privacy Commission

EDF,

Complainant,

- versus -

**BANK OF THE PHILIPPINE
ISLANDS,**

Respondent.

X X

NPC 21-016

For: Violation of
the Data Privacy
Act of 2012

DECISION

AGUIRRE, D.P.C.:

Before this Commission is a Complaint filed by EDF against the Bank of the Philippine Islands (BPI) for a violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

On 11 November 2020, EDF received a call from a woman claiming to be a BPI employee who was supposedly conducting security enhancements on his BPI online account.¹ EDF alleges that the woman informed him of his full name and that she needed to log-in to his BPI online account to implement the security enhancements.² EDF maintains that the woman requested him to dictate several “number codes” that he received through text messages.³ EDF admits that he cooperated with her requests only to belatedly realize that it was a scam.⁴

On the same day, EDF reported the incident to BPI – Zamboanga Main.⁵ He asserts that a BPI customer representative informed him

¹ Complaints-Assisted Form, 15 January 2021, at 3-4, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

² *Id.*

³ *Id.*

⁴ *Id.*

⁵ *Id.*

that his BPI Online account and BPI credit card were already blocked, that an online funds transfer to a GCash account amounting to Four Thousand Four Hundred Pesos (P4,400.00) could no longer be reversed, and that several transactions with Lazada amounting to Ninety Thousand Pesos (P90,000.00) were still floating.⁶

On 15 January 2021, EDF filed a complaint against BPI.⁷ He alleges that BPI committed a “privacy violation” because the woman claiming to be its personnel had knowledge of his BPI online account.⁸ He prays for the reversal of the Lazada transactions and the arrest of the woman purporting to be BPI’s personnel.⁹

On 21 July 2021, the Commission issued an Order directing BPI to file a verified comment fifteen (15) calendar days from receipt of the Order and to appear for preliminary conferences on 25 August 2021 and 08 September 2021.¹⁰

On 25 August 2021, EDF appeared for the first preliminary conference and expressed his willingness to undergo mediation proceedings.¹¹ BPI did not appear due to a conflict of schedule.¹²

On 08 September 2021, both parties appeared for the second preliminary conference and manifested their willingness to undergo mediation proceedings.¹³

On 20 October 2021, BPI filed its Comment.¹⁴ BPI explains that it investigated the disputed online funds transfer transaction to GCash and the disputed credit card transactions.¹⁵ It maintains that the complaint should have been dismissed outright by the Commission according to Rule IV, Section 1 of NPC Circular No. 2021-01 (2021 NPC Rules of Procedure).¹⁶ BPI argues that the cause of action neither pertains to a violation of the DPA nor involve a privacy violation or

⁶ *Id.*

⁷ Complaints-Assisted Form, 15 January 2021, at 3-4, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

⁸ *Id.*

⁹ *Id.* at 5.

¹⁰ Order (To File Verified Comment and Appear Virtually for Preliminary Conference), 21 July 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

¹¹ Fact-Finding Report, 17 September 2022, at 2, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

¹² *Id.*

¹³ *Id.*

¹⁴ Comment, 20 October 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

¹⁵ *Id.* at 1-3.

¹⁶ *Id.*

personal data breach, and that EDF presented insufficient information to substantiate the allegations in the complaint.¹⁷

It also alleges that EDF failed to establish by competent evidence that the disputed online funds transfer and credit card transactions were unauthorized.¹⁸ It reiterates the validity of the transactions:

Your Online Banking account was accessed using your nominated User Name and Password. Succeeding transactions were further authenticated by a One-Time PIN (OTP)/ Mobile Key.

May we reiterate that the transactions done via the [sic] BPI Online can only be completed by undergoing several security measures:

1. Device binding – The device must be linked to client's online account to ensure that the account can only be accessed in client's trusted devices. One-Time PIN [OTP] (which is sent only to client's registered mobile number with the Bank) is required to link the device.
2. User Name and Password – The user is required to input his online credentials to access the account.
3. One-Time PIN (OTP) or Mobile Key for transactions – The user is required to input an OTP or Mobile key [sic] to execute financial transactions, except for transfer to own account.

Given these security measures in place, the Bank had discharged its obligation in providing a safe and secure online banking platform. Since the personal banking information, which were under your control, were unfortunately compromised at your end, we regret to state that we are unable to grant reversal of your disputed transactions under the terms of use of the Internet Banking Service Agreement in place.¹⁹

It further explains that it implements a multi-factor authentication method to verify online fund transfers through BPI Online and online credit card transactions:

10. It must be emphasized that the Respondent implements a multi-factor authentication method to verify online funds transfers through BPI Online, and online credit card transactions. BPI Online transactions are authenticated through the concurrence of the following personal data conclusively presumed to be known only to the depositor:

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.* at 2.

1. BPI Online username;
2. BPI Online password; and
3. one-time-password (“OTP,” for brevity) sent to the depositor’s registered mobile number at the time of the transaction.

11. With regard to online credit card transactions, they are authenticated through the concurrence of the following personal data conclusively presumed to be known only to the depositor:

1. 16-digit credit card number printed on the face of the credit card;
2. expiry date printed on the face of the card;
3. 3-digit CVC printed on the back of the card; and
4. one-time-password (“OTP,” for brevity) sent to the cardholder’s registered mobile number, or his/her static 16- digit Customer Number.

12. In the present case, the disputed transactions would not have been made without the concurrence of the foregoing personal data. Therefore, the transactions are conclusively presumed to be made by the Complainant himself. He has the burden to present clear and convincing evidence to prove otherwise. Bare self- serving allegations do not equate to proof.²⁰

On 19 October 2021, the parties conferred for mediation but failed to reach a settlement.²¹ On 25 November 2021, the Commission issued an Order for the resumption of complaint proceedings and ordered the parties to submit their respective Memoranda within fifteen (15) calendar days from receipt of the Order.²²

On 06 December 2021, EDF filed a Motion for Extension of Time to Submit Memoranda.²³ The Commission granted EDF until 26 December 2021 to submit his Memorandum.²⁴

On 27 December 2021, EDF filed his Memorandum.²⁵ He alleges that he “never shared his mobile number to individuals not known to him, more so his BPI Accounts are only known to him and [BPI].”²⁶ He further argues that BPI failed to perform its mandatory obligations

²⁰ Comment, 20 October 2021, at 2-3, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

²¹ Order to Mediate, 14 September 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

²² Order (Resumption of Complaints Proceedings and Submission of Memoranda), 25 November 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

²³ Motion for Extension, 06 December 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

²⁴ Order (Granting the Request for Extension of Time to Submit Memoranda filed by Complainant), 13 December 2021, *in*

EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

²⁵ Memorandum for the Complainant, 27 December 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21- 016 (NPC 2021).

²⁶ *Id.* at 6.

under Section 20 of the DPA in implementing reasonable and appropriate organizational, physical, and technical measures for the protection of his personal information, particularly his personal mobile number, BPI Accounts, office address, date of birth, and mother's maiden name.²⁷

He maintains that his confidential personal information was breached because BPI was remiss in its mandatory obligation to secure his personal information, which are "under the safekeeping of BPI."²⁸ He also avers that BPI did not exercise the necessary due diligence when it failed to inform him of the dubious Lazada transactions that were charged to his BPI credit card.²⁹

Because of BPI's supposed failure to safeguard EDF's personal information, he prays that BPI should be held liable for Section 26 (Accessing of Personal Information and Sensitive Personal Information Due to Negligence), Section 27 (Improper Disposal of Personal Information and Sensitive Personal Information), and Section 32 (Unauthorized Disclosure) of the DPA.³⁰ He also prays that BPI should be ordered to reverse the Lazada transactions and all other related charges as damages.³¹

BPI did not file its Memorandum.

Issue

Whether BPI's supposed failure to safeguard EDF's personal information constitutes a violation of the DPA.

Discussion

The Commission dismisses the case for lack of substantial evidence.

²⁷ *Id.* at 6-7.

²⁸ *Id.* at 7.

²⁹ *Id.* at 10.

³⁰ *Id.* at 8-9.

³¹ Memorandum for the Complainant, 27 December 2021, at 11, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

BPI argues that the case before the Commission should have been dismissed outright according to Rule IV, Section 1 of the 2021 NPC Rules of Procedure.³²

Section 1. *Outright dismissal, when allowed.* – Within thirty (30) calendar days from receipt of the complaint, the investigating officer may give the complaint due course or dismiss the complaint without prejudice, on any the following grounds:

1. The complaint is insufficient in form or did not comply with Section 3, Rule II of these Rules, unless failure to do so is justified or excused with good cause;
2. The complainant did not give the respondent an opportunity to address the complaint, unless failure to do so is justified;
3. **The complaint does not pertain to a violation of the Data Privacy Act of 2012 or does not involve a privacy violation or personal data breach;**
4. **There is insufficient information to substantiate the allegations in the complaint; or**
5. The parties, other than the responsible officers in case of juridical persons, cannot be identified or traced despite diligent effort to determine the same.³³

BPI's contention is untenable. EDF's complaint should not have been dismissed outright. First, the complaint asserts a cause of action for a privacy violation, which requires the Commission's careful consideration. The mere allegation, however, that EDF's BPI Online Account, credit card, and other details are involved is not, by itself, sufficient. In this case, as stated in EDF's complaint, the unidentified caller knew of EDF's full name and other pieces of personal information, such as his office address, date of birth, and mother's maiden name.³⁴ This allegation, together with his allegations concerning the disputed transactions using his BPI Online Account and online credit card transactions, show that a cause of action is sufficiently stated in the complaint.

Second, an outright dismissal based on "insufficient information to substantiate the allegations in the complaint" would have been unfair to EDF.

³² Comment, 20 October 2021, at 1-3, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

³³ National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC 2021 Rules of Procedure], rule IV, § 1 (28 January 2021). Emphasis supplied.

³⁴ Complaints-Assisted Form, 15 January 2021, at 3-4, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021)

To substantiate his complaint, EDF submitted Statements of Account showing the supposedly unauthorized transactions on his BPI Online account and credit card, and an email containing the results of BPI's internal investigation.³⁵ The Commission, however, recognizes that EDF could not have had been able to submit other pieces of evidence to substantiate his claims apart from those that he submitted when the complaint was filed. As such, to dismiss the case outright without giving EDF the opportunity to confer for preliminary conference and avail himself of discovery proceedings would have been unfair to him.

In this case, the parties conferred for preliminary conference according to Rule V, Section 1 (2) of the 2021 NPC Rules of Procedure:

Section 1. *Order to confer for preliminary conference.* – No later than thirty (30) calendar days from the lapse of the reglementary period to file the comment, the investigating officer shall hold a preliminary conference to determine:

1. whether alternative dispute resolution may be availed by the parties;
2. **whether discovery is reasonably likely to be sought in the proceeding;**
3. simplification of issues;
4. possibility of obtaining stipulations or admissions of facts and of documents to avoid unnecessary proof; or
5. such other matters as may aid in the prompt disposition of the action.³⁶

The Supreme Court explained the purpose of discovery proceedings:

What is chiefly contemplated is the discovery of every bit of information which may be useful in the preparation for trial, such as the identity and location of persons having knowledge of relevant facts; those relevant facts themselves; and the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things.³⁷|||

Discovery proceedings are essential, such as in this case, where the complainant cannot simply rely on the evidence it has to properly substantiate its allegations.³⁸ In this case, the evidence that EDF

³⁵ *Id.* Annex.

³⁶ NPC 2021 Rules of Procedure, rule V, § 1. Emphasis supplied.

³⁷ *Producers Bank of the Philippines v. Court of Appeals*, G.R. No. 11049 (1998).

³⁸ *See id.*

could have presented to prove the existence of a privacy violation and BPI's supposed liability are most likely in the hands of BPI. Aside from the pieces of evidence that EDF submitted with his complaint, he could not have been able to produce other pieces of evidence to substantiate his allegations.

Following this, EDF could have availed himself of discovery proceedings to seek additional information and documents from BPI to substantiate his claims during the preliminary conference. Yet, he did not. Instead, he merely relied on the evidence that he submitted with his complaint.

Further, EDF himself admitted in his complaint that he received a call from an unverified person and gave several "number codes" that he received through text messages.³⁹ Although EDF never used the term one-time password (OTP), these "number codes" seemingly correspond to the OTP sent to the BPI depositor's registered mobile number at the time of the transaction in order to validate the BPI Online account and online credit card transactions.

By admitting that he dictated these "number codes" or OTP to the unverified person, the burden of evidence shifted to EDF requiring him to present evidence to support his claims against BPI. Section 1, Rule 131 of the 2019 Amendments to the Revised Rules on Evidence provides:

Section 1. *Burden of proof and burden of evidence.* - Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim or defense by the amount of evidence required by law. Burden of proof never shifts.

Burden of evidence is the duty of a party to present evidence sufficient to establish or rebut a fact in issue to establish a *prima facie* case. Burden of evidence may shift from one party to the other in the course of the proceedings, depending on the exigencies of the case.⁴⁰

In his Memoranda, EDF asserts BPI's supposed failure to implement security measures and to safeguard his personal

³⁹ Complaints-Assisted Form, 15 January 2021, at 3, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

⁴⁰ 2019 AMENDMENT TO THE 1989 REVISED RULES ON EVIDENCE, A.M. No. 19-08-15-SC, Rule 131, §1 (1 May 2020). Emphasis supplied.

information resulted in a breach of his confidential personal information following Section 20 of the DPA, which provides:

Section 20. *Security of Personal Information.* – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.⁴¹

EDF claims that as a result of BPI's inaction, his BPI Online account and credit card were used for the disputed transactions.⁴² EDF, however, failed to provide evidence to categorically substantiate his claim. Despite being given the opportunity to do so, EDF did not seek additional information and documents from BPI.

It is not sufficient for EDF to make allegations without substantial evidence to support his claims, considering that:

The basic rule is that mere allegation is not evidence and is not equivalent to proof. Likewise, charges based on mere suspicion and speculation cannot be given credence.⁴³

Contrary to EDF's assertions, BPI was not remiss in its obligation to implement security measures under the DPA. It maintains that it implements a multi-factor authentication method, which requires "personal data conclusively presumed to be known only to the depositor" to verify online fund transfers through BPI Online and online credit card transactions.⁴⁴ As explained in BPI's Comment, such transactions require a user-nominated user name and password, and an OTP that is sent only to the user's registered mobile number.⁴⁵ The fact that there was an OTP required in the supposedly unauthorized transactions shows that BPI implemented its multi-factor authentication.

⁴¹ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (a) (2012).

⁴² Memorandum for the Complainant, 27 December 2021, at 7, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

⁴³ BSA Tower Condominium Corp. v. Reyes II, A.C. No. 11944 (2018).

⁴⁴ Comment, 20 October 2021, at 1-3, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

⁴⁵ See Comment, 20 October 2021, at 2, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

As admitted in his complaint, EDF's own actions directly resulted in the disputed transactions. To reiterate, it was EDF himself who dictated the "number codes" or OTP to the unverified caller.⁴⁶ The fact that the unverified caller allegedly knew EDF's personal information does not automatically mean that there was a breach or negligence on the part of BPI.

The Commission reminds data subjects that they should endeavor to protect their personal data, including bank account numbers, log-in credentials, credit card details, and OTP through email links, text messages or phone calls, to avoid possible risk or harm. As this Commission ruled in CID 17-K-004, "[the] security of personal information is a joint obligation of both the data subjects and data controller or processor. Implementation of a 'reasonable' security measure does not mean that the measure is a foolproof [sic] for any contributory negligence on the part of the data subject."⁴⁷

EDF's admission, and the lack of substantial evidence to support his allegations cannot give rise to the conclusion that BPI's failed to implement security measures and that this supposed failure resulted in the unauthorized transactions. Given the foregoing, the Commission cannot find BPI liable for violating Section 26 (Accessing of Personal Information and Sensitive Personal Information Due to Negligence), Section 27 (Improper Disposal of Personal Information and Sensitive Personal Information), and Section 32 (Unauthorized Disclosure) of the DPA.

As to EDF's prayer on the reversal of the unauthorized transactions, such is beyond the jurisdiction of the Commission.

WHEREFORE, premises considered, the Commission resolves to **DISMISS** the Complaint of EDF against the Bank of the Philippine Islands.

SO ORDERED.

Pasay City, Philippines.

⁴⁶ See Complaints-Assisted Form, 15 January 2021, at 3-4, *in* EDF v. Bank of the Philippine Islands, NPC 21- 016 (NPC 2021).

⁴⁷ CBI v. XXX, CID 17-K-004, 29 September 2020, at 5-6, *available at* <https://www.privacy.gov.ph/wp-content/uploads/2020/12/CID-17-K-004-CBI-v-XXX-Decision-ADJU1.pdf> (last accessed 04 April 2022).

17 March 2022.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

EDF
Complainant

BANK OF THE PHILIPPINE ISLANDS
Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT

National Privacy Commission

JCB,

Complainant,

-versus-

NPC 21-031

For: Violation of
the Data Privacy
Act of 2012

FRL,

Respondent.

X-----X

DECISION

AGUIRRE, D.P.C.;

Before this Commission is a Complaint filed by JCB against FRL (FRL) for an alleged violation of the Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

On 02 February 2021, JCB filed a Complaint against FRL.¹ In his Complaint Affidavit, JCB stated that he is a teacher at Don Andres Soriano National High School.² FRL is a teacher, guidance counselor, and a member of the Grievance Committee in the same school.³

JCB alleged that on 26 August 2020, MSG, a co-teacher, filed an administrative complaint against him before the Office of the Regional Director of the Department of Education (DepEd) Region

VII. The administrative complaint was filed for dishonesty, grave misconduct, being notoriously undesirable, and violation of the Code of Ethics for Professional Teachers.⁴

¹ Complaints-Assisted Form, 02 February 2021, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

² Complaint Affidavit, 26 January 2021, ¶ 1, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

³ *Id.* ¶ 3.

⁴ *Id.* ¶ 4.

One of the attachments in the administrative complaint was FRL's sworn statement that narrated several incidents involving JCB. JCB alleged that the incidents mentioned in FRL's affidavit were already settled amicably by the parties involved.⁵ He also asserted that the settlement should be treated as confidential to preserve its integrity.⁶

In disclosing confidential information relating to the incidents, JCB claimed that FRL should be held liable for violating the DPA.⁷

On 02 September 2021, the Commission issued an Order giving due course to JCB's Complaint and ordering FRL to file her Comment within fifteen (15) calendar days from receipt of the Order.⁸ The Order also provided the schedule for the preliminary conference.⁹

On 30 September 2021, the preliminary conference was held, however, only JCB attended. Thus, the preliminary conference was reset to 28 October 2021.¹⁰

FRL failed to appear for the second time in the preliminary conference. Therefore, the Commission issued an Order dated 28 October 2021 stating that FRL was deemed to have waived her rights to the benefits of the preliminary conference.¹¹

On 03 November 2021, FRL filed her Comment.¹² She argued that the Complaint should be dismissed for JCB's failure to exhaust administrative remedies.¹³

Particularly, FRL alleged that JCB failed to comply with Section 2, Rule II of NPC Circular No. 2021-01 (2021 NPC Rules of Procedure). She cited JCB's statement in his Complaints-Assisted Form that he did not contact FRL because "[she] is not a person-in-interest and has no legal standing."¹⁴

⁵ *Id.* ¶ 5.

⁶ *Id.* ¶ 25.

⁷ *Id.* ¶ 43.

⁸ Order, 02 September 2021, at 1, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

⁹ *Id.*

¹⁰ Order, 30 September 2021, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

¹¹ Order, 28 October 2021, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

¹² Comment, 03 November 2021, at 1, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

¹³ *Id.* at 3-4.

¹⁴ *Id.* at 4.

Further, FRL alleged that JCB's Complaint was not verified and did not contain a certification against forum shopping. As such, FRL argued that the Complaint should be dismissed for failure to comply with Section 3 (1) and (10), Rule II of NPC Circular No. 2021-01.¹⁵

Nonetheless, FRL argued that she did not violate the DPA because the processing of personal information was exempted from the coverage of the law.¹⁶

In applying Section 4 (a) of the DPA, FRL argued that she merely processed the information of JCB, who is an employee of DepEd, a government institution.¹⁷ She also claimed that the information processed were related to JCB's position or function as a government employee.¹⁸

Further, FRL stated that the processing of information was exempted under Section 13 (f) of the DPA.¹⁹ According to her, the affidavit was executed to support the administrative case filed by MSG, who intended "to exercise her legal right and responsibility to the Republic of the Philippines in helping it to get rid of unfit government officials and employees."²⁰

Issue

- I. Whether the case should be dismissed on procedural grounds.
- II. Whether FRL had lawful basis in processing JCB's personal information.
- III. Whether FRL is liable under Section 31 (Malicious Disclosure) of the DPA.
- IV. Whether FRL is liable under Section 32 (Unauthorized Disclosure) of the DPA.

¹⁵ *Id.* at 4-6.

¹⁶ *Id.* at 6.

¹⁷ *Id.* at 7.

¹⁸ Comment, 03 November 2021, at 7, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

¹⁹ *Id.*

²⁰ *Id.*

Discussion

The Commission shall limit its disposition of the case to the issues on the processing of personal information. Therefore, it shall not discuss the alleged violations of laws and administrative orders that are beyond its jurisdiction.²¹

I. The case should be dismissed outright on procedural grounds.

FRL argued that the case should be dismissed because JCB failed to inform her of the alleged privacy violation or personal data breach as required under Section 2, Rule II of NPC Circular No. 2021-01.²²

Further, FRL asserted that JCB's Complaint was not verified and did not contain a certification against forum shopping in violation of the procedural requirement under Section 3, Rule II of NPC Circular No. 2021-01.²³ She alleged that "the Complaint is defective on its face and should be dismissed outright."²⁴

Section 2, Rule II of NPC Circular No. 2021-01 provides:

Section 2. *Exhaustion of remedies.* – No complaint shall be given due course unless it has been sufficiently established and proven that:

1. the complainant has informed, in writing, the personal information controller (PIC), personal information processor (PIP), or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same; and
2. the PIC, PIP, or concerned entity did not take timely or appropriate action on the claimed privacy violation or personal data breach, or there is no response from the PIC, PIP, or concerned entity within fifteen (15) calendar days from receipt of written information from the complainant.

²¹ See Complaint Affidavit, 26 January 2021, ¶¶ 33, 36-38, 40, *in* JCB v. FRL, NPC 21-031 (NPC 2021); Complainant's

Memorandum, 12 November 2021, ¶¶ 32-34, 49-58, 63-64, 66, 71, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

²² Comment, 03 November 2021, at 3, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

²³ *Id.* at 4-5.

²⁴ *Id.* at 6.

The NPC may waive any or all of the requirements of this Section at its discretion upon (a) good cause shown, properly alleged and proved by the complainant; or (b) if the allegations in the complaint involve a serious violation or breach of the Data Privacy Act of 2012, taking into account the risk of harm to the affected data subject, including but not limited to:

- i. when there is grave and irreparable damage which can only be prevented or mitigated by action of the NPC;
- ii. when the respondent cannot provide any plain, speedy or adequate remedy to the alleged violation; or
- iii. the action of the respondent is patently illegal.²⁵

In this case, there is no showing that JCB informed FRL of the alleged privacy violation or personal data breach. He even stated in his Complaints-Assisted Form that he did not contact FRL because she “is not a person-in-interest and has no legal standing.”²⁶ Contrary to JCB’s allegation, FRL should have been informed prior to the filing of his Complaint. Otherwise, pursuant to Section 2, Rule II of NPC Circular No. 2021-01, the Complaint should not be given due course.

While it is true that Section 2, Rule II of NPC Circular No. 2021-01 provides for instances where the Commission may exercise its discretion to waive any or all of the requirements, none of these are present in this case.

The allegations in JCB’s Complaint do not establish a good cause or a potential serious violation or breach of the DPA that would warrant the waiver of the procedural requirements. The facts alleged in his Complaint, even assuming they were all true, still do not support his claim that FRL violated the DPA or that FRL acquired the personal information complained of in her role as a guidance counselor. Furthermore, JCB failed to support any of his allegations with substantial proof. Given that JCB’s case does not fall under the instances provided under Section 2, Rule II of NPC Circular No. 2021- 01, the Commission, therefore, finds no reason to waive the procedural requirements.

²⁵ National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission, [NPC 2021 Rules of Procedure], rule II, § 2 (28 January 2021).

²⁶ Complaints-Assisted Form, 02 February 2021, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

As regards verification and certification against forum shopping, Section 3, Rule II of NPC Circular No. 2021-01 provides:

Section 3. *Form and contents of the complaint.* – The complaint should be in the proper form, as follows:

1. The complaint must be in writing, signed by the party or his or her counsel, and verified in the format prescribed under the Rules of Court.

...

10. A certification against forum shopping must accompany the complaint. The complainant shall certify under oath in the complaint, or in a sworn certification annexed and simultaneously filed with the pleading: (a) that he or she has not commenced any action or filed any claim involving the same issues in any court, tribunal or quasi-judicial agency and, to the best of his or her knowledge, no such other action or claim is pending with such court, tribunal or quasi-judicial agency; (b) if there is such other pending action or claim, a complete statement of its present status; and (c) if he or she should thereafter learn that the same or similar action or claim has been filed or is pending, he or she shall report that fact within five (5) calendar days therefrom to the NPC.

Failure to comply with the proper form and contents of the complaint may cause for outright dismissal under Section 1(1), Rule IV: *Provided*, an application that does not comply with the foregoing requirements may be acted upon if it merits appropriate consideration on its face, or is of such notoriety that it necessarily contains sufficient leads or particulars to enable the taking of further action.²⁷

As such, Complaints filed before the Commission should be “verified in the format prescribed under the Rules of Court.”²⁸

Section 4, Rule 7 of the Rules of Court provides:

Section 4. *Verification.* –

...

²⁷ NPC 2021 Rules of Procedure, rule II, § 3.

²⁸ *Id.* rule II, § 3 (1).

A pleading is verified by an affidavit of an affiant duly authorized to sign said verification. The authorization of the affiant to act on behalf of a party, whether in the form of a secretary's certificate or a special power of attorney, should be attached to the pleading, and shall allege the following attestations:

- (a) The allegations in the pleading are true and correct based on his personal knowledge, or based on authentic documents;
- (b) The pleading is not filed to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and
- (c) The factual allegations therein have evidentiary support or, if specifically so identified, will likewise have evidentiary support after a reasonable opportunity for discovery.

The signature of the affiant shall further serve as a certification of the truthfulness of the allegations in the pleading.²⁹

In the case at bar, the Complaint filed by JCB does not specifically state the attestations enumerated under the Rules of Court. While the Supreme Court has previously ruled that technical rules of procedure do not strictly apply to administrative bodies,³⁰ the notarized Complaint still failed to effectively provide the attestations required because the only thing certified by the notarization is the fact that it was personally executed by JCB.

Additionally, Section 3 (10), Rule II of NPC Circular No. 2021-01 provides that the complaint should be accompanied by a certification against forum shopping.³¹ JCB, however, similarly failed to observe this procedural requirement when he did not attach any certification with his Complaint, nor provided any attestation enumerated in the Section.

The Supreme Court explained the mandatory nature of the requirement on certification:

²⁹ 2019 AMENDMENTS TO THE 1997 RULES OF CIVIL PROCEDURE, rule 7, § 4.

³⁰ DP v. Florentino International, Inc., G.R. No. 186967 (2017).

³¹ NPC 2021 Rules of Procedure, rule II, § 3 (10).

[T]he rules on forum shopping, which were designed to promote and facilitate the orderly administration of justice, should not be interpreted with such absolute literalness as to subvert its own ultimate and legitimate objective. Strict compliance with the provision regarding the certificate of non- forum shopping underscores its mandatory nature in that the certification cannot be altogether dispensed with or its requirements completely disregarded.³²

The Court further elucidated on the difference between non-compliance and substantial compliance with procedural requirements:

A distinction must be made between non-compliance with the requirement on or submission of defective verification, and non-compliance with the requirement on or submission of defective certification against forum shopping.

...

As to certification against forum shopping, non-compliance therewith or a defect therein, unlike in verification, is generally not curable by its subsequent submission or correction thereof, unless there is a need to relax the Rule on the ground of "substantial compliance" or presence of "special circumstances or compelling reasons."

Here, JCB's failure to attach any certification with his Complaint shows non-compliance with the mandatory procedural requirement. Further, there can be no substantial compliance since he did not provide any attestation that could effectively be considered as certification against forum shopping.

As JCB failed to observe the procedural requirements provided under Sections 2 and 3, Rule II of NPC Circular No. 2021-01, JCB's Complaint should have been dismissed outright and not be given due course.

Nevertheless, the Commission proceeds to explain the substantial aspect of the case for the education and guidance of the public.

³² P v. Coca-Cola Philippines, Inc., G.R. No. 157966 (2008).

II. FRL had lawful basis in processing JCB's personal information.

A. The information included in the affidavit are personal information.

FRL's affidavit narrates the incidents involving JCB and his colleagues and contained the names of JCB and his co-teachers.³³

Personal information is defined under Section 3 (g) of the DPA:

Section 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

...

(g) *Personal information* refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.³⁴

The names stated in the affidavit can reasonably and directly ascertain the identities of the individuals involved in the incidents. The names, therefore, are considered personal information, the processing of which must be in accordance with the DPA.

B. The processing of personal information is lawful.

Apart from the claim that FRL violated Sections 32 and 36 of the DPA,³⁵ JCB's Complaint-Affidavit did not contain a specific allegation on the unlawful processing of his personal information. Despite this, the Commission takes into consideration his narration of facts and proceeds to discuss the lawfulness of the processing of personal information.

³³ Complaint Affidavit, 26 January 2021, Annex C, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

³⁴ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (g) (2012).

³⁵ Complaint Affidavit, 26 January 2021, ¶ 43, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

FRL's processing of personal information is based on a lawful criteria under Section 12 (f) of the DPA. Section 12 (f) of the DPA provides:

Section 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

...

- (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.³⁶

The Commission previously ruled that the protection of lawful rights and interests under Section 13 (f) of the DPA is considered as legitimate interest pursuant to Section 12 (f) of the DPA, thus: ³⁷

Although Section 13 (f) applies to sensitive personal information while the information involved in this case is just personal information, the protection of lawful rights and interests under Section 13 (f) by the Respondent is considered as legitimate interest pursuant to Section 12 (f) of the DPA. This section provides that it is lawful to process personal information if it is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.³⁸

Section 13 (f) of the DPA provides:

Section 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information

³⁶ Data Privacy Act of 2012, § 12 (f).

³⁷ CID Case No. 17-K003, 19 November 2019, (NPC 2019) (unreported).

³⁸BGM v. IPP, NPC 19-653, 17 December 2020, available at <https://www.privacy.gov.ph/wp-content/uploads/2021/02/NPC-19-653-BGM-vs-IPP-Decision-FINAL-Pseudonymized-21Dec2020.pdf> (last accessed 17 March 2022).

and privileged information shall be prohibited, except in the following cases:

...

- (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.³⁹

The phrase “for the protection of lawful rights and interests of **natural or legal persons** in court proceedings” cannot be interpreted to relate only to the person asserting the lawful basis of the processing of personal information. It also contemplates situations where those persons whose lawful rights and interests are protected in court proceedings may not be the same individuals who processed the personal information, such as in the case of witnesses. Similarly, the next clause “establishment, exercise or defense of legal claims” may be interpreted to refer to the legal claims of persons other than those who processed the personal information.

In this case, FRL asserted in her Comment that the purpose of the affidavit was to support the administrative complaint filed by MSG against JCB.⁴⁰ She argued that the narration of the incidents in the affidavit would help “in establishing the facts surrounding the undesirability of JCB to teach in DepEd.”⁴¹ Given that Section 13 (f) may refer to the legal claims of persons other than those who processed the personal information, the act of FRL in issuing the affidavit to support MSG’s legal claim filed before the DepEd can, therefore, be considered as lawful processing.

III. FRL did not violate Section 31 of the DPA (Malicious Disclosure).

Section 31 of the DPA provides that a PIC or a PIP may be held liable for Malicious Disclosure if he discloses unwarranted or false personal

³⁹ Data Privacy Act of 2012, § 13 (f).

⁴⁰ Comment, 03 November 2021, at 7, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

⁴¹ *Id.* at 6.

information or sensitive personal information with malice or in bad faith.⁴²

The requisites of Malicious Disclosure are:

1. The perpetrator is a personal information controller or personal information processor or any of its officials, employees, or agents;
2. The perpetrator disclosed personal or sensitive personal information;
3. The disclosure was with malice or in bad faith; and
4. The disclosed information relates to unwarranted or false information.⁴³

In this case, FRL disclosed personal information, particularly the names of JCB and his co-teachers, when she narrated the incidents involving him in her affidavit.

The disclosure, however, was done without malice or bad faith. The existence of malice or bad faith cannot be presumed.⁴⁴ In this case, JCB alleged that FRL acted with malice or in bad faith in disclosing the incidents that were already amicably settled.⁴⁵ Further, he attempted to demonstrate the existence of malice or bad faith by claiming that the information disclosed were confidential and were obtained by FRL in her official position.⁴⁶ He, however, failed to substantially provide evidence to support this claim. It is fundamental that he who alleges has the burden to prove his allegation with the quantum of evidence prescribed by law.⁴⁷

Section 6, Rule 133 of the Rules of Court provides for the quantum of evidence required in administrative proceedings, thus:

Section 6. *Substantial evidence.* – In cases filed before administrative or quasi-judicial bodies, a fact may be deemed established if it is supported by substantial evidence, or that

⁴² Data Privacy Act of 2012, § 31.

⁴³ NPC 21-015, 03 February 2022, (NPC 2022) (unreported).

⁴⁴ Cruz v. Intermediate Appellate Court, G.R. No. 66327 (1984).

⁴⁵ Complainant's Memorandum, 12 November 2021, at 15, *in* JCB v. FRL, NPC 21-031 (NPC 2021).

⁴⁶ *Id.* at 16.

⁴⁷ Tacis v. Shields Security Services, Inc., G.R. No. 234575 (2021).

amount of relevant evidence which a reasonable mind might accept as adequate to justify a conclusion.⁴⁸

Mere allegations that the information were confidential and were obtained by FRL in her official capacity are not sufficient to substantiate that there was indeed malice or bad faith. JCB, who made the allegations, has the burden to provide substantial evidence to establish his claim. He, however, was unable to discharge this burden as his allegations failed to show that there was a violation of the DPA.

JCB also argued that the information disclosed were privileged communication under Section 24 (e), Rule 130 of the Rules of Court,⁴⁹ which provides:

Section 24. *Disqualification by reason of privileged communication.* – The following persons cannot testify as to matters learned in confidence in the following cases:

...

(e) A public officer cannot be examined during or after his or her tenure as to communications made to him or her in official confidence, when the court finds that the public interest would suffer by the disclosure.⁵⁰

He alleged that FRL acquired these information in her role as a guidance counselor, thus making it privileged information.⁵¹ These claims, however, remained to be unfounded since JCB failed to provide any proof to substantiate his claim. Aside from this, in detailing how FRL acquired the information, his own narration of events belies his claim that FRL received the information in her capacity as a guidance counselor.

Considering the foregoing, the information relating to the incidents were, therefore, not privileged communication.

⁴⁸ 2019 AMENDMENTS TO THE 1989 REVISED RULES ON EVIDENCE, rule 133, § 6.

⁴⁹ Complainant's Memorandum, 12 November 2021, at 16, in JCB v. FRL, NPC 21-031 (NPC 2021).

⁵⁰ AMENDMENTS TO THE 1989 REVISED RULES ON EVIDENCE, rule 130, § 24 (e).

⁵¹ Complainant's Memorandum, 12 November 2021, at 16, in JCB v. FRL, NPC 21-031 (NPC 2021).

The last element of Malicious Disclosure is also lacking in this case since the disclosure does not relate to unwarranted nor false information. Here, the personal information disclosed were the names of JCB and his co-teachers. The inclusion of the names are justified to identify the individuals involved in the incidents and to help establish the legal claim against JCB. Lastly, the truthfulness of the names were not refuted by JCB and were bolstered by the affidavits of the other persons involved.

Absent the third and fourth requisite, FRL cannot be deemed to have violated Section 31 of the DPA on Malicious Disclosure.

IV. FRL did not violate Section 32 of the DPA (Unauthorized Disclosure).

With respect to Unauthorized Disclosure, Section 32 of the DPA provides:

Section. 32. *Unauthorized Disclosure.* – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one

(1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).⁵²

A strict and literal reading of Section 32 of the DPA shows that a PIC or PIP is liable if it discloses to a third party personal information without the consent of the data subject.⁵³ This interpretation, however, will result in absurdity as a PIC or a PIP will be held liable for Unauthorized Disclosure if the disclosure is without the consent of the data subject even if the disclosure is justified under Section 12 or Section 13 of the DPA. Following the rules of statutory construction:

Where a literal meaning would lead to absurdity, contradiction, or injustice, or otherwise defeat the clear purpose of the

⁵² Data Privacy Act of 2012, § 32.

⁵³ *Id.*

lawmakers, the spirit and reason of the statute may be examined to determine the true intention of the provision.⁵⁴

Thus, the provision should be further examined and be read together with other provisions of the DPA:

A law must not be read in truncated parts; its provisions must be read in relation to the whole law. It is the cardinal rule in statutory construction that a statute's clauses and phrases must not be taken as detached and isolated expressions, but the whole and every part thereof must be considered in fixing the meaning of any of its parts in order to produce a harmonious whole. Every part of the statute must be interpreted with reference to the context, *i.e.*, that every part of the statute must be considered together with other parts of the statute and kept subservient to the general intent of the whole enactment.⁵⁵

Thus, Section 32 of the DPA should be read and interpreted as follows: Unauthorized Disclosure is committed when the perpetrator processes personal information without any of the lawful basis for processing under Sections 12 and 13.⁵⁶ This reading is more in line with the principle that “when two or more interpretations are possible, that interpretation which is favorable or beneficial to the accused must be adopted.”⁵⁷ This interpretation benefits the accused since it narrows the extent to which the disclosure of personal information may be considered as Unauthorized Disclosure.⁵⁸

To determine whether there is Unauthorized Disclosure, the following requisites must concur:

1. The perpetrator is a personal information controller or personal information processor;
2. The perpetrator disclosed information;
3. The information relates to personal or sensitive personal information;
4. The perpetrator disclosed the personal or sensitive personal information to a third party;

⁵⁴ Metropolitan Bank and Trust Co. v. Liberty Corrugated Boxes Manufacturing Corp., G.R. No.184317 (2017).

⁵⁵ Fort Bonifacio Development Corp. v. Commissioner of Internal Revenue, G.R. Nos. 158885 & 170680 (Resolution) (2009).

⁵⁶ See NPC 18-010, 17 December 2020 (NPC 2020) (unreported); NPC 19-134, 10 December 2021 (NPC 2021) (unreported);

NPC 21-010, 03 February 2022 (NPC 2022) (unreported).

⁵⁷ People v. Liban, G.R. Nos. 136247 & 138330 (2000).

⁵⁸ NPC 19-134, 10 December 2021 (NPC 2021) (unreported).

5. The disclosure was without any of the lawful basis for processing, consent or otherwise, under Sections 12 and 13 of the DPA; and
6. The disclosure is neither malicious nor done in bad faith and the information disclosed is not unwarranted or false information.⁵⁹

In this case, FRL disclosed personal information to third parties when she narrated the incidents involving JCB in her affidavit. As previously discussed, the disclosure does not relate to unwarranted or false information. Further, the disclosure was based on a lawful criteria under Section 12 (f) in relation to Section 13 (f) of the DPA. FRL's processing of personal information is a legitimate interest to establish the legal claims against JCB. Considering that the requisites are lacking, FRL cannot, therefore, be held liable under Section 32 of the DPA on Unauthorized Disclosure.

WHEREFORE, premises considered, the Commission resolves that the case filed by JCB against FRL is hereby **DISMISSED**.

SO ORDERED.

City of Pasay,
Philippines. 03 March
2022.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

JOHN HENRY D. NAGA
Privacy Commissioner

⁵⁹ NPC 21-010, 03 February 2022 (NPC 2022) (unreported).

Copy furnished:

JCB
Complainant

FRL
Respondent

IAL
Counsel of Respondent

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

JDB,

Complainant,

-versus-

JME,

Respondent.

X-----X

NPC 21-032

For: Violation of
the Data Privacy
Act of 2012

DECISION

AGUIRRE, D.P.C.;

Before this Commission is a complaint filed by JDB against JME for an alleged violation of the Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

JDB and JME are public school teachers at Don Andres Soriano National High School.¹ In JDB's complaint, he alleged that he had a confrontation with JME on 24 June 2019 when the latter tried to occupy his working area.² According to JDB, the incident was thereafter settled through the help of the school principal and some members of the school's Grievance Committee.³

JDB alleged that despite the parties' agreement to not file formal charges, JME filed a report about the incident before the Barangay Public Safety Office on 25 June 2019.⁴ He further alleged that JME also narrated about the incident in an Incident Report dated 24 June 2019 and an Affidavit dated 24 August 2020, which were attached to an administrative complaint filed by MDG against JDB before the

¹ Complaint-Affidavit, 26 January 2021, ¶¶ 1-2, *in* JDB v. JME, NPC 21-032 (NPC 2021).

² Complaints-Assisted Form, 02 February 2021, *in* JDB v. JME, NPC 21-032 (NPC 2021).

³ *Id.*

⁴ *Id.*

Department of Education (DepEd).⁵ JDB argued that JME's disclosure of the incident constituted malicious disclosure of confidential information.⁶

On 27 August 2021, the Commission issued an Order requiring JME to file a verified comment within fifteen (15) calendar days from receipt of the Order.⁷ The Order also provided the schedule for the preliminary conference.⁸

During the Preliminary Conference on 30 September 2021, only JDB was present; thus, it was reset to 28 October 2021.⁹

JME once again failed to appear in the Preliminary Conference dated 28 October 2021.¹⁰ He, however, sent an e-mail requesting for its resetting since he only received the link to the meeting conference a minute before the schedule and he was not admitted to the meeting.¹¹ In a Resolution dated 02 November 2021, the Commission granted JME request and required the parties to appear for the Preliminary Conference on 01 December 2021.¹²

On 08 November 2021, JME filed a Comment.¹³ He denied JDB's allegation that the Affidavit dated 24 August 2020 was malicious.¹⁴ He argued that the Affidavit was executed under oath and was based on his personal knowledge.¹⁵

JME also denied JDB's allegation that he committed a data privacy breach when he disclosed the incident between them.¹⁶ He argued that following JDB's reasoning would result in an "absurd situation wherein witnesses will be afraid to testify even when it is in defense of the rights of other people – in fear and under threat that the witness will be sued for [a] data privacy breach, which is not the essence of [the DPA]."¹⁷ Further, he argued that if there was indeed

⁵ Complaint-Affidavit, 26 January 2021, ¶¶ 3-4, *in* JDB v. JME, NPC 21-032 (NPC 2021).

⁶ *Id.* ¶ 13.

⁷ Order, 27 August 2021, at 1, *in* JDB v. JME, NPC 21-032 (NPC 2021).

⁸ *Id.*

⁹ Order, 30 September 2021, *in* JDB v. JME, NPC 21-032 (NPC 2021).

¹⁰ Order, 28 October 2021, *in* JDB v. JME, NPC 21-032 (NPC 2021).

¹¹ Respondent's Email, 28 October 2021, *in* JDB v. JME, NPC 21-032 (NPC 2021).

¹² Resolution, 02 November 2021, *in* JDB v. JME, NPC 21-032 (NPC 2021).

¹³ Comment, 08 November 2021, at 3, *in* JDB v. JME, NPC 21-032 (NPC 2021).

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.* at 5.

¹⁷ *Id.* Emphasis omitted.

sensitive personal information that was processed, the processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings in accordance with Section 13 (f) of the DPA.¹⁸

As affirmative defenses, JME argued that JDB’s complaint should be dismissed on the following grounds:

- (1) the complaint failed to state a cause of action;¹⁹
- (2) the complaint is “frivolous, vexatious, and made in bad faith”;²⁰
- (3) the complaint lacks verification and certification against forum shopping;²¹
- (4) JDB failed to exhaust administrative remedies;²² and
- (5) the act of executing an affidavit does not constitute a violation of the DPA.²³

During the Preliminary Conference on 01 December 2021, JDB requested a period of forty-five (45) calendar days to file his memorandum, to which JME did not object.²⁴ Both parties were thus ordered to submit their respective memoranda within forty-five (45) calendar days from receipt of the Order.²⁵

On 06 January 2022, JDB submitted his Memorandum.²⁶ He alleged that JME should have respected his right to privacy and his rights as a data subject in accordance with the DPA.²⁷

On 12 January 2022, JME submitted his Memorandum, which contained similar arguments that he had raised in his Comment.²⁸

Issue

I. Whether the case should be dismissed on procedural grounds.

¹⁸ *Id.* at 7.

¹⁹ *Id.*

²⁰ Comment, 08 November 2021, at 11-12, *in* JDB v. JME, NPC 21-032 (NPC 2021).

²¹ *Id.* at 7-9.

²² *Id.* at 9-10.

²³ *Id.* at 10-11.

²⁴ Order, 01 December 2021, *in* JDB v. JME, NPC 21-032 (NPC 2021).

²⁵ *Id.*

²⁶ Complainant’s Memorandum, 06 January 2022, *in* JDB v. JME, NPC 21-032 (NPC 2022).

²⁷ *Id.* at 11.

²⁸ Respondent’s Memorandum, 12 January 2022, *in* JDB v. JME, NPC 21-032 (NPC 2022).

- II. Whether JME had lawful basis in processing JDB's personal information.
- III. Whether JME is liable under Section 31 (Malicious Disclosure) of the DPA.
- IV. Whether JME is liable under Section 32 (Unauthorized Disclosure) of the DPA.

Discussion

I. The case should be dismissed outright on procedural grounds.

JME argued that the case should be dismissed because JDB failed to exhaust administrative remedies as required under Section 2, Rule II of NPC Circular No. 2021-01 (2021 NPC Rules of Procedure).²⁹

He also argued that JDB did not observe Section 3, Rule II of the 2021 NPC Rules of Procedure because the complaint was not verified and did not contain a certification against forum shopping.³⁰ He argued that “a pleading that lacks proper verification is treated as unsigned pleading, which produces no legal effect” and that the complaint is “clearly defective on its face and thus, should be dismissed.”³¹

Section 2, Rule II of the 2021 NPC Rules of Procedure provides:

Section 2. *Exhaustion of remedies.* – No complaint shall be given due course unless it has been sufficiently established and proven that:

1. the complainant has informed, in writing, the personal information controller (PIC), personal information processor (PIP), or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same; and
2. the PIC, PIP, or concerned entity did not take timely or appropriate action on the claimed privacy violation or

²⁹ Comment, 08 November 2021, at 9-10, *in* JDB v. JME, NPC 21-032 (NPC 2021).

³⁰ *Id.* at 8.

³¹ *Id.* at 9.

personal data breach, or there is no response from the PIC, PIP, or concerned entity within fifteen (15) calendar days from receipt of written information from the complainant.

The NPC may waive any or all of the requirements of this Section at its discretion upon (a) good cause shown, properly alleged and proved by the complainant; or (b) if the allegations in the complaint involve a serious violation or breach of the Data Privacy Act of 2012, taking into account the risk of harm to the affected data subject, including but not limited to:

- i. when there is grave and irreparable damage which can only be prevented or mitigated by action of the NPC;
- ii. when the respondent cannot provide any plain, speedy or adequate remedy to the alleged violation; or
- iii. the action of the respondent is patently illegal.³²

In this case, there is no evidence on record that JDB informed JME of the alleged privacy violation or personal data breach. He even admitted in his Complaints-Assisted Form that he did not contact JME and reasoned out that “[t]he Respondent is hostile.”³³ Such reasoning, however, is not a valid excuse to disregard the requirement provided in the 2021 NPC Rules of Procedure.

Further, there is nothing to warrant the exercise of the Commission of its discretion to waive the requirement of exhaustion of administrative remedies. JDB failed to properly allege and prove a good cause in his complaint to justify the waiver of the requirement. A review of his complaint did not also show a potential serious violation or breach of the DPA. In fact, and as will be discussed subsequently, the Commission finds that the allegations of JDB do not constitute a privacy violation.

Given the foregoing, the Commission finds no reason to waive the procedural requirement of exhaustion of administrative remedies.

Hence, the complaint should not be given due course for JDB’s failure to sufficiently establish and prove that he has exhausted the remedies under Section 2, Rule II of the 2021 NPC Rules of Procedure.

³² National Privacy Commission, 2021 Rules on Procedure of the National Privacy Commission [NPC 2021 Rules of Procedure], rule II, § 2 (28 January 2021).

³³ Complaints-Assisted Form, 02 February 2021, *in* JDB v. JME, NPC 21-032 (NPC 2021).

With regard to the requirement of verification and certification against forum shopping, Section 3, Rule II of the 2021 NPC Rules of Procedure provides:

Section 3. *Form and contents of the complaint.* – The complaint should be in the proper form, as follows:

1. The complaint must be in writing, signed by the party or his or her counsel, and verified in the format prescribed under the Rules of Court.

...

10. A certification against forum shopping must accompany the complaint. The complainant shall certify under oath in the complaint, or in a sworn certification annexed and simultaneously filed with the pleading: (a) that he or she has not commenced any action or filed any claim involving the same issues in any court, tribunal or quasi-judicial agency and, to the best of his or her knowledge, no such other action or claim is pending with such court, tribunal or quasi-judicial agency; (b) if there is such other pending action or claim, a complete statement of its present status; and (c) if he or she should thereafter learn that the same or similar action or claim has been filed or is pending, he or she shall report that fact within five (5) calendar days therefrom to the NPC.

Failure to comply with the proper form and contents of the complaint may cause for outright dismissal under Section 1(1), Rule IV: *Provided*, an application that does not comply with the foregoing requirements may be acted upon if it merits appropriate consideration on its face, or is of such notoriety that it necessarily contains sufficient leads or particulars to enable the taking of further action.³⁴

The abovementioned provision requires that the complaints filed before the Commission should be “verified in the format prescribed under the Rules of Court.”³⁵

Section 4, Rule 7 of the Rules of Court provides:

Section 4. *Verification.* –

³⁴ NPC 2021 Rules of Procedure, rule II, § 3.

³⁵ *Id.* rule II, § 3 (1).

...

A pleading is verified by an affidavit of an affiant duly authorized to sign said verification. The authorization of the affiant to act on behalf of a party, whether in the form of a secretary's certificate or a special power of attorney, should be attached to the pleading, and shall allege the following attestations:

- (a) The allegations in the pleading are true and correct based on his personal knowledge, or based on authentic documents;
- (b) The pleading is not filed to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and
- (c) The factual allegations therein have evidentiary support or, if specifically so identified, will likewise have evidentiary support after a reasonable opportunity for discovery.

The signature of the affiant shall further serve as a certification of the truthfulness of the allegations in the pleading.³⁶

In the case at bar, the Complaint-Affidavit filed by JDB was not verified nor did it specifically state the attestations provided under the Rules of Court. While the Supreme Court has previously ruled that technical rules of procedure do not strictly apply to administrative bodies,³⁷ JDB's complaint still failed to effectively provide the attestations required because it only certified that the complaint was true and based on JDB's personal knowledge.³⁸ Since the complaint was not verified in the format required under the Rules of Court, it could not be considered to have complied with the form prescribed under the 2021 NPC Rules of Procedure.

Additionally, Section 3, Rule II of the 2021 NPC Rules of Procedure provides that the complaint should be accompanied by a certification against forum shopping.³⁹ JDB failed to observe this procedural requirement when he neither attached the required certification with

³⁶ 2019 AMENDMENTS TO THE 1997 RULES OF CIVIL PROCEDURE, rule 7, § 4.

³⁷ DP v. Florentino International, Inc., G.R. No. 186967 (2017).

³⁸ See Complaints-Assisted Form, 02 February 2021, *in* JDB v. JME, NPC 21-032 (NPC 2021); Complaint-Affidavit, 26 January 2021, *in* JDB v. JME, NPC 21-032 (NPC 2021).

³⁹ NPC 2021 Rules of Procedure, rule II, § 3 (10).

his Complaint-Affidavit, nor attested to the facts enumerated in Section 3 (10), Rule II of the 2021 NPC Rules of Procedure.

According to the Supreme Court, a certification against forum shopping is mandatory:

[T]he rules on forum shopping, which were designed to promote and facilitate the orderly administration of justice, should not be interpreted with such absolute literalness as to subvert its own ultimate and legitimate objective. Strict compliance with the provision regarding the certificate of non- forum shopping underscores its mandatory nature in that the certification cannot be altogether dispensed with or its requirements completely disregarded.⁴⁰

The Court also explained that there must be a distinction between non-compliance and substantial compliance with the procedural requirements:

A distinction must be made between non-compliance with the requirement on or submission of defective verification, and non-compliance with the requirement on or submission of defective certification against forum shopping.

...

As to certification against forum shopping, non-compliance therewith or a defect therein, unlike in verification, is generally not curable by its subsequent submission or correction thereof, unless there is a need to relax the Rule on the ground of 'substantial compliance' or presence of 'special circumstances or compelling reasons'.⁴¹

Here, JDB's complaint did not contain a certification against forum shopping. He cannot be considered to have substantially complied with the procedural requirement since he did not submit any attestation that could effectively be considered similar to a certification against forum shopping.

While the 2021 NPC Rules of Procedure provides that the procedural requirements on form may be waived, a review of JDB's complaint

⁴⁰ *Pacquing v. Coca-Cola Philippines, Inc.*, G.R. No. 157966 (2008).

⁴¹ *Altres v. Empleo*, G.R. No. 180986 (2008).

demonstrates that it does not “[merit] appropriate consideration on its face, or is of such notoriety that it necessarily contains sufficient leads or particulars to enable the taking of further action.”⁴² The allegations of JDB, even assuming they were all true, do not substantially prove his claim that JME violated the DPA nor directly contravene specific portions of the DPA and its related issuances. These allegations on its face, do not serve as sufficient basis nor warrant the exercise of the waiver of the procedural requirements.

Section 1 (1), Rule IV of the 2021 Rules of Procedure also provides that a complaint may be dismissed outright when it is insufficient in form or it did not comply with Section 3, Rule II of the 2021 NPC Rules of Procedure:

Section 1. *Outright dismissal, when allowed.* – Within thirty (30) calendar days from receipt of the complaint, the investigating officer may give the complaint due course or dismiss the complaint without prejudice, on any the following grounds:

1. The complaint is insufficient in form or did not comply with Section 3, Rule II of these Rules, unless failure to do so is justified or excused with good cause[.]⁴³

Considering that JDB failed to observe the formal requirements, the complaint should have been dismissed outright pursuant to Section 1 (1) Rule IV of the 2021 NPC Rules of Procedure.

The Commission, however, shall discuss the substantial aspect of the case for the education and guidance of the public.

II. JME had lawful basis in processing JDB’s personal information.

A. The information included in the Affidavit and in the Incident Report are personal information.

The Affidavit and the Incident Report executed by JME contained personal information, specifically the names of JDB and JME.⁴⁴

⁴² NPC 2021 Rules of Procedure, rule III, § 3.

⁴³ *Id.* rule IV, § 1 (1).

Section 3 (g) of the DPA defines personal information:

Section 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

...

(g) *Personal information* refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.⁴⁵

Given that the names stated in the Affidavit and in the Incident Report can reasonably and directly ascertain the identities of the individuals involved in the incident, they are considered personal information. The processing of these personal information must, therefore, be in accordance with the DPA.

B. The processing of personal information is lawful.

JDB's complaint failed to provide specific allegations of unlawful processing of his personal information committed by JME. It merely contained a general allegation that JME act of disclosing the issue between them in his Affidavit and Incident Report amounted to unlawful processing of his personal information.⁴⁶

Nevertheless, the Commission proceeds to discuss the lawfulness of the processing of personal information.

JME processing of personal information is based on a lawful criteria under Section 12 (f) of the DPA. Section 12 (f) of the DPA provides:

⁴⁴ Complaint-Affidavit, 26 January 2021, Annexes A & B, *in* JDB v. JME, NPC 21-032 (NPC 2021).

⁴⁵ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (g) (2012).

⁴⁶ See Complaint-Affidavit, 26 January 2021, ¶ 13, *in* JDB v. JME, NPC 21-032 (NPC 2021); Complainant's Memorandum, 06 January 2022, at 2-3, 10-12, *in* JDB v. JME, NPC 21-032 (NPC 2022).

Section 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

...

- (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.⁴⁷

The protection of lawful rights and interests under Section 13 (f) is considered as legitimate interest pursuant to Section 12 (f) of the DPA:⁴⁸

Although Section 13 (f) applies to sensitive personal information while the information involved in this case is just personal information, the protection of lawful rights and interests under Section 13 (f) by the Respondent is considered as legitimate interest pursuant to Section 12 (f) of the DPA. This section provides that it is lawful to process personal information if it is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.⁴⁹

Section 13 (f) of the DPA provides:

Section 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

...

⁴⁷ Data Privacy Act of 2012, § 12 (f).

⁴⁸ CID Case No. 17-K003, 19 November 2019, (NPC 2019) (unreported).

⁴⁹ BGM v. IPP, NPC 19-653, 17 December 2020, available at <https://www.privacy.gov.ph/wp-content/uploads/2021/02/NPC-19-653-BGM-vs-IPP-Decision-FINAL-Pseudonymized-21Dec2020.pdf> (last accessed 06 June 2022).

- (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.⁵⁰

The Commission has previously interpreted the phrase "for the protection of lawful rights and interests of **natural or legal persons** in court proceedings" in Section 13 (f) of the DPA:

The phrase 'for the protection of lawful rights and interests of **natural or legal persons** in court proceedings' cannot be interpreted to relate only to the person asserting the lawful basis of the processing of personal information. It also contemplates situations where those persons whose lawful rights and interests are protected in court proceedings may not be the same individuals who processed the personal information, such as in the case of witnesses. Similarly, the next clause 'establishment, exercise or defense of legal claims' may be interpreted to refer to the legal claims of persons other than those who processed the personal information.⁵¹

In this case, JME asserted that the purpose of the Affidavit was to support the administrative complaint filed by MDG against JDB.⁵² Given that Section 13 (f) of the DPA may refer to the legal claims of persons other than those who processed the personal information, the act of JME in issuing the Affidavit to support MDG legal claim can, therefore, be considered as lawful processing.

III. JME did not violate Section 31 of the DPA (Malicious Disclosure).

Under Section 31 of the DPA, a PIC or a PIP may be held liable for Malicious Disclosure if he or she discloses unwarranted or false personal information or personal sensitive personal information with malice or in bad faith.⁵³

The requisites of Malicious Disclosure are:

⁵⁰ Data Privacy Act of 2012, § 13 (f).

⁵¹ NPC 21-031, 03 March 2022, at 11, (NPC 2022) (unreported).

⁵² Comment, 08 November 2021, at 10, *in* JDB v. JME, NPC 21-032 (NPC 2021).

⁵³ Data Privacy Act of 2012, § 31.

1. The perpetrator is a personal information controller or personal information processor or any of its officials, employees, or agents;
2. The perpetrator disclosed personal or sensitive personal information;
3. The disclosure was with malice or in bad faith; and
4. The disclosed information relates to unwarranted or false information.⁵⁴

JME disclosed personal information, particularly the name of JDB, when he narrated the incident between them in his Affidavit and his Incident Report.

The disclosure, however, was done without malice or bad faith. JDB alleged that JME acted with malice or in bad faith in disclosing “an old and settled issue” between them.⁵⁵ To support his claim, JDB argued that JME acted in bad faith in disclosing the incident after they have both agreed that “the matter was no longer an issue to be raised again” to support the “malicious administrative complaint” of MDG.⁵⁶ The Commission, however, finds no malice or bad faith on the part of JME in disclosing the incident in the Affidavit and the Incident Report. The act of disclosing a settled issue in an affidavit or a report does not automatically amount to malice or bad faith. Further, JME had a lawful purpose in disclosing the incident in the Affidavit, that is, to support the administrative complaint of Gepitulan against JDB.

As to the last element of Malicious Disclosure, the disclosure in this case neither relates to unwarranted nor false information. Here, the personal information disclosed were the names of JDB and JME. The inclusion of the names is necessary to identify the individuals involved in the incident and to support the establishment of the legal claim against JDB.

Considering that the third and fourth requisites are not present, JME cannot be held to have committed Malicious Disclosure under Section 31 of the DPA.

⁵⁴ NPC 21-015, 03 February 2022, (NPC 2022) (unreported).

⁵⁵ Complainant’s Memorandum, 06 January 2022, at 3, *in* JDB v. JME, NPC 21-032 (NPC 2022).

⁵⁶ *Id.* at 3-5.

IV. JME did not violate Section 32 of the DPA (Unauthorized Disclosure).

Unauthorized Disclosure is defined and penalized under Section 32 of the DPA:

Section. 32. *Unauthorized Disclosure.* – (a) Any personal information controller or personal information processor

or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one

(1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).⁵⁷

The Commission has previously explained the interpretation of Section 32 of the DPA as follows:

A strict and literal reading of Section 32 of the DPA on Unauthorized Disclosure shows that a personal information controller (PIC) or personal information processor (PIP) is liable if it discloses to a third-party personal information without the consent of the data subject. Such reading, however, will result in absurdity since it penalizes a PIC or a PIP if the disclosure is without the consent of the data subject even if such disclosure is justified under some other criteria for lawful processing in Sections 12 and 13 of the DPA.⁵⁸

In the same case, the Commission cited the following rule in statutory construction:

Where a literal meaning would lead to absurdity, contradiction, or injustice, or otherwise defeat the clear purpose of the lawmakers, the spirit and reason of the statute may be examined to determine the true intention of the provision.⁵⁹

In line with this, Section 32 of the DPA should be further examined and be read together with other provisions of the DPA:

⁵⁷ Data Privacy Act of 2012, § 32.

⁵⁸ NPC 19-134, 10 December 2021 (NPC 2021) (unreported).

⁵⁹ *Metropolitan Bank and Trust Co. v. Liberty Corrugated Boxes Manufacturing Corp.*, G.R. No.184317 (2017).

A law must not be read in truncated parts; its provisions must be read in relation to the whole law. It is the cardinal rule in statutory construction that a statute's clauses and phrases must not be taken as detached and isolated expressions, but the whole and every part thereof must be considered in fixing the meaning of any of its parts in order to produce a harmonious whole. Every part of the statute must be interpreted with reference to the context, *i.e.*, that every part of the statute must be considered together with other parts of the statute and kept subservient to the general intent of the whole enactment.⁶⁰

Therefore, Unauthorized Disclosure is committed when the perpetrator processes personal information without any of the lawful basis for processing under Sections 12 and 13 of the DPA.⁶¹ The interpretation is in line with the principle that “when two or more interpretations are possible, that interpretation which is favorable or beneficial to the accused must be adopted.”⁶² It benefits the accused since it narrows the extent to which the disclosure of personal information may be considered as Unauthorized Disclosure.⁶³

To determine whether there is Unauthorized Disclosure, the following requisites must concur:

1. The perpetrator is a personal information controller or personal information processor;
2. The perpetrator disclosed information;
3. The information relates to personal or sensitive personal information;
4. The perpetrator disclosed the personal or sensitive personal information to a third party;
5. The disclosure was without any of the lawful basis for processing, consent or otherwise, under Sections 12 and 13 of the DPA; and
6. The disclosure is neither malicious nor done in bad faith and the information disclosed is not unwarranted or false information.⁶⁴

⁶⁰ Fort Bonifacio Development Corp. v. Commissioner of Internal Revenue, G.R. Nos. 158885 & 170680 (Resolution) (2009).

⁶¹ See e.g., NPC 18-010, 17 December 2020 (NPC 2020) (unreported); NPC 19-134, 10 December 2021 (NPC 2021) (unreported); NPC 21-010, 03 February 2022 (NPC 2022) (unreported).

⁶² People v. Liban, G.R. Nos. 136247 & 138330 (2000).

⁶³ NPC 19-134, 10 December 2021 (NPC 2021) (unreported).

⁶⁴ NPC 21-010, 03 February 2022 (NPC 2022) (unreported).

JME disclosed personal information when JDB's name was included in his Affidavit and his Incident Report. The personal information was disclosed to third parties since the Affidavit and the Incident Report were submitted together with the administrative complaint filed by MDG before the DepEd.

As previously discussed, however, the disclosure does not relate to unwarranted or false information. Further, the disclosure was based on a lawful criteria under Section 12 (f) in relation to Section 13 (f) of the DPA. Thus, the processing of personal information is a legitimate interest to establish the legal claim against JDB.

Considering that the requisites are lacking, JME cannot be held liable under Section 32 of the DPA on Unauthorized Disclosure.

WHEREFORE, premises considered, the Commission resolves that the case filed by JDB against JME is hereby **DISMISSED**.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases before any other forum or tribunal, if any.

SO ORDERED.

City of Pasay, Philippines.
16 May 2022.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

JOHN HENRY D. NAGA
Privacy Commissioner

DUG CHRISTOPHER B. MAH
Deputy Privacy Commissioner

Copy furnished:

JDB
Complainant

JME
Respondent

JRB
Counsel for Respondent

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

GSS

Complainant,

NPC 21-064

-versus-

For: Violation of
the Data Privacy
Act of 2012

GLOBAL DOMINION FINANCING INC.,

Respondent.

X-----X

DECISION

AGUIRRE, D.P.C.;

Before this Commission is a complaint filed by GSS against Global Dominion Financing Inc. (GDFI) for an alleged violation of Section 25 (Unauthorized Processing) and Section 28 (Processing for Unauthorized Purposes) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

On 22 March 2021, GSS. filed a complaint with the National Privacy Commission (NPC) against Global Dominion Financing Inc. (GDFI).¹

GSS alleged that on 02 March 2021, he applied for a car loan with GDFI.² In GSS's complaint, he stated that he followed up on his application with GDFI and received a reply via email on 04 March 2021,³ which stated "Good morning po. [P]inapaunlock ko lang po yung name sa affiliate namin. [P]ossible po common name. [R]equested na po ito. Thank you[.]"⁴

¹ Complaints Assisted Form, 22 March 2021, at 3, *in* GSS. v. Global Dominion Financing Inc., NPC 21-064 (NPC 2021).

² *Id.*

³ *Id.*

⁴ Complainant's Memorandum, Exhibit A, 22 October 2021, *in* GSS v. Global Dominion Financing Inc., NPC 21-064 (NPC 2021).

On 05 March 2021, GSS again asked GDFI for an update on the status of his loan but there was no response from GDFI.⁵ He claimed that he “felt something suspicious about why [his] namesake from [GDFI’s] affiliate is not yet cleared.”⁶

On 11 March 2021, GSS cancelled his car loan application and requested an explanation regarding the unlocking of his account with GDFI’s affiliate.⁷ He claimed that he had no personal knowledge of applying for other loan products from them or any of their affiliates.⁸ He further averred that “[he] fears that someone might have used the personal data [he] had with GDFI without [his] knowledge whatsoever.”⁹

GSS alleged that GDFI violated Section 25 (Unauthorized Processing) and Section 28 (Processing for Unauthorized Purposes) of the DPA.¹⁰ GSS also prayed for damages and a fine to be issued against GDFI.¹¹

On 23 June 2021, the Commission, through its Complaints and Investigation Division (CID), issued an Order directing GDFI to file its comment within fifteen (15) calendar days from receipt of the Order.¹²

On 12 July 2021, GDFI filed its Verified Comment.¹³ GDFI averred that it did not violate any provision of the DPA.¹⁴ GDFI claimed that it informs its clients of its Privacy Notice and secures the consent of its clients through the Privacy Notice and Consent Form which states:

The privacy and security of your personal data (“Personal Information”) which we collect from you is important to us. It is equally important that you understand how we handle this data.

In conducting our business, we must collect “Personal Information” from you. It will be strictly used to administer your account and to provide the products and services you have requested from us and to further meet your needs and the standard procedures of our business.

⁵ Complaints Assisted Form, 22 March 2021, at 3, *in* GSS v. Global Dominion Financing Inc., NPC 21-064 (NPC 2021).

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ *Id.* at 4.

¹⁰ *Id.* at 3.

¹¹ Complaints Assisted Form, 22 March 2021, at 5, *in* GSS v. Global Dominion Financing Inc., NPC 21-064 (NPC 2021).

¹² Order to Comment, 23 June 2021, *in* GSS v. Global Dominion Financing Inc., NPC 21-064 (NPC 2021).

¹³ Respondent’s Verified Comment, 15 July 2021, *in* GSS v. Global Dominion Financing Inc., NPC 21-064 (NPC 2021).

¹⁴ *Id.* at 2.

We will treat your “Personal Information” confidential. It will only be disclosed, subject to our permission to our affiliates such as credit bureaus, collection companies and other financial institutions for the purpose of assisting you in your financial needs and for the effective handling of your account.

Further, for the proper assessment of your loan application, you hereby allow GDFI to collect information from any institutions that you are connected with or related to such as but not limited to bank, agencies, employer, airlines and supplier.

Furthermore, in case of restructuring your loan obligation, you are giving consent and allowing GDFI to disclose and collect information from the above mentioned institutions and people.

For further information regarding the privacy policy, you may visit our website at www.gdfi.com.ph.¹⁵

GDFI claimed that it secured GSS’s consent before it proceeded with handling his personal data.¹⁶

On 12 July 2021, an Order was issued, ordering both parties to appear for a preliminary conference on 26 August 2021.¹⁷ After the Preliminary Conference held on 26 August 2021, both parties agreed to undergo mediation proceedings of this Commission to explore the possibility of an amicable settlement.¹⁸ The complaint proceedings were suspended for the conduct of mediation proceedings.¹⁹

On 29 September 2021, the mediation officer, however, issued a Notice of Non-Settlement of Dispute as the parties were unable to reach a settlement.²⁰ The parties were then ordered to submit their respective memoranda.²¹

On 19 October 2021, GSS submitted his Memorandum.²² GSS admitted that he was a former client of GDFI.²³ GSS stated that he previously

¹⁵ *Id.* at 2-3.

¹⁶ *Id.* at 3.

¹⁷ Order to Appear for Preliminary Conference, 12 July 2021, *in* GSS v. Global Dominion Financing Inc. NPC 21-064 (NPC 2021).

¹⁸ Order After the First Preliminary Conference, 26 August 2021, *in* GSS v. Global Dominion Financing Inc. NPC 21-064 (NPC 2021).

¹⁹ Order to Mediate, 13 September 2021, *in* GSS v. Global Dominion Financing Inc. NPC 21-064 (NPC 2021).

²⁰ Notice of Non-Settlement of Dispute, 29 September 2021, *in* GSS v. Global Dominion Financing Inc. NPC 21-064 (NPC 2021).

²¹ Order, 05 October 2021, *in* GSS v. Global Dominion Financing Inc. NPC 21-064 (NPC 2021).

²² Complainant’s Memorandum, 22 October 2021, *in* GSS v. Global Dominion Financing Inc., NPC 21-064 (NPC 2021).

²³ *Id.* at 2.

applied and was granted a car loan by GDFI sometime in the year 2016.²⁴ GSS contended that he has settled and paid his previous car loan with GDFI.²⁵ According to him, “[p]art of the process prior to the grant of the [2016] loan, [GSS] disclosed vital personal information such as his name, age, address, sex, marital status, occupation, financial capacity, and other relevant information to [GDFI].”²⁶ He then reiterated the events that happened from 02 March 2021 to 11 March 2021 regarding his application for a car loan in 2021.²⁷ He claimed that GDFI failed to explain and provide a straightforward answer on the use of his personal information as well as the existence of his namesake with respect to the car loan application.²⁸

GSS contended that GDFI violated Section 25 (Unauthorized Processing) and Section 28 (Processing for Unauthorized Purposes) of the DPA²⁹ and the general data privacy principle of transparency.³⁰ GSS also claimed that GDFI violated his rights as a data subject, specifically the right to be informed and the right to access.³¹ Further, GSS prayed for damages.³²

On 20 October 2021, GDFI submitted its Memorandum.³³ GDFI alleged that the filing of the present case is grounded on suspicion and fear.³⁴ GDFI claimed that it is compliant with the mandate of the DPA as it ensures that the personal information of its clients are secured and protected.³⁵ It submitted a copy of the Loan Application Form that bears GSS’s signature.³⁶ It claimed that the signed Loan Application Form shows GSS authorizing GDFI to process GSS’s personal data for an authorized purpose that is solely in relation with his loan application.³⁷

GDFI alleged that it met the criteria for lawful processing of personal information stating Section 12 (a) and (b), and Section 13 (a) of the DPA

²⁴ *Id.* .

²⁵ *Id.* Exhibit F and G.

²⁶ *Id.* at 2.

²⁷ *Id.* at 2-3.

²⁸ Complainant’s Memorandum, 22 October 2021, at 2, *in* GSS v. Global Dominion Financing Inc., NPC 21-064 (NPC 2021).

²⁹ *Id.* at 5-6.

³⁰ *Id.* at 7.

³¹ *Id.* at 6-7.

³² *Id.* at 8-9.

³³ Respondent’s Memorandum, 22 October 2021, *in* GSS v. Global Dominion Financing Inc., NPC 21-064 (NPC 2021).

³⁴ *Id.* at 2.

³⁵ *Id.* at 3.

³⁶ *Id.* Annex A-1.

³⁷ *Id.* at 4.

as bases for its lawful processing.³⁸ GDFI prayed that the case be dismissed for lack of merit.³⁹

Issue

Whether the complaint should have been dismissed outright on procedural grounds.

Discussion

I. The complaint should not have been given due course pursuant to Section 2 of Rule II of NPC Circular No. 2021-01 (2021 NPC Rules of Procedure).

Section 2 of Rule II of the 2021 NPC Rules of Procedure provides:

Section 2. *Exhaustion of remedies.* – No complaint shall be given due course unless it has been sufficiently established and proven that:

1. the complainant has informed, in writing, the personal information controller (PIC), personal information processor (PIP), or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same; and
2. the PIC, PIP, or concerned entity did not take timely or appropriate action on the claimed privacy violation or personal data breach, or there is no response from the PIC, PIP, or concerned entity within fifteen (15) calendar days from receipt of written information from the complainant.

The NPC may waive any or all of the requirements of this Section at its discretion upon (a) good cause shown, properly alleged and proved by the complainant; or (b) if the allegations in the complaint involve a serious violation or breach of the Data Privacy Act of 2012, taking into account the risk of harm to the affected data subject[.]⁴⁰

³⁸ *Id.* at 4-5.

³⁹ Respondent's Memorandum, 22 October 2021, at 5, *in* GSS v. Global Dominion Financing Inc., NPC 21-064 (NPC 2021).

⁴⁰ National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC 2021 Rules of Procedure], rule II, § 2 (28 January 2021).

In order for the complaint to be given due course, Section 2 of Rule II of the 2021 NPC Rules of Procedure requires that the complainant must first inform, in writing, the concerned entity of the alleged privacy violation or personal data breach.⁴¹ Following the written notification, the concerned entity did not take timely or appropriate action on the alleged privacy violation nor did it respond within fifteen

(15) calendar days from receipt of written information from the complainant.⁴² The fifteen (15) calendar days granted by the 2021 NPC Rules of Procedure affords the concerned entity an opportunity to address the alleged privacy violation by either taking timely or appropriate action, or responding to the written information given by the complainant.⁴³ These two requisites should have been sufficiently established and proven before a complaint is given due course.⁴⁴

The Commission finds that GSS's complaint should not have been given due course by the CID because GSS failed to comply with exhaustion of remedies. In *MRS v. National Conciliation and Mediation Board (NCMB) and Department of Labor and Employment (DOLE)*, the Commission dismissed the case for failure to exhaust remedies.⁴⁵ The Commission held that "where circumstances permit, it is a condition precedent to the filing of complaints that complainants give the respondents the opportunity to address the complaints against them."⁴⁶

In this case, GSS cancelled his application for a car loan through email on 11 March 2021.⁴⁷ In the email, GSS did not inform GDFI in writing of the alleged privacy violation committed against him but merely notified GDFI of the cancellation of his application for the car loan.⁴⁸ Subsequently, on 22 March 2021, eleven (11) calendar days after GSS cancelled his application for the car loan with GDFI, GSS filed a complaint with the NPC.⁴⁹

Even assuming that GSS was able to inform GDFI of the alleged privacy violation in his Notice of Cancellation, GSS failed to observe

⁴¹ *Id.*

⁴² *Id.*

⁴³ *KRL v. Trinity University of Asia*, CID Case No. 17-K-003, 19 November 2019, at 6, *available at* <https://www.privacy.gov.ph/wp-content/uploads/2020/10/CID-17-K-003-KRL-v-Trinity-Decision-PSD-10Aug2020.pdf> (last accessed 23 June 2022).

⁴⁴ NPC 2021 Rules of Procedure, rule II, § 2.

⁴⁵ *MRS v. National Conciliation and Mediation Board (NCMB) and Department of Labor and Employment (DOLE)*, NPC Case No. 18-152, 08 June 2020, at 4, *available at* <https://www.privacy.gov.ph/wp-content/uploads/2020/12/NPC-18-152-MRS-v-NCMB-Pseudonymized-16Dec2020-ADJ1.pdf> (last accessed 1 July 2022).

⁴⁶ *Id.*

⁴⁷ Complaints-Assisted Form, 22 March 2021, at 3, *in* *GSS v. Global Dominion Financing Inc.*, NPC 21-064 (NPC 2021).

⁴⁸ *Id.*

⁴⁹ *Id.*

the fifteen-day period in Section 2 (1) of Rule II of the 2021 NPC Rules of Procedure. GSS filed a complaint before the lapse of fifteen (15) calendar days from receipt of written information to GDFI, giving an opportunity for it to take timely or appropriate action or respond to GSS's written notification.

Although Section 2 of Rule II of the 2021 NPC Rules of Procedure provides exceptions to the requirement of exhaustion of remedies, nothing in the records show that GSS's case warrants a waiver of the requirement of exhaustion of remedies. The Commission finds that there is neither a serious violation nor breach of the DPA that gives rise to a risk of harm to the affected data subject.⁵⁰ Thus, the complaint filed by GSS should not have been given due course.

II. The case should have been dismissed outright pursuant to Section 1 (3) and (4) of Rule IV of the 2021 NPC Rules of Procedure.

GSS's case should have been dismissed outright as there was no privacy violation. Section 1 (3) of Rule IV of the 2021 NPC Rules of Procedure provides:

Section 1. *Outright dismissal, when allowed.* – Within thirty (30) calendar days from receipt of the complaint, the investigating officer may give the complaint due course or dismiss the complaint without prejudice, on any the following grounds:

. . .

3. The complaint does not pertain to a violation of the Data Privacy Act of 2012 or does not involve a privacy violation or personal data breach[.]⁵¹

A privacy violation pertains to the processing of personal information in violation of a person's reasonable expectation of confidentiality or privacy or in violation of any law, rules, or regulation relating to the protection of personal data, such as the DPA. It includes but is not limited to a violation of the general principles of privacy, a violation of the rights of the data subjects, unauthorized processing, improper disposal of personal data, processing for an unauthorized purpose,

⁵⁰ NPC 2021 Rules of Procedure, rule II, § 2.

⁵¹ *Id.* rule IV, § 1 (3).

concealment of security breaches, and unauthorized or malicious disclosure.⁵²

In this case, the complaint filed by GSS does not involve a privacy violation. GSS filed the case primarily based on speculation and fear. As admitted by GSS in his Memorandum, he states that “[he] feared that he might be exposed to identity theft considering someone might have used the personal data he had with GDFI without his knowledge”.⁵³

Mere speculation of a supposed privacy violation cannot be considered ripe for adjudication. The Supreme Court has held:

A question is ripe for adjudication when the act being challenged has had a direct adverse effect on the individual challenging it. **For a case to be considered ripe for adjudication, it is a prerequisite that something has then been accomplished or performed by either branch before a court may come into the picture, and the petitioner must allege the existence of an immediate or threatened injury to himself as a result of the challenged action.** He must show that he has sustained or is immediately in danger of sustaining some direct injury as a result of the act complained of.⁵⁴

The challenged act must have been accomplished or performed and must have a direct adverse effect against the complainant for the case to be considered ripe for adjudication. The complainant must also show that the act complained of has an immediate and direct injury to himself or herself.

In this case, the act that GSS is complaining of is GDFI’s delay in processing his car loan application due to his having a namesake in GDFI’s records. GSS, however, failed to substantiate how GDFI processed his personal information in violation of the DPA. To substantiate his claim, GSS presented the written communication between him and GDFI, which shows his inquiry about his car loan application and GDFI’s response and explanation that he has a namesake in its records.⁵⁵ There is nothing in the complaint and

⁵² See An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

⁵³ Complainant’s Memorandum, 22 October 2021, at 3, *in* GSS v. Global Dominion Financing Inc., NPC 21-064 (NF 2021).

⁵⁴ *Samahan ng mga Progresibong Kabataan v. Quezon City*, G.R. No. 225442 (2017). Emphasis Supplied.

⁵⁵ Complainant’s Memorandum, Exhibit A-D, 22 October 2021, *in* GSS v. Global Dominion Financing Inc., NPC 21-064 (NPC 2021).

evidence presented that credibly supports his fear of being “exposed to identity theft,”⁵⁶ any unauthorized processing of his personal information, or processing of his personal information for an unauthorized purpose. GSS failed to show that he has sustained or is immediately in danger of sustaining some direct injury as a result of the act complained of.

In any case, GSS’s complaint should have been dismissed outright because there is insufficient information to substantiate the allegations in the complaint. Section 1 (4) of Rule IV of the 2021 NPC Rules of Procedure provides.

Section 1. *Outright dismissal, when allowed.* – Within thirty (30) calendar days from receipt of the complaint, the investigating officer may give the complaint due course or dismiss the complaint without prejudice, on any the following grounds:

...

4. There is insufficient information to substantiate the allegations in the complaint[.]⁵⁷

The 2021 NPC Rules of Procedure allows the outright dismissal of the case when there is insufficient information to substantiate the allegations in the complaint.⁵⁸ In this case, GSS alleges that GDFI committed unauthorized processing and processing for an unauthorized purpose.⁵⁹ GSS’s evidence, however, failed to substantiate how the personal information was processed. The evidence merely showed GDFI informing GSS of a namesake in its records that caused the delay of granting his application for a car loan.⁶⁰

Contrary to GSS’s allegations, having a namesake in the database of the company or its affiliate by itself does not automatically result to unauthorized processing or processing for an unauthorized purpose. GSS’s fear of someone else using his personal information is primarily based on speculation. Thus, the Commission finds that the written communication between GSS and GDFI and the documents related to

⁵⁶ *Id.* at 3.

⁵⁷ NPC 2021 Rules of Procedure, rule IV, § 1 (4).

⁵⁸ *Id.*

⁵⁹ Complainant’s Memorandum, 22 October 2021, at 5-6, *in* GSS v. Global Dominion Financing Inc., NPC 21-064 (NPC 2021).

⁶⁰ *Id.* Exhibit A-D.

the application of a car loan that GSS submitted as evidence failed to substantiate GSS's claim of unauthorized processing or processing for an unauthorized purpose committed by GDFI.

The Commission observes that although there may be fraud-related issues that fall under the DPA, the filing of cases pertaining solely to fraud-related issues without a privacy issue is not within the jurisdiction of the Commission. For the education of the public, the DPA covers data privacy-related issues. It cannot be used to seek redress against fraud-related issues that do not involve any privacy violations. Thus, the Commission's jurisdiction to hear and decide a case is based on whether the allegations in the complaint sets forth a violation of the DPA, its IRR, and other issuances of the Commission. Otherwise, the case is not within the jurisdiction of the Commission and it should be heard and decided by other appropriate bodies.

As discussed, the complaint should not have been given due course not only because GSS failed to comply with the requirement of exhaustion of remedies but also because the complaint did not involve any privacy violation. Further, GSS failed to present anything aside from fear and speculation to substantiate the allegations in his complaint.

WHEREFORE, premises considered, this Commission resolves that the instant Complaint filed by Gaudencio S. GSS Jr. against Global Dominion Financing Inc. (GDFI) is hereby **DISMISSED** for lack of merit.

This is without prejudice to the filing of appropriate civil, criminal, or administrative cases against GDFI before any other forum or tribunal, if any.

SO ORDERED.

City of Pasay, Philippines.
16 June 2022.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

WE CONCUR:

JOHN HENRY D. NAGA
Privacy Commissioner

DUG CHRISTOPHER B. MAH
Deputy Privacy Commissioner

Copy furnished:

GSS
Complainant

GLOBAL DOMINION FINANCING INC.
Respondent

RVL
Counsel for Complainant

MCS
Counsel for Respondent

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

RTB,
Complainant,

- versus -

**EAST WEST BANKING
CORPORATION,**
Respondent.

X _____ X

NPC 21-086
For: Violation of
the Data Privacy
Act of 2012

DECISION

AGUIRRE, D.P.C.:

Before this Commission is a Complaint filed by RTB (RTB) against East West Banking Corporation (EWBC) for an alleged disclosure of his personal information without a lawful basis under the Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (DPA).

Facts

On 25 July 2017, RTB applied for a car loan with Philippine Bank of Communications (PBComm). He executed a Promissory Note with Chattel Mortgage with PBComm.¹

On 25 June 2019, EWBC and PBComm entered into a Deed of Assignment where PBComm assigned and transferred several mortgage amortized loan accounts to EWBC.² RTB's loan account and the rights and obligations accruing to PBComm was included in the assignment.³

In November 2020, RTB furnished EWBC with several post-dated checks for the payment of his loan.⁴

¹ Memorandum, 13 December 2021, at 2, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2021) (pending).

² *Id.* at 3.

³ *Id.*

⁴ *Id.*

In December 2020, EWBC's system tagged RTB's loan account as past due despite RTB's submission of post-dated checks.⁵ EWBC then referred the matter to its third-party collection agency which resulted in RTB's harassment in the form of misleading phone calls and attempts to take away his car.⁶

Sometime in January 2021, RTB brought the issue to EWBC's attention and stated that his loan account is current since he submitted the necessary post-dated checks for the payment of the loan.⁷

EWBC conducted an internal investigation and determined that its branch personnel inadvertently failed to deposit RTB's post-dated check designated for the payment due on 28 December 2020.⁸ EWBC's inaction resulted in the system's classification of RTB's account as past due and consequently, the referral of the account to its third-party collection agency for collection.⁹

On 25 May 2021, RTB filed a Complaint dated 14 May 2021 against EWBC.¹⁰ He alleges that EWBC processed and disclosed his personal information to third-party collection agents.¹¹ He argues that EWBC violated Section 25 (Unauthorized Processing), Section 26 (Access due to Negligence), Section 28 (Processing for Unauthorized Purpose), and Section 32 (Unauthorized Disclosure) of the DPA.¹² He prays for damages, issuance of a fine against EWBC, and a waiver of the outstanding balance of the car loan.¹³

On 24 June 2021, the Commission issued an Order directing EWBC to file a verified comment within fifteen (15) calendar days from receipt of this Order.¹⁴

In EWBC's Comment dated 28 July 2021, it maintains that RTB consented to the sharing of his personal information with third parties

⁵ *Id.*

⁶ *Id.*

⁷ Complaints-Assisted Form, 25 May 2021, Annex A, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2021) (pending).

⁸ Memorandum, 13 December 2021, at 3, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2021) (pending).

⁹ *Id.*

¹⁰ Complaints-Assisted Form, 25 May 2021, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2021) (pending).

¹¹ *Id.* at 4.

¹² *Id.* at 3.

¹³ *Id.* at 5.

¹⁴ Order to Comment, 24 June 2021, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2021) (pending).

when he entered into the car loan.¹⁵ EWBC explained that RTB signed a Promissory Note with Chattel Mortgage with PBComm and agreed to the Terms and Conditions of the car loan. The relevant provision of the Terms and Conditions states:

29. The MORTGAGEE may appoint or designate a representative, agent, attorney-in-fact, or upon written notice, a collection agency to perform any and all acts which may be required or necessary to enforce MORTGAGEE'S right. For such purpose, the MORTGAGOR hereby gives his consent as to the disclosure of all relative information in connection with the subject loan or his account to such authorized representative, agent or attorney-in- fact and agrees to hold PBComm free and harmless against any and all damages, cost, or liability arising from such disclosure.¹⁶

Given the foregoing, EWBC argues that it is within its authority to share RTB's loan account with its third-party collection agency. EWBC prays for the dismissal of the case.¹⁷

On 06 October 2021, the parties conferred for mediation but failed to reach a settlement.¹⁸ On 03 November 2021, the Commission issued an Order for the resumption of complaint proceedings and ordered the parties to submit their respective Memoranda within fifteen (15) calendar days from receipt of the Order.¹⁹

On 15 November 2021, RTB, by email, reiterated the arguments he raised in his Complaint.²⁰ He maintained that EWBC should have exercised, as expected from banks, extraordinary diligence in handling his loan account.²¹ EWBC, however, failed to do so and forwarded his personal information to its third-party collection agent even if he submitted the necessary post-dated checks for payment of his car loan.²² He alleged that EWBC's carelessness resulted in "scandalous situations" in his neighborhood thus, besmirching his reputation.²³

¹⁵ Comment (To Complaint dated 14 May 2021), 28 July 2021, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2021) (pending).

¹⁶ *Id.* at 3.

¹⁷ *Id.* at 7.

¹⁸ Order to Mediate, 15 September 2021, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2021) (pending).

¹⁹ Order to Mediate, 03 November 2021, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2021) (pending).

²⁰ Email from RTB to Complaints and Investigation Division, National Privacy Commission (15 November 2021).

²¹ *Id.*

²² *Id.*

²³ *Id.*

On 13 December 2021, EWBC filed its Memorandum.²⁴ It reiterated that RTB executed a Promissory Note with Chattel Mortgage with PBComm and consequently, agreed to the Terms and Conditions of the car loan.²⁵ It stated that it should not be held liable for damages since the collecting personnel conducting the standard collection efforts acted in good faith.²⁶ Contrary to RTB's assertions, neither unnecessary harassment nor public humiliation occurred.²⁷ Thus, EWBC prays for the dismissal of the case.²⁸

Issue

Whether EWBC has a lawful basis to process RTB's personal information, particularly the referral of RTB's loan account to its third- party collection agency.

Discussion

EWBC has lawful basis to process RTB's personal information under Section 12 (b) of the DPA, which provides:

Section 12. *Criteria for Lawful Processing of Personal Information.* – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

...

(b) **The processing of personal information is necessary and is related to the fulfilment of a contract with the data subject** or in order to take steps at the request of the data subject prior to entering into a contract;²⁹

In this case, RTB executed a Promissory Note with Chattel Mortgage for his car loan. The Promissory Note with Chattel Mortgage includes a set of Terms and Conditions, which RTB also agreed to.

²⁴ Memorandum, 13 December 2021, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2021) (pending).

²⁵ *Id.* at 8.

²⁶ *Id.* at 10.

²⁷ *Id.*

²⁸ *Id.* at 11.

²⁹ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 12 (b) (2012). Emphasis supplied.

Although RTB initially entered into a loan agreement with PBComm, the loan contract was assigned to EWBC pursuant to a Deed of Assignment between PBComm and EWBC.

As stated in Section 29 of the Terms and Conditions of the loan agreement, EWBC, as the mortgagee, may designate a collection agency to perform acts necessary to enforce its right, including debt collection. Section 29 of the Terms and Conditions provides:

29. The MORTGAGEE may appoint or designate a representative, agent, attorney-in-fact, or upon written notice, a collection agency to perform any and all acts which may be required or necessary to enforce MORTGAGEE'S right. For such purpose, the MORTGAGOR hereby gives his consent as to the disclosure of all relative information in connection with the subject loan or his account to such authorized representative, agent or attorney-in- fact and agrees to hold PBComm free and harmless against any and all damages, cost, or liability arising from such disclosure.³⁰

For this reason, EWBC's act of processing RTB's personal information is necessary and related to the fulfillment of a contract, which is a lawful basis for processing under Section 12 (b) of the DPA.

The existence of a lawful basis to process personal information must be properly applied based on the factual conditions of the case. Here, EWBC was remiss in its obligation as a Personal Information Controller (PIC) despite the lawful criterion to process based on the fulfillment of a contract. More so, it failed to exercise extraordinary diligence as is expected from a banking institution.³¹

Section 11 of the DPA requires PICs, such as EWBC, to ensure that the personal information of the data subject is kept up to date:

Section 11. *General Data Privacy Principles.* – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

Personal information must, be:

³⁰ Comment (To Complaint dated 14 May 2021), 28 July 2021, at 3, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2021) (pending).

³¹ Banta v. Equitable Bank, Inc., et al., G.R. No. 223694 (2021).

...

(c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;³²

As a PIC, EWBC should have complied with its obligation under Section 11 (c) of the DPA and practiced proper record-keeping. Corollary to this, it should have been mindful of the corresponding deposit dates of the post-dated checks that RTB submitted. Its inadvertence to deposit a post-dated check on the designated date resulted in the unnecessary disclosure of RTB's personal information to EWBC's third-party collection agency.

EWBC also failed to strictly comply with the provisions of Section 29 of the Terms and Conditions attached to the Promissory Note with Chattel Mortgage when it did not provide RTB a written notice of its intention to designate a third-party collection agency to conduct debt collection.

EWBC was sorely remiss in its duty to exercise the diligence required from it as a banking institution. Had EWBC complied with its obligations under Section 11 (c) of the DPA and the loan contract, then it would not have unnecessarily disclosed RTB's personal information.

Nonetheless, EWBC's carelessness is insufficient to warrant a recommendation for its prosecution. After all, EWBC's processing of RTB's personal information is still based on a lawful basis to process under Section 12 (b) of the DPA.

EWBC's actions and consequently, the third-party collection agency's inaccurate use of RTB's personal information, however, justify an award of nominal damages. Section 16 (f) of the DPA provides:

Section 16. *Rights of the Data Subject.* – The data subject is entitled to:

...

³² Data Privacy Act of 2012, § 11 (c).

(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information;³³

Indeed, it is part of the Commission's mandate to award indemnity on matters affecting any personal information.³⁴ The DPA does not require actual or monetary damages for data subjects to exercise the right to damages.³⁵ As provided in the law, the consequences of processing inaccurate information are enough for the right to arise.³⁶

WHEREFORE, premises considered, the Commission resolves to **DISMISS** the Complaint of RTB against East West Banking Corporation (EWBC). The Commission **AWARDS** nominal damages, in the amount of Fifteen Thousand Pesos (P15,000.00), to RTB for EWBC's failure to fulfill its obligation as a Personal Information Controller under Section 11 (c) of the Data Privacy Act of 2012. EWBC is **ORDERED** to submit its compliance within fifteen (15) days from receipt of this Decision.

SO ORDERED.

Pasay City, Philippines.
03 February 2022.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

³³ *Id.* § 16 (f).

³⁴ Data Privacy Act of 2012, § 7 (b).

³⁵ NPC 18-038, 21 May 2020 (NPC 2020) (unreported).

³⁶ *Id.*

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Copy furnished:

RTB
Complainant

OPBLO
Counsel for East West Banking Corporation

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION**
GENERAL RECORDS UNIT
National Privacy Commission

AC, *Complainant,*

-
versus-

NPC 21-096

For: Violation of
the Data Privacy
Act of 2012

ISG,

Responde

X-----*nt.*-----X

DECISION

AGUIRRE, D.P.C.;

Before this Commission is a complaint filed by AC against ISG for an alleged violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

On 06 November 2020, before AC filed a complaint with the National Privacy Commission (NPC), ISG filed before the Office of the City Prosecutor of Manila a criminal complaint against AC and her adoptive mother, Victoria AC, for unjust vexation and violation of Section 8 of Republic Act No. 11494, otherwise known as Bayanihan to Recover as One Act.¹

The criminal complaint stemmed from a Barangay Kagawad and a Manila Health Officer's house visit to ISG's residence pertaining to the RT-PCR test result of ISG's sister.² The Barangay Kagawad visited ISG's residence to inform them that ISG's sister tested positive for COVID-19.³ Myka Santos, ISG's niece, received the news and denied

¹ Complaint-Affidavit, 19 May 2021, Annex A, *in* AC v. ISG, NPC 21-096 (NPC 2021).

² *Id.*

³ *Id.*

that her aunt tested positive for COVID-19.⁴ This conversation was overheard by VC who lived across ISG's residence.⁵

In the criminal complaint, ISG used Closed-circuit Television (CCTV) footages as evidence in support of the criminal charges against the ACs.⁶ The CCTV footage showed AC spraying a liquid substance, presumably alcohol, all over his body when he saw ISG and her sister passing near him.⁷ Another CCTV footage showed VC telling a delivery driver to prepare alcohol because he was delivering food to a COVID-19 positive resident.⁸ These incidents happened along the narrow alley that the ACs and the ISGs share.⁹

On 24 February 2021, the City Prosecutor issued a Resolution dismissing the charges for violation of Section 8 of R.A. No. 11494 against the ACs, while dismissing the charges of unjust vexation only against AC.¹⁰

On 19 May 2021, AC filed a Complaint-Affidavit with the Commission against ISG.¹¹ In AC's Complaint-Affidavit, he alleged that ISG committed gross violation of his privacy when she installed the CCTV camera with audio inside her property.¹² AC claims that the CCTV footages show the entrance of ISG's residence, the narrow alley that the ACs and ISGs share, and the façade of AC's residence.¹³ AC claims that he was "taken aback" when he saw the contents of the criminal complaint and saw that the evidence used against him were the CCTV footages.¹⁴ He further claims that the CCTV footages contained "very sensitive footages" of himself and others going about their daily business and they were being recorded without their knowledge and consent.¹⁵

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ Complaint-Affidavit, 19 May 2021, Annex A, *in* AC v. ISG, NPC 21-096 (NPC 2021).

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*, Annex B.

¹¹ *Id.*

¹² *Id.*, at 3.

¹³ Complaint-Affidavit, 19 May 2021, Annex C, *in* AC v. ISG, NPC 21-096 (NPC 2021).

¹⁴ *Id.*, at 2.

¹⁵ *Id.*

AC alleges that ISG recorded his everyday doings in the neighborhood.¹⁶ AC states that “[t]he microphone of [ISG’s] CCTV could pick up the slightest sound from a distance. Hence, it could pick up any conversation from a distance, like a spy satellite.”¹⁷

AC contends that since the criminal case against him has been dismissed, ISG has been using her CCTV to purposely pry into the ACs’ private lives and to watch his every move.¹⁸ AC considers this a gross violation of his privacy.¹⁹ Thus, he alleges that ISG violated the provisions of the DPA and Republic Act No. 4200 otherwise known as Anti-Wire Tapping Act.²⁰

On 13 July 2021, the Commission, through the Complaints and Investigation Division (CID) issued an Order directing ISG to file a verified comment within fifteen (15) calendar days from receipt and to appear for a Preliminary Conference on 21 September 2021.²¹

On 06 August 2021, ISG filed her Verified Comment.²² She admits that she used the CCTV footages as evidence in the criminal case filed against AC.²³ She avers the complaint must be dismissed because it does not allege which provision of the DPA has been violated by the CCTV recording.²⁴ She claims that “[AC] should not be allowed to ISG on a fishing expedition by alleging a violation of the law in general, and then picking out a particular violation as the proceedings ISG on.”²⁵

Further, ISG contends that under Sec. 4(A)(2) of NPC Advisory 2020- 04 (Guidelines on the Use of Closed-Circuit Television (CCTV) Systems)²⁶ “security of properties and protection of vitally important interests of individuals is a legitimate reason for installing a CCTV system.”²⁷ ISG contends that she installed the CCTV system to

¹⁶ *Id.* at 2-3.

¹⁷ *Id.* at 1-2.

¹⁸ *Id.*

¹⁹ Complaint-Affidavit, 19 May 2021, at 2-3, *in AC v. ISG*, NPC 21-096 (NPC 2021).

²⁰ *Id.* at 3.

²¹ Order, 13 July 2021, , *in AC v. ISG*, NPC 21-096 (NPC 2021).

²² Verified Comment, 06 August 2021, *in AC v. ISG*, NPC 21-096 (NPC 2021).

²³ *Id.* at 1.

²⁴ *Id.* at 1-2.

²⁵ *Id.*

²⁶ National Privacy Commission, Guidelines on the Use of Closed-Circuit Television (CCTV) Systems, Advisory No. 04, Series of 2020 [NPC Advisory No. 20-04], § 4 (A) (2) (16 November 2020).

²⁷ Verified Comment, 06 August 2021, at 2, *in AC v. ISG*, NPC 21-096 (NPC 2021).

protect her rights and to document acts of harassment by AC.²⁸ She also claims that the CCTV system was recording outdoors in a public place. Under Section 4 (E) of NPC Advisory No. 2020-04, CCTV cameras cannot record in places where there is a heightened expectation of privacy.²⁹ She avers that an alley is not a place where there is such heightened expectation.³⁰

On 21 September 2021, both parties appeared in the Preliminary Conference and manifested that they are not seeking the discovery of any evidence or document from each other.³¹ AC manifested his unwillingness to under ISG mediation proceedings.³² The Commission ordered the parties to submit, within fifteen (15) calendar days after the Preliminary Conference, their respective Memoranda discussing and summarizing their respective causes of action, claims, and defenses.³³

On 05 October 2021, AC submitted his Memorandum which merely reiterated the allegations contained in his Complaint-Affidavit.³⁴

On 06 October 2021, ISG filed her Memorandum which contains a mere repetition of the arguments raised in her Verified Comment.³⁵

Issue

Whether the case should be dismissed outright on procedural grounds.

Discussion

The Commission dismisses the case for lack of merit.

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Id.*

³¹ Order After the 1st Preliminary Conference, 21 September 2021, *in* AC v. ISG, NPC 21-096 (NPC 2021).

³² *Id.*

³³ *Id.*

³⁴ Complainant's Memorandum, 05 October 2021, *in* AC v. ISG, NPC 21-096 (NPC 2021).

³⁵ Respondent's Memorandum, 06 October 2021, *in* AC v. ISG, NPC 21-096 (NPC 2021).

Section 1 (1) of Rule IV of NPC Circular No. 21-01 (2021 NPC Rules of Procedure) states:

Section 1. *Outright dismissal, when allowed.* – Within thirty (30) calendar days from receipt of the complaint, the investigating officer may give the complaint due course or dismiss the complaint without prejudice, on any the following grounds:

1. **The complaint is insufficient in form or did not comply with Section 3, Rule II of these Rules**, unless failure to do so is justified or excused with good cause[.]³⁶

A complaint may be dismissed outright when it is insufficient in form or it did not comply with Section 3, Rule II of the 2021 NPC Rules of Procedure. Section 3 (1) and (10) of Rule II of the 2021 NPC Rules of Procedure provides:

Section 3. *Form and contents of the complaint.* – The complaint should be in the proper form, as follows:

1. The complaint must be in writing, signed by the party or his or her counsel, and verified in the format prescribed under the Rules of Court.

...

10. **A certification against forum shopping must accompany the complaint.** The complainant shall certify under oath in the complaint, or in a sworn certification annexed and simultaneously filed with the pleading: (a) that he or she has not commenced any action or filed any claim involving the same issues in any court, tribunal or quasi-judicial agency and, to the best of his or her knowledge, no such other action or claim is pending with such court, tribunal or quasi-judicial agency; (b) if there is such other pending action or claim, a complete statement of its present status; and (c) if he or she should thereafter learn that the same or similar action or claim has been filed or is pending, he or she shall report that fact within five (5) calendar days therefrom to the NPC.

Failure to comply with the proper form and contents of the complaint may cause for outright dismissal under Section

³⁶ National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC 2021 Rules of Procedure] rule IV, § 1 (1) (28 January 2021). Emphasis supplied.

1(1), Rule IV: Provided, an application that does not comply with the foregoing requirements may be acted upon if it merits appropriate consideration on its face, or is of such notoriety that it necessarily contains sufficient leads or particulars to enable the taking of further action.³⁷

Section 3 (1) of Rule II of the 2021 NPC Rules of Procedure states that complaints filed before the Commission should be “verified in the format prescribed under the Rules of Court.”³⁸ Section 4, Rule 7 of the Rules of Court provides:

Section 4. *Verification.* –

...

A pleading is verified by an affidavit of an affiant duly authorized to sign said verification. The authorization of the affiant to act on behalf of a party, whether in the form of a secretary's certificate or a special power of attorney, should be attached to the pleading, and shall allege the following attestations:

- (a) The allegations in the pleading are true and correct based on his personal knowledge, or based on authentic documents;
- (b) The pleading is not filed to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and
- (c) The factual allegations therein have evidentiary support or, if specifically so identified, will likewise have evidentiary support after a reasonable opportunity for discovery.

The signature of the affiant shall further serve as a certification of the truthfulness of the allegations in the pleading.³⁹

The Supreme Court ruled that “[v]erification is deemed substantially complied with when one who has ample knowledge to swear to the truth of the allegations in the complaint or petition signs the verification, and when matters alleged in the petition have been made in good faith or are true and correct.”⁴⁰

³⁷ NPC 2021 Rules of Procedure. Rule II, § 3 (1). Emphasis supplied.

³⁸ *Id.*

³⁹ 2019 AMENDMENTS TO THE 1997 RULES OF CIVIL PROCEDURE, rule 7, § 4.

⁴⁰ Heirs of Josefina Gabriel v. Cebrero, G.R. 222737 (2018).

In this case, AC's Complaint-Affidavit does not specifically state the attestations enumerated under the Rules of Court. While technical rules of procedure do not strictly apply to administrative bodies,⁴¹ the notarized complaint still failed to effectively provide for the required attestations. The notarization only certifies the fact that AC personally executed the document.⁴² Thus, AC's complaint does not substantially comply with the requirement of verification.

As to Section 3 (10) of Rule II of the 2021 NPC Rules of Procedure, it requires that a certification against forum shopping must accompany the complaint.⁴³ AC failed to observe this procedural requirement when he did not attach the certification to his complaint.

The Supreme Court explained the mandatory nature of the certification against forum shopping:

The rule on certification against forum shopping is intended to prevent the actual filing of multiple petitions/complaints involving identical causes of action, subject matter and issues in other tribunals or agencies as a form of forum shopping. This is rooted in the principle that a party-litigant should not be allowed to pursue simultaneous remedies in different forums, as this practice is detrimental to orderly judicial procedure. **Although not jurisdictional, the requirement of a certification of non-forum shopping is mandatory. The rule requires that a certification against forum shopping should be appended to or incorporated in the initiatory pleading filed before the court.** The rule also requires that the party, not counsel, must certify under oath that he has not commenced any other action involving the same issue in the court or any other tribunal or agency.⁴⁴

The Supreme Court further clarified the difference between non-compliance and substantial compliance with the procedural requirements:

A distinction must be made between non-compliance with the requirement on or submission of defective verification, and

⁴¹ Divina Palao v. Florentino International, Inc., G.R. No. 186967 (2017).

⁴² Complaint-Affidavit, 19 May 2021, *in* AC v. ISG, NPC 21-096 (NPC 2021).

⁴³ NPC 2021 Rules of Procedure, Rule II, § 3 (10).

⁴⁴ Philippine Public School Teachers Association v. Austria-Martinez, G.R. No. 171562 (2006). Emphasis supplied.

non-compliance with the requirement on or submission of defective certification against forum shopping.

...

As to certification against forum shopping, non-compliance therewith or a defect therein, unlike in verification, is generally not curable by its subsequent submission or correction thereof, unless there is a need to relax the Rule on the ground of "substantial compliance" or presence of "special circumstances or compelling reasons".⁴⁵

In this case, AC's failure to append or incorporate his certification against forum shopping with his complaint shows non-compliance with the mandatory procedural requirement. There could also be no substantial compliance. He did not provide any attestation that could effectively be considered as a certification against forum shopping incorporated in his complaint.

The 2021 NPC Rules of Procedure provides that there may be a waiver of failure to submit a certification against forum shopping if the complainant may be excused with good cause,⁴⁶ or if it merits appropriate consideration on its face, or, if it is of such notoriety that it necessarily contains sufficient leads or particulars to enable the taking of further action.⁴⁷ In this case, there is nothing in the records that show any of the circumstances to justify the non-compliance of the procedural requirement.

AC has not alleged or shown anything in his complaint that will warrant a waiver of the procedural requirement of a certification against non-forum shopping. Mere allegations in a complaint without submitting any further evidence neither merits appropriate consideration on its face nor is of such notoriety that it necessarily contains sufficient leads or particulars to enable the taking of further action.⁴⁸

In AC's complaint, he alleged that "ISG recorded his everyday doings in the neighborhood"⁴⁹ and that "ISG has been using her CCTV to

⁴⁵ Heirs of Josefina Gabriel v. Cebrero, G.R. 222737 (2018).

⁴⁶ NPC 2021 Rules of Procedure. Rule IV, § 1 (1).

⁴⁷ NPC 2021 Rules of Procedure. Rule II, § 3 (10).

⁴⁸ See NPC 2021 Rules of Procedure. Rule II, § 3 (1).

⁴⁹ Complaint-Affidavit, 19 May 2021, at 1, *In* AC v. ISG, NPC 21-096 (NPC 2021).

purposely pry into their private lives.”⁵⁰ The only evidence he submitted to support his allegations were the same CCTV footages that ISG used as evidence in the criminal case for unjust vexation and a violation of R.A. No. 11494. AC did not actually produce his own evidence to support his allegations but merely used the evidence that ISG submitted in a previous case as basis for his complaint before this Commission. Since AC’s complaint lacks evidence to support his allegations, there is nothing in his complaint that warrants a waiver of the procedural requirements.

As a result of the non-compliance with Section 3 of Rule II of the 2021 NPC Rules of Procedure, AC’s complaint should have been dismissed outright and should not have been given due course.

Although this case warrants an outright dismissal for failure to submit a certification against forum shopping, the Commission takes this opportunity to discuss the general considerations of CCTV systems.

NPC Advisory No. 2020-04 (Guidelines on the Use of Closed-Circuit Television (CCTV) Systems) was issued to guide the public on the use of CCTV systems considering its impact on the rights and freedoms of data subjects.⁵¹ The use of CCTV Systems shall be subject to regular review to ensure that its use remains to be necessary for specified and legitimate purposes.⁵²

Section 5 (A) of NPC Advisory No. 2020-04 provides:

Section 5. *Specific use cases.* The use of CCTV systems shall be limited to and consistent with the purpose/s for which the same was established. The use of CCTVs may be for the following instances:

- A. Household. Generally, the use of CCTV systems for purely personal, family or household affairs is outside the purview of this Advisory. Nonetheless, the use of these

⁵⁰ *Id.* at 3.

⁵¹ NPC Advisory No. 20-04, § 1 (B).

⁵² *Id.*

systems shall still bear in mind the rights of every individual to privacy.

Where a CCTV faces outwards from an individual's private property and it captures images of individuals beyond the boundaries of such property, particularly where it monitors a public space, the CCTV system cannot be considered as being for a purely personal, family or household purpose. As such, the operator of such CCTV system is deemed as a PIC and will be subjected to the obligations under the DPA and the provisions of this Advisory.⁵³

Pursuant to Section 5 (A) of NPC Advisory No. 2020-04, a natural or juridical person who sets up a CCTV system for household purposes is generally not considered a Personal Information Controller (PIC), thus, outside the purview of the Advisory and the DPA. Section 5 (A) of NPC Advisory No. 2020-04 also provides that the CCTV system cannot be considered as being for purely household purposes where a CCTV system faces outwards and captures a public space beyond the perimeter of an individual's private property. In such cases, the operator of the CCTV system may be considered a PIC.

Section 5 (A) of NPC Advisory No. 2020-04, however, should be read and understood in accordance with the guidelines provided for in Section 4 of NPC Advisory No. 2020-04.

Section 4(A)(2) and (B) of the same Advisory provides:

Section 4. *Guidelines.* — The processing of personal data in CCTV systems shall be subject to the following guidelines:

A. Legitimate purpose. Prior to installing a CCTV system, the purpose/s for personal data processing using such system must be clearly determined. Such processing may be permitted for the following purposes, except where the same are overridden by the fundamental rights and freedoms of the data subject:

...

2. Security of properties and protection of vitally important interests of individuals;

⁵³ *Id.* § 5 (A).

...

B. Proportionality. The PIC should evaluate whether the installation and operation of CCTV systems and the nature and kind thereof is necessary for its legitimate purpose, considering whether such purposes could be reasonably fulfilled by other less intrusive means.⁵⁴

Under Section 4(A)(2) of NPC Advisory No. 2020-04, security of properties and protection of vitally important interests of individuals are legitimate reasons for installing a CCTV system.⁵⁵ Further, Section 4 (B) of the NPC Advisory No. 2020-04, on proportionality, provides that the operator of the CCTV system should evaluate whether his or her usage of the CCTV system is necessary for its legitimate purpose, and considering whether its legitimate purpose could be reasonably fulfilled by other less intrusive means.⁵⁶ Thus, the processing of personal information shall be adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified legitimate purpose.⁵⁷

In this case, ISG claims that the purpose for the installation of CCTV systems is to protect her interest in her security and property⁵⁸ as well as protect her rights and document the acts of harassment committed by the ACs against her and her family.⁵⁹ ISG, however, should accomplish her legitimate purpose through the least intrusive means.

To determine whether the installation and operation of the CCTV system is proportional to the operator's legitimate purpose, the location and placement of the CCTV system must also be considered. Section 4 (E) of NPC Advisory No. 2020-04 provides guidelines on the location and placement of the CCTV system:

Section 4. *Guidelines.* — The processing of personal data in CCTV systems shall be subject to the following guidelines:

⁵⁴ *Id.* § 4 (A) (2), (B).

⁵⁵ *Id.* § 4 (A) (2).

⁵⁶ *Id.* § 4 (B).

⁵⁷ National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule IV, 18 (c) (2016).

⁵⁸ Respondent's Memorandum, 06 October 2021, *in* AC v. ISG, NPC 21-096 (NPC 2021).

⁵⁹ Verified Comment, 06 August 2021, *in* AC v. ISG, NPC 21-096 (NPC 2021).

...

E. Location and placement. To ensure that CCTV systems capture footages in a manner consistent with the DPA, the location and angles of the cameras must be carefully considered. CCTVs shall only be used to monitor the intended spaces, taking into consideration the purpose for monitoring the same.⁶⁰

The manner of positioning the CCTV system and the purpose for monitoring the intended spaces govern the intention of the operator of the CCTV system. In this case, ISG's CCTV system captures the entrance to her residence, the alley, and the façade of AC's house.⁶¹ Considering the narrowness of the alley in this situation, it is, however, unavoidable for the CCTV system to capture the alley and the façade of AC's house. Nevertheless, the CCTV operator must exert a concerted effort in capturing more of his or her household rather than public spaces such as a shared alley, or another's property.

Here, the angle of ISG's CCTV system may be repositioned to capture more of her own residence and not the public space and façade of AC's house. Otherwise, ISG's usage of the CCTV system may not be in accordance with the guidelines of legitimate purpose and proportionality.

As discussed, AC did not substantially comply with the verification requirement and did not attach a certification against forum shopping with his complaint. The non-observance of these procedural requirements is deemed fatal to his case. Thus, the Commission finds that AC's failure to comply with the verification and certification requirements under the 2021 NPC Rules of Procedure warrants an outright dismissal of the case.

WHEREFORE, premises considered, this Commission resolves that the complaint filed by AC against ISG is hereby **DISMISSED** for lack of merit.

⁶⁰ NPC Advisory No. 20-04, § 4 (E).

⁶¹ Complaint-Affidavit, 19 May 2021, Annex C, *in* AC v. ISG, NPC 21-096 (NPC 2021).

This is without prejudice to the filing of appropriate civil, criminal, or administrative cases before any other forum or tribunal, if any.

SO ORDERED.

City of Pasay, Philippines.
16 May 2022.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

JOHN HENRY D. NAGA
Privacy Commissioner

DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

AC
Complainant

ISG
Respondent

ACF
Counsel for Complainant

RCD

Counsel for Respondent

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

MEC
Complainant,

-versus-

NPC 19-501
(Formerly CID Case No. 19-G-501) *For: Violation of the Data Privacy Act of 2012*

ROBOCASH FINANCE CORPORATION,
Respondent,

X ----- X

DECISION

NAGA, D.P.C.:

This is a complaint filed by MEC (Complainant) against Robocash Finance Corporation (Respondent) for violation of her rights under the Data Privacy Act (DPA).

The Facts

On 02 April 2019, Complainant obtained a loan from Respondent in the amount of Php5,500.00. When Complainant failed to follow through on her payment, she found out that the Respondent had been calling and sending text messages to her phone contact list. Complainant also avers that the Respondent threatened to file a case in small claims court against her. Lastly, Complainant said that the acts of Respondent made her feel anxious, embarrassed, and depressed causing her to file the instant complaint before the Commission.

On 20 August 2019, the parties and their respective counsels were ordered to appear for a Discovery Conference. During the conduct of the Conference, the parties agreed to apply for a mediated settlement.

On 17 September 2019, Complainant failed to appear on the scheduled mediation conference without justifiable reason. Thus, the parties were ordered to appear for another mediation conference.

On 24 October 2019, the investigating officer ordered the resumption of the complaint proceedings considering that the Complainant again failed to appear in the mediation conference. Thus, the mediation officer issued a Notice of Non-Settlement of Dispute.

On 19 November 2019, the parties were then ordered to appear for the resumption of the complaint proceedings. However, only the Respondent appeared. Thereafter, Respondent was ordered to submit its responsive comment within ten (10) days.

On 28 November 2019, Respondent submitted its responsive comment. They prayed for the dismissal of the instant complaint alleging that Complainant failed to appear for two (2) consecutive mediation conferences and discovery conference, without justifiable reason.

Respondent also averred that Complainant failed to exhaust available remedies and did not notify them of their alleged violation of her data privacy rights prior to the filing of the instant complaint.

Finally, the Respondent emphasized that the Complainant's bare allegations, which were unsubstantiated by any evidence, were insufficient to constitute proof that the Respondent violated the data privacy rights of the Complainant.

Discussion

Before going to the main issue of the case, this Commission deems it proper to discuss a procedural matter that was raised in the Respondent's responsive comment, specifically on the requirement to

exhaust administrative remedies as provided in Section 4 (a) of NPC Circular 16-04.¹

The Respondent argued that the Complainant failed to exhaust remedies by going straight to this Commission without notifying the Respondent on the alleged data privacy violation committed by them against her. Such action they argued prevented the Respondent to take appropriate measures to address the concerns of the Complainant. The Respondent then concluded that this should cause the outright dismissal of the Complaint.

While the intention of the abovementioned provision is to promote settlement of data privacy disputes between Personal Information Controller (PIC) or the concerned entity and the data subject before going through the formal procedures in this Commission, the Respondent herein must be reminded that the Commission may waive any and all of the requirements of Section 4 at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act.² Thus, this Commission deems it proper to adjudicate on the substantial issues of this case.

Now, on the main issue on whether the Respondent violated the data privacy rights of the Complainant.

This Commission finds that the Complainant failed to provide sufficient information to substantiate the allegations made in her complaint.

Section 10 of NPC Circular No. 16-04 (Rules of Procedure) provides: “The **complaint shall include a brief narration of the material facts and supporting documentary and testimonial evidence**, all of which show: (a) the violation of the Data Privacy Act of related issuance; or (b) the acts or omissions allegedly committed

¹Section 4. **Exhaustion of remedies.** a. The complainant has informed, in writing, the personal information controller or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same;

²Paragraph 3, Id.,

by the respondent amounting to a privacy violation or personal data breach...” (Emphasis Supplied)

Furthermore, Section 22 of the NPC Circular No. 16-04 provides that, “the Commission shall adjudicate the issues raised in the complaint on the basis of all the evidence presented and its own consideration of the law the grounds for the dismissal of complaint.”

In the case at hand, Complainant solely relied on the averments contained in her complaints-assisted form without procuring evidence to support the allegations made. Further, the Complainant failed to cite a single provision in the Data Privacy Act which was violated by the Respondent. This Commission then finds that the Complainant failed to satisfy the requisite quantum of proof in an administrative case.

In *Primo vs. Mendoza, et. al.*, the Supreme Court defined the required burden of proof in administrative cases as follows,

“Substantial evidence is defined as such amount of relevant evidence which a reasonable mind might accept as adequate to support a conclusion. It is more than a mere scintilla of evidence. The standard of substantial evidence is satisfied when there is reasonable ground to believe, based on the evidence submitted, that the respondent is responsible for the misconduct complained of. It need not be overwhelming or preponderant, as is required in an ordinary civil case, or evidence beyond reasonable doubt, as is required in criminal cases, but the evidence must be enough for a reasonable mind to support a conclusion.”³

Pursuant to the above-cited reasons, the insufficiency of the information substantiating Complainant’s allegations warrants the dismissal of the instant complaint.

³G.R. Nos. 172532 172544-45, 20 November 2013

WHEREFORE, premises considered, this Commission resolves to **DISMISS** the instant complaint filed by MEC against Robocash Finance Corporation, on the ground that Complainant failed to provide sufficient information to substantiate the allegations in her complaint.

SO ORDERED.

Pasay City, Philippines;
02 July 2020.

Sgd.

JOHN HENRY D. NAGA
Deputy Privacy Commission

WE CONCUR:

Sgd.

RAYMUND ENRIQUEZ LIBORO
Privacy Commission

Sgd.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

MEC

Complainant

ROBOCASH FINANCE CORP.

DATA PROTECTION OFFICER
Robocash Finance Corporation

**ENFORCEMENT DIVISION
COMPLAINTS AND INVESTIGATION DIVISION GENERAL
RECORDS UNIT**

National Privacy Commission

The background of the entire page is a teal-tinted photograph. It shows two tall palm trees in the center, flanked by modern, angular buildings on either side. The sky is filled with white clouds. The overall aesthetic is clean and modern.

RESOLUTIONS

CL,
Complainant,

-versus-

NPC No. 19-030
(formerly CID Case No. 19-A-030)
For: Violation of the Data Privacy Act of 2012

CL, DDZ,
Respondent.

X-----X

DM,
Complainant,

-versus-

NPC No. 19-132
(formerly CID Case No. 19-B-132)
For: Violation of the Data Privacy Act of 2012

DDZ,
Respondent.

X-----X

Resolution

NAGA, P.C.;

For consideration of the Commission is the Motion for Reconsideration dated 11 September 2021 filed by CL and DM (Complainants) on the Decision dated 10 June 2021 which dismissed their Complaints against DDZ (Respondent) for lack of merit.

Facts

The Commission issued a Decision dated 10 June 2021, dismissing the Complaints filed by CL and DM, with the following dispositive portion:

WHEREFORE, all premises considered, this Commission resolves that the instant Complaints filed by CL and DM are hereby **DISMISSED** for lack of merit.

SO ORDERED.¹

Complainants filed a Motion to Suspend the Period of Filing of Pleadings dated 13 August 2021, seeking for the application of the Supreme Court Administrative Circular No. 56-2021 (SC Circular).²

On 02 September 2021, the Commission issued an Order denying the Motion to Suspend the Period of Filing of Pleadings. However, in the Order, the Commission granted Complainants a non-extendible period of five (5) days upon receipt of the Order to make the filing and service of necessary pleadings and motion.³

On 07 September 2021, Complainants filed a Manifestation that since the fifth day of the period it was given in the Order fell on 11 September 2021, a Saturday, they had until 13 September 2021 to submit their Motion for Reconsideration (Motion).⁴

On 13 September 2021, Complainants filed their Motion dated 11 September 2021.

In their Motion, Complainants stated that it is not clear how Respondent obtained a copy of their personal files and closed-circuit television (CCTV) footages of the MVP worksite.⁵ Complainants argued that Respondent readily proposed that he obtained it from SM and DMV through a legitimate request. However, no evidence was presented to show that such request was made. Further, the letter-request was omitted and no affidavit from SM and DMV was presented.⁶

Complainants then stated that no request appears in the records of the MVP office and that they were never informed that such request was processed by SM and DMV.⁷ Moreover, Complainants argued that they made the averment related to the database break-in by Respondent in their Complaints because they are unaware of

¹ Decision, 10 June 2021 at p. 10. NPC 19-030 and NPC 19-132.

² Id. at p. 2.

³ Order dated 02 September 2021.

⁴ Id at p. 3.

⁵ Motion for Reconsideration dated 11 September 2021. At. p. 3.

⁶ Id.

⁷ Id.

any purported request for copies of their passports made to the responsible officers of MVP.⁸

Complainants further submits that Respondent is not a public authority, did not act under compulsion by order of such public authority, and that the passports were not essential to the prosecution of any of Respondent's claims.⁹

Complainants, being aware of Respondent's allegation that the passports were obtained through a valid request from the previous officers of MVP, the said corporation through its authorized representative, AR instituted a Complaint dated 11 September 2020 against SM, DMV, and DDZ.¹⁰

Complainants stated that such Complaint was received and duly acknowledged by the Commission's Complaints and Investigation Division (CID).¹¹ However, despite the acknowledgement of receipt and promise to review the Complaint, it remains to be undocketed and has not been acted upon by the Commission.¹²

Complainants filed a Motion to Consolidate on 16 December 2020. Additionally, they stated that more than two (2) months have passed without any Resolution on the Motion, they filed a Motion to Resolve on the issue of consolidation dated 24 February 2021.¹³ However, according to Complainants, the Commission did not act on these two (2) pending Motions and that it seems that the pending Motions and verified Complaint filed by MVP were not considered when the Commission rendered the Decision dated 10 June 2021.¹⁴

Complainants emphasized that the consolidation of the cases are important since it would expedite the resolution of the issue. Complainants added "if the cases were consolidated, DMV and SM could have been summoned and shed light on the factual

8 Id.

9 Id.

10 Id. at p. 5.

11 Id.

12 Id.

13 Id.

14 Id.

circumstances claimed by Respondent DDZ.”¹⁵ Further, they stated that the proper resolution of this case will be incomplete, unfair, and unjust since SM and DMV are not allowed to be made part of the case and that the situation calls for a proper remand for investigation.¹⁶

On Respondent’s reliance on Section 13(f) of the Data Privacy Act (DPA) of 2012, Complainants argued that attaching the passports to Respondent’s Complaint-letter was not necessary since Complainants being Australian citizens without working visas is not relevant to the criminal and labor cases then existing.¹⁷ The nationality or citizenship is also neither an essential element of the crimes mentioned nor would constitute part of the labor case for dismissal. Complainants argued that the virtual nexus between Respondent and Complainants with regard to the contents of the passports does not exist and therefore fail the test provided by NPC Case No. 17-018.¹⁸

Moreover, according to Complainants it was Respondent, together with his cohorts, SM and DMV, who should be guilty of theft of Complainants’ sensitive personal information.¹⁹

Complainants also stated that the Office of the Prosecutor, Department of Labor and Employment (DOLE), Clark Development Corporation (CDC), and the Bureau of Immigration (BI) did not ask for the documents.²⁰

The exemption in processing sensitive personal data only applies to the Government entities as part of their function which cannot be said on the part of Respondent since he is not public office or functionary and thus, cannot claim such exemption as a privilege.²¹ Complainants cited Section 19 of the DPA which states that “the personal information shall be held in strict confidentiality and shall be used only for the declared purpose”, but since Complainants’ have not seen a copy of Respondent’s request, they do not know

¹⁵ Id. at p. 6.

¹⁶ Id.

¹⁷ Id at p. 7

¹⁸ Id.

¹⁹ Id. at p. 8.

²⁰ Id. at. p. 9

²¹ Id. at p. 10

for what purpose his request was made.²² Further, they argued that there is no transparency in the processing of their sensitive personal information.

Moreover, Complainants stated “the Personal Privacy Controller [sic] of the MVP is not even aware that a request was made by Respondent.”²³ According to Complainants, it was SM and DMV who processed the sensitive personal information, without informing the data subjects and without authority to do so. Complainants stated that DDZ, SM, and DMV connived to steal their sensitive personal information for a malicious purpose.²⁴

Complainants stated that there is also no legitimate purpose since Respondent did not provide the request made to MVP which shall state the purpose of processing. Further, there is also no proportionality since the information processed was already with the agencies concerned or within the grasp of government agencies, Respondent cannot borrow government’s rights and privileges.²⁵ According to Complainants, Respondent should provide the evidence of the valid request for processing the information. Respondent has the burden of proving, as a matter of defense, that he is within the exception in the statute creating the offense. Complainants stated that like all matters of defense, the burden of establishing such claim is on the party relying or invoking it.²⁶

They stated that there is no evidence to support Respondent’s supposed claim of a valid request existed. However, there is ample evidence that there were no requests appearing in the MVP records.²⁷

Based on the Data Protection Officer (DPO) report by Atty. EV, the internal investigation shows that no consent was obtained from the management for the release of Complainants’ documents. There are also no copies of the request claimed by Respondent in the files of MVP.²⁸ Complainants alleged that the intrusion to the data banks of

22 Id. at p. 11.

23 Id. at. p. 12.

24 Id. at p. 13

25 Id.

26 Id. at p.14.

27 Id. at p. 17.

28 Id. at p. 17-18.

MVP was accomplished in connivance with SM and DMV since they have access even without authority and without informing the data subjects of the processing.²⁹

Further, if a valid request exist, it is within the capacity of Respondent to produce a copy of such request.³⁰

Complainants prayed then that: (a) Decision dated 10 June 2021 be reconsidered and appropriate remedies and penalties be imposed against Respondent DDZ; and (b) Alternatively, that the cases be consolidated with the undocketed case filed by MVP as the issues are intimately related to each other. Should the Commission deem it fit and proper, to remand the case for proper determination with proper issuance of summons to DMV and SM so they can be held responsible for the violation of the DPA.³¹

On 17 September 2021, the Commission issued an Order, ordering Respondent DDZ, to file a Comment on the Motion for Reconsideration dated 11 September 2021 filed by Complainants and to submit the same within fifteen (15) days from receipt of the Order.³²

On 22 October 2021, Respondent filed a Motion to Admit Comment together with his Comment.³³

In his Comment, Respondent argued that Complainants' arguments in their Motion are trivial and inconsequential and do not affect the substantial and material discussions of the Commission.³⁴

According to Respondent, Complainants attached as Annex "A" in their Motion, a purported complaint which is totally unrelated to the case decided by the Commission and deserves no consideration to the resolution of the said Motion.³⁵

²⁹ Id. at p. 18.

³⁰ Id.

³¹ Id. at p. 20.

³² Order dated 17 September 2021.

³³ Motion to Admit Comment and Comment dated 22 October 2021.

³⁴ Id. at p. 1.

³⁵ Id.

Respondent also stated that the separate Complaints arose from the same set of facts, arguments, and evidence. However, Complainants opted to initiate a Complaint separately to harass and vex Respondent.³⁶ Further, Respondent stated “the undocketed Complaint attached as Annex “A”, also falls to the same malicious story. These only proved Respondent’s claim that the instant cases were filed to unjustly annoy Respondent.”³⁷

Respondent reiterated his allegations that the Complaints were being utilized by Complainants to have leverage over Respondent’s labor case. Since the Labor Arbiter ruled in favor of Respondent on the said labor case, Respondent stated that Complainants will hardly but uselessly pursue these cases, or any other cases against Respondent to get even.³⁸

In addition, Respondent stated that not only that the Complaints were vexatious, but also absurd. According to Respondent, first, Complainants themselves disclosed their passport information with the Commission when they filed their Complaints.³⁹ Second, following to their line of thinking, Complainants are guilty of the same charge of violation of the DPA considering that they disclosed sensitive personal information of Respondent, particularly his Alien Certificate of Registration as attachment to their Complaints.⁴⁰

On Complainants’ allegation that he broke into MVP’s database, Respondent stated that Complainants solely relied on surmises and conjectures which are wholly unsupported by legal and factual bases.⁴¹

Respondent argued that like any other cases, Complainants have the burden of proof to show that Respondent violated the DPA.⁴² He further stated that Complainants failed to provide substantial evidence that Respondent knowingly and unlawfully broke into MVP’s database. Complainants also did not show that there was an actual storage of scanned copies of passports. Moreover, the

36 Id. at p. 2

37 Id.

38 Id.

39 Id.

40 Id.

41 Id.

42 Id. at p. 3.

facilities of MVP are covered by CCTV cameras but Complainants did not attach video clip or screen capture to prove their claims.⁴³ Respondent stated that he fully subscribe to the findings of the Commission that he cannot be held liable for the violation of Section 29 of the DPA (Unauthorized Access or Intentional Breach).⁴⁴

Further, Respondent stated that he agrees to a certain extent on Complainants' allegations that passport contains personal and sensitive personal information.⁴⁵ However, he reiterated that such information is excluded from the coverage of the DPA pursuant to Section 4(e) of the DPA. Additionally, he stated that the processing of information contained in the passport is permitted under Section 12(e) and (f) of the DPA, and exempted under Section 13(e) of the DPA.⁴⁶

He also reiterated that the information of Complainants were necessary in order for the government agencies to perform their statutorily mandated functions.⁴⁷

Moreover, Respondent stated "Complainants argued that Respondent's processing of information were not exempted since it was not 'necessary' to protect his claim or interest. Complainants argued that the word 'necessary' connotes that the sensitive information that was processed should be needed to protect the claim or interest of the party using that information. However, the exemption that Respondent and the Honorable Commission pointed out is found under the phrase 'or when provided to government or public authority' of Section 13(f)."⁴⁸

He also stated that he only processed Complainants' information with the government agencies which were tasked to enforce laws and protect lawful rights and interests of natural or legal persons, the Philippine Government, and the Filipino citizens.⁴⁹

Respondent stated that his legitimate interest was to report the illegal acts of Complainants, and although he is not a Personal Information Controller (PIC), his processing is permitted as a "third

43 Id. at p. 4

44 Id. at p. 4 to 5.

45 Id. at p. 5.

46 Id.

47 Id. at p. 7.

48 Id.

49 Id.

party” pursuant to Section 13(f) of the DPA.⁵⁰ Further, Respondent stated that he processed the information in good faith pursuant to his moral obligation to promptly report on what he believes is an illegal act under Philippine Laws.⁵¹

Respondent prays that Complainants’ Motion for Reconsideration dated 11 September 2021 be denied for the lack of merit.⁵²

Issues

Whether the Motion for Reconsideration dated 11 September 2021 on the Decision dated 10 June 2021 filed by Complainants should be granted.

Discussion

The Commission partially grants the Motion for Reconsideration filed by Complainants.

The Commission finds that in order to properly resolve the case, it shall first solely focus on the procedural issues raised by Complainants. The Commission shall not delve on the substantive issues raised by both parties in their respective pleadings until such time that Complainant’s pending Motions have been properly resolved.

In its Motion, Complainants stated that MVP, through its authorized representative, AR, instituted a Complaint dated 11 September 2020 against SM, DMV, and DDZ which was received and duly acknowledged by the Commission’s CID. Complainants attached in their Motion as Annex “A”, the copy of the Complaint.⁵³ They also attached as Annex “B”, the copy of CID’s email stating that the Complaint has been received and will be reviewed shortly.⁵⁴

⁵⁰ Id. at p.7 to 8.

⁵¹ Id. at p. 8 to 9.

⁵² Id. at p. 9

⁵³ Motion for Reconsideration dated 11 September 2021. At p. 23.

⁵⁴ Id. at p. 52.

Also, a Motion to Consolidate was filed by Complainants on 16 December 2020 stating that their Complaints and the Complaint filed by MVP contains issues are intimately related to each other. Additionally, since the Commission has yet to issue a resolution on the Motion to Consolidate, Complainants filed a Motion to Resolve on the issue of consolidation dated 24 February 2021.

However, Complainants stated that the Commission did not act on these two (2) pending Motions and that the pending Motions and verified Complaint filed by MVP were not considered when the Decision dated 10 June 2021 was rendered.⁵⁵

In terms of procedural issues, the resolution of the Motion to Consolidate and Motion to Resolve is a material fact that needs to be considered by the Commission. Further, the Commission notes that addressing the pending Motions filed by Complainants is imperative in the holistic resolution of the case, given that the Complaints filed by CL and DM and the Complaints filed by MVP are alleged to have similar and interrelated issues that must be reviewed and resolved by the Commission.

Moreover, in this case, the Commission deems that the proper resolution of the pending Motions shall be addressed by the Commission. Thus, the Commission finds that the Motions filed by Complainants shall be remanded to the Complaints and Investigation Division (CID) of the Commission to resolve whether the Complaints filed may be consolidated, as allowed by Section 7 of the NPC Circular No. 2021-01 (2021 NPC Rules of Procedure), viz:

SECTION 7. Consolidation of cases. – Except when consolidation would result in delay or injustice, the NPC may, upon motion or in its discretion, consolidate two (2) or more complaints involving common questions of law or fact and/or same parties.⁵⁶

Further, the Commission shall await for the Resolution of the CID on the pending Motions filed by Complainants before fully

⁵⁵Id.

⁵⁶ Section 7 of the NPC Circular No. 2021-01

deciding on Complainants' Motion including its substantive issues. Hence, the Commission partially grants Complainants' Motion for Reconsideration.

As to the Motion to Admit Comment and the attached Comment dated 22 October 2021 filed by Respondent, the Commission notes that Respondent received the Commission's Order dated 17 September 2021 on 30 September 2021. Therefore, Respondent has fifteen (15) days from receipt of the Order or until 15 October 2021 to submit his Comment. However, Respondent only submitted his Comment on 22 October 2021 which is beyond the allowed period. Hence, it was filed out of time.

Nonetheless, in consideration of substantial justice, the Commission resolves to admit Respondent's Motion to Admit Comment and Comment despite being filed out time.

WHEREFORE, premises considered, this Commission resolves to PARTIALLY GRANT the Motion for Reconsideration dated 11 September 2021 filed by Complainants CL and DM.

SO ORDERED.

City of Pasay, Philippines.
11 November 2021.

SGD.

JOHN HENRY D. NAGA

Deputy Privacy Commissioner

WE CONCUR:

SGD.

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

SGD.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

Copy furnished:

CL

Complainant

DM

Complainant

MJRVLO

Counsel for Complainants

DDZ

Respondent

PMB

Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

IN RE: MEDICARD PHILIPPINES, INC.

NPC 18-205

X-----X

Resolution

NAGA, P.C.;

This Resolution refers to the compliance of MediCard Philippines, Inc. (MediCard) to the Resolution dated 10 December 2021.

Facts

On 10 December 2021, the Commission issued a Resolution¹ to MediCard, to wit:

WHEREFORE, premises considered, the request of MediCard Philippines, Inc. for exemption of notifying the remaining one thousand two hundred forty-one (1,241) affected data subjects is hereby DENIED.

Further, MediCard Philippines, Inc. is ORDERED to notify the remaining affected data subjects that are not yet notified through e-mail based on the available e-mail addresses in MediCard's database and at the same time post the notice couched in general terms on its official website for faster dissemination of information.

Finally, MediCard Philippines, Inc. shall submit to the Commission within fifteen (15) days from receipt of this Resolution a compliance report, which shall include details of notification to the data subjects (i.e., proof of the email notifications, postings, and their respective links).

SO ORDERED.²

¹ In re: Mediacard Philippines Inc., NPC BN 18-205, Resolution dated 10 December 2022, at p. 11.

² Id.

On 09 March 2022, in compliance with the Resolution of the Commission, MediCard posted on its website³ the notice to affected data subjects, to wit:

Unauthorized Disclosure

09 Mar 2022

We at MediCard Philippines, Inc. protect your privacy seriously and recognize our duty to take care of our customers whose data we hold. As such, we take every precaution to ensure that your personal information is protected at all times while maintaining our transparency to our customers

Last October 2018, we reported a data breach to the National Privacy Commission (NPC) involving a billing statement that was unintentionally delivered to the wrong company. The notification was made pursuant to the mandatory data breach notification procedure of the NPC. Unfortunately, data of some AIG Shared Services employees, limited to: employee number, MediCard ID number, name, and age were exposed in this data breach.

To validate this, if you have been an active employee of AIG Shared Services – Business Processing Inc. in October 2018, please access the following link: <https://webportal.medicardphils.com/DataBreachNotice> and enter your Member ID and date of birth.

We sincerely apologize that this has happened, and we want to assure you, as our valued member, that we have taken steps to prevent a recurrence of the incident. Also, the company has been in close coordination with the National Privacy Commission (NPC) to address this.

Should you have clarifications, feel free to reach us by mail at privacy@medicardphils.com.⁴

On 15 March 2022, MediCard submitted screenshots of its webpage posting and its e-mail notifications.⁵

³ See <https://www.medicardphils.com/news-promos-announcements/article/35>

⁴ See Unauthorized Disclosure, available at <https://www.medicardphils.com/news-promos-announcements/article/35>, last accessed on 22 June 2022

⁵ Compliance Report of MediCard Philippines, at pp. 1-2.

In relation to the e-mail notifications, MediCard submitted its Compliance dated 15 March 2022 and 25 May 2022. Along with the 25 May 2022 Compliance are the sworn affidavits of FC and JM, the persons responsible for notifying the affected data subjects through e-mail.

In Mr. FC's affidavit, he attested that on 09 March 2022, the e-mail notification was sent via the email address, privacy@medicard.phils.com, with the subject: MANDATORY PERSONAL DATA BREACH NOTIFICATION to a total of three hundred (300) data subjects following the required e-mail settings: (a) request a read receipt and (b) request a delivery receipt.⁶ He was able to send the e-mail notification to the three hundred (300) e-mail addresses and the delivery receipts provided were "Delivery to these recipients or groups is complete, but no delivery notification was sent by the destination server."⁷ Among the three hundred (300) email notifications, three (3) were not delivered due to "E-mail wasn't found at gmail.com", "E-mail address you entered could not be found", and "Your message could not be delivered."⁸ Despite repeated attempts to contact the recipients e-mail system, it did not respond.⁹

While in Ms. JM's affidavit, she attested that on 09 March 2022, she sent an e-mail notification with subject: Mandatory Personal Data Breach Notification to a total of three hundred and one (301) data subjects via the email address, privacy@medicardphils.com.¹⁰ She was able to send the e-mail notifications to the three hundred and one (301) e-mail addresses.¹¹ Some of the delivery receipts stated, "Delivery to these recipients or groups is complete, but no delivery notification was sent by the destination server," while only five (5) have "read receipts".¹² Among the three hundred one (301) e-mail notifications, six (6) were identified as "Undeliverable" and with a "Failure Notice" due to "E-mail wasn't found at gmail.com" and

6 Affidavit of FC, p. 2

7 Id.

8 Id.

9 Id.

10 Affidavit of JM, p. 2.

11 Id.

12 Id.

“Delivery has failed to these recipients or groups”.¹³

Mediacard was able to successfully deliver five hundred ninety-two (592) e-mail notifications out of the total six hundred and one (601) e-mail addresses available to it. Nine (9) e-mail addresses available were not delivered for reasons: “E-mail wasn’t found at gmail.com”, “E-mail address you entered could not be found”, “Your message could not be delivered”, and “Delivery has failed to these recipients or groups”.

Discussion

The Commission finds MediCard compliant with the Resolution dated 10 December 2021.

Mediacard was able to notify the remaining one thousand two hundred forty one (1,241) affected data subjects by sending the notification to the available e-mail addresses of the data subjects¹⁴ and by posting the notice on its website.¹⁵

Section 18 (C) of NPC Circular 16-03, otherwise known as Personal Data Breach Management, provides:

C. Content of Notification. The notification shall include, but not be limited to:

1. nature of the breach;
2. personal data possibly involved;
3. measures taken to address the breach;
4. measures taken to reduce the harm or negative consequences of the breach;
5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and

¹³ Id.

¹⁴ Compliance Report dated 15 March 2022 and Compliance Report dated 25 May 2022

¹⁵ Unauthorized Disclosure, available at <https://www.mediaphil.com/news-promos-announcements/article/35>, last accessed on 22 June 2022

6. any assistance to be provided to the affected data subjects. Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.¹⁶

Medicard's website notification¹⁷ contained the nature of the breach, the personal data possibly involved, measures taken to address the breach and reduce the harm or negative consequences of the breach, such as prevention of recurrence of the incident, and contact details of the personal information controller. Thus, the website notification of Medicard sufficiently complied with Section 18(C) of NPC Circular 16-03.

With respect to the e-mail notifications sent to the available e-mail addresses in its records, Medicard was able to submit its Compliance dated 15 March 2022¹⁸ and 25 May 2022.¹⁹

According to the Compliance Report dated 25 May 2022, the affidavits of Mr. FC and Ms. JM stated that nine (9) out of the six hundred one (601) e-mail address available to MediCard were not successfully delivered for reasons: "E-mail wasn't found at gmail.com", "E-mail address you entered could not be found", "Your message could not be delivered", and "Delivery has failed to these recipients or groups."²⁰

The failure to send e-mail notifications to the remaining nine (9) data subjects, despite MediCard's repeated attempts, rendered the individual e-mail notification impossible.²¹

Even though there is an impossibility in sending e-mail notifications to these data subjects, the Commission provides for alternative

16 National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, ¶ 18 (C) (15 December 2016) (NPC Circular 16-03).

17 Unauthorized Disclosure, available at <https://www.medicardphils.com/news-promos-announcements/article/35>, last accessed on 22 June 2022

18 Compliance Report dated 15 March 2022

19 Compliance Report dated 25 May 2022

20 Affidavit of FC; Affidavit of JM

21 Final Enforcement Assessment Report, 23 June 2022, p. 6

means of notifying them through NPC Circular No. 16-03 (Personal Data Breach Management).²²

Particularly, Section 18(D) of NPC Circular No. 16-03 allows for alternative means of notification in which data subjects would be informed about the personal data breach in an equally effective manner if individual notification is impossible or would require disproportionate effort, to wit:

SECTION 18. Notification of Data Subjects. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:

xxx

D. Form. Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: Provided, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.²³ (Emphasis supplied)

Based on the records, the nine (9) remaining data subjects still could not be reached despite repeated attempts, and the e-mails could not be delivered for various reasons.²⁴ Given these circumstances, the Commission finds that there is an impossibility in individually notifying these data subjects. Consequently, alternative notification is allowed for these data subjects.

²² National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18 (D) (15 December 2016) (NPC Circular 16-03).

²³ National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18 (15 December 2016) (NPC Circular 16-03).

²⁴ See Affidavit of FC and Affidavit of JM.

The Commission notes that MediCard has already posted the notification on its official website, which was in compliance with the Resolution dated 10 December 2021. Thus, the Commission deems the alternative notification sufficient with regard to the nine (9) remaining data subjects who could not receive email notifications of the data breach.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC 18-205 “In re: MediCard Philippines, Inc.” is hereby considered CLOSED.

SO ORDERED.

Pasay City, Philippines;
14 July 2022.

Sgd.

JOHN HENRY D. NAGA

Privacy Commissioner

WE CONCUR:

Sgd.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

Sgd.

DUG CHRISTOPHER B. MAH

Deputy Privacy Commissioner

COPY FURNISHED:

RTM

Data Protection Officer

4th The World Center Building

330 Sen. Gil Puyat Ave., Makati City

COMPLAINTS AND INVESTIGATION DIVISION

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

JO,
Complainant,

-versus-

NPC No. 19-278

For: Violation of the Data Privacy Act of 2012

MSM, Inc.
Respondent.

X-----X

RESOLUTION

NAGA, P.C.;

Before the Commission is a Motion for Reconsideration dated 15 May 2022 filed by JO on the Commission's Decision dated 31 March 2022.

Facts

JO, through a Complaints-Assisted Form dated 27 March 2019, filed a case against the Respondent, MSM, Inc (MSMI).¹ On 31 March 2022, the Commission issued a Decision dismissing the complaint for lack of merit.²

The Decision was served via email to both parties on 29 April 2022.³ Subsequently, JO submitted an unsigned Motion for Reconsideration on 16 May 2022 via email.⁴ In the email, JO stated that, "I will send physical copy personally (signed),"⁵ and attached his unsigned Motion.⁶ Based on the records, JO filed a signed physical copy of his Motion on 17 May 2022.⁷

¹ Complaints-Assisted Form dated 27 March 2019 of JO.

² JO vs MSM, Inc., NPC 19-278, Decision dated 31 March 2022.

³ See Electronic mail dated 29 April 2022 to JO and MSM, Inc.; Electronic Mail Delivery Receipts.

⁴ Motion for Reconsideration dated 15 May 2022 (unsigned) of JO.

⁵ Electronic Mail dated 16 May 2022 from JO.

⁶ Id.

⁷ Motion for Reconsideration dated 15 May 2022 (signed) with stamp receipt of JO.

In his Motion, JO claims that there was no “cogent reason” for the dismissal of his complaint.⁸ He states that “the complaint itself has shown an exceptionally good cause that indeed respondents unquestionably, deliberately and seriously violated the right(s) of the complainant and complaint itself involves a serious violation or wanton breach of the Data Privacy Act.”⁹

He claims that there was bias or partiality in the dismissal of his complaint. To support this claim, JO cites an alleged incident in the course of the preliminary investigation:

The Investigating Officer have already decided the favorable resolution of the complaint to the respondent(s) since, quoted thereat the following remarks, “MADEDEHADO KA DITO (REFERRING TO NPC) KUNG WALA KANG ABOGADO” (sic)¹⁰

JO also argues that MSMI has committed data privacy violations, especially by MSMI’s alleged admission that it was using “the account name and code of complainant who has effectively resigned since 31 December 2018.”¹¹ He further contends that MSMI should be penalized under Section 33 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA).¹² Lastly, JO claims that MSMI could have performed its tasks manually, but opted to breach his personal data.¹³

In response, MSMI filed an Opposition (to the Motion for Reconsideration dated 15 May 2022) dated 01 June 2022.¹⁴ MSMI argues that “[JO’s] Motion should be outrightly denied for being pro forma inasmuch as it fails to point out specifically the findings or conclusions of the Commission in its Decision which are not supported by the evidence or which are contrary to law...”,¹⁵ and thereafter citing Rule 37 of the 2019 Rules of Civil Procedure.¹⁶

8 Id., at pp. 1-2.

9 Id., at p. 2.

10 Id.

11 Motion for Reconsideration dated 15 May 2022 of JO, at p. 2.

12 Id.

13 Id.

14 Opposition (to the Motion for Reconsideration dated 15 May 2022) dated 01 June 2022 of MSM, Inc.

15 Id., at ¶ 2.

16 Id.

MSMI also counters that JO “fails to provide any iota of evidence to show that this Honorable Commission exhibited any bias or partiality in its Decision other than to reference the period within which the said Decision was issued and to quote the Investigating Officer.”¹⁷ According to MSMI, the alleged statement, if true, also does not show bias but “only reflects the Investigating Officer’s prudent act of advising Complainant of the possibility of engaging counsel.”¹⁸ Even if this showed bias or partiality, MSMI claims that it is not one of the grounds for a motion for reconsideration.¹⁹

MSMI cites the Decision in claiming that there was no privacy violation, in that JO’s email and Philippine Overseas Employment Administration (POEA) code are company-owned assets, and not owned by JO.²⁰ Thus, MSMI prays that the Commission deny JO’s Motion.

Issue

Whether the Motion for Reconsideration merits the reversal of the Decision dated 31 March 2022.

Discussion

The Commission denies JO’s Motion for Reconsideration.

I. The Decision has already attained finality. JO’s period to file a motion for reconsideration has already lapsed.

Rule VII, Section 30 of the NPC Circular 2016-04 or the Rules of Procedure (2016 NPC Rules of Procedure) states:

¹⁷ Id., ¶ 4.

¹⁸ Opposition (to the Motion for Reconsideration dated 15 May 2022) dated 01 June 2022 of Multinational Ship Management, Inc., ¶ 4(b).

¹⁹ Id., ¶ 4(c).

²⁰ Id., ¶ 7. See JO vs MSM, Inc., NPC 19-278, Decision dated 31 March 2022, at p. 12.

SECTION 30. Appeal. – The decision of the National Privacy Commission shall become final and executory fifteen (15) days after the receipt of a copy thereof by the party adversely affected. One motion for reconsideration may be filed, which shall suspend the running of the said period. Any appeal from the Decision shall be to the proper courts, in accordance with law and rules.²¹ (Emphasis supplied)

Likewise, Rule VIII, Section 4 of NPC Circular No. 2021-01, otherwise known as the 2021 NPC Rules of Procedure (2021 NPC Rules) states:

SECTION 4. Appeal. – The decision of the Commission shall become final and executory fifteen (15) calendar days after receipt of a copy by both parties. One motion for reconsideration may be filed, which shall suspend the running of the said period. Any appeal from the Decision shall be to the proper courts, in accordance with law and rules.²²

The Decision dismissing the case was served to the parties via email on 29 April 2022. JO, in his Motion, claims that he received the Decision on 10 May 2022.²³ Based on the records, this was the day he received the physical copy of the Decision after it was sent through private courier.²⁴

Nevertheless, it should be noted that electronic service is allowed under Rule III, Section 6 of the NPC Rules.²⁵ Also, there was no notification or other proof that there were problems with the electronic service.²⁶ JO even sent an email attaching his unsigned Motion by replying to the Commission's email which electronically served him the Decision.²⁷

Thus, the Commission finds that the electronic service of its Decision on 29 April 2022 was valid. Consequently, the Decision already became final on 14 May 2022, which was the fifteenth day from receipt of the Decision, since there was no appeal filed within the fifteen (15)-day period.

²¹ National Privacy Commission, Rules of Procedure of the National Privacy Commission, NPC Circular No. 16-04, Rule VII, § 30 (15 December 2016) (2016 NPC Rules of Procedure)

²² National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission, NPC Circular No. 2021-01, Rule VIII, § 4 (28 January 2021) (2021 NPC Rules of Procedure).

²³ Motion for Reconsideration dated 15 May 2022 of JO, at p. 1.

²⁴ As per LBC tracking number.

²⁵ 2021 NPC Rules of Procedure, Rule III, § 6.

²⁶ See Electronic mail delivery receipts.

²⁷ Electronic mail dated 16 May 2022 of JO.

JO electronically mailed his unsigned Motion on 16 May 2022. However, under Rule 7, Section 3 of the 2019 Rules of Civil Procedure (which finds suppletory application in this case),²⁸ “[e]very pleading and other written submissions to the court must be signed by the party or counsel representing him or her.”²⁹ JO, as the party filing the Motion, did not follow this clear obligation. It was only on 17 May 2022 when the Commission received a physical and signed copy of his Motion. Moreover, it bears emphasis that regardless whether JO filed his Motion on 16 May 2022 or 17 May 2022, the Decision had already attained finality.

Even if the Commission were to consider the unsigned Motion as duly filed, JO’s period to file a motion for reconsideration had already lapsed since the Decision was already final. On this ground alone, the Commission has sufficient cause to deny JO’s Motion.

II. On the merits, JO did not provide any substantial or adequate ground to reverse the Decision.

Setting aside the procedural infirmity, the Commission still finds that the Decision must be upheld. JO has not shown any substantial or adequate ground that would merit the reversal of the Decision.

JO does not explicitly state that the Commission is biased. His Motion does not even cite any particular statement from the Decision that would be indicative of partiality. However, he claims that during the preliminary investigation proceedings, the Investigating Officer “already decided the favorable resolution of the complaint to the respondent(s)”³⁰ due to the alleged statement “MADEDEHADO KA DITO (REFERRING TO NPC) KUNG WALA KANG ABOGADO.”³¹

²⁸ See 2021 NPC Rules of Procedure, Rule XII, § 8.

²⁹ 2019 Rules of Civil Procedure, Rule VII, § 3. (Emphasis supplied)

³⁰ Motion for Reconsideration dated 15 May 2022 of JO, at p. 2.

³¹ Id.

The Commission view allegations of bias seriously given that the National Privacy Commission is an independent body mandated to administer and implement the DPA.³² Taking into consideration its role, the Commission finds that JO has not proven that the Decision is tainted with bias against him.

In fact, in resolving JO's complaint, the Commission even exercised its authority to rule on the merits, rather than dismissing the complaint outright for non-exhaustion of remedies based on Section 4(a) of NPC Circular 16-04. To quote the Decision:

I. The Commission exercises its authority to resolve the case on the merits.

MSMI contends that the case should be dismissed since JO did not prove that he complied with Section 4(a) of NPC Circular No. 16-04, also known as the 2016 NPC Rules of Procedure.

In response, JO claims that after resigning, he immediately informed the company to refrain from accessing his personal information.

XXX

Based on the record, JO has not concretely provided evidence that it has complied with Section 4(a) of NPC Circular No. 16-04, since there is no proof that he informed MSMI, in writing, about the alleged privacy violation. Other than his allegations stated in his various pleadings before the Commission, JO did not attach any letter or other written correspondence to MSMI relating to the alleged privacy violation. Thus, he did not provide substantial evidence that will lead the Commission to conclude that he complied with Section 4(a) of NPC Circular No. 16-04.

Nevertheless, the Commission exercises its authority to waive the requirement of exhaustion of administrative remedies, based on the last paragraph of Section 4 of the 2016 Rules of Procedure.

JO's allegations, if substantially proven, may lead the Commission to conclude that there was a serious violation of the DPA. The allegations also show that there may be serious risk of harm to JO, given that the

³² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes, [Data Privacy Act of 2012], Republic Act No. 10173, Chapter II, § 7 (2012).

emails he provided allegedly show acts which he did not do, but may be liable for.

Thus, the Commission finds it appropriate to exercise its authority to resolve the case on the merits.³³ (Emphases supplied, citations omitted.)

The Commission could have just resolved to dismiss outright JO's complaint simply because he failed to prove that he informed MSMI in writing about the alleged privacy violation in order for it to appropriately act on the matter.³⁴ Instead, it approached the case from the lens of substantial justice by assessing JO's complaints based on the merits of his case. These actions are inconsistent with claims of bias or partiality against JO.

Further, regardless of the propriety of the Investigating Officer's alleged statement, the Decision was made only after the Commission scrutinized each party's submissions, evidence, and the law. The Commission ultimately decides on the matter, independent of the recommendations of the investigating officer, since "[t]he Commission shall review the evidence presented, including the Fact-Finding Report and supporting documents."³⁵ Though his complaint was dismissed, this in itself does not automatically prove that there was bias.

JO also repeats his claim that MSMI committed privacy violations when it "[used] the account name and code of complainant who has effectively resigned since 31 December 2018... There was a categorical admittance that the e-mail was provided for by the company (respondents), hence, bolster the fact that it is still being wantonly utilized by the company even after the complainant (data subject) effectively resigned since December 31, 2018 by another person. (sic)".³⁶ He also claims that MSMI should be penalized for Section 33 of the DPA to act as deterrence for those similarly inclined to violate the law or commit data breaches.³⁷

33 JO v. MSM, Inc., NPC 19-278, Decision dated 31 March 2022, at pp. 9-11.

34 See National Privacy Commission, Rules of Procedure, NPC Circular No. 16-04, § 4(a) (15 December 2016).

35 2021 NPC Rules of Procedure, Rule VIII, § 1.

36 Motion for Reconsideration dated 15 May 2022 of JO, at p. 2.

37 *Id.*

The Commission has already extensively discussed JO's contentions in its Decision. Further, the Commission finds that there are no new material facts or information presented by JO in his Motion that would warrant the reversal of the Commission's Decision.

As explained in the Decision, the POEA code is a company asset and cannot be considered as part of JO's personal information. While JO's company-issued email indicates his name, its use after his resignation does not automatically equate to a violation of the DPA. MSMI had a legitimate interest to continue using the POEA Account to access the Sea-based e-Contracts System (SBECS). MSMI's interest stems from POEA Memorandum Circular No. 06, series of 2018, which established the mandate for licensed manning agencies, like MSMI, to use POEA's web-based facility for its business processes with the agency.³⁸

MSMI also proved that it timely informed POEA about JO's resignation, and that it had to rely on POEA in order for MSMI to gain access to SBECS.³⁹

Lastly, the Commission finds that JO failed to justify why MSMI should be penalized under Section 33 of the DPA "[a]s a deterrent to others who are similarly inclined to commit such serious Data Privacy Violations or Personal Data Breach (sic)."⁴⁰

Section 33 of the DPA provides:

SEC. 33. Combination or Series of Acts. – Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).⁴¹

38 Philippine Overseas Employment Administration, Memorandum Circular No. 06, series of 2018, New Procedure for Online Registration of Seafarers and Seabased e-Contracts System (SBECS).

39 JO vs MSM, Inc., NPC 19-278, Decision dated 31 March 2022, at p. 14; see Motion to Dismiss dated 02 July 2019 of Multinational Ship Management, Inc., Annex "F".

40 Motion for Reconsideration dated 15 May 2022 of JO at p. 2.

41 Data Privacy Act of 2012, Chapter VIII, § 33.

JO has not proven that MSMI is liable for violating any of Sections 25 to 32 of the DPA, much more be penalized for a combination or series of acts meriting the application of Section 33 of the law.

Indeed, after reviewing the records and considerably weighing the evidence and arguments of both parties, the Commission finds no reason to reverse its Decision.

WHEREFORE, premises considered, the Motion for Reconsideration is DENIED. The Decision dated 31 March 2022 is hereby AFFIRMED.

SO ORDERED.

City of Pasay, Philippines.
16 June 2022.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
DUG CHRISTOPHER B. MAH
Deputy Privacy Commissioner

(Inhibited)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

JO
Complainant

MSM, INC.
Respondent

ATTY. FT
Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

**IN RE: FCASH GLOBAL LENDING,
INC., OPERATING FASTCASH
ONLINE LENDING
APPLICATION.**

NPC 19-909

For: Violation of the Data Privacy Act

X-----X

RESOLUTION

NAGA, P.C.;

Before us is a Motion for Reconsideration dated 28 February 2022 (Motion) by Respondents FCash Global Lending Inc., KDM, TH, JPS, JCT, and ZS (Respondents) assailing the Decision dated 23 February 2021 (Decision), copy of which was received through counsel on 17 February 2022. The challenged Decision disposed as follows:

WHEREFORE, all the above premises considered, this Commission hereby:

1. FINDS Respondent FCash Global Lending Inc. and its Board of Directors to have violated Section 25, 28, and Section 31 of the Data Privacy Act of 2012; and
2. FORWARDS this Decision and a copy of the pertinent case records to the Secretary of Justice, recommending the prosecution of the Respondents for the crimes of Unauthorized Processing of Personal Information and Sensitive Personal Information under Section 25 of the DPA, Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes under Section 28 of the DPA, and Malicious Disclosure under Section 31 of the DPA. The maximum penalty for violations of the abovementioned provisions is recommended to be imposed following Section 35 of the DPA.^t

Respondents' Motion reiterated the grounds they relied upon in

¹ Decision dated 23 February 2021

their Motion to Dismiss, to wit:

1. The Decision was issued not in compliance with the National Privacy Commission (NPC) Rules of Procedure, hence, with grave abuse of discretion amounting to a lack or excess of jurisdiction;
2. The Decision ignored the rule on exhaustion of remedies under Section 4, Rule II of the NPC Rules;
3. The Decision ignored the rule on *litis pendentia*, there being pending cases involving Respondent FCash filed by specific individual complainants who appear to be the same parties in the case;
4. The Decision violates and renders nugatory the provisions of the DPA on amicable settlement and alternative modes of dispute resolution which are expressly promoted by law;
5. The Decision arbitrarily, unfairly, and erroneously impleaded the corporate officers of Respondent FCash despite the lack of evidence, let alone allegations, that any of them participated in the alleged acts nor committed any gross negligence.²

Thus, Respondents pray for the reconsideration and the setting aside of the Decision dated 23 February 2021, which in effect dismisses the case against FCash.

The Commission now resolves the Motion.

The Commission has, time and time again, adequately ruled on this matter. The Commission already addressed these issues in its Resolution dated 02 October 2019 for the Motion to Dismiss dated 16 September 2019 and the Resolution dated 23 January 2020 for the Motion for Reconsideration dated 10 December 2019.

Furthermore, in relation to the Petition for Certiorari under Rule 65 of the Rules of Court filed by Respondents with the Honorable Court of Appeals in reference to its denied Motion for Reconsideration dated 23 January 2020, the Commission argued that “[a]t the outset, it bears to point that the resort to certiorari is not the proper remedy to assail the denial [of Respondent’s] motion to dismiss.”³ The

² Motion to Dismiss dated 16 September 2019

Commission reminded that it is settled in jurisprudence that the writ of certiorari is “available only where the tribunal, board or officer exercising judicial functions has acted without or in excess of their jurisdiction, or with grave abuse of discretion, and there is no appeal, or any plain, speedy and adequate remedy in the ordinary course of law. The special civil action should not be allowed as substitute for any ordinary appeal or where there are other remedies available.”⁴ Nevertheless, the Commission shall take this final opportunity to clarify matters with Respondents.

- I. The assailed Decision was issued in compliance with the NPC Rules of Procedure

Respondents argue that the proceeding was not conducted in compliance with NPC Circular 16-04 or the NPC Rules of Procedure (Rules) as there was no complaint filed but instead a Fact-Finding Report, which Respondents argued does not satisfy the requirement to initiate a sua sponte investigation. Such matter has already been resolved by the Commission in its 02 October 2019 Resolution.

To reiterate, Section 23 of Rule IV of the Rules provides for the power of the Commission to investigate on its own initiative the circumstances surrounding a possible serious privacy violation or personal data breach, taking into account the risks of harm to a data subject. Consequently, the investigation shall be made in accordance with Rule III of the same Rules following the principle of uniform procedure sufficiently complied with in this case.⁵

The Fact-Finding Report dated 29 August 2019⁶ (FFR) that was served to Respondents contains a narration of the material facts and the supporting documentary evidence which showed, among other things, the violations allegedly committed by Respondent FCash in operating its online lending application.⁷ The same FFR was submitted to the Commission for its perusal to determine whether violations of the Data Privacy Act of 2012 (DPA) were committed.

3 FCash Global Lending Inc., rep by KDM vs National Privacy Commission, Comment of Respondent National Privacy Commission dated 02 August 2021

4 Id.

5 Resolution dated 02 October 2019.

6 In re: FCash Global Lending Inc Fact-Finding Report dated 29 August 2019

7 Resolution dated 02 October 2019

Considering that the FFR contains all the findings of the investigating division of the NPC, such document is the complaint initiating the administrative proceedings in cases of sua sponte investigation. As sua sponte means “of one’s own accord”, the NPC, through the CID, has initiated, on its own, a complaint against Respondent by filing the FFR.

Further, in accordance with the Rules, Respondents, then, were given an opportunity to submit an Answer, as prescribed by Rule IV of the Rules wherein the Responsive Comment or Answer is immediately required from Respondents after it receives the Fact-Finding Report, to wit:

SECTION 24. Uniform procedure. – The investigation shall be in accordance with Rule III of these Rules, provided that the respondent shall be provided a copy of the fact-finding report and given an opportunity to submit an answer. In cases where the respondent or respondents fail without justification to submit an answer or appear before the National Privacy Commission when so ordered, the Commission shall render its decision on the basis of available information.⁸

As discussed by this Commission in its NPC 19-910 Resolution, “the procedure for a sua sponte investigation does not include a Discovery Conference because all the information and evidence in the hands of the Commission are already set out in and attached to the Fact-Finding report when it is provided to respondent.”⁹

It was emphasized by the Commission in NPC 19-910 Resolution that:

[W]hile Section 24 of Rule IV of the Rules provides that the investigation be in accordance with Rule III, it includes a provision: ‘that the respondent shall be provided with a copy of the Fact-Finding Report and given an opportunity to submit an answer.’ Rule IV does not state that the procedure should be exactly identical to the one described under Rule III. As used in Section 24 of Rule IV, ‘in accordance with Rule III’ simply means as far as practicable taking into consideration and giving effect to the difference between the two (2) procedures.¹⁰

Further, to recall, in the Resolution dated 02 October 2019:

⁸ Section 24, Rule IV of NPC Circular 16-04

⁹ NPC 19-910, Resolution dated 11 March 2021

¹⁰ Id

[T]he provision on the Uniform Procedure under the Rules should be read in light of the unique situation arising from the sua sponte nature of the present investigation. Under the NPC Rules, discovery is a procedure employed by parties to avail of, to compel the production of, or to preserve the integrity of electronically stored information. This procedure need not be resorted to by the Commission, however, in its exercise of its power of original inquiry. This is all the more true in this case considering that there are no private parties that can be called to confer for discovery. It must be emphasized that this case was initiated by a team of investigators in the Commission in response to serious allegations of data privacy violations allegedly committed upon a large number of data subjects.¹¹

Respondents claimed that the FFR already contained conclusions and recommendations for the prosecution of all the respondents for alleged violation of the provisions of the DPA.¹² To recall, it has been pointed out by this Commission that “no judgement of any kind has been made on this case for or against Respondents.”¹³ As previously discussed, the FFR is treated as the complaint in cases that are initiated through a sua sponte proceeding. The FFR is not the view of the Commission En Banc but rather a brief narration of the material facts and the supporting evidence which shows among other things, the cause of action of the complainant against the respondent.

Further, as the FFR is the complaint in cases of sua sponte investigations, Respondents were given the opportunity to be heard by ordering them to file their Answer or Comment to the submitted FFR. However, despite these opportunities given by the Commission to Respondents, the orders were left unanswered and ignored. Instead, Respondents questioned the authority of the Commission to determine this case.

Given this, the investigation and procedure of recommending a possible violation of the DPA has all been done in accordance with the powers vested in the Commission to institute sua sponte cases provided by the DPA and the Rules. Respondents should note that the response of the Commission upon receiving the FFR was an Order to File an Answer and not a decision.

The fact that there exist hundreds of pending cases before the Commission against Respondents is no bar to the filing of the case

¹¹ Resolution dated 02 October 2019

¹² R.A. 10173

¹³ Resolution dated 02 October 2019

on hand but instead highlights the seriousness of the data privacy violations and risks of harm to data subjects. The Commission notes that the other pending cases against the Respondents and the case at hand involves different parties with different causes of action and prayers for relief.

As held by the Supreme Court in *Yap vs. Court of Appeals*¹⁴

Litis pendentia as a ground for the dismissal of a civil action refers to that situation wherein another action is pending between the same parties for the same cause of action, such that the second action becomes unnecessary and vexatious. The underlying principle of *litis pendentia* is the theory that a party is not allowed to vex another more than once regarding the same subject matter and for the same cause of action. This theory is founded on the public policy that the same subject matter should not be the subject of controversy in courts more than once, in order that possible conflicting judgments may be avoided for the sake of the stability of the rights and status of persons.

The requisites of *litis pendentia* are: (a) the identity of parties, or at least such as representing the same interests in both actions; (b) the identity of rights asserted and relief prayed for, the relief being founded on the same facts; and (c) the identity of the two cases such that judgment in one, regardless of which party is successful, would amount to *res judicata* in the other.¹⁵

In the present case, none of the foregoing requisites were met. As it was repeatedly emphasized, the pending cases against the Respondents and the case at hand involves different parties with different causes of action and prayers for relief.

As argued by the Commission in its Comment dated 02 August 2021 for the case C.A.– G.R. SP No. 168046:

The cause of the individual complaints is to enforce the individuals rights vested by the DPA. Meanwhile, a complaint which arose from a *sua sponte* investigation is hinged on the [Commission's] responsibility, as representative of the State, 'to protect the fundamental human rights of privacy, of communication while ensuring free flow of information to promote innovation and growth.' The individual complaints were only cited in the Fact-Finding Report to demonstrate the seriousness of the

¹⁴ G.R. No. 186730, June 13, 2012

¹⁵ *Id.*

possible data privacy violation.

The [FFR] itself shows that the Task Force conducted an independent investigation against [FCash]. It reviewed [FCash's] Privacy Policy, the user reviews alleging serious privacy violations, and the mobile application itself. The investigators evaluated how [FCash's] application operates and the extent to which the privacy of its users is protected by examining the Android Manifest, including 'permissions' required by the application. The Fact-Finding Report itself states: 'Examination of publicly accessible information and the initial technical evaluation of FCash and the Fast Cash online lending application shows that the company has failed to demonstrate compliance with the DPA.'

Clearly, the investigators made findings beyond the scope of the individual complaints filed by the data subjects. These includes inaccessible information regarding [FCash's] Data Protection Officer, failure to exercise efforts in response to privacy complaints, inadequate Privacy Policy, and presence of dangerous permissions violating the principle of proportionality.¹⁶

II. The assailed Decision did not ignore the rule on exhaustion of remedies under Section 4, Rule II of the NPC Rules.

Respondents contend that the Commission failed to observe the mandatory exhaustion of remedies requirement under Section 4, Rule II of the NPC Rules as Respondents were not granted the opportunity to "take timely or appropriate action on the claimed privacy violation or personal data breach"¹⁷ before a complaint can be filed.

As held by the Commission in NPC 19-910, to wit:

The Respondent's interpretation that the Commission should first reach out to respondents to be 'given the opportunity to institute appropriate actions to rectify the alleged criminal violations of the DPA' is purpose-defeating, if not plainly absurd. Sua sponte investigations are only conducted under specific premises under the Rules of Procedure, thus:

Section 23. Own initiative. – Depending on the nature of the incident, in cases of a possible serious privacy violation or personal

¹⁶ Supra Note 3, page.23

¹⁷ Section 4 (b), Rule II of NPC Circular No. 16-04

data breach, taking into account the risks of harm to a data subject, the Commission may investigate on its own initiative the circumstances surrounding the possible violation. Investigations may include on-site examination of systems and procedures. If necessary, the Commission may use its enforcement powers to order cooperation of the personal information controller or other persons, with the investigation or to compel appropriate action to protect the interests of data subjects.

subjects.

As seen with the abovementioned criteria for a sua sponte investigation, complaints are only initiated in cases of a possible serious privacy violation or personal data breach. In these actions, the Commission considers evident risks of harm to a data subject. The privacy violation or personal data breach that can be directly acted upon by the Commission is qualified with a degree of seriousness that makes it different from complaints under Rule III. This degree of seriousness is considered in relation to the level of risks posed to the data subjects, and may be manifested in different ways such as the scale of processing or the number of reports received by the Commission.

Thus, in cases of sua sponte investigations, it is futile for the Commission to exhaust remedies by communicating with the respondent. The provision on the exhaustion of remedies is meant to provide an opportunity for parties to amicably settle among themselves and rectify the situation. This is only resorted to when the possibility of rectification still exists

The nature and purpose of sua sponte investigations make such exhaustion of remedies futile because by the time the Commission detects a privacy violation or personal data breach, the opportunity for rectification is no longer available. The requirement of exhaustion of remedies is thus inapplicable to sua sponte investigations.

Furthermore, such provision for the exhaustion of remedies is not an absolute rule that renders all non-conforming complaints invalid. The Commission has previously discussed the purpose for the exhaustion of remedies in an earlier Decision:

This rule was intended to prevent a deluge of vexatious complaints from those who waited for a long period of time to pass before deciding to lodge a complaint with the NPC, unduly clogging its dockets. Notably, however, the same Section provides that the Commission has the discretion to waive such period for filing upon good cause shown, or if the complaint involves a serious violation or breach of the DPA, taking into account the risk of harm to Complainant.¹⁸

Respondents also argue that the conduct of a sua sponte investigation is unnecessary as there were already several pending complaints against it.

As held by the Commission in NPC 19-910, the Commission wishes to highlight:

Nowhere in its Decision did the Commission ‘admit that the sua sponte investigation was conducted in lieu of the several complaints received by the Honorable Commission against Respondent[.]’ On the contrary, the Decision explicitly stated that the sua sponte investigation is independent and separate from the individual cases by stating that ‘the pending cases and the case on hand involve different parties, different causes of action with different prayers of relief.’

XXX

The individual complaints were only cited to demonstrate the seriousness of the possible data privacy violation.¹⁹

The sua sponte investigation was conducted due to the potential harm to the data subjects. This is in consideration of the Commission’s mandate in the DPA to ensure a personal information controller’s compliance with the law²⁰ and institute investigations when necessary.²¹ This is likewise in consideration of the provision in NPC Circular 2021-01, which allows conduct of sua sponte investigations of possible privacy violations or personal data breaches.²² Hence,

18 NPC 19-910, Resolution

19 Id.

20 An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter II, § 7(a) (2012).

21 Id. § 7(b).

the sua sponte investigation of the Commission was conducted due to its mandate and function and not because of several complaints.

III. The assailed Decision did not ignore the rule on litis pendentia, there being pending cases involving Respondent FCash filed by specific individual complainants who appear to be the same parties in the case

Further, Respondents claim that the conduct of a separate proceeding involving the same subject matter as cases which are currently being investigated and pending for adjudication by this Commission through its investigating officers violates the principle of litis pendentia. As previously discussed, the pending cases before the Commission filed by different complainants is entirely different from the case initiated by a sua sponte investigation. These cases have different parties, different causes of action with different prayers of relief. The cited complaints in the FFR were, to reiterate, used to emphasize the gravity and seriousness of the violation of data privacy. Respondents erred in saying that they are being vexed for the same subject matter.

IV. The assailed Decision does not violate nor renders nugatory the provisions of the DPA on amicable settlement and alternative modes of disputes resolution which are expressly promoted by law.

As to the contention that the Decision is totally in conflict with the other decisions of this Commission approving the amicable settlement entered into by specific complainants, the Commission wishes to remind Respondents that the previous decisions of the Commission approving the amicable settlements are entirely different from the case initiated by the sua sponte investigation. These cases which are settled and dismissed by virtue of an amicable settlement are not decided based on the merits of the case but due to the mutual understanding of the parties. The final amicable settlement that contains the terms and conditions of the parties for the settlement of the case has the force and effect of law between these parties. No provision of the DPA was used to arrive at the settlement. As held by the Supreme Court in the case of Miguel v. Montanez:

Being a by-product of mutual concessions and good faith of the parties,

22 NPC Circular No. 2021-01, rule X, §§ 5-6.

an amicable settlement has the force and effect of res judicata even if not judicially approved. It transcends being a mere contract binding only upon the parties thereto, and is akin to a judgment that is subject to execution in accordance with the Rules.²³

Further, “[w]hile the Rules on Mediation embodied in NPC Circular No. 18-03 did not provide a distinction between cases which can and cannot undergo mediation, NPC Circular No. 16-04 categorically states that ‘no settlement is allowed for criminal acts.’”²⁴

The Commission also wishes to emphasize that the purpose of the mediation settlement is to help parties arrive at an acceptable compromise. Considering that the cause of action in a complaint borne out of a sua sponte investigation is the State’s duty to protect the right to privacy and not to prosecute to claim reparation on behalf of private individuals, no compromise can be had between the State and the Respondent.

Hence, the previous decisions of the Commission confirming the amicable settlement of the parties are not contrary to the Decision as no interpretation and application of the DPA was used nor preceding decisions of the Commission was applied. The decisions of the Commission were merely a recognition of the agreement of the parties to settle the case based on their mutual understanding and not through the remedial procedures of this Commission.

V. The assailed Decision does not arbitrarily, unfairly, and erroneously impleaded the corporate officers of Respondent Fcash despite the lack of evidence, let alone allegation, that any of them participated in the alleged acts nor committed any gross negligence.

Lastly, Respondents contend that impleading its corporate officers of despite the lack of evidence, let alone allegations, that any of them participated in the alleged acts or committed any gross negligence is arbitrary, unfair, and erroneous.²⁵ This Commission points out that the DPA is clear that the liability of the responsible officers in cases where the offender is a corporation does not rely on active participation alone. Gross negligence is explicitly stated in the DPA as a ground for criminal liability, to wit:

SEC. 34. Extent of Liability. – If the offender is a corporation, partnership

²³ Miguel v. Montañez, G.R. No. 191336, 25 January 2012

²⁴ NPC 19-910, Resolution

²⁵ Motion for Reconsideration dated 28 February 2022

or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and he or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.²⁶

There is no reason for the Commission to reverse its earlier finding that the Respondent officers are liable for gross negligence. As stated in the Decision of this Commission in the case of NPC 19-910:

The Supreme Court has consistently defined gross negligence as ‘the negligence characterized by the want of even slight care, or by acting or omitting to act in a situation where there is a duty to act, not inadvertently but willfully and intentionally, with a conscious indifference to the consequences of, insofar as other persons may be affected. It is the omission of that care that even inattentive and thoughtless men never fail to give their own property.’²⁷

The fact that the Board of Directors (BOD) failed to act on the voluminous and alarming privacy issues of their borrowers negates the legal presumption that the BOD employed ordinary care in the discharge of their duties and instead, presumes that the BOD knew about these collection practices and approved of it. There are one hundred and sixty-six (166) complaints against Respondent as of July 2019. The Complaint also attached user reviews on Respondent application in Google Play Store. The user comments narrated experiences on how the Respondent gains access to mobile phonebook/directory/contact list for the purpose of disclosing their transactions without their consent and authority.²⁸ It can be reasonably said that the privacy complaints against Respondent have reached into the public’s consciousness.²⁹ Thus, it is the

²⁶ Section 34 of R.A. 10173

²⁷ Fernandez vs Office of the Ombudsman, GR No. 193983, March 14 2012.

²⁸ Fact-Finding Report dated 29 August 2019, pg. 11-13.

responsibility of the BOD to show to this Commission that they have employed the necessary diligence expected from them. However, no evidence was presented by the Respondent to rebut this presumption against them. Further, despite the BOD's responsibility to show the Commission that it employed necessary diligence, it unfortunately still refuses to present any evidence demonstrating that it addressed, or at the very least, did not allow such actions.

Citing the SEC registration records of the Respondent, the Complaint specifically named KDM, TH, JPS, JCT, and ZS as the original incorporators, registered directors, and officers of Respondent. Thus, the abovementioned violations of the DPA shall be imputed against all of them due to their gross negligence following Section 34.³⁰

Considering the foregoing, Respondents have not provided any new or material allegations that would merit the reversal of the Decision.

WHEREFORE, all the above premises considered, this Commission hereby resolves to DENY the Motion for Reconsideration filed by FCash Global Lending Inc. The Decision of the Commission dated 23 February 2021 is hereby AFFIRMED.

SO ORDERED.

City of Pasay, Philippines.
28 April 2022.

Sgd.

JOHN HENRY D. NAGA

Privacy Commissioner

WE CONCUR:

Sgd.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

Sgd.

DUG CHRISTOPHER B. MAH

Deputy Privacy Commissioner

²⁹ See: <https://manilastandard.net/business/biz-plus/335368/sec-voids-license-of-fcash-global.html>.

³⁰ Fact-Finding Report dated 29 August 2019, pg. 9-10.

Copy furnished:

BTLO

Counsel for FCash Lending Inc.

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

**IN RE: BREACH NOTIFICATION
REPORT OF PHILIPPINE NATIONAL
BANK (PNB)**

**NPC BN 17-
034**

X-----X

RESOLUTION

NAGA, D.P.C.

This resolution refers to the security breach notification that the Commission received dated 17 November 2017 from the Philippine National Bank (“PNB”) involving its inControl Portal (“Portal”), a self- service offering for enrolled customers to control the spending of their supplementary credit card.

The facts are the following:

On 14 November 2017, through the conduct of their regular monitoring of credit card service availability, the PNB’s IT Credit Card Operator reported that the Portal issued a database error response. Following their standard operating procedures on incident reports, PNB conducted an investigation and discovered that the inControl server files are encrypted with the Arena ransomware, which is a kind of malware that infects the victims’ computer with a code that restricts the user’s access to systems and files.

To initially address the security breach, PNB shut down the Portal. Subsequently, the server was removed from the main network to prevent other applications and devices to be infected by the ransomware.

On 17 November 2017, the Commission received the notification from the PNB regarding the security breach that transpired on its Portal.

Through a letter dated 22 November 2017, the PNB stated that according to their initial forensic report, no customer record was compromised, and no other system was impacted by the breach. However, the self-service feature became unavailable, and this affected 655 active and 257 inactive customers, out of 33,000 credit card customers of the PNB.

On 2 July 2018, the PNB has successfully restored the inControl portal. No issues were detected after the conduct of an independent VAPT.

On 13 July 2018, the Commission issued a Compliance Order to PNB requiring them to:

1. Submit a report on the status of the security measured being implemented within one (1) month from receipt of the Order; and
2. Submit all pertinent documents for remediation within three (3) months from receipt of the Order.

The PNB was able to submit the required reports on 24 August 2018 and 26 July 2019, respectively. The documents provided details on PNB's implementation of several remediation measures to improve the security of its systems. PNB manifested that they executed the following measures:

1. Installed new servers and segregated the application and database servers;
2. Upgraded the operating systems, database and secure socket layer ("SSL") encryption versions;
3. Implemented Anti Distributed Denial of Service ("DDOS") facility and improved Domain Name System ("DNS"); and
4. Subjected the new environment to vulnerability and penetration tests ("VAPT"), remediating findings before the release production.

On 3 July 2019, the Commission's Enforcement Division sought the assistance of the Data Security and Technology Standards Division ("DSTSD") in order to review PNB's compliance and whether the remediation measures implemented is commensurate with the industry standards.

In the DSTSD report dated 07 August 2019, they concluded that PNB's remediation measures are at par with the industry standard requirements, specifically the Payment Card Industry Data Security Standard ("PCI DSS"). The DSTSD report also underlined the noticeable improvement on PNB's security measures after the Commission's issuance of the 13 July 2018 Order.

The Enforcement Assessment Report dated 13 December 2019 categorically stated that the measures undertaken by PNB complies with the R.A. 10173 or the Data Privacy Act, its Implementing Rules and Regulation, and NPC Circular 16-03 on Personal Data Breach Management. Further, it was recommended that the PNB shall regularly review these measures and policies to further protect the interests of the data subjects.

This Commission, after thoroughly reviewing all the pertinent documents and giving due credence to the evaluation and examination made by its two Divisions, finds that the PNB was able to substantially comply with the Commission's Compliance Order dated 13 July 2018. This Commission also notes that no complaint against PNB has been filed in any of its offices in relation to said security breach.

WHEREFORE, premises considered, this Commission hereby resolves that this case be **CLOSED**.

SO ORDERED.

Pasay City, Philippines
23 January 2020.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

PHILIPPINE NATIONAL BANK

ATTN: **MR. STY**
Data Privacy Officer, PNB

ENFORCEMENT DIVISION GENERAL

RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION

NAGA, D.P.C.:

Before this Commission is a request made by Sun Life of Canada Philippines Inc. (Sun Life) to be exempted from notifying affected data subjects from a data breach incident that occurred last 29 November 2017.

The Facts

On 01 September 2017, Sun Life's Unit Manager (UM) was transferred from Eucalyptus New Business Office (NBO) to Empress NBO. By reason of such transfer, the Licensing Department updated her Agent Information System (AIS). On 26 November 2017, the UM reported to their Helpdesk that she was able to generate the production report that belongs to her Branch Manager (BM) and her direct advisors when she used her personal laptop via Google Chrome browser.

On 27 November 2017, the incident was escalated to the Advisor Technology Support (ATS) and Compliance. It was identified that because of the update, the code of her new BM was saved as the UM's Team Lead Code which allowed her to generate the production report.

Sun Life reported that one hundred one (101) accounts with one hundred (100) policy owners were affected by the breach. The personal data involved are as follows: Due Date; Policy Number; Insured Name; Submitted Applications; Settled Applications; Net Sales Credit; First Year Premium; and Renewal Premium Income.

In response, Sun Life mentioned that they have taken the following measures to address the breach:

- a. On 27 November 2017, the UM was requested to delete the production report that she has downloaded from the agent's portal and send confirmation that the same was deleted;
- b. The UM code was updated to her own team code in the Agent's Information System;
- c. The Licensing Department will file a maintenance request to update the AIS. The Team code field will not accept the code if it does not belong the advisor/UM whose account is being updated; and
- d. IT will be requested to sweep or check the system for another similar occurrence.

On 29 November 2017, Sun Life submitted the breach notification report before the Commission with a request to be exempted from notifying its clients and advisors that were affected by the breach, on the ground that the breach will not cause real risk of serious harm to the rights and freedoms of the policy holders considering that it was the UM herself who reported the said breach.

Discussion

As provided by Section 11 of the NPC Circular 16-03, notification to the affected data subjects shall be required upon knowledge of or when there is reasonable belief by the Personal Information Controller (PIC) or Personal Information Processor (PIP) that a personal data breach requiring notification has occurred, under the following conditions:

- A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
- B. There is reason to believe that the information may have been acquired by an unauthorized person; and

- C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

The Commission recognizes that Sun Life has premised its request for exemption on the ground that the incident does not meet the third condition laid down by the abovementioned provision as the personal data were disclosed only to the UM.

However, Sun Life failed to take into account that the number of affected data subjects is more than one hundred (100) individuals which falls under the mandatory breach notification as provided by Section 13 (B) of NPC Circular 16-03.

According to Section 38 of the Data Privacy Act of 2012 (DPA), “Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.” Thus, the DPA and the rules and regulations in relation to data privacy should be interpreted in a manner that will uphold the data privacy rights of the individual. Hence, the Commission does not see any reason to disturb the general rule for the PIC to notify the data subjects affected by a personal data breach¹.

The Commission then deems it wise to order Sun Life to notify the affected data subjects to provide them the reasonable opportunity to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.

On another matter, the Commission notes that as of the date of the promulgation of this Resolution, it has yet to receive its full breach report as required under NPC Circular 16-03. The Commission reminds Sun Life that the DPA requires two (2) different reports in case of a data breach.

As held by the Commission in the case of *In re: SLGF (NPC BN 19- 115)*:

Section 17 of the NPC Circular 16-03 speaks of two notification requirements to be submitted to the Commission in case a data breach cases. First is the initial notification² that

¹ Section 18 of the NPC Circular 16-03

² Section 17 (A) of the NPC Circular 16-03

informs to the Commission that a personal data breach has occurred. This has no particular form or content as it merely requires that the Commission to be notified within seventy-two (72) hours. The second notification³ is the Full Breach Report which contains a more specific and concrete narration of facts surrounding the incident, the effect of such incident and the remedial actions taken by the PIC. The full breach report that the Commission requires must include, but not be limited to:

1. Nature of the Breach
 - a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
 - b. a chronology of the events leading up to the loss of control over the personal data;
 - c. approximate number of data subjects or records involved;
 - d. description or nature of the personal data breach;
 - e. description of the likely consequences of the personal data breach; and
 - f. name and contact details of the data protection officer or any other accountable persons.
2. Personal Data Possibly Involved
 - a. description of sensitive personal information involved; and
 - b. description of other information involved that may be used to enable identity fraud.
3. Measures Taken to Address the Breach
 - a. description of the measures taken or proposed to be taken to address the breach;
 - b. actions being taken to secure or recover the personal data that were compromised;
 - c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
 - d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
 - e. the measures being taken to prevent a recurrence of the incident.⁴

The foregoing content and information is needed by the Commission in order to determine if the PIC has acted adequately in order to protect the rights of the affected data subject and to see if the PIC has undertaken measures to avoid further damage. These two documents are very much different from one another not only as to its form and content but also as to its purpose.

³ Section 17 (D) of the NPC Circular 16-03

⁴ Section 17 (A) of NPC Circular 16-03

Sun Life submitted before the Commission a breach notification dated 29 November 2017. The breach notification submitted can only be considered as a notification as prescribed under Section 17

(A) of NPC Circular 16-03 as it lacks the necessary content and information required in a full breach report. Therefore, Sun Life is not yet compliant in terms of the submission of the required full breach report.

WHEREFORE, premises considered, this Commission **DENIES** the request of Sun Life to be exempted from notifying data subjects affected by the breach.

Sun Life is hereby **ORDERED** to comply within ten (10) days from receipt of this Resolution with the following:

(1) **NOTIFY** with dispatch the affected data subjects, including proof of compliance consistent with NPC Circular 16-03; and

(2) **SUBMIT** a full breach report detailing the measures it has since undertaken to prevent, avoid or reduce the recurrence of a similar personal data breach.

SO ORDERED.

Pasay City, Philippines;
15 October 2020.

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

(*On Official Business*)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

JSC
Data Privacy Officer

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION

NAGA, D.P.C.:

On 21 May 2020, the Commission issued a Resolution with a dispositive portion as follows:

WHEREFORE, premises considered, PSC is ordered by this Commission to SUBMIT a full breach report in compliance with Section 9 of NPC Circular 16-03, including the updates on the proposed remediation measures and post-breach review by the PSC, within fifteen (15) days from the receipt of this order.

On 07 August 2020, the PSC through its Data Protection Officer (DPO) complied with the aforementioned order when it sent its proposed remediation measures and post-breach review to the Commission.

PSC's post-breach review indicates the following actions that were already completed:

1. BDD completed the revision of its franchise qualification processes and forms aligned with PSC's data privacy manual;
2. Re-training of PSC personnel on Data Privacy;
3. BDD data controller issued a reminder of data privacy compliance immediately after the incident and completed training to BDD personnel on PSC's data privacy policies and security measures;
4. Information Technology Division (ITD) and BDD reviewed PSC's email settings and strictly implemented the following:

- i. Standard notices in email requesting unintended recipient to alert the sender and delete the message attachments
 - ii. 2-factor authentication for emails
 - iii. Cascading information on use of the confidential and undo function in Gmail as a security feature to Data Controllers
5. Human Resources Administration Division (HRAD) posted a video reminder in PSC's Data Privacy portal to remind all personnel of PSC on use of before sending emails to multiple recipients and included in the module for orientation of new employees a topic on data privacy with special reminder on proper use of email; and
6. Implementation of above action plans were complied with.

The Enforcement Division issued its findings on the compliance of PSC, *viz*:

Upon reviewing the report submitted by PSC, we found that the corporation has complied with the order and resolution of the Commission dated 21 May 2020 and NPC Circular No. 16-03 on Personal Data Breach Management.

xxx xxx xxx

WHEREFORE, premises considered, the Enforcement Division respectfully recommends to CLOSE the instant case, CID BN 18-091 **In The Matter Of The Philippine Seven Corporation Data Breach Notification Report.**

In addition, the Commission sternly reminds PSC that notifying data subject in cases of data breach should be swift and immediate to reduce the risk to the data subject arising from the personal data breach. There is no need for the personal information controller (PIC) or Personal Information Processor (PIP) to await any order or positive action from the Commission to make such notification.

Section 20 (f) of the Republic Act No. 10173 or the Data Privacy Act of 2012 provides:

“The personal information controller **shall promptly notify the Commission and affected data subjects** when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise”

Further Section 11 of the NPC Circular 16-03 provides:

“Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions: ...“

The language of the abovementioned provisions are clear and direct. The PIC or PIP are required to promptly and immediately notify the affected data subject in case of a data breach. The act of notifying should be automatic. Hence, it is expected from PSC that the incidents that transpired in this case in relation to the notification of the affected data subject will no longer happen.

WHEREFORE, premises considered, it is resolved that the matter of CID BN 18-081 “In Re: Philippine Seven Corporation” is hereby considered **CLOSED**.

SO ORDERED.

Pasay City, Philippines;
10 September 2020.

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

ESE
Data Protection Officer
Philippine Seven Corporation

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

X ----- X

RESOLUTION

LIBORO, P.C:

Before this Commission is a breach case involving University of the East (UE) for the violation of Data Privacy Act of 2012 (DPA).

Facts

On April 14, 2019, S.B.N. - Dean of University of the East College of Computer Studies and Systems, received a message in his Facebook Messenger from username: C.D. that reads: *“Magandang umaga. Gsto namin ipaalam na hawak na naming ang libo libong data at mga MOA mula sa inyong mga web systems na gawa ng inyong research department. Hindi kami magdadalawang isip na ikalat ito sa publiko kapag ipinagpatuloy mo ang pag balewala sa hinain ng mga estudyante at ang pagkampi sa mga tao na umaapak sa mga karatapan nila”*. A snapshot of the message was sent to Professor N.K.T., a CCSS faculty member designated as RnD Coordinator, who then informed RnD Team Leader and UE-CCSS student - D.G., and Assistant Team Leader – N.B.Z. D.G. and N.B.Z. both verified the claims of C.D. by checking the servers (Google Servers) maintained by the RnD Unit.

Their verification discovered unauthorized logs on the server maintained by N.B.Z. The said server sustained brute force attacks from more than 4,000 I.P. addresses, trying to get into the system's database. Notably, the server that was attacked contains the registration databases for UE school activities: “Pasiklaban 2019” and “CCSS Alumni Homecoming 2018”. The same server includes databases for the “MOA Signing System” and “Research Archiving System.”

On 17 April 2019, UE University Manila (“UE”) notified the Commission on the incident involving unauthorized access to personal information stored in the database of the Research and Development (“RnD”) unit of the UE College of Computer Studies and System (“CCSS”). According to incident report, the hacking involved a breach of personal data of 1,572 Senior High School Students and around 200 for CCSS Alumni.

In the same Data Breach Notification (Preliminary), UE requested for a postponement of notification to Data Subjects as the system hacking happened during the period of semestral break that is within the Holy Week, and this made it difficult for them to notify all affected data subjects, as well as to summon key persons for an interview concerning the incident.

On 9 September 2019, the Commission En Banc, denied¹ the request for postponement of UE. It emphasized the need of notification hence UE was ordered to notify the data subjects without further delay and to submit within fifteen (15) days a complete breach report, including details of notification and assistance provided to data subjects.

On 21 July 2020, due to UE’s non-compliance with the Commission En Banc’s directive on the Resolution dated 09 September 2019, the Commission sent an Enforcement Letter to UE which contains directive upon UE’s Data Protection Officer to ensure immediate compliance with the Commission En Banc’s directive on the said Resolution.

On 19 August 2020, Ms. T., responded to the Enforcement Letter explaining that they previously sent the complete breach report with details of notification (Final Report) on 09 October 2019 to complaints@privacy.gov.ph. However, this Division found deficiencies in the submitted Final Report. Thus, in the light of a thorough assessment, this Division further directed UE to submit the annexes and proofs of notification for a bona fide complete report.

¹ 09 September 2019, Resolution

On 16 September 2020, Ms. T. submitted the required annexes and proofs of notification, which finally cured the report's previously found deficiencies.

Discussion

This case before the Commission can now be considered closed.

Under circumstances where sensitive personal information or other information are reasonably believed to have been acquired by an unauthorized person, Section 20(f) of the Data Privacy Act of 2012 (DPA) provides that:

The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

Section 18 of NPC Circular No. 16-03 (Circular) provides for the procedure on which the personal information controller (PIC) must follow in notifying the affected data subjects affected by a personal breach.

As to the content of notification, the Circular² provides that the notification shall include, but not be limited to:

nature of the breach;
personal data possibly involved;
measures taken to address the
breach;

² Section 18 (c), NPC Circular 16-03 – Personal Data Breach Management

measures taken to reduce the harm or negative consequences of the breach;
representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
any assistance to be provided to the affected data subjects.

Where it is not possible to provide the foregoing information all at the same time, PIC may be provided in phases without undue delay.

The Circular³ further provides that the PIC shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach. Hence, the notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. Where individual notification is not possible or would require a disproportionate effort, the PIC may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner.

In this case, it is shown that UE received the Resolution on 24 September 2019. UE was given a fifteen (15) day period to notify the affected data subjects. Based on the submitted screenshot⁴ of e-mail notifications, it shows that UE started notifying the affected data subjects on 1 October 2019, which was well within the period given to it comply with the order.

As to examination of the content and form of the Notification, the Commission found that the notification thoroughly outlined the nature of the breach, the personal data that was possibly affected, the measures UE had undertaken to address the breach, reduce harm or

³ Section 18 (d) Form. Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: Provided, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.

⁴ Screenshot of Email Notifications to Affected Data Subjects from U.E. DPO.

negative consequences of the breach, and contact details of the DPO where an affected subject could reach out for clarifications and further assistance. In addition, the said notifications were electronically sent individually to the affected data subjects via e-mail.

Aside from UE's compliance with the notification requirement provided in the Circular, UE provided measures it took to address the breach, to wit: 1. An immediate shut down of its main server to prevent further data compromise; 2. Verification of the sample data/data portion showed by 'C.D.' and confirmed that such is a part of the database; 3. Checking of the integrity of the database existing on the main server vis-a-vis the sample data from C.D. From there, it was verified that the data was merely copied and not altered nor destroyed; and 4. Migration of the databases and systems to a highly protected/secured cloud storage/service provider, such as Google Cloud Platform that provides a higher and stricter security level.

In order to prevent the recurrence of the same incident, the RnD unit of UE had further undertaken to perform the following additional measures: 1. UE's Information Technology Department was tapped to act as an Administrator for any and all designed Information System in their official UE Server for any and all conduct of Student Council Voter Registration and Elections, as well as Registration Systems for various Conferences/Seminars; 2. Definition of 'turnover responsibilities' of the RnD Unit which comprised of students whose engagement to the said unit can be terminated anytime; 3. All new measures, such as but not limited to procedures related to the collection, storage, sharing, and disposal of data shall be put in writing and be incorporated in the Operations Manual of the RnD Unit.

UE further adopted measures for non-RnD Unit Activities and Student-led projects, to wit: a. Higher and Stricter level of security on Google Cloud Platform; b. Incorporation of Cost of Subscription to a More secure Cloud Service in the College Budget; c. Designation of RnD Unit as an Institutional Account Holder for the migration of all its system/database to a new server; d. Definition of Duties and Responsibilities of the members of the RnD Unit, especially to members who shall manage the server; and e. For every system developed and deployed, the following items will be defined to closely monitor access to data among the members of the unit: i. System Development: a. Composition and definition of responsibilities of the

Systems Development Team; b. Access permission to files and databases; c. Use of password, encryption, and other security measures; d. Use of Google Drive and other cloud storage facilities; e. Use of mobile devices to access e-mail, Google Drive, and other facilities necessary for systems development; and ii. System Deployment: a. Collection procedure for the actual/live data and the security protocol applied to its access; b. Access Permission requirement for each member of the team to the system. A set of procedures will be formulated to define awarding to access rights and removal of access rights. Hierarchy of Access (such as Viewing, Editing Privileges, etc.) will also be considered; and c. Access Permission for databases for the RnD coordinator, team leader, assistant team leader.

A careful examination of UE's complete breach report reveals the organization's judicious and suitable put-up of measures, steps, and policies to address the breach incident. However, the said breach report also stated that they "emphasize herein that the data was just copied, not altered or destroyed⁵". With this, the Commission underscores the importance of data protection. Hence, PICs is directed to take by heart the provision of Section 4⁶ of the Circular which mandates the implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system, and mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach. It is not enough to conclude that the data were just copied and not altered or destroyed without the PIC's in-depth investigation of the matter. The PIC's investigation should have considered the possibility that the information may have been accessed and used by unauthorized persons, in an effort to mitigate the risks to the data subjects.

Nonetheless, with the twin notification made by UE to this Commission and upon the affected data subjects, this shows consonance with Section 20(f) of the Data Privacy Act, which requires

⁵ Complete breach report (Final Report), page 4.

⁶ "A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure, among others, the implementation of organizational, physical, and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident, implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system, and mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach."

prompt notification upon the National Privacy Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person (in this case by one under the guise of “C.”), which may likely give rise to a real risk of serious harm to any affected data subject.

With the foregoing, the Commission deduced from the careful examination of the reports and other documents submitted by UE that there is a bona fide compliance with the directives of the Commission’s Resolution and the Circular. The measures undertaken by UE are responsive to the required personal data management, which includes prevention, incident response, mitigation, and compliance with notification requirements. More so, preventive measures were also undertaken by UE in its effort to deter future breach. Accordingly, due to the apparent bona fide compliance of UE in this case, there is nothing more left for the Commission than to close the case.

WHEREFORE, premises considered, the case CID BN 19-067 In the Matter of University of the East Manila, is hereby considered CLOSED.

SO ORDERED.

Pasay City, Philippines.
22 October 2020.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

F.B.H.

Head of the Organization
Office of the Chancellor, Manila

M.Q.T.

Data Protection Officer
Office of the Chancellor, Manila

S.B.N.

Process Owner
Office of the Chancellor, Manila

**LEGAL DIVISION ENFORCEMENT
DIVISION GENERAL RECORDS
UNIT**

National Privacy Commission

CBP,

Complainant,

-versus-

NPC 16-004

ORANI WATER DISTRICT

(formerly CDBJ and SRM),

Respondents.

x

x

RESOLUTION

AGUIRRE, D.P.C.;

This Commission resolves the sufficiency of Orani Water District's (OWD) Privacy Manual and Notices, and proof of participation in a data privacy orientation of its employees, as directed in the Decision dated 15 December 2017.

Facts

On 15 December 2017, the Commission issued a Decision requiring OWD to submit its Privacy Manual and Notices, and proof of participation in any orientation on the Data Privacy Act of 2012 (DPA):

WHEREFORE, premises considered, CDBJ and SRM, [officers of Orani Water District] are STERNLY WARNED that repetition of the same or similar acts will be dealt with more severely. Respondents are hereby further ordered:

1. To coordinate with the head of agency of Orani Water District and submit to National Privacy Commission the organization's privacy notice and existing privacy policies pertaining to their employees within fifteen (15) days from receipt of this Decision; and

2. To submit to the National Privacy Commission proof of their attendance or participation in any orientation on the Data Privacy Act or similar events within (60) days from receipt of the Decision.

SO ORDERED.¹

On 19 November 2020, the Commission issued an Order noting OWD's non-compliance with the Decision dated 15 December 2017, despite the passage of three years.² Giving OWD a final opportunity to comply with the Commission's directives, the Commission ordered OWD to submit its Privacy Manual and Notices within thirty (30) days from its receipt of the Order:

WHEREFORE, premises considered, OWD is hereby ordered to **SUBMIT** the final draft of its Privacy Manual and Notices **within thirty (30) days** from receipt of this Order.

SO ORDERED.³

On 05 March 2021, OWD submitted its Privacy Manual and Notices.⁴

On 20 April 2021, the EnD informed OWD of the issues it identified in the submitted Privacy Manual and Notices:

In OWD's Privacy Manual's provision for Security Measures IMB was identified as the Personal Information Controller. However, under the R.A. 10173 or the Data Privacy Act of 2012 (DPA), a Personal Information Controller is clearly defined as:

(h) Personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

- (1) A person or organization who performs such functions as instructed by another person or organization; and
- (2) An individual who collects, holds, processes or uses personal

¹ Decision, 15 December 2017, at 7, *in* CBP v. Orani Water District, NPC 16-004 (NPC 2017) (pending).

² Order, 19 November 2020, *in* CBP v. Orani Water District, NPC 16-004 (NPC 2020) (pending).

³ *Id.* at 6.

⁴ Final Draft of OWD Privacy Manual and Notices, 05 March 2021, *in* CBP v. Orani Water District (NPC 2021) (pending).

information in connection with the individual's personal, family or household affairs.

From the foregoing, it should be noted that under these circumstances, OWD is the Personal Information Controller and not a specific individual or employee thereof. Hence, we suggest that OWD's Privacy Manual be amended to reflect the clear and correct designation of officers including their functions and responsibilities pursuant to the DPA and relevant issuances. In this regard, the Data Privacy Officer may be supported by different compliance officers for privacy (COP) or other team members as your organization may see fit.

Further, upon reviewing the OWD's Data Privacy Manual, we found that the draft does not include the manner of verification and/or validation of the contents of the Personal Data Sheet of employees. To recall, this instant case arose because one of your employees verified the contents of the PDS of another employee by requesting documents from the Philippine Statistics Authority. In the NPC's Decision, the Commission posed the question '[W]as the complainant informed that the verification and validation of contents in the PDS include requesting relevant documents from other government agencies or information repositories?'

While in OWD's Privacy Manual, you indicated that the data subjects will be provided specific information regarding the purpose and extent of the processing of their data, the information regarding the extent of the processing of the employees' PDS is not clearly specified defined in the employee consent forms. Without such provision, likely, similar incidents could not be avoided.

An agency should adhere to the principle of transparency or openness in the processing of personal data. Personal information controllers like OWD must demonstrate that there are existing policies and procedures to ensure that data subjects are fully informed of the intended processing of their personal information.⁵

It directed OWD to submit within thirty (30) days from receipt of the letter a revised Privacy Manual and Notices that indicate the manner of verification and validation of the contents of employees' PDS, and a detailed and concrete Security Incident Management Policy according

⁵ Compliance with Decision dated 15 December 2017 "CBP v. CDBJ, et al.", 20 April 2021, at 1-3, *in* CBP v. Orani Water District (NPC 2021) (pending).

to the DPA and Section 4 of NPC Circular No. 16-03 (Personal Data Breach Management)).⁶

On 19 May 2021, OWD complied with the EnD's directive and submitted its revised Privacy Manual and Notices, which includes its Security Incident Management Policy, for the Commission's perusal.⁷

On 12 August 2021, the EnD informed OWD that it identified inconsistencies between the Privacy Manual and Notices and the DPA, its Implementing Rules and Regulations, and the Commission's relevant issuances.⁸ It instructed OWD to revise the following:

1. Functions of the Personal Information Controller (PIC), Data Protection Officer (DPO), and Compliance Officer for Privacy (COP)

The obligations, duties, and responsibilities of a PIC, which in your case, the OWD itself, must not be delegated to either DPO or COP, unless allowed by DPA or its rules. In the same vein, duties and obligations imposed explicitly by law upon DPO and COP must not be placed upon the OWD, especially when the OWD has already designated a DPO and COP within its organization.⁹

2. OWD's measures on storage, retentions, and disposal procedure found under its Manual

An observation of the 'Retention Records Table' vis-à-vis 'Storage, Retention, and Destruction (means of storage, security measures, the form of information stored, retention period, disposal procedure, etc.)' of the OWD Manual reveals that the former is blank at the latter appears to be leaving the discretion of the matter to its individual employees. The means of storage, period of retention, and manner of disposal should not be merely placed under the discretion of an individual employee; the discretion on the matter must be carefully determined by OWD, taking into consideration the specific purpose of each category of personal data. The said policy on retention should already be documented in the OWD Manual.¹⁰

⁶ *Id.* at 3.

⁷ Submission of Revised Draft of OWD Privacy Manual, 19 May 2021, *in* CBP v. Orani Water District (NPC 2021) (pending).

⁸ Compliance with Decision dated 15 December 2017 "CBP v. CDBJ, et al.", 12 August 2021, *in* CBP v. Orani Water District (NPC 2021) (pending).

⁹ *Id.* at 2.

¹⁰ *Id.* at 3.

3. Collection of Data Table

The Manual on the Use and Purpose of Data Collection referred to a Collection of Data Table which is supposed to include further details of the types of data collected and its purposes, the same is supposed to also demonstrate any data sharing to which the particular data is involved. However, the said table is left blank and it is not made clear who is responsible to accomplish the table. It should be reiterated that Data Inventory must be made part of the preparation of your Records of Processing Activities as required under Section 26(c) of the IRR of DPA which forms part of the organization's data privacy compliance documentation.¹¹

4. Keeping Records of Processing Activities

OWD must attach to its Privacy Manual its Records of Processing Activities for each of its data processing systems, program, project, or activity.¹²

5. Contact Details of the Data Protection Officer

Section I of the OWD Manual on Inquiries and Complaints discussed the data subject's rights and the means to exercise them, however, the contact details of the Data Protection Officer to whom any data privacy concern, dispute, issues, or complaints should be escalated is left blank. It is necessary to complete these details since this manual will serve as the organization's guide in addressing any data privacy concerns, disputes and grievances and it will be advantageous to have this information on hand.¹³

6. Conduct of Training or Seminars for the DPO and OWD Personnel

The authority phrase found under paragraph 4 of the Consent Letter, which reads: "to share my information to affiliates and necessary third parties for any legitimate business purpose." is ambiguous and fails to meet the requirements of transparency. At this point, OWD must have already identified its affiliates and third parties with whom it shares data. Therefore, the phrase in

¹¹ *Id.* at 3-4.

¹² *Id.* at 4.

¹³ *Id.*

question must be revised to convey to the data subject the recipients or classes of recipients to whom their data will be disclosed and the purpose/s for its disclosure.¹⁴

The EnD directed OWD to correct the deficiencies and submit a revised Privacy Manual and Notices within fifteen (15) days from receipt of the letter.¹⁵

On 28 August 2021, OWD submitted its revised Privacy Manual and Notices.¹⁶

On 15 September 2021, the EnD again directed OWD to correct the following deficiencies:

1. The Manual still refers to the Personal Information Controller (PIC) as if it is another entity or person

On pages 17 and 38, it is written:

'1. Organization Security Measures Every personal information controller or personal information processor must also consider the human aspect of data protection.

...

➤General Obligations and Functions of the PIC, DPO, COP and/or any other responsible personnel with similar functions.

...

2. Functions of DPO

a. The Data Protection Officer shall monitor the PIC's or PIP's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, he or she may:'

...

The Manual's Definition of Terms even defined the PIC as it is defined in the law: "refers to a natural or juridical person, or any other body who controls the processing of personal data, or

¹⁴ Compliance with Decision dated 15 December 2017 "CBP v. CDBJ, et al.," 12 August 2021, at 4, *in* CBP v. Orani Water District (NPC 2021) (pending).

¹⁵ *Id.*

¹⁶ Letter from EFS, Orani Water District, to Enforcement Division, National Privacy Commission, *in* CBP v. Orani Water District (28 August 2021).

instructs another to process personal data on its behalf" and not how you use the term in the Manual which in this case should be used as referring to Orani Water District as the PIC.OWD must make it clear that when it refers to a PIC in its Manual, it is referring to itself and not to a separate entity or a person.¹⁷

2. The Data Protection Office has no specific e-mail address intended only for privacy-related complaints and inquiries in its Privacy Notice

OWD must provide a dedicated e-mail address for proper escalation and reporting of privacy-specific inquiries, issues, and concerns instead of giving a general customer service e-mail address where the privacy-related concerns will be comingled with customer service-related concerns (e.g., billing, account, change request).¹⁸

3. Consent Letter for Concessionaires does not provide specific information as to the purpose for data sharing

On Annex A, Consent Letter (Concessionaires), number 4, it is stated:

‘4. Share my information to Primewater Infrastructure Corp. for any legitimate business purpose.’

For transparency and in line with the general principles of data sharing, please revise the underlined text to be more specific to discuss the type of data being shared, the purpose of sharing, the extent of data sharing, and how Primewater Infrastructure shall process these data.¹⁹

4. Conduct of Training or Seminars for the DPO and OWD personnel did not occur

Once again, OWD is ordered to conduct DPA training for its employees by submitting a training request once again to NPC’s PIAD or find alternative means to comply with this directive.²⁰

On 24 September 2021, OWD submitted its revised Privacy Manual and Notices.²¹

¹⁷ Compliance with Decision dated 15 December 2017 “CBP v. CDBJ, et al.”, 15 September 2021, at 1-2, *in* CBP v. Orani Water District (NPC 2021) (pending).

¹⁸ *Id.* at 2.

¹⁹ *Id.*

²⁰ *Id.* at 3.

²¹ Letter from EFS, Orani Water District, to Enforcement Division, National Privacy Commission, *in* CBP v. Orani Water District (24 September 2021).

On 10 November 2021, OWD submitted the Certificates of Participation of its employees to the DPO Ace Level 1 Training Program organized by the National Privacy Commission.²²

Discussion

The Commission finds that OWD has sufficiently complied with the Commission's directives. As reflected in the revised Privacy Manual and Notices, OWD has fully addressed and corrected the deficiencies to the satisfaction of the Commission. It has also caused the participation of its employees in a data privacy orientation, as shown by the submission of Certificates of Participation to the NPC's DPO Ace Level 1 Training Program.²³

Section 7 of the DPA authorizes the Commission to ensure that personal information controllers (PICs) comply with the DPA, its IRR, and other issuances of the Commission:

Section 7. Functions of the National Privacy Commission. – To administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection, there is hereby created an independent body to be known as the National Privacy Commission, which shall have the following functions:

(a) Ensure compliance of personal information controllers with the provisions of this Act;

...

(d) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy;

...

(f) Coordinate with other government agencies and the private sector on efforts to formulate and implement plans

²² Letter from EFS, Orani Water District, to Enforcement Division, National Privacy Commission, in CBP v. Orani Water District (10 November 2021).

²³ *Id*

and policies to strengthen the protection of personal information in the country;²⁴

Based on the EnD's assessment, it determined that OWD has sufficiently complied with its directives. It identified that the OWD has revised its Privacy Manual and Notices to reflect the following:

1. On the functions of the Personal Information Controller (PIC), Data Protection Officer (DPO), and Compliance Officer for Privacy (COP):

The revised OWD Privacy Manual was already updated, the provisions as to the PIC, DPO, and COP functions are now addressed in accordance and in compliance with NPC Advisory No. 2017-01. Further, the Manual now refers to OWD as the PIC, and its functions as the PIC are now clear and adequately discussed.²⁵

2. On OWD's Measures on Storage, Retentions, and Disposal Procedure found under its Manual:

As discussed in the previous report, the Retention Records Table shows that the same is filled out with the relevant data existing in and being processed in OWD. The said table also illustrates who are the 'data subjects,' the means of storage of such data, location, security measures employed upon for protection, period of retention, and the manner of disposal. The means of storage, retention period, and disposal manner is no longer left to individual employees but already determined and documented as an attachment to the revised Manual.²⁶

3. On the Collection of Data Table and Data Inventory:

The Collection Data Table is filled out with relevant information such as the process owners (department involved in the collection and responsible persons), categories of the data subject, categories of personal data, the purpose for

²⁴ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 7 (a), (d), (f) (2012). Emphasis supplied.

²⁵ Final Enforcement Assessment Report, 26 November 2021, at 5, *in* CBP v. Orani Water District (NPC 2021) (pending).

²⁶ *Id.*

which data is collected, the mode of data collection, forms employed to collect, and the responsible person.²⁷

4. On Contact Details of the Data Protection Officer:

The OWD's Revised manual now designated a contact e-mail address (oraniwaterdistrictdataprivacy@gmail.com) specific to privacy concerns and questions.²⁸

5. On Consent Letter (Concessionaries):

Likewise, it is now clearly specified under the 'Consent Letter (Concessionaires)' portion the kinds of processing (applications for water service connections, reconnection, termination, billing, and payment) that Primewater Infrastructure Corporation conducts upon the shared data from OWD in place of the previous general phrase 'for any legitimate business purpose.'²⁹

6. On the Conduct of Training or Seminars for the DPO and OWD Personnel:

Lastly, the submission of the Certificate of Participation DPO Ace Level 1 Training Program for Mixed Sector issued to the key employees within its organization as proof of conduct of training fully satisfies the Order of the Commission.³⁰

Considering the foregoing, the Commission finds that OWD has, to the satisfaction of the Commission, rectified its Privacy Manual and Notices and has caused the attendance of its employees to a data privacy orientation.

WHEREFORE, premises considered, the Commission hereby finds that Orani Water District has sufficiently notified its affected data subjects and complied with the Decision dated 15 December 2017. This Commission hereby considers the matter **CLOSED**.

SO ORDERED.

²⁷ *Id.*
²⁸ *Id.* at 6.
²⁹ *Id.*
³⁰ *Id.*

City of Pasay, Philippines.
27 January 2022.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

JOHN HENRY D. NAGA
Privacy Commissioner

Copy furnished:

CBPCBP
Complainant

CDBJ
SRM

EFS*General Manager*
Orani Water District

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION**
GENERAL RECORDS UNIT
National Privacy Commission

N.I.H.

Complainant,

- versus -

WSQ MEDICAL CENTER,
represented by **N.W.W.E., DR.**
N.O. and DR. O.P.,

Respondents.

X-----X

NPC 16-005

*For: Violation of Data
Privacy Act of 2012*

RESOLUTION

LIBORO, PC.:

Before this Commission is a Compromise Agreement (CA) between the complainant N.I.H. (Complainant) and respondent WSQ Medical Center, as represented by N.W.W.E., Dr. N.O., and Dr. O.P. (collectively referred as Respondents).

Facts

On 06 November 2016, Complainant, through an email, filed a complaint against Respondents for violation of her right to access. In her Complaint, Complainant alleged that she asked for a copy of the medical records of her late brother, who died at the Intensive Care Unit of the WSQMC.

After the discovery conference and several hearings, parties received an Order from the Commission dated 06 December 2017 stating that the case will be submitted for resolution unless the parties submit their Joint-Settlement Agreement.

On 11 January 2018, the parties through their counsels filed before the Commission a Joint Manifestation dated 09 January 2018 asking for an extension of time to finalize and submit the Compromise Agreement, which was granted in the Order issued by the Commission dated 17 January 2018.

On 17 January 2018, the parties executed a Compromise Agreement, containing the following provisions:

xxx

2. Without admitting any claim or liability, and solely for the purpose of buying peace and amicably settling their dispute, the Parties agree to terms and conditions of this Compromise Agreement and to perform their respective obligations as outlined herein.

3. In consideration thereto, WSQ Medical Center, Dr. N.O. and Dr. O.P. shall tender to Ms. N.I.H., the total amount of THREE HUNDRED THOUSAND PESOS (P300,000.00), as full and final settlement of all claims of Ms. N.I.H. against WSQ Medical Center, Dr. N.O. and Dr. O.P., by reason of or arising from the confinement and treatment of S.H. at the WSQMC.

4. Ms. N.I.H. shall release and discharge, as she hereby releases and forever discharges Dr. N.O., Dr. O.P. and the WSQ Medical Center, its officers, employees, agents and representatives from any and all claim, demands, and/or causes of action of whatever nature arising from the case m or in relation to the confinement and treatment of S.H. at the WSQMC.

xxx

On 23 January 2018, the parties, through their counsels, submitted their Joint Motion to render judgment based on the Compromise Agreement.

On 01 March 2018, the following were submitted by the parties: (1) the Ex Parte Manifestation dated 27 February 2018; (2) the corrected copy of the Compromise Agreement due to several typographical errors on the document; and (3) the Check Voucher that was prepared and issued by the Respondents bearing the amount agreed upon.

Discussion

This Commission confirms the Compromise Agreement dated 27 February 2018 between the Complainant and the Respondents.

Section 25 of the National Privacy Commission Circular No. 16-04 provides that the Commission shall facilitate or enable settlement through the use of alternative dispute resolution processes.

After a thorough study and adjudication of the case on hand, the Commission finds that the Compromise Agreement dated 27 February 2018 by and between the Complainant and Respondent is not contrary to law, public policy, morals, or good customs.

In the case of *Municipal Board of Cabanatuan City v. Samahang Magsasaka, Inc.*,¹ the Court ruled that a compromise agreement is a contract between the parties, which if not contrary to law, morals, or public policy, is valid and enforceable between them.

With the foregoing, the Commission finds the executed Compromise Agreement dated 27 February 2018 by and between the Complainant and the Respondent as valid and enforceable.

WHEREFORE, in view of the foregoing, this Commission resolves to

CONFIRM the Compromise Agreement executed by and between N.I.H. and WSQ MEDICAL CENTER and DR. N.O. and DR. O.P. The case **NPC 16-005 - “N.I.H. vs. WSQ MEDICAL CENTER, represented by N.W.W.E., DR. N.O. and DR. O.P.”** is hereby considered CLOSED.

SO ORDERED.

Pasay City, Philippines;
10 September 2020.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

¹ *Municipal Board of Cabanatuan City v. Samahang Magsasaka, Inc.*, 62 SCRA 435 (1975).

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy

Commissioner Copy furnished:

N.I.H.
Complainant
t xxxxxx
xxxxxx
xxxxxxxxx

N.W.W.E.
DR. N.O.
DR. O.P.
Respondents
WSQ Medical
Center xxxxxxxxx
xxxxxxxxxx
xxxxxxxxxx

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION GENERAL
RECORDS UNIT
National Privacy Commission

A.N.M.,

Complainant,

-versus-

MDMC, INC.,

*Responde
nt.*

x

-----x

NPC 18-028
*FOR: Violation of
Data Privacy
Act of 2012*

LIBORO, P.C.:

RESOLUTION

This Resolution refers to the Complaint filed by A.N.M. (Complainant) against MDMC, Inc. (Respondent), for alleged violations of Republic Act No. 10173 (Data Privacy Act).

The Facts

On 25 September 2017, Complainant received a letter dated 07 September 2017 from MDMC, Inc. informing him that he won twenty thousand (20,000) Mabuhay Miles points. Attached to the letter is a claim form that Complainant must fill out and submit to R.C., branch marketing manager of MD Fairview. In compliance, Complainant submitted photocopies of his Philippine Airlines Mabuhay Card, Tax Identification Number Identification Card, voter's Identification Card, and MD Card. However, Complainant did not hear anything from Respondent despite numerous follow up for the past eight (8) months.

On 15 May 2018, Complainant filed a complaint against Respondent. He avers that the documents he submitted to Respondent contains sensitive personal information that might fall into the wrong hands and be used for purposes other than those he intended. Thus, as a precautionary measure, he appealed to the National Privacy Commission so that adequate protection may be accorded to the personal data that he submitted to Respondent.

On 14 March 2019, the parties were ordered to appear for discovery conference, with a reminder to the parties that the case will be deemed submitted for resolution should they fail to appear.

During the discovery conference, only Respondent appeared through counsel, Atty. M.R.A. Respondent manifested that the complaint should be dismissed outright for lack of merit, because the Complaint was only filed as a precautionary measure.

On 25 March 2019, Respondent filed its Formal Entry of Appearance and Manifestation with Motion to Dismiss on the ground of non- exhaustion of administrative remedies by the Complainant before filing the Complaint, non-compliance with formal requisites of a formal complaint, and for lack of merit since the Complaint contained no material allegation of any act or omission on the part of Respondent which violated Complainant's right to data privacy. Further, Respondent manifests that the twenty thousand (20,000) Mabuhay Miles points had already been credited to Complainant's account.

Issue

Whether Respondent processed the sensitive personal information of Complainant for an unauthorized purpose.

Discussion

The Commission hereby resolves to dismiss the instant the case.

NPC Circular 16-04¹ (Rules) provides that the National Privacy Commission, sua sponte, or persons who are the subject of a privacy violation or personal data breach, or who are otherwise personally affected by a violation of the Data Privacy Act (DPA), may file complaints for violations of the Act.

¹ Section 3, NPC Rules of Procedure

In this case, Complainant avers that the documents he submitted to Respondent contains sensitive personal information that might fall into the wrong hands and be used for purposes other than those he intended. Thus, as a precautionary measure, he appealed to the Commission so that adequate protection may be accorded to the personal data that he submitted to Respondent.

Justice Alicia Austria-Martinez, speaking for the Supreme Court, ruled that he who alleges a fact has the burden of proving it and a mere allegation is not evidence².

Similarly, in NPC 17-015, the Commission held that, “Complainant’s stand-alone allegation is not sufficient to file a complaint before the Commission because she is neither the subject of a privacy violation or personal data breach, or who is otherwise personally affected by a violation of the DPA. Put simply, Complainant does not have a legal standing to sue Respondent since she is not the affected data subject or was personally affected by a violation of the DPA.”

With the aforementioned provisions and pronouncement of the Commission, the burden lies on Complainant to prove whether or not Respondent committed a violation of the DPA.

After a thorough evaluation, the Commission finds that the Complaint was filed merely for a precautionary measure because he is worried that his personal information might fall into the wrong hands and might be used for purposes other than those he intended. Other than the allegation of eight (8) months delay of crediting the Mabuhay Miles points on his account, Complainant did not allege any wrongdoing on the part of Respondent that would result to a violation of the Data Privacy Act or involve a privacy violation or a personal data breach.

² Luxuria Homes Inc. vs. CA, GR No. 125986, Jan 28, 1999

Being that Complainant is neither the subject of a privacy violation or personal data breach, or is otherwise personally affected by a violation of the DPA, he does not have a legal standing to sue Respondent. The allegations based on mere suspicion that Complainant's personal information might be used for purposes other than those he intended is insufficient for any action by the Commission against Respondent.

In view of the foregoing, the Commission adjudged that the case be dismissed as there is no actual and justiciable controversy that warrants the attention of the Commission.

WHEREFORE, premises considered, the case of A.N.M. vs. MDMC, Inc. is hereby **DISMISSED** for lack of merit.

SO ORDERED.

Pasay City, Philippines;
21 May 2020.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commission

COPY FURNISHED:

A.N.M.
Complainant

MDMC, INC.
Respondent

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION**

GENERAL RECORDS UNIT
National Privacy Commission

CL,	Complainant,	NPC No. 19-030 (formerly CID Case No. 19-A-030) <i>For: Violation of the Data Privacy Act of 2012</i>
- versus		
-		
DDZ,	Respondent.	
X-----X		
DM,	Complainant,	NPC No. 19-030, NPC No. 19132 (formerly CID Case No. 19-B-132) <i>For: Violation of the Data Privacy Act of 2012</i>
- versus		
-		
DDZ,	Respondent.	
X-----X		

RESOLUTION

NAGA, D.P.C.:

For consideration of the Commission is the Motion for Reconsideration dated 11 September 2021 filed by CL and DM (Complainants) on the Decision dated 10 June 2021 which dismissed their Complaints against DDZ (Respondent) for lack of merit.

Facts

The Commission issued a Decision dated 10 June 2021, dismissing the Complaints filed by CL and DM, with the following dispositive portion:

WHEREFORE, all premises considered, this Commission resolves that the instant Complaints filed by CL and DM are hereby **DISMISSED** for lack of merit.

SO ORDERED.¹

Complainants filed a Motion to Suspend the Period of Filing of Pleadings dated 13 August 2021, seeking for the application of the Supreme Court Administrative Circular No. 56-2021 (SC Circular).²

On 02 September 2021, the Commission issued an Order denying the Motion to Suspend the Period of Filing of Pleadings. However, in the Order, the Commission granted Complainants a non-extendible period of five (5) days upon receipt of the Order to make the filing and service of necessary pleadings and motion.³

On 07 September 2021, Complainants filed a Manifestation that since the fifth day of the period it was given in the Order fell on 11 September 2021, a Saturday, they had until 13 September 2021 to submit their Motion for Reconsideration (Motion).⁴

On 13 September 2021, Complainants filed their Motion dated 11 September 2021.

In their Motion, Complainants stated that it is not clear how Respondent obtained a copy of their personal files and closed-circuit television (CCTV) footages of the MVP worksite.⁵ Complainants argued that Respondent readily proposed that he obtained it from SM and DMV through a legitimate request. However, no evidence was presented to show that such request was made. Further, the letter- request was omitted and no affidavit from SM and DMV was presented.⁶

Complainants then stated that no request appears in the records of the MVP office and that they were never informed that such request was processed by SM and DMV.⁷ Moreover, Complainants argued that they made the averment related to the database break-in by Respondent in their Complaints because they are unaware of any

¹ Decision, 10 June 2021 at p. 10. NPC 19-030 and NPC 19-132.

² Id. at p. 2.

³ Order dated 02 September 2021.

⁴ Id at p. 3.

⁵ Motion for Reconsideration dated 11 September 2021. At. p. 3.

⁶ Id.

⁷ Id.

purported request for copies of their passports made to the responsible officers of MVP.⁸

Complainants further submits that Respondent is not a public authority, did not act under compulsion by order of such public authority, and that the passports were not essential to the prosecution of any of Respondent's claims.⁹

Complainants, being aware of Respondent's allegation that the passports were obtained through a valid request from the previous officers of MVP, the said corporation through its authorized representative, AR instituted a Complaint dated 11 September 2020 against SM, DMV, and DDZ.¹⁰

Complainants stated that such Complaint was received and duly acknowledged by the Commission's Complaints and Investigation Division (CID).¹¹ However, despite the acknowledgement of receipt and promise to review the Complaint, it remains to be undocketed and has not been acted upon by the Commission.¹²

Complainants filed a Motion to Consolidate on 16 December 2020. Additionally, they stated that more than two (2) months have passed without any Resolution on the Motion, they filed a Motion to Resolve on the issue of consolidation dated 24 February 2021.¹³ However, according to Complainants, the Commission did not act on these two (2) pending Motions and that it seems that the pending Motions and verified Complaint filed by MVP were not considered when the Commission rendered the Decision dated 10 June 2021.¹⁴

Complainants emphasized that the consolidation of the cases are important since it would expedite the resolution of the issue. Complainants added "if the cases were consolidated, DMV and SM could have been summoned and shed light on the factual

⁸ Id.

⁹ Id.

¹⁰ Id. at p. 5.

¹¹ Id.

¹² Id.

¹³ Id.

¹⁴ Id.

circumstances claimed by Respondent DDZ.”¹⁵ Further, they stated that the proper resolution of this case will be incomplete, unfair, and unjust since SM and DMV are not allowed to be made part of the case and that the situation calls for a proper remand for investigation.¹⁶

On Respondent’s reliance on Section 13(f) of the Data Privacy Act (DPA) of 2012, Complainants argued that attaching the passports to Respondent’s Complaint-letter was not necessary since Complainants being Australian citizens without working visas is not relevant to the criminal and labor cases then existing.¹⁷ The nationality or citizenship is also neither an essential element of the crimes mentioned nor would constitute part of the labor case for dismissal. Complainants argued that the virtual nexus between Respondent and Complainants with regard to the contents of the passports does not exist and therefore fail the test provided by NPC Case No. 17-018.¹⁸

Moreover, according to Complainants it was Respondent, together with his cohorts, SM and DMV, who should be guilty of theft of Complainants’ sensitive personal information.¹⁹

Complainants also stated that the Office of the Prosecutor, Department of Labor and Employment (DOLE), Clark Development Corporation (CDC), and the Bureau of Immigration (BI) did not ask for the documents.²⁰

The exemption in processing sensitive personal data only applies to the Government entities as part of their function which cannot be said on the part of Respondent since he is not public office or functionary and thus, cannot claim such exemption as a privilege.²¹

Complainants cited Section 19 of the DPA which states that “the personal information shall be held in strict confidentiality and shall be used only for the declared purpose”, but since Complainants’ have not seen a copy of Respondent’s request, they do not know for what

¹⁵ Id. at p. 6.

¹⁶ Id.

¹⁷ Id at p. 7

¹⁸ Id.

¹⁹ Id. at p. 8.

²⁰ Id. at. p. 9

²¹ Id. at p. 10

purpose his request was made.²² Further, they argued that there is no transparency in the processing of their sensitive personal information.

Moreover, Complainants stated “the Personal Privacy Controller [sic] of the MVP is not even aware that a request was made by Respondent.”²³ According to Complainants, it was SM and DMV who processed the sensitive personal information, without informing the data subjects and without authority to do so. Complainants stated that DDZ, SM, and DMV connived to steal their sensitive personal information for a malicious purpose.²⁴

Complainants stated that there is also no legitimate purpose since Respondent did not provide the request made to MVP which shall state the purpose of processing. Further, there is also no proportionality since the information processed was already with the agencies concerned or within the grasp of government agencies, Respondent cannot borrow government’s rights and privileges.²⁵

According to Complainants, Respondent should provide the evidence of the valid request for processing the information. Respondent has the burden of proving, as a matter of defense, that he is within the exception in the statute creating the offense. Complainants stated that like all matters of defense, the burden of establishing such claim is on the party relying or invoking it.²⁶

They stated that there is no evidence to support Respondent’s supposed claim of a valid request existed. However, there is ample evidence that there were no requests appearing in the MVP records.²⁷

Based on the Data Protection Officer (DPO) report by Atty. EV, the internal investigation shows that no consent was obtained from the management for the release of Complainants’ documents. There are also no copies of the request claimed by Respondent in the files of MVP.²⁸ Complainants alleged that the intrusion to the data banks of

²² *Id.* at p. 11.

²³ *Id.* at. p. 12.

²⁴ *Id.* at p. 13

²⁵ *Id.*

²⁶ *Id.* at p.14.

²⁷ *Id.* at p. 17.

²⁸ *Id.* at p. 17-18.

MVP was accomplished in connivance with SM and DMV since they have access even without authority and without informing the data subjects of the processing.²⁹

Further, if a valid request exist, it is within the capacity of Respondent to produce a copy of such request.³⁰

Complainants prayed then that: (a) Decision dated 10 June 2021 be reconsidered and appropriate remedies and penalties be imposed against Respondent DDZ; and (b) Alternatively, that the cases be consolidated with the undocketed case filed by MVP as the issues are intimately related to each other. Should the Commission deem it fit and proper, to remand the case for proper determination with proper issuance of summons to DMV and SM so they can be held responsible for the violation of the DPA.³¹

On 17 September 2021, the Commission issued an Order, ordering Respondent DDZ, to file a Comment on the Motion for Reconsideration dated 11 September 2021 filed by Complainants and to submit the same within fifteen (15) days from receipt of the Order.³²

On 22 October 2021, Respondent filed a Motion to Admit Comment together with his Comment.³³

In his Comment, Respondent argued that Complainants' arguments in their Motion are trivial and inconsequential and do not affect the substantial and material discussions of the Commission.³⁴

According to Respondent, Complainants attached as Annex "A" in their Motion, a purported complaint which is totally unrelated to the case decided by the Commission and deserves no consideration to the resolution of the said Motion.³⁵

²⁹ *Id.* at p. 18.

³⁰ *Id.*

³¹ *Id.* at p. 20.

³² Order dated 17 September 2021.

³³ Motion to Admit Comment and Comment dated 22 October 2021.

³⁴ *Id.* at p. 1.

³⁵ *Id.*

Respondent also stated that the separate Complaints arose from the same set of facts, arguments, and evidence. However, Complainants opted to initiate a Complaint separately to harass and vex Respondent.³⁶ Further, Respondent stated “the undocketed Complaint attached as Annex “A”, also falls to the same malicious story. These only proved Respondent’s claim that the instant cases were filed to unjustly annoy Respondent.”³⁷

Respondent reiterated his allegations that the Complaints were being utilized by Complainants to have leverage over Respondent’s labor case. Since the Labor Arbiter ruled in favor of Respondent on the said labor case, Respondent stated that Complainants will hardly but uselessly pursue these cases, or any other cases against Respondent to get even.³⁸

In addition, Respondent stated that not only that the Complaints were vexatious, but also absurd. According to Respondent, first, Complainants themselves disclosed their passport information with the Commission when they filed their Complaints.³⁹ Second, following to their line of thinking, Complainants are guilty of the same charge of violation of the DPA considering that they disclosed sensitive personal information of Respondent, particularly his Alien Certificate of Registration as attachment to their Complaints.⁴⁰

On Complainants’ allegation that he broke into MVP’s database, Respondent stated that Complainants solely relied on surmises and conjectures which are wholly unsupported by legal and factual bases.⁴¹

Respondent argued that like any other cases, Complainants have the burden of proof to show that Respondent violated the DPA.⁴² He further stated that Complainants failed to provide substantial evidence that Respondent knowingly and unlawfully broke into MVP’s database. Complainants also did not show that there was an actual storage of scanned copies of passports. Moreover, the facilities of MVP are covered by CCTV cameras but Complainants did not

³⁶ Id. at p. 2

³⁷ Id.

³⁸ Id.

³⁹ Id.

⁴⁰ Id.

⁴¹ Id.

⁴² Id. at p. 3.

attach video clip or screen capture to prove their claims.⁴³ Respondent stated that he fully subscribe to the findings of the Commission that he cannot be held liable for the violation of Section 29 of the DPA (Unauthorized Access or Intentional Breach).⁴⁴

Further, Respondent stated that he agrees to a certain extent on Complainants' allegations that passport contains personal and sensitive personal information.⁴⁵ However, he reiterated that such information is excluded from the coverage of the DPA pursuant to Section 4(e) of the DPA. Additionally, he stated that the processing of information contained in the passport is permitted under Section 12(e) and (f) of the DPA, and exempted under Section 13(e) of the DPA.⁴⁶

He also reiterated that the information of Complainants were necessary in order for the government agencies to perform their statutorily mandated functions.⁴⁷

Moreover, Respondent stated "Complainants argued that Respondent's processing of information were not exempted since it was not 'necessary' to protect his claim or interest. Complainants argued that the word 'necessary' connotes that the sensitive information that was processed should be needed to protect the claim or interest of the party using that information. However, the exemption that Respondent and the Honorable Commission pointed out is found under the phrase 'or when provided to government or public authority' of Section 13(f)."⁴⁸

He also stated that he only processed Complainants' information with the government agencies which were tasked to enforce laws and protect lawful rights and interests of natural or legal persons, the Philippine Government, and the Filipino citizens.⁴⁹

Respondent stated that his legitimate interest was to report the illegal acts of Complainants, and although he is not a Personal Information

⁴³ Id. at p. 4

⁴⁴ Id. at p. 4 to 5.

⁴⁵ Id. at p. 5.

⁴⁶ Id.

⁴⁷ Id. at p. 7.

⁴⁸ Id.

⁴⁹ Id.

Controller (PIC), his processing is permitted as a “third party” pursuant to Section 13(f) of the DPA.⁵⁰ Further, Respondent stated that he processed the information in good faith pursuant to his moral obligation to promptly report on what he believes is an illegal act under Philippine Laws.⁵¹

Respondent prays that Complainants’ Motion for Reconsideration dated 11 September 2021 be denied for the lack of merit.⁵²

Issues

Whether the Motion for Reconsideration dated 11 September 2021 on the Decision dated 10 June 2021 filed by Complainants should be granted.

Discussion

The Commission partially grants the Motion for Reconsideration filed by Complainants.

The Commission finds that in order to properly resolve the case, it shall first solely focus on the procedural issues raised by Complainants. The Commission shall not delve on the substantive issues raised by both parties in their respective pleadings until such time that Complainant’s pending Motions have been properly resolved.

In its Motion, Complainants stated that MVP, through its authorized representative, AR, instituted a Complaint dated 11 September 2020 against SM, DMV, and DDZ which was received and duly acknowledged by the Commission’s CID. Complainants attached in their Motion as Annex “A”, the copy of the Complaint.⁵³ They also attached as Annex “B”, the copy of CID’s email stating that the Complaint has been received and will be reviewed shortly.⁵⁴

⁵⁰ Id. at p.7 to 8.

⁵¹ Id. at p. 8 to 9.

⁵² Id. at p. 9

⁵³ Motion for Reconsideration dated 11 September 2021. At p. 23.

⁵⁴ Id. at p. 52.

Also, a Motion to Consolidate was filed by Complainants on 16 December 2020 stating that their Complaints and the Complaint filed by MVP contains issues are intimately related to each other. Additionally, since the Commission has yet to issue a resolution on the Motion to Consolidate, Complainants filed a Motion to Resolve on the issue of consolidation dated 24 February 2021.

However, Complainants stated that the Commission did not act on these two (2) pending Motions and that the pending Motions and verified Complaint filed by MVP were not considered when the Decision dated 10 June 2021 was rendered.⁵⁵

In terms of procedural issues, the resolution of the Motion to Consolidate and Motion to Resolve is a material fact that needs to be considered by the Commission. Further, the Commission notes that addressing the pending Motions filed by Complainants is imperative in the holistic resolution of the case, given that the Complaints filed by CL and DM and the Complaints filed by MVP are alleged to have similar and interrelated issues that must be reviewed and resolved by the Commission.

Moreover, in this case, the Commission deems that the proper resolution of the pending Motions shall be addressed by the Commission. Thus, the Commission finds that the Motions filed by Complainants shall be remanded to the Complaints and Investigation Division (CID) of the Commission to resolve whether the Complaints filed may be consolidated, as allowed by Section 7 of the NPC Circular No. 2021-01 (2021 NPC Rules of Procedure), *viz*:

SECTION 7. Consolidation of cases. – Except when consolidation would result in delay or injustice, the NPC may, upon motion or in its discretion, consolidate two (2) or more complaints involving common questions of law or fact and/or same parties.⁵⁶

Further, the Commission shall await for the Resolution of the CID on the pending Motions filed by Complainants before fully deciding on

⁵⁵*Id.*

⁵⁶ Section 7 of the NPC Circular No. 2021-01

Complainants' Motion including its substantive issues. Hence, the Commission partially grants Complainants' Motion for Reconsideration.

As to the Motion to Admit Comment and the attached Comment dated

22 October 2021 filed by Respondent, the Commission notes that Respondent received the Commission's Order dated 17 September 2021 on 30 September 2021. Therefore, Respondent has fifteen (15) days from receipt of the Order or until 15 October 2021 to submit his Comment. However, Respondent only submitted his Comment on 22 October 2021 which is beyond the allowed period. Hence, it was filed out of time.

Nonetheless, in consideration of substantial justice, the Commission resolves to admit Respondent's Motion to Admit Comment and Comment despite being filed out time.

WHEREFORE, premises considered, this Commission resolves to **PARTIALLY GRANT** the Motion for Reconsideration dated 11 September 2021 filed by Complainants CL and DM.

SO ORDERED.

City of Pasay, Philippines.
11 November 2021.

SGD.

JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

SGD.

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

CL
Complainant

DM
Complainant

MJRVLO
Counsel for Complainants

DDZ
Respondent

PMB
Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

JO,

Complainant,

NPC 19-278

-
versus-

MSM, Inc.

Respondent.

For: Violation of
the Data Privacy
Act of 2012

X-----X

RESOLUTION

NAGA, P.C.;

Before the Commission is a Motion for Reconsideration dated 15 May 2022 filed by JO on the Commission's Decision dated 31 March 2022.

Facts

JO, through a Complaints-Assisted Form dated 27 March 2019, filed a case against the Respondent, MSM, Inc (MSMI).¹ On 31 March 2022, the Commission issued a Decision dismissing the complaint for lack of merit.²

The Decision was served via email to both parties on 29 April 2022.³ Subsequently, JO submitted an unsigned Motion for Reconsideration on 16 May 2022 via email.⁴ In the email, JO stated that, "I will send physical copy personally (signed),"⁵ and attached his unsigned Motion.⁶ Based on the records, JO filed a signed physical copy of his Motion on 17 May 2022.⁷

¹ Complaints-Assisted Form dated 27 March 2019 of JO.

² *JO vs MSM, Inc.*, NPC 19-278, Decision dated 31 March 2022.

³ See Electronic mail dated 29 April 2022 to JO and MSM, Inc.; Electronic Mail Delivery Receipts.

⁴ Motion for Reconsideration dated 15 May 2022 (unsigned) of JO.

⁵ Electronic Mail dated 16 May 2022 from JO.

⁶ *Id.*

⁷ Motion for Reconsideration dated 15 May 2022 (signed) with stamp receipt of JO.

In his Motion, JO claims that there was no “cogent reason” for the dismissal of his complaint.⁸ He states that “the complaint itself has shown an exceptionally good cause that indeed respondents unquestionably, deliberately and seriously violated the right(s) of the complainant and complaint itself involves a serious violation or wanton breach of the Data Privacy Act.”⁹

He claims that there was bias or partiality in the dismissal of his complaint. To support this claim, JO cites an alleged incident in the course of the preliminary investigation:

The Investigating Officer have already decided the favorable resolution of the complaint to the respondent(s) since, quoted thereat the following remarks, “MADEDEHADO KA DITO (REFERRING TO NPC) KUNG WALA KANG ABOGADO”
(sic)¹⁰

JO also argues that MSMI has committed data privacy violations, especially by MSMI’s alleged admission that it was using “the account name and code of complainant who has effectively resigned since 31 December 2018.”¹¹ He further contends that MSMI should be penalized under Section 33 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA).¹² Lastly, JO claims that MSMI could have performed its tasks manually, but opted to breach his personal data.¹³

In response, MSMI filed an Opposition (to the Motion for Reconsideration dated 15 May 2022) dated 01 June 2022.¹⁴ MSMI argues that “[JO’s] Motion should be outrightly denied for being *pro forma* inasmuch as it fails to point out specifically the findings or conclusions of the Commission in its Decision which are not supported by the evidence or which are contrary to law...”,¹⁵ and thereafter citing Rule 37 of the 2019 Rules of Civil Procedure.¹⁶

⁸ *Id.*, at pp. 1-2.

⁹ *Id.*, at p. 2.

¹⁰ *Id.*

¹¹ Motion for Reconsideration dated 15 May 2022 of JO, at p. 2.

¹² *Id.*

¹³ *Id.*

¹⁴ Opposition (to the Motion for Reconsideration dated 15 May 2022) dated 01 June 2022 of MSM, Inc.

¹⁵ *Id.*, at ¶ 2.

¹⁶ *Id.*

MSMI also counters that JO “fails to provide any iota of evidence to show that this Honorable Commission exhibited any bias or partiality in its Decision other than to reference the period within which the said Decision was issued and to quote the Investigating Officer.”¹⁷ According to MSMI, the alleged statement, if true, also does not show bias but “only reflects the Investigating Officer’s prudent act of advising Complainant of the possibility of engaging counsel.”¹⁸ Even if this showed bias or partiality, MSMI claims that it is not one of the grounds for a motion for reconsideration.¹⁹

MSMI cites the Decision in claiming that there was no privacy violation, in that JO’s email and Philippine Overseas Employment Administration (POEA) code are company-owned assets, and not owned by JO.²⁰ Thus, MSMI prays that the Commission deny JO’s Motion.

Issue

Whether the Motion for Reconsideration merits the reversal of the Decision dated 31 March 2022.

Discussion

The Commission denies JO’s Motion for Reconsideration.

I. The Decision has already attained finality. JO’s period to file a motion for reconsideration has already lapsed.

Rule VII, Section 30 of the NPC Circular 2016-04 or the Rules of Procedure (2016 NPC Rules of Procedure) states:

¹⁷ *Id.*, ¶ 4.

¹⁸ Opposition (to the Motion for Reconsideration dated 15 May 2022) dated 01 June 2022 of Multinational Ship Management, Inc., ¶ 4(b).

¹⁹ *Id.*, ¶ 4(c).

²⁰ *Id.*, ¶ 7. See *JO vs MSM, Inc.*, NPC 19-278, Decision dated 31 March 2022, at p. 12.

SECTION 30. Appeal. – The decision of the National Privacy Commission shall become final and executory fifteen (15) days after the receipt of a copy thereof by the party adversely affected. One motion for reconsideration may be filed, which shall suspend the running of the said period. Any appeal from the Decision shall be to the proper courts, in accordance with law and rules.²¹ (Emphasis supplied)

Likewise, Rule VIII, Section 4 of NPC Circular No. 2021-01, otherwise known as the 2021 NPC Rules of Procedure (2021 NPC Rules) states:

SECTION 4. Appeal. – The decision of the Commission shall become final and executory fifteen (15) calendar days after receipt of a copy by both parties. One motion for reconsideration may be filed, which shall suspend the running of the said period. Any appeal from the Decision shall be to the proper courts, in accordance with law and rules.²²

The Decision dismissing the case was served to the parties via email on 29 April 2022. JO, in his Motion, claims that he received the Decision on 10 May 2022.²³ Based on the records, this was the day he received the physical copy of the Decision after it was sent through private courier.²⁴

Nevertheless, it should be noted that electronic service is allowed under Rule III, Section 6 of the NPC Rules.²⁵ Also, there was no notification or other proof that there were problems with the electronic service.²⁶ JO even sent an email attaching his unsigned Motion by replying to the Commission's email which electronically served him the Decision.²⁷

Thus, the Commission finds that the electronic service of its Decision on 29 April 2022 was valid. Consequently, the Decision already became final on 14 May 2022, which was the fifteenth day from receipt

²¹ National Privacy Commission, Rules of Procedure of the National Privacy Commission, NPC Circular No. 16-04, Rule VII, § 30 (15 December 2016) (2016 NPC Rules of Procedure)

²² National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission, NPC Circular No. 2021-01, Rule VIII, § 4 (28 January 2021) (2021 NPC Rules of Procedure).

²³ Motion for Reconsideration dated 15 May 2022 of JO, at p. 1.

²⁴ As per LBC tracking number.

²⁵ 2021 NPC Rules of Procedure, Rule III, § 6.

²⁶ See Electronic mail delivery receipts.

²⁷ Electronic mail dated 16 May 2022 of JO.

of the Decision, since there was no appeal filed within the fifteen (15)- day period.

JO electronically mailed his unsigned Motion on 16 May 2022. However, under Rule 7, Section 3 of the 2019 Rules of Civil Procedure (which finds suppletory application in this case),²⁸ **“[e]very pleading and other written submissions to the court must be signed by the party** or counsel representing him or her.”²⁹ JO, as the party filing the Motion, did not follow this clear obligation. It was only on 17 May 2022 when the Commission received a physical and signed copy of his Motion. Moreover, it bears emphasis that regardless whether JO filed his Motion on 16 May 2022 or 17 May 2022, the Decision had already attained finality.

Even if the Commission were to consider the unsigned Motion as duly filed, JO’s period to file a motion for reconsideration had already lapsed since the Decision was already final. On this ground alone, the Commission has sufficient cause to deny JO’s Motion.

II. On the merits, JO did not provide any substantial or adequate ground to reverse the Decision.

Setting aside the procedural infirmity, the Commission still finds that the Decision must be upheld. JO has not shown any substantial or adequate ground that would merit the reversal of the Decision.

JO does not explicitly state that the Commission is biased. His Motion does not even cite any particular statement from the Decision that would be indicative of partiality. However, he claims that during the preliminary investigation proceedings, the Investigating Officer “already decided the favorable resolution of the complaint to the respondent(s)”³⁰ due to the alleged statement “MADEDEHADO KA DITO (REFERRING TO NPC) KUNG WALA KANG ABOGADO.”³¹

²⁸ See 2021 NPC Rules of Procedure, Rule XII, § 8.

²⁹ 2019 Rules of Civil Procedure, Rule VII, § 3. (Emphasis supplied)

³⁰ Motion for Reconsideration dated 15 May 2022 of JO, at p. 2.

³¹ *Id.*

The Commission view allegations of bias seriously given that the National Privacy Commission is an independent body mandated to administer and implement the DPA.³² Taking into consideration its role, the Commission finds that JO has not proven that the Decision is tainted with bias against him.

In fact, in resolving JO's complaint, the Commission even exercised its authority to rule on the merits, rather than dismissing the complaint outright for non-exhaustion of remedies based on Section 4(a) of NPC Circular 16-04. To quote the Decision:

1. The Commission exercises its authority to resolve the case on the merits.

MSMI contends that the case should be dismissed since JO did not prove that he complied with Section 4(a) of NPC Circular No. 16-04, also known as the 2016 NPC Rules of Procedure.

In response, JO claims that after resigning, he immediately informed the company to refrain from accessing his personal information.

xxx

Based on the record, JO has not concretely provided evidence that it has complied with Section 4(a) of NPC Circular No. 16-04, since there is no proof that he informed MSMI, in writing, about the alleged privacy violation. Other than his allegations stated in his various pleadings before the Commission, JO did not attach any letter or other written correspondence to MSMI relating to the alleged privacy violation. **Thus, he did not provide substantial evidence that will lead the Commission to conclude that he complied with Section 4(a) of NPC Circular No. 16-04.**

Nevertheless, the Commission exercises its authority to waive the requirement of exhaustion of administrative remedies, based on the last paragraph of Section 4 of the 2016 Rules of Procedure.

JO's allegations, if substantially proven, may lead the Commission to conclude that there was a serious violation of the DPA. The allegations also show that there may be serious risk of

³² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes, [Data Privacy Act of 2012], Republic Act No. 10173, Chapter II, § 7 (2012).

harm to JO, given that the emails he provided allegedly show acts which he did not do, but may be liable for.

Thus, the Commission finds it appropriate to exercise its authority to resolve the case on the merits.³³ (Emphases supplied, citations omitted.)

The Commission could have just resolved to dismiss outright JO's complaint simply because he failed to prove that he informed MSMI in writing about the alleged privacy violation in order for it to appropriately act on the matter.³⁴ Instead, it approached the case from the lens of substantial justice by assessing JO's complaints based on the merits of his case. These actions are inconsistent with claims of bias or partiality against JO.

Further, regardless of the propriety of the Investigating Officer's alleged statement, the Decision was made only after the Commission scrutinized each party's submissions, evidence, and the law. The Commission ultimately decides on the matter, independent of the recommendations of the investigating officer, since "[t]he Commission shall review the evidence presented, including the Fact-Finding Report and supporting documents."³⁵ Though his complaint was dismissed, this in itself does not automatically prove that there was bias.

JO also repeats his claim that MSMI committed privacy violations when it "[used] the account name and code of complainant who has effectively resigned since 31 December 2018... There was a categorical admittance that the e-mail was provided for by the company (respondents), hence, bolster the fact that it is still being wantonly utilized by the company even after the complainant (data subject) effectively resigned since December 31, 2018 by another person. (*sic*)".³⁶ He also claims that MSMI should be penalized for Section 33 of the DPA to act as deterrence for those similarly inclined to violate the law or commit data breaches.³⁷

³³ *JO v. MSM, Inc.*, NPC 19-278, Decision dated 31 March 2022, at pp. 9-11.

³⁴ See National Privacy Commission, Rules of Procedure, NPC Circular No. 16-04, § 4(a) (15 December 2016).

³⁵ 2021 NPC Rules of Procedure, Rule VIII, § 1.

³⁶ Motion for Reconsideration dated 15 May 2022 of JO, at p. 2.

³⁷ *Id.*

The Commission has already extensively discussed JO's contentions in its Decision. Further, the Commission finds that there are no new material facts or information presented by JO in his Motion that would warrant the reversal of the Commission's Decision.

As explained in the Decision, the POEA code is a company asset and cannot be considered as part of JO's personal information. While JO's company-issued email indicates his name, its use after his resignation does not automatically equate to a violation of the DPA.

MSMI had a legitimate interest to continue using the POEA Account to access the Sea-based e-Contracts System (SBECS). MSMI's interest stems from POEA Memorandum Circular No. 06, series of 2018, which established the mandate for licensed manning agencies, like MSMI, to use POEA's web-based facility for its business processes with the agency.³⁸

MSMI also proved that it timely informed POEA about JO's resignation, and that it had to rely on POEA in order for MSMI to gain access to SBECS.³⁹

Lastly, the Commission finds that JO failed to justify why MSMI should be penalized under Section 33 of the DPA "[a]s a deterrent to others who are similarly inclined to commit such serious Data Privacy Violations or Personal Data Breach (*sic*)."⁴⁰

Section 33 of the DPA provides:

SEC. 33. Combination or Series of Acts. – Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).⁴¹

³⁸ Philippine Overseas Employment Administration, Memorandum Circular No. 06, series of 2018, New Procedure for Online Registration of Seafarers and Seabased e-Contracts System (SBECS).

³⁹ *JO vs MSM, Inc.*, NPC 19-278, Decision dated 31 March 2022, at p. 14; see Motion to Dismiss dated

02 July 2019 of Multinational Ship Management, Inc., Annex "F".

⁴⁰ Motion for Reconsideration dated 15 May 2022 of JO at p. 2.

⁴¹ Data Privacy Act of 2012, Chapter VIII, § 33.

JO has not proven that MSMI is liable for violating any of Sections 25 to 32 of the DPA, much more be penalized for a combination or series of acts meriting the application of Section 33 of the law.

Indeed, after reviewing the records and considerably weighing the evidence and arguments of both parties, the Commission finds no reason to reverse its Decision.

WHEREFORE, premises considered, the Motion for Reconsideration is **DENIED**. The Decision dated 31 March 2022 is hereby **AFFIRMED**.

SO ORDERED.

City of Pasay,
Philippines. 16 June
2022.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
DUG CHRISTOPHER B. MAH
Deputy Privacy Commissioner

(Inhibited)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

JO
Complainant

MSM, INC.
Respondent

ATTY. FT
Counsel for Respondent

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

RPR,

Complaint,

NPC 19-438

-
versus-

For: Violation of
the Data Privacy
Act of
2012

EDUKASYON.PH,

Respondent.

X-----X

RESOLUTION

AGUIRRE, D.P.C.;

Before the Commission is a complaint filed by RPR for a possible personal data breach committed by Edukasyon.ph (Edukasyon) when it emailed a “thank you letter” to all the participants of one of its events.

Facts

Rufino participated in the Amazon Web Services Siklab Pilipinas Online Conference (Conference) co-organized by Edukasyon and held in 2019.¹

On 06 June 2019, the National Privacy Commission (NPC) received RPR’s Complaint-Assisted Form.² RPR alleged that after the Conference, Edukasyon sent a “thank you letter” through email in which all participants were entered and exposed in the email field “To:”.³ He further alleged that the email contained a Dropbox link that points to a zip file.⁴ When he opened the zip file, it had the

¹ Final Enforcement Assessment Report, Enforcement Division, 17 August 2022, *in* RPR v. Edukasyon.ph NPC 19-438 (NPC 2022).

² Complaints Assisted Form, 06 June 2019, *in* RPR v. Edukasyon.ph NPC 19-438 (NPC 2019).

³ *Id.* at 3.

⁴ *Id.* at 5.

names and corresponding certificates of one hundred and three (103) participants, including himself.⁵

RPR contended that Edukasyon violated Sections 25, 26, 29, 32, 33, and 35 of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).⁶ RPR prayed for a fine to be imposed and a cease and desist order to be issued against Edukasyon.⁷

On 12 September 2019, the parties were ordered to appear before the Commission to confer for discovery on 02 October 2019.⁸

On 02 October 2019, an Order was issued directing Edukasyon to file its responsive comment to the complaint within ten (10) days from receipt of the Order, while RPR was ordered to file its reply within ten (10) days from receipt of Edukasyon's comment.⁹

Edukasyon submitted its Response to the Complaint dated 10 October 2019.¹⁰ Edukasyon stated that the personal data involved is limited to the names and email addresses of the participants, which in its view "are not of a particularly sensitive nature."¹¹ Edukasyon argued that "[t]he file of all certificates with full names served the same purpose as university entrance exam passer websites, or board exam passer announcements, where all full names of participants in the classroom setting are published online to the public."¹²

On 03 February 2022, the Commission issued an Order directing Edukasyon to individually notify the participants affected by the personal data breach and to submit its Security Incident Management Policy.¹³ The dispositive portion of the Order provides:

WHEREFORE, premises considered, the Commission **ORDERS** Edukasyon.ph to submit its Security Incident Management Policy and to notify its affected data subjects of the breach and

⁵ *Id.* at 5.

⁶ *Id.* at 3-4.

⁷ *Id.* at 6-8.

⁸ Order to Confer for Discovery, 12 September 2019, *in* RPR v. Edukasyon.ph, NPC 19-438 (NPC 2019).

⁹ Order, 02 October 2019, *in* RPR v. Edukasyon.ph, NPC 19-438 (NPC 2019).

¹⁰ Respondent's Response to the Complaint, 10 October 2019, *in* RPR v. Edukasyon.ph, NPC 19-438 (NPC 2019).

¹¹ *Id.*

¹² *Id.*

¹³ Order, 03 February 2022, *in* RPR v. Edukasyon.ph, NPC 19-438 (NPC 2022).

submit proof of notification thereof to the Commission within a **non-extendible period of thirty (30) days** from its receipt of the Order.

SO ORDERED.¹⁴

Thus, the Commission shall determine Edukasyon's Compliance with the Order dated 03 February 2022.

Issue

Whether Edukasyon sufficiently complied with the Order dated 03 February 2022.

Discussion

Section 18 (D) of NPC Circular 16-03 (Personal Data Breach Management) provides:

Section 18. *Notification of Data Subjects.* The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:

...

D. *Form.* Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.

The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the

¹⁴ *Id.*

personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.¹⁵

Whenever a personal data breach occurs, the personal information controller (PIC) shall identify the data subjects who are affected by the breach and shall notify all of them individually using secure means of communication. In this case, Edukasyon, as the PIC, should individually notify all affected data subjects through secure means of communication, whether written or electronically.

On 17 July 2022, Edukasyon submitted its Entry of Appearance with Compliance to the Order dated 03 February 2022.¹⁶ Edukasyon stated that in compliance with the Order, “individual emails were sent to each of the respective participants of the Online Conference on 13 July 2022.”¹⁷

RPR alleged that the names of one hundred and three (103) participants with corresponding certificates were exposed to third parties.¹⁸ The NPC’s Enforcement Division (EnD) assessed Edukasyon’s Entry of Appearance with Compliance (Initial Compliance) as incomplete.¹⁹ The EnD reported that Edukasyon sent its individual notification of the breach through email wherein Edukasyon attached its proof of individual notification that contained merely ninety-one (91) email addresses in its list of recipients of the notification breach.²⁰ Thus, the EnD issued a Compliance Letter dated 25 July 2022 directing Edukasyon to:

- A. Complete participants and their email addresses who attended the [Conference], to check if all participants were actually included in the email notifications made by respondent; and

¹⁵ National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16- 03], § 18 (D) (15 December 2016).

¹⁶ Respondent’s Entry of Appearance with Compliance to the Order dated 03 February 2022, 07 July 2022, in Rainier P. Rufino v. Edukasyon.ph, NPC 19-438 (NPC 2022).

¹⁷ *Id.* at 3.

¹⁸ Complaints Assisted Form, 06 June 2019, at 5, in RPR v. Edukasyon.ph NPC 19-438 (NPC 2019).

¹⁹ Final Enforcement Assessment Report, Enforcement Division, 17 August 2022, in RPR v. Edukasyon.ph NPC 19-438 (NPC 2022).

²⁰ *Id.* at 4.

- B. Provide the status of the remaining notifications needed to the participants who are not included in Annex G of said Compliance.²¹

On 08 August 2022, the NPC, through the EnD, received Edukasyon's Supplemental Compliance.²² Edukasyon explained that only seventy-eight (78) participants, instead of ninety-one (91) participants, were actually notified of the personal data breach.²³ From the seventy-eight (78) participants notified as reported in Edukasyon's Initial Compliance, some of the participants had inputted multiple email addresses.²⁴ As such, the multiple email addresses caused the discrepancy in the number of actual participants notified.²⁵ In Edukasyon's Initial Compliance, there were thirteen (13) surplus breach notification emails sent to the same set of participants.²⁶

Since only seventy-eight (78) participants were notified by the initial breach notification emails, Edukasyon still had to notify the remaining twenty-five (25) participants to complete the one hundred and three (103) participants who were affected by the personal data breach. Edukasyon attached its proof of notification sent to the remaining twenty-five (25) participants via "BCC" on 04 August 2022, thus completing the list of sending individual breach notification to the affected data subject.²⁷

Edukasyon was also ordered to submit its Security Incident Management Policy. Section 4 of NPC Circular 16-03 (Personal Data Breach Management) provides:

Section 4. *Security Incident Management Policy.* A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure:

²¹ Enforcement Division Compliance Letter, 25 July 2022, in *RPR v. Edukasyon.ph* NPC 19-438 (NPC 2022).

²² Respondent's Supplemental Compliance to the Compliance Letter dated 25 July 2022, 08 August 2022, in *Rainier P. Rufino v. Edukasyon.ph*, NPC 19-438 (NPC 2022).

²³ *Id.* at 3-4.

²⁴ *Id.* at 3-4.

²⁵ *Id.* at 3-4.

²⁶ *Id.* at 3-4.

²⁷ *Id.* at 4 & Annex D.

A. Creation of a data breach response team, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach;

B. Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident;

C. Implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system;

D. Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach; and

E. Compliance with the Act, its IRR, and all related issuances by the Commission pertaining to personal data breach notification.²⁸

In its compliance with the directive to submit its Security Incident Management Policy, Edukasyon attached its Incident Response Program that it implemented in October 2018.²⁹ The EnD assessed the submission of Edukasyon:

Here, the respondent's Security Incident Management Policy developed a process and/or procedure that ensures the proper management of breach incidents. In the program indicated in said policy, the latter is responsible for training and awareness needed for the employees' enrichment in the field of Cyber Security. Further, the respondent explained their flowchart when it comes to handling their breach incidents. Furthermore, the latter likewise indicated therein the mitigation or vulnerability eradication in breach incidents. Lastly, the respondent similarly assured that their system is in accordance with the DPA of 2012 and its IRR and related issuances.³⁰

Based on the EnD's assessment, Edukasyon's Incident Response Program is adequate to comply with the requirements found in

²⁸ NPC Circ. No. 16-03, § 4.

²⁹ Respondent's Entry of Appearance with Compliance to the Order dated 03 February 2022, 07 July 2022, at 4, in *RPR v. Edukasyon.ph*, NPC 19-438 (NPC 2022); *Id.* Annex H.

³⁰ Final Enforcement Assessment Report, Enforcement Division, 17 August 2022, at 3, in *Rainier P. Rufino v. Edukasyon.ph* NPC 19-438 (NPC 2022).

Section 4 of NPC Circular 16-03 (Personal Data Breach Management). As such, the Commission finds that Edukasyon’s submission of its Security Incident Management Program adheres to the DPA, its IRR and related issuances.

The Commission finds that Edukasyon has properly notified all affected data subjects in the personal data breach of the “thank you letter” sent by email to the participants of the Conference. The Commission also finds Edukasyon’s submission of its Incident Response Program as a form of Security Incident Management Policy adequate. As such, Edukasyon’s compliance with the Order dated 03 February 2022 is deemed sufficient.

WHEREFORE, premises considered, this Commission finds the compliance of Edukasyon.ph with the Order dated 03 February 2022 **SUFFICIENT**. This Commission considers the matter **CLOSED**.

SO ORDERED.

City of Pasay,
Philippines. 22
September 2022.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

JOHN HENRY D. NAGA
Privacy Commissioner

Copy furnished:

RPR
Complainant

EDUKASYON.PH
Respondent

VASIG ABARQUEZ LUMAUIG ABARQUEZ PUNO LAW OFFICE
Counsel for Respondent

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

**IN RE: NSO LENDING COMPANY INC.
(CASHLENDING ONLINE LENDING
APPLICATION)**

NPC 19-908
*For: Violation of the
Data Privacy Act of
2012*

X-----X

RESOLUTION

LIBORO, P.C.:

This refers to the Motion for Reconsideration dated 10 December 2019 filed by NSO Lending Company, Inc., A.I., U.U., L.O., I.A.O., and E.U. (collectively referred to as Respondents) assailing the Resolution dated 02 October 2019 issued by this Commission.

Facts

On 29 August 2019, a Fact-Finding Report (“Report”) was submitted to the Commission containing a brief narration of the material facts and the supporting documentary evidence which showed, among other things, the acts that were allegedly committed by NSO Lending Company, Inc. (“NSO”) in operating the Cashlending Online Lending Application that may result in prosecution under the Data Privacy Act of 2012¹ (DPA).

On 30 August 2019, an Order to File an Answer (“Answer”) was issued by the Commission to the Respondents. The Commission instructed all the Respondents to file their respective Answers to the allegations in the Fact-Finding Report within ten (10) days from the receipt of said Order.

¹ Rep. Act 11073(2012)

On 16 September 2019, Respondents filed their Motion to Dismiss² (“Motion”) instead of an Answer. Respondents argued among other things, that the case is dismissible under the rules on *litis pendentia*, there being pending cases involving Respondent NSO filed by specific individual complainants who appear to be same parties in this case, and that the instant *sua sponte* case failed to comply with National Privacy Commission (NPC) Circular No. 16-04, otherwise known as the Rules of Procedure of the NPC (“Rules”), and hence violated their right to due process.

On 02 October 2019, the Commission issued a Resolution denying the Respondents’ Motion to Dismiss. The Resolution also stated that Respondents “xxx having failed to substantiate their claims for dismissal, should do well to submit their Answer if they truly want to exercise their right to be heard.”

On 10 December 2019, Respondents filed the instant Motion for Reconsideration, which is nothing but a mere rehash of the Respondents arguments in its earlier Motion to Dismiss.

Discussion

The Commission hereby resolves to deny the Motion for Reconsideration of the Respondents.

In the case of *Yap vs. Court of Appeals, et. al*³, it was held that:

The underlying principle of *litis pendentia* is the theory that a party is not allowed to vex another more than once regarding the same subject matter and for the same cause of action. This theory is founded on the public policy that the same subject matter should not be the subject of controversy in courts more than once, in order that possible conflicting judgments may be avoided for the sake of the stability of the rights and status of persons.

² Motion to Dismiss dated 16 September 2019

³ *Jesse Yap vs. Court of Appeals, Eliza Chua and Evelyn Te*, G.R. No. 186730, June 13, 2012

Moreover, in the case of *Villarica Pawnshop, Inc. v. Gernale*⁴, the Supreme Court held that:

The requisites of *litis pendentia* are: (a) the identity of parties, or at least such as representing the same interests in both actions; (b) the identity of rights asserted and relief prayed for, the relief being founded on the same facts; and (c) the identity of the two cases such that judgment in one, regardless of which party is successful, would amount to res judicata in the other.

Borrowing the words of the Respondents, “at the risk of sounding repetitive”, the Commission gives emphasis again on the fact that the pending cases with the NPC and the case at hand involve different parties and different causes of action with different prayers for relief. Therefore, the requisites for *litis pendentia* are sorely lacking and the dismissal on the ground of *litis pendentia* by Respondents is devoid of any merit.

Respondents argued on both of its Motion to Dismiss and Motion for Reconsideration that a group of NPC personnel had come up with the Fact-Finding Report with no clear mandate to conduct investigation. Furthermore, Respondents called out the Commission and boldly claimed that the Commission has no power to constitute an investigating body under the NPC Rules.

The power of the Commission to investigate on its own initiative flows from the law creating the Commission itself pursuant to Section 7(b) of the DPA which provides that:

xxx

b) Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: *Provided*, That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access

⁴ Villarica Pawnshop, Inc. v. Gernale, G.R. No. 163344, March 20, 2009

to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act;" (Emphasis supplied)

Furthermore, Section 3 of the Rules in providing definite procedure to the foregoing provision, provides as follows:

SECTION 3. Who may file complaints. – **The National Privacy Commission, sua sponte**, or persons who are the subject of a privacy violation or personal data breach, or who are otherwise personally affected by a violation of the Data Privacy Act, may file complaints for violations of the Act. (Emphasis supplied)

Furthermore, Section 23 of the same Rules provides for the power of original inquiry:

SECTION 23. Own initiative. – Depending on the nature of the incident, **in cases of a possible serious privacy violation or personal data breach, taking into account the risks of harm to a data subject, the Commission may investigate on its own initiative the circumstances surrounding the possible violation.** Investigations may include on-site examination of systems and procedures. If necessary, the Commission may use its enforcement powers to order cooperation of the personal information controller or other persons, with the investigation or to compel appropriate action to protect the interests of data subjects. (Emphasis supplied)

Considering the aforesaid provisions, it is undisputed that this Commission has the power to institute a *sua sponte* proceeding as clearly provided in the DPA, its rules and regulations, and other Circular of this Commission.

Due to the influx of complaints received by the NPC against several online lending mobile applications, on 14 May 2019, the Commission created the NPC Task Force on Online Lending Mobile Application.⁵ The Task Force which is composed of highly respected officials and

⁵ Privacy Commission Special Order No. 028, Privacy Commission Special Order No. 032-A.

not just a “group of personnel” as Respondents called it was later reconstituted by virtue of Special-Order No. 032-A. Under the said issuance, the authority to investigate was validly delegated to the Task Force. It is responsible to investigate the influx of complaints against several online lending companies for potential violations of the DPA. The Task Force is also mandated to provide options and recommendations for the Commission to immediately address concerns of the public. In accomplishing this function, the Task Force submitted fact-finding reports on several online lending companies, one of which is the herein Respondents.

Corollary to the foregoing, the Commission, in the exercise of its quasi-judicial function and acting as a collegial body is acting within its mandate, to receive complaints and investigate possible violations of the Rules by the Respondents, issue an order to create a Task Force to investigate violations of the Rules, and file a complaint *sua sponte*.

The Commission received several complaints against the Respondents. Independently of these complaints from different aggrieved parties, the Commission in the exercise of its *sua sponte* power, delegated to the Task Force the investigation of the herein Respondents in response to allegations of serious and copious data privacy violations allegedly committed upon a large number of data subjects.

It is also worth noting that Respondents’ arguments are nothing but a product of their plain ignorance and misunderstanding of the DPA, its Implementing Rules and Regulation, and the NPC Rules of Procedure. Having failed to substantiate its claims, Respondents must submit its Answer if it truly wants to exercise its right to be heard. Otherwise, the Commission is left with no recourse but to consider the case submitted for resolution. This is pursuant to Rule III, Section 17 of the Rules which provides that, **“Failure to submit a comment results to the submission of the complaint for resolution”**. (emphasis supplied)

It is worth emphasizing that the period to file an Answer by the Respondents have already lapsed, and even this Motion for Reconsideration is filed out of time. It must be noted that on 30 August 2019, the Commission ordered the Respondents to file an Answer to the Fact-Finding Report dated 30 August 2019 no later than ten (10)

days from its receipt. The said Order was received by the Respondents on 11 September 2019. Therefore, Respondents should have until 21 September 2019 to file an Answer.

However, instead of filing an Answer, the Respondents filed a Motion to Dismiss on 16 September 2019. At this point, Respondents have already consumed five (5) days of the ten (10)-day period provided to them to file an Answer.

Pursuant to Section 32 of the Rules, the Rules of Court shall apply in a suppletory character, and whenever practicable and convenient. Considering that the NPC Rules of Procedure is silent on how to treat a Motion to Dismiss, Rule 16 (Motion to Dismiss) of the 1997 Rules of Civil Procedure (Rules of Procedure) shall have a suppletory application.

It is also worth noting that on 29 November 2019, Respondents received the assailed Resolution dated 02 October 2019 that denied their Motion to Dismiss. Instead of filing an Answer, the Respondents further filed a Motion for Reconsideration on 10 December 2019.

Now, Section 4, Rule 16 of the Rules of Procedure finds application, thus, stated:

Section 4. Time to plead. — If the motion is denied, the movant shall file his answer within the **balance of the period** prescribed by Rule 11 to which he was entitled at the time of serving his motion, but not less than five (5) days in any event, computed from his receipt of the notice of the denial. If the pleading is ordered to be amended, he shall file his answer within the period prescribed by Rule 11 counted from service of the amended pleading, unless the court provides a longer period. (Emphasis supplied)

Based on the foregoing provision, the Respondents had already exhausted their remaining period to file for a Motion or an Answer.

The Respondents only have a remaining balance of five (5) days or up to 04 December 2019 to file an Answer. However, instead of filing an Answer, the Respondents filed the subject Motion for Reconsideration on 10 December 2019, which is already beyond the ten (10)-day reglementary period.

Time and time again, litigants must be reminded of their responsibility to properly adhere to the reglementary period imposed by the applicable rules.

Further, the Respondents will not be able to rely on the application of the fresh period rule, as enunciated by the Court in ***Neypes vs. Court of Appeals***⁶ because the rule is only applicable in judicial proceedings. What is applicable in administrative agencies are their own rules of procedures. The jurisprudence is clear on this matter.

In the case of ***San Lorenzo Ruiz Builders and Developers Group, Inc. vs. Bayang***⁷, the petitioner's appeal was filed out of time because Paragraph 2, Section 1 of Administrative Order No. 18, s. 1987 provides that in case the aggrieved party files a motion for reconsideration from an adverse decision of any agency/office, the said party has only the remaining balance of the prescriptive period within which to appeal. Thus, stated:

...the subject appeal, i.e., appeal from a decision of the HLURB Board of Commissioners to the OP, is **not judicial but administrative in nature; thus, the "fresh period rule" in Neypes does not apply.** (Emphasis supplied)

XXXXX

Corollary thereto, paragraph 2, Section 1 of Administrative Order No. 18, series of 1987, provides that **in case the aggrieved**

⁶"To standardize the appeal periods provided in the Rules and to afford litigants fair opportunity to appeal their cases, the Court deems it practical to allow a fresh period of 15 days within which to file the notice of appeal, counted from the receipt of the order dismissing a motion for new trial or motion for reconsideration" (Neypes vs. CA, G.R. No. 141524, 14 September 2005)

⁷G.R. No. 194702, 20 April 2015

party files a motion for reconsideration from an adverse decision of any agency/office, the said party has the only remaining balance of the prescriptive period within which to appeal, reckoned from receipt of notice of the decision denying his/her motion for reconsideration. (Emphasis supplied)

The Supreme Court emphasized in the case of ***Puerto Del Sol Palawan, Inc. vs. Gabaen***⁸ that the fresh period rule was applicable because the specific administrative rules of procedure explicitly provided for the application of the fresh period rule.

Furthermore, it must be noted that the fresh period rule only applies to appeal to a final decision of a court and not in *interlocutory orders*. This case involves a Motion for Reconsideration on preliminary matters and a proceeding on the merits is yet to be held⁹.

Following the state of our jurisprudence in the matter, the NPC Rules of Procedure does not provide for a fresh period when a litigant's motion is denied, in fact it expressly bars the application of the rule in its proceedings. Section 30 of the NPC Rules of Procedure provides:

SECTION 30. Appeal. – The decision of the National Privacy Commission shall become final and executory **fifteen (15) days after the receipt** of a copy thereof by the party adversely affected. **One motion for reconsideration may be filed, which shall suspend the running of the said period.** Any appeal from the Decision shall be to the proper courts, in accordance with law and rules. (Emphasis supplied)

Hence, this Motion for Reconsideration was filed out of time, has no merit, and should be dismissed. Therefore, this case can now be considered as submitted for final resolution.

However, in the interest of substantial justice, this Commission will grant a final and non-extendible period of five (5) days for the Respondents to provide their Answer to the Fact-Finding Report dated

⁸G.R. No. 212607, 27 March 2019

⁹Priscilla Alma Jose v. Romon C. Javellana, Et Al., G.R. No. 158239, 25 January 2012

29 August 2019. The running of the five (5) days shall commence from the actual receipt of this Resolution.

WHEREFORE, premises considered, the Commission resolves that the instant Motion for Reconsideration filed by Respondent NSO Lending Company, Inc. on the Resolution dated 02 October 2019, is hereby **DENIED**. Respondents are **ORDERED** to submit its Answer within five (5) days from date of receipt hereof.

Failure to file an Answer by the Respondents within the above indicated period, the instant case shall be deemed submitted for Resolution of the Commission.

SO ORDERED.

Pasay City, Philippines;
15 January 2020.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy

Commissioner Copy furnished:

**BAUTISTA ROLEDA JABLA YUSI &
TOMAS LAW OFFICES (BRJYT LAW)**
Counsel for Respondents

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

**IN RE: FCASH GLOBAL LENDING,
INC., OPERATING FASTCASH
ONLINE LENDING APPLICATION.**

NPC 19-909
For: Violation of the
Data Privacy Act

X-----X

RESOLUTION

NAGA, P.C.;

Before us is a Motion for Reconsideration dated 28 February 2022 (Motion) by Respondents FCash Global Lending Inc., KDM, TH, JPS, JCT, and ZS (Respondents) assailing the Decision dated 23 February 2021 (Decision), copy of which was received through counsel on 17 February 2022. The challenged Decision disposed as follows:

WHEREFORE, all the above premises considered, this Commission hereby:

1. **FINDS** Respondent FCash Global Lending Inc. and its Board of Directors to have violated Section 25, 28, and Section 31 of the Data Privacy Act of 2012; and
2. **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice, recommending the prosecution of the Respondents for the crimes of Unauthorized Processing of Personal Information and Sensitive Personal Information under Section 25 of the DPA, Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes under Section 28 of the DPA, and Malicious Disclosure under Section 31 of the DPA. The maximum penalty for violations of the abovementioned provisions is recommended to be imposed following Section 35 of the DPA.¹

¹ Decision dated 23 February 2021

Respondents' Motion reiterated the grounds they relied upon in their Motion to Dismiss, *to wit*:

1. The Decision was issued not in compliance with the National Privacy Commission (NPC) Rules of Procedure, hence, with grave abuse of discretion amounting to a lack or excess of jurisdiction;
2. The Decision ignored the rule on exhaustion of remedies under Section 4, Rule II of the NPC Rules;
3. The Decision ignored the rule on *litis pendentia*, there being pending cases involving Respondent FCash filed by specific individual complainants who appear to be the same parties in the case;
4. The Decision violates and renders nugatory the provisions of the DPA on amicable settlement and alternative modes of dispute resolution which are expressly promoted by law;
5. The Decision arbitrarily, unfairly, and erroneously impleaded the corporate officers of Respondent FCash despite the lack of evidence, let alone allegations, that any of them participated in the alleged acts nor committed any gross negligence.²

Thus, Respondents pray for the reconsideration and the setting aside of the Decision dated 23 February 2021, which in effect dismisses the case against FCash.

The Commission now resolves the Motion.

The Commission has, time and time again, adequately ruled on this matter. The Commission already addressed these issues in its Resolution dated 02 October 2019 for the Motion to Dismiss dated 16 September 2019 and the Resolution dated 23 January 2020 for the Motion for Reconsideration dated 10 December 2019.

Furthermore, in relation to the Petition for Certiorari under Rule 65 of the Rules of Court filed by Respondents with the Honorable Court of Appeals in reference to its denied Motion for Reconsideration dated 23 January 2020, the Commission argued that “[a]t the outset, it bears to

² Motion to Dismiss dated 16 September 2019

point that the resort to *certiorari* is not the proper remedy to assail the denial [of Respondent's] motion to dismiss.”³ The Commission reminded that it is settled in jurisprudence that the writ of *certiorari* is “available only where the tribunal, board or officer exercising judicial functions has acted without or in excess of their jurisdiction, or with grave abuse of discretion, and there is no appeal, or any plain, speedy and adequate remedy in the ordinary course of law. The special civil action should not be allowed as substitute for any ordinary appeal or where there are other remedies available.”⁴ Nevertheless, the Commission shall take this final opportunity to clarify matters with Respondents.

I. The assailed Decision was issued in compliance with the NPC Rules of Procedure

Respondents argue that the proceeding was not conducted in compliance with NPC Circular 16-04 or the NPC Rules of Procedure (Rules) as there was no complaint filed but instead a Fact-Finding Report, which Respondents argued does not satisfy the requirement to initiate a *sua sponte* investigation. Such matter has already been resolved by the Commission in its 02 October 2019 Resolution.

To reiterate, Section 23 of Rule IV of the Rules provides for the power of the Commission to investigate on its own initiative the circumstances surrounding a possible serious privacy violation or personal data breach, taking into account the risks of harm to a data subject. Consequently, the investigation shall be made in accordance with Rule III of the same Rules following the principle of uniform procedure sufficiently complied with in this case.⁵

The Fact-Finding Report dated 29 August 2019⁶ (FFR) that was served to Respondents contains a narration of the material facts and the supporting documentary evidence which showed, among other things, the violations allegedly committed by Respondent FCash in operating its online lending application.⁷ The same FFR was submitted

³ FCash Global Lending Inc., rep by KDM vs National Privacy Commission, Comment of Respondent National Privacy Commission dated 02 August 2021

⁴ *Id.*

⁵ Resolution dated 02 October 2019.

⁶ In re: FCash Global Lending Inc Fact-Finding Report dated 29 August 2019

⁷ Resolution dated 02 October 2019

to the Commission for its perusal to determine whether violations of the Data Privacy Act of 2012 (DPA) were committed. Considering that the FFR contains all the findings of the investigating division of the NPC, such document is the complaint initiating the administrative proceedings in cases of *sua sponte* investigation. As *sua sponte* means “of one’s own accord”, the NPC, through the CID, has initiated, on its own, a complaint against Respondent by filing the FFR.

Further, in accordance with the Rules, Respondents, then, were given an opportunity to submit an Answer, as prescribed by Rule IV of the Rules wherein the Responsive Comment or Answer is immediately required from Respondents after it receives the Fact-Finding Report, *to wit*:

SECTION 24. *Uniform procedure.* – The investigation shall be in accordance with Rule III of these Rules, provided that the respondent shall be provided a copy of the fact-finding report and given an opportunity to submit an answer. In cases where the respondent or respondents fail without justification to submit an answer or appear before the National Privacy Commission when so ordered, the Commission shall render its decision on the basis of available information.⁸

As discussed by this Commission in its NPC 19-910 Resolution, “the procedure for a *sua sponte* investigation does not include a Discovery Conference because all the information and evidence in the hands of the Commission are already set out in and attached to the Fact-Finding report when it is provided to respondent.”⁹

It was emphasized by the Commission in NPC 19-910 Resolution that:

[W]hile Section 24 of Rule IV of the Rules provides that the investigation be in accordance with Rule III, it includes a provision: ‘that the respondent shall be provided with a copy of the Fact-Finding Report and given an opportunity to submit an answer.’ Rule IV does not state that the procedure should be exactly identical to the one described under Rule III. As used in Section 24 of Rule IV, ‘in accordance with Rule III’ simply means as far as practicable taking into consideration and giving effect to the difference between the two (2) procedures.¹⁰

⁸ Section 24, Rule IV of NPC Circular 16-04

⁹ NPC 19-910, Resolution dated 11 March 2021

¹⁰ *Id*

Further, to recall, in the Resolution dated 02 October 2019:

[T]he provision on the Uniform Procedure under the Rules should be read in light of the unique situation arising from the *sua sponte* nature of the present investigation. Under the NPC Rules, discovery is a procedure employed by parties to avail of, to compel the production of, or to preserve the integrity of electronically stored information. This procedure need not be resorted to by the Commission, however, in its exercise of its power of original inquiry. This is all the more true in this case considering that there are no private parties that can be called to confer for discovery. It must be emphasized that this case was initiated by a team of investigators in the Commission in response to serious allegations of data privacy violations allegedly committed upon a large number of data subjects.¹¹

Respondents claimed that the FFR already contained conclusions and recommendations for the prosecution of all the respondents for alleged violation of the provisions of the DPA.¹² To recall, it has been pointed out by this Commission that “no judgement of any kind has been made on this case for or against Respondents.”¹³ As previously discussed, the FFR is treated as the complaint in cases that are initiated through a *sua sponte* proceeding. The FFR is not the view of the Commission En Banc but rather a brief narration of the material facts and the supporting evidence which shows among other things, the cause of action of the complainant against the respondent.

Further, as the FFR is the complaint in cases of *sua sponte* investigations, Respondents were given the opportunity to be heard by ordering them to file their Answer or Comment to the submitted FFR. However, despite these opportunities given by the Commission to Respondents, the orders were left unanswered and ignored. Instead, Respondents questioned the authority of the Commission to determine this case.

Given this, the investigation and procedure of recommending a possible violation of the DPA has all been done in accordance with the powers vested in the Commission to institute *sua sponte* cases provided by the DPA and the Rules. Respondents should note that the response

¹¹ Resolution dated 02 October 2019

¹² R.A. 10173

¹³ Resolution dated 02 October 2019

of the Commission upon receiving the FFR was an Order to File an Answer and not a decision.

The fact that there exist hundreds of pending cases before the Commission against Respondents is no bar to the filing of the case on hand but instead highlights the seriousness of the data privacy violations and risks of harm to data subjects. The Commission notes that the other pending cases against the Respondents and the case at hand involves different parties with different causes of action and prayers for relief.

As held by the Supreme Court in *Yap vs. Court of Appeals*¹⁴

Litis pendentia as a ground for the dismissal of a civil action refers to that situation wherein another action is pending between the same parties for the same cause of action, such that the second action becomes unnecessary and vexatious. The underlying principle of litis pendentia is the theory that a party is not allowed to vex another more than once regarding the same subject matter and for the same cause of action. This theory is founded on the public policy that the same subject matter should not be the subject of controversy in courts more than once, in order that possible conflicting judgments may be avoided for the sake of the stability of the rights and status of persons.

The requisites of litis pendentia are: (a) the identity of parties, or at least such as representing the same interests in both actions; (b) the identity of rights asserted and relief prayed for, the relief being founded on the same facts; and (c) the identity of the two cases such that judgment in one, regardless of which party is successful, would amount to res judicata in the other.¹⁵

In the present case, none of the foregoing requisites were met. As it was repeatedly emphasized, the pending cases against the Respondents and the case at hand involves different parties with different causes of action and prayers for relief.

As argued by the Commission in its Comment dated 02 August 2021 for the case C.A.– G.R. SP No. 168046:

The cause of the individual complaints is to enforce the individuals rights vested by the DPA. Meanwhile, a complaint which arose from

¹⁴ G.R. No. 186730, June 13, 2012

¹⁵ *Id.*

a *sua sponte* investigation is hinged on the [Commission's] responsibility, as representative of the State, 'to protect the fundamental human rights of privacy, of communication while ensuring free flow of information to promote innovation and growth.' The individual complaints were only cited in the Fact-Finding Report to demonstrate the seriousness of the possible data privacy violation.

The [FFR] itself shows that the Task Force conducted an independent investigation against [FCash]. It reviewed [FCash's] Privacy Policy, the user reviews alleging serious privacy violations, and the mobile application itself. The investigators evaluated how [FCash's] application operates and the extent to which the privacy of its users is protected by examining the Android Manifest, including 'permissions' required by the application. The Fact-Finding Report itself states: 'Examination of publicly accessible information and the initial technical evaluation of FCash and the Fast Cash online lending application shows that the company has failed to demonstrate compliance with the DPA.'

Clearly, the investigators made findings beyond the scope of the individual complaints filed by the data subjects. These includes inaccessible information regarding [FCash's] Data Protection Officer, failure to exercise efforts in response to privacy complaints, inadequate Privacy Policy, and presence of dangerous permissions violating the principle of proportionality.¹⁶

II. *The assailed Decision did not ignore the rule on exhaustion of remedies under Section 4, Rule II of the NPC Rules.*

Respondents contend that the Commission failed to observe the mandatory exhaustion of remedies requirement under Section 4, Rule II of the NPC Rules as Respondents were not granted the opportunity to "take timely or appropriate action on the claimed privacy violation or personal data breach"¹⁷ before a complaint can be filed.

As held by the Commission in NPC 19-910, *to wit*:

The Respondent's interpretation that the Commission should first reach out to respondents to be 'given the opportunity to institute appropriate actions to rectify the alleged criminal violations of the DPA' is purpose-defeating, if not plainly absurd. *Sua sponte*

¹⁶ Supra Note 3, page.23

¹⁷ Section 4 (b), Rule II of NPC Circular No. 16-04

investigations are only conducted under specific premises under the Rules of Procedure, thus:

Section 23. Own initiative. – Depending on the nature of the incident, **in cases of a possible serious privacy violation or personal data breach**, taking into account the risks of harm to a data subject, the Commission may investigate on its own initiative the circumstances surrounding the possible violation. Investigations may include on-site examination of systems and procedures. If necessary, the Commission may use its enforcement powers to order cooperation of the personal information controller or other persons, with the investigation or to compel appropriate action to protect the interests of data subjects. subjects.

As seen with the abovementioned criteria for a *sua sponte* investigation, complaints are only initiated in cases of a possible serious privacy violation or personal data breach. In these actions, the Commission considers evident risks of harm to a data subject. The privacy violation or personal data breach that can be directly acted upon by the Commission is qualified with a degree of seriousness that makes it different from complaints under Rule III. This degree of seriousness is considered in relation to the level of risks posed to the data subjects, and may be manifested in different ways such as the scale of processing or the number of reports received by the Commission.

Thus, in cases of *sua sponte* investigations, it is futile for the Commission to exhaust remedies by communicating with the respondent. The provision on the exhaustion of remedies is meant to provide an opportunity for parties to amicably settle among themselves and rectify the situation. This is only resorted to when the possibility of rectification still exists

The nature and purpose of *sua sponte* investigations make such exhaustion of remedies futile because by the time the Commission detects a privacy violation or personal data breach, the opportunity for rectification is no longer available. The requirement of exhaustion of remedies is thus inapplicable to *sua sponte* investigations.

Furthermore, such provision for the exhaustion of remedies is not an absolute rule that renders all non-conforming complaints invalid. The Commission has previously discussed the purpose for the exhaustion of remedies in an earlier Decision:

This rule was intended to prevent a deluge of vexatious complaints from those who waited for a long period of time to pass before deciding to lodge a complaint with the NPC, unduly clogging its dockets. Notably, however, the same Section provides that the Commission has the discretion to waive such period for filing upon good cause shown, or if the complaint involves a serious violation or breach of the DPA, taking into account the risk of harm to Complainant.¹⁸

Respondents also argue that the conduct of a *sua sponte* investigation is unnecessary as there were already several pending complaints against it.

As held by the Commission in NPC 19-910, the Commission wishes to highlight:

Nowhere in its Decision did the Commission ‘admit that the *sua sponte* investigation was conducted in lieu of the several complaints received by the Honorable Commission against Respondent[.]’ On the contrary, the Decision explicitly stated that the *sua sponte* investigation is independent and separate from the individual cases by stating that ‘the pending cases and the case on hand involve different parties, different causes of action with different prayers of relief.’

xxx

The individual complaints were only cited to demonstrate the seriousness of the possible data privacy violation.¹⁹

The *sua sponte* investigation was conducted due to the potential harm to the data subjects. This is in consideration of the Commission’s mandate in the DPA to ensure a personal information controller’s compliance with the law²⁰ and institute investigations when necessary.²¹ This is likewise in consideration of the provision in NPC Circular 2021-01, which allows conduct of *sua sponte* investigations of

¹⁸ NPC 19-910, Resolution

¹⁹ *Id.*

²⁰ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter II, § 7(a) (2012).

²¹ *Id.* § 7(b).

possible privacy violations or personal data breaches.²² Hence, the *sua sponte* investigation of the Commission was conducted due to its mandate and function and not because of several complaints.

- III. *The assailed Decision did not ignore the rule on litis pendentia, there being pending cases involving Respondent FCash filed by specific individual complainants who appear to be the same parties in the case*

Further, Respondents claim that the conduct of a separate proceeding involving the same subject matter as cases which are currently being investigated and pending for adjudication by this Commission through its investigating officers violates the principle of *litis pendentia*. As previously discussed, the pending cases before the Commission filed by different complainants is entirely different from the case initiated by a *sua sponte* investigation. These cases have different parties, different causes of action with different prayers of relief. The cited complaints in the FFR were, to reiterate, used to emphasize the gravity and seriousness of the violation of data privacy. Respondents erred in saying that they are being vexed for the same subject matter.

- IV. *The assailed Decision does not violate nor renders nugatory the provisions of the DPA on amicable settlement and alternative modes of disputes resolution which are expressly promoted by law.*

As to the contention that the Decision is totally in conflict with the other decisions of this Commission approving the amicable settlement entered into by specific complainants, the Commission wishes to remind Respondents that the previous decisions of the Commission approving the amicable settlements are entirely different from the case initiated by the *sua sponte* investigation. These cases which are settled and dismissed by virtue of an amicable settlement are not decided based on the merits of the case but due to the mutual understanding of the parties. The final amicable settlement that contains the terms and conditions of the parties for the settlement of the case has the force and effect of law between these parties. No provision of the DPA was used to arrive at the settlement. As held by the Supreme Court in the case of *Miguel v. Montanez*:

²² NPC Circular No. 2021-01, rule X, §§ 5-6.

Being a by-product of mutual concessions and good faith of the parties, an amicable settlement has the force and effect of *res judicata* even if not judicially approved. It transcends being a mere contract binding only upon the parties thereto, and is akin to a judgment that is subject to execution in accordance with the Rules.²³

Further, “[w]hile the Rules on Mediation embodied in NPC Circular No. 18-03 did not provide a distinction between cases which can and cannot undergo mediation, NPC Circular No. 16-04 categorically states that ‘no settlement is allowed for criminal acts.’”²⁴

The Commission also wishes to emphasize that the purpose of the mediation settlement is to help parties arrive at an acceptable compromise. Considering that the cause of action in a complaint borne out of a *sua sponte* investigation is the State’s duty to protect the right to privacy and not to prosecute to claim reparation on behalf of private individuals, no compromise can be had between the State and the Respondent.

Hence, the previous decisions of the Commission confirming the amicable settlement of the parties are not contrary to the Decision as no interpretation and application of the DPA was used nor preceding decisions of the Commission was applied. The decisions of the Commission were merely a recognition of the agreement of the parties to settle the case based on their mutual understanding and not through the remedial procedures of this Commission.

- V. *The assailed Decision does not arbitrarily, unfairly, and erroneously impleaded the corporate officers of Respondent Fcash despite the lack of evidence, let alone allegation, that any of them participated in the alleged acts nor committed any gross negligence.*

Lastly, Respondents contend that impleading its corporate officers of despite the lack of evidence, let alone allegations, that any of them participated in the alleged acts or committed any gross negligence is arbitrary, unfair, and erroneous.²⁵ This Commission points out that the DPA is clear that the liability of the responsible officers in cases where the offender is a corporation does not rely on active participation

²³ Miguel v. Montañez, G.R. No. 191336, 25 January 2012

²⁴ NPC 19-910, Resolution

²⁵ Motion for Reconsideration dated 28 February 2022

alone. Gross negligence is explicitly stated in the DPA as a ground for criminal liability, *to wit*:

SEC. 34. *Extent of Liability.* – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.²⁶

There is no reason for the Commission to reverse its earlier finding that the Respondent officers are liable for gross negligence. As stated in the Decision of this Commission in the case of NPC 19-910:

The Supreme Court has consistently defined gross negligence as ‘the negligence characterized by the want of even slight care, or by acting or omitting to act in a situation where there is a duty to act, not inadvertently but willfully and intentionally, with a conscious indifference to the consequences of, insofar as other persons may be affected. It is the omission of that care that even inattentive and thoughtless men never fail to give their own property.’²⁷

The fact that the Board of Directors (BOD) failed to act on the voluminous and alarming privacy issues of their borrowers negates the legal presumption that the BOD employed ordinary care in the discharge of their duties and instead, presumes that the BOD knew about these collection practices and approved of it. There are one hundred and sixty-six (166) complaints against Respondent as of July 2019. The Complaint also attached user reviews on Respondent application in *Google Play Store*. The user comments narrated experiences on how the Respondent gains access to mobile phonebook/directory/contact list for the purpose of disclosing their transactions without their consent and authority.²⁸ It can be reasonably said that the privacy complaints against Respondent have reached into

²⁶ Section 34 of R.A. 10173

²⁷ Fernandez vs Office of the Ombudsman, GR No. 193983, March 14 2012.

²⁸ Fact-Finding Report dated 29 August 2019, pg. 11-13.

the public's consciousness.²⁹ Thus, it is the responsibility of the BOD to show to this Commission that they have employed the necessary diligence expected from them. However, no evidence was presented by the Respondent to rebut this presumption against them. Further, despite the BOD's responsibility to show the Commission that it employed necessary diligence, it unfortunately still refuses to present any evidence demonstrating that it addressed, or at the very least, did not allow such actions.

Citing the SEC registration records of the Respondent, the Complaint specifically named KDM, TH, JPS, JCT, and ZS as the original incorporators, registered directors, and officers of Respondent. Thus, the abovementioned violations of the DPA shall be imputed against all of them due to their gross negligence following Section 34.³⁰

Considering the foregoing, Respondents have not provided any new or material allegations that would merit the reversal of the Decision.

WHEREFORE, all the above premises considered, this Commission hereby resolves to **DENY** the Motion for Reconsideration filed by FCash Global Lending Inc. The Decision of the Commission dated 23 February 2021 is hereby **AFFIRMED**.

SO ORDERED.

City of Pasay,
Philippines. 28 April
2022.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

²⁹See: <https://manilastandard.net/business/biz-plus/335368/sec-voids-license-of-fcash-global.html>.

³⁰ Fact-Finding Report dated 29 August 2019, pg. 9-10.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

BTLO
Counsel for FCash Lending Inc.

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

MVC,

Complainant,

NPC 21-010

For: Violation of
the Data Privacy
Act of 2012

DSL,

Respondent,

X-----nt-----X

RRB,

Complainant,

NPC 21-011

For: Violation of
the Data Privacy
Act of 2012

-versus-

DSL,

Respondent,

X-----nt-----X

NMB,

Complainant,

NPC 21-012

For: Violation of
the Data Privacy
Act of 2012

-versus-

DSL,

Respondent,

X-----nt-----X

RMP,

Complainant,

NPC 21-013

For: Violation of
the Data Privacy
Act of 2012

-versus-

DSL,

Respondent,

X-----nt-----X

NDL,

Complainant,

-versus-

NPC 21-014

For: Violation of
the Data Privacy
Act of 2012

DSL,

Respondent

X-----nt-----X

MBN,

Complainant,

-versus-

NPC 21-015

For: Violation of
the Data Privacy
Act of 2012

DSL,

Respondent

X-----nt-----X

RESOLUTION

AGUIRRE, D.P.C.;

Before the Commission is the Motion for Reconsideration dated 05 April 2022 filed by DSL (Lee).

Facts

On 03 February 2022, the Commission issued a Decision finding Lee liable for Section 32 of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) and recommending his prosecution to the Department of Justice:

WHEREFORE, premises considered, the Commission hereby:

1. **FINDS** DSL liable for Section 32 (Unauthorized Disclosure) of the Data Privacy Act of 2012; and

2. **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice and recommends the prosecution of Lee for the offense of Unauthorized Disclosure under Section 32 of the DPA.

SO ORDERED.¹

On 21 March 2022, DSL, through his counsel, received a copy of the Decision dated 03 February 2022.²

On 05 April 2022, DSL filed his Motion for Reconsideration alleging that the Commission erred in finding him liable for Unauthorized Disclosure under Section 32 of the DPA and recommending for his prosecution.³ He further asserted that the Commission committed an error when it took cognizance of the case despite the procedural lapses.⁴

In DSL's Motion for Reconsideration, he claimed that he should not be held liable for Unauthorized Disclosure because as the President of the GA Tower 1 Condominium Corporation (GAT1CC), he was authorized to disclose the names of delinquent unit owners pursuant to the House Rules and Regulations of GAT1CC.⁵ He argued that the members of GAT1CC, which included Complainants MVC, RRB, NMB, RMP, NDL, and MBN (Complainants), are bound by the House Rules and Regulations of GAT1CC.⁶ Thus, according to Lee, the disclosure of the names of delinquent members through the publication of the letter dated 23 November 2021 was an obligation in accordance with Section 12 (c) of the DPA.⁷

¹ NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015, 03 February 2022, at 13 (NPC 2022) (unreported).

² Motion for Reconsideration, 05 April 2022, ¶ 2, *in MVC, et al. v. DSL*, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).

³ *Id.* ¶ 5.

⁴ *Id.* ¶ 18.

⁵ *Id.* ¶¶ 7 & 9.

⁶ *Id.* ¶¶ 8-9.

⁷ *Id.* ¶ 8.

He claimed that the Complainants failed to substantially prove that he was not authorized to bind GAT1CC.⁸ He also claimed that there was no evidence to prove that he did not issue the letter dated 23 November 2021 in the interest of GAT1CC nor was there evidence to support the Commission's finding that he disclosed the personal information of the Complainants to cast doubt on their capability to manage the affairs of GAT1CC.⁹ To support his contentions, DSL pointed out that the Complainants "were not singled out" considering that the list included all the delinquent members.¹⁰

Further, DSL argued that the Commission did not have jurisdiction over the case because it involved an intra-corporate controversy:

19. [...] [T]he contentions of the [C]omplainants clearly make out an intra[-]corporate controversy. The parties involved are the members of the corporation against the board members and officers of the corporation. In fact, the [C]omplainants did not deny and even admitted that they are members of the [C]ondominium [C]orporation, and [Lee] is the President of GAT1CC.

20. The issues as to the right of the [C]ondominium [C]orporation to impose condominium dues, the validity of the provisions of its by-laws, enforce the provisions of its master deed and house rules are issues related to intra[-]corporate controversy.¹¹

In relation to DSL's allegation that the case should have been dismissed outright due to procedural lapses, he claimed that the Complainants failed to observe the procedural requirement under NPC Circular 2021-01 (2021 NPC Rules of Procedure) when they did not attach their respective certificates against forum shopping to their complaints.¹² He further alleged that the Complainants committed forum shopping since they failed to disclose that there were four (4)

⁸ Motion for Reconsideration, 05 April 2022, ¶¶ 10-11, *in MVC, et al. v. DSL*, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).

⁹ *Id.* ¶¶ 10 & 13.

¹⁰ *Id.* ¶ 13.

¹¹ *Id.* ¶¶ 19-20.

¹² *Id.* ¶ 26.

cases with same issues as the case at bar pending before various courts.¹³ To recall, DSL enumerated the following pending cases:

- a. SEC Case No. 01-18-463, Jesus Melegrito et., al., vs. GAT1CC, Delfin Lee et., al. [...]
- b. HSAC Case No. REM-050918-16656 entitled Regidor Pablo, Selected Homeowners of GA Tower 1 vs. Delfin Lee et., al. [...]
- c. Injunction Case (Condominium Dues and Cable Fees Issue), RTC, Br. 211, Mandaluyong City, Belnas et., al., vs. GAT1CC, Delfin Lee et., al., [...]
- d. Injunction Case. GAT1CC vs. Janet Reyes, Rose Anna Banal et., al., RTC, BR. 211, Mandaluyong City, Civil Case No. R- MND-20-01767-CV[.]¹⁴

DSL argued that the Commission should set aside the Decision dated 03 February 2022 and issue a new decision dismissing the complaint filed against him.¹⁵

On 28 April 2022, the Commission issued an Order directing Complainants to comment on the Motion for Reconsideration dated 05 April 2022.¹⁶

In the Complainants' Consolidated Comment/Opposition dated 08 July 2022, they manifested that the Commission should deny Lee's Motion for Reconsideration dated 05 April 2022.¹⁷ They argued that the Motion for Reconsideration is *pro forma* as it raised the same arguments already threshed out in the Decision dated 03 February 2022.¹⁸ According to the Complainants, the Motion for Reconsideration dated 05 April 2022, being merely *pro forma*, should

¹³ *Id.* ¶ 28.

¹⁴ Memorandum, 06 October 2021, at 6, *in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).*

¹⁵ Motion for Reconsideration, 05 April 2022, *in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).*

¹⁶ Order, 28 April 2022, *in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).*

¹⁷ Consolidated Comment/Opposition, 08 July 2022, at 1, *in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).*

¹⁸ *Id.* at 2.

be considered as “a mere scrap of paper that produces no legal and procedural effect.”¹⁹

In the alternative, the Complainants further argued that DSL failed to sufficiently establish any reason for the Commission to set aside and reverse its Decision dated 03 February 2022.²⁰

The Complainants asserted that the Commission has jurisdiction over the subject matter considering that the issue involved the processing of personal information.²¹ They pointed out that the allegations concerning corporate issues “were only crucial to show the timing of the release of the personal information, as proof of malice which attended the disclosure.”²²

As to DSL’s allegation that they committed forum shopping, the Complainants argued that the (4) pending cases that DSL cited do not have the same parties, issues, and reliefs as the case at bar.²³

Lastly, the Complainants argued that the Commission correctly ruled that DSL’s processing of their personal information was done without lawful basis.²⁴

Issue

Whether the Motion for Reconsideration dated 05 April 2022 should be granted.

Discussion

¹⁹ *Id.* at 3.

²⁰ *Id.* at 3.

²¹ *Id.*

²² *Id.*

²³ Consolidated Comment/Opposition, 08 July 2022, at 3, *in MVC, et al. v. DSL*, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).

²⁴ *Id.*

The Commission denies DSL's Motion for Reconsideration dated 05 April 2022.

DSL asserted that GAT1CC, through him as the President, may post the names of delinquent unit owners pursuant to Section 12 (c) of the DPA:

8. As members of GAT1CC, [C]omplainants are indisputably bound by the [C]ondominium House Rules which are authorized by GAT1CC's Articles of Incorporation, By-Laws, the Master Deed, the Corporation Code, and the Condominium Act. As such, [GAT1CC] may validly disclose information such as the names of delinquent members pursuant to Section 12 (c) of the Data Privacy Act.

9. It goes then without saying that GAT1CC, through its President [Lee], was well within its right when it posted the names of the delinquent unit owners of the subject [C]ondominium. Complainants are bound by law and contract to follow and respect the provisions of the House Rules and Regulations of GAT1CC.²⁵

He further argued that "being the President of [GAT1CC] and being a member of the managing body thereof, [he] was in fact acting for the benefit of [GAT1CC] in the absence of proof to the contrary."²⁶

The Commission, in its Decision dated 03 February 2022, held that the publication of the letter dated 23 November 2021 was not necessary for compliance of GAT1CC's legal obligation.²⁷ It further ruled that DSL's purpose for disclosing the Complainants' personal information was not for the interest of GAT1CC.²⁸

The Commission recognized that GAT1CC may process the personal information of delinquent unit owners to assess and collect

²⁵ Motion for Reconsideration, 05 April 2022, ¶¶ 8-9, *in MVC, et al. v. DSL*, NPC 21-010, NPC 21-

011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).

²⁶ *Id.* ¶ 11.

²⁷ NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015, 03 February 2022, at 7 (NPC 2022) (unreported).

²⁸ *Id.*

outstanding obligations.²⁹ It, however, ruled that DSL's processing was neither necessary nor proportional to the alleged purpose:

The purpose of the letter was not for the collection of delinquent dues. Rather, the evidence on record shows that Lee disclosed Complainants' personal information as delinquent unit owners to cast doubt on their capability to manage the affairs of the condominium corporation in light of the recently held election of the Board of Directors.³⁰

DSL's claim that the disclosure of personal information was based on a lawful criterion under Section 12 (c) of the DPA was insufficient considering that they were not substantiated by evidence.³¹ The Commission further explained that the Personal Information Controller (PIC) claiming lawful processing has the burden to prove that it complied with the requirements of the lawful criterion it was alleging:

When a PIC claims lawful processing on the basis of a legal obligation, the burden is on the PIC to show that all that is required by that particular lawful criterion is present. A PIC must be able to prove that the legal obligation it cites as basis exists and applies to the processing it performed, and that the processing is necessary to comply with the legal obligation.³²

The Commission cannot give credence to DSL's assertion since he failed to identify the actual Board of Directors that authorized his act nor was he able to present any document certifying that he was authorized by the Board of Directors to publish the letter dated 23 November 2021. The burden is on DSL to prove that he really had authority to represent GAT1CC.

The Commission emphasizes that once the complainant has proven that there was indeed a processing that occurred, it is incumbent upon the PIC that processed the personal data to prove that it is

²⁹ *Id.* at 8.

³⁰ *Id.*

³¹ *Id.* at 9.

³² *Id.* at 7-8.

either exempted from the scope of the DPA or that the processing was based on lawful criteria under Sections 12 or 13 of the DPA.

Here, however, DSL failed to prove that he is exempted from the scope of the DPA or that his processing was based on any of the lawful criteria under Sections 12 or 13 of the DPA.

As regards the procedural issues, DSL argued that the Commission “inadvertently committed palpable error when it proceeded to decide the case despite having no jurisdiction over the subject matter thereof.”³³ He claimed that the issue in the case at bar is an intra- corporate controversy because the parties involved are members and officers of a corporation.³⁴ Thus, according to DSL, it is the Regional Trial Court that has jurisdiction over the case.³⁵

He also claimed that the Commission should have dismissed the case outright because the Complainants failed to disclose that there were four (4) pending cases before different courts that have the same issues and circumstances with that of the case at bar.³⁶

Further, DSL pointed out that the Complainants failed to comply with Section 3 (10), Rule II of the 2021 NPC Rules of Procedure when they did not attach certificates against forum shopping to their respective complaints.³⁷

Contrary to DSL’s assertions, the Commission did not commit an error when it took cognizance of the case. The issue in the case at bar relates to the processing of personal information, which is within the scope of the DPA and under the jurisdiction of the Commission.³⁸

³³ Motion for Reconsideration, 05 April 2022, *in MVC, et al. v. DSL*, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).

³⁴ *Id.* ¶ 19.

³⁵ *Id.* ¶ 22.

³⁶ *Id.* ¶ 28.

³⁷ *Id.* ¶ 24-26.

³⁸ See An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 4 (2012).

The fact that the parties in the case at bar are members and officers of a corporation does not automatically result in the existence of an intra-corporate dispute. In addition, even if there was an intra-corporate dispute, the issue in this case is the propriety of the processing of personal information undertaken by DSL. This is precisely within the mandate of the Commission.

Further, the four (4) pending cases and the case at bar do not have the same issue and cause of action. As previously stated, the issue in the case at bar relates to data privacy, particularly on the processing of personal information, and the Complainants' cause of action stems from their rights as data subjects. The four (4) pending cases relate to a dispute in the election of the Board of Directors of GAT1CC, which is an intra-corporate controversy, and to the main actions for injunction of the implementation of the condominium's rule on cable services.³⁹ The issues and the circumstances of the four (4) pending cases in comparison to the present case are not identical.

As to the issue on the certificate against forum shopping, the Commission maintains that it did not err when it did not dismiss the case outright due to the lack of certificate against forum shopping. The Complaints-Assisted Forms were filed on 15 January 2021, when NPC Circular 16-04, which does not require a certificate against forum shopping, was still in effect. Thus, the lack of a certificate against forum shopping does not result in any error on the part of the Complainants.

Given the foregoing, the Commission finds that the issues raised in the Motion for Reconsideration dated 05 April 2022 failed to sufficiently establish a reason to set aside and reverse the Decision dated 03 February 2022. The Commission, therefore, reiterates its Decision dated 03 February 2022 finding DSL liable for Unauthorized Disclosure under Section 32 of the DPA and recommending for his prosecution to the Department of Justice.

³⁹ See Comment, 06 October 2021, Annexes 2-8, *in MVC, et al. v. DSL*, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).

NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015
MVC v. DSL, RRB v. DSL,
NMB v. DSL, RMP v. DSL,
NDL v. DSL, and MBN v. DSL

Resolution

Page 11 of 12

WHEREFORE, premises considered, the Commission resolves to **DENY** the Motion for Reconsideration dated 05 April 2022 filed by DSL. The Decision dated 03 February 2022 is hereby **AFFIRMED**.

SO ORDERED.

City of Pasay, Philippines.
13 October 2022.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

JOHN HENRY D. NAGA
Privacy Commissioner

Copy furnished:

MVC
Complainant

RRB
Complainant

NMB
Complainant

RMP
Complainant

NDL

NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015

*MVC v. DSL, RRB v. DSL,
NMB v. DSL, RMP v. DSL,
NDL v. DSL, and MBN v. DSL*

Resolution

Page 12 of 12

Complainant

MBN

Complainant

CHRISTIAN BENEDICT T. BRIBON

Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

RTB,

Complainant,

-versus-

**EAST WEST BANKING
CORPORATION,**

Respondent.

X

X-----
RESOLUTION

NPC 21-086

For: Violation of
the Data Privacy
Act of
2012

AGUIRRE, D.P.C.;

Before the Commission is the Compliance and Manifestation (Re: Letter/Order dated 25 April 2022 and Decision dated 03 February 2022) dated 02 May 2022 submitted by East West Banking Corporation (EWBC) in relation to the payment of nominal damages to RTB.¹

Facts

On 03 February 2022, the Commission issued a Decision dismissing the complaint filed by RTB against EWBC upon determining that EWBC's processing of RTB's personal information was based on a lawful criterion under Section 12 (b) of the Data Privacy Act of 2012 (DPA).² As a consequence of EWBC's carelessness in the processing of RTB's personal information, however, the Commission awarded nominal damages to RTB.³ In this case, EWBC did not comply with

¹ Compliance and Manifestation (Re: Letter/Order dated 25 April 2022 and Decision dated 03 February 2022), 02 May 2022, in RTB v. East West Banking Corporation, NPC 21-086 (NPC 2022).

² RTB v. East West Banking Corporation, NPC 21-086, 03 February 2022, available at <https://www.privacy.gov.ph/wp-content/uploads/2022/04/NPC-21-086-RTB-v.-East-West-Banking-Corporation-Decision-2022.02.03..pdf> (last accessed 01 August 2022).

³ *Id.*

its obligation as a Personal Information Controller under Section 11

(c) of the DPA.⁴ The dispositive portion of the Decision states:

WHEREFORE, premises considered, the Commission resolves to **DISMISS** the Complaint of RTB against East West Bank Corporation (EWBC). The Commission **AWARDS** nominal damages, in the amount of Fifteen Thousand Pesos (P15,000.00), to RTB for EWBC's failure to fulfill its obligation as a Personal Information Controller under Section 11 (c) of the Data Privacy Act of 2012. EWBC is **ORDERED** to submit its compliance within fifteen (15) days from receipt of this Decision.

SO ORDERED.⁵

EWBC submitted its Compliance and Manifestation dated 01 April 2022.⁶ It informed the Commission that it attempted to coordinate the payment of nominal damages with RTB through calls, text messages, and emails but it did not receive any response.⁷ It then manifested that RTB “may claim the Manager’s Check representing payment of nominal damages at the EastWest Bank Cavite-Silang Bank.”⁸ EWBC further offered, in the alternative, to submit the Manager’s Check with the Commission for safekeeping.⁹

Thereafter, the National Privacy Commission’s Enforcement Division (EnD) sent emails to RTB to confirm if EWBC had paid the nominal damages and to verify the date and proof of payment.¹⁰

On 25 April 2022, the EnD also sent a letter to EWBC, through its counsel, instructing EWBC to comply with the Decision dated 03 February 2022 and to submit proof of compliance within ten (10) days from receipt of the letter.¹¹ On the same day, RTB replied to the EnD’s email and submitted photos of the Manager’s Check dated 01 April 2022 in the amount of Fifteen Thousand Pesos (P15,000.00) and the

⁴ *Id.* at 5.

⁵ *Id.*

⁶ Compliance and Manifestation (Re: Decision dated 03 February 2022), 01 April 2022, at 1, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2022).

⁷ *Id.*

⁸ *Id.* at 2.

⁹ *Id.*

¹⁰ Email *from* Enforcement Division, National Privacy Commission, to RTB (20 April 2022); Email *from* Enforcement Division, National Privacy Commission, to RTB (21 April 2022); Email *from* Enforcement Division, National Privacy Commission, to RTB (25 April 2022).

¹¹ Re: Compliance with the Decision dated 03 February 2022 in NPC 21-086 entitled “RTB vs. East West Banking Corporation”, 25 April 2022, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2022).

acknowledgement receipt with his signature.¹² In his email, RTB also stated that he “[w]ill still file for a Motion for Reconsideration.”¹³

In response to the EnD’s letter, EWBC filed its Compliance and Manifestation (Re: Letter/Order dated 25 April 2022 and Decision dated 03 February 2022) dated 02 May 2022.¹⁴ It informed the Commission that on 06 April 2022, it released the Manager’s Check dated 01 April 2022 in the amount of Fifteen Thousand Pesos (P15,000.00) to RTB through its Cavite-Silang Branch.¹⁵ As proof of compliance, it submitted a copy of the acknowledgement receipt that RTB signed.¹⁶

Discussion

The Commission resolves to close the case.

The Commission notes that EWBC complied with the order to pay RTB nominal damages in the amount of Fifteen Thousand Pesos (P15,000.00) as stated in the Decision dated 03 February 2022.¹⁷ The acknowledgement receipt signed by RTB together with RTB’s confirmation of the payment of nominal damages through his email to the Commission are deemed sufficient to prove that the payment has been made.¹⁸

As regards RTB’s statement in his email that he intends to file a Motion for Reconsideration,¹⁹ the Commission notes that he did not file a Motion for Reconsideration within the prescribed period under NPC Circular 2021-01 (2021 NPC Rules of Procedure).

WHEREFORE, premises considered, Commission resolves that NPC 21-086 – RTB v. East West Banking Corporation is hereby **CLOSED.**

¹² Email from RTB, to Enforcement Division, National Privacy Commission (25 April 2022).

¹³ *Id.*

¹⁴ Compliance and Manifestation (Re: Letter/Order dated 25 April 2022 and Decision dated 03 February 2022, 02 May 2022, *in* RTB v. East West Banking Corporation, NPC 21-086 (NPC 2022).

¹⁵ *Id.* at 1.

¹⁶ *Id.* Annex A.

¹⁷ *See id.*

¹⁸ Email from RTB, to Enforcement Division, National Privacy Commission (25 April 2022).

¹⁹ *Id.*

Further, East West Banking Corporation's Compliance and Manifestation (Re: Letter/Order dated 25 April 2022 and Decision dated 03 February 2022) dated 02 May 2022 is hereby **NOTED**.

SO ORDERED.

City of Pasay, Philippines.
28 July 2022.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

JOHN HENRY D. NAGA
Privacy Commissioner

DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

RTB
Complainant

ONA PAMFILO & BUBAN LAW OFFICES
Counsel for East West Banking Corporation

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

**IN RE: DATA BREACH INVOLVING
THE COMELEC DATA PROCESSING
SYSTEM IN WAO, LANAOS DEL SUR**

NPC BN 17-002
*For: Violation of
Data Privacy Act
of 2012*

X-----X

RESOLUTION

NAGA, D.P.C.:

Before this Commission is the Compliance¹ submitted by the Commission on Elections – Wao, Lanao del Sur (COMELEC), in compliance with the orders of the Commission indicated in its Decision dated 15 August 2019.

Facts

On 28 January 2017, COMELEC submitted a Data Breach Notification Report to the Commission which narrated a potential data breach that occurred in its regional field office located in the Municipality of Wao, Province of Lanao del Sur.

According to the report, unidentified men broke into the office and took one of the desktop computer units containing programs used for registration and storage of both sensitive and personal information of registered voters.²

In another letter dated 3 February 2017, COMELEC EDT sent to the Commission a formal data breach report. According to the report, the incident was discovered by MA , who noticed that the door was

¹ Compliance letter dated 07 December 2019.

² Letter by COMELEC Executive Director dated 28 January 2017.

opened leading to the office of CTL , the EO of Wao, Lanao del Sur and the computer unit installed was missing. Unidentified persons were suspected of gaining entry to the office. The incident was immediately reported to CTL and to the police authorities on the same day.³

The stolen computer contained the following systems and programs:

- 1) Voter Registration System (VRS) - the application used by EO to encode the demographic data, and to capture the biometrics data, of applicants for registration. The output of VRS is the list of registered voters for the Municipality of Wao. The VRS contains a total of fifty-eight thousand three hundred and sixty- four (58, 364) registration records for the Municipality of Wao.
- 2) Voter Search (VS) – the application uses the National List of Registered Voters to determine if an applicant is already registered in the same, or another, city/municipality to enable the EO to advise the applicant which of the following application should be filed such as registration, reactivation, transfer/transfer with reactivation, change/correction of entries, and inclusion/reinstatement of records in the list of voters.
- 3) National List of Registered Voters (NLRV) - the database containing the demographics data, with no biometrics data, of all registered voters in the country (both active and deactivated). The NLRV contained approximately seventy-five million eight hundred ninety-eight thousand three hundred and thirty-six (75, 898, 336) records as of 17 October 2016.⁴

Both the VRS and NLRV contains personal and sensitive personal information, specifically as follows: Name; Sex; Civil Status; Name of spouse, if married; Precinct and Precinct Code; Address (Street, Barangay, City/Municipality, and Province); and Birthday.

³ Data Breach Notification Report submitted by COMELEC Office of the Executive Director dated

3 February 2017.

⁴ *Id.* at p. 3.

On 07 February 2017, the Commission issued an Order⁵ for on-site Examination of Systems and Procedures to obtain more information in connection with the robbery incident in the Municipality of Wao. The Commission ordered the OEO (OEO) of the COMELEC in Taguig and Muntinlupa City to cooperate with the investigation and allow the on-site examination of its systems and procedures by officials and representatives of the Commission.

On 08 February 2017, the Commission conducted the on-site examination in the COMELEC office in Taguig City. A preliminary report on the on-site inspection was submitted by the Commission on 09 February 2017.

On 10 February 2017, the Commission En Banc issued a Compliance Order⁶, ordering COMELEC to erase all NLRV RV in the computer systems in different municipalities and cities and to notify the affected data subjects, among others. COMELEC was also ordered to submit its proposed revised measures in the voters' registration process in keeping with the Data Privacy Act (DPA) and other issuances of the Commission.

On 28 February 2017, EDT submitted to the Commission a Compliance Report in response to the Compliance Order dated 10 February 2017. The report stated the modifications implemented in the VRS, VS, and NLRV systems of the COMELEC in terms of registration of voters and access to the system. COMELEC also stated that it has notified the affected data subjects through publication of the notice through newspapers of general circulation in the Philippines. For those with records in the VRS in the Municipality of Wao, notification was done individually.⁷

On 09 February 2018, CTL received from the Commission a fact-finding report recommending him to be held liable for negligence in relation to the robbery incident and the purported concealment of the data breach incident to the Commission and the data subjects.

⁵ Order for On-site Examination of Systems and Procedures dated 7 February 2017.

⁶ Compliance Order dated 10 February 2017.

⁷ Compliance Order submitted by COMELEC dated 28 February 2017. At p. 2 and 4.

On 12 March 2018, CTL executed an affidavit contending that he was not negligent from the moment he assumed the duties as an EO of Wao, Lano del Sur. According to CTL, he implemented necessary precautions to ensure security of the office such as installing padlocks, assigned a casual officer to ensure security of the office, and installed strong passwords on the computer. CTL also stated that he immediately informed the PES ANY, of the incident the day after. He also went to the police station of the Municipality of Wao on the same day the robbery occurred to report the incident.

On 15 August 2019, the Commission En Banc promulgated its Decision ruling that there was no negligence on the part of CTL as he was able to implement reasonable and appropriate security measures to prevent the taking of the desktop computer containing personal data. The Commission held that, with COMELEC's continued efforts to strengthen security measures, there was insufficient evidence to warrant a criminal prosecution for providing access due to negligence.⁸

The Commission also ruled that there was no concealment of the personal data breach. Based on the case records, the incident was reported to the superiors of the office on the same day it was discovered by its employees. The policemen in the locality were also apprised of the incident and immediately conducted an investigation.

Further, the Commission ordered COMELEC to comply with the following orders within thirty (30) days from receipt of the decision:

- 1) The designation of Data Protection Officers/Compliance Officers for Privacy for every Regional Unit and the names and contact information thereof;
- 2) A copy of its Security Incident Management Policy, pursuant to Sections 4 and 5 of NPC Circular 16-04, including documents demonstrating:
 - a. Creation of its Breach Response Team, and the composition of thereof;

⁸ Decision dated 15 August 2019. At pp. 6 to 7.

- b. Dissemination of this Security Policy to all election field offices;
- 3) Complete Post-Breach Report on its management of this Personal Data Breach in compliance with Section 9 of NPC Circular 16-03.19

In a letter dated 07 December 2019, COMELEC submitted its compliance along with the pertinent attachments as proof of compliance with the orders of the Commission.

Discussion

The Compliance submitted by COMELEC conforms with the orders of the Commission.

In its Compliance Letter dated 07 December 2019, COMELEC attached the List of Data Protection Officers/Compliance Officers for Privacy of every Regional Unit with their contact information. COMELEC also attached their Security Management Policy and Post- Breach Report.

The List of Data Protection Officers/Compliance Officers for Privacy of every Regional Unit with their contact information and their functions was embodied in COMELEC 's Memorandum addressed to all REDs with the subject Security Measures and Controls on Data Privacy dated 01 February 2017.

In terms of their Security Management Policy, the said Memorandum also contains the interim security measures and controls to be implemented by all field offices which states that the access to personal data be restricted to the heads of filed office concerned and their duly representatives. It also included protocols on access of personal data such as logging of date, time, purpose of such access, and nature of data accessed, among others.

Further, the Memorandum ordered for the accountable officers to protect personal data from loss; and unauthorized access, disclosure, alteration or misuse.⁹ COMELEC also provided proof that the Security Measures and Controls on Data Privacy is disseminated to all election field offices.¹⁰ A copy of the Memorandum dated 30 June 2017 was also attached addressed to all RED's, PES's, and EO's ordering the immediate compliance to their Security Incident Management Policy.

Additionally, COMELEC also provided the copy of the Memorandum¹¹ stating that in the Minute Resolution 17-0110, COMELEC's Commission En Banc approved the recommendations of their Data Protection Officer (DPO), EDT. Part of the DPO's recommendation stated that the ARMM Compliance Officer (ARMM- CO) shall issue the notices to the registered voters whose personal information were affected by the incident. The ARMM-CO shall also coordinate with the Administrative Services Department and the Finance Service Department on the logistical requirements for purposes of complying to the sending of notices to the data subjects.¹²

Moreover, the Memorandum also stated that the appointed the Response Team consists of the Executive Director, Finance Services Department, Administrative Service Department, and Information Technology Department.

COMELEC has also distributed to the field offices COMELEC ICT Policy No. ICT-2017-001 which is the Field Office Systems and Data Policy. This is the new system adopted by COMELEC for VR. According to a Technical Report issued by the Commission's Enforcement Division (EnD), the technical measures employed by COMELEC are sufficient to prevent future data exploits.¹³

⁹ COMELEC Memorandum: Security Measures and Controls on Data Privacy dated 01 February 2017.

¹⁰ Proof of sending Security Measures and Controls on Data Privacy through e-mail, Compliance Report.

¹¹ COMELEC Memorandum: Data Breach in Wao, Lanao del Sur dated 05 December 2019.

¹²*Id.* at p. 1.

¹³ Technical Report on BN 17-002 In re: Data Breach Notification dated 28 January 2017 of the COMELEC.

In its Post-Breach Report, COMELEC documented the actions it implemented since the occurrence of the breach incident.¹⁴ COMELEC included a copy of the Memorandum dated 23 January 2017 with the subject Report on NPC Workshop-Conference. The Report includes the finalization of their Privacy Impact Assessment (PIA) submitted to the Commission on 27 February 2017.

Further, among the actions taken was the installation of CCTV cameras in all field offices as an added security measure. According to COMELEC, there will be series of seminars in relation to security measures and data protection in connection with the DPA. There will also be an introduction of a new program for the COMELEC VR system which will improve the current VRS and VS systems.¹⁵

Through careful review and evaluation of the contents of the Compliance submitted, this Commission finds that the submissions and actions implemented by COMELEC are adequate, sufficient, and compliant to its order indicated in its Decision dated 15 August 2019.

Moreover, this Commission would like to take this opportunity to remind Personal Information Controllers (PICs), specially government agencies whose processing of personal and sensitive personal information, that establishing a resilient organizational, physical, and technical security measures and data privacy policies intended to prevent or minimize the occurrence of a data breach is important aspect of abiding by our mandates.¹⁶ This Commission reiterates that such measures are not only designed for legal compliance but more importantly it aims to protect both the PICs and data subjects from the possibility and/or effects of a data breach.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 17-002 “In re: COMELEC Data Processing System In Wao, Lanao Del Sur” is hereby considered **CLOSED**.

SO ORDERED.

¹⁴ Memorandum issued by COMELEC Main Office regarding the breach incident in Wao, Lanao Del Sur dated 20 February 2017, Compliance Report.

¹⁵ *Id.*

¹⁶ Section 20 of R. A. 10173 or the Data Privacy Act of 2012

Pasay City, Philippines;
08 July 2021.

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

JMTJR
Data Protection Officer and Executive Director
COMELEC

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

X-----X

RESOLUTION

**NAGA,
D.P.C.:**

This Resolution refers to the data breach notifications that the Commission received on four (4) separate occasions dated as follows: 17 December 2016; 18 October 2017; 25 October 2017; and 26 October 2017 from Jobstreet.com (Jobstreet) in relation to a data breach pertaining to a single data set containing sensitive personal information of more than seventeen (17) million users.

The Facts

In 2017, Jobstreet submitted data breach notifications on four (4) separate occasions dated 17 December 2016, 18 October 2017, 25 October 2017, and 26 October 2017 before this Commission. The notifications involve similar incident in which Jobstreet's IT Manager discovered a website forum concerning the purported sale of data belonging to, "Jobstreet.com".

On 09 November 2017, Jobstreet submitted a Cyber Incident Analysis which stated that the data pertains to a single set and contains the personal information of more than seventeen (17) million users. According to the said report, the data set was not recent and was last updated on 07 March 2012. The report also stated that the data set was more likely obtained before June 2012. Lastly, Jobstreet's investigation concluded that there were no evidence that the compromised accounts were accessed by unauthorized person/s.

In terms of security and remediation measures, Jobstreet has implemented the following actions:

1. notified the affected data subjects;

2. implemented a password reset policy; and
3. provided information on how data subjects can secure their personal information.

On 01 August 2019, this Commission issued a Resolution¹ directing Jobstreet to submit a complete report on its Personal Data Breach Management within thirty (30) days upon receipt of the Order. The said Resolution was delivered to Jobstreet in Malaysia through DHL Express² on 16 August 2019; however, Jobstreet failed to comply within the prescribed period.

On 15 July 2020, this Commission's Enforcement Division (EnD) sent a Compliance Letter to Jobstreet's Data Protection Officer (DPO), MM, instructing Jobstreet to comply with the abovementioned Resolution. The said letter was received on 03 August 2020³, where again, Jobstreet failed to submit the report required by this Commission.

Discussion

This Commission finds that the submission of Personal Data Breach Management report as a necessary step to improve the personal data breach management and policies of Personal Information Controllers (PICs) such as Jobstreet. **Section 9 of the NPC Circular 16-03 provides:**

"All actions taken by a personal information controller or personal information processor shall be properly documented. Reports should include:

- a. Description of the personal data breach, its root cause and circumstances regarding its discovery;
- b. Actions and decisions of the incident response team;
- c. Outcome of the breach management, and difficulties encountered; and
- d. Compliance with notification requirements and assistance provided to affected data subjects.

A procedure for post-breach review must be established for the purpose of improving the personal data breach management policies and procedures of the personal information controller or personal information processor."
(Emphasis Supplied)

¹ Resolution dated 01 August 2019

² DHL Express Proof of Delivery dated 30 June 2020

³ Proof of Delivery dated 03 August 2020

As often reminded by this Commission in previous cases, the complete submission of reports, including the policies and procedures that govern imperative actions performed by PICs in cases of data breach, are one of its strict responsibilities under the Data Privacy Act (DPA) and the NPC Circular 16-03. Further, this Commission deem such reports as necessary not only for the Commission to ascertain the actions implemented by Jobstreet to prevent the recurrence of the breach, reduce its harm, and protect the affected data subjects, but to provide the opportunity to continuously develop and strengthen its personal data breach management policies and procedures to lessen the risks of serious harm and protect personal information in the event of a data breach. Such is also in accordance with Section 20 (a) of the DPA, *viz*: “(a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.”

While Jobstreet sent several submissions, participated in coordination meetings, and provided numerous updates to the Commission on its investigation, security and remediation measures, and breach management, it failed to provide the proper documentation of such actions which is required under NPC Circular 16-03. Despite the Commission’s reminder to Jobstreet of its obligation to comply to its Resolution dated 01 August 2019, which was reiterated through the Compliance Letter dated 15 July 2020 sent by EnD, the Commission has not yet received Jobstreet’s Personal Data Breach Management report.

Furthermore, this Commission clarifies and reiterates that in cases of data breach, the PICs’ obligations does not end with the mere provisions of updates on their investigation and the measures it implemented. Compliance with the law also warrants the PICs’ rigorous and complete submission of documents required by the Commission and timely observance of its orders.

WHEREFORE, premises considered, Jobstreet.com is hereby **ORDERED** to comply with the following **within ten (10) days from receipt of this Order**:

1. **SUBMIT** a Personal Data Breach Management report in compliance with Section 9 of the NPC Circular 16-03; and

2. **SHOW CAUSE** in writing why it should not be subject to contempt proceedings, as permitted by law, before the appropriate court, and other actions as may be available to the Commission, for its failure to comply with the Resolution dated 01 August 2019 and the Compliance Letter dated 15 July 2020.

SO ORDERED.

Pasay City, Philippines;
17 December 2020.

(Sgd.)

JOHN HENRY D. NAGA

Deputy Privacy Commissioner

WE CONCUR:

(Sgd.)

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

(Sgd.)

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

COPY FURNISHED:

MM

Data Protection Officer, General Counsel

Seek Asia (Jobstreet.com Shared Services Sdn. Bhd.)

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION***NAGA,
D.P.C.:***

This Resolution refers to the data breach notification report that the Commission received from the Social Security System (SSS)¹ dated 04 November 2017 involving the unauthorized disclosure of personal information of an SSS member.

The Facts

On 16 November 2017, this Commission received a breach notification report from SSS dated 04 November 2017 involving the unauthorized disclosure of personal information of MSA, a member of SSS. The Senior Representative of SSS Malolos Branch, FCPJ, posted the Member Data Form (E-1) of MSA on the Facebook Page “Malayang Kawani ng SSS” on 29 March 2017. The aforementioned posting was reported to the SSS by a concerned employee on 28 October 2017.

The E-1 Form contained the following personal information of MSA: (1) Name of SSS Member; (2) Address; (3) Social Security Number; (4) Birth date; (5) Parents’ Name; (6) Beneficiaries; and (7) Specimen Signature.

To address the data breach that had occurred, FL, SSS Malolos Branch Head, called the attention of FCPJ and required him to delete the post. On 03 November 2017, FL and FCPJ went to the residence of MSA to explain the incident and apologize.

To prevent further occurrence of the breach, GS, the Data Protection Officer (DPO) of SSS and members of the Data Breach Response Team requested the assistance of the Facebook Page administrators to confirm the deletion of the post. Also, the

¹ SSS Breach Notification Report dated 04 November 2017

administrators were requested to become advocates of data privacy and exercise vigilance in ensuring that their page is in compliance with the Data Privacy Act of 2012 (DPA).

The affected data subject did not file any complaint in relation to the said breach.

On 15 August 2019, this Commission issued a Resolution² disposing, thus:

“WHEREFORE, premises considered, this Commission finds that no further action is necessary in this case, without prejudice to such other relief in case of new information. The SSS is **ORDERED** to submit a complete report on its management of this Personal Data Breach in compliance with Section 9 of Circular 16-03, within thirty (30) days from receipt of this Order.”

On 11 October 2019, SSS submitted a Compliance Report³ dated 09 October 2019 before this Commission.

Discussion

The Compliance Report submitted by SSS is deemed sufficient.

The SSS Compliance Report contained the following attachments:

1. Incident Report submitted by the Head of SSS Malolos Branch;
2. Photos of the SSS Malolos Branch Head, together with the Senior Member Service Representative (MSR) and OIC Section Head, who personally informed and apologized to the data subject about the incident on 03 November 2017;
3. Hand-written letter of the affected data subject dated 03 November expressing his intention not to file complaint against Senior MSR now or in the future;
4. Proof of confirmation by the administrators of the Malayang Kawani ng SSS Facebook page on 03 November 2017 of the deletion of the post from page on 30 March 2017;

² Resolution dated 15 August 2019

³ SSS Compliance with NPC Resolution dated 15 August 2019 “Re: Data Breach Notification of SSS” NPC BN 17-032, dated 09 October 2019

5. Data Breach Notification Report submitted to NPC on 04 November 2017, thru email; and
6. Office Memorandum confirming the conduct of series of seminars to SSS Personnel on Data Privacy Act of 2012 from 26 October 2017 to 17 January 2018.

As provided in Section 9 of the NPC Circular 16-03, all actions that are implemented by a Personal Information Controller (PIC) shall be properly documented, which shall include the following:

- A. Description of the personal data breach, its root cause and circumstances regarding its discovery;
- B. Actions and decisions of the incident response team;
- C. Outcome of the breach management, and difficulties encountered; and
- D. Compliance with notification requirements and assistance provided to affected data subjects.

A procedure for post-breach review must be established for the purpose of improving the personal data breach management policies and procedures of the personal information controller or personal information processor.⁴

In the attached Incident Report and Data Breach Notification Report, SSS has identified description of the personal data breach, its root cause and discovery. SSS stated in the Reports that the posting was done in a Facebook Closed Group and was made by FCPJ with no malicious intent as he only seeks clarification and advice from the SSS employee using the E-1 Form of MSA. Upon discovery, the PIC immediately reached out to FCPJ and requested him to delete the post.

Furthermore, this Commission finds that the SSS through their Malolos Branch Head with their Senior MSR and OIC Section Head, have effectively informed the affected data subject of the incident by personally appearing to explain and apologize to him. With this, the Commission notes the attached hand-written letter of the affected data subject expressing his intention not to file complaint in relation to the breach.

In terms of the remediation measures, SSS has implemented sufficient measures, such as providing proof of confirmation by the administrators of the Malayang Kawani ng SSS Facebook page of

Section 9 of NPC Circular 16-03

the deletion of the post, as well as their compliance to the Notification Requirement through the timely submission of the Data Breach Notification Report before this Commission.⁵

In addition, to improve their data breach management and to prevent similar incidents in the future, SSS conducted a series of seminars to acquaint their personnel with the DPA, its IRR, and other related issuances of this Commission.

Through careful review and evaluation of the contents of the report submitted, this Commission finds that the abovementioned submission and actions implemented by SSS are adequate, sufficient, and compliant to its order indicated in its Resolution dated 15 August 2019.

Moreover, this Commission takes this opportunity to stress to PICs, specifically to government agencies whose processing of personal and sensitive personal information are vital in fulfilling their mandate, the significance of implementing robust organizational, physical, and technical security measures and data privacy policies intended to prevent or minimize the occurrence of a data breach.⁶ Such measures are not only designed for legal compliance but more importantly it aims to protect both the PICs and data subjects from the possibility of a data breach.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 17-032 “In re: SSS” is hereby considered **CLOSED**.

SO ORDERED.

Pasay City, Philippines;
21 January 2021.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

⁵ Section 17 of the NPC Circular 16-03

⁶ Section 20 of R. A. 10173 or the Data Privacy Act of 2012

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

JAV
Data Protection Officer
SSS

GMJDS
Data Protection Officer, VP – Program Services Division
SSS

RCG
Data Protection Officer
SSS

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISON
GENERAL RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION

NAGA, D.P.C.:

This Resolution refers to the data breach notification report dated 21 March 2018 that the Commission received from Acesite (Phils.) Hotel Corporation (Acesite) in relation to the loss of personal data caused by fire.

The Facts

On 18 March 2018, a significant portion of the Hotel was razed by fire.

According to the report of the Bureau of the Fire Protection, the fire was caused by high-temperature electric discharge of a wiring inside the ceiling near the slot machine area, which resulted in short circuit accompanied by a massive electrical ignition. Further, the detected electric default was caused by prolonged usage and normal wear and tear of conductive material of the electrical wiring.¹

The significant portion of the Hotel was affected by the fire and caused damages to the properties of the Hotel including several records containing data relating to the Hotel's operations, guests, and employees, among others. According to Acesite, the

¹Galupo, R. (2018). *Hotel fire accidental – BFP*. Retrieved from <https://www.philstar.com/nation/2018/09/06/1849003/manila-pavilion-hotel-fire-accidental-bfp#:~:text=MANILA%2C%20Philippines%20%E2%80%94%20The%20Bureau%20of,wiring,%E2%80%9D%20and%20deemed%20the%20investigation>

personal data possibly involved in the breach cause by the incident includes:

1. Name of guest and employees;
2. Contact Numbers;
3. Email Addresses;
4. Copies of IDs and Passports;
5. Credit Card Details: Name of Cardholder Masked Card Numbers Signature of the Guest; and
6. Employee Payroll Details:
 - Employee ID Numbers
 - SSS Contributions
 - HDMF Contributions
 - Philhealth Contributions
 - SSS ID Numbers
 - Tax Identification Numbers Pag-ibig (HDMF) Numbers.²

On 21 March 2018, Acesite sent a notification on the incident, which informed the Commission that the Hotel shall be temporarily inaccessible and non-operational.

On 29 August 2019, Acesite submitted its Full Breach Report (Report). On 13 January 2021, Acesite resubmitted the Full Breach Report.

In an Order dated 21 January 2021, the Commission required Acesite to submit an Updated Report expounding the details of the incident, supplying the lacking information required pursuant to Section 17(D) of the NPC Circular 16-03, and attaching the specified documents to further help with the investigation of the data breach incident.³ On 01 March 2021, Acesite resubmitted its Full Breach Report.

Issues

The issues in this case are follows:

² Full Report on Breach Notification dated 21 March 2018, p. 1-2.

³ Order dated 21 January 2021, p. 1-2.

1. Whether the matter is a personal data breach; and
2. Whether the matter falls under the mandatory breach notification.

Discussion

- I. *The matter reported is an availability breach with regard to the loss of the personal data caused by fire.*

This Commission finds that the matter reported by Acesite is an availability breach which is one of the natures of a personal data breach. **Section 3(F) of the NPC Circular 16-03 provides:**

F. “Personal data breach” refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:

1. **An availability breach resulting from loss, accidental or unlawful destruction of personal data;**
2. Integrity breach resulting from alteration of personal data; and/or
3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data. (Emphasis Supplied)

On the other hand, a security incident has a more extensive definition, which is an event or occurrence that affects or tends to affect data protection or may compromise the availability, integrity, and confidentiality of personal data. Further, it includes incidents that would result to a personal data breach, if not for safeguards that have been put in place.⁴

Thus, a data breach is a kind of a security incident considering that it occurs when there is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.⁵

⁴ Section 3(J) of the NPC Circular 16-03

⁵ National Privacy Commission. (n.d.). *Exercising Breach Reporting Procedures*. Retrieved from <https://www.privacy.gov.ph/exercising-breach-reporting-procedures/>

In this case, the storage and backup storage of the records and files containing personal data of the Hotel's employees and guests is within the premises of the Hotel which was significantly affected by the fire. From the moment that the records and files were destroyed by the fire, the incident becomes an occurrence which affected the data protection and compromised the availability of the personal data of the Hotel's employees and guests.

Considering that the records and files were accidentally destroyed and the personal data of employees and guests were lost, the incident is within the nature of an availability breach resulting from loss and accidental destruction of personal data which cannot be retrieved anymore.

II. The incident does not fall within the scope of the mandatory breach notification requirements.

This Commission finds that this case does not fall under the mandatory breach notification requirements. In order to determine whether an incident falls under the mandatory breach notification requirement, **Section 11 of the NPC Circular 16-03 provides:**

Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

- a. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

- b. There is reason to believe that the information may have been acquired by an unauthorized person; and
- c. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

With the data breach being caused by fire that resulted to the accidental destruction of the personal data involved, there is no reason to believe that the personal data of the Hotel's guests and employees may have been obtained by an unauthorized person and may give rise to real risk of serious harm to the affected data subjects. Although the incident involves personal and sensitive personal information which satisfies the first criteria of the abovementioned section, in order to fall within the scope of the mandatory breach notification requirement, it must also satisfy that the incident may result to unauthorized disclosure or access of personal data and such access may give rise to real risk of serious harm to the affected data subjects.

Thus, with the case only satisfying the first criteria of the Section 11 of the NPC Circular 16-03 and the matter being classified as an availability breach, the notification is not mandatory in this case.

However, in an Order dated 21 January 2021, the Commission through the Complaints and Investigation Division (CID), required Acesite to attach specified documents to further help with the investigation of the incident and submit the lacking information from its initial notification, specifically:

- 1. Nature of the Breach
 - a. Description or nature of the personal data breach;
 - b. Description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;**
 - c. A chronology of the events leading up to the loss of control over personal data;
 - d. Approximate number of individuals and/or personal records affected;**

e. Description of the likely consequences of the personal data breach on the institution, data subjects and the public;

f. Description of safeguard in place that would minimize harm or mitigate the impact of the personal data breach;

- Attach and specify on a report the changes in the data privacy and security policy after the incident particularly on the storage and availability of personal data; Name and contact details of the data protection officer or any other accountable persons.

2. Personal Data Possibly Involved

- a. List of the sensitive personal information involved;
- b. List of other information involved that may be used to identity fraud;

3. Remedial Measures Taken Subsequent to Suspected Breach

a. Description of the measures taken or proposed to be taken to address the breach;

b. Actions being taken to secure or recover the personal data that were compromised;

c. Actions performed or proposed to mitigate or limit the possible harm or negative consequences, damage or distress to those affected by the incident;

d. Actions being taken to inform the data subjects affected by the incident or reasons for any delay in the notification in accordance with Section 21 of the said Circular;

e. The measures being taken to prevent a recurrence of the incident.

- Physical, organizational and technical measures undertaken after the incident, as well as proof thereof.
- Where is your backup storage located prior to and after the incident?

In response to the Order, on 01 March 2021, Acesite resubmitted its Report dated 21 March 2018. This Commission notes that Acesite stated in the Report that as part of the mitigating measures and considering that most of the documents were destroyed by the fire, the remaining documents which were beyond retrieval were destroyed through shredding last August 2018. According to Acesite, as a preventive measure against future similar incident, the backup storage of their data will now be isolated in a different location. Acesite also committed to conduct

a Privacy Impact Assessment (PIA) and information asset inventory once the hotel is operational again.⁶

However, the Report resubmitted was the same document initially submitted by Acesite on 29 August 2019 with no new information, additional updates, and attachments required by the previous Order. The resubmitted Report also lacks the updates on the conduct of the PIA and information asset inventory which was initially stated in Acesite's Report and details on the security measures implemented such as details on the isolated backup storage they were planning to implement.

With the resubmission of its initial Report, Acesite has yet to comply with the submission of an Updated Report that consists of the essential information required in the Commission's previous Order dated 21 January 2021.

This Commission then emphasizes that in cases of data breach, including an availability breach, it is within the obligations of the PICs that any or all of their reports are to be made available to the Commission.⁷ Moreover, the Commission stresses that the lacking information being required is essential in order for the Commission to be able to identify whether adequate actions were implemented by the PIC to avoid further damage and recurrence of similar incidents, and protect the rights of the data subjects. The Commission's evaluation of such information will not only be beneficial to the data subjects but also to the PICs in improving their personal data breach management policies and procedures.

WHEREFORE, premises considered, Acesite is hereby **ORDERED** to comply with the following within **fifteen (15) days** from receipt of this Resolution:

1. **SUBMIT** its Updated Report with the contents required in the Order dated 21 January 2021; and

⁶ Ibid. at p. 2.

⁷ Section 22 of the NPC Circular 16-03

2. **SUBMIT** proof and details of the measures taken to address the breach, such as but not limited to, details of implementation of isolated backup storage, information asset inventory, and Privacy Impact Assessment (PIA).

SO ORDERED.

Pasay City, Philippines;
15 April 2021

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

JTL
Data Protection Officer

**COMPLAINTS AND INVESTIGATION DIVISION GENERAL
RECORDS UNIT**
National Privacy Commission

**IN RE: MANILA SHARED SERVICES
EMPLOYEES CREDIT AND
SAVINGS COOPERATIVE**

NPC BN 18-186
(Formerly CID BN 18-186)

X-----X

RESOLUTION

LIBORO, P.C.:

This case before the Commission is a breach notification report from Manila Shared Services Employees Credit and Savings Cooperative (MSSECSC) concerning the unauthorized disclosure of data subjects' information caused by a misdirected email.

Facts

On 27 July 2018, the Cooperative's associates accidentally transmitted the Statement of Accounts (SOA) containing the full name, share capital and savings deposit, and existing loan balances of its three (3) members to another recipient who is not entitled to receive the same when the aforementioned associates transmitted the SOA of the latter using mail merge.¹

On 02 August 2018, MSSECSC conducted a breach investigation and undertook the following measures to address the incident: i) It ordered the discontinuance of its original practice of sending SOA to all its members using email. As an alternative, it instead manually distributes the SOA to its members in order to prevent further disclosure or exposure; ii) It also sent notification to the affected data subjects; and iii) Asked the recipient who mistakenly received the email for its immediate deletion.²

¹ SOA Incident Report

² Fact-Finding Report dated 25 March 2021, page 2 of 4

On 28 October 2020, the Commission, through the Complaints and Investigation Division (CID), issued an Order requiring MSSECSC to submit a Post Breach Report detailing the incident, pursuant to NPC Circular No. 16-03 on Personal Data Breach Management.³

On 12 November 2020, the MSSECSC sent via email, a response to the aforementioned Order of the Commission.

Issue

Whether or not MSSECSC has implemented reasonable and appropriate measures to address the incident.

Discussion

MSSECSC had implemented reasonable and appropriate measures in addressing the unauthorized disclosure of the data subjects' information caused by a misdirected email.

Section 11 of NPC Circular No. 16-03 provides the criteria when notification is required:

1. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
2. There is reason to believe that the information may have been acquired by an unauthorized person; and

³ Id.

3. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

Further, Section 20(b) of the Republic Act No. 10173 known as the Data Privacy Act of 2012 (DPA) requires the personal information controller to implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

In this breach notification before the Commission, the information in the said accidental disclosure contains the full name, share capital, savings deposit, and existing loan of the data subjects that can be used to directly and certainly identify them. Hence, in light of the above- cited provisions, it is evident that there was a necessity for MSSECSC to notify both this Commission and the affected data subjects due to the significant risk associated with it, and the likelihood that the information contained therein may be used to vitiate the privacy of the data subject.

MSSECSC, taking the mandates of the DPA in mind, undertook swift remediation measures to protect the personal information contained on the said e-mail against human dangers. It immediately stopped sending the SOA via email and made efforts to notify the Commission⁴ and the affected data subjects through a letter to the recipient who was not entitled to receive the same, asking for its immediate deletion⁵.

Accordingly, the Commission resolved that the prompt notifications to the Commission and to the affected data subjects and the remediation measures implemented by MSSECSC are considered reasonable and appropriate remediation measures to address, correct, and mitigate the incident that can lead to issues arising from data breach.

⁴ Breach Notification dated 02 October 2018.

⁵Manila Shared Services Employees Credit and Savings Cooperative's Incident Report

WHEREFORE, premises considered, this Commission hereby resolves that NPC BN 18-186 – In re: Manila Shared Services Employees Credit and Savings Cooperative is now considered **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
29 April 2021.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
LEANDRO ANGELAO Y. AGUIRRE
Deputy Privacy Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

H.A.
*Authorized Representative of
Manila Shared Services
Employees Credit And
Savings Cooperative*

COMPLAINTS AND INVESTIGATION DIVISION

**ENFORCEMENT DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

X-----X

RESOLUTION

AGUIRRE, D.P.C.:

This Resolution refers to the Breach Notification Report¹ dated 24 October 2018 submitted by Infosys BPM-Philippines (Infosys) to this Commission.

The Facts

On 24 October 2018, a Human Resource (HR) personnel from Compensation and Benefits unintentionally disclosed the Marital Status of a fellow employee to unauthorized individuals via e-mail.²

On 26 October 2018, or two (2) days after the incident, the affected employee filed a complaint with the HR and Legal Department about the incident. The Corporate Counsel then forwarded the complaint to the Data Protection Officer (DPO) for further investigation.³ On the same day, the DPO called each of the nine (9) unauthorized recipients of the e-mail, and notified them to sensitize, not to forward, and ensure the deletion of the e-mail.⁴ Furthermore, an incident report was also logged in the incident management tool of the company to formalize the complaint and started the investigation.⁵

On 30 October 2018, as part of the investigation, the DPO had a meeting with the affected employee and assured her that her concern is being handled accordingly.⁶

¹ Annual Security Incident Report (Data Breach Information) dated 24 October 2018 submitted by Infosys BPM- Philippines.

² *Ibid.*

³ *Ibid.*

⁴ *Ibid.*

⁵ *Ibid.*

⁶ *Ibid.*

Infosys also reported that the effects or consequences of the incident are: (1) privacy breach of confidential information, and (2) employee dissatisfaction.⁷

Lastly, Infosys enumerated the remedial steps it has undertaken to address the incident:

- (1) The DPO called all the unauthorized recipients of the e-mail to notify them not to forward and ensure the deletion of said mail;
- (2) A Notice to Explain was issued to the erring employee who was given five (5) days from receipt to comply with the same;
- (3) An administrative hearing was conducted for the alleged offense of Serious Violation of the company Code of Conduct;
- (4) The unauthorized recipients of the e-mail were asked to sign a non-disclosure agreement;
- (5) A disciplinary sanction was given to the erring employee; and
- (6) Further awareness on Data Privacy is being conducted across the organization.

Issues

1. Whether there was a personal data breach; and
2. Whether the remedial measures implemented by Infosys BPM Philippines were sufficient to address and prevent the recurrence of the incident.

Discussion

There was a personal data breach.

This Commission finds Infosys to have committed a personal data breach.

Section 3(F) of NPC Circular 16-03 provides that:

“Personal data breach” refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, **unauthorized disclosure of, or access to, personal data** transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:

⁷ *Ibid.*

1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
2. Integrity breach resulting from alteration of personal data; and/or
- 3.A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.⁸**

In this case, there was unauthorized disclosure of an employee's sensitive personal information, which is the latter's marital status.

Hence, a personal data breach has been committed.

This Commission notes that Infosys failed to submit its Full Breach Report on the subject incident, as required by Section 17(C) of NPC Circular 16-03. It provides that:

There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. **The full report of the personal data breach must be submitted within five (5) days**, unless the personal information controller is granted additional time by the Commission to comply.⁹

Section 17(D) of the same Circular provides the necessary information for a Full Breach Report, thus:

A. The notification shall include, but not be limited to:

1. Nature of the Breach

- a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
- b. a chronology of the events leading up to the loss of control over the personal data;
- c. approximate number of data subjects or records involved;
- d. description or nature of the personal data breach;
- e. description of the likely consequences of the personal data breach; and

⁸ Emphasis supplied.

- f. name and contact details of the data protection officer or any other accountable persons.

2. Personal Data Possibly Involved

- a. description of sensitive personal information involved; and
- b. description of other information involved that may be used to enable identity fraud.

3. Measures Taken to Address the Breach

- a. description of the measures taken or proposed to be taken to address the breach;
- b. actions being taken to secure or recover the personal data that were compromised;
- c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
- d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
- e. the measures being taken to prevent a recurrence of the incident.

The Commission reserves the right to require additional information, if necessary.¹⁰

The remedial measures implemented by Infosys BPM-Philippines were sufficient to address and prevent the recurrence of the incident.

Nevertheless, the Commission notes that the Initial Report contained the necessary information of a Full Breach Report and acknowledges the remedial measures taken by Infosys to address the breach incident and protect the personal information of the affected data subject. Aside from this, it is noteworthy that the DPO communicated with the unauthorized recipients of the disclosed personal data and they were asked to sign a non-disclosure agreement.

Furthermore, the administrative hearing that was conducted, the disciplinary sanction that was imposed upon the erring employee, and the conduct of Data Privacy awareness activity across the

¹⁰ Emphasis supplied.

organization were important steps to prevent the recurrence of the incident.

Considering the actions taken by Infosys, the Commission will no longer require it to submit a full breach report.

Nevertheless, the Commission expects Infosys to take the necessary steps to ensure not only that this situation will not be repeated, but, more importantly, that it will be in a better position to safeguard the personal information of its data subjects. Infosys is sternly warned that a similar case in the future will be dealt with more severely.

WHEREFORE, premises considered, this Commission hereby resolves that the instant case NPC BN 18-217 “In re: Infosys BPM- Philippines” is considered **CLOSED** and **TERMINATED**.

Infosys BPM-Philippines is given a **STERN WARNING** that a repetition of similar instances violative of the right of data subjects or a similar conduct or infraction shall be dealt with more severely.

SO ORDERED.

Pasay City, Philippines;
17 December 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

AO
Data Protection Officer

**COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION**
GENERAL RECORDS UNIT
National Privacy Commission

IN RE: HENNES & MAURITZ**NPC BN 18-223**
(Formerly CID BN 18-223)

Initiated as an Independent NPC Investigation into the Possible Data Privacy Violations Committed by the Hennes & Mauritz.

X-----X

RESOLUTION**LIBORO, P.C.:**

Before this Commission is the Compliance submitted by Hennes & Mauritz (H&M) with the Commission's directive stated in the Resolution dated 15 April 2021.

Facts

On 15 April 2021, this Commission issued a Resolution with the following dispositive portion:

WHEREFORE, premises considered, this Commission resolves to give Hennes & Mauritz a period of thirty (30) days from receipt of this Resolution to EXPLAIN its failure to report and notify the Commission and the data subject within the required periods under NPC Circular No. 16-03.

The Resolution dated April 15 was received by H&M on 07 May 2021, in the aforesaid Resolution, the Commission determined that H&M failed to comply with the notification requirements pursuant to NPC Circular No. 16- 03 on Personal Data Breach Management. Particularly, H&M failed to promptly notify this Commission within seventy-two (72)-hours about the data breach from the time it figured out the incident on 14 November 2018, when the credit cards owner came back to the store and reported the incident.

In its letter dated 19 May 2021, H&M stated that they were unable to confirm or even have a reasonable belief that a personal data breach has occurred until a thorough investigation was conducted and completed according to the company's standard operating procedure.

Furthermore, H&M alleged that without due process, there could be many other potential and reasonable causes behind the unknown transactions and therefore may not be linked to an occurrence of data breach stemmed from the lost card found in its store.

Therefore, H&M also argued that the seventy-two (72) hour period shall apply from the time H&M concluded its investigation and not from the time the customer informed them about the incident.

Discussion

This Commission, upon reviewing the breach report and explanation submitted by H&M, finds that H&M has complied with the directive in the previous Resolution dated 15 April 2021 of the Commission and consider this matter closed.

However, this Commission would like to reiterate that Section 11 of the NPC Circular No. 16-03 provides for the requirements of notification to this Commission and to the affected data subjects regarding the existence of a data breach, *to wit*:

Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" shall include, but not be limited to data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

- B. There is reason to believe that the information may have been acquired by an unauthorized person; and
- C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

Corollary to this, Section 17 of the same Circular provides:

SECTION 17. Notification of the Commission. The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:

A. When Notification Should be Done. The Commission shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.

xxx

C. When delay is prohibited. There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days, unless the personal information controller is granted additional time by the Commission to comply.

This Commission would like to note that the counting of the seventy- two (72) hours shall be reckoned from the time the breach itself was made known to H&M. It must be noted that the breach was made known to H&M when the credit card owner came back to the store and reported the incident on 14 November 2018, a day after the breach occurred. H&M only submitted its report to its HR on 20 November 2018, and to this Commission on 28 November 2018, fourteen (14) days after the incident ensued.

It must be pointed out that the manager on duty discovered said credit card in the drawer on the night of 13 November 2018 and just recorded the same on their Lost and Found register before finally storing it in their safe/vault for security. It is understandable that any supposed subsequent actions to find and contact the data subject the next day might have been preempted by the card owner herself who went back

to the store on 14 November 2018, nevertheless, H&M should have still reported the breach to this Commission as part of the obligations as a PIC.

It is also worth noting that records show that the H&M concluded its investigation on 20 November 2018 but still belatedly notified the Commission on 28 November 2018.

At this juncture, this Commission wants to emphasize that in case of a mandatory data breach, Personal Information Controllers (PICs) have the obligation to notify the Commission and the affected data subject within the periods mandated under NPC Circular No. 16-03.

This Commission would like to note that H&M was able to demonstrate that it implemented reasonable and appropriate security measures to uphold data privacy and protection.

H&M undertook the following measures to address the data breach incident:

1. The Store Management and its Security Department investigated the facts and circumstances surrounding the incident.
2. After the completion of the investigation report, H&M through its Human Resource Department (HR) issued a Notice to Explain (NTE) letter to N.A. and M.D. to hear each side of their story.
3. Final Written Warning was served to N.A. due to neglect of duty, while dismissal from service was also served to M.D. grounded in an unauthorized taking of credit card's information for the purpose of removing funds from it.

Moreover, H&M was able to investigate and determine the circumstances of the data breach using its CCTV recordings. H&M also immediately imposed a penalty to both erring employees. A Final Written Warning was issued against the erring employee and grounded on his failure to return the credit card to the customer while on the other hand, dismissal of service was served against the other

erring employee for just cause, grounded on the unauthorized taking of credit card information and for the violation of company's Code of Conduct.

In view of the foregoing, it is therefore recognized that the security measures undertaken by H&M were sufficient in addressing the subject breach.

WHEREFORE, premises considered, this Commission **NOTES** the explanation given by Hennes & Mauritz as to its failure to report and notify the Commission and the data subject within the required periods under NPC Circular No. 16-03.

Further, this Commission resolves that the matter NPC BN 18-223 – “In re: Hennes & Mauritz” is hereby considered **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
01 June 2021.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

A.G.Z.
Data Protection Officer
H&M Hennes & Mauritz Inc.

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

X-----X

RESOLUTION

On 22 March 2020, a line list from the Research Institute for Tropical Medicine (RITM) that contained the personal information of at least nine (9) persons under investigation (PUI) for COVID-19 circulated on Twitter and Facebook. The source tracing conducted by RITM found possible persons who may have leaked the data from two (2) of their laboratories that mainly handled the data gathering.

As a response, RITM implemented a “No Cellphone Policy” within their units and circulated a non-disclosure agreement among their employees. Consequently, the Data Protection Officer (DPO) of RITM has sent a request to the National Privacy Commission (NPC) for assistance to conduct a full investigation of this matter.

The Commission reiterates the requirement of NPC Circular No. 16-03 (Circular) for a personal information controller (PIC) like RITM to have a data breach response team, which may include its DPO. As provided in the Circular, “the team must be ready to assess and evaluate a security incident, restore integrity to the information and communications system, mitigate and remedy any resulting damage, and comply with reporting requirements.”¹ Thus, the Commission finds that compliance with the Circular must first be made before NPC extends additional assistance, if warranted. The data breach response team, being the most familiar with the security incident management policy of RITM, should first conduct a proper investigation of the breach and immediately enforce the necessary remedial measures to prevent further security risks to the data subjects.

¹ NPC Circular 16-03, Section 5.

It must be stressed that notification is the general rule during a personal data breach. Considering the reported discriminations against COVID-19 patients and those who are connected or related to them, the Commission finds that this personal data breach gives rise to the risk of serious harm to those PUI whose identity may have been revealed by said breach. As such, Section 11 of the Circular requires notification upon the occurrence of this kind of personal data breach. Notably, RITM has failed to show that the breach falls under any of the exemptions allowed by law.

The Commission enjoins RITM to review its rules on personal data breach management² as a guide to the proper procedures to be undertaken during a security incident including a personal data breach to ensure the mitigation of possible harm and negative consequences to the affected data subjects.

WHEREFORE, premises considered, the request for assistance in investigation and exemption for notification is hereby DENIED. The Research Institute for Tropical Medicine is ordered to submit, within ten (10) days of receipt of this Resolution, their full breach report including, but not limited to, the following matters:

1. Facts surrounding the incident and its effects;
2. Remedial actions taken by RITM;
3. Outcome of the breach management, and difficulties encountered;
4. Security measures in place for the protection of personal data;
5. Any other policies and procedures undertaken to prevent possible harm and negative consequences to the data subject; and
6. Compliance with notification requirements and assistance provided to affected data subjects.

SO ORDERED.

Philippines.
22 June
2020.

² NPC Circular No. 16-03.

(SGD.)
RAYMUND ENRIQUEZ LIBORO
Privacy
Commissioner

WE CONCUR:

(SGD.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner
Commissioner

(SGD.)
JOHN HENRY D. NAGA
Deputy Privacy

Copy furnished:

O.B.O.
Representative for RITM

**COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

IN RE: HEALTH DELIVERY
SYSTEM, INC.

NPC BN 20-
049

X-----X

RESOLUTION

LIBORO, PC.:

For the Resolution of this Commission is the Compliance submitted by Health Delivery Systems Inc. (HDSI) to the Resolution dated 01 June 2021 issued by the Commission.

Facts

On 01 June 2021, this Commission issued a Resolution to HDSI containing the following dispositive portion, viz:

WHEREFORE, premises considered, the Commission resolves to **GRANT a final and non-extendible extension of thirty (30) days** from 19 May 2021 or until 18 June 2021 for Health Delivery System, Inc. to produce and submit the document specified in the Resolution dated 25 March 2021.

Failure to comply with the foregoing shall cause the Commission to adjudicate on the basis of the evidence on record.

On 18 June 18, 2021, the Commission received the notarized Letter- Attestation dated 04 April 2020 of Mr. FN of CSB at PDM from HDSI.

According to Ms. SNR, HDSI's Legal Officer/OIC-Data Privacy Officer, the Letter-Attestation was authenticated by a public notary in Milan, Italy. They were informed that apostillation of such document was not recognized by the public prosecutors who conduct such process in Milan, hence, they have advised that they are still looking into the possibility of performing such process. She assured that they shall inform the Commission should they receive any update

regarding this and hoped that the Commission will consider favorably the submitted document.

On 30 June 2021, HDSI submitted the apostilled version of the Letter- Attestation dated 04 April 2020 of Mr. FN, which was allowed to be apostilled by the Italian Embassy in Milan on 22 June 2021.

Issue

Whether or not the request for exemption from the requirement of notification of affected data subjects filed by HDSI should be granted.

Discussion

The initial compliance submitted by HDSI on 18 June 2021 is not compliant with the Order of the Commission in its Resolution dated 25 March 2021. On 30 June 2021, HDSI belatedly submitted the apostilled Attestation Letter dated 04 April 2020 of Mr. FN of CSB at PDM.

The translation of the authenticated portion of the apostilled Attestation Letter states that the document presented to the notary public which is the Attestation Letter is a certified copy of the original exhibited to him. It does not even certify that the signature of Mr. FN in the document was authentic which is what the Commission needs in order to determine the authenticity and due execution of the Attestation Letter to help it decide whether or not to grant the request for exemption of notification to the affected data subjects filed by the PIC.

This Commission resolves to deny the request for exemption from the requirement of notification to the affected data subjects filed by HDSI. Upon careful perusal of the apostilled Attestation Letter submitted by HDSI, this Commission finds that the notification to the affected data subjects is necessary.

In the Attestation Letter,¹ Mr. FN confirmed that they were running a project which is gently scanning the publicly available and potentially

¹ Attestation Letter dated 04 April 2020 submitted by Mr. FN, PH

misconfigured data sources. He stated that it is purely motivated by research purposes, amongst other publicly available sources of data, they accessed ETH Server on 21 March 2021.² Furthermore, he alleged that they designed the experiment to download a minimal amount of information from the systems they contact, and they did not maintain any record nor gathered any information on any of the accessed systems.³ All information and data they acquired from the ETH server has been purged from their systems. What they retained were only a statistical analysis of the data, aggregated with the data of all other systems they analyzed in the course of their project.⁴

Mr. FN further attested that they will not use any of the data to harm the affected data subjects and that they have not or will not use this data for financial fraud, spam, identity theft, or any other purposes that may cause harm to the data subjects. He stated that they have purposefully designed the experiment to make this impossible, to the fullest extent of their ability.⁵

Moreover, their statistical analysis will be exclusively for academic and scientific purposes and will be published only in aggregated form to further academic research and to provide security considerations and suggestions. No personally identifying information will ever be released. The only form of release will be scientific and academic publication.⁶

With these statements in the Attestation Letter, HDSI is requesting for exemption from notification of affected data subjects.

Even assuming the authenticity and due execution of the Attestation Letter, based on its contents, this Commission finds that the justification for the request for exemption from the requirement of notification to the affected data subjects is insufficient to show that the notification would not be in the public interest or in the interest of the affected data subjects. Even if it is for research purposes, it is undisputed that a breach has occurred, and the data compromised contained personal and sensitive personal information. Therefore, a breach notification to the affected data subjects is necessary.

² *Id* at pp. 1-2.

³ *Id* at pp. 2

⁴ *Ibid.*

⁵ *Ibid.*

⁶ *Ibid.*

This Commission notes that the purpose of the required notification to the affected data subjects of a breach incident is for them to protect themselves against possible negative consequences or effects of the data breach. That is why if the PIC cannot prove that it will not be in the public interest or in the interest of the affected data subjects, a breach notification is required.

The Commission reiterates that notification of the data subjects is the general rule. Section 18(B) of NPC Circular No. 16-03 provides that, “a personal information controller may be exempted from notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of affected data subjects.”

As to the manner of notification to the affected data subjects, Section 18(A) of NPC Circular No. 16-03 provides that:

The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. **It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.** It may be supplemented with additional information at a later stage on the basis of further investigation.⁷

Moreover, Section 18(D) of same Circular provides that:

Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. **The personal information controller shall establish all**

⁷ National Privacy Commission, Personal Data Breach Management, Circular No. 16-03 (December 15, 2016). Emphasis supplied.

reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.⁸

The Commission, in its Resolution for NPC BN 20-161, emphasized the importance of ensuring that affected data subjects receive timely notification, *viz*:

It is noteworthy that the avowed purpose of the required notification to data subjects of a breach incident is for them to take the necessary precautions or other measures to protect themselves against possible effects of the breach. Moreover, personal information controllers (PICs) are required to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach. It therefore follows that PICs should guarantee that the notification they sent to data subjects has been received. Otherwise, it defeats the very purpose of notification of data subjects.⁹

Notification of the affected data subjects in cases of personal data breach is an essential obligation in data privacy protection. Section 20(f) of the DPA of 2012¹⁰ states that:

SEC. 20. *Security of Personal Information.* –

xxx

(f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give

⁸ *Id.* Emphasis supplied.

⁹ NPC BN 20-161, 17 December 2021.

¹⁰ An Act Protecting Individual Personal Information In Information And Communications Systems In The Government And The Private Sector, Creating For This Purpose A National Privacy Commission, And For Other Purposes [DATA PRIVACY ACT], Republic Act No. 10173 (2012).

rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

This Commission finds no merit in granting the request for exemption from the notification of the affected data subjects by HDSI.

HDSI failed to adduce sufficient evidence for this Commission to conclude that granting the request for exemption from the notification of the affected data subject would not cause harm or negative consequences to the affected data subjects. HDSI also failed to prove that granting the request for exemption from the notification of the affected data subject would not be in the public interest or in the interest of the affected data subjects.

WHEREFORE, premises considered, the instant request for exemption from the requirement of notification of affected data subjects dated 13 April 2020 filed by Health Delivery Systems Inc. is hereby **DENIED**.

Health Delivery Systems Inc. is hereby **ORDERED** to comply with the following within **fifteen (15) days** from receipt of this Resolution:

1. **NOTIFY** the affected data subjects; and
2. **SUBMIT** proof of notification to the data subjects who were affected by the breach, including proof of receipt of the data subjects of the notification.

SO ORDERED.

Pasay City, Philippines.
01 July 2021.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

SNR
Legal Officer / OIC-Data Privacy
Health Delivery System, Inc.

RJR
Data Protection Officer
Health Delivery System, Inc.

**COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT**
National Privacy Commission

X-----X

RESOLUTION

LIBORO, P.C.:

Before this Commission is a request for an exemption from the requirement of notifying the affected data subjects filed by De La Salle Health Sciences Institute (DLSHSI).

Facts

On 10 June 2020, this Commission received a breach notification from the DLSHSI on an incident involving the vulnerability of the search link in its Employee and Student System called School Automate (SA). According to the initial breach report submitted by the DLSHSI, visitors of the SA can look for the ID number of students or employees. The SA contains records of around eleven thousand (11,000) employees and students (collectively referred to as data subjects).¹

In its report,² DLSHSI requested for exemption from notification of the data subject on the following grounds:

Notification to the data subject would further expose the data subjects' vulnerability as against the remote possibility of any harm that can befall them. All other computer applications are reviewed for similar weakness and this weakness will be included among the criteria in all future software acquisitions.

Discussion

¹ NPC BN 20-101 In re DLSHSI Initial Report dated 10 June 2020 at pp. 1.

² *Id* at pp. 1.

Section 3 of the National Privacy Commission Circular 16-03 (Circular) defines security incident and data breach in this wise:

“Personal data breach” refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:

1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
2. Integrity breach resulting from alteration of personal data; and/or
3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.

“Security incident” is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place;

Personal data breach occurs when one of the circumstances provided by Section 3 (F) of NPC Circular 16-03 are present.

It comes in three forms: (1) when personal data is accessed by or disclosed to third persons without authority (confidentiality breach)³; or due to the accidental destruction or loss of personal data (availability breach)⁴; or when there is alteration of personal data (integrity breach).⁵

Outside of the foregoing definition, any event or occurrence that tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data fall within the broader category of security incident.⁶

In the case at hand, the system vulnerability in the SA that was discovered by DLSHSI in its routine inspection is not a data breach,

³ Item 3, Section 3 (F), NPC Circular 16-03

⁴ Item 1, *id.*

⁵ Item 2, *id.*

⁶ Section 3 (J), *id.*

but rather a security incident. There was no evidence on record that the SA was accessed by third persons unlawfully, or that the contents of the SA was disclosed to unauthorized individuals.

Moreover, DLSHSI was able to take preventive actions before the security incident ripened into a full data breach. DLSHSI was able to remove the search link few hours after discovery, and it also advised its HR and Registrar to thoroughly validate the identity of any person that would request for any information or documents from the institution.

Considering that the system vulnerability of the SA is a mere security incident which did not give rise to a real risk of serious harm to any affected data subjects, and that DLSHSI was able to take subsequent measures that ensure that the negative consequences to the data subjects will not materialize, the Commission resolves to grant the request for exemption from the notification of the affected data subjects. Nevertheless, DLSHSI is directed to continue its monitoring activities to allow timely notification in case any evidence of unauthorized use of the information arises.

WHEREFORE, all premises considered, the request for exemption is hereby **GRANTED**. The matter of BN 20-101: In Re De La Salle Health Sciences Institute is hereby considered **CLOSED**.

SO ORDERED.

Pasay City, Philippines;
23 July 2020.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy

Commissioner Copy furnished:

A.B.R.
Data Protection Officer

COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION

**NAGA,
D.P.C.:**

This Resolution refers to the Compliance Letter¹ that the Commission received dated 27 November 2020 from Home Credit Consumer Finance Philippines, Inc. (Home Credit) in compliance to this Commission's Resolution dated 22 October 2020 in relation to the security and confidentiality breach resulting from unauthorized disclosure of personal information of one of their employees.

The Facts

On 22 October 2020, this Commission issued a Resolution² with the following dispositive portion:

WHEREFORE, premises considered, Home Credit Consumer Finance Philippines, Inc. is hereby ORDERED to submit the following documents: (1) Copy of the SMS containing the notification letter; and (2) Proof of receipt of the notification letters that were sent to the affected data subjects within ten (10) days upon receipt of this Resolution. The Full Breach Report dated 12 October 2020 submitted by Home Credit Consumer Finance Philippines, Inc. is hereby NOTED, subject to the recommendations of the Compliance and Monitoring Division and further actions of this Commission.

On 18 November 2020, Home Credit received the abovementioned Resolution.

On 27 November 2020, Home Credit submitted a Compliance Letter as proof of compliance to the Commission's Resolution which

¹ Home Credit Consumer Finance Philippines, Inc. Compliance Letter dated 27 November 2020

² Resolution dated 22 October 2020

includes the copy of the Short Message Service (SMS) notification with the hyperlink that directs the recipient to the notification letter, copy of the notification letter, and updates on the notification to the affected data subjects.

Discussion

The Commission duly notes Home Credit's submission of the copy of the SMS notification with the hyperlink that directs the recipient to the notification letter and the copy of the notification letter.

On the proof of receipt of the notification, Home Credit stated in its Compliance that they have no knowledge of an IT solution that provides proof of receipt when an SMS is received by the intended recipient. Further, while other messaging service applications such as Viber, WhatsApp, or Telegram has visual indicators once the message is received and read, such applications are not practical as a large-scale Client Relationship Management (CRM) platform. Home Credit stated that their CRM platform is currently not capable of providing any proof that the SMS was received by the data subjects.³

Additionally, Home Credit outlined the communication process they followed and adopted for the data subject notification. Home Credit stated that they opted for SMS as the communication channel since it was the contact information available for both customers and character reference. Home Credit conducted two (2) batches of notification which includes a small pilot and the final batch consisting with the rest of affected data subjects. Home Credit also mentioned that they note the success of their communication through increased engagement and feedback.⁴

However, upon the evaluation of their system to determine whether they can provide proof of receipt, their data showed a processing error since only around 13, 299 messages were sent from the SMS gateway. Home Credit then scheduled a repeat notification to 72, 697 data subjects, however, only 72, 593 were forwarded by their SMS service provider while the remaining 104 entries cannot

³ Home Credit Consumer Finance Philippines, Inc. Compliance Letter dated 27 November 2020, p. 2

⁴ *Ibid.*

be forwarded since it does not meet the required number of characters.

This Commission finds that Home Credit failed to provide sufficient proof of the data subject's receipt of notification as previously ordered by this Commission. Home Credit only submitted the system log showing that the notification was sent and resent. While Home Credit argues that NPC Circular 16-03 only imposes a general principle when the notification to data subjects is mandatory, the fact still remain that whether written or electronic, Personal Information Controllers (PICs) have the obligation under the said Circular to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach.⁵

Moreover, this Commission stresses that a thorough reading of the NPC Circular 16-03 would reveal that the responsibility of the PICs to notify the affected data subjects is not limited to sending the notification to the affected data subjects alone, but comes hand-in-hand with the responsibility of using secure means of communication and providing all reasonable mechanisms to guarantee that the notification reaches the affected data subjects they intend to notify. Such obligation is regarded by this Commission as crucial and necessary for PICs to establish, especially in cases that falls under the mandatory breach notification requirement.

Time and time again, this Commission reminds PICs of the purpose in notifying the affected data subjects, which is to allow them to take the necessary precautions to protect themselves against the possible risk of serious harm resulting from the breach; wherein such purpose and objective is defeated once PICs failed to establish all reasonable mechanisms to ensure that the affected data subjects are informed of the breach.

WHEREFORE, premises considered, Home Credit Consumer Finance Philippines, Inc. is hereby **ORDERED** to submit, within **fifteen (15) days upon receipt of this Resolution**, an affidavit stating that the recipients of the SMS notification are active users and that the users' numbers indicated in Home Credit's system are all active.

⁵ Section 18(D) of NPC Circular 16-03

Further, in the event that Home Credit Consumer Finance Philippines, Inc. will determine inactive users, they shall provide the notification to the affected data subjects who are inactive through alternative means as provided in NPC Circular 16-03.

SO ORDERED.

Pasay City, Philippines;
17 December 2020.

Sgd.

JOHN HENRY D. NAGA

Deputy Privacy Commissioner

WE CONCUR:

Sgd.

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

Sgd.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

COPY FURNISHED:

RBS

Data Protection Officer

Home Credit Consumer Finance Philippines, Inc.

**COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION**

GENERAL RECORDS UNIT

National Privacy Commission

RESOLUTION***LIBORO, P.C.:***

This Resolution refers to the request for postponement of notification to affected data subjects filed by TravelServices, Inc. (TravelServices), a subsidiary of TravelPeople, Inc., dated 02 September 2020, involving a personal data breach caused by a ransomware attack in the company's system.

The Facts

In its Initial Report filed with the Commission, TravelServices stated that in the morning of 26 August 2020, the company was advised by its in-house IT that there was a problem with the Magsaysay network which currently houses its systems which resulted in difficulties in connection. It was later found that the Travel Management Systems of the company, the system that holds information of its clients and suppliers, were affected by a strain of ransomware virus. As a result, the company have to manually input details of ticket issued, requests for cash advance, and requests for payment to its suppliers.

Upon further investigation, TravelServices have established that no personal data or records have been exposed to the public. It is unclear at this time what vulnerabilities in the data processing system allowed the breach. Further investigation is being conducted by the cybersecurity experts they engaged.

According to the company, as the security incident involves ransomware, there is no indication that personal data has been acquired by unauthorized persons. They believe the most likely consequence of this incident is data loss arising from an inability to decrypt the affected files. However, they expect the data loss to be minimal and temporary, as they back up their data constantly, and the backups are still intact.

Records shows that the total number of data subjects who may be affected, as well as the personal information involved were not indicated in the report.

According to the Initial Report, the following are the measures taken to address the breach incident:

- i. All servers were shut down to contain the virus and to allow IT to conduct check each server.
- ii. An incident advisory was sent to all users and to management on August 26, 2020. All units were advised to apply their Business Continuity Plans and workarounds while the servers/systems are down.
- iii. Security patches for the ransomware was applied to non-affected servers.
- iv. Cybersecurity vendors were tapped to assist on the containment, clean-up, and possible decryption of affected files.

While an incident advisory was sent to all users and to the management, they have yet to notify the affected data subjects at this time, as they have yet to determine precisely who were affected.

If notification is necessary in the determination of the Commission, TravelServices request for a postponement in notifying the affected data subjects until such time as they have ascertained the identities of the affected data subjects.

Hence, the instant request for postponement of notification of data subjects until such time that it has ascertained the identities of the affected data subjects.

Discussion

This Commission denies the herein request for postponement of notification to data subjects of TravelServices in accordance with NPC Circular No. 16-03 (Personal Data Breach Management).

At the outset, it should be emphasized that notification of data subjects of data breaches is the general rule. Under Section 18(A) of NPC Circular No. 16-03, it provides that:

The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.¹

The exemption or postponement will only be allowed in exceptional circumstances under Section 18(B) of NPC Circular No. 16-03, which provides that:

If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification. A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects. The Commission may authorize the postponement of notification **where it may hinder the progress of a criminal investigation related to a serious breach,** taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.²

The Initial Report by TravelServices does not contain any narration of a “criminal investigation related to a serious breach that may hinder the progress thereof, taking into account circumstances provided in Section 13 of the said Circular, and other risks posed by the personal data breach” in order for the Commission to consider its request for postponement of notification to data subjects. Thus, a request for postponement is not proper and must be denied.

¹ Emphasis supplied.

² Emphasis supplied.

The Company's Initial Report and request also contains a contention that since the security incident involves ransomware and that there is no indication that personal data has been acquired by unauthorized persons, no evidence was submitted to support this. On this issue, the Commission finds that no evidence was presented to support this claim.

Furthermore, this Commission wants to clarify the obvious misconception of TravelServices that since the security incident involved ransomware, there is no reason to believe that the information may have been accessed by unauthorized persons.

Section 11 of NPC Circular 16-03 states the conditions for notification, thus:

SECTION 11. When notification is required. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

1. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.

For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

2. There is reason to believe that the information may have been acquired by an unauthorized person; and

3. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

It should be noted that a loss of control over personal data held in custody should be enough for a personal information controller to have "reason to believe that the information may have been acquired by an unauthorized person." An indication of

exfiltration of data is not a requirement in Section 11(b). Absolute certainty of acquisition by an unauthorized person is not required by either the Circular or the Data Privacy Act (DPA), considering that the condition only provides for a determination based on the existing circumstances that can give a “reason to believe.”

This liberal interpretation of the conditions necessitating mandatory breach notification is rooted in Section 20(f) of the DPA itself, which provides:

The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are **reasonably believed to have been acquired by an unauthorized person**, and the personal information controller or the Commission **believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject**. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.³

In the previous Resolutions⁴ issued by this Commission, it was held that:

The infection of the system by a ransomware should be sufficient to form a reasonable belief for the personal information controllers. Ransomware is defined as “a type of malicious software that infects a computer and restricts users’ access to it until a ransom is paid to unlock it... Typically, these alerts state that the user’s systems have been locked or that the user’s files have been encrypted. Users are told that unless a ransom is paid, access will not be restored.” While ransoms primarily cause availability breaches, it is different from other availability breaches because a malefactor intentionally causes them. This is unlike other types of availability breaches that are caused by accidents or system glitches. In these cases, the total exercise of control over the data is removed from the personal information controller and is taken by the malefactor. Without this control, the personal information controller will be unable to exercise its obligations in

³ Emphasis supplied.

⁴ NPC BN 20-157, NPC BN 20-158, NPC BN 20-159, NPC BN 20-160, NPC BN 20-161, NPC BN 20-162, NPC BN 20-163, NPC BN 20-164, NPC BN 20-165.

processing the personal data according to the provisions of the DPA. Recent ransomware attacks have also shown a capability to release the encrypted data over the internet upon non-payment of the ransom, potentially leading to a confidentiality breach contemplated in Section 11(2). For the protection of the data subjects, such incidents must be notified both to the Commission and the affected data subjects.

This construction of Section 11(2) is guided by the Interpretation Clause in the DPA which states:

Section. 38. *Interpretation.* – Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.

WHEREFORE, premises considered, the request for Postponement of Notification to Data Subjects filed by TravelServices, Inc. is hereby **DENIED**. TravelServices, Inc. is **ORDERED** to comply with the following **within fifteen (15) days from receipt of this Resolution**:

1. **SUBMIT** full breach report with the complete information required under NPC Circular 16-03 which includes among others, the nature of personal data involved and a determination of the affected data subjects; and
2. **NOTIFY** the affected data subjects of the breach incident in accordance with the provisions of NPC Circular 16-03 and to **SUBMIT** proof of compliance thereto.

SO ORDERED.

Pasay City, Philippines;
21 September 2020.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner
Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy

Copy furnished:

N.H.H.C.
Data Protection Officer
TravelServices, Inc.

**COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION**
GENERAL RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION

LIBORO, P.C.:

This Resolution refers to the request for postponement of Notification to affected data subjects filed by TravelPeople Ltd., Inc. (“TPLI”) of the Magsaysay Group of Companies dated 02 September 2020,¹ involving a personal data breach caused by a ransomware attack in the company’s system.

The Facts

In its Initial Report filed with the Commission, TPLI stated that in the morning of 26 August 2020, the company was advised by its in-house IT that there was a problem with the Magsaysay network which currently houses its systems which resulted in difficulties in connection. It was later found that the Travel Management Systems of the company, the system that holds information of its clients and suppliers, were affected by a strain of ransomware virus. As a result, the company have to manually input details of ticket issued, requests for cash advance, and requests for payment to its suppliers.

According to the Initial Report Submitted by TPLI, it has established that no personal data or records have been exposed to the public. It is unclear at this time what vulnerabilities in the data processing system allowed the breach. Further investigation is being conducted by the cybersecurity experts they engaged.

According to the company, as the security incident involves ransomware, there is no indication that personal data has been acquired by unauthorized persons. They believe the most likely consequence of this incident is data loss arising from an inability to

¹ Notification: Personal Data Breach for the National Privacy Commission dated 02 September 2020.

decrypt the affected files. However, they expect the data loss to be minimal and temporary, as they back up their data constantly, and the backups are still intact.

Records also shows that the total number of data subjects who may be affected, as well as the personal information involved were not indicated in the report.

According to its Initial Report, the following were measures taken to address the breach:

- i. All servers were shut down to contain the virus and to allow IT to conduct check each server.
- ii. An incident advisory was sent to all users and to management on August 26, 2020. All units were advised to apply their Business Continuity Plans and workarounds while the servers/systems are down.
- iii. Security patches for the ransomware was applied to non-affected servers.
- iv. Cybersecurity vendors were tapped to assist on the containment, clean-up, and possible decryption of affected files.

While an incident advisory was sent to all users and to the management, they have yet to notify the affected data subjects at this time, as they have yet to determine precisely who were affected.

If notification is necessary in the determination of the Commission, TPLI request for a postponement in notifying the affected data subjects until such time as they have ascertained the identities of the affected data subjects.

Hence, the instant request for postponement of notification of data subjects until such time that it has ascertained the identities of the affected data subjects.

Discussion

This Commission denies the herein request for postponement of notification to data subjects of TPLI in

accordance with NPC Circular No. 16-03 (Personal Data Breach Management).

At the outset, it should be emphasized that notification of data subjects of data breaches is the general rule. Under Section 18(A) of NPC Circular No. 16-03, it provides that:

The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.²

The exemption or postponement will only be allowed in exceptional circumstances under Section 18(B) of NPC Circular No. 16-03, which provides that:

If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification. A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects. The Commission may authorize the postponement of notification **where it may hinder the progress of a criminal investigation related to a serious breach,** taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.³

The Initial Report submitted by TPLI does not contain any narration of a “criminal investigation related to a serious breach that may hinder the progress thereof, taking into account circumstances provided in Section 13 of the said Circular, and other risks posed by the personal data breach” in order for the

² Emphasis supplied.

³ Emphasis supplied.

Commission to consider its request for postponement of notification to data subjects. Thus, a request for postponement is not proper and must be denied.

The company's Initial Report and request also contains a contention that since the that the security incident involves ransomware and that there is no indication that personal data has been acquired by unauthorized persons, no evidence was submitted to support this. On this issue, the Commission finds that no evidence was presented to support this claim.

Furthermore, this Commission wants to clarify the obvious misconception of TPLI that since the security incident involved ransomware, there is no reason to believe that the information may have been accessed by unauthorized persons.

Section 11 of NPC Circular 16-03 states the conditions for notification, thus:

SECTION 11. *When notification is required.* Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

1. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.

For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

2. There is reason to believe that the information may have been acquired by an unauthorized person; and

3. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

It should be noted that a loss of control over personal data held in custody should be enough for a personal information controller to have “reason to believe that the information may have been acquired by an unauthorized person.” An indication of exfiltration of data is not a requirement in Section 11(b). Absolute certainty of acquisition by an unauthorized person is not required by either the Circular or the Data Privacy Act (“DPA”), considering that the condition only provides for a determination based on the existing circumstances that can give a “reason to believe.”

This liberal interpretation of the conditions necessitating mandatory breach notification is rooted in Section 20(f) of the DPA itself, which provides:

The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are **reasonably believed to have been acquired by an unauthorized person**, and the personal information controller or the Commission **believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject**. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.⁴

In the previous Resolutions⁵ issued by this Commission, it was held that:

The infection of the system by a ransomware should be sufficient to form a reasonable belief for the personal information controllers. Ransomware is defined as “a type of malicious software that infects a computer and restricts users’ access to it until a ransom is paid to unlock it... Typically, these alerts state that the user’s systems have been locked or that the user’s files have been encrypted. Users are told that unless a ransom is paid,

⁴ Emphasis supplied.

⁵ NPC BN 20-157, NPC BN 20-158, NPC BN 20-159, NPC BN 20-160, NPC BN 20-161, NPC BN 20-162, NPC BN 20-163, NPC BN 20-164, NPC BN 20-165.

access will not be restored.”⁶ While ransomwares primarily cause availability breaches, it is different from other availability breaches because a malefactor intentionally causes them. This is unlike other types of availability breaches that are caused by accidents or system glitches. In these cases, the total exercise of control over the data is removed from the personal information controller and is taken by the malefactor. Without this control, the personal information controller will be unable to exercise its obligations in processing the personal data according to the provisions of the DPA. Recent ransomware attacks have also shown a capability to release the encrypted data over the internet upon non-payment of the ransom, potentially leading to a confidentiality breach contemplated in Section 11(2). For the protection of the data subjects, such incidents must be notified both to the Commission and the affected data subjects.

This construction of Section 11(2) is guided by the Interpretation Clause in the DPA which states:

Section. 38. *Interpretation.* – Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.

WHEREFORE, premises considered, the request for Postponement of Notification to Data Subjects filed by TravelPeople Ltd., Inc. is hereby **DENIED**. TravelPeople Ltd., Inc. is **ORDERED** to comply with the following **within fifteen (15) days from receipt of this Resolution**:

1. **SUBMIT** full breach report with the complete information required under NPC Circular 16-03 which includes among others, the nature of personal data involved and a determination of the affected data subjects; and
2. **NOTIFY** the affected data subjects of the breach incident in accordance with the provisions of NPC Circular 16-03 and to **SUBMIT** proof of compliance thereto.

⁶ UC Berkeley Information Security Office (n.d). *Frequently Asked Questions- Ransomware*. Retrieved from <https://security.berkeley.edu/faq/ransomware/>.

SO ORDERED.

Pasay City, Philippines;
21 September 2020.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner
Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy

Copy furnished:

N.K.D.
Data Protection Officer
TravelPeople Ltd., Inc.

**COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION**
GENERAL RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION**NAGA, D. P.C.;**

Before the Commission is a Breach Notification filed by Costa Crociere S.p.A. (Costa) with a request for exemption from individual data subject notification dated 09 September 2021.

Facts

On 25 December 2020, Costa detected an unauthorized third-party access to portions of its information technology (IT) systems and the IT systems of its subsidiaries, AIDA Cruises (Aida), AIDA Kundencenter GmbH, and Carnival Maritime GmbH.¹

According to Costa, the Costa Cruises domain (Costa Network) and Aida Cruises domain (Aida Network) are on separate but connected networks. Based on a comprehensive analysis of the available logs and artifacts, they believe that the event began via multiple malicious Excel document(s), sent via email, containing SDBot remote access tooling which was opened by employees at Aida.²

Costa stated that on 21 December 2020, the threat actor was able to use their access to the Aida Network to gain access to the Costa Network. On the succeeding days, the threat actor gradually exfiltrated approximately 329 GB of data then 719 GB of data using the Rclone tool.³

¹ Costa Crociere S.p.A Data Breach Notification dated 09 September 2021

² Id. at page 2.

³ Id.

On 24 December 2020, the threat actor disabled both the Costa anti-virus software, TrendMicro and Aida anti-virus software, Windows Defender. The threat actor then launched DoppelPaymer ransomware onto the Costa Network and the Aida Network. Such activity was detected by Costa at CET 00:21 a.m. on 25 December 2020.⁴

The unauthorized access was used to launch a malware that encrypted a number of IT systems. The unauthorized persons then demanded a ransom from Costa to restore access to those systems. Further, the unauthorized persons exfiltrated approximately 1.1 TB of unstructured data from Costa and its subsidiaries' domains.

Costa, its subsidiaries, and their IT systems are all located outside of the Philippines.

In terms of the security measures Costa implemented to address the breach, it stated that it shut down the intrusion, restored operations, performed measures to prevent further unauthorized access to other parts of its IT systems, and will conduct a technical and forensic investigation.

Further, Costa also stated that it informed and notified following authorities:

1. Italian Data Protection Authority, Garante per la protezione dei dati personali (Garante) as the lead supervisory authority in the European Economic Area (EEA);
2. Italian Ministero delle Infrastrutture e dei Trasporti (MIT) and CSIRT Italia (CSIRT) of in accordance with the Costa's obligations as a designated Operator of Essential Services (OES) under the Italian NIS Directive and Legislative Decree no. 65/2018;
3. Polizia Postale e delle Comunicazioni (Polizia Postale) on 12 January 2021;

⁴ Id.

4. State Commissioner for Data Protection and Freedom of Information of Mecklenburg-Vorpommern and the Hamburg Commissioner for Data Protection and Freedom of Information in Germany due to the involvement of AIDA Cruises; and
5. German law enforcement authorities where it have cooperated with their investigation.⁵

Moreover, Costa stated that at the time the reports were submitted to the Garante and other Italian and German authorities, it was not aware that Filipino data subjects were affected by the breach. It was only recently that Costa determined the possibility that the unauthorized persons who accessed its IT systems may have been able to access limited amount of personal data relating to approximately seventy-four thousand (74,000) Filipino data subjects.

The Filipino data subjects are either guests of Costa's cruise lines or its employees or crew members. The personal data that may have been possibly affected by the breach includes name, date of birth, passport number, nationality, and cruise trip information.

With this, Costa stated that it has been conducting comprehensive dark web monitoring to mitigate any harm that the said breach may cause to the data subjects.⁶ According to Costa, no evidence suggests that the data has been made available for sale or misused. Hence, it believes that the breach has a low risk of harm to the Filipino data subjects.

Additionally, Costa stated that it is regularly reviewing its security and privacy policies and procedures. It is also implementing changes when needed to enhance its information security and privacy program and controls and to prevent a recurrence of any incident similar to the breach.

Further, Costa has administrative and technical measures in place to further secure personal data such as: global identity standardization and synchronization; improvement of key security tools, such as

⁵ Id. at page 1 to 2.

⁶ Id. at page 2 to 3.

Carbon Black, and antivirus solutions; implemented firewall rule adjustments and governance; and optimized alert logging process to allow for earlier detection and remediation. It also has a suite of data protection programs, trainings, and several online training courses focused on cybersecurity and privacy.⁷

Costa stated that it already published the notices regarding the breach on its websites beginning March 2021 in the languages most commonly served by Costa and its subsidiaries, namely on its Italian, French, Spanish, Brazilian, Chinese and Japanese websites. Further, Aida also published notifications on its website. Each notice contained an email address, to enable any individual who had any question or concerns regarding the breach to communicate directly with the company's privacy team.⁸

With the measures undertaken to address the breach and protect the information of its data subjects, and the fact that to its knowledge no data subject has filed a complaint in connection with the breach, Costa then respectfully requests that it be exempted from sending individual notification to data subjects.⁹

Discussion

This Commission finds that the case falls under the mandatory breach notification requirement and the notification of the affected data subjects is necessary in order to protect them from the risk of serious harm. Section 11 of the NPC Circular No. 16-03 (Personal Data Breach Management) provides:

SECTION 11. *When notification is required.* Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

⁷ Id at page 3.

⁸ Id.

⁹ Id.

- A. The personal data involves **sensitive personal information or any other information that may be used to enable identity fraud.**
- B. **There is reason to believe that the information may have been acquired by an unauthorized person; and**
- C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.¹⁰
(Emphasis Supplied)

Moreover, Section 13 of the same Circular states:

SECTION 13. Determination of the Need to Notify.

Where there is uncertainty as to the need for notification, the personal information controller shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred. The personal information controller shall also consider if the personal data reasonably believed to have been compromised involves:

- A. Information that would likely affect national security, public safety, public order, or public health;
- B. **At least one hundred (100) individuals;**
- C. **Information required by applicable laws or rules to be confidential;** or
- D. Personal data of vulnerable groups.¹¹
(Emphasis supplied)

In Costa's initial breach notification, it stated that the total number of affected Filipino data subjects is approximately seventy-four thousand (74,000). Further, the breach involves both personal information and sensitive personal information including name, date of birth, passport number, nationality, and cruise trip information.¹²

Considering that the breach involves more than one hundred (100) individuals and includes sensitive personal information, the incident herein is covered by the mandatory breach notification rule. This

¹⁰ Section 11 of the NPC Circular No. 16-03.

¹¹ Section 13 of the NPC Circular 16-03.

¹² Costa Crociere S.p.A Data Breach Notification dated 09 September 2021 at page 2.

Commission reiterates the importance of the obligation of Personal Information Controllers (PICs) to notify to the affected data subjects in cases of breach that falls under the mandatory notification rule.

This Commission emphasizes that the notification to the affected data subjects is fundamental in order to allow them to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.¹³

This Commission also recognizes that Costa's request for exemption from individual notification of the affected data subjects is based on its report that it already published the notices regarding the breach on its websites. However, it must be emphasized that it only published the notices on its Italian, French, Spanish, Brazilian, Chinese and Japanese websites. With this, the affected Filipino data subjects may not be fully informed of the breach since it is not in the language commonly known to Filipinos, such as English or Filipino.

In view of the foregoing, this Commission deems the notification to the affected data subjects as urgent and necessary while also taking into consideration the number of the affected data subjects and the disproportionate effort that Costa may have to undertake in order to notify them.

Section 18(D) of NPC Circular No. 16-03 provides that, where individual notification is not possible or would require a disproportionate effort, the PIC may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner.¹⁴ Accordingly, Section 4(c), Rule XI of the 2021 NPC Rules of Procedure, for the Commission to grant the use of alternative means of notification, a request has to be made by the PIC.¹⁵

However, in this case, considering the large number of the affected data subjects and the urgency to notify them, the Commission orders

¹³ Section 18(A) of the NPC Circular 16-03.

¹⁴ Section 18(D) of the NPC Circular No. 16-03

¹⁵ Section 4(c), Rule XI of the NPC Circular No. 2021-01

Costa to use alternative modes of notification for a portion of the affected data subjects to enable Costa to comply with the orders of the Commission. For the affected data subjects with e-mail addresses, Costa shall individually notify them through e-mail. As for the affected data subjects without e-mail addresses, Costa shall notify the affected data subjects through publication in a newspaper of general circulation in the Philippines.

This Commission also notes that Costa anchored its request on the security measures it has implemented to address the breach and prevent its reoccurrence. However, Costa failed to include any proof of such security measures it implemented to address the breach and ensure that the risk of harm or negative consequence to the data subjects will not materialize as indicated in its initial breach notification.

In addition, the Commission has yet to receive the Full Breach Report from Costa. The Commission finds that Costa failed to provide within five (5) days from the initial report the Full Breach Report¹⁶ that contains the complete and necessary information as prescribed under Section 9 and Section 17(D) of the NPC Circular No. 16-03.

WHEREFORE, premises considered, this Commission resolves that the request for exemption from individual data subject notification filed by Costa Crociere S.p.A is hereby **DENIED**.

Costa Crociere S.p.A is hereby **ORDERED** to comply with the following **within ten (10) days** from receipt of this Resolution:

1. **NOTIFY** the affected data subjects. The affected data subjects with e-mail addresses shall be notified pursuant to Section 18 of the NPC Circular No. 16-03. The notification shall be done individually using secure means of communication, through e-mail. Costa shall submit proof of compliance, including the proof of receipt of the data subjects of such notification.

¹⁶ Section 17(C) of the NPC Circular No. 16-03

The affected data subjects without e-mail addresses shall be notified through alternative means pursuant to Section 18(D) of the NPC Circular No. 16-03, through publication in a newspaper of general circulation in the Philippines. Costa shall also provide proof of compliance, including proof of notification / publication

2. **SUBMIT** its Full Breach Report pursuant to Section 9 and Section 17(D) of the NPC Circular No. 16-03;
3. **SUBMIT** proof of the security measures Costa implemented to address the breach; and
4. **SHOW CAUSE** in writing why it should not be subjected to contempt proceedings, as permitted by law, before the appropriate court, and other actions as may be available to the Commission, for its failure to submit its Full Breach Report within the required period.

SO ORDERED.

City of Pasay, Philippines.
23 September 2021.

SGD.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

SGD.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

CP
General Counsel

KB

**COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION**
GENERAL RECORDS UNIT
National Privacy Commission

X

X

RESOLUTION

NAGA, D.P.C.:

This Order refers to a Security Incident Report submitted by Tuitt Philippines dated 21 November 2017 and the Full Breach Report dated 26 July 2019, involving a security incident that may have exposed its WIFI network to unauthorized persons.

The Facts

On 19 November 2017, during a meetup event, Tuitt became aware of a potential security incident when the WIFI login credentials of their training laboratory's network were shared by a staff member with the event participants.

On 21 November 2017, the Data Protection Officer (DPO) of Tuitt submitted to the Commission a Security Incident Report¹ via email detailing that the unauthorized disclosure of WIFI login credentials may have compromised their network's security and the information of data subjects who accessed their machines through the same network. Tuitt also described in the Incident Report the measures they implemented to address the incident.

¹Security Incident Report dated 21 November 2017.

On 08 July 2019, the Commission, through the Complaints and Investigation Division (CID), informed Tuitt the initial report they submitted did not comply with the reportorial requirements provided under NPC Circular 16-03. TPI was then required to submit a Full Breach Report in accordance with said Circular.

On 26 July 2019, Tuitt submitted its Full Breach Report. In the Report, Tuitt claimed that upon review of the incident that occurred on 19 November 2017, such was not a personal data breach as initially reported, but a security incident. Tuitt based its assertion that the nature of the incident did not fit the definition of a personal data breach as defined in the same Circular considering that the network that was accessed contains no personal data.

Discussion

This Commission deems the incident as a Security Incident since it only affected the data protection aspect of Tuitt system and does not involve personal data. Section 3 (F) of the NPC Circular provides:

“Personal data breach” refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:

1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
2. Integrity breach resulting from alteration of personal data; and/or
3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.

xxx

“Security incident” is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include

incidents that would result to a personal data breach, if not for safeguards that have been put in place.

Tuitt stated on their Full Breach Report² (Report) that they store personal information and sensitive personal information on secure cloud servers (AWS), and not on the training laboratory's network which was the subject of the incident. Upon review of the incident, Tuitt stated that the lab network where any of their data subjects' information are stored is isolated from the rest of their staff's network which reduced the potential risk of any form of data breach.³ Therefore, no personal data breach occurred.

This Commission emphasizes that for an incident to be considered a personal data breach it must involve unlawful loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed, among other factors defined under Section 3 (F) of the NPC Circular 16-03. The aforementioned factors were not present in this case. Thus, the incident does not fall under personal data breach.

However, as correctly pointed out by Tuitt, the unauthorized disclosure of the WIFI login credentials shall be treated as a Security Incident since it may affect data protection, including the availability, integrity, and confidentiality of personal data. Further, the distinction between the two is that a security incident may result to a personal data breach if not for the safeguards in place implemented by the Personal Information Controllers (PICs).

In terms of the measures implemented by Tuitt to address the incident, they stated that the network passwords were changed, and the machines have been reformatted. Tuitt issued a Standard Operating Procedure (SOP) to the staffs who interact with the lab daily which includes the prohibition of sharing any WIFI credentials to non-staff personnel. Also, Tuitt white-listed all authorized machines where access is denied to other unauthorized devices.⁴

²Full Breach Report dated 26 July 2019.

³Ibid. At p. 2.

⁴Ibid. At p. 3.

However, the Commission finds that there was no proof submitted showing the measures implemented by Tuitt to address the incident as mentioned in their Report. Although the incident is considered a Security Incident, it is part of the PICs obligation to provide proof of the security measures they have implemented to address the incident along with their Report.

Further, the PICs also have the responsibility to implement policies and procedures in managing security incidents under Section 4 of the NPC Circular 16-03 which provides, viz:

SECTION 4. Security Incident Management Policy. A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure:

- A. Creation of a data breach response team, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach;
- B. Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident;
- C. Implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system;
- D. Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach; and
- E. Compliance with the Act, its IRR, and all related issuances by the Commission pertaining to personal data breach notification.

This Commission highlights that the submission of the proof of the security measures implemented by Tuitt and their Security Incident Management Policy is necessary in order for the Commission to ensure and confirm that the security measures

implemented are sufficient to prevent the security incident in resulting to personal data breach.

WHEREFORE, premises considered, the Commission hereby **ORDER** Tuitt Philippines, Inc. to comply with the following within fifteen (15) days upon receipt of this Order:

- (1) **SUBMIT** the proof of the security measures they have implemented as stated in their Full Breach Report dated 26 July 2019; and
- (2) **SUBMIT** their Security Incident Management Policy pursuant to Section 4 of the NPC Circular 16-03.

SO ORDERED.

Pasay City, Philippines;
18 March 2021.

Sgd.

JOHN HENRY D. NAGA
*Deputy Privacy
Commissioner*

WE CONCUR:

Sgd.

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.

LEANDRO ANGELO Y. AGUIRRE
*Deputy Privacy
Commissioner*

COPY FURNISHED:

AGCA

Data Protection Officer (Acting)

Tuitt Philippines, Inc.

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION**

GENERAL RECORDS UNIT

National Privacy Commission

**IN RE: DEPARTMENT OF FOREIGN
AFFAIRS (DFA) PASSPORT BREACH**

NPC SS 19-001

INITIATED AS A *SUA SPONTE* NPC
INVESTIGATION INTO THE
POSSIBLE DATA PRIVACY
VIOLATIONS COMMITTED BY THE
DEPARTMENT OF FOREIGN
AFFAIRS

X-----X

RESOLUTION

AGUIRRE, D.P.C.;

This Resolution refers to a *sua sponte* investigation of the possible data breach regarding the alleged mishandling of personal information processed by third parties on behalf of the Department of Foreign Affairs (DFA) for the issuance and printing of passports.

Facts

In January 2019, several newspaper outlets reported that the DFA is requiring some applicants for passport renewal to bring their birth certificates because its previous outsourced passport maker “took away” all its applicants’ data.¹

¹ Helen Flores, *DFA Passport Maker Runs Off with All Data*, THE PHILIPPINE STAR, 12 January 2019, available at <https://www.philstar.com/headlines/2019/01/12/1884444/dfa-passport-maker-runs-all-data> (19 July 2022); John Nieves, *Its Like The Government Doesn't Care About Protecting Our Data*, UNBOX, 13 January 2019, available at <https://unbox.ph/editorials/its-like-the-government-doesnt-care-about-protecting-our-data/>; Catalina Ricci S. Madarang, *Making Sense of DFA's Passport Data Theft Controversy*, INTERAKSYON, 14 January 2019, available at <https://interaksyon.philstar.com/special/features/2019/01/14/142166/making-sense-dfas-passport-data-theft-controversy-teddyboy-locsir/>.

On 14 January 2019, National Privacy Commission (NPC), through its Complaints and Investigation Division (CID), sent a formal correspondence to DFA Secretary Teodoro L. Locsin, Jr. informing him of reports of alleged mishandling of data for the issuance and printing of passports.²

On 23 February 2021, the Commission, through the CID, issued an Order for DFA to submit the following:

1. Updated Report detailing the facts surrounding the incident;
2. Copy of DFA's contract with the involved third-party provider; and
3. Proof or Certification that the applicant's data is within DFA's custody and control.³

On 18 March 2021, DFA submitted proof of its compliance with the Order dated 23 February 2021 and provided the Commission with the following:

1. Updated Report denying the alleged mishandling of the personal data of passport applicants that were processed by the Bangko Sentral ng Pilipinas (BSP) when it was handling passport printing for DFA;
2. Copies of the Memorandum of Agreement between the DFA and BSP in 2006; and
3. A certification stating that the server, with passport applicants' data contained therein, is under the DFA's custody and control.⁴

On 07 September 2021, the CID submitted its Technical Report to the Commission on the results of the Vulnerability Assessment Penetration Testing (VAPT) conducted on DFA's online passport appointment system "www.passport.gov.ph", and its search of the dark web for evidence of database exfiltration.⁵ On the possible data breach reported in the newspaper article, the CID determined that

² Letter from National Privacy Commission to DFA Secretary Teodoro L. Locsin, 14 January 2019, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NPC 2019).

³ CID Order, 23 February 2021, at 1, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NPC 2019).

⁴ Letter from Undersecretary Brigido J. Dulay, 18 March 2018, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NPC 2019).

⁵ CID Technical Report, 07 September 2021, at 4, *in* In the Matter of Department of Foreign Affairs (DFA) Office of Consular Affairs Passport Appointment System (passport.gov.ph) Vulnerability, NPC SS 19-001 (NPC 2019).

there was no personal data exfiltration that had occurred despite the alleged “taking away” of passport data.⁶ The CID, however, discovered that several pieces of personal information remain publicly available and may be downloaded using a web browser and a specific search criterion.⁷ The CID assessed that the website “www.passport.gov.ph” is vulnerable to an Insecure Direct Object Reference (IDOR) attack.⁸ The CID’s investigation also revealed that attackers could bypass security controls and use the website as a platform for attacks against its users.⁹

Based on the CID’s Technical Report,¹⁰ the Commission issued an Order on 11 November 2021 directing DFA to comply with the following within thirty (30) days from its receipt:

WHEREFORE, premises considered, the Commission **ORDERS** the Department of Foreign Affairs (DFA) within thirty (30) days from receipt of this Order to:

- (1) **ADDRESS** the vulnerabilities on the DFA passport system available on the website, “passport.gov.ph” by performing Vulnerability Assessment Penetration Testing on passport.gov.ph and adding a “noindex” parameter to the HTTP header to prevent any indexing of saved information by any search engine; and
- (2) **SUBMIT** proof that it has addressed the vulnerabilities of the DFA passport system.

The Commission shall furnish the DFA with its Technical Report dated 07 September 2021 to guide the DFA in addressing the technical vulnerabilities identified in the DFA passport system.

SO ORDERED.¹¹

Since DFA did not comply with the Order, on 31 May 2022, the Commission, through the Enforcement Division (EnD), issued its

⁶ *Id.*

⁷ *Id.* at 1.

⁸ *Id.* at 3.

⁹ *Id.* at 3.

¹⁰ Order, 11 November 2021, *in* *In re: DFA – Passport Breach*, NPC SS 19-001 (NPC 2019).

¹¹ *Id.*

Enforcement Letter, reiterating the directives in the Order dated 11 November 2021.¹²

On 09 June 2022, the DFA sent a letter to the NPC in compliance with the Enforcement Letter dated 31 May 2022.¹³ It provided the results of the VAPT conducted by the its hosting and application service provider for the passport system, APO Production Unit Inc. (APO), as well as the measures taken after the assessment.¹⁴ Further, it included APO's report on the implementation of a "noindex" parameter to the http header to prevent any indexing of saved information by any search engine.¹⁵

On 21 June 2022, the DFA sent another letter reiterating the results of the VAPT conducted by APO and emphasizing that "links to specific passport application forms when "site:passport.gov.ph" is typed in the browser's search box no longer generate the questionable result."¹⁶

Issue

Whether the DFA implemented sufficient measures to manage security incidents.

Discussion

A security incident is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data.¹⁷ It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place.¹⁸

¹² Final Enforcement Assessment Report, 28 June 2022, at 3, *in* In the Matter of Department of Foreign Affairs (DFA) Office of Consular Affairs Passport Appointment System (passport.gov.ph) Vulnerability, NPC SS 19-001 (NPC 2019).

¹³ Letter *from* Medardo G. Macaraig, Assistant Secretary and Data Protection Officer, Department of Foreign Affairs, *to* Rodolfo S. Cabatu, Jr. and Maria Theresita E. Patula, National Privacy Commission, Enforcement Division (09 June 2022) ¹⁴ Final Enforcement Assessment Report, 28 June 2022, at 3, *in* In the Matter of Department of Foreign Affairs (DFA) Office of Consular Affairs Passport Appointment System (passport.gov.ph) Vulnerability, NPC SS 19-001 (NPC 2019).

¹⁵ *Id.* at 3.

¹⁶ Letter *from* Medardo G. Macaraig, Assistant Secretary and Data Protection Officer, Department of Foreign Affairs, *to* Rodolfo S. Cabatu, Jr. and Maria Theresita E. Patula, National Privacy Commission, Enforcement Division (21 June 2022)

¹⁷ National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16- 03], Rule I § 3 (J) (15 December 2016).

¹⁸ *Id.*

When the Commission, through the CID, discovered that several pieces of personal information remain publicly available and may be downloaded using a web browser and a specific search criterion,¹⁹ there is no question that a security incident occurred in this case.

Section 4 of Rule II of NPC Circular 16-03 (Personal Data Breach Management) states that Personal Information Controllers (PICs) should implement policies and procedures to manage security incidents:

Section 4. Security Incident Management Policy. A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure:

- A. Creation of a data breach response team, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach;
- B. Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident;
- C. Implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system;
- D. Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach; and
- E. Compliance with the Act, its IRR, and all related issuances by the Commission pertaining to personal data breach notification.²⁰**

The Commission issued an Order dated 11 November 2021 directing the DFA to address the security incidents that the Commission found while conducting its investigation. The DFA submitted its report

¹⁹ Final Enforcement Assessment Report, 28 June 2022, at 3, *in* In the Matter of Department of Foreign Affairs (DFA) Office of Consular Affairs Passport Appointment System (passport.gov.ph) Vulnerability, NPC SS 19-001 (NPC 2019).

²⁰ NPC Circ. No. 16-03, § 4. (Emphasis Supplied).

addressing the vulnerabilities of the DFA passport system and adding the “noindex” parameter to the HTTP header that resulted to the vulnerability assessment “Risk Level: High” scoring zero (0) when the CID conducted its own vulnerability check.²¹ The score zero (0) means that the updated website is less likely to be breached by potential digital attack.²² The EnD determined:

On 16 June 2022, the former performed the vulnerability assessment using the OWASP ZAP vulnerability assessment tool. As such, the vulnerability assessment “Risk Level: High” scored 0, which means the updated website is less likely to be breached by potential digital attacks. Moreso, the EnD further conducted a test to verify previously publicly available data that could be downloaded from the passport appointment system using Google and Firefox web browsers which specifies a certain search criterion example “site:passport.gov.ph” as the keyword.

Furthermore, the OWASP ZAP scanned zero (0) high-risk vulnerability, which means no critical threat or high potential breach may occur that needs urgent fixing or concerns. The OWASP ZAP gives an overview of the improvement on the website compared to the previous result of twenty-nine (29) high-risk vulnerabilities on the technical report dated 07 September 2021. Therefore, the passport appointment system website has now addressed the two (2) recommendations and is able to improve its security against potential attackers or hackers.²³

Following DFA’s compliance with the Order dated 11 November 2021 the Commission finds that DFA has sufficiently addressed the vulnerabilities on the DFA passport system available on the website “www.passport.gov.ph”.

Although the DFA already addressed the vulnerabilities identified by the Commission, it is still obliged to periodically conduct vulnerability assessments as a preventive or minimization measure for possible personal data breach.²⁴ Section 6 of Rule III of NPC

²¹ Final Enforcement Assessment Report, 28 June 2022, at 5, *in* In the Matter of Department of Foreign Affairs (DFA) Office of Consular Affairs Passport Appointment System (passport.gov.ph) Vulnerability, NPC SS 19-001 (NPC 2019).

²² *Id.*

²³ *Id.*

²⁴ NPC Circ. No. 16-03, § 6 (D).

Circular 16-03 provides for preventive measures to minimize the occurrence of a security incident:

Section 6. *Preventive or Minimization Measures.* A security incident management policy shall include measures intended to prevent or minimize the occurrence of a personal data breach. Such safeguards may include:

. . .

D. Regular monitoring for security breaches and vulnerability scanning of computer networks[.]²⁵

The Commission emphasizes the duty of PICs to implement adequate safeguards to prevent or minimize occurrences of personal data breach or security incidents. Considering that the monitoring and implementation of security measures remains a continuing responsibility of PICs, the DFA, as a PIC, shall regularly monitor for security breaches and conduct vulnerability scans of its computer network and the DFA passport system.

WHEREFORE, premises considered, this Commission finds the submission of the Department of Foreign Affairs in response to the Order dated 11 November 2021 **SUFFICIENT**. This Commission resolves that the matter is hereby **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
14 July 2022.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

²⁵ *Id.*

JOHN HENRY D. NAGA
Privacy Commissioner

DUG CHRISTOPHER B. MAH
Deputy Privacy Commissioner

Copy furnished:

DEPARTMENT OF FOREIGN AFFAIRS
2330 Roxas Boulevard, Pasay City

MGM
Data Protection Officer

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION**
GENERAL RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION

AGUIRRE, D.P.C.:

This Resolution refers to the Letter¹ of the Commission on Elections (COMELEC) providing notice to this Commission of a possible personal data breach concerning the registered voters of Talavera, Nueva Ecija, and its request for extension of time to notify the data subjects.

The Facts

On 10 November 2020, COMELEC received an unsigned memorandum dated 04 November 2020 from JBR, Election Officer (EO), Office of the Election Officer (OEO) of Talavera, Nueva Ecija, reporting that on 30 October 2020, a burglary incident happened at the OEO of Talavera, Nueva Ecija.²

After the inventory was conducted, the following items were found missing:

- (1) One portable hard drive which contains the voter registration records and VRS backups (COMELEC property);
- (2) One Lenovo Think Pad Laptop with SN XXXXXXXX8 (COMELEC property) which contains the voter registration system program, other VRS reports and data backup;
- (3) One Acer laptop (LGU property);
- (4) One Samsung Notebook (LGU property);
- (5) Php 350.00 hidden inside an employee's drawer; and
- (6) Two hundred pieces of face shields.³

¹ Letter dated 16 November 2020.

² *Ibid.*

³ *Ibid.*

JBR also reported the following:

- (1) The lock of the office vault was smashed and destroyed;
- (2) The incident was immediately reported to the local police and investigation is on-going;
- (3) The concerned officers of COMELEC were informed; and
- (4) Inventory of all office documents is on-going.⁴

Furthermore, COMELEC requested that since such notice has been submitted beyond the seventy-two (72) hour period, within which the Commission should be notified, the same be considered justified and reasonable considering the consecutive work suspensions that followed after the receipt of JBR's report, thus:

Please note that while this Office received the report of JBR on 10 November 2020, work in government offices in the National Capital Region as well as in Region III, among other regions, was suspended effective 3:00 o'clock in the afternoon of 11 November 2020 (Thursday) until 13 November 2020 (Friday).⁵

COMELEC informed this Commission of their security measures, thus:

Relatedly, undersigned respectfully informs the NPC that, as a security feature, all the data encoded in the computers of all OEOs involved the voters of their respective cities and municipalities only, and are already encrypted in AES 256. The portable hard disks containing said data are likewise encrypted.⁶

According to the letter, the COMELEC Executive Director and Data Protection Officer issued a memorandum dated 10 November 2020 for the Director IV of COMELEC's Information Technology Department, as well as Director III of the Finance Services Department and Data Compliance Officer, informing them about the report of JBR with a directive to investigate the incident.⁷

⁴ *Ibid.*

⁵ *Ibid.*

⁶ *Ibid.*

⁷ *Ibid.*

Lastly, COMELEC claims that since the investigation is on-going and the challenges posed by the threat of COVID-19, it is not reasonably possible to notify the data subjects within the prescribed period. For these reasons, COMELEC requests for an extension of time to comply with the notification of data subjects⁸ without stating a specific timeline for such.

Discussion

This Commission denies the request for an indefinite extension of COMELEC to notify the affected data subjects.

Section 18(B) of NPC Circular 16-03 provides that:

If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification. A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects. **The Commission may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach,** taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.⁹

In this case, COMELEC requests for an extension to comply with the notification of data subjects on two (2) grounds, namely, (1) that an investigation is on-going, and (2) the challenges posed by the threat of COVID-19.¹⁰

A careful scrutiny of the records reveals that there are two (2) investigations referred to in this case. First, the on-going investigation conducted by the local police. Second, the

⁸ *Ibid.*

⁹ Emphasis supplied.

¹⁰ *Supra* note 1.

investigation under the directive of COMELEC through its Information Technology Department and Finance Services Department.

As to the on-going investigation by the local police, there is no showing how the notification to data subjects will hinder the investigation on robbery or other relevant crime thereto. Not all criminal investigations, even those conducted as a result of the breach as in this case, can be considered as a ground for postponement of notification of data subjects. Simply mentioning that a criminal investigation is being undertaken is not sufficient. The burden is on the party requesting for postponement to show that the notification will indeed affect the outcome of the investigation.

As to the investigation within the COMELEC, this is not the investigation contemplated by Section 18 of NPC Circular 16-03, which specifically refers to criminal investigations.

Furthermore, while the challenges posed by the threat of COVID-19 pandemic was raised by the COMELEC as a reason for its postponement to notify the data subjects, it was not explained how it is not reasonably possible to notify the data subjects within the prescribed period. More importantly, it did not state what period of additional time is requested for. The request for an indefinite extension of notification of the affected data subjects is hereby denied.

The Commission, however, notes that no mention was made about the COMELEC's concrete steps for the retrieval of the affected data subjects' information which may have been stored in the stolen equipment. In order to effect the notification of the data subjects which will enable them to take the necessary precautions, the Commission directs the COMELEC to conduct notification through alternative means under Section 18(D) of NPC Circular 16-03¹¹, thus:

Notification of affected data subjects shall be
done individually, using secure
means of communication,

¹¹ NPC Circular 16-03. Personal Data Breach Management. Dated 15 December 2016.

whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: *Provided*, that **where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner:** *Provided further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.¹²

This Commission likewise brings to the attention of COMELEC the required submission of its Full Breach Report. Section 17(C) of NPC Circular 16-03 provides that:

There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. **In both instances, the Commission shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days**, unless the personal information controller is granted additional time by the Commission to comply.¹³

While COMELEC has requested for additional time to notify the data subjects herein, no request for additional time to submit the full report has been made. The COMELEC is reminded that the notification of data subjects and notification of the Commission are two (2) different requirements to be complied with by personal information controllers (PICs).

WHEREFORE, premises considered, the Commission on Elections is **ORDERED, within ten (10) days** from receipt of this Resolution, to: (1) Submit its Full Breach Report, and (2) Notify the data

¹² Emphasis supplied.

¹³ Emphasis supplied.

subjects through alternative means and submit proof of compliance thereto.

SO ORDERED.

Pasay City, Philippines
26 November 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

BJS
Executive Director and Data Protection Officer
Commission on Elections

THRU: MRA
Representative
Commission on Elections

**COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION**
GENERAL RECORDS UNIT
National Privacy Commission

**IN RE: BREACH NOTIFICATION
REPORT OF PHILIPPINE NATIONAL
BANK (PNB)**

**NPC BN 17-
034**

X-----X

RESOLUTION

NAGA, D.P.C.

This resolution refers to the security breach notification that the Commission received dated 17 November 2017 from the Philippine National Bank (“PNB”) involving its inControl Portal (“Portal”), a self- service offering for enrolled customers to control the spending of their supplementary credit card.

The facts are the following:

On 14 November 2017, through the conduct of their regular monitoring of credit card service availability, the PNB’s IT Credit Card Operator reported that the Portal issued a database error response. Following their standard operating procedures on incident reports, PNB conducted an investigation and discovered that the inControl server files are encrypted with the Arena ransomware, which is a kind of malware that infects the victims’ computer with a code that restricts the user’s access to systems and files.

To initially address the security breach, PNB shut down the Portal. Subsequently, the server was removed from the main network to prevent other applications and devices to be infected by the ransomware.

On 17 November 2017, the Commission received the notification from the PNB regarding the security breach that transpired on its Portal.

Through a letter dated 22 November 2017, the PNB stated that according to their initial forensic report, no customer record was compromised, and no other system was impacted by the breach. However, the self-service feature became unavailable, and this affected 655 active and 257 inactive customers, out of 33,000 credit card customers of the PNB.

On 2 July 2018, the PNB has successfully restored the inControl portal. No issues were detected after the conduct of an independent VAPT.

On 13 July 2018, the Commission issued a Compliance Order to PNB requiring them to:

1. Submit a report on the status of the security measured being implemented within one (1) month from receipt of the Order; and
2. Submit all pertinent documents for remediation within three (3) months from receipt of the Order.

The PNB was able to submit the required reports on 24 August 2018 and 26 July 2019, respectively. The documents provided details on PNB's implementation of several remediation measures to improve the security of its systems. PNB manifested that they executed the following measures:

1. Installed new servers and segregated the application and database servers;
2. Upgraded the operating systems, database and secure socket layer ("SSL") encryption versions;
3. Implemented Anti Distributed Denial of Service ("DDOS") facility and improved Domain Name System ("DNS"); and
4. Subjected the new environment to vulnerability and penetration tests ("VAPT"), remediating findings before the release production.

On 3 July 2019, the Commission's Enforcement Division sought the assistance of the Data Security and Technology Standards Division ("DSTSD") in order to review PNB's compliance and whether the remediation measures implemented is commensurate with the industry standards.

In the DSTSD report dated 07 August 2019, they concluded that PNB's remediation measures are at par with the industry standard requirements, specifically the Payment Card Industry Data Security Standard ("PCI DSS"). The DSTSD report also underlined the noticeable improvement on PNB's security measures after the Commission's issuance of the 13 July 2018 Order.

The Enforcement Assessment Report dated 13 December 2019 categorically stated that the measures undertaken by PNB complies with the R.A. 10173 or the Data Privacy Act, its Implementing Rules and Regulation, and NPC Circular 16-03 on Personal Data Breach Management. Further, it was recommended that the PNB shall regularly review these measures and policies to further protect the interests of the data subjects.

This Commission, after thoroughly reviewing all the pertinent documents and giving due credence to the evaluation and examination made by its two Divisions, finds that the PNB was able to substantially comply with the Commission's Compliance Order dated 13 July 2018. This Commission also notes that no complaint against PNB has been filed in any of its offices in relation to said security breach.

WHEREFORE, premises considered, this Commission hereby resolves that this case be **CLOSED**.

SO ORDERED.

Pasay City, Philippines
23 January 2020.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

PHILIPPINE NATIONAL BANK

ATTN: **MR. STY**
Data Privacy Officer, PNB

ENFORCEMENT DIVISION GENERAL

RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION***NAGA, D.P.C.:***

Before this Commission is a data breach notification from Tulay sa Pag-unlad, Inc., (“TSPI”) in relation to the personal data breach on one of its employee’s personal bank account.

The Facts

On 04 June 2018, an employee of TSPI went to the Banco De Oro (“BDO”) ATM in Paniqui, Tarlac to withdraw from her personal account. Upon checking the balance, she found out that the amount of P10,000.00 had been deducted from the account.

BDO then informed the TSPI employee that there had been two (2) debit transactions in her account amounting to P5,000.00 each occurred on 03 June 2018, and both consummated at Makati City. Said payments were used for purchases made from Lazada.

On 05 June 2018, FSS, Data Protection Officer (“DPO”) of TSPI, submitted a breach notification report to the Commission involving the incident.

On 13 June 2018, upon the query of the Complaints and Investigation Division (“CID”), the DPO of TSPI confirmed that the account involved was the personal account of their employee and not the actual account of the TSPI. The DPO also informed the CID that the amount deducted had already been credited back to the employee on 11 June 2018.

On 28 April 2020, the case was submitted by the CID for Resolution of this Commission.

Discussion

The Data Privacy Act (“DPA”) and the NPC Circular 16-03 require every Personal Information Controller (“PIC”) the twin responsibility of notifying the Commission and the affected data subjects when personal data breach occurs. **Section 20 (f) of the DPA** provides:

“(f) The **personal information controller shall promptly notify the Commission and affected data subjects** when sensitive personal information or other information that may, under the circumstances, be used **to enable identify fraud are reasonably believed to have been acquired by an unauthorized person**, and the personal information controller or the Commission believes (that such unauthorized acquisitions is likely to give rise to real risk of serious harm to any affected data subjects...” (Emphasis supplied)

Further, **Section 15 of NPC Circular 16-03**, states:

“The **personal information controller shall notify the Commission and the affected data subjects upon knowledge of, or when there is reasonable belief that a personal data breach has occurred**. The **obligation to notify remains with the personal information controller** even if the processing of information is outsourced or subcontracted to a personal information processor. The personal information controller shall identify the designated data protection officer or other individual responsible for ensuring its compliance with the notification requirements provided in this Circular...” (Emphasis supplied)

It can be inferred from the above that the PIC has the responsibility of notifying both the Commission and the affected data subjects when personal data breach occurs. Notification becomes necessary if the personal or sensitive personal information may be used for identity fraud, may have been acquired by an unauthorized person, and the PIC or this Commission believes that the unauthorized acquisition is likely to give rise to a real of serious harm to any affected data subject.¹

In the case at hand, TSPI was clearly not the PIC responsible to report the incident to the Commission considering that it does not decide on what information is collected, or the purpose or extent of the processing in the TSPI employee’s personal bank account. Otherwise stated, TSPI is not the PIC that has the duty to notify the Commission about the personal data breach. However, reviewing the factual antecedents of the case, BDO and Lazada are the proper PICs that should have reported this breach to the

Commission. BDO as the bank who holds the personal account of the TSPI employee and Lazada as the merchant who processed the payments made on 03 June 2018.

Further, the return of the P10,000.00 to the TSPI employee's personal account would reveal that his or her account was accessed and used by an unauthorized person. Clearly, this case falls under the required notification as provided in the above-cited Section 11 of NPC Circular 16-03.

This Commission will then carry out its solemn duty of ensuring compliance of PICs with the DPA and its issuances in the end of protecting the rights of the affected data subject.

WHEREFORE, premises considered, this Commission resolves to **CLOSE AND TERMINATE** this particular case, **In Re: Tulay sa Pag-Unlad Inc.**, without prejudice to the **sua sponte investigation** that the CID shall be conducting as to the responsibility of both BDO and Lazada under the DPA and the issuances of the Commission.

SO ORDERED.

Pasay City, 21 May 2020.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commission

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commission

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

FSS

Data Protection Officer
Tulay sa Pag-unlad, Inc

**COMPLAINTS AND INVESTIGATION DIVISION GENERAL
RECORDS UNIT**

National Privacy Commission

FGP,

NPC Case No. 18-038

Complainant, (formerly CID Case No.
18 E-038)

-versus-

*For: Violation of the
Data Privacy Act of
2012*

**MAERSK GLOBAL SERVICE
CENTRES, PHILIPPINES, LTD.,**

*Respondent
s.*

X-----X

RESOLUTION

**NAGA,
D.P.C.:**

This Resolution refers to the Manifestation¹ filed by Respondent Maersk Global Service Centres, Philippines, Ltd. (Maersk) in response to the Order of the Commission indicated in its Decision dated 21 May 2020 to award Complainant FGP the amount of Five Thousand Pesos (Php 5,000.00).

The Facts

On 21 May 2020, this Commission issued a Decision² with the following dispositive portion, *to wit*:

WHEREFORE, all these premises considered, this Commission resolves to **AWARD** Complainant FGP damages in the amount of P5,000.00 for Respondent Maersk Global Service Centres, Philippines, Ltd.'s violation of his right to access. Respondent is hereby **ORDERED** to submit its compliance within fifteen (15) days from receipt of this Decision.

¹ Manifestation dated 01 February 2021, *FGP vs. Maersk Global Service Centres, Philippines, Ltd.*, NPC CN 18-038

² Decision dated 21 May 2020, *FGP vs. Maersk Global Service Centres, Philippines, Ltd.*, NPC CN 18-038

On 15 January 2021³, the Respondent received a copy of the Decision. On 01 February 2021, Respondent filed its Manifestation which stated that on even date, Respondent has sent the payment the Complainant through an issuance of a check amounting to Five Thousand Pesos (Php 5,000.00) in compliance with the 21 May 2020 Decision of this Commission.

Respondent also attached in its Manifestation copies of the email between them and the Complainant stating that Complainant prefers the check to be sent via courier, Satisfaction of Judgement, check amounting to Five Thousand Pesos (Php 5,000.00), and the official receipt of courier addressed to Complainant.

Discussion

This Commission deems the submission of the Respondent's Manifestation sufficient and satisfactory to its Order as indicated in its Decision dated 21 May 2020.

In cases where the data subject files a complaint for the violation of his or her rights as a data subject, it is within this Commission's powers to award indemnity on the basis of applicable provisions of the Data Privacy Act of 2012 (DPA) and the New Civil Code.⁴ In the instant case, this Commission found that the Complainant's right to access under the DPA has been violated by the Respondent. Thus, the award of nominal damages is warranted.

Respondents duly complied with the Commission's Order to pay nominal damages to Complainant within fifteen (15) days from receipt of the Decision. Further, this Commission recognizes the fact that the last day of the compliance period is on 30 January 2021 which falls on a Saturday and therefore, Respondent was able to comply with the Order on the next working day or on 01 February 2021.

Upon review of the Manifestation and the attachments submitted by the Respondent, this Commission finds that they have submitted sufficient proof which shows their full compliance to the

³ Proof of receipt of Decision dated 21 May 2020

⁴ Section 51 of the Implementing Rules and Regulations of the Data Privacy Act of 2012

Order. The Respondent attached the copies of the following documents as proof of compliance: the Bank of the Philippine Islands (BPI) check to Complainant; the LBC official delivery receipt; Satisfaction of Judgment; and the screenshot of the delivery tracking details showing that the check was claimed by FGP on 02 February 2021.⁵ Moreover, this Commission, through the Enforcement Division, conducted a follow-up call on 11 February 2021, where the Complainant confirmed the receipt of the Respondent's payment on 02 February 2021.

In consideration of the above information, this Commission finds that the Manifestation filed by Respondent and proof of payment of the nominal damages to Complainant adequately complies with the Commission's Decision. Further, this Commission avails the opportunity of once again reminding Personal Information Controllers (PICs), the importance of upholding the data subject rights such as the right to access, whereas PICs are required to provide reasonable access, upon demand, specific information such as the contents of their personal information that were processed, the manner by which they were processed, and the designation or name or identity and address of the PIC to the data subjects.⁶ Such exercise of rights should be liberally interpreted in a manner mindful of the rights and interests of the individual, subject only to few conditions provided in the DPA and its Implementing Rules and Regulations (IRR).

WHEREFORE, premises considered, this Commission hereby finds the submission of Maersk Global Service Centres, Philippines, Ltd., in its Manifestation **SUFFICIENT** in compliance with the Commission's Decision dated 21 May 2020. Further, this Commission hereby considers NPC Case No. 18-038, FGP v. Maersk Global Service Centres, Philippines, Ltd., **CLOSED**.

SO ORDERED.

Pasay City, Philippines;
23 February 2021.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commission

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

On Official Business
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

FGP
Complainant

RMBSD
Counsel for Respondent

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

GMT,

Complainant,

-versus-

NPC 19-605

For: Violation of the Data
Privacy Act of 2012

**FCASH GLOBAL LENDING
INCORPORATED (FAST
CASH),**

Respondent.

X-----X

RESOLUTION

NAGA, D.P.C.;

This resolves the Motion for Reconsideration (Motion) dated 9 February 2021 filed by FCash Global Lending Inc. (Respondent), which seeks reconsideration of the Decision issued by the Commission dated 5 November 2020. The dispositive portion reads:

“WHEREFORE, premises considered, FCash Global Lending Inc. is hereby **ORDERED** by this Commission to pay GMT nominal damages in the amount of fifteen thousand peso (Php 15,000.00).

This Commission **FORWARDS** this Decision and a copy of the pertinent case records to the Department of Justice, recommending the prosecution of FCash Global Lending Inc. for the crimes of Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes as provided under Section 28 and Malicious Disclosure as provided under Section 31 of Republic Act No. 10173 otherwise known as the Data Privacy Act of 2012.”

Arguments of the Respondent

The Respondent's Motion for Reconsideration¹ raises the following arguments in questioning the Decision of this Commission:

- I. Evidence on record does not establish the commission of any violation of the Data Privacy Act (DPA).
- II. There is no evidence to support the finding that Respondent's Board of Directors are criminally liable for being negligent.
- III. There is no factual nor legal basis for the finding and imposition of nominal damages against the Respondent
- IV. There is no showing of compliance with the requirement of exhaustion of administrative remedy or of good cause to warrant a waiver thereof.

Discussion

This Commission finds no reversible error that would warrant reconsideration of the Decision dated 5 November 2020. We discuss the matter point-by-point.

I. There is a violation of the Data Privacy Act of 2012 (DPA).

Respondent argued that nothing in the records would warrant that they committed acts in violation of the DPA. The processing of Complainant's personal data was conducted by the Respondent to impel the Complainant to comply with her legal obligations, which are due and demandable under the loan agreement. Such act, according to the Respondent, is allowable and is in adherence to the data privacy principles of transparency, legitimate purpose, and proportionality of the DPA. Complainant has given full, free, and voluntary consent to Respondent having entered in a contractual relation as obligor-obligee. Thus, according to the Respondent, the processing of personal information is lawful and permissible. Further, the allegations in the complaint were vague if not nonexistent. The pieces of information are insufficient to

¹ Motion for Reconsideration dated 09 February 2021

substantiate the allegations in the complaint. Respondent concluded that such is a ground for the outright dismissal of the complaint.

As held by the Commission in its Decision,² it acknowledges that the collection of the personal information was in the exercise of the lending company's legitimate interest and part of fulfilling its contractual obligation. The Commission finds the Respondent liable not because of processing for collection per se but because of unauthorized and malicious sending of text blasts to Complainant's contact lists for the purpose of collecting the latter's loan. Such processing, as established in the 05 November 2020 Decision of this Commission, was not authorized by the data subject nor in accordance with the precepts of the DPA.

Further, even if the Complainant consented to give out a few references in her contact list for purpose of identity verification and alternative contacts for reaching out to Complainant in the event of default, this does not negate the fact that Respondent herein violated Section 28 of the DPA³. The processing was done without authority from the data subject as it goes beyond the original agreement between the Complainant and the Respondents. Moreover, the processing was made without being authorized by some other legal basis to process under the DPA.

From the foregoing, such violation was made clear when Respondent processed more personal information without her consent,⁴ specifically when it accessed and communicated with Complainant's contact list without her consent. This is shown in the email sent by Complainant to the Commission seeking help as

² Decision dated 5 November 2020

³ SEC. 28. *Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.* – The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

The processing of sensitive personal information for unauthorized purposes shall be penalized by imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

⁴ Records, page 39

Respondent were sending messages to all her mobile contacts and not only to the few references she permitted to give.⁵ Further, when Respondent sent a malicious message to Complainant's contact list, it resulted in the violation of the same provision as it used the contact information given by Complainant in ways other than the agreed purpose.

II. There is substantial evidence to recommend the prosecution of the Respondent's Board of Directors

Respondent also argued that there is no evidence to support the finding that the members of Respondent's Board of Directors (BOD) are criminally liable for being negligent. Respondent contends that the Commission declared that its BODs are criminally liable based solely on the fact that they are directors of the board.

Further, Respondent argued that the cited jurisprudence⁶ has a different set of facts from those of the instant case. In the cited case, Respondent was indicted not on the fact of being a corporate officer but based on the execution of the trust receipt.

Respondent further contended that the BOD should not be held to prove that they are not negligent and in the absence of proof to the contrary the legal presumption that they employed ordinary care in the discharge of their duties as the BOD stands. Nothing in the records prove that Respondent was duly informed of the alleged offensive text messages for it to be able to address Complainant's grievance before the filing of the instant case.

While it is true that the facts of the case cited is different from the case at bar, the jurisprudence was cited to expound on the concept that the BOD's gross negligence in overseeing its employees and the operational model of the company may warrant criminal prosecution if such gross negligence allowed the corporation, through its employees, to commit a criminal act, which is analogous to Section 34 of the DPA, viz:

⁵ Id., page 34

⁶ Alfredo Ching vs Secretary of Justice, G.R. No. 164317, February 6, 2006

GMT,

Complainant,

-versus-

NPC 19-605

For: Violation of the Data
Privacy Act of 2012

**FCASH GLOBAL LENDING
INCORPORATED (FAST
CASH),**

Respondent.

X-----X

RESOLUTION

NAGA, D.P.C.;

This resolves the Motion for Reconsideration (Motion) dated 9 February 2021 filed by FCash Global Lending Inc. (Respondent), which seeks reconsideration of the Decision issued by the Commission dated 5 November 2020. The dispositive portion reads:

“WHEREFORE, premises considered, FCash Global Lending Inc. is hereby **ORDERED** by this Commission to pay GMT nominal damages in the amount of fifteen thousand peso (Php 15,000.00).

This Commission **FORWARDS** this Decision and a copy of the pertinent case records to the Department of Justice, recommending the prosecution of FCash Global Lending Inc. for the crimes of Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes as provided under Section 28 and Malicious Disclosure as provided under Section 31 of Republic Act No. 10173 otherwise known as the Data Privacy Act of 2012.”

Arguments of the Respondent

The Respondent's Motion for Reconsideration¹ raises the following arguments in questioning the Decision of this Commission:

- I. Evidence on record does not establish the commission of any violation of the Data Privacy Act (DPA).
- II. There is no evidence to support the finding that Respondent's Board of Directors are criminally liable for being negligent.
- III. There is no factual nor legal basis for the finding and imposition of nominal damages against the Respondent
- IV. There is no showing of compliance with the requirement of exhaustion of administrative remedy or of good cause to warrant a waiver thereof.

Discussion

This Commission finds no reversible error that would warrant reconsideration of the Decision dated 5 November 2020. We discuss the matter point-by-point.

I. There is a violation of the Data Privacy Act of 2012 (DPA).

Respondent argued that nothing in the records would warrant that they committed acts in violation of the DPA. The processing of Complainant's personal data was conducted by the Respondent to impel the Complainant to comply with her legal obligations, which are due and demandable under the loan agreement. Such act, according to the Respondent, is allowable and is in adherence to the data privacy principles of transparency, legitimate purpose, and proportionality of the DPA. Complainant has given full, free, and voluntary consent to Respondent having entered in a contractual relation as obligor-obligee. Thus, according to the Respondent, the processing of personal information is lawful and permissible. Further, the allegations in the complaint were vague if not nonexistent. The pieces of information are insufficient to

¹ Motion for Reconsideration dated 09 February 2021

substantiate the allegations in the complaint. Respondent concluded that such is a ground for the outright dismissal of the complaint.

As held by the Commission in its Decision,² it acknowledges that the collection of the personal information was in the exercise of the lending company's legitimate interest and part of fulfilling its contractual obligation. The Commission finds the Respondent liable not because of processing for collection per se but because of unauthorized and malicious sending of text blasts to Complainant's contact lists for the purpose of collecting the latter's loan. Such processing, as established in the 05 November 2020 Decision of this Commission, was not authorized by the data subject nor in accordance with the precepts of the DPA.

Further, even if the Complainant consented to give out a few references in her contact list for purpose of identity verification and alternative contacts for reaching out to Complainant in the event of default, this does not negate the fact that Respondent herein violated Section 28 of the DPA³. The processing was done without authority from the data subject as it goes beyond the original agreement between the Complainant and the Respondents. Moreover, the processing was made without being authorized by some other legal basis to process under the DPA.

From the foregoing, such violation was made clear when Respondent processed more personal information without her consent,⁴ specifically when it accessed and communicated with Complainant's contact list without her consent. This is shown in the email sent by Complainant to the Commission seeking help as

² Decision dated 5 November 2020

³ SEC. 28. *Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.* – The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

The processing of sensitive personal information for unauthorized purposes shall be penalized by imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

⁴ Records, page 39

Respondent were sending messages to all her mobile contacts and not only to the few references she permitted to give.⁵ Further, when Respondent sent a malicious message to Complainant's contact list, it resulted in the violation of the same provision as it used the contact information given by Complainant in ways other than the agreed purpose.

II. There is substantial evidence to recommend the prosecution of the Respondent's Board of Directors

Respondent also argued that there is no evidence to support the finding that the members of Respondent's Board of Directors (BOD) are criminally liable for being negligent. Respondent contends that the Commission declared that its BODs are criminally liable based solely on the fact that they are directors of the board.

Further, Respondent argued that the cited jurisprudence⁶ has a different set of facts from those of the instant case. In the cited case, Respondent was indicted not on the fact of being a corporate officer but based on the execution of the trust receipt.

Respondent further contended that the BOD should not be held to prove that they are not negligent and in the absence of proof to the contrary the legal presumption that they employed ordinary care in the discharge of their duties as the BOD stands. Nothing in the records prove that Respondent was duly informed of the alleged offensive text messages for it to be able to address Complainant's grievance before the filing of the instant case.

While it is true that the facts of the case cited is different from the case at bar, the jurisprudence was cited to expound on the concept that the BOD's gross negligence in overseeing its employees and the operational model of the company may warrant criminal prosecution if such gross negligence allowed the corporation, through its employees, to commit a criminal act, which is analogous to Section 34 of the DPA, viz:

⁵ Id., page 34

⁶ Alfredo Ching vs Secretary of Justice, G.R. No. 164317, February 6, 2006

SEC. 34. *Extent of Liability.* – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the **responsible officers**, as the case may be, who participated in, or **by their gross negligence, allowed the commission of the crime**. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and he or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be. (Emphasis supplied)

Further, while it is true that the legal presumption that the BOD employed ordinary care in the discharge of their duties, such presumption was already disputed when they failed to act and address the malicious disclosure at hand. Considering the voluminous number of complaints that were filed before this Commission prior to this case which contains similar issues, it is presumed that the BOD was already properly notified and informed of the subject matter. If they employed ordinary care in the discharge of their duties, they should have already acted and undertook remedial actions to change their collection practices after the company received all the complaints that they did. Having done none, this is gross negligence on their part.

Additionally, since they didn't undertake any remedial actions as shown by the fact they didn't allege or present any evidence on this, then the legal presumption that they exercised ordinary care in the discharge of their duties shows that they knew about the collection practices and their operational model and were fine with it or approved it. In which case, it's not just gross negligence but actual participation on the part of the board of directors.

It is expected from the BOD to be alerted and immediately address the incident to protect its goodwill, but that is not what happened in this case. Nothing in the records would show that the Respondent, through its BOD, properly supervised or reprimanded the acts of the employees who committed such processing. Respondent also did not report remedial actions that they have

undertaken to place organizational, physical, and technical measures to protect the personal information of their borrowers. Hence, the BOD's inaction and omission to perform their duties to protect the processed personal information amounted to gross negligence.

The Supreme Court defines gross neglect of duty or gross negligence as follows:

"refers to negligence characterized by the want of even slight care, or by acting or omitting to act in a situation where there is a duty to act, not inadvertently but wilfully and intentionally, with a conscious indifference to the consequences, insofar as other persons may be affected. It is the omission of that care that even inattentive and thoughtless men never fail to give to their own property."⁷

Evidently, and as can be seen from the records, there was no showing that the BOD herein performed any act that would demonstrate that they have the slightest care to address the incident.

It was further contended by Respondent that the BOD should not be held to prove that they are not negligent and in the absence of proof to the contrary, the legal presumption that they employed ordinary care in the discharge of their duties as BOD stands.

As discussed by the Commission in the case of NPC 18-103,
viz:

"The obligation to comply with the provisions of the DPA, IRR and other issuances of the Commission primarily rest on the PIC. The Respondent cannot use the fault of its staff to evade responsibility under the DPA.

xxx

xxx. It is its responsibility as PIC to secure personal information of its customers and relay the company's privacy policies and procedures to its personnel, especially

⁷ *Fernandez v. Office of the Ombudsman*, G.R. No. 193983. March 14, 2012,

to those responsible in processing personal information of customers.”

Considering the mandate of the DPA and the responsibility vested in the PICs, Respondent’s BOD cannot deny that it was negligent in overseeing its employees and operational model.

In the case at bar, Respondent is the PIC of the personal data.⁸ Hence, Respondent, acting through its BOD, has the utmost legal responsibility to ensure that the personal data acquired is protected and used only for its authorized purposes. The BOD is responsible for ensuring that the provisions of the DPA are being observed and employed by their employees in the exercise of their functions, considering the nature and amount of personal data being collected from their customers. Thus, Respondent erred in contending that they should not be held to prove that they were not negligent.

Anent the argument that the BOD was not duly informed of the alleged offensive text messages for it to be able to address the Complainant’s grievance, Respondent should be reminded that under Section 20 (a) of the DPA, the personal information controller must, “implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing”. If the said mandate of the law is being strictly observed and implemented in the company wherein reasonable and appropriate organizational measures are in place, it is certain that the BOD would have known and acted on the incident. Otherwise, if Respondent would deny that the BOD was not informed of the alleged offensive text messages, then this just adds to the conclusion that the provisions of the DPA are ineptly implemented in the company.

Further, Respondent asserts that the instant proceeding, although administrative in nature, criminally penalizes the person or organization who violated its provisions. Therefore, the standard of evidence of proof beyond reasonable doubt must be strictly observed.

⁸ Section 2 (h) of R.A. 10173

The Commission wishes to clarify this misplaced argument. It is true that the violation of the DPA can lead to criminal prosecution. However, it is beyond the jurisdiction of the Commission to decide on cases that are criminal in nature. The Commission is only empowered to recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of the DPA⁹. Hence, the standard of evidence for a criminal case does not apply at this stage. The Commission only requires substantial evidence as basis for its proceedings considering that it is an administrative agency.¹⁰

Respondent concluded that due to the absence of any proof, the findings of the Commission of negligence against Respondent's BOD is not merely an error in judgement but constitute grave abuse of discretion that is tantamount to lack or excess of jurisdiction.

The Commission disagrees. In the case of *Yu vs Judge Reyes- Carpio*¹¹, the Supreme Court explained:

"The term "grave abuse of discretion" has a specific meaning. An act of a court or tribunal can only be considered as with grave abuse of discretion when such act is done in a "capricious or whimsical exercise of judgment as is equivalent to lack of jurisdiction." The abuse of discretion must be so patent and gross as to amount to an "evasion of a positive duty or to a virtual refusal to perform a duty enjoined by law, or to act at all in contemplation of law, as where the power is exercised in an arbitrary and despotic manner by reason of passion and hostility." Furthermore, the use of a petition for certiorari is restricted only to "truly extraordinary cases wherein the act of the lower court or quasi-judicial body is wholly void." From the foregoing definition, it is clear that the special civil action of certiorari under Rule 65 can only strike an act down for having been done with grave abuse of discretion if the petitioner could manifestly show that such act was patent and gross x x x."

⁹ Section 7(l) of R.A. No. 10173

¹⁰ Department of Health vs Aquintey, G.R. No. 204766, March 5, 2017

¹¹ 667 Phil. 474 (2011)

In this case, there is no hint of whimsicality, nor of gross and patent abuse of discretion as would amount to an evasion of a positive duty or a virtual refusal to perform a duty enjoined by law or to act at all in contemplation of law on the part of the Commission. The Commission is clothed with authority to decide on the subject matter while carefully following its Rules of Procedure. Absent clear and convincing evidence from the Respondent herein the presumption of regularity shall remain.

As aptly described by the Supreme Court in *Yap v. Lagtapon*,
viz:

“The presumption of regularity in the performance of official duties is an aid to the effective and unhampered administration of government functions. Without such benefit, every official action could be negated with minimal effort from litigants, irrespective of merit or sufficiency of evidence to support such challenge. To this end, our body of jurisprudence has been consistent in requiring nothing short of clear and convincing evidence to the contrary to overthrow such presumption.”¹²

III. The Commission is mandated to award nominal damages

Respondent further argued that there is no factual nor legal basis for the finding and imposition of nominal damages against the Respondent. Respondent contends that the authority of this Commission to award “indemnity on matters affecting any personal information” is limited only to actual and compensatory damage. Respondent argued that nominal damages are adjudicated not for the purpose of indemnifying the plaintiff for any loss suffered by him. Thus, Respondent finds that the Commission may have overstepped the bounds of its statutory authority by granting a form of civil damages that it has no power to grant under the law creating it.

¹² G.R. No. 196347, 23 January 2017

Respondent's interpretation of the power of the Commission to award indemnity is restrictive and defeats the wisdom and spirit behind the legislative intent of the DPA.

As held by the Supreme Court in the case of *Office of the Ombudsman vs Court of Appeals*¹³:

"In our recent ruling in *Office of the Ombudsman v. Court of Appeals*, we reiterated Ledesma and expounded that taken together, the relevant provision of RA 6770 vested petitioner with "full administrative disciplinary authority" including the power to "determine the appropriate penalty imposable on erring public officers or employees as warranted by the evidence, and, necessarily, impose the said penalty," thus:

[The] provisions in Republic Act No. 6770 taken together reveal the manifest intent of the lawmakers to bestow on the Office of the Ombudsman *full* administrative disciplinary authority. These provisions cover the entire gamut of administrative adjudication which entails the authority to, *inter alia*, receive complaints, conduct investigations, hold hearings in accordance with its rules of procedure, summon witnesses and require the production of documents, place under preventive suspension public officers and employees pending an investigation, determine the appropriate penalty imposable on erring public officers or employees as warranted by the evidence, and, necessarily, impose the said penalty. (Italicization in the original; boldfacing supplied)

We see no reason to deviate from these rulings. They are consistent with our earlier observation that unlike the "classical Ombudsman model" whose function is merely to "receive and process the people's complaints against corrupt and abusive government personnel," the Philippine Ombudsman, as protector of the people, is armed with the power to prosecute erring public officers and employees, giving him an active role in the enforcement of laws on anti-graft and corrupt practices and such other offenses that may be committed by such officers and employees. The legislature has vested

¹³GR No. 167844. November 22, 2006

him with broad powers to enable him to implement his own actions.” (*Emphasis supplied*)

Similarly, Section 7(b)¹⁴ and Section 37¹⁵ of the DPA when taken together reveals the manifest intent of the lawmakers to bestow to the NPC the full administrative disciplinary authority, which includes the authority to award all types of damages that deems appropriate to the circumstances to warrant justice and equity to the injured party. Limiting the word “indemnity” to actual and compensatory damages will only be prejudicial to the injured party especially in privacy cases, where the magnitude of the damages sustained cannot be quantified most of the time and the gravity of the effect cannot be immediately determined.

Further, as discussed by the Commission in one of its decided cases¹⁶, viz:

“The DPA provides that every data subject has the right to be indemnified for “any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.”¹⁷ Indeed, it is part of the Commission’s mandate to award indemnity on matters affecting any personal information.¹⁸

xxx

xxx. The DPA does not require actual or monetary damages for data subjects to exercise the right to damages.

¹⁴ SEC. 7. *Functions of the National Privacy Commission.* – To administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection, there is hereby created an independent body to be known as the National Privacy Commission, which shall have the following functions:

xxx

(b) Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: *Provided*, That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act;

¹⁵ SEC. 37. *Restitution.* – Restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.

¹⁶ Pascual vs Maersk, NPC 18-038

¹⁷ R.A. No 10173, Section 16(f)

¹⁸ R.A. No. 10173, Section 7(b)

As provided in the law, the consequences of processing inaccurate information is enough for the right to arise.¹⁹

The DPA provides that restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.²⁰ The relevant provision in this Code states:

Art. 2221. Nominal damages are adjudicated in order that a right of the plaintiff, which has been violated or invaded by the defendant, may be vindicated or recognized, and not for the purpose of indemnifying the plaintiff for any loss suffered by him.

The DPA gives individuals the right to receive indemnification from personal information controllers and personal information processors for both material and non- material damages.²¹ The Supreme Court has also clarified that no actual present loss is required to warrant the award of nominal damages, thus:

Nominal damages are recoverable where a legal rights is technically violated and must be vindicated against an invasion that has produced no actual present loss of any kind or where there has been a breach of contract and no substantial injury or actual damages whatsoever have been or can be shown.²²

In consideration of the foregoing, the Commission does not find any reversible error in awarding the Complainant with nominal damages.

IV. The requirement of exhaustion of administrative remedies is not absolute.

Respondent claims that there is no showing of compliance with the requirement of exhaustion of administrative remedy or of good cause to warrant a waiver thereof. Respondent contends that there was no allegation in the Complaint that the requirement of exhaustion of administrative remedy under Section 4, Rule II of the

¹⁹ Pascual vs. Maersk

²⁰ RA NO 10173, Section 37

²¹ See, Handbook on European Data Protection Law, p. 246.

²² Seven Brothers Shipping Corporation vs. DMC-Construction Resources, Inc., G.R. No. 193914, November 26, 2014.

NPC Rules has been complied with prior to the filing thereof. Respondent further states that neither was there any allegations in the Complaint of good cause to warrant the waiver of the said requirement. Hence, Respondent concludes that the complaint is dismissible on the ground that a condition precedent for filing the claim has not been complied with under Paragraph (j), Section 1, Rule 16 of the Rules of Court.

The Commission would like to point out to Respondent that the provision of the law is not absolute and is subject to certain exceptions. As provided by Section 4 of NPC Circular 16-04 in relation to Section 2, Rule II of the 2021 NPC Rules of Procedure²³:

“ xxx. The National Privacy Commission may waive any or all of the requirements of this Section, at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to the affected data subject.”

Clearly, the Commission is given the discretionary power, upon good cause shown, to waive any or all the requirements of this Section.

In this case, the Commission cannot turn a blind eye on the harm done to the Complainant's data privacy rights considering that the very contents of the text blast sent by the Respondent to the Complainant's contact list contain malicious disclosure of the Complainant's personal information.

WHEREFORE, premises considered, the Motion for Reconsideration dated 9 February 2021 of FCash Global Lending

²³ Section 2. Exhaustion of remedies. – No complaint shall be given due course unless it has been sufficiently established and proven that:

xxx

The NPC may waive any or all of the requirements of this Section at its discretion upon (a) good cause shown, properly alleged and proved by the complainant; or (b) if the allegations in the complaint involve a serious violation or breach of the Data Privacy Act of 2012, taking into account the risk harm to the affected data subject, including but not limited to:

xxx

Inc. is hereby **DENIED** for lack of merit. The Decision of this Commission dated 5 November 2020 is hereby **AFFIRMED**.

SO ORDERED.

Pasay City, Philippines
11 March 2021.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

GMT
Complainant

BRJYTLO
Counsel for FCash Lending Inc.

**COMPLAINTS AND INVESTIGATION DIVISION ENFORCEMENT
DIVISION**

GENERAL RECORDS UNIT

National Privacy Commission

X-----X

RESOLUTION**NAGA, D.P.C.:**

This refers to the breach notification report of Social Security System (SSS) dated 28 January 2017 concerning the loss of a paper bag containing documents and a USB flash drive with the information of Five thousand six hundred ninety-four (5,694) SSS employees. The flash drive contains an electronic report of SSS to PHILHEALTH and PAG-IBIG.

On 13 July 2018, the Commission issued a Compliance Order with a dispositive portion as follows:

“The Commission, pursuant to Section 7(a), 7(b), 7(d) and 7(e) of the Data Privacy Act of 2011, and NPC Circular 16- 03 on Personal Data Breach Management, finding the need for measure to address the current breach and to minimize the likelihood of the occurrence of another data breach, hereby ORDERS SSS to submit a report to this Commission on the status of the security measures being and proposed to be implemented within three (3) months from receipt of this Order.”

On 19 November 2018, SSS submitted a report on the status of the security measures being and proposed to be implemented. After evaluating said report, the Enforcement Division of this Commission directed the Data Protection Officer (DPO) of SSS to submit copies of the agency’s policies and procedures on the storage and transfer of personal data.

On 15 August 2019, in compliance to the order of the Enforcement Division, SSS submitted the following documents:

1. Revised Guidelines on Records Management;

2. General Information and Communication Technology Security Policy;
3. Electronic File Transfer Policy;
4. Password Policy; and
5. The Implementation of the Data Privacy Manual.

Further, SSS reported that they are implementing the following measures to ensure security of data stored and transported through removable media:

1. All files must be protected with encrypted passwords to prevent unauthorized disclosure and modification of files. Passwords must be in accordance with the Password Policy;
2. Ensure that only necessary files are copied and stored;
3. Full implementation of the Endpoint Encryption software acquired in May 2019. This software is capable of full disk and removable media encryption;
4. As a matter of policy, the SSS has discontinued acquisition and issuance of removable media;
5. Ensure the utmost security of removable media while in transport including provision of service vehicle; and
6. Preparation of the SSS Information Security Manual.

The Enforcement Division, through the assistance of this Commissions' Data Security and Technology Standards Division (DSTSD), issued its findings on the compliance of SSS, viz:

“The measures in the Letter that the SSS are currently implementing appear to be adequate. These measures can be improved by using AES-256 encryption for USB flash drives and to the individual records or files contained thereto. Further, whenever using removal media, the transfer of information to such media should be monitored, and procedures and authorization levels should be documented accordingly... The policies and procedures met most of the matching requirements from the NPC Circular 16-01 and ISO/IEC 27002.

xxx xxx xxx

WHEREFORE, premises considered, the Enforcement Division respectfully recommends to CLOSE the instant case.”

Given the sufficiency of the submissions of SSS in compliance with the orders of this Commission, and the absence of error and abuse of discretion on the part of the Enforcement Division and DSTSD, this Commission finds no reason to disturb their recommendations.

WHEREFORE, premises considered, it is resolved that the matter of NPC BN 17-048 “In re: Social Security System” is hereby considered **CLOSED**.

SO ORDERED.

Pasay City, Philippines;
21 January 2021.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

GDS

Data Protection Officer

JAV

Data Protection Officer

RCG

Data Protection Officer

ENFORCEMENT DIVISION

**COMPLIANCE AND MONITORING DIVISION GENERAL
RECORDS UNIT**

National Privacy Commission

**IN RE: PROFESSIONAL REGULATION
COMMISSION**

X ----- X

NPC BN No. 18-069

*(Formerly CID BN No. 18-069) For: Violation of the
Data Privacy Act of 2012*

RESOLUTION

NAGA, D.P.C.:

This Resolution refers to the data breach notification that the Commission received dated 25 May 2018 from the Professional Regulation Commission (PRC) in relation to a social media post of a citizen questioning the data privacy compliance and practice of said agency.

The Facts

On 07 May 2018, a certain citizen posted on his social media account a redacted photo questioning the data privacy compliance of PRC and other government agencies. According to the post, the PRC's logbook has fields that require the name and PRC license number of its guest.

On 09 May 2018, PRC's Data Protection Officer (DPO) reported the incident to the Complaints and Investigation Division (CID). The CID then requested PRC to submit a full breach report.

After a considerable delay and upon CID's follow-up, on 19 May 2020, PRC's new DPO submitted a letter stating that there was no data breach since no personal data was divulged in the post of the citizen and that no evidence was presented or submitted to prove that any unauthorized disclosure has occurred. Further, PRC also stated that upon the inquiry of their DPO with its different offices, the logbook described in the social media post is not in the possession of any of the offices nor such logbook can be found within the premises of the PRC.

On 08 July 2020, the CID submitted the case to the Commission for its resolution.

Discussion

Personal data refers to all types of personal information. Under the Data Privacy Act (DPA), it is divided into two major categories, namely: Personal Information¹ and Sensitive Personal Information².

On the other hand, Personal data breach is defined in the DPA Implementing Rules and Regulations (IRR) as, “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.”³

Given the above definitions, it can be deduced that no personal information was accidentally and unlawfully disclosed in the social media post of the citizen. The post contains a redacted photo of an alleged PRC logbook that has data fields on Registration No., Profession, and Name.⁴ No other personal information was disclosed other than the name of the citizen that posted said redacted photo.

On the concern regarding PRC and other government agencies logbook policies, while it is true that the logbook policy of every agency of the government should abide by the general data privacy principles of transparency, legitimate purpose, and proportionality⁵; the concerned citizen failed to substantiate his general claim that the PRC violated the DPA.

¹ Section 2 (g) Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

² Section 2 (l) Sensitive personal information refers to personal information: (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (4) Specifically established by an executive order or an act of Congress to be kept classified.

³ Section 3 (k) of the DPA IRR.

⁴ Attachment in the 08 May 2020 letter of the PRC to the CID

⁵ Section 18 of the DPA IRR in relation to Section 11 of the DPA.

Section 22 of NPC Circular 16-04 or The Rules of Procedure of the National Privacy Commission provides that the Commission shall adjudicate the issues raised in the complaint on the basis of all the evidence presented and its own consideration of the law. Hence, this Commission gives greater weight to PRC's statement that the logbook described in the social media post has not been in the possession or custody of any of its office over the bare allegations of the citizen in his social media post.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN No. 18-069 "In re: Professional Regulation Commission" is considered **CLOSED**.

SO ORDERED.

Pasay City, Philippines
23 July 2020.

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commission

WE CONCUR:

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commission

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

HCS
Data Protection Officer

ENFORCEMENT DIVISION
COMPLAINTS AND INVESTIGATION DIVISION GENERAL
RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION

**NAGA,
D.P.C.:**

This refers to the submission of Sun Life Grepa Financial, Inc. (SLGFI) of the copy of notification letter that was sent to the affected data subject in compliance with the Order of this Commission dated 15 October 2020.

The Facts

On 15 October 2020, the Commission issued a Resolution disposing, thus:

WHEREFORE, premises considered, this Commission **ORDERS** Sun Life Grepa Financial, Inc. to **SUBMIT** a copy of the notification letter that was sent to the affected data subject **within five (5) days** from receipt of this Order.

The Full Breach Report dated 12 October 2020 submitted by Sun Life Grepa Financial, Inc. is hereby **NOTED**, subject to the recommendations of the Compliance and Monitoring Division and further action of this Commission.

On 19 November 2020, this Commission received SLGFI's submission of the copy of notification letter dated 12 October 2020 that was sent to the affected data subject. The letter was divided in three major parts, namely: description of the incident, measures that SLGFI had taken to address the breach, and the assistance that SLGFI can provide to the affected data subjects.

Discussion

Evaluating the current submission of SLGFI, together with the Compliance letter dated 12 October 2020 and the Supplemental

Report dated 13 October 2020, this Commission finds the totality of SLGFI's submission to be compliant with the requirements of NPC Circular 16-03.

In the 15 October 2020 Order of the Commission, we noted that SLGFI's submission to be incomplete due to the non- attachment of the notification letter that was sent to the affected data subjects. Upon review of the submitted notification, this Commission now finds the contents to satisfy the requirements of Section 18 (C) of NPC Circular 16-03¹.

WHEREFORE, premises considered, this Commission finds SLGFI's notification letter dated 12 October 2020 to be **COMPLIANT** with the requirements of NPC Circular 16-03.

Pending the review of this Commission's Compliance and Monitoring Division (CMD) on the full breach report of SLGFI, the matter on data subject notification is hereby considered to be a closed matter.

SO ORDERED.

Pasay City, Philippines;
26 November 2020.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

¹ Content of Notification. The notification shall include, but not be limited to: 1. nature of the breach; 2. personal data possibly involved; 3. measures taken to address the breach; 4. measures taken to reduce the harm or negative consequences of the breach; 5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and 6. any assistance to be provided to the affected data subjects. Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

JSC
Data Protection Officer

**COMPLIANCE AND MONITORING DIVISION GENERAL
RECORDS UNIT**
National Privacy Commission

**IN RE: BREACH
NOTIFICATION REPORT OF
SUN LIFE OF CANADA**

CID BN 17-021

X-----

RESOLUTION

AGUIRRE, D.P.C.

In an Order dated 23 July 2020, the Commission required Sun Life of Canada (Philippines), Inc. (“Sun Life”) to show cause why it should not be subject to contempt proceedings and other actions available to the Commission for failing to comply with the Commission’s decision, thus:

WHEREFORE, the above premises considered, the Commission resolves to **ORDER** Sun Life of Canada (Philippines), Inc. to show cause in writing, within fifteen (15) calendar days from receipt of this Order, why it should not be liable for Failure to Notify under Section 20 of NPC Circular 16-03 and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.

In response to the Show Cause Order, Sun Life sent a letter dated 26 August 2020 explaining that:

1. A notification two years after the incident would cause undue alarm on the part of the data subjects.
2. The December 2019 Letter is not prohibited under NPC Circular 16-03.
3. Sun Life merely tried to exhaust all administrative remedies.
4. Sun Life believed in good faith that the Honorable Commission had yet to resolve the December 2019 Letter.
5. Sun Life did not willfully violate the Resolutions of this Honorable Commission.

**A. Requirements for exemption
from notification of data
subjects**

At the outset, it should be emphasized that notification of data subjects of data breaches is the general rule and exemption will only be allowed in exceptional circumstances when the Commission determines that

“such notification would not be in the public interest or in the interest of the affected data subjects.”¹ It is a basic rule of evidence and procedure that the Commission, in making this determination, cannot simply rely on bare allegations. It looks at the available evidence on record to see whether these are sufficient to overcome the presumption that notification is in the best interest of the data subjects.

In this case, in seeking to be exempted from notifying its data subjects, Sun Life alleged in its 19 October 2017 breach notification that the breach is unlikely to give rise to a real risk of serious harm to data subjects since controls are in place to prevent the takeover of the account or any amendment, withdrawal or cancellation.² It also alleges that “notification would not be in the best interest of the affected policy holders and may cause undue alarm.”³ No evidence being submitted to support Sun Life’s claims, this Commission denied its request for exemption.

Seeking the reconsideration of the Commission’s 29 July 2019 Resolution, Sun Life filed a letter dated 5 September 2019 reiterating its earlier submissions emphasizing the measures it has taken to prevent a recurrence of the incident, the controls it has in place to prevent any fraudulent use of the information on its system, and the lack of any concern or complaints received in relation to the information that was disclosed. Despite the Commission’s finding in its previous Resolution regarding Sun Life’s failure to submit any evidence to support its claims, Sun Life again chose not to provide this Commission with any evidence to support its assertions. Instead, it simply asserts that “there is no vulnerability pertaining to access in this case that may be exploited by others.”

While Sun Life may have taken the necessary steps to secure its system and prevent a recurrence of that incident, these remain mere assertions in the absence of any evidence to support them. In addition, the steps outlined by Sun Life are only with regard to the risks that may arise in relation to its own system. It did not consider the other risks, such phishing or social engineering attacks, that its data subjects may be subjected to as a result of the breach.

¹ National Privacy Commission Circular 16-03, Sec. 18(b).

² See, 19 October 2017 letter of Sunlife.

³ *Id.*

When the Data Privacy Act (“DPA”) states as one of the criteria for notification that the “unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject,”⁴ it does not qualify that the risks and harms that should be considered are only those within the control of the personal information controller that was breached. Instead, the risks and harms that data subjects may face must be viewed holistically taking into consideration all the relevant circumstances.

B. The procedure followed by Sun Life is improper

In response to this Commission’s Show Cause Order, Sun Life explained that the procedure it followed was not prohibited under this Commission’s rules and that it was merely trying to exhaust all administrative remedies when it met with our Enforcement Division to submit additional documents in support of its request for reconsideration. These will be discussed *in seriatim*.

i. A second Motion for Reconsideration is not allowed.

Sun Life asserts that: “there is nothing in NPC Circular 16-03 that prohibits a second motion for reconsideration. Absent such prohibition, the Honorable Commission cannot categorically state that ‘a second request or motion for reconsideration is not allowed under NPC Circular 16-03.’”⁵

Sun Life correctly states that NPC Circular 16-03 does not contain any prohibition on the filing of a second motion for reconsideration. It also does not contain anything on the process of filing a motion for reconsideration. As Sun Life is undoubtedly aware, NPC Circular 16- 03 only provides for the obligation of personal information controllers in relation to breaches, including the obligation to notify the Commission and data subjects in the event of a breach.⁶ The Commission’s Rules of Procedure are contained in NPC Circular 16- 04, Section 2 of which states:

⁴ Republic Act No. 10173, Sec. 20 (f).

⁵ Sun Life’s letter dated 26 August 2020, p. 4.

⁶ See, NPC Circular 16-03, Sec. 2. *Emphasis supplied.*

SECTION 2. Scope and Coverage. – These rules shall apply to all complaints filed before the National Privacy Commission or such other grievances, requests for assistance or advisory opinions, and **other matters cognizable by the National Privacy Commission.**

The proceedings involving personal data breach notifications clearly fall under “other matters cognizable by the National Privacy Commission.” Hence, the determination whether a personal information controller such as Sun Life may be exempted from the requirement of notifying its data subjects is a matter falling within the scope of NPC Circular 16-04.

It is a basic rule of statutory construction that statutes must be construed and harmonized with other statutes to form a uniform system of jurisprudence.⁷ Simply because NPC Circular 16-03 does not contain a provision prohibiting the filing of a second motion for reconsideration does not mean that it is allowed, as Sun Life claims, especially since it is expressly prohibited by NPC Circular 16-04:

SECTION 30. Appeal. – The decision of the National Privacy Commission shall become final and executory fifteen (15) days after the receipt of a copy thereof by the party adversely affected. **One motion for reconsideration may be filed**, which shall suspend the running of the said period. Any appeal from the Decision shall be to the proper courts, in accordance with law and rules.⁸

On the basis of this same provision, this Commission’s 28 October 2019 Resolution denying Sun Life’s Motion for Reconsideration has already become final and executory. As Sun Life itself admitted in its response to the Show Cause Order:

4. On 04 December 2019, Sun Life received the Honorable Commission’s Resolution dated 28 October 2019 (the “October Resolution”) denying the request for reconsideration in the September 2019 Letter.

5. On 23 December 2019, Sun Life responded to the October Resolution by submitting a letter dated 23 December 2019 (the “December 2019 Letter”) requesting for the deferment of the running of the period within which to comply with the requirements of the July Resolution pending a meeting with the Honorable Commission’s Enforcement Division.⁹

⁷ See, *Akbayan-Youth v. Commission on Elections*, G.R. No. 147066, 26 March 2011.

⁸ Emphasis supplied.

⁹ Sun Life’s letter dated 26 August 2020, p. 2.

Even assuming Sun Life's filing of the 23 December 2019 letter is allowed, it was filed beyond reglementary period having been filed nineteen (19) days after Sun Life received a copy of this Commission's resolution denying its request for reconsideration.

ii. Sun Life's reliance on the doctrine of exhaustion of administrative remedies is misplaced.

Its second request for reconsideration having been filed out of time and in clear contravention of the prohibition on the filing of second motions for reconsideration, Sun Life cannot now claim that it was merely exhausting administrative remedies when it sought to meet with this Commission's Enforcement Division and submit additional evidence.

In the first place, the proper time to submit evidence to substantiate its request for exemption was when it first filed the same or, at the very least, when this Commission called its attention to this deficiency in the 29 July 2019 Resolution. In both instances, Sun Life either failed or chose not to.

If Sun Life believes that this Commission's decision denying its request for exemption did not consider all the relevant factors, it only has itself to blame for not submitting all the necessary evidence and raising all of its arguments when it had numerous opportunities to do so.

Similar to parties coordinating with the sheriff in the execution stage of a court case, it should be stressed that there is nothing wrong with meeting with the Enforcement Division to clarify how compliance with this Commission's resolution should best be carried out. It is an altogether different matter, however, to attempt to get the sheriff to intercede on a party's behalf to reverse the decision of the court. This is what Sun Life attempted to do in this case. While this Commission endeavors to keep an open line of communication with its stakeholders, this does not mean that proper procedure can be dispensed with especially in pending cases and more so in cases, such as this one, where a decision has already been rendered. This is not what the doctrine of exhaustion of administrative remedies contemplates.

In addition, Sun Life attempts to justify its refusal to comply with this Commission's decision by pointing to the length of time that has passed from the time it requested for exemption until the denial, stating:

Without a doubt, it heightened Sun Life's earlier concern that a notification would cause undue alarm on the part of the data subjects.

Considering the foregoing factual antecedents, it was reasonable for Sun Life to be persistent in seeking a reconsideration of the July Resolution and the October Resolution, hence, the submission of the October 2019 Letter and the December 2019 Letter.¹⁰

To reiterate, the notification of data subjects is the general rule. In asking for exemption from this general rule, personal information controllers like Sun Life bind themselves to comply with this Commission's Decision on their request. They cannot impose as a condition to such compliance that the Decision must be rendered within a period of time convenient to them. In the absence of a change in circumstances that would render compliance impossible, and Sun Life has not alleged much less submitted any evidence in this regard, it is subject to the requirements of the DPA and NPC Circular 16-03, as clarified by the Commission in its Decision.

Nevertheless, at its core, the notification requirement under NPC Circular 16-03 is for the protection and benefit of data subjects. This Commission acknowledges the efforts Sun Life made to address the breach when it occurred and, although delayed, the efforts it has since undertaken to properly notify and protect its data subjects as shown in its 07 July 2020 and 28 July 2020 letters.

Despite the issues discussed herein being straightforward, rooted as they are in express provisions and clear principles of the Data Privacy Act and its related issuances, this Commission recognizes that misconceptions and misapplications of these doctrines still persist. Considering that the factual antecedents of this case all occurred during the time of Sun Life's previous data protection officer, hopefully Sun Life will take stock of the circumstances of this case and the Commission expects it to take the necessary steps to ensure not only that this situation will not be repeated but, more importantly, that it will be in a better position to safeguard its data subjects. Compliance

¹⁰ Sun Life's letter dated 26 August 2020, p. 3.

with the DPA entails more than simply ticking off boxes on a checklist such as the registration of a Data Protection Officer, conduct of a privacy impact assessment, creation of a data protection policy, or the exercise of breach reporting procedures. Companies must realize that compliance with the DPA involves doing such activities within a framework of protecting the data subjects from very real risks, such as what the affected data subjects faced in this case.

Guided by the principle that the power of contempt should be used sparingly, judiciously, and with utmost self-restraint,¹¹ this Commission resolves to consider Sun Life as having satisfactorily complied with the Show Cause Order. Sun Life is warned, however, that any violation of a similar nature will be dealt with more severely.

WHEREFORE, the above premises considered, the Commission resolves to consider this matter **CLOSED**. Sun Life of Canada (Philippines), Inc. is hereby given a **STERN WARNING** that a repetition of this conduct or a similar infraction shall be dealt with more severely.

SO ORDERED.

City of Pasay, Philippines;
10 September 2020.

Sgd

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

¹¹ See, *Baustista v. Yujuico*, G.R. No. 199654, 03 October 2018.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JSC
Data Protection Officer

ENFORCEMENT DIVISION
COMPLIANCE AND MONITORING DIISION
GENERAL RECORDS UNIT
National Privacy Commission

MNLC, INC., represented by
IKP,

Complainant,

-versus-

NPC Case No. 19-528

(Formerly CID Case No. 19-G-528)

*For: Violation of Section 13, in
relation to Section 25(b) of the
Data Privacy Act of 2012*

**PXXX CORPORATION, RCM AND
AD**

Respondents.

X _____ X

RESOLUTION

For consideration of the Commission is the Motion filed by the respondents PXXX Corporation, RCM, and AD seeking reconsideration of the Order dated 11 September 2019, which stated the following:

The DPA provides that it is the policy of the State to protect the fundamental human right of privacy.¹ This policy taken together with the DPA's interpretation provision that states "[a]ny doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interest of the individual about whom personal information is processed," signifies that the protection of the rights of the data subject is considered public interest as contemplated in Section 7(c) of the DPA.

XXX

In view of the foregoing, a temporary ban on the processing of personal data is hereby issued against the respondent PXXX Corporation. The temporary ban shall cover the following:

¹ Data Privacy Act of 2012, Section 2.

1. The processing of personal data of the MNLCI's church members who have not yet provided their identification documents to respondents for validation; and
2. The requirement for the use of PXXX-issued IDs for the MNLCI church members who have already submitted their passports and IDs.

PXXX Corporation is hereby ordered to (1) return to MNLCI's church members all the copies of their passports and valid IDs; (2) delete or dispose all copies of the passports and valid IDs, digital or otherwise; and (3) to allow MNLCI to provide IDs for their church members and officers bearing only their photos and English names.

On 25 September 2019, the respondents filed their Motion for Reconsideration which argues that “[t]o consider the complaint of MNLC as one permeated with public interest would create an absurdity.”² The respondents also stated, in their Motion, that they have conformed and observed, “not just a sole condition mandated in the [Data Privacy] Act but several of which, if not all.”³

The Commission denies the Motion for Reconsideration.

The respondents argue that “public interest refers to what will benefit, affects or related [to] the public in general not those merely of a particular class. MNLC is a corporation, a particular and specified class, composed of church members which are mostly foreign individuals, certainly they cannot be considered public in general for the protection against public interest to apply.”⁴

The respondents enumerate cases decided by the Supreme Court that gave “illustrations of entities imbued with public interests” which they claim to have “common denominators,” yet they also admit that “the High Court did not categorically define public interest.”⁵ They also cited the case of *Valmonte v. Belmonte Jr.* which held that:

In determining whether or not a particular information is public concern there is no rigid test which can be applied. “Public concern” like “public interest” is a term that eludes exact definition. Both terms embrace a broad spectrum of subjects which the public may want to know, either because these directly affect their lives, or simply because such matters naturally arouse the interest of an ordinary citizen. In the final analysis, **it is for the courts to determine on a case by case basis whether the matter at issue is of interest or important, as it related to or affects the public.**⁶

² *Motion for Reconsideration*, p. 3.

³ *Ibid.*, p. 5.

⁴ *Ibid.*, p. 3.

⁵ *Ibid.*, p. 3.

⁶ G.R. No. 74930 (1989). Emphasis in the original.

This supports the basis of the Order dated 11 September 2019. Based on the pronouncements of the Supreme Court, the respondents cannot limit the definition of “public interest” on the basis of the number of individuals involved. The Supreme Court has even pronounced the term “public” is a “comprehensive, all-inclusive term” and said that “properly construed, it embraces everyone.”⁷

What the Data Privacy Act of 2012 (DPA) provides is that the Commission may “impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest.”⁸ The Commission upholds the investigating officer’s position in the DPA provision stating “it is the policy of the State to protect the fundamental human right of privacy” is considered public interest as contemplated in Section 7(c) of the law. This declaration of policy in the DPA, having been enacted by Congress and the President, as representatives of the people, is a manifestation of a matter relating to the general welfare of the public.

Given all these, respondents’ position that it is absurd to consider the complaint of MNLC as one that is permeated with public interest is not convincing.

It must be emphasized that the personal data involved (citizenship, passport number, and individual’s ID number as determined by the issuing authority) fall under the enumeration of sensitive personal information which can only be processed based on the criteria provided under Section 13 of the DPA.⁹

⁷ Subido v. Ozaeta (1948), G.R. No. L-1631.

⁸ Section 7(c).

⁹ SEC. 13. *Sensitive Personal Information and Privileged Information.* – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

(b) The processing of the same is provided for by existing laws and regulations: *Provided*, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further*, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided*, That such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further*, That the

The respondents anchor their claim of observing and conforming to the DPA on having obtained the consent of the members of MNLC to use the MXXX ID. They cite an e-mail dated 28 June 2019 from IKP, an elder of MNLC, that stated:

I am now writing this letter to you as Head of the Elder Committee of MNLC that we MNLC officially confirm that all our church member including Pastors and Elders will use MXXX ... for purposes of smooth and quick entrance to process for normal and spiritual worship on Sunday...because serving normal and spiritual worship for their Good God is really most important and worthy matter in their whole life.¹⁰

Indeed, consent is one criteria for the lawful processing of sensitive personal information under the DPA. A proper reliance on consent by a personal information controller, however, requires adherence to the provisions of the law.

The DPA provides that the consent of a data subject must be a “freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.”¹¹

In determining whether consent was freely given, the data subject must be given a real choice – that is, without any element of pressure or influence which could affect the outcome of the choice, resulting from an imbalance between the controller and the data subject. In relation to the requirement that consent be specific, such consent cannot be overly broad. For instance, “bundled” consent will generally not suffice as the data subject is not empowered to make a true choice.¹² This means that consent to an enumeration of various, unrelated purposes of processing combined in a single paragraph cannot be considered specific because the data subject will be bound to sign off on the entire provision in toto.¹³ Consent given through an informed

sensitive personal information are not transferred to third parties: *Provided, finally*, That consent of the data subject was obtained prior to processing;

(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

¹⁰ Motion for Reconsideration, p. 6.

¹¹ Section 3(b).

¹² NPC Advisory Opinion 2018-063 dated 23 October 2018.

¹³ *Id.*

indication of will may include a signature, an opt-in box, sending a confirmation e-mail, or oral confirmation, among other means.

The e-mail that respondents cited in their Motion, supposedly an indication of consent as a lawful basis for processing, must be contextualized. This Commission notes that this e-mail was written after several events that have already unfolded involving the respondent corporation and their policies and the MNLC church members. The respondents have not refuted the allegations in the Complaint-Affidavit dated 19 July 2019 which stated thus:

On 12 May 2019, tempers flared resulting in exchange of words between MNLCI members and PXXX's guards. In a letter dated 15 May 2019, PXXX banned two (2) respected church members, Senior Pastor MH and LSB, from entering the Building from 14 to 19 May 2019.

xxx

Guard dogs are posted at the entrance and churchgoers are delayed for as long as an hour and a half before they can enter the Building." They attach pictures of the long line at the entrance endured by MNLCI's members on 23 June 2019, thereby leaving mostly vacant seats by 11:00AM, which is the start of our time of worship during Sundays. Such form of harassment was implemented by PXXX by significantly reducing the entrance line to one, intended to force churchgoers to surrender their passports and valid ID's for processing by PXXX's employees, supposedly for the production of PXXX-issued ID's that shall be paid for by MNLCI's members.¹⁴

While the consent evidenced by the e-mail dated 28 June 2019 may be considered as specific and an informed indication of will, such cannot be considered "freely given" as contemplated in the law. An imbalance already exists between the controller and data subject, considering that the respondents control the MNLC members' access to their worship service which they describe as a "really most important and worthy matter in their whole life."¹⁵ As cited in the Motion, the e-mail confirming the use of the MXXX ID was "purely for the purpose of smooth and quick entrance process for normal and spiritual worship on Sunday."

Even assuming that the email from IKP can be taken as validly obtained consent, the collection of sensitive personal data for the mandatory issuance of uniform IDs to the members of MNLC still

¹⁴ Records, pp. 3&5.

¹⁵ Motion for Reconsideration, p. 6.

cannot find justification under the law for failing to meet the requirements of the proportionality principle.

In their Motion, the respondents state that “to ensure safety, security measures are needed to be imposed and part of which is to identify the tenants of the buildings, visitors coming to and from and requiring them to wear identification cards.”¹⁶

In arguing the observance of proportionality, the respondents state that “while indeed it is true that other tenants provide an ID of their own...[t]he reason why respondents allow them is due to the fact that other tenant’s [sic] employees have 201 files (employee record) with them.”¹⁷

Notably, this is a new argument that is inconsistent with their earlier position on the supposed need for stricter security measures imposed on the members of MNLC. During the summary hearings, respondent AD, acting as the respondent corporation’s Legal and Corporate External Affairs Head, stated that while the MNLC-issued IDs showed both the Korean and English names of the church members, the Korean characters were bigger and more prominent. He stated that this was a security threat to the other tenants of the building, because only the church members can read and understand the Korean characters. Also included in the annexes of the Complaint-Affidavit is a letter dated 16 May 2019¹⁸ from the respondent corporation, through respondent AD, stating that “...after much review of your identification cards, our security and safety consultants have observed that the archetype of the MNLCI Identification Cards are without a doubt susceptible to security breach, which may include but not limited to meagre [sic] identification control system and counterfeit.”

The investigating officer’s Order imposing a temporary ban on processing by PXXX corporation was issued based on the evidence on record, pursuant to the NPC Rules of Procedure.¹⁹ The respondents cannot now assail such Order using arguments that have not been previously presented, much less substantiated.

Nevertheless, it remains undisputed that these stricter security measures applied only to MNLCI’s church members and not to the other tenants of the building.

¹⁶ *Ibid* at p. 7.

¹⁷ *Id.*

¹⁸ *Complaint Affidavit*, Annex E. Records, p. 34.

¹⁹ See NPC Circular 16-04, § 19. Dated 15 December 2016.

The Implementing Rules and Regulations of the DPA elaborates on the requirements of the principle of proportionality stating that the “processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed **only if the purpose of the processing could not reasonably be fulfilled by other means.**”²⁰

The MXXX Building House Rules and Regulations explain their access policies in this way:

3. ACCESS AND OPERATING HOURS

XXX

- 3.4 Office visitors and clients may be allowed entry when properly identified and acknowledged by the person/s to be visited and prior processing by building security. Person/s not properly identified or covered by an **authorization from unit owners or tenants** shall not be allowed entry beyond regular hours.²¹

In determining what information can be collected for and displayed on the ID card, the respondents must consider the purpose for such ID. The above-cited House Rules and Regulations signifies that the ID is an exhibit of such authorization to enter from the building tenant. There is no documented policy which declares that the ID card should serve other purposes, nor is there anything that requires the tenant to be supported by 201 file records or to have specific security measures. Notably, the respondents in this case wrote to a letter dated 24 June 2019 to the Bureau of Immigration, which stated:

Dear [Bureau of Immigration] Commissioner Jaime H. Morente, xxx [We] are dumbfounded by the blatant disregard of the simple NO-ID, NO-ENTRY Policy of the MNLC. In this regard, we ardently request your office to look into this matter as there might be Korean Nationals of the MNLC who have expired VISA or undesirable aliens or fugitives from other countries.²²

All these premises considered, the Commission finds that there are no substantial grounds to overturn the investigating officer’s Order imposing a temporary ban on the processing of personal data by PXXX Corporation.

²⁰ IRR, § 18(c), emphasis supplied.

²¹ Records, pp. 190-191. Emphasis supplied.

²² *Ibid.*, at p. 62.

WHEREFORE, all premises considered, the Motion for Reconsideration of the Order dated 11 September 2019 is hereby DENIED and the respondents are ordered to submit an affidavit of compliance to the Order's directive to (1) return to MNLCI's church members all the copies of their passports and valid IDs; (2) delete or dispose all copies of the passports and valid IDs, digital or otherwise; and (3) to allow MNLCI to provide IDs for their church members and officers bearing only their photos and English names.

Let the records of this case be REMANDED to the Complaints and Investigation Division for the continuation of the proceedings.

Pasay City, 18 November 2019.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
IVY D. PATDU
Deputy Privacy Commissioner

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

COPY FURNISHED:

ABELLERA AND CALICA LAW OFFICES
Counsel for Complainant

MTCP
Counsel for Respondents

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION

AGUIRRE, D.P.C.

This Resolution refers to the notification logs submitted by E-Science Corporation (E-Science)¹ in response to the Order of this Commission for it to submit the confirmation logs or other proof that the affected data subjects received the required notification under NPC Circular 16-03.²

The Facts

On 22 October 2020, this Commission issued a Resolution³ with the following disposition, to wit:

WHEREFORE, premises considered, E-Science Corporation is **ORDERED** to submit the confirmation logs or other proof of receipt in compliance to the Notification of the Data Subjects **within five (5) days** from receipt of this Resolution.

Furthermore, having found the Explanation of E-Science Corporation sufficient, the Show Cause Order is hereby considered as a **CLOSED** matter.

In response to the said Resolution, E-Science submitted a letter with the subject “Notification Logs as Compliance for NPC BN No. 20-124.”⁴ In its submission, it indicated the notification message and read status of the data subjects as of 14 December 2020. As to those data subjects who were not able to read the notification message, E-Science enumerated the following possible reasons thereof:

¹ Letter with the subject “Notification Logs as compliance for NPC BN 20-124 submitted by E- Science Corporation.” Dated 14 December 2020.

² NPC Circular 16-03. Personal Data Breach Management. Dated 15 December 2016.

³ Resolution dated 22 October 2020, *In re: E-Science Corporation*, NPC BN 20-124.

⁴ *Supra* note 1.

- (a) Resigned employee;
- (b) The user is no longer active; and
- (c) No internet connectivity to access or receive the notification.⁵

E-Science expressed its hope that such submission satisfies the Commission's Order⁶ for it to submit the confirmation logs or other proof of receipt in compliance with the requirements for notification of the data subjects under NPC Circular 16-03.

Discussion

Section 18 (C) of NPC Circular 16-03 provides that:

The notification shall include, but not be limited to:

1. **nature of the breach;**
2. **personal data possibly involved;**
3. **measures taken to address the breach;**
4. **measures taken to reduce the harm or negative consequences of the breach;**
5. **representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and**
6. **any assistance to be provided to the affected data subjects.**

Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.⁷

Moreover, Section 18 (D) of same Circular provides that:

Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. **The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made**

⁵ *Ibid.*

⁶ *Supra* note 3.

⁷ Emphasis supplied.

aware of the breach: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.⁸

The submission made by E-Science to this Commission indicated the automated message it sent to the affected data subjects, thus:

Hi Team,

We have recently found out from one of our service providers that some names and email addresses of our employees may have been included in a computer that was hacked, which happened early July of this year. While the information hacked does not include sensitive personal information and/or that said information may not be useful or updated, the hacker may use the data to send you spam and other malicious content. As such, please be extra careful in opening emails and links that are not familiar to you. Also, we encourage you to change your passwords regularly for additional security. If you have questions, you may direct your queries to ABG, for clarification.⁹

The submission also attached an enumeration of the names of the affected data subjects, their respective user codes, the status on whether they have read the notification message, and the date when the message was sent.

In consideration of the above information and the large number of data subjects involved, the Commission finds that the notification sent by E-Science and proof of its receipt by the affected data subjects complies with R.A. 10173 or the Data Privacy Act, its Implementing Rules and Regulations, and NPC Circular 16-03.

⁸ Emphasis supplied.

⁹ *Supra*, at note 1.

WHEREFORE, premises considered, this Commission hereby finds E-Science Corporation's submission of confirmation logs **SUFFICIENT** for compliance with its Order stated in the Resolution dated 22 October 2020. This Commission hereby considers the matter **CLOSED**.

SO ORDERED.

Pasay City, Philippines
17 December 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
WE CONCUR: Deputy Privacy
Commissioner

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:
JYP
Data Protection Officer

**COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION**
GENERAL RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION

AGUIRRE, D.P.C.:

This Resolution refers to the Letter¹ of the Commission on Elections (COMELEC) providing notice to this Commission of a possible personal data breach concerning the registered voters of Talavera, Nueva Ecija, and its request for extension of time to notify the data subjects.

The Facts

On 10 November 2020, COMELEC received an unsigned memorandum dated 04 November 2020 from JBR, Election Officer (EO), Office of the Election Officer (OEO) of Talavera, Nueva Ecija, reporting that on 30 October 2020, a burglary incident happened at the OEO of Talavera, Nueva Ecija.²

After the inventory was conducted, the following items were found missing:

- (1) One portable hard drive which contains the voter registration records and VRS backups (COMELEC property);
- (2) One Lenovo Think Pad Laptop with SN XXXXXXXX8 (COMELEC property) which contains the voter registration system program, other VRS reports and data backup;
- (3) One Acer laptop (LGU property);
- (4) One Samsung Notebook (LGU property);
- (5) Php 350.00 hidden inside an employee's drawer; and
- (6) Two hundred pieces of face shields.³

¹ Letter dated 16 November 2020.

² *Ibid.*

³ *Ibid.*

JBR also reported the following:

- (1) The lock of the office vault was smashed and destroyed;
- (2) The incident was immediately reported to the local police and investigation is on-going;
- (3) The concerned officers of COMELEC were informed; and
- (4) Inventory of all office documents is on-going.⁴

Furthermore, COMELEC requested that since such notice has been submitted beyond the seventy-two (72) hour period, within which the Commission should be notified, the same be considered justified and reasonable considering the consecutive work suspensions that followed after the receipt of JBR's report, thus:

Please note that while this Office received the report of JBR on 10 November 2020, work in government offices in the National Capital Region as well as in Region III, among other regions, was suspended effective 3:00 o'clock in the afternoon of 11 November 2020 (Thursday) until 13 November 2020 (Friday).⁵

COMELEC informed this Commission of their security measures, thus:

Relatedly, undersigned respectfully informs the NPC that, as a security feature, all the data encoded in the computers of all OEOs involved the voters of their respective cities and municipalities only, and are already encrypted in AES 256. The portable hard disks containing said data are likewise encrypted.⁶

According to the letter, the COMELEC Executive Director and Data Protection Officer issued a memorandum dated 10 November 2020 for the Director IV of COMELEC's Information Technology Department, as well as Director III of the Finance Services Department and Data Compliance Officer, informing them about the report of JBR with a directive to investigate the incident.⁷

⁴ *Ibid.*

⁵ *Ibid.*

⁶ *Ibid.*

⁷ *Ibid.*

Lastly, COMELEC claims that since the investigation is on-going and the challenges posed by the threat of COVID-19, it is not reasonably possible to notify the data subjects within the prescribed period. For these reasons, COMELEC requests for an extension of time to comply with the notification of data subjects⁸ without stating a specific timeline for such.

Discussion

This Commission denies the request for an indefinite extension of COMELEC to notify the affected data subjects.

Section 18(B) of NPC Circular 16-03 provides that:

If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification. A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects. **The Commission may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach,** taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.⁹

In this case, COMELEC requests for an extension to comply with the notification of data subjects on two (2) grounds, namely, (1) that an investigation is on-going, and (2) the challenges posed by the threat of COVID-19.¹⁰

A careful scrutiny of the records reveals that there are two (2) investigations referred to in this case. First, the on-going investigation conducted by the local police. Second, the

⁸ *Ibid.*

⁹ Emphasis supplied.

¹⁰ *Supra* note 1.

investigation under the directive of COMELEC through its Information Technology Department and Finance Services Department.

As to the on-going investigation by the local police, there is no showing how the notification to data subjects will hinder the investigation on robbery or other relevant crime thereto. Not all criminal investigations, even those conducted as a result of the breach as in this case, can be considered as a ground for postponement of notification of data subjects. Simply mentioning that a criminal investigation is being undertaken is not sufficient. The burden is on the party requesting for postponement to show that the notification will indeed affect the outcome of the investigation.

As to the investigation within the COMELEC, this is not the investigation contemplated by Section 18 of NPC Circular 16-03, which specifically refers to criminal investigations.

Furthermore, while the challenges posed by the threat of COVID-

19 pandemic was raised by the COMELEC as a reason for its postponement to notify the data subjects, it was not explained how it is not reasonably possible to notify the data subjects within the prescribed period. More importantly, it did not state what period of additional time is requested for. The request for an indefinite extension of notification of the affected data subjects is hereby denied.

The Commission, however, notes that no mention was made about the COMELEC's concrete steps for the retrieval of the affected data subjects' information which may have been stored in the stolen equipment. In order to effect the notification of the data subjects which will enable them to take the necessary precautions, the Commission directs the COMELEC to conduct notification through alternative means under Section 18(D) of NPC Circular 16-03¹¹, thus:

Notification of affected data subjects shall be
done individually, using secure
means of communication,

¹¹ NPC Circular 16-03. Personal Data Breach Management. Dated 15 December 2016.

whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: *Provided*, that **where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner:** *Provided further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.¹²

This Commission likewise brings to the attention of COMELEC the required submission of its Full Breach Report. Section 17(C) of NPC Circular 16-03 provides that:

There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. **In both instances, the Commission shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days**, unless the personal information controller is granted additional time by the Commission to comply.¹³

While COMELEC has requested for additional time to notify the data subjects herein, no request for additional time to submit the full report has been made. The COMELEC is reminded that the notification of data subjects and notification of the Commission are two (2) different requirements to be complied with by personal information controllers (PICs).

WHEREFORE, premises considered, the Commission on Elections is **ORDERED, within ten (10) days** from receipt of this Resolution, to: (1) Submit its Full Breach Report, and (2) Notify the data

¹² Emphasis supplied.

¹³ Emphasis supplied.

subjects through alternative means and submit proof of compliance thereto.

SO ORDERED.

Pasay City, Philippines
26 November 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

BJS
Executive Director and Data Protection Officer
Commission on Elections

THRU: MRA

Representative
Commission on Elections

**COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION**

GENERAL RECORDS UNIT

National Privacy Commission

MNLC, INC. represented by
IKP,
Complainant,

-versus-

NPC Case No. 19-528
(Formerly CID Case No. 19-G- 528) *For: Violation of Section 13, in relation to Section 25(b) of the Data Privacy Act*

PXXX CORPORATION, RCM and AD,
Respondent.

X-----X

RESOLUTION

NAGA, D.P.C.:

For consideration of the Commission is the Motion for Reconsideration dated 17 January 2021 filed by Respondents PXXX Corporation, RCM, and AD of the Decision dated 29 October 2020 which finds that Respondents have violated Section 25(b) of the Data Privacy Act of 2012 (DPA). Respondents pray for the Decision to be reconsidered and set-aside and a new one should be issued dismissing the present complaint.

The Facts

On 18 January 2021, Respondents filed a Motion for Reconsideration dated 17 January 2021 before this Commission. In their Motion for Reconsideration, Respondents questioned the jurisdiction of the Commission over the case considering that the Complainant has no personality to file the instant complaint.¹

The Respondents further argued that the real party-in-interest are the individual members of the MNLCI (MNLCI) which have not

¹ Motion for Reconsideration dated 17 January 2021, p. 1

executed authorization for Ill KP, GSP, and HCM to represent MNLCI in the proceedings before this Commission. Further, Respondents contended that for the Commission to have jurisdiction, the complaints must be filed by a data subject. They stated that it is a serious error not to dismiss the case since it is filed by a person with no legal interest nor personality to institute the case. Respondents argued that considering MNLCI is a corporate or artificial being, no personal information could be processed nor there is a privacy right to be protected.²

Respondents maintained that as stated in the NPC Circular No. 2021-01³, there is a need of a special power of attorney in case one or more data subjects is represented by a single juridical entity. Ill KP, who filed the complaint, does not have the required special power of attorney empowering him to represent MNLCI in this case. Further, Respondents stated that since Ill KP does not have authority to represent the individual members of the MNLCI, they are deemed to not have participated in this case. Hence, it is improper for the Commission to award damages to the said members.⁴ In relation thereto, Respondents stated that the Commission may not capriciously nor arbitrarily waive its own rules by mere invocation of, “serious violation of the Data Privacy Act”.⁵

Moreover, Respondents argued that the Complainant failed to exhaust the remedies available to them as provided by Section 4 of the NPC Circular 16-04⁶, which provides that no complaint shall be entertained unless the complainant has informed the concerned entity. Respondents added that the individual members of the MNLCI have not informed them of the alleged privacy violation. Although letters were sent to ACLO (Counsel for the Respondents), Respondents stated that they have the right not to entertain letters considering that the Complainant does not have Special Power of Attorney nor Secretary’s Certificate.

On the substantive matters, Respondents maintained that MNLCI consented on the processing of their personal data. They

² *Ibid.* at p. 2

³ 2021 Rules of Procedure of the National Privacy Commission, effective on 12 February 2021

⁴ *Ibid.* at p. 3

⁵ *Ibid.* at p. 5

⁶ 2016 Rules of Procedure of the National Privacy Commission

further argued that there is no need to contextualize the contents of the emails and Secretary's Certificate given that MNLCI explicitly consented on the processing of personal information.

On the issue of legitimate interest to collect and process personal information, the Respondents stated that the processing of personal information was made pursuant to their legitimate interest. They argued that as manager and administrator of the MXXX Plaza Building, they have the duty and legal obligation to protect and secure said premises.⁷

Lastly, on the Commission's finding that the Complainants are entitled to damages, Respondents contended that the data subjects must be individually identified to be entitled to damages. They stated that the identities of the individual members of MNLCI must be established and it must be proven that they are indeed members of the church. Respondents stated that in this case, there is no evidence presented to establish the names of MNLCI members.⁸

Complainant submitted an Opposition to the Respondents' Motion for Reconsideration dated 29 January 2021. In their Opposition/Comment to the Motion for Reconsideration, the Complainant stated that the Respondents based their argument on the Frequently Asked Questions (FAQs) of the 2021 Rules of Procedure in arguing that the Commission has no jurisdiction over the case. Complainant argued that FAQs to a proposed administrative rule have no bearing on the matter of jurisdiction and that the Commission correctly ruled in its Decision that jurisdiction was validly acquired.⁹

In terms of jurisdiction over the parties, Complainant stated that there was implied consent of the church members to bring the violation of data privacy rights to the Commission, and that the Respondents themselves admitted that the data processing involved all the MNLCI church members.¹⁰

⁷ *Ibid.* at p. 9

⁸ *Ibid.* at p. 10

⁹ Opposition to the Respondents Motion for Reconsideration dated 29 January 2021. at p. 2

¹⁰ *Ibid.*

On the Respondents' argument that the Complainant failed to exhaust remedies when the latter failed to inform them in writing of the privacy violation, the Complainant assailed the Respondents' argument by stating that the NPC Rules of Procedure should be liberally interpreted to better serve the objective of the DPA.

On the issue of consent and legitimate purpose in the processing of personal information, the Complainant agreed to the previous ruling made by the Commission in its Decision. First, their consent was not validly obtained considering the imbalance of power between the parties. And the legitimate interest of the Respondents, however legitimate, was disproportionate to the means used by them.¹¹

Complainants stated that they failed to see the Respondents' argument that in awarding the damages, the data subjects must first be identified as basis to reverse the Decision¹². They argued that if it is the Respondent's belief that church members must be identified before awarding the damages, then they only need to ask for the list of church members to MNLCI. Complainant then opined that the Respondents filed the Motion for Reconsideration just to delay the payment of indemnification. Lastly, Complainant prayed that the Motion for Reconsideration be denied by this Commission for lack of merit.¹³

Issue

Whether the Motion for Reconsideration merits the reversal of the 29 October 2020 Decision of this Commission.

Discussion

We deny the Respondents' Motion for Reconsideration.

Ruling on the Procedural Issues

¹¹ *Ibid.* at p. 5

¹² Decision dated 29 October 2020.

¹³ Opposition to the Respondent's Motion for Reconsideration dated 29 January 2021, at p. 5

This Commission finds that there are no new material facts added for our consideration and that the Respondents merely restated their prior arguments in their 17 January 2021 Motion for Reconsideration.

On the Respondents' contention of this Commission's jurisdiction over the case, this Commission reminds that the essential aspect of determining the Commission's jurisdiction is whether the allegations manifest a privacy violation against a data subject. Again, the fact that Ill KP in his Complaint-Affidavit alleged the Respondents committed acts that are violative of his privacy rights and other church members executed affidavit in support of his Complaint-Affidavit does not alter their status as affected data subjects, who are clearly within the scope of DPA's protection and this Commission's jurisdiction.

On the matter concerning the exhaustion of remedies, the Respondents maintain their argument that the individual members of MNLCI have not informed PXXX Corporation with regard to the alleged privacy violation. Respondents contested this Commission's statement in the previous Decision whereas Section 4 of the NPC Circular 16-04 provides that the Commission has the discretion to waive any of the requirements upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to Complainant.¹⁴ As stated by the Respondents in their Motion for Reconsideration:

With all due respect, respondents posit that the Honorable Commission may not capriciously or arbitrarily waive its own Rules simply because of mere invocation of "serious violation or breach of Data Privacy Act" on the part of the complainant. If we are to follow such reasoning, there can be no occasion where the rule on exhaustion of remedies will be applied because of every litigant's bare invocation of "serious violation or breach of the Data Privacy Act."

Again, this Commission refers to the last paragraph of Section 4 of NPC Circular 16-04 which was carried over in the NPC Circular 2021-01, viz:

¹⁴ Decision dated 29 October 2020. At p. 12.

SECTION 4. Exhaustion of remedies. – No complaint shall be entertained unless:

- a. the complainant has informed, in writing, the personal information controller or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same;
- b. the personal information controller or concerned entity did not take timely or appropriate action on the claimed privacy violation or personal data breach, or there is no response from the personal information controller within fifteen (15) days from receipt of information from the complaint ;
- c. and the complaint is filed within six (6) months from the occurrence of the claimed privacy violation or personal data breach, or thirty (30) days from the last communiqué with the personal information controller or concerned entity, whichever is earlier.

The failure to comply with the requirements of this Section shall cause the matter to be evaluated as a request to the National Privacy Commission for an advisory opinion, and for the National Privacy Commission to take such further action, as necessary. **The National Privacy Commission may waive any or all of the requirements of this Section, at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to the affected data subject.¹⁵ (Emphasis supplied)**

Just the same, Rule II, Section 2 of the NPC Circular 2021-01 provides:

SECTION 2. Exhaustion of remedies. – No complaint shall be given due course unless it has been sufficiently established and proven that:

1. the complainant has informed, in writing, the personal information controller (PIC), personal information processor (PIP), or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same; and

¹⁵ Section 4 of NPC Circular 16-04

2. the PIC, PIP, or concerned entity did not take timely or appropriate action on the claimed privacy violation or personal data breach, or there is no response from the PIC, PIP, or concerned entity within fifteen (15) calendar days from receipt of written information from the complainant.

The NPC may waive any or all of the requirements of this Section at its discretion upon (a) good cause shown, properly alleged and proved by the complainant; or (b) if the allegations in the complaint involve a serious violation or breach of the Data Privacy Act of 2012, taking into account the risk of harm to the affected data subject, including but not limited to:

- i. **when there is grave and irreparable damage which can only be prevented or mitigated by action of the NPC;**
- ii. **when the respondent cannot provide any plain, speedy or adequate remedy to the alleged violation;**
- iii. **or the action of the respondent is patently illegal. (Emphasis supplied)**

This Commission reiterates its ruling that Section 4 of the NPC Circular 16-04 was intended to avoid the undue clogging of the Commission's dockets and prevent instances that a case shall be dismissed even if there is good cause shown by the Complainant or the case involves serious violation or breach of the DPA. Further, the rule is intended to avoid instances of deciding cases based on mere technicalities. This approach in resolving issues was expounded by the Supreme Court in, *Agum v. Court of Appeals*:

"The law abhors technicalities that impede the cause of justice. The court's primary duty is to render or dispense justice. 'A litigation is not a game of technicalities.' 'Lawsuits unlike duels are not to be won by a rapier's thrust. Technicality, when it deserts its proper office as an aid to justice and becomes its great hindrance and chief enemy, deserves scant consideration from courts.' **Litigations must be decided on their merits and not on technicality.**"¹⁶ (Emphasis supplied)

In this case, there was good cause shown by the Complainant, considering the Complaint-Affidavit alleges series of acts of harassment by PXXX Corporation to force MNLCI's members to

¹⁶ Paz Reyes Agum vs. Court of Appeals, G. R. No. 137672, 31 May 2000

comply and submit their passports and ID's. Further, as already expounded in our 29 October 2020 Decision, the case involves a serious violation or breach of the DPA due to violations of the General Data Privacy Principles¹⁷ and Criteria for Lawful Processing of Personal Information and Sensitive Personal Information¹⁸. Such are enough grounds for this Commission to waive the requirement of Section 4.

Moreover, this Commission highlights that as the country's independent body mandated to implement the Data Privacy Act, the Commission is afforded with broad range of powers in implementing the legislation that was solemnly delegated to it.

Ruling on the Substantive Issues

On the Respondents' argument that there is no need to contextualize the emails and Secretary's Certificate provided that MNLCI explicitly consented the processing of personal information, the Respondents must be reminded that context is essential in determining validity of consent and cannot be brushed aside as espoused by the Respondents. This Commission emphasizes that in determining whether consent was freely given, the data subject must have a real choice where there is no risk of deception, intimidation, coercion or significant negative consequences if he or she does not consent. If the consequences of giving consent undermine the individual's freedom of choice, consent would not be free.¹⁹ The allegations of the Complainant against Respondent remain unrefuted wherein Complainant alleges that two church members were banned from entering the church and guard dogs were posted at the entrance of the building which resulted in the delay of entrance of church members for over an hour and a half. Clearly, there is already an imbalance of power between PC and MNLCI.²⁰ With this imbalance existing between the two, the supposed consent given by the church members cannot be deemed as freely given.

¹⁷ Section 11, DPA

¹⁸ Sections 12 and 13, DPA

¹⁹ National Privacy Commission. Advisory Opinion 2019-034 Re: Consent and Its Withdrawal for Employment Purposes. 02 September 2019, citing European Commission, Article 29, Data Protection Working Party, Opinion 15/2011.

The Respondents further argued that the processing of personal information was made to pursue their legitimate interest. Although protecting the safety of the tenants of the building and security of the premises is a legitimate interest, Respondents only implemented stricter security measures to Complainant's church members and not to other tenants of the building. There was no record that exhibits that church members were suspected to cause any of the security incidents mentioned by Respondents. Such fact is disproportionate to the Respondents' claim that processing of personal information was made to pursue their legitimate interest of protecting and securing the premises since it is only targeted to only a specific group of individuals, in this case, the MNLCI church members.

On the issue of award of damages, this Commission reiterates that our Decision used a clear language and had a clear directive- that nominal damages shall be awarded to each member of the church, thus:

3. AWARDS damages, in the amount of P1,000.00, **to each member of Complainant MNLCI** as of the date of filing of the Complaint Affidavit on 23 July 2019 for Respondent's unlawful collection of their sensitive personal information, pursuant to Section 16 (f) of the Data Privacy Act; and²¹ (Emphasis supplied)

The Respondents cannot insert additional requirements which was not given by the law in awarding nominal damages. Article 2221 of the New Civil Code is clear that nominal damage can be awarded in recognition of the violated legal rights of a plaintiff or complainant.²² In this case and as ruled by the Commission, the award of nominal damages to Complainant is warranted, pursuant to the Commission's findings that the Respondents unlawfully processed the data subjects' sensitive personal information and failed to observe the general privacy principle of proportionality. Hence, compliance to the Decision in awarding nominal damages to the Complainant is within the responsibility and obligation of the Respondents, which includes coordination with the Complainant to obtain the official list of MNLCI church members.

²¹ Decision dated 29 October, at p. 30

²² Republic Act No. 286, at § 2, Article 2221

In summary and as established above, the Respondents failed to present new material facts and evidence for the Commission to reconsider and/or amend its Decision.²³ The Respondents' Motion for Reconsideration is a mere reiteration of its previous arguments and submissions to the Commission.

Lastly, this Commission maintains its Decision²⁴ where the Commission: (1) finds that Respondent ACD, Respondent ACM, and the Board of Directors of PXXX Corporation, namely EPA, CAS, RCM, HABJR, and JRB, as its responsible officers, have violated Section 25(b) of the Data Privacy Act; (2) forwards this Resolution and Decision dated 29 January 2020 and a copy of the pertinent case records to the Secretary of Justice, recommending the prosecution of respondents for the crime of Unauthorized Processing under Section 25 of the Data Privacy Act, and for its further actions; (3) awards damages, in the amount of P1,000.00, to each member of Complainant MNLCI as of the date of filing of the Complaint Affidavit on 23 July 2019 for Respondent's unlawful collection of their sensitive personal information, pursuant to Section 16 (f) of the Data Privacy Act; and (4) orders the submission of proof of compliance by Respondents with abovementioned award within thirty (30) days of receipt of this Decision.

WHEREFORE, premises considered, this Commission resolves to **DENY** the Motion for Reconsideration filed by Respondents PXXX Corporation, RCM, and AD. The Decision of this Commission dated 29 October 2020 is hereby **AFFIRMED**.

SO ORDERED.

Pasay City, Philippines;
23 February 2021

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

On Official Business
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

ACLO
Counsel for the Complainant

M.C. PLO
Counsel for the Respondents

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

CCMC,

Complainant,

CID 18-K-200

*For: Violation of the
Data Privacy Act
of 2012*

-
versus-

QXXX FINANCING CO., INC.,

Respondent.

X-----X

RESOLUTION

AGUIRRE, D.P.C.;

Before the Commission are the submissions of QXXX Financing Co., Inc. in response to the Commission's Decision dated 17 January 2020. This case involves an "Early Payment Reminder" sent by Respondent via email where the names and email addresses of all one hundred thirty-six (136) recipients were visible to all the recipients.

Facts

On 17 January 2020, the Commissioner rendered a Decision on this case, thus:

"WHEREFORE, all the above premises considered, the Commission hereby **ORDERS** Respondent to submit **within thirty (30) days** from receipt of this Decision, their security incident management policy that is compliant with the guidelines stated in NPC Circular 16-03, pursuant to the undertaking in their 5 November 2018 letter to the Commission that a report to management will be made by 25 November 2018 regarding the review and recommendation of the procedures by the DPO and his team.

SO ORDERED."¹

¹ NPC Decision dated 17 January 2020.

On 16 September 2020, the Commission received QXXX's Privacy Manual.² After assessing the Privacy Manual, the Commission found that while it included a section on Security Management, it did not include the required provisions in NPC Circular No. 16-03³ that will ensure the following:

- a. Implementation of an Incident Response Procedure intended to contain a security incident or personal data breach and restore integrity to the information and communication system.
- b. Steps to be undertaken to mitigate possible harm and negative consequences to a data subject in the event of a personal data breach.

The Commission found that the submitted document only discussed in general that QXXX will recover and restore the affected data but lacked concrete steps to mitigate or contain the breach to prevent greater harm. Moreover, the Commission found that there was no discussion regarding the steps that QXXX would undertake to mitigate possible harm to data subjects.

Consequently, the Commission, through the Enforcement Division (EnD), sent an Enforcement Letter to QXXX directing it to submit a Security Incident Management Policy that augmented the identified deficiencies within fifteen (15) days from the receipt of the letter.⁴ In a letter dated 09 November 2020, which was received by the Commission on 16 November 2020, the Respondent sent its complete Security Incident Management Policy to comply with the aforementioned directive.⁵

Issue

Whether or not QXXX implemented sufficient measures to manage data privacy breach incidents

² Letter from QXXX Financing Co. Inc. dated 14 September 2020.

³ Section 4, NPC Circular No. 16-03. Personal Data Breach Management, dated 15 December 2016.

⁴ Enforcement Letter dated 22 October 2020.

⁵ Letter from QXXX Financing Co. Inc. dated 9 November 2020.

Discussion

Rule II, Section 4 of NPC Circular No. 16-03 states that personal information controllers should implement policies and procedures to manage security incidents:

SECTION 4. *Security Incident Management Policy.* A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure:

- A. Creation of a data breach response team, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach;
- B. Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident;
- C. Implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system;
- D. Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach; and
- E. Compliance with the Act, its IRR, and all related issuances by the Commission pertaining to personal data breach notification.

The Commission finds that the Data Privacy Security Incident Management Policy (SIMP) submitted by QXXX has substantially complied with the Decision dated 17 January 2020 and NPC Circular No. 16-03 on Personal Data Breach Management.

In its SIMP, QXXX outlined eight (8) steps that it will follow in cases of security incidents and data breaches.⁶ These are:

⁶ QXXX Financing Co., Inc.'s Security Incident Management Policy.

- (1) Reporting – Any person, whether connected to QXXX or not, should report an incident or breach to the QXXX DPO within two (2) hours from discovery;⁷
- (2) Categorization - A member of the Breach Response Team (BRT) shall categorize the event whether it is a security incident, a personal data breach, or non-urgent matter;⁸
- (3) Investigation and Identification – If the event is categorized as either a security incident or a personal data breach, the BRT should investigate it to discover the nature and circumstances of the incident or breach, the data processing systems involved and the persons responsible, involved and affected, as well as their contact details;⁹
- (4) Reporting and Notification – If the incident or the breach falls under the mandatory breach notification of NPC Circular No. 16-03, QXXX shall notify the Commission within seventy-two (72) hours from the discovery of the incident. Aside from notifying the Commission, QXXX shall also notify the affected data subjects upon knowledge of, or when there is reasonable belief that a personal data breach has occurred;¹⁰
- (5) Containment and eradication – The BRT shall conduct steps to stop the cause of the incident or the breach and its effects;¹¹
- (6) Recovery – The BRT shall restore the system or application to a working state and disclose details of the incident to affected users, if necessary;¹²
- (7) Feedback – The BRT shall categorize the Security Incident or Personal Data Breach based on the actions taken;¹³ and

⁷ *Id.* at 6.

⁸ *Ibid.*

⁹ *Id.* at 7.

¹⁰ *Ibid.*

¹¹ *Id.* at 8.

¹² *Id.* at 9.

¹³ *Ibid.*

- (8) Learning – The BRT should discuss the lessons learned and may document lessons to prevent similar incidents from occurring again.¹⁴

In its Mitigation Response Plan,¹⁵ QXXX enumerated specific examples of how it plans to contain an incident:

Step 5 - Containment and Eradication

The BRT shall conduct steps to stop the cause of the Security Incident or Personal Data Breach and its effects. The BRT is responsible to contain the Security Incident or Personal Data Breach so that it does not spread and cause further damage. Steps that may be taken are:

- Disconnect the affected devices from (*sic*) the internet or intranet
- Commence short-term and long-term containment strategies
- Ensure that there is a backup system to help us in the restoration process
- Update and patch the system
- Review remote access protocols
- Change user and administrative access credentials
- Secure passwords

The QXXX DPO shall address the Concern. The DPO shall facilitate all forms of resolutions by ensuring that the support provided by the QXXX BRT responsively and effectively addresses the Concern without causing new Concerns.

Step 6 – Recovery

The BRT, in coordination with relevant QXXX I.T. personnel, shall endeavor to restore the system or application to a working state and take necessary actions to recover affected records, systems and other matters affected by the Security Incident. The following tasks may be conducted:

- restoring system data to a known good state
- repairing or rebuilding the system or application that was compromised

¹⁴ *Ibid.*

¹⁵ *Id.* at 8.

- validating that the problem that caused the incident has been addressed
- communicating to users that the system is back online
- disclosing the incident to affected (*sic*) users if necessary
- taking any appropriate administrative action related to the incident¹⁶

The Commission acknowledges that these policies and procedures comply with NPC Circular No. 16-03 and can help mitigate the possible harm to a data subject. Moreover, these clear policies on security incidents will help avoid delays in notification to the Commission and the affected data subjects.

WHEREFORE, premises considered, this Commission finds that the submission of QXXX Financial Co., Inc. in response to the Decision dated 17 January 2020 is **SUFFICIENT**. This Commission considers the matter **CLOSED**.

SO ORDERED.

City of Pasay,
Philippines. 29 April
2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy
Commissioner

WE CONCUR:

¹⁶ *Ibid.*

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

CCMC
Complainant

JNB
Data Protection Officer of Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

**COMPLAINTS AND
INVESTIGATION DIVISION –
NATIONAL PRIVACY
COMMISSION**

Complainant,

-versus-

*For: Violation of
the Data Privacy
Act of 2012*

**PHILIPPINE NATIONAL POLICE
REPRESENTED BY THE CHIEF,
PNP, NATIONAL
HEADQUARTERS CAMP Crame,
QUEZON CITY**

Respondent.

X

X

RESOLUTION

AGUIRRE, D.P.C.:

Before this Commission is an application by the Complaints and Investigation Division (CID) for the issuance of a Cease-and-Desist Order (CDO) against the Philippine National Police (PNP), particularly the Calbayog-PNP, for an alleged unauthorized profiling and processing of personal information and sensitive personal information.

The Facts

On 19 March 2021, the Commission received an application from the CID for an issuance of a CDO against the PNP. It's factual narration states thus:

On 15 March 2021, the Quick Response Team of the Complaints and Investigation Division (CID) received instructions to investigate the possible data privacy violations

committed by the Calbayog-Philippine National Police (PNP) in relation to a letter requesting the list of lawyers representing Communist Terrorist Group (CTG) personalities. The letter was addressed to the Office of the Clerk of Court of the Calbayog PNP (sic) issued by FGCJ, Police Lieutenant, Chief Intel / SEU of Calbayog-PNP.

Below are the facts gathered about the matter:

On 12 March 2021, the Calbayog Journal posted on their Facebook page a photo of the Calbayog-PNP letter requesting for a list of lawyers representing the CTG personalities in court.

On the same day, news outlets such as Rappler, and ABS-CBN News online, reported that Supreme Court Spokesperson BKH said the Calbayog Regional Trial Court (RTC) received request signed by a certain PLT FGCJ, from the Calbayog City Police Station, but “no action” has been done by the said court so far. In addition, the ABS-CBN report showed that the police also attached a table, which included a “mode of neutralization,” and the lawyer’s affiliations, among others. On the other hand, MN posted the same letter on his Twitter account and reported the same. xxx¹

The CID included the subject letter-request and a table for the RTC Calbayog to fill out, with the fields “legal personality, affiliations, client (CTG personality), mode of neutralization, case filed, status.”²

The CID prays for the issuance of a Cease and Desist Order, stating thus:

The act of requesting for the names of lawyers representing suspected communist terrorist group is not part of the PNP’s mandate. It is detrimental to public interest, and the practice of the legal profession. It blatantly interferes and discriminates against lawyers for doing their professional duty. Moreover, we note that such request was made without any authority or statement of purpose and is therefore in gross disregard and violation of the rights of the data subjects involved. The letter request poses a palpable risk that can cause grave and irreparable injury to affected data subjects.

¹ Application for Cease and Desist Order In re: The Calbayog-PNP Letter Request. Dated 16 March 2021. Page 2.

² *Id.*, at page 15.

Hence, based on the foregoing, it is clear that grounds for the issuance of a cease-and-desist order are present, pursuant to Section 4 of NPC Circular No. 20-02³⁷. Said Section of NPC Circular No. 20-02 provides that the grounds for the issuance of Cease and Desist Order are the following: (A) the Adverse Party is doing, threatening or is about to do, is procuring to be done, some act or practice in violation of the DPA, its IRR, or other related issuances; (B) such act or practice is detrimental to national security or public interest, or the CDO is necessary to preserve and protect the rights of a data subject; and (C) the commission or continuance of such act or practice, unless restrained, will cause grave and irreparable injury to a data subject.³

Issue

The sole issue for this application is whether or not a Cease and Desist Order shall be issued against the PNP in relation to the letter-request made by P/Lt. FGCJ. to the Calbayog RTC.

Discussion

The NPC Circular No. 2020-02⁴ (NPC Circular 2020-02) provides the Rules for the Issuance of a Cease and Desist Order. It provides the following grounds:

Section 4. Grounds for the Issuance of Cease and Desist Order.
– No CDO shall be issued unless it is established by substantial evidence that all of the following concur:

A. the Adverse Party is doing, threatening or is about to do, is procuring to be done, some act or practice in violation of the DPA, its IRR, or other related issuances;

B. such act or practice is detrimental to national security or public interest, or the CDO is necessary to preserve and protect the rights of a data subject; and

C. the commission or continuance of such act or practice, unless restrained, will cause grave and irreparable injury to a data subject.

³ *Id.*, at Page 12.

⁴ NPC Rules On The Issuance Of Cease And Desist Orders. Dated 06 October 2020.

The grounds are stated in a cumulative manner, requiring the concurrence of each ground.

The ground that “the Adverse Party is doing, threatening or is about to do, is procuring to be done, some act or practice in violation of the DPA, its IRR, or other related issuances” is not present.

The act of processing that is subject to the application for a CDO in this case is the “unauthorized profiling and processing of personal information and sensitive personal information.”⁵

The application specifically hinged on the letter-request made by P/Lt. FGCJ to the Calbayog RTC. The material facts alleged by CID to establish the grounds for such issuance, however, indicates that the PNP is no longer “doing, threatening, or is about to do, is procuring to be done, some act or practice in violation of the DPA, its IRR, or other related issuances.”

The CID, in their application, included attachments of news articles reporting the official statement from Supreme Court Spokesperson BKH that no action has been made by the RTC on the letter-request.⁶

The CID likewise stated that P/Lt. FGCJ was ordered to be relieved from his post. It reproduced the full statement of PNP Officer-in- Charge Lt. Gen. GE with regard to this issue, stating thus:

In view of these initial findings and in consultation with our Chief PNP, Police General DMS, I have already directed the relief of Plt FGCJ as the Chief of the Intelligence Unit of the Calbayog City Police Station.

⁵ Application for Cease and Desist Order In re: The Calbayog-PNP Letter Request. Dated 16 March 2021. Page 1.

⁶ Application for Cease and Desist Order In re: The Calbayog-PNP Letter Request. Dated 16 March 2021. Pages 14, 16, 18.

We are currently checking if there were similar actions in other areas. At the same time, we are investigating to determine up to what level of police hierarchy is involved in this incident.

What is certain at this point is that the PNP top brass did not issue any order pertaining to that, and will never tolerate such unprofessional method of information-gathering.

We fully understand the sentiments of the members of the legal community and for this, I, on behalf of the men and women of the Philippine National Police, sincerely apologize for this reckless behavior.⁷

This disavowal and condemnation of the PNP of P/Lt. FG CJ's letter request, including their action of relieving him from his post, together with the fact that the Calbayog RTC refused to disclose any lawyer's name, affiliation, their clients' names, cases filed and case statuses, prevent the PNP from doing, threatening to do, or procuring to be done, some act or practice in violation of the DPA, its IRR, or other related issuances. The first ground is therefore not applicable in this case.

The ground that "such act or practice is detrimental to national security or public interest, or the CDO is necessary to preserve and protect the rights of a data subject" is present.

This second ground is based on the Data Privacy Act (DPA) and further elaborated in the Implementing Rules and Regulations (IRR) as an instance when the Commission may issue cease and desist orders. Section 9(f)(3) of the IRR states:

Section 9. *Functions.* The National Privacy Commission shall have the following functions:

f. Enforcement. The Commission shall perform all acts as may be necessary to effectively implement the Act, these Rules, and its other issuances, and to enforce its Orders, Resolutions or

⁷ *Id.*, at page 3.

Decisions, including the imposition of administrative sanctions, fines, or penalties. This includes:

xxx

3. Issuing cease and desist orders, or imposing a temporary or permanent ban on the processing of personal data, upon finding that **the processing will be detrimental to national security or public interest, or if it is necessary to preserve and protect the rights of data subjects.**⁸

It is important to consider that this ground provides for two (2) alternative conditions for its application – the first one being “such act or practice is detrimental to national security or public interest” and the second one being that “the CDO is necessary to preserve and protect the rights of a data subject.” Given the alternative nature of the conditions, the presence of either one will be sufficient for the application of this ground.

The first condition looks at the nature of the act *per se* and whether it can be considered as detrimental to national security or public interest.

The Supreme Court discussed public interest in the case of *Valmonte v. Belmonte Jr.*, stating thus:

In determining whether or not a particular information is public concern there is no rigid test which can be applied. “Public concern” like “public interest” is a term that eludes exact definition. Both terms embrace a broad spectrum of subjects which the public may want to know, either because these directly affect their lives, or simply because such matters naturally arouse the interest of an ordinary citizen. In the final analysis, **it is for the courts to determine on a case by case basis whether the matter at issue is of interest or important, as it related to or affects the public.**⁹

Notably, the CID alleges the following in their Application for the issuance of the CDO:

[T]he Calbayog-PNP did not state in their letter the purpose of having a list of lawyers who represent CTG personalities

⁸ Section 9, Implementing Rules and Regulations of the Republic Act No. 10173, known as “The Data Privacy Act of 2012.” Dated August 24, 2016.

⁹ G.R. No. 74930 (1989). Emphasis in the original.

in court but said it was “for subsequent submission to PNP higher offices.”

The PNP is mandated to prevent and investigate crimes, however, the lawyer-data subjects who are involved in this instance are not criminals nor are they involved in any criminal act, as such this request of the PNP to process their data is outside of their mandate.

Lawyers who represent their clients, whether CTG personalities or not, are merely carrying out their sworn duties as officers of the court to defend and uphold the rights of their clients. This kind of profiling of lawyers goes against the Basic Principles on the Role of Lawyers, to wit:

1. “Governments shall ensure that lawyers are able to perform all of their professional functions without intimidation, hindrance, harassment or improper interference and shall not suffer, or be threatened with, prosecution or administrative, economic or other sanctions for any action taken in accordance with recognized professional duties, standards and ethics.”
2. Lawyers shall not be identified with their clients or their clients’ causes as a result of discharging their functions

Such processing of personal data also interferes with the lawyer’s code of professional responsibility, to wit:

Rule 2.01 – “A lawyer shall not reject, except for valid reasons, the cause of the defenseless or the oppressed.”

A lawyer, by one’s oath, swears to be an instrument of justice. It is a lawyer’s duty to protect the rights and interests of their clients, whoever their clients may be. In turn, the Government must ensure that lawyers are able to perform their duties without threats and intimidation. The PNP should well be reminded of the fact, ***that lawyers are vital partners of the Government in the administration of justice, even when a lawyer’s advocacy may be adversarial to the State. But in protecting the rights of the accused, lawyers should not be identified as one with the accused.***¹⁰

¹⁰ Application for Cease and Desist Order In re: The Calbayog-PNP Letter Request. Dated 16 March 2021. Page 9. Emphasis supplied.

The Commission recognizes the destructive effect of such letter- requests not just to the legal profession but, as cited by the CID, in the Government's administration of justice. The fact that the lawyers subject to the letter-request are part of a specific class of those who represent CTG personalities in the Calbayog RTC is of no moment.

The law does not require a large number of individuals or a large scope of area to be involved for a matter to be considered public interest. The Supreme Court has even pronounced the term "public" is a "comprehensive, all-inclusive term" and said that "properly construed, it embraces everyone."¹¹

The inability of lawyers to perform their duties without threats and intimidation is a matter that directly affects the lives of the general public. This is likewise recognized by the Supreme Court which issued an official statement a few days after public reports of the letter- request:

The Supreme Court is mindful that nothing prevents it from standing by all court officers, judges and lawyers alike, as it now does in no uncertain terms. This principle is not in debate, but has remained fixed on administering justice amid a history of shifting social and political tides. Every threat to a lawyer or judge that prevents them from exercising their functions has very serious repercussions on the ideal that the rule of law must be accessible in an impartial and transparent manner to all parties. Every right guaranteed in the Constitution must be protected.

We are all too aware that everything the Court stands for must bend its arc toward ensuring that all its officers can fairly and equitably dispense their duties within the legal system, unbridled by the constant fear that such exercise may exact the highest cost. In this light, the Court condemns in the strongest sense every instance where a lawyer is threatened or killed, and where a judge is threatened and unfairly labeled. We do not and will not tolerate acts that only perverse justice, defeat the rule of law, undermine the most basic of constitutional principles, and speculate on the worth of human lives.

We acknowledge and share the legitimate concerns of the public, the profession, the Judiciary, as well as law enforcers

¹¹ Subido v. Ozaeta, G.R. No. L-1631. Feb. 27, 1948.

and public servants in general. We are aware that there are wayward elements who, in their zeal to do what is necessary, would simply brush aside the limitations in our law as mere obstacles. This should never be countenanced, for it is only in the enjoyment of our inalienable and indivisible rights that our freedoms become meaningful.¹²

Finding that the act of P/Lt. FG CJ, whether or not abated, was “detrimental to national security or public interest”, the Commission need not discuss the alternative ground requiring that “the CDO is necessary to preserve and protect the rights of a data subject.” The second ground is therefore present in this case.

The ground that “the commission or continuance of such act or practice, unless restrained, will cause grave and irreparable injury to a data subject” is not present.

This ground pertains to a grave and irreparable injury that a data subject stands to incur if the complained act is not restrained.

The relief of P/Lt. FG CJ from his post and express disavowal by the PNP following the incident are material facts that already demonstrate the desistance of processing. The CID has likewise established in their Application and its attachments that the Calbayog RTC did not disclose any lawyer’s personal data, despite the request. The Supreme Court¹³ has also renounced any disclosure or such other act that may jeopardize its judges and lawyers, who are considered officers of the Court. Their official statement declared:

We encourage lawyers who have experienced harassment, or whose clients have experienced threats or harassment, to file the necessary motions in pending cases, petitions, or complaints in order that our courts may receive the evidence, determine the facts, and, based on the issues framed, provide

¹² Memorandum to Atty. BKH, Chief, Public Information Office, Supreme Court. Re: Instructions to Read the Statement of the Members of the Court En Banc Responding to Calls for Action Regarding the Killing of Lawyers and Threats to Judges. Dated 23 March 2021.

¹³ CONST. art. VIII, §6. The Supreme Court shall have administrative supervision over all courts and the personnel thereof.

the relevant reliefs for each case. General invocations of policy will be better supported by experience with the system. In so doing, we can assess what revision or institutional change is necessary to effectively and efficiently further protect our basic rights.

The Supreme Court has always operated within institutional restraints, but it is far from resigned to spectate as clear breaches of constitutional rights are carried out beyond its halls. We remain conscious of our role to ensure that the rule of law is resilient and effective in a just, fair, and timely manner. The Bench and the Bar, as well as the public, can rest assured that we will continue to unflinchingly comply with our constitutional duty to act decisively when it is clear that injustices are done. xxx¹⁴

These facts, when put together, show that the act sought to be restrained with the issuance of the CDO has already ceased to exist as a result of its invalidation by the PNP itself and the subsequent actions of the Calbayog RTC and the Supreme Court. Taking these material facts into consideration, the Commission finds that there is no grave and irreparable injury to be incurred by the data subjects if the CDO will not be issued.

The third ground, therefore, does not apply in this case.

Absent the first and third grounds required under Section 4 of NPC Circular No. 2020-02, the application for a CDO against the PNP must be denied.

WHEREFORE, all these premises considered, this Commission hereby **DENIES** the application by the Complaints and Investigation Division for a Cease and Desist Order against the Philippine National Police.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against the Respondents before any other forum or tribunal, if any.

SO ORDERED.

¹⁴ Memorandum to Atty. BKH, Chief, Public Information Office, Supreme Court. Re: Instructions to Read the Statement of the Members of the Court En Banc Responding to Calls for Action Regarding the Killing of Lawyers and Threats to Judges. Dated 23 March 2021.

Pasay City, Philippines;
25 March 2021.

(sgd)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

(sgd)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(sgd)
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION

AGUIRRE, D.P.C.:

This Resolution refers to the request for exemption from data subject notification filed by the National Privacy Commission (“PIC”) dated 07 August 2020, involving a data breach incident affecting one (1) data subject caused by sending a case assignment to a wrong e-mail address.¹

The Facts

The Complaints and Investigation Division (CID) of the PIC hired Case Decongestion Officers (CDOs) in its effort to declog its dockets. At the time of the initial case assignments, the CDOs were not yet provided with the Commission-issued (@privacy.gov.ph) e-mail addresses. However, in order to ensure that the CDOs start their work after signing of their contracts, copies of a certain case docket containing the complaint and evaluation form were sent to their personal e-mail addresses.²

On 03 August 2020, the supervising lawyer sent an e-mail to pa@gmail.com, the e-mail address registered under the name of the concerned CDO, containing PDF copies of the complaints- assisted form, complaint evaluation, briefing documents for CDOs and word documents, cover memorandum guide, summary sheet guide, and fact-finding report guide.³

On 04 August 2020, the breach incident was discovered when the concerned CDO informed the CID that he did not receive the subject e-mail and inquired if the same was sent to

¹ Confidentiality Breach dated August 7, 2020.

² *Ibid.*, at p. 2.

³ *Ibid.*, at p. 2.

pga@gmail.com. In an excel file containing the names and email addresses of CDOs, the e-mail address indicated under the name of the concerned CDO is pa@gmail.com instead of pga@gmail.com, the one indicated in his Personal Data Sheet (PDS).⁴ It was then realized that the subject e-mail was sent to the wrong e-mail address.

On the same day, the supervising lawyer recalled the e-mail sent to pa@gmail.com but as of the writing of the Initial Report, no notification has been received from Outlook whether the recall was successful. It was also noted by the PIC that the recall function of Outlook will only work if the recipient has not yet opened the e-mail. The supervising lawyer then sent a notification of the incident to the CID's Officer-in-Charge (OIC).⁵

On 05 August 2020, the OIC met with the Legal and Enforcement Office (LEO) personnel to determine what actions they will take on the breach incident.⁶

On 08 August 2020, the PIC submitted an Initial Report with the subject "Confidentiality Breach dated August 06, 2020 for sending case assignment to wrong email address" stating that one (1) data subject is affected, the complainant in the subject case file. The sensitive personal information involved are the TIN ID No. and the date of issuance of the TIN. Other information of the complainant were also involved that may be used to enable identity fraud, namely, first name, middle initial, last name, home address, e-mail address, mobile number, and signature.⁷

The PIC has taken the following measures to address the breach and actions to secure or recover the personal data that were compromised:

- (1) Activation of the recall function of Outlook; and
- (2) Sending of letter to the e-mail address pa@gmail.com to ask him to delete the e-mail and refrain from sharing its contents to anyone.⁸

⁴ *Ibid.*, at p. 2.

⁵ *Ibid.*, at p. 2.

⁶ *Ibid.*, at p. 2.

⁷ *Ibid.*, at p. 3.

⁸ *Ibid.*, at p. 3.

Furthermore, the PIC has performed or proposed the following actions and measures to mitigate possible harm or negative consequences, limit the damage or distress to those affected by the incident, and prevent a recurrence of the incident:

- (1) To use only Commission-issued (@privacy.gov.ph) e-mail addresses in sending case assignments containing the case files to CDOs;
- (2) In case of non-availability of Commission-issued e-mail addresses, to confirm and verify with the CDOs their personal e-mail addresses to be used in receiving case assignments with attached case files;
- (3) Double check the sent e-mails to CDOs to fully determine that it was only that of the concerned CDO that was mistakenly sent; and
- (4) Remind the employees of CID, especially those in charge of collecting the e-mail addresses of the CDOs to double check their personal e-mail addresses and other contact information they have provided.⁹

Citing Section 19 of NPC Circular 16-03,¹⁰ the PIC requests to be exempted from notifying the data subject considering the personal information involved, the reasonable security measures implemented to ensure the protection of the data subject's personal information, and the notification may only result to unnecessary stress to the data subject. The PIC also claims that the actions it has taken will reduce the risk of harm or that the negative consequence to the data subject will not materialize. In the event of identity fraud committed against the data subject, the PIC also stated that it can be ascertained that it originated from the owner of the e-mail address pa@gmail.com.¹¹

Discussion

The Commission resolves to deny the request of the PIC for exemption from data subject notification.

Under Section 11 of NPC Circular No. 16-03,¹² notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

⁹ *Ibid.*, at pp. 3-4.

¹⁰ Personal Data Breach Management, 15 December 2016.

¹¹ *Ibid.*, at p. 4.

¹² *Supra* note 10.

- A. **The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.** For this purpose, “other information” shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, **TIN number; or other similar information**, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
- B. **There is reason to believe that the information may have been acquired by an unauthorized person;** and
- C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a **real risk of serious harm to any affected data subject.**¹³

In this case, the sensitive personal information involved is the TIN ID No. as well as its date of issuance. Other personal information of the data subject are also involved, namely, the first name, middle initial, last name, home address, e-mail address, mobile number, and signature. These are personal information that may be used to enable identity fraud. As these personal information were included in the subject e-mail sent to an unintended recipient and that the recall function was not found to be successful, there is already reason to believe that the information may have been acquired by an unauthorized person and such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

The PIC is therefore obliged to notify the affected data subject of the breach incident in accordance with Section 18(A) of the same Circular, which provides that:

The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. **It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.** It may be supplemented with additional information at a later stage on the basis of further investigation.¹⁴

¹³ Emphasis supplied.

Instead of notifying the data subject, however, the PIC requested for an exemption from notification requirements under Section 19 of the same Circular which provides that:

The following additional factors shall be considered in determining whether the Commission may exempt a personal information controller from notification:

- A. Security measures that have been implemented and applied to the personal data at the time the personal data breach was reasonably believed to have occurred, **including measures that would prevent use of the personal data by any person not authorized to access it;**
- B. Subsequent measures that have been taken by the personal information controller or personal information processor to **ensure that the risk of harm or negative consequence to the data subjects will not materialize;**
- C. Age or legal capacity of affected data subjects: *Provided*, that in the case of minors or other individuals without legal capacity, notification may be done through their legal representatives.

In evaluating if notification is unwarranted, the Commission may take into account the compliance by the personal information controller with the law and existence of good faith in the acquisition of personal data.¹⁵

While the PIC recalled the e-mail sent to the wrong e-mail address, no notification was however received from Outlook to show that the recall was successful. In fact, the PIC even noted that the recall function of Outlook will only work if the recipient has not yet opened the e-mail. Considering that no such notification from Outlook was received, it cannot therefore be ascertained whether such measure taken by the PIC will prevent the use of the personal data by the unintended recipient of the subject e-mail – a person who is not authorized to access it.

Moreover, while one of the measures taken by the PIC to address the breach was sending a letter to the e-mail address of the unintended recipient asking him to delete the subject e-mail and refrain from sharing its contents, there is nothing on record to show that the unintended recipient replied and agreed to such request. Given these, there is no assurance that the risk of harm or negative consequence to the affected data subject will not materialize.

¹⁵ Emphasis supplied.

Lastly, the assertion of the PIC that the notification may only result in unnecessary stress to the data subject is unsubstantiated. The personal information involved in the incident contains sensitive personal information and those that can enable identity fraud. Despite this, the security measures it implemented are prospective and does not protect the data subject from the risk he was already exposed to. Merely stating the grounds for exemption without any justification is not sufficient.

In view of the foregoing, the PIC cannot therefore rely on Section 19 of NPC Circular 16-03 to be exempted from notifying the data subject on the data breach incident. It is worth noting that under Section 18(A) of the that Circular, it provides that the notification shall be undertaken in such a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. If the PIC will be exempted from the required notification, the affected data subject will not be able to take such the necessary precautions or measures to protect himself from the possible adverse effects of the breach. This is all the more true considering that the security measures undertaken by the PIC are inadequate to protect the data subject from the unauthorized use of his exposed data.

WHEREFORE, premises considered, the request for exemption from data subject notification filed by the National Privacy Commission is hereby **DENIED**.

The National Privacy Commission is **ORDERED** to notify the affected data subject of the breach incident in accordance with the provisions of NPC Circular 16-03 and to **SUBMIT** proof of compliance thereto within fifteen (15) days of receipt of this Resolution.

SO ORDERED.

Pasay City, Philippines;
20 August 2020.

(sgd)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

(sgd)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(sgd)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JRYR
Data Protection Officer
National Privacy Commission

**COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION**
GENERAL RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION

AGUIRRE, D.P.C.:

This Resolution refers to the Proof of Compliance¹ submitted by Batangas Bay Carriers, Inc. (Batangas Bay), a subsidiary of Magsaysay Shipping & Logistics, to this Commission's Order² for it to notify the affected data subjects of the breach incident in accordance with the provisions of NPC Circular 16-03 and to submit proof of compliance thereto, involving a personal data breach caused by a ransomware attack.

The Facts

On 21 September 2020, this Commission issued a Resolution³ with the following dispositive portion, to wit:

WHEREFORE, premises considered, the request for Postponement of Notification to Data Subjects filed by Batangas Bay Carriers, Inc. is hereby **DENIED**.

Batangas Bay Carriers, Inc. is **ORDERED** to notify the affected data subjects of the breach incident in accordance with the provisions of NPC Circular 16-03 and to **SUBMIT** proof of compliance thereto **within fifteen (15) days** from receipt of this Resolution.

On 09 December 2020, Batangas Bay submitted its proof of compliance⁴ to this Commission showing that it has sent the required notification to affected data subjects.

The notification contains the nature of the breach, personal data possibly involved, measures taken to address the breach and to reduce its harm or negative consequences, and the names of the

¹ Notification to Data Subjects on temporary availability breach due to ransomware affecting Payroll Database dated 02 December 2020.

² Resolution dated 21 September 2020.

³ *Ibid*.

⁴ *Supra* note 1.

Data Protection Officer (DPO) and Process Owner stating that if the affected data subjects should require further information, they can be contacted.⁵

Discussion

This Commission finds the proof of compliance submitted by Batangas Bay insufficient for this Commission's Order to submit proof of compliance that it has notified the affected data subjects of the breach incident.

Section 18(A) of NPC Circular No. 16-03 provides that:

The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. **It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.** It may be supplemented with additional information at a later stage on the basis of further investigation.⁶

Moreover, Section 18(D) of same Circular provides that:

Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. **The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach:** *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the personal information

⁵ *Ibid.*

⁶ Emphasis supplied.

controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.⁷

It is noteworthy that the avowed purpose of the required notification to data subjects of a breach incident is for them to take the necessary precautions or other measures to protect themselves against possible effects of the breach. Moreover, personal information controllers (PICs) are required to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach. It therefore follows that PICs should guarantee that the notification they sent to data subjects has been received. Otherwise, it defeats the very purpose of notification of data subjects.

In this case, Batangas Bay merely submitted to this Commission its proof that it has sent the notification to its affected data subjects. There was, however, no showing that said notification has been received by the data subjects. Notably, the initial report also estimated more than one hundred (100) affected data subjects. However, in its instant submission, the e-mail addresses are far less than one hundred (100).

In view of the foregoing, Sections 18(A) and 18(D) of NPC Circular 16-03 have not been complied with by Batangas Bay. Hence, this Commission finds its proof of compliance to the notification of data subjects insufficient.

This Commission also brings to the attention of Batangas Bay that it has failed to submit its Full Breach Report. Section 17(C) of same Circular provides that:

There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. **The full report of the personal data breach must be submitted within five (5) days**, unless the personal information controller is granted additional time by the Commission to comply.⁸

⁷ Emphasis supplied.

⁸ Emphasis supplied.

The submission of a Full Breach Report is a different requirement that Batangas Bay should have complied with accordingly. Notification of the Commission and Notification of Data Subjects are two (2) different and separate requirements under Sections 17(C) and 18(A) of NPC Circular No. 16-03, respectively, that the PICs should promptly comply with.

WHEREFORE, premises considered, Batangas Bay Carriers, Inc. is hereby ordered, **within five (5) days from receipt of this Resolution**, to:

- (1) **SUBMIT** confirmation logs or other proof of receipt in compliance to the Notification of the Data Subjects;
- (2) **SHOW CAUSE** in writing why it should not be held liable for failure to submit a Full Report within the required period and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission, and
- (3) **SUBMIT** its Full Breach Report.

SO ORDERED.

Pasay City, Philippines;
17 December 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

CRD
Data Protection Officer

**COMPLIANCE AND MONITORING DIVISION ENFORCEMENT
DIVISION**
GENERAL RECORDS UNIT
National Privacy Commission

X-----X

RESOLUTION

For Resolution of the Commission is the request of Bombardier Transportation (Shared Services) Philippines, Inc. (Bombardier) for assistance and/or investigation of a suspected personal data breach which allegedly compromised some of its data.

Facts

On 23 April 2021, Bombardier allegedly received a notification about a data exposure.¹ According to an external report from Alstom's data leakage monitoring supplier, fourteen (14) documents from Bombardier Transportation Cebu / Philippines have been exposed via an unprotected FTP server.²

On 29 April 2021, an employee from the Human Resources department of Bombardier reported a suspected personal data breach. According to the Incident Report, a laptop used to send files was allegedly infected with Malware or Trojan virus.³ The file sent was captured in the IP address block for DDT Konstract Inc. Compromised data included the name, age, birthdate, gender, status, and insurance details such as medical insurance coverage of thirteen (13) employees and nine (9) of their dependents.⁴

¹ "Form for Reporting a Suspected Personal Data Breach" dated 29 April 2021, hereinafter referred to as the "Incident Report," p. 2

² *Ibid.* at p. 3.

³ *Ibid.* at p. 1.

⁴ *Ibid.* at p. 2.

On 30 April 2021, the Commission received an email from Bombardier requesting for “assistance/investigation on a suspected personal data breach due to a computer virus compromising some Alstom data.”⁵

In the same email, Bombardier stated that it implemented the following as part of its remediation measures:

- 1) Even though DDT Konstract is not a company supplier, their IS & Risk compliance Team are now in contact with this supplier to cease processing or forwarding such data accessed/received and delete all the data received.
- 2) PIC is asked to shut down laptop used in sending the files while investigation is going on.⁶

On 11 May 2021, Bombardier submitted proof of notification to five (5) data subjects and their dependents.⁷

Discussion

The Commission resolves to deny the request of Bombardier for assistance and/or investigation.

The responsibility of the PIC to investigate a security incident or a personal data breach follows the Accountability Principle provided in the Data Privacy Act:

Section 21. Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

In the exercise of its rule-making power and to flesh out the provision above, the Commission issued NPC Circular No. 16-03 which

⁵ Email from Bombardier dated 30 April 2021.

⁶ “Form for Reporting a Suspected Personal Data Breach” dated 29 April 2021, hereinafter referred to as the “Incident Report.”

⁷ Notification and Confirmation emails to five (5) affected data subjects submitted on 11 May 2021.

recommends, among others, the establishment of policies and procedures by PICs for the conduct of investigations and the full assessment and evaluation of a security incident or a personal data breach.

In case of a security incident or a personal data breach, a PIC is expected to conduct an investigation as part of its policies and procedures. Section 8 of NPC Circular No. 16-03 provides that:

SECTION 8. Policies and Procedures. The personal information controller or personal information processor shall implement policies and procedures for guidance of its data breach response team and other personnel in the event of a security incident. These may include:

- A. A procedure for the timely discovery of security incidents, including the identification of person or persons responsible for regular monitoring and evaluation of security incidents;
- B. Clear reporting lines in the event of a possible personal data breach, including the identification of a person responsible for setting in motion the incident response procedure, and who shall be immediately contacted in the event of a possible or confirmed personal data breach;
- C. Conduct of a preliminary assessment for purpose of:
 - 1. Assessing, as far as practicable, the nature and scope of the personal data breach and the immediate damage
 - 2. Determining the need for notification of law enforcement or external expertise; and
 - 3. Implementing immediate measures necessary to secure any evidence, contain the security incident and restore integrity to the information and communications system;
- D. Evaluation of the security incident or personal data breach as to its nature, extent and cause, the adequacy of safeguards in place, immediate and long-term damage, impact of the breach, and its potential harm and negative consequences to affected data subjects;
- E. Procedures for contacting law enforcement in case the security incident or personal data breach involves possible commission of criminal acts;

F. Conduct of investigations that will evaluate fully the security incident or personal data breach;

- G. Procedures for notifying the Commission and data subjects when the breach is subject to notification requirements, in the case of personal information controllers, and procedures for notifying personal information controllers in accordance with a contract or agreement, in the case of personal information processors; and
- H. Policies and procedures for mitigating the possible harm and negative consequences to a data subject in the event of a personal data breach. The personal information controller must be ready to provide assistance to data subjects whose personal data may have been compromised.⁸

The PIC, upon knowledge of or when there is reasonable belief that a personal data breach requiring notification has occurred, is required to notify the Commission and the affected data subjects within seventy- two (72) hours.⁹

SECTION 17. *Notification of the Commission.* The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:

- A. ***When Notification Should be Done.*** **The Commission shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.**

XXX

SECTION 18. *Notification of Data Subjects.* The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:

- A. ***When should notification be done.*** **The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.** The notification may be made on the basis of

⁸ Section 8, NPC Circular No. 16-03, "Personal Data Breach Management."

⁹ Sections 17(A) and 18(A), NPC Circular No. 16-03.

available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.

Aside from the initial notification, the PIC should submit a full breach report in accordance with the requirements of NPC Circular No. 16-03:

SECTION 17. Notification of the Commission. The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:

xxx

- C. There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. **The full report of the personal data breach must be submitted within five (5) days,** unless the personal information controller is granted additional time by the Commission to comply.

- D. *Content of Notification.* The notification shall include, but not be limited to:
 - 1. Nature of the Breach
 - a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
 - b. a chronology of the events leading up to the loss of control over the personal data;
 - c. approximate number of data subjects or records involved;
 - d. description or nature of the personal data breach;
 - e. description of the likely consequences of the personal data breach; and
 - f. name and contact details of the data protection officer or any other accountable persons.

 - 2. Personal Data Possibly Involved
 - a. description of sensitive personal information involved; and

- b. description of other information involved that may be used to enable identity fraud.
- 3. Measures Taken to Address the Breach
 - a. description of the measures taken or proposed to be taken to address the breach;
 - b. actions being taken to secure or recover the personal data that were compromised;
 - c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
 - d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
 - e. the measures being taken to prevent a recurrence of the incident.

The Commission reserves the right to require additional information, if necessary.

- E. *Form.* Notification shall be in the form of a report, whether written or electronic, containing the required contents of notification: *Provided*, that the report shall also include the name and contact details of the data protection officer and a designated representative of the personal information controller: *Provided further*, that, where applicable, the manner of notification of the data subjects shall also be included in the report. Where notification is transmitted by electronic mail, the personal information controller shall ensure the secure transmission thereof. Upon receipt of the notification, the Commission shall send a confirmation to the personal information controller. A report is not deemed filed without such confirmation. Where the notification is through a written report, the received copy retained by the personal information controller shall constitute proof of such confirmation.¹⁰

A PIC should have processes and procedures in place to prevent security incidents and personal data breaches. The DPA and its issuances provide that a PIC should have protocols for investigating a breach, notification of the Commission and the affected data subjects, and for implementation of remediation measures to address the situation and to prevent the incident from recurring.

¹⁰ Section 17(C), (D) and (E), NPC Circular No. 16-03.

The Commission notes from Bombardier's request that it has not even conducted its own investigation and wants to merely rely on the Commission to conduct it for them. The Commission stresses the responsibility of a PIC to conduct its own investigation on any security incident or personal data breach in their systems, its responsibility to notify all the affected data subjects and its responsibility to submit a Full Breach Report within the time prescribed in NPC Circular No. 16-

03. As of this date, Bombardier has neither submitted its full breach report nor requested for an extension of time to file the same. Moreover, from the documents submitted, only five (5) of the thirteen

(13) affected employees have been notified of the incident.

WHEREFORE, all premises considered, the Commission hereby **DENIES** the request of Bombardier Transportation (Shared Services) Philippines, Inc. for assistance and investigation and hereby **ORDERS** Bombardier to **NOTIFY** the affected data subjects, and to **SUBMIT** the following **within fifteen (15) days** from receipt of this Resolution:

1. Privacy Policy, particularly its policies and processes relating to breach response;
2. A Full Breach Report; and
3. Proof of notification to the eight (8) remaining affected data subjects.

SO ORDERED.

City of Pasay, Philippines;
01 June 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy
Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
*Deputy Privacy
Commissioner*

COPY FURNISHED:

MDC

HR Business Partner – SSC Cebu
Bombardier Transportation (Shared Services)
Philippines, Inc. (Alstom)

**COMPLIANCE AND MONITORING DIVISION GENERAL
RECORDS UNIT**
National Privacy Commission

A photograph of a modern, minimalist building with a concrete facade. The building features a large, dark rectangular cutout in its upper section. The entire image is overlaid with a semi-transparent red filter. In the foreground, there is a low concrete wall and some sparse vegetation. The sky is visible at the top, showing some clouds.

CIRCULARS

NPC Circular No. 2022-01

Date : 08 August 2022

Subject : GUIDELINES ON ADMINISTRATIVE FINES

WHEREAS, it is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth;

WHEREAS, the National Privacy Commission (Commission) was created under Republic Act No. (R.A.) 10173, otherwise known as the “Data Privacy Act of 2012” (DPA), in order to discharge the duty of the State to protect individual personal information in information and communications systems in the government and the private sector;

WHEREAS, the Commission has the express mandate under R.A. 10173 and its Implementing Rules and Regulations (IRR) to: (1) ensure compliance with the provisions of R.A. 10173; (2) receive complaints, institute investigations, and adjudicate on matters affecting any personal information; (3) compel any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy; and (4) generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection;

WHEREAS, the Commission shall perform all acts as may be necessary to implement the DPA, its IRR, and its issuances, and to enforce its Orders, Resolutions, or Decisions, including the imposition of administrative sanctions, fines, or penalties; **WHEREAS**, the Commission encourages Personal Information Controllers (PICs) and Personal Information Processors (PIPs) to promote organizational accountability by initiating measures to enhance their compliance with the DPA to protect the rights of their data subjects;

WHEREAS, the Commission recognizes that it is necessary for public interest to impose administrative fines that are proportionate and dissuasive for the effective exercise of its mandate;

WHEREFORE, in consideration of these premises, the Commission hereby issues this Circular fixing the amount of administrative fines to be imposed for infractions of R.A. 10173, its IRR, and other issuances of the Commission;

Section 1. Scope. This Circular is applicable to PICs and PIPs as defined in the DPA.

Section 2. Administrative Fines. Any PIC or PIP who shall violate the following provisions of R.A. 10173, its IRR, and the issuances of the Commission shall be liable for an administrative fine for each infraction. The amount of the fine for each infraction shall fall within the ranges identified below and shall be determined in accordance with the factors enumerated in Section 3. In any case, the total imposable fine for a single act of a PIC or PIP, whether resulting in single or multiple infractions, shall not exceed Five Million Pesos (Php 5,000,000.00).

GRAVE INFRACTIONS
<p>Any natural or juridical person processing personal data that infringes on the following provisions and implementing issuances of the Commission shall be subject to administrative fines of 0.5% to 3% of the annual gross income of the immediately preceding year when the infraction occurred:</p> <p>a. For each infraction of any of the general privacy principles in the processing of personal data pursuant to Section 11 of the DPA, where the total number of affected data subjects exceeds one thousand (1,001 or more);</p> <p>b. For each infraction of any of the data subject rights pursuant to Section 16 of the DPA, where the total number of affected data subjects exceeds one thousand (1,001 or more); or</p> <p>c. Any repetition of the same infraction penalized under this Circular, regardless of the classification as Major Infraction</p>
MAJOR INFRACTIONS
<p>Any natural or juridical person processing personal data that infringes on the following provisions and implementing issuances of the Commission shall be subject to administrative fines of 0.25% to 2% of the annual gross income of the immediately preceding year when the infraction occurred:</p>

- a. For each infraction of any of the general privacy principles in the processing of personal data pursuant to Section 11 of the DPA, where the total number of affected data subjects is one thousand or below (1-1,000);
- b. For each infraction of any of the data subject rights pursuant to Section 16 of the DPA, where the total number of affected data subjects is one thousand or below (1-1,000);
- c. Any failure by a PIC to implement reasonable and appropriate measures to protect the security of personal information pursuant to Section 20 (a), (b), (c), or (e) of the DPA;
- d. Any failure by a PIC to ensure that third parties processing personal information on its behalf shall implement security measures pursuant to Section 20 (c) or (d) of the DPA; or
- e. Any failure by a PIC to notify the Commission and affected data subjects of personal data breaches pursuant to Section 20 (f) of the DPA, unless otherwise punishable by Section 30 of the DPA.

OTHER FRACTIONS

a. Any natural or juridical person processing personal data that commits any of the omissions provided hereunder shall be subject to an administrative fine of not less than Fifty Thousand Pesos (Php 50,000) but not exceeding Two Hundred Thousand Pesos (Php 200,000):

- i. The failure to register the true identity or contact details of the PIC, the data processing system, or information on automated decision making, pursuant to Section 7(a), Section 16, and Section 24 of the DPA and its corresponding implementing issuances; or
- ii. The failure to provide updated information as to the identity or contact details of the PIC, the data processing system, or information on automated decision making, pursuant to Section 7(a), Section 16, and Section 24 of the DPA and its corresponding implementing issuances.

b. Any natural or juridical person processing personal data that fails to comply with any Order, Resolution, or Decision of the Commission, or of any of its duly authorized officers, pursuant to Section 7 of the DPA and its corresponding implementing issuances, shall be subject to an administrative fine not exceeding Fifty Thousand Pesos (Php 50,000).

The fine to be imposed as a result of this infraction shall be in addition to the fine imposed for the original infraction subject of the Order, Resolution, or Decision of the Commission.

(e.g., If the Order, Resolution, or Decision imposes a fine that pertains to the implementation of security measures, a maximum of Php 50,000 shall be added to the fine for that infraction.)

This Circular shall also apply to infractions to be provided in future issuances of the Commission. In those instances, the range of applicable fines shall be set out in such issuance.

Section 3. Factors Affecting Fines. The Commission shall consider the following factors in determining the amount of the fine within the range provided in Section 2:

- a. Whether the infraction occurred due to negligence or through intentional infraction on the part of the PIC or PIP;
- b. Whether the infraction resulted in damage to the data subject, taking into account the degree of damage to the data subject, if any;
- c. The nature or duration of the infraction, in relation to the nature, scope, and purpose of the processing;
- d. The action or measure taken prior to the infraction to protect the personal data being processed as well as the rights of the data subject under Section 16 of the DPA;
- e. Any previous infractions determined by the Commission as contained in its Orders, Resolutions or Decisions, whether these infractions have led to the imposition of fines, and the length of time that has passed since those infractions;
- f. The categories of personal data affected;
- g. The manner in which the PIC or PIP discovered the infraction, and whether it informed the Commission;
- h. Any mitigating action adopted by the PIC or PIP to reduce the harm to the data subject; and
- i. Any other aggravating or mitigating circumstances as appreciated by the Commission, including financial benefits incurred or losses avoided by the PIC or PIP.

For the purpose of ascertaining the annual gross income of the PIC or PIP that committed the infraction, the Commission may evaluate and require the submission of the PIC's or PIP's audited financial statements filed with the appropriate tax authorities for the immediately preceding year when the infraction occurred, the last regularly prepared balance sheet or annual statement of income and expenses, and such other financial documents as may be deemed relevant and appropriate.

In cases where a PIC or PIP has not been operating for more than one year, the base to be used for the computation of the administrative fine shall be its gross income at the time the infraction was committed.

Section 4. Due Process. The administrative fine shall only be imposed after notice and hearing are afforded to the PICs or PIPs, in accordance with the NPC Rules of Procedure.

In case the PIC or PIP fails to appear or submit its comment or pleading, despite due notice, the Commission shall decide on the alleged infraction based on the evidence on record.

If the complaint alleges a violation of the DPA that incurs criminal liability, but the facts proven only constitute one or some of the infractions subject to administrative fines, the PIC or PIP shall be fined for the infraction proven, provided it is included in the violation alleged.

A violation charged includes the infraction proven when some of the essential elements of the former, as alleged in the complaint, constitute the latter.

A PIC or PIP may be held liable for an infraction, even if it is different from the infraction impleaded, provided that (1) the essential requisites of the infraction for which the PIC or PIP is found liable are alleged in the complaint, and (2) such infraction is proven based on substantial evidence.

Section 5. Appeal. The Decision or Resolution of the Commission shall be immediately executory unless otherwise restrained by the Court of Appeals or the Supreme Court.

Section 6. Posting of Bond on Imposed Administrative Fines. In any or all actions assailing the Decisions or Resolutions of the Commission pertaining to the administrative fine imposed, a cash or surety bond equivalent to the total amount of fine imposed shall be posted, exclusive of the damages, attorney's fees, and other monetary awards, upon such filing of any action with the appropriate courts. Non-posting of a cash or surety bond shall result in the immediate execution of the administrative fine imposed.

The cash or surety bond shall be valid and effective from the date of deposit or posting until the case is finally decided, resolved, or terminated, or the administrative fine imposed is satisfied. In case of a surety bond, the PIC or PIP must (1) post the bond through a bonding company included in the latest list of bonding companies accredited by the Supreme Court for Civil Cases and Special Proceedings, and (2) comply with the requirements of such bonding company.

No motion to reduce bond shall be entertained by the Commission.

Section 7. Refusal to Comply. In case of refusal to pay the adjudged administrative fine under this Circular, the PIC or PIP may be subject to a Cease and Desist Order (CDO), other processes or reliefs as the Commission may be authorized to initiate pursuant to Section 7 of the DPA, and appropriate contempt proceedings under the Rules of Court.

Notwithstanding the provisions of NPC Circular No. 20-02 or the Rules on the Issuance of Cease and Desist Orders, the failure to comply with the Order, Resolution, or Decision of the Commission may, after notice and hearing, result in the issuance of a CDO.

Section 8. Periodic Review and Modification. This Circular may be modified, amended, supplemented, or repealed as may be deemed necessary and proper by the Commission.

Section 9. Separability Clause. In the event that any provision of this Circular be declared invalid or unconstitutional, the remaining provisions shall remain effective and in full force and effect.

Section 10. Applicability Clause. These rules apply to PICs and PIPs for the above infractions prospectively. All issuances inconsistent with the provisions of this Circular shall be deemed repealed, amended, or modified accordingly.

Section 11. Effectivity. – This Circular shall take effect fifteen (15) days following its publication in a newspaper of general circulation.

Approved:

Sgd.
ATTY. JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
ATTY. LEANDRO ANGELO Y.
AGUIRRE
Deputy Privacy Commissioner

Sgd.
ATTY. DUG CHRISTOPER B.
MAH
Deputy Privacy Commissioner

NPC Circular No. 2022-02

Date : 01 December 2022

Subject : AMENDING CERTAIN PROVISIONS OF NPC CIRCULAR NO. 20-01 ON THE GUIDELINES ON THE PROCESSING OF PERSONAL DATA FOR LOAN-RELATED TRANSACTIONS

SECTION 1. Objective. — This Circular aims to expound on NPC Circular No. 20-01 to respond to exigencies in the processing of personal data for loan-related transactions by lending and financing companies and other persons acting as such.

SECTION 2. Amendments. — The following provisions of NPC Circular No. 20-01 are hereby amended as stated below:

A. In Section 3(A), fifth and sixth paragraphs shall be inserted to read:

5. LCs, FCs and other persons acting as such shall obtain consent for the processing of personal data at the point where the personal data is necessary. They should provide just-in-time notices before obtaining the consent of the data subjects.

A just-in-time notice provides data subjects with information on how a particular piece of information he or she is asked to provide will be processed. This information is provided at the point in time where the LCs, FCs, or other persons acting as such is about to process or processes such personal data of the data subject.

6. The most appropriate format in providing details of processing to borrowers, as required by Section 16 (b) of the DPA and Section 34 (a) (2) of its Implementing Rules and Regulations (IRR), shall be the format which is aligned with the business processes of the LCs, FCs, or other persons acting as such, with utmost consideration to the accessibility of the information and convenience of the borrowers [e.g., if the loan transaction is being facilitated through a mobile application, the aforementioned information, shall be readily accessible and easily located within the mobile application].

B. Section 3 (D) is hereby amended to read as follows:

D. Where online applications are used for loan processing activities, LCs, FCs, or other persons acting as such shall be prohibited from conducting unnecessary processing including requiring unnecessary permissions that involve personal and sensitive personal information.

1. Mobile applications shall only require data subjects to provide access to personal data through permissions or protected resources when suitable, necessary, and not excessive to the legitimate purposes provided in Section 3 (B) (1) and Section 3 (C) of this Circular, and debt collection, subject to the limitations provided by law and in accordance with applicable provisions of law.

Processing of personal data from application permissions, such as but not limited to accessing contact lists and cameras of data subjects, should only commence at the point where the information is necessary for the purposes provided for in the preceding paragraph.

In cases where the data subjects provide information that was not obtained through application permissions, such information should still be processed in a manner that is not excessive to the legitimate purpose.

2. When the purpose for accessing an application permission has already been achieved and there are no other applicable lawful criteria for such access, such online applications shall prompt the data subject to turn off, disallow these permissions, or inform the data subject that access to the relevant application permissions may already be revoked.

3. Where an online application requires access to the borrower's phone camera, or access to the photo gallery to choose a photo for the legitimate purposes of KYC and preventing fraud at the beginning of the loan application or for payment verification and other similar legitimate purposes, permissions for such access may be allowed during that particular stage in the loan process and must be turned-off after the fulfillment of such purposes or the data subject shall be informed when such purposes have been fulfilled and access to the relevant application permission(s) may already be revoked.

Where the photo has already been taken and saved in the application, the application should already turn off the relevant application permission by default, or at the very least, prompt the borrower through appropriate means (e.g., just-in time, pop-up notices) that he or she may already turn off or disallow such permission as the same is no longer necessary for the operation of the application. In no way shall the borrower's photo be used to

harass or embarrass the borrower in order to collect a delinquent loan or for any unfair collection practices.

4. Access to and processing of contact lists may be allowed for the purpose of deriving proportional metadata¹ about such contact lists subject to Section 3 (D) (1) and the requirements of Section 4. “Contact list” refers to any compilation or list of information maintained by the data subject that enables him or her to communicate with other individuals. This includes the data subject’s phone contact lists, email lists, or social media contacts.

Unbridled processing of contact list, in whatever form, is prohibited. “Unbridled processing” refers to processing, that is unconstrained, excessive, and disproportional to its purpose such as but is not limited to:

- a) Processing that leads to harassment;
- b) Processing for collection of debt outside of the guarantors provided by the borrower; and
- c) Processing that results in unfair collection practices.²

5. Subject to the limitations of the immediately preceding paragraph, the processing of contact lists for purposes of identifying and contacting the character references or guarantors provided by the borrowers themselves is allowed. Online lending applications must have separate interfaces where borrowers can provide character references and guarantors of their own choosing. LCs, FCs, and other persons acting as such may only be provided limited access to and only to the minimum extent necessary to allow the borrowers to choose from their phone contact list their character references and guarantors, if any.

C. The following provisions shall be added to Section 3:

G. LCs, FCs, and other persons acting as such shall, as part of their registration with the NPC, submit a complete list of the names of all publicly available applications owned or operated by such entities including all publicly available online applications used for loan processing activities, in accordance with the applicable Rules on Registration of Data Processing Systems and Notifications regarding Automated Decision-Making;

¹ Metadata as used in this Circular is understood to be any information that may define or describe contact lists.

² Securities and Exchange Commission, “Prohibition on Unfair Debt Collection Practices of Financing Companies (FC) and Lending Companies (LC),” SEC Memorandum Circular No. 18, series of 2019 [SEC MEMO. CIRC. 18, s. 2019], § 1 (19 August 2019): Unfair collection practices are as those which use or involve threats of use of violence or other criminal means to harm the physical person, reputation or property of any person, as well as those which use threats to take any action that cannot be legally taken.

H. PIPs or third-party service providers operating in the Philippines, engaged by LCs, FCs, and other persons acting as such, shall likewise be required to register with the NPC whenever they are engaged in the processing of personal data under the instructions of the LCs, FCs, or other persons acting as such;

I. For PIPs or third-party service providers outside the Philippines, LCs, FCs, and other persons acting as such, shall ensure that appropriate technical and contractual controls are in place to ensure appropriate protection in the processing of personal data, taking into consideration Sections 28 to 29 and 43 to 45 of the IRR of the DPA;

J. Upon determination of any violation of this Circular, the NPC shall revoke the registration of the PIC or PIP upon due notice and after providing the PIC or PIP an opportunity to explain pursuant to the NPC's existing rules on revocation of registration; and

K. LCs, FCs, and other persons acting as such or PIPs or third-party service providers whose Certificate of Registration has been revoked by the NPC or those determined to have violated the registration requirements, shall be subject to penalties and disciplinary measures as provided in the DPA, its IRR and other issuances of the NPC

D. Section 4 is hereby amended to read as follows:

SECTION 4. Character references. — A character reference is a person whose contact information is provided for verification of the identity and veracity of the information provided by the borrower for the grant of a loan.

A. A borrower may be required to provide names and contact numbers of character references to support the evaluation of the loan application process. To this end, it shall be the responsibility of the borrower to inform his or her character reference regarding the latter's inclusion as such.

B. LCs, FCs, and other persons acting as such shall adopt policies and procedures in handling the personal data of such character references, which may include policies on handling calls.

C. LCs, FCs, and other persons acting as such shall adequately inform the concerned individuals that they were chosen as character reference of the loan applicant and how their contact details were obtained. LCs, FCs and other persons acting as such shall also provide the character reference with the option of having his or her personal data removed as a character reference.

D. Contacting character references for purposes other than for the verification of identity and veracity of the information provided by the borrower, such as but not limited to, marketing, cross-selling, or sharing to third parties for purposes of offering other products or services, is prohibited.

E. A character reference shall not be automatically treated as a guarantor.

E. A new Section 5 is hereby added to read as follows:

SECTION 5. Guarantors. — A guarantor is one who expressly binds himself or herself to the creditor to fulfill the obligation of the individual borrower in case the latter should fail to do so. For a person to be considered a guarantor, he or she should have given his or her consent to be a guarantor in accordance with the provisions of the Civil Code on guaranty.

A. The guarantor's separate consent must be obtained by the LC, FC or other persons acting as such, in accordance with the applicable provisions of the DPA, particularly those on transparency, the right of data subjects to be informed, and consent as a lawful basis for processing personal data.

B. For purposes of debt collection, LCs, FCs or persons acting as such may only contact the guarantor. Contacting persons in the borrower's contact list other than those who were named as guarantors is prohibited in accordance with this Circular and the applicable issuances of the Securities and Exchange Commission on unfair debt collection practices.³

F. The succeeding Sections on Credit Data, Outsourcing, Rights of the data subject are hereby renumbered accordingly:

SECTION 6. Credit Data. — x x x

SECTION 7. Outsourcing. — x x x

SECTION 8. Rights of the data subjects. — x x x

SECTION 3. Transitory Provisions. —All LCs, FCs, and other persons acting as such shall register all online applications used for loan processing activities with the NPC in accordance with the applicable Rules on Registration of Data Processing Systems and Notifications regarding Automated Decision-Making within fifteen (15) days after the effectivity of this Circular or within thirty (30) days from the availability of the NPC's registration system, whichever comes later.

³ See: Securities and Exchange Commission, "Prohibition on Unfair Debt Collection Practices of Financing Companies (FC) and Lending Companies (LC)," SEC Memorandum Circular No. 18, series of 2019 [SEC MEMO. CIRC. 18, s. 2019], § 1 (19 August 2019).

All online applications which will be made publicly available after the effectivity of this Circular shall be registered with the Commission in accordance with Section 2 (C) of this

Circular.

SECTION 4. *Separability Clause.* — If any portion or provision of this Circular is declared null and void, or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 5. *Repealing Clause.* — All other rules, regulations, and issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified accordingly.

SECTION 6. *Effectivity.* — This Circular shall take effect fifteen (15) days after its publication in the Official Gazette or a newspaper of general circulation.

Approved:

SGD.

JOHN HENRY D. NAGA
Privacy Commissioner

SGD.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

NPC Circular No. 2022-03

Date : 05 December 2022

**Subject : GUIDELINES FOR PRIVATE SECURITY AGENCIES ON
THE PROPER HANDLING OF CUSTOMER AND VISITOR
INFORMATION**

WHEREAS, the National Privacy Commission (NPC) recognizes the vital role of Private Security Agencies (PSA) and Security Guards in ensuring the safety and security of persons and properties;

WHEREAS, entities classified as personal information controllers (PICs) under Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), generally engage PSAs and Security Guards to secure and control access to identified areas or properties, among others;

WHEREAS, the NPC received reports concerning the apparent disregard by some Security Guards of the data privacy rights of customers, visitors, and other data subjects;

WHEREAS, pursuant to the Philippine National Police-Supervisory Office for Security and Investigation Agencies Memorandum dated 15 June 2020 and the Housing and Land Use Regulatory Board Administrative Order 3, Series of 2017 dated 19 May 2017, PSAs and other similar entities engaged by homeowners' associations (HOA) do not have the authority to require motorists to surrender their driver's license, even temporarily, as a condition for entry to gated communities, as such authority is lodged by law¹ only upon the Land Transportation Office (LTO) or others it may deputize;

WHEREAS, the sole purpose for requiring an Identification Card (ID) from the customers, visitors, and other data subjects is to verify their identity;

WHEREAS, there is a need to inform and acquaint PSAs and Security Guards with the proper processing of personal data during the performance of their duties to avoid violating the rights of data subjects under the DPA;

WHEREAS, Section 11 of the DPA allows the processing of personal information subject to compliance with the requirements of the DPA and other laws allowing disclosure of information to the public, and adherence to the general principles of transparency, legitimate purpose, and proportionality;

¹ Land Transportation and Traffic Code, § 29: Confiscation of Driver's License. – Law enforcement and peace officers of other agencies duly deputized by the Director shall, in apprehending a driver for any violation of this Act or any regulations issued pursuant thereto, or of local traffic rules and regulations not contrary to any provisions of this Act, confiscate the license of the driver concerned and issue a receipt prescribed and issued by the Bureau therefor which shall authorize the driver to operate a motor vehicle for a period not exceeding seventy-two hours from the time and date of issue of said receipt. The period so fixed in the receipt shall not be extended, and shall become invalid thereafter. Failure of the driver to settle his case within fifteen days from the date of apprehension will be a ground for the suspension and/or revocation of his license.

WHEREAS, Section 14 of the DPA states that a PIC may subcontract the processing of personal information: provided, that the PIC shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the DPA and other laws for processing of personal information;

WHEREAS, Section 21 (a) of the DPA further states that a PIC is accountable for complying with the requirements of the law and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party;

WHEREAS, PSAs and Security Guards engaged by a PIC are considered personal information processors (PIPs) and are also bound to observe the requirements of the DPA and other applicable laws;

WHEREAS, pursuant to Section 7 of the DPA, the NPC is charged with the administration and implementation of the provisions of the law, which includes ensuring the compliance by PICs with the provisions of the DPA, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal information in the country, in coordination with other government agencies and the private sector;

WHEREAS, Section 9 of the Implementing Rules and Regulations of the DPA (IRR) provides that the Commission shall, among its other functions, develop, promulgate, review or amend rules and regulations for the effective implementation of the law;

WHEREFORE, in consideration of the foregoing premises, and without prejudice to the application of other pertinent laws and regulations on the matter, the NPC hereby issues this Circular that prescribes the guidelines for PICs as well as PSAs and Security Guards acting as PIPs, on the proper handling of data subjects' personal data.

SECTION 1. Scope. — This Circular shall apply to all PICs, and to PSAs and Security Guards acting as PIPs, in the processing of personal data of customers, visitors, and other data subjects as part of their security services.

SECTION 2. Definition of Terms. — The definition of terms in the DPA and its IRR, as amended, are adopted herein. In addition, whenever used in this Circular, the following terms shall mean or be understood as follows:

A. "Private Security Agency" or "PSA" refers to any person or entity engaged in contracting, recruitment, training, furnishing, or posting of Security Guards and other private security personnel to individuals, corporation, offices, and organizations, whether private or public, for their security needs as the Philippine National Police (PNP) may approve;²

² See: Department of Labor and Employment, Revised Guidelines Governing the Employment and Working Conditions of Security Guards and other Private Security Personnel in the Private Security Industry, Department Order No. 150-16, series of 2016 [DOLE DO No. 150-16], § 2 (i) (Feb. 9. 2016).

B. “Security Guard” refers to any person who offers or renders personal service to watch or secure either a residence, business establishment, buildings, compounds, areas, or property, inspects, monitors, or performs bodily checks or searches of individuals or baggage, and other forms of security inspection,³ as authorized by the PIC or by the PSA to perform such functions, regardless of his or her designation;

C. “Service Agreement” refers to the contract between the PIC and the PSA acting as a PIP containing the terms and conditions governing the performance or completion of security service, jobs, or work being farmed out for a definite or predetermined period;⁴

D. “Subcontracting” refers to the outsourcing, assignment, or delegation of the processing of personal data by a PIC to a PIP. In this arrangement, the PIC retains control over the processing;

E. “Subcontracting Agreement” refers to a contract, agreement, or any similar document which sets out the obligations, responsibilities, and liabilities of the parties to a subcontracting arrangement. It shall contain mandatory stipulations prescribed by the IRR.

SECTION 3. General Obligations of PICs engaging the services of PSAs. — All PICs engaging the services of PSAs shall have the following obligations:

- A. Transparency. PICs, in coordination with the PSAs, shall be responsible for developing a privacy notice in clear and plain language which shall explain to all customers, visitors, and other data subjects:
 - 1. The purpose of collecting personal data, e.g., monitoring or controlling access to premises for the security, safety, and protection of persons and properties, pursuant to legitimate interests (for private sector PICs) or laws and regulations (for government PICs);
 - 2. The security measures implemented to safeguard personal data;
 - 3. The fact that the personal data collected, whether manually or through electronic systems, shall be turned over to the pertinent PIC who engaged the PSA or the Security Guard;
 - 4. The retention period of personal data; and
 - 5. Their rights as a data subject and mechanisms on how to exercise the same;
- B. Proportionality. PICs shall observe proportionality in all personal data processing activities including those outsourced or subcontracted to PSAs. They shall not require PSAs acting as PIPs as well as the Security Guards to access, record, copy, or otherwise collect any sensitive personal information for purposes of ascertaining the identity of an individual, nor shall they direct them to keep ID cards containing sensitive personal information.

³Id. § 2 (h).

⁴DOLE DO No. 150-16, § 2 (j).

However, PICs may instruct PSAs and authorized Security Guards to visually examine a government-issued ID within a reasonable time: provided, that there is prior sufficient explanation to the data subject of the necessity of processing sensitive personal information for that purpose: provided further, that the government-issued ID shall not be kept by the PSA or authorized Security Guards.

- C. Accountability. PICs shall use contractual or other reasonable means to ensure that proper safeguards are in place to guarantee the confidentiality, integrity, availability of the personal data processed, and to prevent its use for unauthorized purposes. PICs shall ensure that a Subcontracting Agreement or Service Agreement is executed with PSAs prior to any personal data processing activity. Such agreement shall contain the following:

1. The subject-matter and duration of the processing;
2. The nature and purpose of the processing;
3. The type/s of personal data that will be processed;
4. The categories of data subjects;
5. The geographic location of the processing under the agreement;
6. The obligations and rights of PICs;
7. The specific obligations of PSAs taking into consideration the mandatory stipulations under Section 44 (b) of the IRR of DPA; and
8. The duty of PSAs to comply with the requirements of the DPA and its IRR, other relevant issuances of the Commission, other applicable laws, and any other obligations with the PICs.

- D. Safeguards. PICs shall ensure that reasonable and appropriate safeguards are in place for the processing of personal data by PSAs and their Security Guards which include, but are not limited to:

1. Appropriate data protection policies that provide for organizational, physical, and technical security measures, taking into account the nature, scope, context and purpose of the processing, as well as the risks posed to the rights and freedoms of data subjects;
2. Clear and adequate instructions on the processing of personal data, whether in paper-based or electronic systems, including the strict protocols to be observed by Security Guards in the processing of sensitive personal information, where justified, as provided under Section 3(B) of this Circular;
3. Reasonable retention period of personal data as well as the method to be adopted for the secure return, destruction, or disposal of the same and the timeline therefor, taking into account the purpose for which the personal data was obtained and the provisions of the applicable Subcontracting Agreement or Service Agreement.

- a. The retention of personal data shall only be limited to the time necessary for the fulfillment of the declared, specified, and legitimate purpose/s, or when the processing relevant to the purpose has been terminated.
- b. For government agencies, the retention period under the applicable law shall be observed.⁵

SECTION 4. *Obligations of PSAs acting as PICs.* — All PSAs acting as PICs shall have the following obligations:

- A. Registration. All PSAs acting as PICs shall register with the Commission in accordance with the applicable Rules on the Registration of Data Processing Systems and Notifications regarding Automated Decision-Making;
- B. Training. PSAs shall provide trainings on the DPA, its IRR, and other relevant issuances of the Commission to all Security Guards prior to their assignment or deployment.
 1. The orientation shall include an overview on the proper handling of personal data that comes to their knowledge and possession in the course of providing security services, the requirement to maintain confidentiality, integrity, and availability of personal data, and the corresponding sanctions for any unauthorized processing of personal data;
 2. The conduct of the training shall be properly documented at all times. The Commission may require the submission of the same in accordance with the applicable provisions of the DPA, its IRR, and other issuances on the matter;
- C. Inspection. All PSAs shall ensure that all Security Guards assigned or deployed are complying with the requirements of the DPA. For this purpose, PSAs shall conduct regular onsite visits in establishments where its Security Guards are assigned or deployed.

SECTION 5. *Obligations of PSAs acting as PIPs.* — All PSAs acting as PIPs shall have the following obligations:

- A. Privacy Notice. PSAs shall make reasonable efforts to notify the data subjects of the relevant information about the processing of their personal data through a privacy notice developed by the PIC in coordination with the PSAs.
- B. Proportionality. For purposes of ascertaining the identity of an individual, PSAs and authorized Security Guards shall not access, record, copy,

⁵ See: National Archives of the Philippines, General Records Disposition Schedule common to all Government Agencies, series 2009 which provides for the retention period of two (2) years after date of last entry for logbooks (available at <https://nationalarchives.gov.ph/wp-content/uploads/2015/04/NAP-Gen.-Circular-1-2-and-GRDS-2009.pdf>).

or otherwise collect any sensitive personal information such as date of birth, government-issued ID numbers, images of government-issued IDs, nor shall they keep ID cards containing sensitive personal information.

However, PSAs and authorized Security Guards may be allowed to examine a government-issued ID within a reasonable time: provided, that there is prior sufficient explanation to the data subject of the necessity of processing sensitive personal information for that purpose: provided further, that the government-issued ID shall not be kept by the PSA or authorized Security Guards.

C. Security measures. PSAs and their Security Guards shall, in coordination with the PIC, implement appropriate security measures that:

1. Aim to maintain the availability, integrity, and confidentiality of personal data processed;
2. Provide adequate protection against any accidental or unlawful destruction, alteration, disclosure, and unlawful processing, as well as against natural and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

PSAs and Security Guards shall, at all times, ensure that entries consisting of personal data in the logbooks, health forms, and other records are not visible to or accessible by unauthorized persons, employees, or other data subjects to prevent unlawful processing of personal data.

D. Assistance. PSAs acting as PIPs and its Security Guards shall cooperate with the relevant PIC in addressing any requests for the exercise of data subject rights. PSAs shall not engage another PIP without prior instruction from the PIC.

E. Inspection. PSAs acting as PIPs shall allow audits and inspections conducted by the PIC or another auditor authorized by such PIC.

SECTION 6. Penalties. — The processing of personal data in violation of this Circular shall carry criminal, civil, and administrative liability pursuant to the provisions of the DPA and related issuances of the Commission. This is without prejudice to the administrative penalties that may be imposed under Republic Act No. 5487 or “An Act to Regulate the Organization and Operation of Private Detective, Watchmen or Security Guards Agencies” and other applicable laws.

SECTION 7. Interpretation. — Any doubt in the interpretation of any provision of this Circular shall be liberally interpreted in a manner mindful of the rights and interests of the data subjects.

SECTION 8. Transitory Provisions. — PICs and PSAs acting as PIPs shall be given a period of sixty (60) days from the effectivity of these Guidelines to comply with the requirements provided herein.

SECTION 9. *Separability Clause*. — If any portion or provision of this Circular is declared null and void, or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 10. *Repealing Clause*. — All other rules, regulations, and issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified accordingly.

SECTION 11. *Effectivity*. — This Circular shall take effect fifteen (15) days after its publication in the Official Gazette or a newspaper of general circulation.

Approved:

SGD.

JOHN HENRY D. NAGA
Privacy Commissioner

SGD.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

NPC Circular No. 2022-04

Date : 05 December 2022

Subject : REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION

WHEREAS, Article II, Section 24, of the 1987 Constitution provides that the State recognizes the vital role of communication and information in nation-building. At the same time, Article II, Section 11 thereof emphasizes that the State values the dignity of every human person and guarantees full respect for human rights; WHEREAS, Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), provides that it is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth. The State also recognizes its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secure and protected;

WHEREAS, Section 16 of the DPA and Section 34 of its Implementing Rules and Regulations (IRR) provide that data subjects shall be furnished with and given access to their personal data that are being processed in Data Processing System, as well as the purpose, scope, method, and manner of such processing, including the existence of automated decision-making;

WHEREAS, pursuant to Section 7 of the DPA, the National Privacy Commission (NPC) is charged with the administration and implementation of the provisions of the law, which includes ensuring the compliance by a personal information controller (PIC) with the provisions thereof, publishing a compilation of an agency's system of records and notices, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal data, in coordination with other government agencies and private entities;

WHEREAS, Section 9 of the IRR provides that, among the NPC's functions, is to develop, promulgate, review, or amend rules and regulations for the effective implementation of the DPA;

WHEREAS, Section 24 of the DPA states that, when entering into any contract that may involve accessing or requiring sensitive personal information from at least one thousand (1,000) individuals, a government agency shall require the contractor and its employees to register its personal information processing system with the NPC in accordance with the DPA and to comply with the law's provisions. Furthermore, Section 14 of the DPA mandates that a personal information processor (PIP) shall also comply with all requirements of the DPA and other applicable laws;

WHEREAS, in line with Sections 46 and 47 of the IRR, a PIC or PIP that employs fewer than two hundred fifty (250) persons shall not be required to register unless the processing it carries out is likely to pose a risk to the rights and freedoms of data subjects, is not occasional, or includes sensitive personal information of at least one thousand (1,000) individuals. Moreover, Section 48 thereof declares that a PIC carrying out any automated processing operation that is intended to serve a single or several related purposes must notify the NPC when the operation becomes the sole basis for making decisions about a data subject, and when such decision would significantly affect the data subject;

WHEREAS, Sections 46 and 47, Rule XI of the IRR also require the effective and efficient monitoring of a Data Processing Systems that are likely to pose a risk to the rights and freedoms of data subjects including those that involve information likely to affect national security, public safety, public order, or public health or information required by applicable laws or rules to be confidential; vulnerable data subjects like minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a PIC or PIP, especially those involving automated decision-making or profiling;

WHEREFORE, in consideration of these premises, the NPC hereby issues this Circular governing the registration of

Data Processing System and Data Protection Officer, notification regarding automated decision-making or profiling, and the NPC seal of registration:

PRELIMINARY PROVISIONS

SECTION 1. Scope. The provisions of this Circular shall apply to any natural or juridical person in the government or private sector processing personal data and operating in the Philippines, subject to the relevant provisions of the DPA, its IRR, and other applicable issuances of the NPC.

SECTION 2. Definition of Terms. For the purpose of this Circular, the definition of terms in the Data Privacy Act of 2012 and its IRR are adopted, and the following terms are defined, as follows:

- A. “Automated Decision-making” refers to a wholly or partially automated processing operation that can make decisions using technological means totally independent of human intervention; automated decision-making often involves profiling;
- B. “Common DPO” refers to an individual who is a member of a group of related companies or an individual consultant under contract with several separate PICs and PIPs who is appointed or designated to be primarily responsible for ensuring the compliance of each of the concerned entities with the DPA, its IRR and all other relevant issuances of the Commission;
- C. “Compliance Officer for Privacy” or “COP” refers to an individual that performs the functions or some of the functions of a DPO in a particular region, office, branch, or area of authority;
- D. “Data Protection Officer” or “DPO” refers to an individual designated by the head of agency or organization to ensure its compliance with the Act, its IRR, and other issuances of the Commission: Provided, that, except where allowed otherwise by law or the Commission, the individual must be an organic employee of the government agency or private entity: Provided further, that a government agency or private entity may not have more than one DPO;

- E. “Datasharing” is the sharing, disclosure, or transfer to a third party of personal data under the custody of a personal information controller to one or more other personal information controllers; In the case of a personal information processor, data sharing should only be allowed if it is carried out on behalf of and upon the instructions of the personal information controller it is engaged with via a subcontracting agreement. Otherwise, the sharing, transfer, or disclosure of personal data that is incidental to a subcontracting agreement between a personal information controller and a personal information processor should be excluded.
- F. “Government Agency” refers to a government branch, body, or entity, including national government agencies, instrumentalities, bureaus, or offices, constitutional commissions, local government units, government-owned and controlled corporations and subsidiaries, government financial institutions, state colleges and universities;
- G. “Head of Agency” refers to:
1. the head of the government entity or body, for national government agencies, constitutional commissions or offices, or branches of the government;
 2. the governing board or its duly authorized official for government-owned and
- controlled corporations, government financial institutions, and state colleges and universities;
 3. the local chief executive, for local government units;
- H. “Head of Organization” refers to the head or decision-making body of a private entity or organization; For private organizations or government-owned and controlled corporations organized as private corporations, the Head of Organization may be the President, the Chief Executive Officer, or the Chairman of the Board of Directors or any officer of equivalent rank in the organization.
- I. “Individual Professional” refers to individuals who are self-employed and who derive income practicing their professions, with or without license from a regulatory board or body, not

being part of a partnership, firm, or other organization, which should otherwise be registered as a personal information controller, and which practice includes the processing of personal data. The individual professional is the de facto DPO;

- J. “Operating in the country” refers to PICs and PIPs who, although not founded or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch, or agency in the Philippines;
- K. “Private entity” or “Private organization” refers to any natural or juridical person that is not a unit of the government, including, but not limited to, a corporation, partnership, company, non-profit organization, or any other legal entity;
- L. “Profiling” refers to any form of automated processing of data consisting of the use of personal data, such as an individual’s economic situation, political or religious beliefs, behavioral or marketing activities, personal preferences, electronic communication data, location data, and financial data, among others, in order to evaluate, analyze, or predict his or her performance, qualities, and behavior, among others;
- M. “Registration information” refers to the completed registration details as inputted by the registrant into the NPC’s official registration platform.

SECTION 3. Purpose. This Circular establishes the following:

- A. The framework for registration of Data Processing Systems in the Philippines, including online web-based and mobile applications that process personal data;
- B. The mandatory or voluntary registration of Data Protection Officers (DPO) in both the government and private entities as hereby prescribed in the succeeding sections; and
- C. The imposition of other requirements to achieve the following objectives:

1. ensure that PICs and PIPs covered by this Circular and as provided for in the succeeding sections are able to register its DPO;
2. ensure that PICs and PIPs keep a record of their data processing activities;
3. guarantee that information about Data Processing System owned by PICs or PIP operating in the country are made accessible to the Commission to enable a more efficient compliance monitoring process and uphold the exercise of data subject rights under the DPA; and
4. promote transparency and accountability in the processing of personal data.

SECTION 4. General Principles. This Circular shall be governed by the following general principles:

- A. Registration of an entity's Data Processing System and DPO with the Commission shall be one of the means through which a PIC or PIP demonstrates its compliance with the DPA, its IRR, and other relevant issuances of the NPC.
- B. Registration information submitted by a PIC or PIP to the NPC are presumed to contain all required information on its Data Processing System that are active or existing during the validity of such registration. Any information excluded therefrom are deemed nonexistent.
- C. Registration information submitted by a PIC or PIP to the NPC on the identity and official contact details of the designated DPO shall remain effective unless otherwise amended or updated in accordance with the process in this Circular.
- D. Unless otherwise provided in this Circular, any information, file, or document submitted by a PIC or PIP to the NPC shall be kept confidential.
- E. Any doubt in the interpretation of the provisions of this Circular shall be liberally interpreted in a manner that would uphold the rights and interests of data subjects.

REGISTRATION OF DATA PROCESSING SYSTEM AND DATA PROTECTION OFFICER

SECTION 5. Mandatory Registration. A PIC or PIP that employs two hundred fifty (250) or more persons, or those processing sensitive personal information of one thousand (1,000) or more individuals, or those processing data that will likely pose a risk to the rights and freedoms of data subjects shall register all Data Processing Systems.

- A. A Data Processing System processing personal or sensitive personal information involving automated decision-making or profiling shall, in all instances, be registered with the Commission.
- B. A PIC or PIP shall register its own Data Processing System. In instances where the PIC provides the PIP with the system, the PIC is obligated to register the same. A PIC who uses a system as a service shall register the same indicating the fact that processing is done through a service provider. A PIP who uses its own system as a service to process personal data must register with the Commission.
- C. A PIC or PIP who is an Individual Professional for mandatory registration shall register with the Commission. For this purpose, the following shall be considered:
 - 1. An Individual Professional is self-employed and practicing his or her profession as defined under this Circular;
 - 2. A business establishment, if registered as a PIC and operating under a different business name, partnership, firm, or other organization, shall not register separately as an Individual Professional;
 - 3. An Individual Professional shall be considered as the de facto DPO.

SECTION 6. Voluntary Registration. An application for registration by a PIC or PIP whose Data Processing System does not operate under any of the conditions set out in the preceding Section may register voluntarily following the process outlined in this Circular.

A PIC or PIP who does not fall under mandatory registration and does not undertake voluntary registration shall submit a sworn declaration (see Annex 1). The Commission through an Order may require a PIC or PIP to submit supporting documents related to this submission.

SECTION 7. When to Register. A covered PIC or PIP shall register its newly implemented Data Processing System or inaugural DPO in the NPC's official registration platform within twenty (20) days from the commencement of such system or the effectivity date of such appointment.

In the event a covered PIC or PIP seeks to apply minor amendments to its existing registration information, which includes updates on an existing Data Processing System, or a change in DPO, the PIC or PIP shall update the system within ten (10) days from the system update or effectivity of the appointment of the new DPO.

SECTION 8. Authority to Register. A PIC or PIP shall file its application for registration through its designated DPO. A PIC or PIP shall only be allowed to register one (1) DPO, provided that in cases where a PIC or PIP has several branches, offices, or has a wide scope of operations, the PIC or PIP may designate one (1) or more Compliance Officers for Privacy (COP) who shall then be indicated as such in the DPO registration. Approval of the Commission is not required for COP designations.

A COP shall always be under the direct supervision of the DPO. Under no circumstance shall the registered COP be treated as a DPO unless the DPO registration is amended to reflect such changes. Further, in cases where a COP is designated by the PIC or PIP, the registration shall be accompanied by the list of COPs clearly indicating the branch, office, unit, or region to which they are assigned along with the official e-mail address and contact number.

In all cases, a PIC or a PIP is required to provide its DPO's dedicated e-mail address that should be separate and distinct from the personal and work e-mail of the personnel assigned as a DPO. The DPO's dedicated e-mail address must be maintained at all times to ensure that the Commission is able to communicate with the PIC and PIP. In case the individual designated as DPO vacates the position, the PIC or PIP should designate an interim DPO to monitor any communications sent through the official DPO e-mail address.

A Common DPO shall be allowed so long as entities are registered separately. The Common DPO shall register each entity individually. Approval of the Commission is not required for Common DPO appointments.

An Individual Professional shall register himself or herself as the DPO. In cases where the Individual Professional contracts another person to act as DPO he or she shall indicate such fact and provide the required contact details of such person in the registration record. The Commission through an Order may require a PIC or PIP to submit supporting documents related to this submission.

SECTION 9. Registration Process. A PIC or PIP shall create an account by signing up in the NPC's official registration platform where it shall provide details about the entity.

- A. Upon signing up, the PIC or PIP shall input the name and contact details of the DPO together with a unique and dedicated email address, specific to the position of DPO pursuant to the provisions of the fourth paragraph of Section 8.
- B. During registration proper, the PIC or PIP shall encode the name and contact details of the Head of the Organization or Head of Agency.
- C. The prescribed application form shall be accomplished and shall be uploaded together with all supporting documents as provided under Section 11.
- D. The details of all Data Processing System owned by the PIC or PIP shall be encoded into the platform. All Data Processing System of the PIC or PIP at the time of initial registration must be encoded into the system.
- E. The PIC or PIP shall identify and register all publicly facing online mobile or web-based applications in accordance with Section 3(A).
- F. The submissions of the PIC or PIP shall undergo review and validation by the Commission. In case of any deficiency, the PIC or PIP shall be informed of the same and shall be given five (5) days to submit the necessary requirements. Once the submissions have been validated and considered complete, the PIC or PIP shall be informed that the Certificate of Registration is available for download.

An Individual Professional shall register only under his or her name, and indicate his or her principal business address and contact details. Registration through physical submission of requirements is not allowed.

SECTION 10. Mandatory Appointment of DPO in the Government. A Government Agency is required to designate and register a DPO with a rank not lower than an Assistant Secretary or Executive Director IV in case the highest ranking official is a Department Secretary or a position of equivalent rank; at least Director IV level in case the highest ranking official is an Undersecretary or a position of equivalent rank; at least Director II level in case the highest ranking official is an Assistant Secretary or a position of equivalent rank; and at least a Division Chief in case the highest ranking official is a Regional Director or a position of equivalent rank.

For Local Government Units (LGUs), the Provincial, City and Municipal levels shall designate and register a DPO with a rank not lower than Department Head.

Cities and Municipalities can designate a COP at the Barangay level, provided that the COP shall be under the supervision of the DPO of the corresponding City, or Municipality that the Barangay is part of.

SECTION 11. Application Form. An application for registration filed by a PIC or PIP must be duly notarized and be accompanied by the following documents:

A. For government agencies:

Special or Office Order, or any similar document, designating or appointing the DPO of the PIC or PIP;

B. For domestic private entities:

1. For Corporations:

- a) (1) duly notarized Secretary's Certificate authorizing the appointment or designation of DPO, or (2) any other document demonstrating the validity of the appointment or designation of the DPO signed by the Head of the Organization with an accompanying

valid document conferring authority to the Head of Organization to designate or appoint persons to positions in the organization.

- b) Securities and Exchange Commission (SEC) Certificate of Registration.
- c) certified true copy of latest General Information Sheet.
- d) valid business permit.

2. For One Person Corporation

- a) (1) duly notarized Secretary's Certificate authorizing the appointment or designation of DPO, or (2) any other document that demonstrates the validity of the appointment or designation of DPO signed by the sole director of the One Person Corporation.
- b) SEC Certificate of Registration
- c) valid business permit.

3. For Partnerships

- a) duly notarized Partnership Resolution or Special Power of Attorney authorizing the appointment or designation of DPO, or any other document that demonstrates the validity of the appointment or designation.
- b) SEC Certificate of Registration.
- c) valid business permit.

4. Sole Proprietorships:

- a) duly notarized document appointing the DPO and signed by the sole proprietor, in case the same should elect to appoint or designate another person as DPO.
- b) DTI Certificate of Registration.
- c) valid business permit.

C. For foreign private entities:

1. Authenticated copy or Apostille of Secretary's Certificate authorizing the appointment or designation of DPO, or any other document that demonstrates the appointment or designation, with an English translation thereof if in a language other than English.
2. Authenticated copy or Apostille of the following documents, with an English translation thereof if in a language other than English, where applicable:
 - a) Latest General Information Sheet or any similar document.
 - b) Registration Certificate (Corporation, Partnership, Sole Proprietorship) or any similar document.
 - c) valid business permit or any similar document.

SECTION 12. Details of Registration. In the NPC's online registration platform, a PIC or PIP shall provide the following registration information:

A. details of the PIC or PIP, the Head of Agency or Organization, and the Data Protection Officer.

- 1.) name and contact details of the PIC or PIP, Head of Agency or Organization, and DPO as well as the designated COP, if any, with supporting documents.
- 2.) a unique and official email address specific to the position of DPO of the PIC or PIP, and not with the person who is the DPO.
- 3.) primary purpose of the private entity or the constitutional or statutory mandate of the government agency;

B. brief description per Data Processing System:

- 1.) name of the system;
- 2.) basis for the processing of information;

- 3.) purpose or purposes of the processing;
 - 4.) whether processing is being performed as a PIC or PIP, if an organization uses the same system as a PIC and as a PIP, then the organization shall register such usage separately;
 - 5.) whether the system is outsourced or subcontracted, and if so, the name and contact details of the PIP;
 - 6.) description of the category or categories of data subjects, and their personal data or categories thereof;
 - 7.) recipients or categories of recipients to whom the personal data might be disclosed;
 - 8.) description of security measures (Organizational, Physical, and Technical)
 - 9.) general information on the Data Life Cycle (Time, Manner, or Mode of Collection, Retention Period, and Disposal/ Destruction/Deletion Method/Procedure)
 - 10.) whether personal data is transferred outside of the Philippines; and 11.) the existence of Data Sharing Agreements with other parties;
- C. Identify all publicly facing online mobile or web-based applications, including internal apps with PIC or PIP employees as clients.
- D. Notification regarding any automated decision-making operation or profiling.

SECTION 13. Certificate of Registration. The Commission shall issue a Certificate of Registration in favor of a PIC or PIP, that has successfully completed the registration process. The Certificate of Registration shall only be considered as proof of such registration and not a verification of the contents thereof.

Any party may request, in writing, an authenticated copy of the Certificate of Registration of a PIC or PIP, subject to payment of reasonable fees covered by a separate issuance for this specific purpose.

SECTION 14. Validity. A Certificate of Registration shall be valid for one (1) year from its date of issuance; provided, that the certificate may be revoked by the Commission on any of the grounds provided for under Section 35 of this Circular and upon service of a Notice of Revocation to the PIC or PIP.

SECTION 15. Verification. The Commission may, at any time, verify any or all registration information provided by a PIC or PIP through its compliance check function. Through a privacy sweep of publicly available information, notices of document submission or during on-site examination of the Data Processing System, all relevant documents shall be made available to the Commission.

SECTION 16. Amendments or Updates. Subject to reasonable fees that may be prescribed by the Commission, major amendments to registration information shall be made within thirty (30) days from the date such changes take into effect. Major amendments are the changes to the following:

- (a) Name of the PIC or PIP; and
- (b) the Office Address of the PIC or PIP.

Minor updates shall be made within ten (10) days from the date such changes take into effect. Updates shall include all other information other than those covered as a major amendment.

The PIC or PIP shall fill-up the necessary form and submit accompanying supporting documents when required.

SECTION 17. Non-Registration. A PIC or PIP shall be considered as unregistered under the following circumstances:

- A. failure to register with the Commission in accordance with Section 7 of this Circular;
- B. expiration and non-renewal of Certificate of Registration;
- C. non-submission of any deficiency in supporting documents within five (5) days from notice;
- D. rejection or disapproval of an application for registration, or an application for renewal of registration; or

E. revocation of the Certificate of Registration.

SECTION 18. Renewal. A PIC or PIP may only renew its registration thirty (30) days before the expiration of the one-year validity of its Certificate of Registration.

SECTION 19. Reasonable Fees. To recover administrative costs, the Commission may require the payment of reasonable fees for registration, renewal, and other purposes in accordance with a schedule that shall be provided in a separate issuance.

SECTION 20. Imposition of Administrative Fines. A PIC or PIP covered by Mandatory Registration who shall be in violation of the same, shall be subject to the corresponding fine in accordance with the Guidelines on Administrative Fines.

A PIC or PIP who failed to comply with an Order of the Commission to submit documents in relation to Section 5(A) and the last paragraph of Section 8 shall be liable for failure to register and failure to comply with an Order of the Commission.

SECTION 21. Inaccessible DPO Accounts. In case a DPO account was not properly transferred, or in cases of inaccessibility to the registration platform due to lost credentials, or upon failure of a prior DPO to properly turn over the accountability to the registration platform, the PIC or PIP shall submit a notarized letter of explanation or any similar document as justification as to why the DPO account was lost or not properly transferred without prejudice to any administrative finding of failure to register or to update registration. Subject to reasonable fees that may be prescribed by the Commission, the Head of Agency or Head of Organization may request the retrieval of the account.

SECTION 22. Withdrawal of Registration. Withdrawal of registration of information due to cessation of business, or in cases when personal data processing is no longer done or for other similar reasons, shall be made in writing and accompanied by supporting documents such as certified photocopy of SEC Certificates of Dissolution of corporation, or board resolutions, within two (2) months from the date such cessation takes effect which shall be submitted electronically via email. It shall be presumed that the PIC or PIP is still processing personal information or is still operating its business in the absence

of an application for the withdrawal of registration. Verily, a PIC or PIP may still be a subject of a compliance check absent any showing that such withdrawal has been applied for.

In case of death of an Individual Professional registrant, withdrawal may be done by the next of kin through written notification with a copy of the death certificate attached as proof which shall be submitted electronically via email.

REGISTRY OF DATA PROCESSING SYSTEM

SECTION 23. Maintenance of Registry. The Commission shall maintain a registry of PICs and PIPs, and of the Data Processing Systems, and designated or appointed Data Protection Officers in electronic format.

SECTION 24. Removal from Registry. The registration information of a PIC or PIP may be removed from the registry, upon prior notice by the Commission, on any of the following grounds:

- A. Incomplete registration;
- B. Expiration and non-renewal of registration;
- C. Revocation of Certificate of Registration;
- D. Expired and void registration; or
- E. Withdrawal of registration by the PIC due to cessation of business, cessation of personal data processing, or death of the Individual Professional registrant.

Except for Section 24(E), the PIC or PIP is given fifteen (15) days from notice to answer and explain why its removal should not be effected.

SECTION 25. Non-inclusion of Confidential Information. Information classified by the Constitution or any statute as confidential shall not be included in the registry.

NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING

SECTION 26. Notification of Automated Decision-Making or Profiling. A PIC or PIP that carries out any automated decision-making operation or profiling shall indicate in its registration record and identify the Data Processing System involved in the automated decision-making or profiling operation.

The PIC or PIP shall also include information on the following:

A. lawful basis for processing personal data;

1. Other relevant information pertaining to the specified lawful basis specifying the specific law or regulation among others.

If consent is used as the basis for processing, submission of the following:

- i. consent form used; or
- ii. other manner of obtaining consent.

B. retention period for the processed data;

C. methods and logic utilized for automated processing; and

D. possible decisions relating to the data subject based on the processed data, particularly if the decisions would significantly affect the data subject's rights and freedoms.

SECTION 27. When to Notify. Notification regarding automated decision-making and profiling shall be included in the registration information that will be provided by a PIC or PIP, as indicated in Section 12 of this Circular, or through amendments or updates to such registration information, as per Section 16 of this Circular, within the prescribed periods.

SECTION 28. Availability of Additional Information. Upon request by the Commission, a PIC or PIP shall make available additional information and supporting documents pertaining to its automated decision-making or profiling operation.

NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION

SECTION 29. Issuance of Seal of Registration. The Seal of Registration shall be issued simultaneously with the Certificate of Registration which will also be available for download.

SECTION 30. Standard Information. The Seal of Registration shall contain the following information:

- A. The word “Registered” indicating that the PIC or PIP has registered its DPS and DPO with the Commission;
- B. The validity period of the registration;
- C. A unique QR code for easy verification of registration indicating the following:
 - 1. Name of the PIC or PIP;
 - 2. Registered DPO email; and
 - 3. Validity of registration

SECTION 31. Validity. The Seal of Registration shall be valid for one (1) year from the date of issuance thereof.

SECTION 32. Mandatory Display of Seal of Registration. The Seal of Registration must be displayed at the main entrance of the place of business, office or at the most conspicuous place to ensure visibility to all data subjects.

A PIC or PIP is also required to display the Seal of Registration in its main website, or at least the webpage specifically pertaining to the Philippines for global websites, and only as either:

- (1) a clickable link leading to the privacy notice; or
- (2) displayed directly on the privacy notice page.

SECTION 33. Use of Seal of Registration. The Seal of Registration shall be exclusively used by the registered PIC or PIP.

The use of the Seal of Registration by any person other than the PIC or PIP for whatever purpose is prohibited.

SECTION 34. Automatic Revocation or Withdrawal. In all instances wherein the Certificate of Registration has been revoked, or the registration of the PIC or PIP has been validly withdrawn, the Seal of Registration shall automatically be revoked or otherwise invalidated.

SANCTIONS AND PENALTIES

SECTION 35. Revocation of Certificate of Registration. The Commission may revoke the registration of a PIC or PIP on any of the following grounds:

- A. failure to comply with any of the provisions of the DPA, its IRR, or any relevant issuances of the Commission;
- B. motu proprio revocation upon failure to comply with any order, condition, or restriction imposed by the Commission;
- C. loss of authority to operate or conduct business, due to the revocation of its license, permit, franchise, or any other similar requirement provided by law;
- D. cessation of operations or of personal data processing;
- E. lack of capacity or inability to securely process personal data in accordance with the DPA as determined by the Commission thru its compliance check function;
- F. issuance by the Commission of a temporary or permanent ban on data processing against the PIC or PIP: Provided, that in the case of a temporary ban, such prohibition is still in effect at the time of filing of the application for renewal of registration;
- G. motu proprio revocation for providing false information in the registration or misrepresenting material information in the registration.

Provided, that, prior to revocation, the Commission shall give the PIC or PIP an opportunity to explain why its Certificate of Registration should not be revoked.

In cases of motu proprio revocation in Sections B or G, it shall be operative upon the administrative finding of liability for the infraction. SECTION 36. Notice of Revocation. Where the registration of a PIC or PIP is revoked, the Commission shall issue a Notice of Revocation of Registration, which shall be served upon the PIC or PIP.

SECTION 37. Penalties and Fines. A PIC or PIP whose Certificate of Registration has been revoked or that is determined to have violated the registration requirements provided in this Circular may, upon notice and hearing, be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent bans on the processing of personal data, or payment of administrative fines. For this purpose, the registration requirements shall pertain to the provisions on mandatory registration, amendments and updates, and renewal of registration.

SECTION 38. Cease and Desist Order. When the Commission, upon notice and hearing, has determined that a PIC or PIP violated this Circular, such as the failure to disclose its automated decision-making or profiling operation through the appropriate notification processes set out in this Circular and noncompliance on the mandatory display of the seal of registration, the Commission may cause upon the PIC or PIP the service of a Cease and Desist Order on the processing of personal data: Provided, that this is without prejudice to other processes or reliefs as the Commission may be authorized to initiate pursuant to Section 7 of the DPA and any other administrative, civil, or criminal penalties that the PIC or PIP may incur under the DPA and other applicable laws.

MISCELLANEOUS PROVISIONS

SECTION 39. Transitory Period. Notwithstanding the period in the first paragraph of Section 7 of this Circular; all covered PICs, and PIPs shall complete their Data Processing System and DPO registration within one hundred eighty (180) days from the effectivity of this Circular.

SECTION 40. Repealing Clause. This Circular supersedes in its entirety NPC Circular No. 17-01. The provisions of the IRR and all other issuances contrary to or inconsistent with the provisions of

this Circular are deemed repealed or modified accordingly.

SECTION 41. Separability Clause. If any portion or provision of this Circular is declared null and void, or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 42. Publication and Effectivity. This Circular shall take effect fifteen (15) days after its publication in the Official Gazette or two newspapers of general circulation and the submission of a copy hereof to the Office of the National Administrative Register of the University of the Philippines.

Approved:

Sgd.

JOHN HENRY D. NAGA

Privacy Commissioner

Sgd.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

FREQUENTLY ASKED QUESTIONS ON THE GUIDELINES ON ADMINISTRATIVE FINES

Section 1- Scope

1. **The Guidelines cover all Personal Information Controllers (PICs) and Personal Information Processors (PIPs) as defined by the Data Privacy Act of 2012 (DPA). Does this cover even PICs and PIPs established outside of the Philippines?**

Yes, the Circular covers PICs and PIPs established outside of the Philippines. Section 1 of the Circular provides that it covers all PICs and PIPs as defined in the DPA, whether from the public or private sector. This also covers PICs and PIPs outside of the Philippines if they fall under the requisites found under Section 4 or Section 6 of the DPA. In such instances, the gross income of the foreign PIC or PIP within the Philippines that committed the infraction will be considered to determine the imposable fine.

2. **Will this apply to companies not registered with the National Privacy Commission (NPC)?**

Yes, the Circular applies to entities not registered with the NPC, provided that those entities are covered by the DPA.

Section 2- Administrative Fines

3. **Why are percentage fines used by the Commission instead of a fixed amount of fine?**

The Commission, in working together with the University of the Philippines Law Center, has determined that using percentage fines, as opposed to standard amounts, is the most effective mechanism to impose administrative fines. This allows the Commission to set effective, proportionate, and dissuasive fines regardless of the size of a violating entity.

In utilizing a percentage range, optimal deterrence will be achieved since it provides ex ante incentives for the PIC or PIP to adopt optimal or reasonable levels of data protection. To deter violations, a fine should be equal or larger than the cost of precaution at the optimal level. Thus, the percentage of fines in the Circular is intended to be equal to or larger than the possible cost of privacy security that the PICs or PIPs will put in place.

Furthermore, the Economic Study, which was prepared by the University of the Philippines Law Center with the help of their economic consultant, has determined that the use of percentage fines allows for the protection of the fundamental human right of privacy of communication while ensuring free flow of information. This mutually beneficial exchange of information leads to the promotion of innovation and growth.

4. **Section 2 of the Circular provides that the PIP can be held equally liable as the PIC for administrative fines. Under the Principle of Accountability in the DPA, however, the PIC is liable for any violations even those performed by its subcontractors. Thus, following Section 21 of the DPA, shouldn't the PIC be solely responsible and liable for the administrative infractions committed by the PIP under its control, subject only to contractual agreements between them on indemnity?**

No, the PIC will not be solely impleaded for purposes of administrative fines. The wording of the Circular includes both the PIC and PIP because in complaints initiated by the data subjects, the complainant may not be aware whether the entity is a PIC or PIP since he or she is not privy to these matters.

Nevertheless, the Principle of Accountability and the contractual arrangements between the PIC and PIP regarding liabilities may be invoked by the parties in their respective submitted pleadings for the evaluation of the Commission.

5. **In determining the total imposable fine, how will the Five Million Peso (Php 5,000,000.00) cap in Section 2 be implemented? Does it mean that the PIC or PIP's maximum penalty for a single action will be Php 5,000,000.00 regardless of the applicable percentages under Section 2 of the Circular?**

As written, Section 2 of the Circular states that "In any case, the total imposable fine for a single act of a PIC or PIP, whether resulting in single or multiple infractions, shall not exceed Five Million Pesos (Php 5,000,000.00)."

The term "single act" refers to an act of processing. A single act may give rise to several violations. Nevertheless, in determining what constitutes a "single act", the number of the affected data subjects whose rights are violated, or the amount of personal information processed are not considered since the term pertains to a "per processing" activity.

At any given time, however, the maximum imposable penalty for a single act is Php 5,000,000.00, regardless of the applicable percentage range under Section 2 of the Circular.

This cap of Php 5,000,000.00 will be subject to periodic review by the Commission to determine if there is a need to revise the amount in the future.

6. How will the type of infraction be determined? Is it by counting the number of provisions under Section 11 or Section 16 of the DPA that were violated by PIC or PIP's single action?

Yes, the type of infraction will be determined by taking into consideration the number of (1) general data privacy principles and (2) data subject rights violated. However, the number of principles and rights violated will not be compounded with the number of data subjects affected. Thus, to be considered a Major Infraction, the total affected data subjects is one thousand or below (1-1,000), while for Grave Infractions, the number of affected data subjects exceeds one thousand (1,001 or more).

7. Under Other Infractions, it states that “any natural or juridical person processing personal data that fails to comply with any Order, Resolution or Decision of the Commission, or of any of its duly authorized officers, pursuant to Section 7 of the DPA and its corresponding implementing issuances shall be subject to an administrative fine not exceeding Fifty Thousand Pesos (Php 50,000.00)”. How will this be determined and computed?

Section 2 of the Circular, under Other Infractions (b) provides “the fine to be imposed as a result of this infraction shall be in addition to the fine imposed for the original infraction subject of the Order, Resolution or Decision of the Commission”.

For instance, if a PIC or PIP fails to comply with the Order, Resolution or Decision imposing fine a for a Grave Infraction amounting to Php 1,000,000.00, it shall be liable for Other Infraction and subject to a Php 50,000.00 fine. Thus, the total amount payable will be Php 1,050,000.00 which represents the Grave Infraction and Other Infraction committed.

Another instance is when a PIC or PIP fails to abide by an Order to furnish documents issued by authorized officers of the

Commission, the PIC or PIP is still required to comply with the Order. Thus, it should submit the documents and pay the fine in an amount not exceeding Php 50,000.00.

The amount of the fine to be imposed, not exceeding Php 50,000.00, shall be determined by the Commission, taking into consideration Section 3 of the Circular on factors affecting fines.

8. Will a company be fined for acts of employees when the company has shown proof that it has implemented appropriate measures?

Yes, a company will be fined for the acts of its employees following the Accountability Principle. Pursuant to this, the Circular specifically covers only PICs or PIPs. Nevertheless, the company is not precluded from impleading or going after the concerned employee in a separate action or proceeding wherein it may show proof that it has implemented appropriate measures.

9. The Grave and Major Infractions penalizing the violation of Section 11 or Section 16 of the DPA are too broad and subject to different interpretations. Will the Commission issue further guidelines on these violations?

No, the Commission has issuances on the interpretation of these general privacy principles under Section 11 and data subject rights under Section 16 of the DPA, which will guide the PICs and PIPs in determining whether an infraction may have been committed. All parties will be given the opportunity to be heard, and due process will be observed in accordance with the NPC Rules of Procedure.

10. Would there be guidelines released per sector just to have a view of what are reasonable and appropriate for the Commission?

No, there will be no guidelines released per sector. The DPA, IRR and NPC issuances are deemed sufficient to inform the public of the appropriate and reasonable security measures expected of all PICs and PIPs.

The Commission shall evaluate PICs and PIPs based on the pleadings and evidence submitted to it. Thus, the compliance of the PICs and PIPs on appropriate and reasonable security measures shall be decided on a case-to-case basis.

- 11. Will the Commission consider a reasonable graduation per year in the imposition of maximum penalty to allow companies to adopt, make changes, and put in measures and processes to avoid a violation of the DPA and its implementing rules and regulations? This is still a relatively new law and not all companies have the expertise and/or system to fully comply with the applicable provisions.**

No, the DPA was enacted in 2012 and the Commission was constituted in 2016. Since then, the Commission has been actively promoting, educating, and assisting the stakeholders, such as the PICs and PIPs. Hence, there is no need to allow additional time for PICs and PIPs to adjust and prepare as the Commission has given these PICs and PIPs sufficient time and support to make the necessary changes, adjustments in processes and implement measures to comply with the law.

Section 3- Factors Affecting Fines

- 12. How will the Commission define the standard for determining the factors that affect fines? Will the Commission provide examples or specific circumstances that may be considered as aggravating or mitigating factors?**

No, the Commission will evaluate these factors on a case-to-case basis. The aggravating or mitigating factors will be decided on each case individually, according to the facts and circumstances presented before the Commission. Nevertheless, the Circular provides for a list of factors affecting fines to be imposed by the Commission. All circumstances that the PIC or PIP thinks should be considered for evaluation should be included in the pleadings submitted to the Commission.

- 13. Does the term “annual gross income” pertain to domestic income of the immediately preceding year of the infraction?**

Yes, for natural and juridical entities established in foreign jurisdictions that committed the infraction, the annual gross income only applies to the domestic income of the immediately preceding year of the infraction or only the income derived from sources within the Philippines.

On the other hand, for natural and juridical entities established in the Philippines, the “gross annual income” includes the income derived from all sources within and without the Philippines, in adherence to the definition of “gross annual income” under the Philippine laws on Taxation.

Section 4 – Due Process

14. Will the 2021 Rules of Procedure of the NPC apply?

Yes, as stated in Section 4 of the Circular, the Rules of Procedure of the NPC will apply. The applicable Rules of Procedure shall depend on whichever set of Rules of Procedure is in effect at the time the infraction is committed.

Section 5- Appeal

15. Will an appeal stay the execution and imposition of administrative fines?

No, an appeal will not stay the execution and imposition of administrative fines. Section 5 of the Circular provides that a Decision or Resolution of the Commission shall be immediately executory.

In any or all actions assailing the Decision or Resolution of the Commission pertaining to the imposition or execution of an administrative fine, the PIC or PIP may post a cash or surety bond equivalent to the total amount of fine imposed, exclusive of the damages, attorney’s fees, and other monetary awards, which shall result in the staying of the execution as provided in Section 6 of the Circular.

16. How will the PICs or PIPs pay for the fine imposed by the Commission?

The PICs or PIPs shall pay the fine imposed, in cash or manager’s check, through the Finance and Administrative Office (FAO) of the Commission.

Section 6- Posting of Bond on Imposed Administrative Fines

17. What will be the effect of the failure to post the cash or surety bond?

The non-posting of bond shall result in the immediate execution of the imposed administrative fine.

18. Are parties allowed to file a Motion to Reduce bond due to valid reasons?

No, the Commission will not entertain a Motion to Reduce bond for whatever reason.

Section 7- Refusal to Comply

19. Section 7 of the DPA and Section 4 of NPC Circular No. 20-02 on the Rules on the Issuance of Cease-and-Desist Orders (CDO) identify the specific parameters within which to issue a CDO. Refusal to pay is not a ground for the issuance of a CDO. How can the foregoing provision be reconciled with Section 7 of the Circular on Administrative Fines?

As worded, Section 7 of the Circular used the word “may” which highlights the Commission’s discretion to issue a CDO depending on the circumstances of each case. The Commission’s power to issue a CDO is rooted in the DPA. Following this, NPC Circular No. 20-02 provides for an initial list of the grounds for the issuance of a CDO. The Commission, through this Circular, provides an additional ground for the issuance of a CDO.

Section 10- Applicability Clause

20. Section 10 states that: “These rules apply to covered PICs and PIPs for the above infractions prospectively.” Does this mean that the Circular would not apply to pending cases?

Yes, the Circular does not apply to pending cases because it applies prospectively. Infractions committed before the issuance of the Circular shall not be covered by its provisions. Continuing infractions or those committed prior to the issuance of the Circular that exists even after its effectivity, however, are covered.

Administrative fines imposed on a PIC or PIP may arise not only from complaints filed against a PIC or PIP but also from a PIC or PIP's failure to comply with Commission orders, directives, or issuances.

Other Matters

21. Is the Commission authorized to impose administrative fines under the DPA?

Yes, the Commission is authorized to impose administrative fines. Section 7 of the DPA mandates the Commission to: (1) to ensure compliance of the PICs and PIPs with the DPA; (2) compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy; and (3) monitor compliance and recommend necessary action to meet minimum standards for protection of personal information.

First, taken together with the authority of the Commission to receive complaints, institute investigations, adjudicate, and award indemnity on matters affecting any personal information, these powers establish the Commission as a quasi-judicial authority with all the necessary and implied powers that come with it, such as the power to impose administrative fines.

Second, the authority of the Commission to impose administrative fines is explicitly provided under Section 9(f)(6) of the IRR.

Third, the authority of the Commission to impose administrative fines stems from long-standing doctrines in administrative law. Under the "doctrine of necessary implication," what is implied in a statute is as much as part thereof as that which is expressed. Every statutory grant of power, right or privilege is deemed to include all incidental powers, rights, or privileges. This includes all such collateral and subsidiary consequences as may be fairly and logically inferred from its terms.

Considering that the Commission exercises quasi-judicial functions as mandated by law, and that such function is integral to the overall authority to administer and implement the DPA, the Commission has the power to impose administrative fines.

22. Do the administrative fines supersede the penalties enumerated under Sections 25 to 33 of the DPA?

No, the administrative fines do not supersede the penalties enumerated under the DPA. On one hand, the penalties under Sections 25 to 33 of the DPA are criminal in nature, punishable by imprisonment or a fine, imposed by judicial courts, and only applicable to natural persons. The Commission may recommend prosecution to the Department of Justice but may not impose the criminal penalties itself.

On the other hand, the penalties found under the Circular are administrative in nature, not punishable by imprisonment, imposed by the Commission after due notice and hearing, and imposed on PICs or PIPs whether they are juridical or natural persons.



JOINT ADMINISTRATIVE ORDER NO. 22-01
Series of 2022

Subject: **GUIDELINES FOR ONLINE BUSINESSES REITERATING THE LAWS AND REGULATIONS APPLICABLE TO ONLINE BUSINESSES AND CONSUMERS**

WHEREAS, the COVID-19 pandemic has disrupted traditional business models and rearranged economic structures forcing the accelerated growth of e-commerce, along with the drastic rise in consumer complaints and fraudulent online transactions;

WHEREAS, the DTI launched the e-commerce Philippines 2022 Roadmap which aims to pursue an e-Commerce policy agenda to drive its objective of gaining the trust and confidence of the Filipinos in e-commerce to increase e-commerce transactions, and to help create a safer environment for online consumers and merchants facilitated by a strong digital consumer and merchant protection framework;

WHEREAS, Section 29 of Republic Act No. 8792, or the “Electronic Commerce Act”, authorizes the DTI to supervise the promotion and development of electronic commerce in the country together with relevant government agencies. Further, it shall promulgate rules and regulations, as well as provide quality standards or issue certifications, as the case may be, and perform such other functions as may be necessary for the implementation of Electronic Commerce Act;

WHEREAS, there is a need to issue a policy directive to implement existing and prevailing trade and industry laws to address the need to improve the regulation of online selling activities, inform online sellers, merchants, or e-retailers about the equal treatment of the law of online and offline businesses, and ensure that they are reminded of the general laws and regulations that may apply to their on line business;

WHEREAS, pursuant Executive Order No. 292, or the Administrative Code of 1987:

1. The Department of Trade and Industry (DTI) shall formulate and implement policies, plans, and programs relative to the regulation of trade, industry, and investments, and protect consumers from trade malpractices and from substandard or hazardous products;
2. The Department of Agriculture (DA) shall promulgate and enforce all laws, rules and regulations governing the conservation and proper utilization of agricultural and fishery resources, and be responsible for the planning, formulation, execution, regulation, and monitoring of programs and activities relating to agriculture, food production and supply;
3. The Department of Health (DOH) shall be primarily responsible for the formulation, planning, implementation, and coordination of policies and programs in the field of health. Its primary function is the promotion, protection, preservation or restoration of the health of the people through the provision and delivery of health services and through the regulation and encouragement of providers of health goods and services. The DOH shall issue orders and regulations concerning the implementation of established health policies;
4. The Department of Environment and Natural Resources (DENR) formulate, implement and supervise the implementation of the government's policies, plans, and programs pertaining to the management, conservation, development, use and replenishment of the country's natural resources. It shall promulgate rules and regulations in accordance with law governing the exploration, development, conservation, extraction, disposition, use and such other commercial activities tending to cause the depletion and degradation of our natural resources;

WHEREAS, Executive Order No. 913, dated 07 October 1983, vests in the DTI the power to promulgate rules and regulations to implement the provision and intent of "trade and industry laws." Even prior to the commencement of a formal investigation on a violation of any trade and industry law, the DTI Secretary has the power to issue orders on seizures, padlocking, withholding, holding of any craft or vessel, prevention of departure, and such other preventive measures and other similar orders;

WHEREAS, Section 125 of Executive Order No. 94, dated 04 October 1947, vests in the DOH the protection of the health of the people, the maintenance of sanitary conditions, and the proper enforcement of

the laws and regulations relative to health, sanitation, food, drugs and narcotics, slum housing, garbage and other waste disposal;

WHEREAS, the Food and Drug Administration (FDA), pursuant to Section 5 (e), and (o) of Republic Act No. 9711 or the “Food and Drug Administration Act of 2009”, as an office under the DOH, has the power: (1) to issue certificates of compliance with technical requirements to serve as basis for the issuance of appropriate authorization and spot-check for compliance with regulations regarding operation of manufacturers, importers, exporters, distributors, wholesalers, drug outlets, and other establishments and facilities of health products, as determined by the FDA; (2) to conduct, supervise, monitor and audit research studies on health and safety issues of health products undertaken by entities duly approved by the FDA; and (3) to prescribe standards, guidelines, and regulations with respect to information, advertisements and other marketing instruments and promotion, sponsorship, and other marketing activities about the health products as covered in the said Act;

WHEREAS, pursuant to Article 6 of Republic Act No. 7394, or the Consumer Act of the Philippines, the DTI established the CONSUMERNET, on 12 November 1996, in order to facilitate the flow of consumer protection information and to provide a speedy resolution of consumer complaints;

WHEREAS, Republic Act No. 8293, or the “Intellectual Property Code of the Philippines”, mandates the Intellectual Property Office of the Philippines (IPOPHL) to coordinate with other government agencies and the private sector efforts to formulate and implement plans and policies to strengthen the protection of intellectual property rights in the country and. administratively adjudicate contested proceedings affecting intellectual property rights. The IPOPHL protects and secures the exclusive rights of scientists, inventors, artists and other gifted citizens to their intellectual property and creations. The Intellectual Property Code of the Philippines grants similar protection to nationals of treaty partners of the Philippines, especially in the area of repression of unfair competition. The Bureau of Legal Affairs of the IPOPHL is authorized to order provisional remedies in accordance with the Rules of Court, such as Preliminary Attachment, Preliminary Injunction, Temporary Restraining Order, and Replevin;

WHEREAS, Republic Act No. 10173, or the “Data Privacy Act of 2012”, authorizes the National Privacy Commission (NPC) to coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country;

WHEREAS, on 09 March 2020, the Philippines, through the NPC, became an official participant in the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (CBPR) system, committing itself to protect personal data through enforceable standards, accountability, risk-based protections, consumer-friendly complaints handling, consumer empowerment, consistent protection, and cross-border enforcement cooperation;

NOW, THEREFORE, pursuant to the above-mentioned, and subject to the limitations of their mandates conferred by law, the DTI, DA, DENR, DOH, IPOPHL, NPC, hereby promulgate the following guidelines through this Joint Administrative Order (JAO).

I. PRELIMINARY PROVISIONS

SEC. 1. OBJECTIVE.

This JAO aims to increase consumer confidence in business-to-consumer (B2C) and business-to-business (B2B) e-commerce transactions. It seeks to ensure that eCommerce platforms, electronic retailers (e-retailers), and online merchants are properly guided about the rules, regulations, and responsibilities in the conduct of their online business, considering the need to protect consumers against deceptive, unfair, and unconscionable sales acts and practices. Moreover, the purpose of this JAO is to ensure that online consumers are informed of their rights and the mechanisms for redress.

SEC. 2. SCOPE AND COVERAGE.

This JAO effectively reiterates existing policies, procedures and guidelines that should apply to online businesses. This JAO likewise integrates the procedures and remedies that online consumers are entitled to.

This JAO shall cover all online businesses, whether natural or juridical,

formal or informal, that are engaged in electronic transactions, including, but not limited to the sale, procurement, or availment of goods, digital content/products, digital financial services, entertainment services, online travel services, transport and delivery services, and education services. Further, online businesses shall include but shall not be limited to e-commerce platforms, online sellers, merchants, e-marketplaces, and a-retailers as defined in Section 4 of this JAO.

SEC. 3. APPLICABILITY OF LAWS AND REGULATIONS.

The laws applicable to physical or offline businesses are, as far as practicable, equally applicable to online businesses. Violations of relevant and pertinent laws governing commerce, including but not limited to the Consumer Act of the Philippines, Electronic Commerce Act, and Data Privacy Act of 2012 shall be penalized with the same penalties as provided in the applicable laws.

Unless expressly specified, nothing in this JAO shall be construed as to diminish or deprive the regulatory jurisdiction conferred by law upon other government agencies, including Local Government Units (LGUs).

SEC. 4. DEFINITION OF TERMS.

As used in this JAO, the following terms are defined to mean:

- 4.1 Business to Business (B2B) transaction** - refers to internet transactions conducted over marketplaces that facilitate business to business electronic sales of new and used merchandise using the internet.
- 4.2 Business to Consumer (B2C) transaction** - refers to the act or process of selling or providing goods or services by businesses to consumers, whether for a profit or not;
- 4.3 Consumer** - refers to a person who is a purchaser, lessee, recipient, or prospective purchaser, lessor or recipient of consumer products, services, advertising or promotion, credit, technology, and other items in e-commerce;
- 4.4 Derivatives** - refer to a substance or material extracted or taken from wildlife such as but not limited to blood, saliva, oils,

resins, genes, gums, honey, cocoon, fur, tannin, urine, serum, spores, pollen and the like; a compound directly or indirectly produced from wildlife and/or products produced from wildlife and wildlife products.

4.5 Digital financial services - refer to services of a financial nature that are made available to the public through the internet, including banking services, insurance and insurance-related services, payment and money transmission services, remittance services, lending services, investment services, and other similar or related services;

4.6 Digital content or product - refers to data which is produced and supplied in electronic form;

4.7 Education service - refers to services designed to promote, impart, share, source, or review knowledge, and to those intended to assist, facilitate, or improve learning, through an online platform, application, website, webpage, social media account, or other similar platform operated by the provider for profit, regardless of whether the provider is authorized to engage in eCommerce in the Philippines. Moreover, it is commonly referring to four categories: Primary Education Services; Secondary Education Services; Higher (Tertiary) Education Services; and Adult Education;

4.8 Electronic commerce or e-commerce - refers to the production, distribution, marketing, sale, or delivery of goods and services by electronic means;

4.9 Electronic data message - refers to information generated, sent, received or stored by electronic, optical or similar means;

4.10 Electronic transaction - refers to the sale or purchase of goods or services, whether between businesses, households, individuals, governments, and other public or private organizations, conducted over computer-mediated networks. The goods and services are ordered over those networks, but the payment and the ultimate delivery of the goods or services may be conducted online or offline.

4.11 E-Commerce platform - refers to a natural or juridical person

that solicits or facilitates the purchase, procurement, or use of goods and services, with the presence and use of monetary transactions, including using, developing, creating, or promoting digital content through digital platforms, websites, and marketplaces, with functions which connects and encourages consumers, online merchants, sellers, and retailers to enter into commercial transactions.

4.12 E-marketplace - refers to an online intermediary that allows participating merchants to exchange information about products or services to enter into an electronic commerce transaction, which may or may not provide information/services about payments and logistics;

4.13 E-retailer - refers to an organization selling products or services directly to customers online.

4.14 Goods - refer to physically or digitally produced items over which ownership rights may be established, and whose economic ownership may be passed from one to another by engaging in transactions; For purposes of this JAO, goods shall include, but not be limited to live animals and seeds.

4.15 Online business - refers to any commercial activity over the internet, whether buying or selling goods and/or services directly to consumers or through a platform, or any business that facilitates commercial transactions over the internet between businesses and consumers. Online businesses shall include e- Commerce platforms, a-marketplace, online sellers/merchants and eretailers (e- tailers) as defined in this section.

4.16 Online travel services - refer to services that facilitate the reservation, purchase or discounting of flights, hotel accommodations, and vacation rental spaces, through an online platform, application, website, webpage, social media account, or other similar platform operated by the provider, regardless of whether the provider is authorized to engage in e-commerce in the Philippines.

4.17 Online seller or merchant - refers to an organization or retailer selling products or services to customers through an e-marketplace.

4.18 Transport and Delivery Service - refers to the delivery of food, goods or other merchandise, or of personal transport services and other courier services, contracted through an online platform, application, website, webpage, social media account, or other similar platform operated by the provider, regardless of whether the provider is authorized to engage in e-commerce in the Philippines.

4.19 Wildlife - refers to wild forms and varieties of flora and fauna, in all developmental stages, including those which are in captivity or are being bred or propagated.

4.20 Wildlife by-product - refers to any part taken from wildlife species such as meat, hides, antlers, feathers, leather, fur, internal organs, bones, roots, trunks, barks, petioles, leaf fibers, branches, leaves, stems, flowers, scales, scutes, shells, coral parts, carapace and the like, or whole dead body of wildlife in its preserved/stuffed state, including compounds indirectly produced in a biochemical process or cycle.

II. RESPONSIBILITIES OF ONLINE BUSINESSES AND PROTECTION OF CONSUMERS

SEC. 5. RESPONSIBILITIES OF ONLINE BUSINESSES.

To build trust in e-commerce and to protect and uphold the interest of consumers at all times, online businesses shall comply with all Philippine laws, rules and regulations, bearing in mind the following principles of the ASEAN Online Business Code of Conduct:

5.1 Fair Treatment of Consumers. Online businesses shall refrain from illegal, fraudulent, unethical, or unfair business practices that may harm consumers. **5.2 Upholding Responsibilities.** Online businesses shall value consumer rights to the same extent as traditional brick-and-mortar businesses.

5.2 Upholding Responsibilities. Online businesses shall value consumer rights to the same extent as traditional brick-and-mortar businesses.

- 5.3 Compliance with Laws and Regulations.** Online businesses shall observe and comply with the policies, laws and regulations in the countries where their goods and services are marketed.
- 5.4 Conformance to Local Standards.** Online businesses shall apply the necessary standards and provide accurate information in the local language of the countries where their goods and services are marketed.
- 5.5 Ensured Quality and Safety.** Online businesses shall ensure shared responsibility along the entire supply chain. They shall not compromise product, health, and food safety, not offer products which have been recalled, banned or prohibited, and shall ensure that their services are of highest quality.
- 5.6 Honest and Truthful Communication.** Online businesses shall provide easily accessible, complete, and correct information about their goods and services, and adhere to fair advertising and marketing practices.
- 5.7 Price Transparency.** Online businesses shall ensure transparency and openness regarding their prices, including any additional costs, such as customs duties, currency conversion, shipping, delivery, taxes, service/processing fees, and convenience fees.
- 5.8 Proper Recordkeeping.** Online businesses shall keep proper records of purchase, provide complete records of the goods purchased, and have them delivered in the promised time and described condition.
- 5.9 Review and Cancellation Options.** Online businesses shall offer options to allow consumers to review their transactions prior to final purchase, and of cancellation and allow consumers to review their transaction before making the final purchase, and to withdraw from a confirmed transaction in appropriate circumstances. Fraudulent acts both by on line businesses and consumers shall be dealt with in accordance with existing penal/special laws.
- 5.10 Responsive Consumer Complaint and Redress System.** Online businesses shall take consumer complaints seriously, establish a fair and transparent system to address complaints,

and provide appropriate compensation, such as refund, repair, and/or replacement.

5.11 Consumer Information Security. Online businesses shall secure the personal information of consumers, actively protect their privacy, be transparent about processing personal data, and if appropriate under the circumstances, ask for permission prior to any personal data processing activity.

5.12 Online Payment Security. Online businesses shall ensure that online payments used are safe and secure. They shall safeguard sensitive data by choosing digital payment platforms with the appropriate secure technology and protocols, such as encryption or SSL, and display trust certificates to prove it.

5.13 Desistance from Online Spamming. Online businesses shall avoid online spamming. They shall allow consumers to choose whether they wish to receive commercial messages by e-mail or other electronic means, and provide adequate mechanisms for them to opt-out from the same.

5.14 Non-proliferation of Fake Online Reviews. Online businesses shall not restrict the ability of consumers to make critical or negative reviews of goods or services, or spread wrong information about competitors.

5.15 Consumer Education on Online Risks. Online businesses shall educate consumers about (online) risks. They shall help consumers in understanding the risks of online transactions, and provide competent guidance if needed.

SEC. 6. PROTECTION OF ONLINE CONSUMERS AGAINST HAZARDS TO HEALTH AND SAFETY.

Online businesses are reminded of the following laws, among others, in order to protect the public against hazards to health and safety:

1. RA. No. 4109 otherwise known as the “Standards Law” shall also apply to all online businesses. This includes compliance to all Department Administrative Orders issued by DTI particularly the Technical Regulations issued to ensure and certify product quality and safety.

2. RA. No. 9211 or the “Tobacco Regulation Act of 2003” and E.O. No. 106 s. 2020, shall also apply to ensure that online businesses abide with the restrictions set forth on advertising, promotions, and access of minors, in order to further protect the consumers against the hazards to health and safety of tobacco, vapor products and heated tobacco products.
4. RA. No. 10611 or the “Food and Safety Act of 2013”, P.O. No. 1619 s. 1979, and FDA Circular No. 2019-006, shall also apply to ensure that online businesses abide with the restrictions set forth on advertising and promotions and access of minors, in order to further protect the consumers against the hazards to health and safety of alcoholic beverages.
6. DA regulations such as, but not limited to, proper handling and stewardship shall also apply to the offer and sale of agricultural products online, such as fertilizers, and pesticides, whether conventional, biotech-traited or those with plant incorporated protectants.
8. All online businesses must comply with DTI Memorandum Circular No. 21-05, series of 2021 which enumerates the eighty-seven (87) products and systems covered under the BPS Mandatory Product Certification Schemes, and classified into three (3) product groups - Electrical and Electronic Products, Mechanical/Building and Construction Materials, and Chemical and Other Consumer Products and Systems. The latest list of products is attached as Annex A. Such list may be updated or revised by the BPS in accordance with its mandate.
10. Requirement for products covered under the DTI-BPS Mandatory Certification Schemes.
 - 6.6.1 Online platforms, including its sellers, merchants, or a-retailers engaged in the sale of products covered under the DTI Bureau of Philippine Standards (DTI-BPS) Mandatory Product Certification Schemes shall ensure that such products sold in online platforms bear a valid Philippine Standard (PS) Quality and/or Safety Certification Mark, Import Commodity Clearance (ICC) sticker, or any certification mark approved and issued by the DTI-BPS.

6.6.2 Manufacturers and importers of the products covered under the BPS Mandatory Certification Schemes shall secure the PS Mark or ICC stickers from the BPS. Only the manufacturer or importer to whom the PS License or ICC certificate is granted shall be allowed to affix the PS Mark or ICC sticker, respectively, on their products consistent with the requirements of the DTI Department Administrative Order (DAO) No. 4, Series of 2008, DAO No. 5, Series of 2008, their respective Implementing Rules and Regulations and other applicable DTI technical regulations related to the BPS Mandatory Product Certification Schemes. The matrix of requirements and procedure to apply for a PS Mark License, ICC certificate and stickers, is attached as **Annex B**.

SEC. 7. PROTECTION OF ONLINE CONSUMERS AGAINST DECEPTIVE, UNFAIR AND UNCONSCIONABLE SALES AND PRACTICES.

Online businesses are reminded of the following laws, among others, in order to protect the public against deceptive, unfair and unconscionable sales acts and practices:

7.1 Prohibition Against Deceptive Online Sales Acts or Practices
- Online businesses are covered by Article 50 of RA. No. 7394 and Sections 155. 1, 155.2, and 165.2(b) of RA. No. 8293 or otherwise known as the “Intellectual Property Code of the Philippines”, which declare deceptive acts or practices by a seller or supplier in connection with a consumer transaction as a violation. This shall occur before, during or after the transaction, in cases where:

7.1.1. A consumer product or service has the sponsorship, approval, performance, characteristics, ingredients, accessories, uses, or benefits it does not have;

7.1.2. A consumer product or service is of a particular standard, quality, grade, style, shape, size, color, or model when in fact it is not;

7.1.3 A consumer product is new, original or unused, when in fact, it is in a deteriorated, altered, repacked, unlabeled,

mislabeled, unknown, reconditioned, reclaimed or second-hand state;

7.1.4 A consumer product or service is available to the consumer for a reason that is different from the fact;

7.1.5 A consumer product or service has been supplied in accordance with the previous representation when in fact it is not;

7.1.6 A consumer product or service can be supplied in a quantity greater than the supplier intends;

7.1.7 A service, or repair of a consumer product is needed when in fact it is not;

7.1.8 A specific price advantage of a consumer product exists when in fact it does not;

7.1.9 The sales act or practice involves or does not involve a warranty, a disclaimer of warranties, particular warranty terms or other rights, remedies or obligations if the indication is false;

7.1.10 The seller or supplier represents that he has a sponsorship, approval, or affiliation he does not have;

7.1.11 The seller or supplier of a product or service has used a trademark, trade name, or other identifying mark, imprint, or device, or any likeness thereof, without the authorization of the owner;

7.1.12 The seller or supplier of a product is not authorized by the trademark holder as a distributor/retailer/seller of the product;

7.1.13 The seller or supplier uses the traditional knowledge of indigenous people on wild food plants, medicinal plants, and animal parts, in sales promotions or trade, without their prior written consent or acknowledgment; and

7.1.14 The seller or supplier misrepresents their products as proprietary, having regulatory approval, or legally compliant with existing laws and regulations when in fact they are not.

7.2 Unfair or Unconscionable Sales Act or Practice - Online businesses are also covered by Article 52 of RA. No. 7394 and Sections 155.1, 155.2, and 165.2(b) of RA. No. 8293 when the seller induces the consumer to enter into a sales or lease transaction grossly inimical to the interests of the consumer or grossly one-sided in favor of the on line seller, merchant, or a-retailer by taking advantage of the consumer's physical or mental infirmity, ignorance, illiteracy, lack of time or the general conditions of the environment or surroundings. In determining whether an act or practice is unfair and unconscionable, the following circumstances shall be considered:

7.2.1 That the producer, manufacturer, distributor, supplier or seller took advantage of the inability of the consumer to reasonably protect his interest because of his inability to understand the language of an agreement, or similar factors;

7.2.2 That when the electronic transaction was entered into, the price grossly exceeded the price at which similar products or services were readily obtainable in similar transaction by like consumers;

7.2.3 That when the electronic transaction was entered into, the consumer was unable to receive a substantial benefit from the subject of the transaction;

7.2.4 That the transaction that the seller or supplier induced the consumer to enter into was excessively one-sided in favor of the seller or supplier; and

7.2.5 That the consumer was misled into purchasing a product or availing of a service by reason of the unauthorized use by the supplier or seller of a trademark, trade name, or other identifying mark, imprint, or device, or any likeness thereof, and which thereby falsely purports or is represented to be the product or service of another.

SEC. 8. RESPONSIBILITIES OF ONLINE BUSINESSES ON CONSUMER PRODUCT AND SERVICE WARRANTIES, PRICE TAG PLACEMENT, AND LABELING.

- 8.2 Consumer Product and Service Warranty - Online businesses shall comply with the pertinent rules on provision of warranty under the Civil Code and under Title III of R.A. No. 7394.
- 8.2 Labeling Requirements - Online businesses shall comply with the following labeling requirements under R.A. No. 7394, R.A. No. 9711, and other pertinent and relevant laws:
 - 8.2.1 The minimum labelling requirements for consumer products whether manufactured locally or imported under Article 77 ;
 - 8.2.2 Additional labeling and packaging requirements necessary to prevent the deception of the consumer or to facilitate value comparisons as to any consumer product under Article 79;
 - 8.2.3 Additional labelling requirements for food under Article 84;
 - 8.2.4 Labeling of drugs under Article 86 and Section 6 of RA No. 667 5, as amended by RA No. 9502 otherwise known as the “Universally Accessible Cheaper and Quality Medicines Act of 2008”;
 - 8.2.5 Additional labeling requirements for cosmetics under Article 87;
 - 8.2.6 Breastmilk substitutes and breastmilk supplements shall follow the guidelines set in the Milk Code, in terms of labelling (Section 1 O of EO 51);
 - 8.2.7 Toys shall comply with the appropriate provisions on safety labelling and manufacturer’s markings found in the Philippine National Standards for the safety of toys (Section 4 of RA No. 10620 otherwise known as the “Toy and Game Safety Labeling Act of 2013”);

- 8.2.8 Household urban hazardous substances must bear warning labels particular to the hazards they present (Chapter IV/Article 91 of RA No. 7394, Section 1.n. of Presidential Decree (PD) No. 881);
 - 8.2.9 Vaping products and heated tobacco products must bear Graphic Health Warnings (Sec. 1 of RA. No. 11346);
 - 8.2.10 Labeling requirements for tobacco products under RA. No. 9211; and
 - 8.2.11 Labeling requirements for alcoholic beverages under RA. No. 10611 and FDA Circular No. 2019-006.
- 8.3 Price Tag Placement - Pursuant to Articles 81 and 83 of RA. No. 7394, the following rules and regulations shall apply to online businesses as regards the price of the product or service offered online:
- 83.1 Product listings by a-retailers or merchants on marketplace/ platforms must contain the price(s) of the product/service in Philippine pesos and must display payment policies, delivery options, returns, refunds and exchange policy, and other charges if applicable;
 - 8.3.2 Total price must be displayed. It must be clear, updated and accurate to avoid misleading online consumers;
 - 8.3.3 Indicate the price in high visibility areas preferably near the product title, or the add-to-cart button and ensure the text used for the price is readable and accessible; and
 - 8.3.4 The practice of providing prices through private (or direct) messages to consumers/buyers is considered a violation of the Price Tag Law.

SEC. 9. REGULATED, RESTRICTED, AND PROHIBITED ITEMS.

Online businesses shall exhibit the corresponding license or permit number as regards the regulated items for sale as prescribed by regulatory agencies. Provided that, delivery platforms shall not be liable for transport of these items when the same cannot, on the face of the package be determined to be in violation of this clause. The liability of the delivery platform in this instance shall be limited to those provided in Section 13.

Online businesses shall not produce, import, distribute, market, sell or transport prohibited goods or services, which are those specifically prohibited by law, such as, but not limited to counterfeit goods and products, precious metals and conflict minerals, weapons, artifacts, sexual services, seditious or treasonous materials, and other such goods and services. Attached hereto as Annex C is a non-exhaustive list of the regulated, restricted, and prohibited items for reference. This list may be revised or updated by the relevant regulatory agencies concerned.

SEC.10. DATA PRIVACY.

This JAO defines the responsibilities of online sellers, merchants, or e-retailers under RA No. 10173, otherwise known as the Data Privacy Act, which seeks to ensure privacy protection to ensure transparency, legitimate purpose, and proportionality in data collection and processing. Through the NPC, the law regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of personal data.

- 10.1 Online sellers, merchants, or a-retailers particularly those that sell through their own websites, or through social media marketplaces are expected to handle all personal data of their consumers with the utmost care and respect;
- 10.2 Personal information collected by the on line sellers, merchants, or e-retailers shall be retained only for as long as necessary:
 - a. For the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
 - b. For the establishment, exercise or defense of legal claims;
 - c. For legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency; or
 - d. As provided by law;

- 10.3 Personal data shall be disposed of or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects. Security measures for the protection of personal data should be implemented;
- 10.4 Online sellers, merchants, or e-retailers shall publish/post in their websites or online platforms, or any other similar platform, a Privacy Notice which shall provide consumers with information regarding the purpose and extent of the processing of their personal data in relation to their transactions, including if applicable, any data sharing, profiling, direct marketing, or the existence of automated decision-making, as well as any other authorized further processing;
- 10.5 Online merchants that operate their own online application, or any other similar platform are prohibited from asking unnecessary permissions from the consumers;
- 10.6 Prior to the collection of personal data of the consumers, the on line sellers, merchants, or e-retailers must determine the most appropriate lawful criteria for such processing, which in the case of sale-related processing need not necessarily be consent. In such a case, processing may still be lawful if based on a contract or legitimate interest of either or both the seller and the buyer;
- 10.7 All personal data supplied by consumers to online sellers, merchants, or e-retailers shall be secured through the implementation of reasonable and appropriate security measures intended for the protection of personal data and shall not be used for purposes not authorized by the consumers;
- 10.8 Upon collection and processing of the personal data, the on line sellers shall inform the consumers of their data privacy rights under the Data Privacy Act, namely:
- a. Right to information
 - b. Right to object
 - c. Right to access

- d. Right to correct
 - e. Right to erase
 - f. Right to damages
 - g. Right to data portability
 - h. Right to file a complaint
- 10.9 Upon request by public authorities pursuant to their respective mandates and in accordance with the provisions of the Data Privacy Act of 2012, on line sellers, merchants, or e-retailers may lawfully disclose personal information to said public authorities, provided, that the request particularly describes the personal information asked for and indicate the relevance of such information to an ongoing investigation.

III. LIABILITIES OF ONLINE BUSINESSES

SEC. 11. LIABILITY FOR DEFECTIVE PRODUCT AND SERVICE.

Online businesses are covered by Title 111, Chapter V of the RA No. 7394, particularly Article 98 (in relation to Article 97) which provides for the liability of the manufacturer, producer, importer, or seller of defective products.

- 11.1 Online merchants or sellers are liable when it is not possible to identify the manufacturer, builder, producer or importer of a defective product;
- 11.2 Online merchants or sellers shall be held liable when the product is supplied, without clear identification of the manufacturer, producer, builder or importer; and
- 11.3 Online merchants or sellers shall be held liable when the perishable goods were not adequately preserved.

SEC. 12. LIABILITY FOR THE SALE OF COUNTERFEIT AND PIRATED GOODS.

The online sale of fake and/or pirated goods is a violation of R.A. No. 8293 and R.A. No. 8203, otherwise known as the “Special Law on Counterfeit Drugs.” Online businesses shall only sell original, genuine, licensed, or unexpired goods.

- 12.1 Should any person holding Intellectual Property (IP) rights, whether or not engaged in selling of goods or services, find that their protected works, creations, designs, trademarks, patented inventions, or other IP are being infringed by unauthorized sellers or merchants online, they may request the online e-Commerce platforms being used by the infringer to take down the infringing goods/contents. In the event that the online e-commerce platform fails to respond to the take down request of the Intellectual Property (IP) rights holder, the rights holder may notify the IPOPHL for appropriate action.
- 12.2 E-commerce platforms have the authority to enforce the rights of the IP holder, in accordance with their internal guidelines. The usual modes of enforcement by platforms include temporary or permanent suspension or restriction of the infringing seller's accounts.
- 12.3 Reports or complaints of possible infringement shall be transmitted by the DTI to the brand owners so that they may check and report the same to the IPOPHL for action.
- 12.4 In addition to the IPOPHL, complaints regarding counterfeit and pirated goods may also be brought before other regulatory agencies having jurisdiction over the same such as, but not limited to, the Optical Media Board and the FDA.
- 12.5 The following persons shall be liable for violations of RA. No. 8203:
- 12.5.1 The manufacturer, exporter or importer of the counterfeit drugs and their agents, Provided, That the agents shall be liable only upon proof of actual or constructive knowledge that the drugs are counterfeit;
- 12.5.2 The seller, distributor, trafficker, broker or donor and their agents, upon proof of actual or constructive knowledge that the drugs sold, distributed, offered or donated are counterfeit drugs;
- 12.5.3 The possessor of counterfeit drugs as provided in Section 4 (b) of R.A. No. 8203;

12.5.4 The manager, operator or lessee of the laboratory or laboratory facilities used in the manufacture of counterfeit drugs;

12.5.5 The owner, proprietor, administrator or manager of the drugstore, hospital pharmacy or dispensary, laboratory or other outlets or premises where the counterfeit drug is found who induces, causes or allows the commission of any act herein prohibited;

12.5.6 The registered pharmacist of the outlet where the counterfeit drug is sold or found, who sells or dispenses such drug to a third party and who has actual or constructive knowledge that said drug is counterfeit; and

12.5.7 Should the offense be committed by a juridical person the president, general manager, the managing partner, chief operating officer or the person who directly induces, causes or knowingly allows the commission of the offense shall be penalized.

SEC. 13. LIABILITY OF E-COMMERCE PLATFORMS AND E-MARKETPLACES.

13.1 E-Commerce platforms, a-marketplaces, and the like, shall be treated, and shall be held liable, in the same manner as online sellers, merchants, and a-retailers, when the latter commits any violation of the laws implemented by these rules.

E-commerce platforms, a-marketplaces, and the like, shall verify if the goods sold by online sellers or merchants, and e-retailers, in their respective platforms are regulated, prohibited, original, genuine, licensed, or unexpired.

13.2 In case of a prima facie violation of any pertinent laws or regulations committed in an online post by the online seller or merchant, a-retailer, e-commerce platform, a-marketplace, and the like, the concerned authorized agency shall issue a notice giving the violator a maximum period of three (3) calendar days from receipt thereof, within which to take down such post, without prejudice to the filing of appropriate

administrative actions against all violators.

Failure to take down the post within three (3) calendar days shall be construed as an intentional and overt act that shall aggravate the offense charged.

13.3 The written notice shall indicate specific information, such as, but not limited to:

- a. the URL of the content in question;
- b. relevant provision or information on the asserted rights or law infringed or violated; and
- c. brief explanation of why the content infringes or violates rights or the law.

13.4 E-commerce platforms, e-marketplaces, and the like, may appeal the take down notice, following the procedures set under the applicable laws if, in their reasonable determination, there is no violation of any law or regulation. However, no reposting may be allowed pending appeal.

13.5 Delivery platforms shall be liable in the same manner as, online sellers, merchants, and a-retailers only upon notice that they are carrying or delivering restricted, prohibited or infringing items.

13.6 The term “use in commerce” under Section 155.1 of RA. No. 8293 shall include the act of sending marketing emails, publishing advertisements online or through traditional media, and similar acts designed to solicit business. The use of registered marks as well as copies or reproductions thereof in marketing emails and advertisements, without the authority of the trademark owner, shall be deemed an act of infringement under Section 155.1 of R.A. No. 8293.

13.7 In general, it shall be unlawful for a-Commerce platforms, a-marketplaces, and the like, to:

- a. Disseminate or to cause the dissemination of any

false, deceptive or misleading advertisement by mail or in commerce by print, radio, television, outdoor advertisement, or any other medium, for the purpose of inducing or which is likely to induce directly or indirectly the purchase of products or services;

- b. Advertise any food, drug, cosmetic, device, or hazardous substance in a manner that is false, misleading or deceptive, or is likely to create an erroneous impression regarding its character, value, quantity, composition, merit, or safety;
- c. Advertise any food, drug, cosmetic, device, or hazardous substance, unless such product is duly registered and approved by the concerned department for use in any advertisement.

13.8 Regulatory Agencies shall designate in writing their respective point of contact, who shall be fully authorized to issue notice of violations to digital platforms and/or a-marketplaces. Moreover, all regulatory agencies shall submit the names of the designated point persons, including their contact details (verified email address and mobile numbers) to DTI-E-commerce Division (DTI-ECD), for consolidation, within 7 days from the effectivity of this JAO.

In case there will be changes on the designated point/focal persons, including their contact details (verified email address and active mobile numbers), the same shall be conveyed to DTI-ECD, immediately.

13.9 Upon the effectivity of this JAO, a-Commerce platforms and a-market places are directed to enact and strictly enforce internal mechanisms or rules aimed to prohibit online sellers or merchants, previously found administratively liable for violation of any pertinent law, rule or regulation, from further selling, posting or offering items for sale in their respective platforms.

Failure to enact, or strictly enforce, such internal mechanisms or rules shall be construed as an intentional and overt act that shall aggravate the offense charged.

IV. RESPONSIBILITIES OF GOVERNMENT AGENCIES

SEC. 14. RESPONSIBILITIES OF CONCERNED GOVERNMENT AGENCIES.

The provisions of this JAO shall be implemented in full effect by the concerned government agencies, in the exercise of their mandate and jurisdiction, in order to establish a trustworthy and conducive a-Commerce environment. Some of these agencies are:

- 14.1 **The Department of Trade and Industry (DTI)**, with respect to registration and monitoring of online sellers, merchants, or a-retailers including handling of consumer complaints.
- 14.2 **The Department of Agriculture (DA)**, with respect to the monitoring and regulation of the manufacture and marketing of agricultural products for the protection of the public from the inherent risk of these products; and in the promotion and protection of animal health and welfare. This shall cover the following pertinent DA offices: (1) the Fertilizer and Pesticide Authority (FPA) for fertilizers, pesticides and seeds with pip and (2) the Bureau of Plant Industry (BPI) for seeds.
- 14.3 **The Department of Environment and Natural Resources (DENR)**, with respect to the monitoring and regulation of the importation, manufacture, processing, handling, storage, transport, sale, distribution, use and disposal of forest products, derivatives, wildlife by-products, chemical substances, mixtures, and chain saws that present unreasonable risk or injury to health or to the environment in accordance with national policies and international commitments.
- 14.4 **The Department of Health (DOH)**, through the Food and Drug Administration (FDA), with respect to the regulation of the manufacture, importation, exportation, distribution, sale, offer for sale, transfer, promotion, advertisement, sponsorship of, and/or use and testing of health products, including food, drugs, cosmetics, devices, biologicals, vaccines, in-vitro diagnostic reagents, household/urban hazardous substances, household/urban pesticides, toys and childcare articles to protect the health of the consumer.

- 14.5 **The Intellectual Property Office of the Philippines (IPOPHL)**, with respect to the protection of intellectual property rights in the conduct of e-commerce and its coordination with online a-Commerce platforms and brand owners in the implementation of the Memorandum of Understanding addressing counterfeit and pirated goods online.
- 14.6 **The National Privacy Commission (NPC)**, with respect to the protection of data privacy rights and regulation of the processing of personal data in the conduct of e-commerce transactions.

SEC. 15. JOINT UNDERTAKING OF GOVERNMENT AGENCIES.

This JAO shall enjoin all government agencies concerned to coordinate and assist in the enforcement of this JAO, in respect to the matters falling under their respective jurisdictions.

The above-mentioned government agencies shall undertake the following:

- 15.1 Work with a-Commerce platforms to establish a mechanism to prevent or remove or take down, within a reasonable period, listings on online platforms of prohibited or regulated but unregistered products;
- 15.2 Implement advocacy campaigns for consumers and businesses on government regulations relative to the marketing, distribution and sale of regulated products;
- 15.3 Explore the possibility of jointly developing a system with a-Commerce platforms, including the use of an Application Programming Interface (API), that will link each Party's respective systems to facilitate the transfer of information regarding listing of keywords, images, and other information on regulated products for regular sweeping by the online platforms; and
- 15.4 Develop a system to exchange intelligence/information on prohibited and regulated items monitored online, including automatic sharing of information with the appropriate regulatory agency, on possible violations detected/discovered. this may include the sharing of and access to a database of products/ items containing sufficient information, keywords, content, for the purpose.

V. REMEDIES OF CONSUMERS

SEC.16. PROVISION OF ADEQUATE RIGHTS AND MEANS OF REDRESS.

16.1 **NO WRONG-DOOR POLICY** - In accordance with Department Administrative Order No. 20-02, series of 2020, any consumer complaint filed with the DTI, whether or not the subject matter falls under its jurisdiction, shall be accepted for appropriate assistance, subject to the limitations imposed by law. The Department shall assist the consumer by guiding them to and forwarding their complaint to the appropriate agency having proper jurisdiction over the subject matter.

16.2 **CONSUMER COMPLAINTS MECHANISM** - The handling of consumer complaints shall be done in accordance with the rules of the government agency having jurisdiction over the product or service complained of. However, the consumer may opt to seek primary resolution through the internal complaint mechanism of the on line business before resorting to intervention by the DTI or any other regulatory agency. Where the DTI is concerned, complaints against online businesses shall be made and handled in accordance with DTI Department Administrative Order 20-02, series of 2020. The established procedure for all types of consumer complaints brought before the DTI, whether against offline (brick and mortar) or online businesses shall apply to online consumers:

16.2.1 Online consumers may file complaints with the DTI regarding their concerns via the following modes:

- a. Walk-in at its national or provincial offices;
- b. Consumer care hotline at 1-384;
- c. SMS at 09178343330; and
- d. Written complaints delivered through postal or messengerial service

16.2.2 Complaints can also be filed electronically through any of the following:

- a. DTI website. Consumers must accomplish Complaint Form
- b. DTI Consumer Care Facebook page
- c. Email to consumercare@dti.gov.ph, ask@dti.gov.ph or fteb@dti.gov.ph addressed to the Director of the Fair Trade Enforcement Bureau (FTEB) or the appropriate official of any of the DTI's provincial offices, with the following details:
 - i. Complete name, address, email and contact number of complainant with attached government-issued ID

16.2.3 Complaint Handling Process

- a. When DTI receives a consumer complaint, the subject matter of which is within the ambit of its primary jurisdiction, it shall schedule the parties to the complaint for appropriate Mediation within seven (7) days of receipt.
- b. Upon agreement of both parties, Mediation may be extended for no longer than ten (10) working days.
- c. If the controversy has not been resolved through Mediation, the matter shall be scheduled for Adjudication, and a decision shall be rendered within fifteen (15) working days from submission for decision.
- d. The decision of the Consumer Arbitration Officer shall become final within fifteen (15) days from receipt thereof, unless appealed to the Secretary of Trade and Industry. The Secretary shall render a decision on appeal within thirty (30) working days from the submission of appeal.
- e. The decision of the Secretary of Trade shall become final and executory after fifteen (15) days from receipt thereof, unless a petition for certiorari

is filed with the proper court, in accordance with Article 166 of the Consumer Act of the Philippines.

- f. The Consumer complaints handling process flow chart is hereby attached as Annex D.

16.3 Online sellers, merchants, or E-retailers and consumers are advised that their communications, whether done via social media, built-in communication services on e-commerce platforms, or any other form of electronic communication using an electronic device, may constitute an electronic data message. Screenshots of such electronic communications may be used as evidence to prove a fact or establish a right in administrative or judicial proceedings, subject to the relevant rules issued by the Supreme Court.

A.M. No. 01-7-01-SC provides for the Rules on Electronic Evidence, to implement the legal recognition, admissibility, and enforcement of electronic documents and signatures in court.

VI. PENALTIES

SEC.17. PENALTIES.

All online businesses may be held liable for violations against laws, rules and regulations covered under this Joint Administrative Order (JAO) and other applicable laws and issuances. Non-exhaustive list of penalties is reflected in Annex E.

VII. FINAL PROVISIONS

SEC. 18. SEPARABILITY CLAUSE.

Should any provision of this Order or any part thereof be declared unconstitutional or otherwise invalid, the validity of other provisions not so declared shall not be affected by such declaration.

SEC. 19. REPEALING CLAUSE.

All previous Orders and Issuances which are inconsistent with this Order are hereby repealed or amended accordingly.

SEC. 20. PUBLICATION AND EFFECTIVITY.

This Order shall take effect fifteen (15) days from its complete publication in the Official Gazette or a newspaper of general circulation, and the submission of a copy hereof to the Office of the National Administrative Register (ONAR) of the University of the Philippines.

Issued this 4th day of March 2022.



RAMON M. LOPEZ

Secretary

Department of Trade and Industry



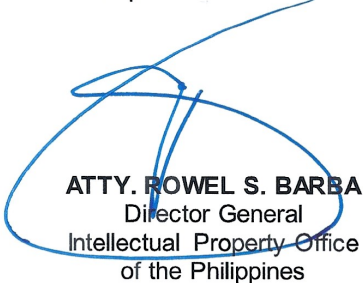
WILLIAM D. DAR, PH.D.

Secretary

Department of Agriculture



DR. FRANCISCO T. DUQUE III
Secretary
Department of Health



JIM O SAMPILNA
Acting Secretary
Department of Environment
and Natural Resources


ATTY. ROWEL S. BARBA
Director General
Intellectual Property Office
of the Philippines


ATTY. JOHN HENRY DU NAGA
Commissioner
National Privacy Commission

WITNESSED BY:


Digitally signed
by Castelo Ruth
Bernardino
ATTY. RUTH B. CASTELO
Undersecretary
Consumer Protection Group
Department of Trade and Industry


Digitally signed by
Pacheco Mary Jean
Tiongson
MARY JEAN T. PACHECO
Assistant Secretary
e-Commerce Lead
Department of Trade and Industry

ANNEX A: LIST OF PRODUCTS UNDER MANDATORY PRODUCT CERTIFICATION

**LIST OF PRODUCTS UNDER MANDATORY PRODUCT CERTIFICATION
AS OF 25 JANUARY 2021**

Products	Philippine National Standard/s (as of Jan 25, 2021)
I. ELECTRONICS AND ELECTRICAL GOODS Testing Duration: approx. 4-15 days	
Household Appliances	
Electric fans	PNS IEC 60335-2-80:2016 (IEC published 2015)
Electric irons	PNS IEC 60335-2-3:2005 (IEC published 2002)
Electric blenders	PNS IEC 60335-2-14:2016 (IEC published 2012)
Microwave ovens	PNS IEC 60335-2-25:2015 (IEC published 2014)
Electric rice cookers	PNS IEC 60335-2-15:2015 (IEC published 2012)
Electric airpots	PNS IEC 60335-2-15:2015 (IEC published 2012)
Electric coffeemakers	PNS IEC 60335-2-15:2015 (IEC published 2012)
Electric toaster	PNS IEC 60335-2-9:2016 (IEC published 2012)
Electric stoves	PNS IEC 60335-2-9:2016 (IEC published 2012)
Electric hot plates	PNS IEC 60335-2-9:2016 (IEC published 2012)
Electric grills	PNS IEC 60335-2-9:2016 (IEC published 2012)
Electric ovens	PNS IEC 60335-2-9:2016 (IEC published 2012)
Turbo broilers	PNS IEC 60335-2-9:2016 (IEC published 2012)
Induction cookers	PNS IEC 60335-2-9:2016 (IEC published 2012)
Washing machines	PNS IEC 60335-2-7:2016 (IEC published 2012)
Spin extractors	PNS IEC 60335-2-4:2016 (IEC published 2012)
Refrigerators Storage capacity 142 liters to 227 liters (5 to 8 cu. ft.)	PNS 396-2:1997 Amd. 01:2000
Storage capacity up to 567 liters (20 cu. ft.)	PNS IEC 60335-2-24:2013
Air conditioners Non-inverter, Window & Split-type up to 36,000 kJ/hr. cooling capacity	PNS 396-1:1998
Inverter, non-inverter, window-type and split-type air-conditioners, with not more than 250 V for single phase and 600 V for all other types and with cooling capacity up to 38,000 kJ/hr.	PNS IEC 60335-2-40:2013
Electric juicers	PNS IEC 60335-2-14:2016 (IEC published 2012)

ANNEX A: LIST OF PRODUCTS UNDER MANDATORY PRODUCT CERTIFICATION

Electric food mixers	PNS IEC 60335-2-14:2016 (IEC published 2012)
Electric food processors	PNS IEC 60335-2-14:2016 (IEC published 2012)
Electric kettles	PNS IEC 60335-2-15:2015 (IEC published 2012)
Electric pressure cookers	PNS IEC 60335-2-15:2015 (IEC published 2012)
Electric slow cookers	PNS IEC 60335-2-15:2015 (IEC published 2012)
Electric multi-cookers	PNS IEC 60335-2-15:2015 (IEC published 2012)
Consumer Electronics	
Television set	PNS IEC 60065:2013 (IEC published 2011)
CD/VCD/DVD player	PNS IEC 60065:2013 (IEC published 2011)
Lightning and Wiring Devices	
Pre-heat / Magnetic ballasts	PNS IEC 61347-2-8:2002 (IEC 61347-2-8:2000)
Electronic ballasts	PNS IEC 61347-2-3:2002 with Amd. 1:2006
Self- ballasted lamps / Compact fluorescent lamps	PNS IEC 968:2006 (IEC published 1988)
Self-ballasted LED lamps	PNS IEC 62560:2012 (IEC 62560:2011)
Christmas lights/ Lighting chains	PNS 189:2000
Double-capped fluorescent lamps	PNS IEC 61195:2006 (IEC 61195:1999)
Single-capped fluorescent lamps	PNS IEC 61199:2006 (IEC 61195:1999)
Incandescent lamps (Bulbs)	PNS 38-1:1995 (IEC 432-1:1993 Amd. 01:1995)
Edison screw lamp holders	PNS 80:1997 (IEC 238:1996)
Lamp holders or tubular fluorescent lamps	PNS 42:1997 (IEC 400:1996)
Starter holders	PNS 42:1997 (IEC 400:1996)
Lamp starters	PNS 45:1997 Amd. 01:1997 (IEC 155:1993 Amd. 01:1995)
Circuit breakers	
a) Moulded case	PNS 519:1991
b) Low voltage switchgear and control gear	PNS 1573-2:1997 (IEC 947-2:1995)
Fuses	PNS 13:1983
Fuseholders	PNS 56:1996 (ANSI/UL 512:1992)
PVC electrical tapes	PNS 79:1992
Plugs, Socket-outlets, and Extension cord sets	
a) Plugs and socket-outlets for household and similar purposes	PNS 1486-1:1996 (IEC 884-1:1994)
b) Plugs and socket outlets for domestic and similar general use standards	PNS 1572:1997 (IEC 83:1975)
Snap switches	
a) Switches for household and similar fixed electrical installations	PNS 1485-1:1996 Amd. 01 & 02:1996 (IEC 669-1:1993 Amd. 01:1994 & Amd. 02:1995)
b) Snap switches for general use	PNS 57:1996 (UL 20:1995)

ANNEX A: LIST OF PRODUCTS UNDER MANDATORY PRODUCT CERTIFICATION

Knife switches	PNS 118:1988
PVC insulated flexible cords	PNS 163:1994
Thermoplastic electric wires and cables	PNS 35-1:2004
II. MECHANICAL, BUILDING, AND CONSTRUCTION MATERIALS	
Testing Duration: approx. 4-6 days	
Steel Products	
BI/GI steel pipes	PNS 26:1992 / PNS 26:2018
Deformed Steel Bars	PNS 49:2002
Equal-Leg Steel Angle Bars	PNS 657:2008
Rerolled Steel Bars	PNS 211:2002
Low Carbon Steel Wires	PNS 113:2005
Steel Wire Nails	PNS 136:2000
Plastic Pipes and Ceramic Products	
Pipes (PB) for potable water supply	PNS 152:1987
Pipes (PE) for potable water supply	PNS ISO 4427:2002 Amd. 01:2002
Pipes (uPVC) for potable water supply	PNS 65:1993
uPVC rigid electrical conduit	PNS 14:1983 Amd. 01:1987
Pipes (PVC-U) for drain waste & vent	PNS 1950:2003 Corrigendum 01:2003
Sanitary wares	PNS 156:2000
Cement and Other Construction Materials	
Portland cement	PNS 07: 2018
Blended hydraulic cement	PNS 63: 2019
Plywood	PNS ISO 12465:2017
Ceramic Tiles	PNS ISO 13006:2019
III. CHEMICAL AND OTHER CONSUMER PRODUCTS AND SYSTEMS	
Testing Duration: 3-90 days	
Chemical Products	
Motor Vehicle brake fluid	PNS 239/MVSS 116:1988
Dry chemical portable fire extinguishers	PNS 15-1:1989
Carbon dioxide portable fire extinguishers	PNS 15-3:1991
Foam portable fire extinguishers	PNS 15-4:1991
Clean extinguishing agent - Halon substitute portable fire extinguishers	PNS 15-5:1996 Amd. 01:1997
Fireworks	PNS 1220-2:1994
Medical grade oxygen	PNS 103:1987
Automotive Related Products	
Safety belts (Seat belts)	PNS 1892:2000 Amd. 01:2002
Child Restraint Systems	PNS UNR 44:2018; PNS UNR 129:2018
Helmets and their visors	PNS/UN ECE 22:2007
Safety glass for automotive	PNS 130:1988 Amd. 01:1998
Lead-Acid Storage Batteries	PNS 06:1987
Inner tubes for tires	PNS 34:2000
Tires for automotive vehicles	PNS 25:1994
Speed Limitation Device	PNS UNR 89: 2016
Other Consumer Products	
Matches	PNS 09-1:2000
Lighters	PNS 47:1998 (ISO 9994:1995)
Monobloc chair/stools	PNS 1478:1998
LPG cylinders for motor vehicles	PNS 04:1983
LPG cylinders for household use	PNS 03-1:2000
LPG cylinders repair	PNS 03-3:2000

**ANNEX B: APPLICATION REQUIREMENTS FOR
PS MARK, ICC STICKERS, COE, AND SOC**

**APPLICATION REQUIREMENTS FOR
PS MARK, ICC STICKERS, COE, AND SOC**

#	Philippine Standard License	Import Commodity Clearance	Certificate of Exemption	Statement of Confirmation
1	Articles of Incorporation or Business Name and Sub-Contracting Agreement, if any	Packing List	Packing List	Packing List
2	Quality Manual	Import Entry (need not be submitted upon filing the application but shall be a requirement for the release of the ICC Certificate)	Import Entry (need not be submitted upon filing the application but shall be a requirement for the release of the ICC Certificate)	Import Entry (need not be submitted upon filing the application but shall be a requirement for the release of the ICC Certificate)
3	Brief description of manufacturing process	Commercial Invoice	Commercial Invoice	Commercial Invoice
4	Reference no. of the Product Identification File to include process flow, materials, process control and drawings among others	Bill of Lading/Airway Bill	Bill of Lading/Airway Bill	Bill of Lading/Airway Bill
5	Listing of measuring and testing equipment with nominal capacities and serial numbers at each inspection point and final product testing together with the evidence of ownership, such as official receipts	Summary of Batch Nos./Serial Nos. of Products	Summary of Batch Nos./Serial Nos. of Products	Summary of Batch Nos./Serial Nos. of Products
6	Brief description of equipment maintenance and calibration program for all testing and measuring equipment with their corresponding calibration certificates	a) DTI Business Name Registration (for single proprietor)	a) DTI Business Name Registration (for single proprietor)	a) DTI Business Name Registration (for single proprietor)
		b) SEC Certificate of Incorporation (for corporation)	b) SEC Certificate of Incorporation (for corporation)	b) SEC Certificate of Incorporation (for corporation)
7	Copies of labels, markings and logos etc. as per requirements of specific standard	a) Special Power of Attorney (for single proprietor)	a) Special Power of Attorney (for single proprietor)	a) Special Power of Attorney (for single proprietor)
		b) Board/Partners' Resolution or (for corporation) / Notarized Secretary's	b) Board/Partners' Resolution or (for corporation) / Notarized Secretary's	b) Board/Partners' Resolution or (for corporation) / Notarized Secretary's

**ANNEX B: APPLICATION REQUIREMENTS FOR
PS MARK, ICC STICKERS, COE, AND SOC**

		Certificate stating the name of authorized company representative	Certificate stating the name of authorized company representative	Certificate stating the name of authorized company representative
8	Description of the supply distribution chain. If new business, identify the target market. If foreign company, identify the Philippine principal and described the organizational relationship of the applicant/license holder and Philippine principal	Surety Bond	BIR Importers Clearance Certificate	Surety Bond (Valued at 10% of the commercial invoice value of the cement shipment)
9	Vicinity map of the factory	BIR Importers Clearance Certificate	Current Proof of Billing (Office and Warehouse)	BIR Importers Clearance Certificate / COR
10	Undertaking to abide by the terms and conditions of the PS License (Annexed to Application Form)	Current Proof of Billing (Office and Warehouse)	**Nothing follows**	Current Proof of Billing (Office and Warehouse)
11	**Nothing follows**	ISO 9001 Certificate of the Manufacturer		Production Record
12		Valid Test Report		List of Distributors
13		Other Documents: a) For rerolled steel bars deformed steel bars and equal leg angle bars: - Submission of logo to BPS prior to importation - Mill Certificate, quality inspection report or its equivalent from the Manufacturer		Audited Financial Statement

**ANNEX B: APPLICATION REQUIREMENTS FOR
PS MARK, ICC STICKERS, COE, AND SOC**

		b) For motorcycle helmet and its visors: <ul style="list-style-type: none"> - Test report per brand per type per model - Certificate of Conformity from the Manufacturer that the batch imported conformed to the requirement of the standard prior to release from the Manufacturer's premises - Updated list of distributors/retailers 		
14				Photocopy of PS License
15		**Nothing follows**		Load Port Survey Report
16				Other documents

ANNEX C: NON-EXHAUSTIVE LIST OF THE PROHIBITED OR RESTRICTED ITEMS

NON-EXHAUSTIVE LIST OF THE PROHIBITED OR RESTRICTED ITEMS

This list may be revised or updated by the relevant regulatory agencies concerned

- i. Wildlife and wildlife by products and derivatives:
 - a. Wild plant/flora, plant parts (i.e. Bark, leaves/shoots, roots, wood, essential oils) and propagules (i.e. Living cuttings and genetic material), and seeds and seedlings of plant species listed under the cites appendices; and threatened species and exotic species which are regulated, restricted by the Wildlife Act (R.A. 9147). Prohibited items: alien invasive species and wildlife species collected from the wild.
 - b. Live wild animals/fauna (including fingerlings, hatchlings, eggs, and/or genetic material); unprocessed and processed by-products and derivatives of fauna listed under the cites appendices and threatened species and exotic species which are restricted by the Wildlife Act (R.A. 9147); prohibited items: alien invasive species and wildlife species collected from the wild.
- ii. Human parts or remains;
- iii. Fertilizers, pesticides (chemical and biorational), other agricultural chemicals, and seeds with plant incorporated protectants, unless, duly licensed or permitted under the Fertilizer and Pesticide Authority (FPA); and seeds, conventional or biotech-traited, unless duly permitted under Bureau of Plant Industry (BPI) regulations and in both instances, compliant with all DA rules and regulations providing for their regulated entry in the Philippine market and in electronic commerce;
- iv. Toxic substances and hazardous wastes¹;
- v. Imported Recyclable Materials Containing Hazardous Substances [scrap metals; scrap plastics; electronic assemblies and scrap (including imported, second-hand or used electrical and electronic equipment); used oil; and fly ash]²;
- vi. Health products, including food, drugs, cosmetics, devices, biologicals, vaccines, in-vitro diagnostic reagents, household/urban hazardous substances, household/urban pesticides, toys and childcare articles, unless, duly licensed or permitted under the Food and Drug Administration (FDA) and compliant to the rules and regulations providing for its regulated or controlled entry in electronic commerce;
- vii. Prohibited Food:
 - a. Listings containing medicinal claims - that is, a claim that the item is intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease in humans and/or animals, contraception, inducing anesthesia or otherwise preventing or interfering with the normal operation of a physiological function, whether permanently or temporarily, and whether by way of terminating, reducing or postponing, or increasing or accelerating, the operation of that function or in any other way (for example, pharmaceutical drugs, contact lenses, misbranded dietary supplements);
 - b. Noxious food items - Food which contains any prohibited substances

¹ DENR revised 01.19.2022

² DENR revised 01.19.2022

ANNEX C: NON-EXHAUSTIVE LIST OF THE PROHIBITED OR RESTRICTED ITEMS

or substances in excess of permitted proportions, adulterated food without fully informing buyer at the time of sale of the nature of the transaction;

c. Non-pasteurized dairy products;

- i. Products marketed as breastmilk substitutes including infant formula, and other milk products, foods and beverages including bottle-fed complementary foods, when marketed or otherwise represented to be suitable, with or without modification, for use as a partial or total replacement of breastmilk; feeding bottles and teat in compliance with the provisions of E.O. 51 or the Milk Code and its implementing rules and regulations;

d. Wild mushrooms; and

e. Any other food items hazardous to human health.

- viii. Drugs, prescription-only medicines, pharmacy-only medicines, drug-like substances and associated paraphernalia;
- ix. Alcoholic beverages, unless duly licensed or permitted by the FDA and compliant with the rules and regulations providing for its regulated or controlled entry in electronic commerce, including restrictions in access and purchase by minors, and in advertising and promotion;
- x. Tobacco or tobacco related products, electronic cigarettes, e-juices, and heated tobacco products, unless duly licensed, or permitted by the FDA, and compliant with the rules and regulations providing for its regulated or controlled entry in electronic commerce, including restrictions in access and purchase by minors, and in advertising and promotion;³
- xi. Ionizing radiation sources and services/activities involving thereof, which include radiation devices and radioactive materials, and services/activities where such sources are used for medical and non-medical purposes; Unless, duly licensed or permitted under the FDA and/or the Philippine Nuclear Research Institute (PNRI) and compliant to the rules and regulations providing for its regulated or controlled entry in electronic commerce
- xii. Lottery tickets;
- xiii. Slot machines;
- xiv. Goods or items that are:
 - a. Embargoed;
 - b. Mislabeled;
 - c. Recalled;
 - d. Stolen;
 - e. Expired;
 - f. Repacked
 - g. Unlabeled
 - h. Smuggled
 - i. Parallel imports, with the exception of drugs and medicines when authorized by law, such as:
 - i. Non-counterfeit product imported from another country without the expressed permission of the intellectual property owner;

³ FDA revised 01.12.2022

ANNEX C: NON-EXHAUSTIVE LIST OF THE PROHIBITED OR RESTRICTED ITEMS

- ii. Non-counterfeit, duty free product declared for personal use;
- xv. Used cosmetics;
- xvi. Counterfeit items, such as:
 - a. Counterfeit currency and stamps;
 - b. Counterfeit goods, pirated goods and/or content;
 - c. Potentially infringing items: Items including but not limited to replicas, counterfeit items, and unauthorized copies of a product or item which may be in violation of certain copyrights, trademarks, or other intellectual property rights of third parties;
 - d. Counterfeit GM seeds that are sold without the mandatory biosafety permits issued by the BPI
- xvii. Currency, credits, and securities such as:
 - a. Currency or credits including, without limitation, digital currency or credits, and stored value cards;
 - b. Credit and debit cards;
 - c. Shares, stock, other securities and stamps;
- xviii. Precious metals such as but not limited to gold bar, silver bar, platinum bar, conflict minerals (natural sources extracted in a conflict zone and sold to perpetuate fighting), conflict diamond (diamond mined in a war zone and sold to finance an insurgency);
- xix. Artifacts and antiquities;
- xx. Weapons, such as:
 - a. Firearms, weapons such as pepper spray, replicas, and stun guns, etc.;
 - b. Lock-picking devices;
- xxi. Equipment and devices critical to surveillance and information gathering, such as:
 - a. Telecommunication equipment that has not been registered with the National Telecommunications Commission of the Philippines, and electronic surveillance equipment and other similar electronic equipment such as cable TV, de-scramblers, radar scanners, traffic signal control devices, wiretapping devices and telephone bugging devices;
 - b. Circumvention devices used in modifying, decoding, recoding of vital information;
- xxii. Government or Police related items such as badges, insignia or uniforms;
- xxiii. Prohibited services: the provision of services that are sexual, or illegal in nature;
- xxiv. Obscene, seditious or treasonous materials, as defined under the revised penal code and other special laws;
- xxv. Publications, books, films, videos and/or video games that do not comply with applicable laws in the country of sale and/or delivery;
- xxvi. Blasphemous materials showing disrespect, irreverence, discrimination to any religion;
- xxvii. Products that:

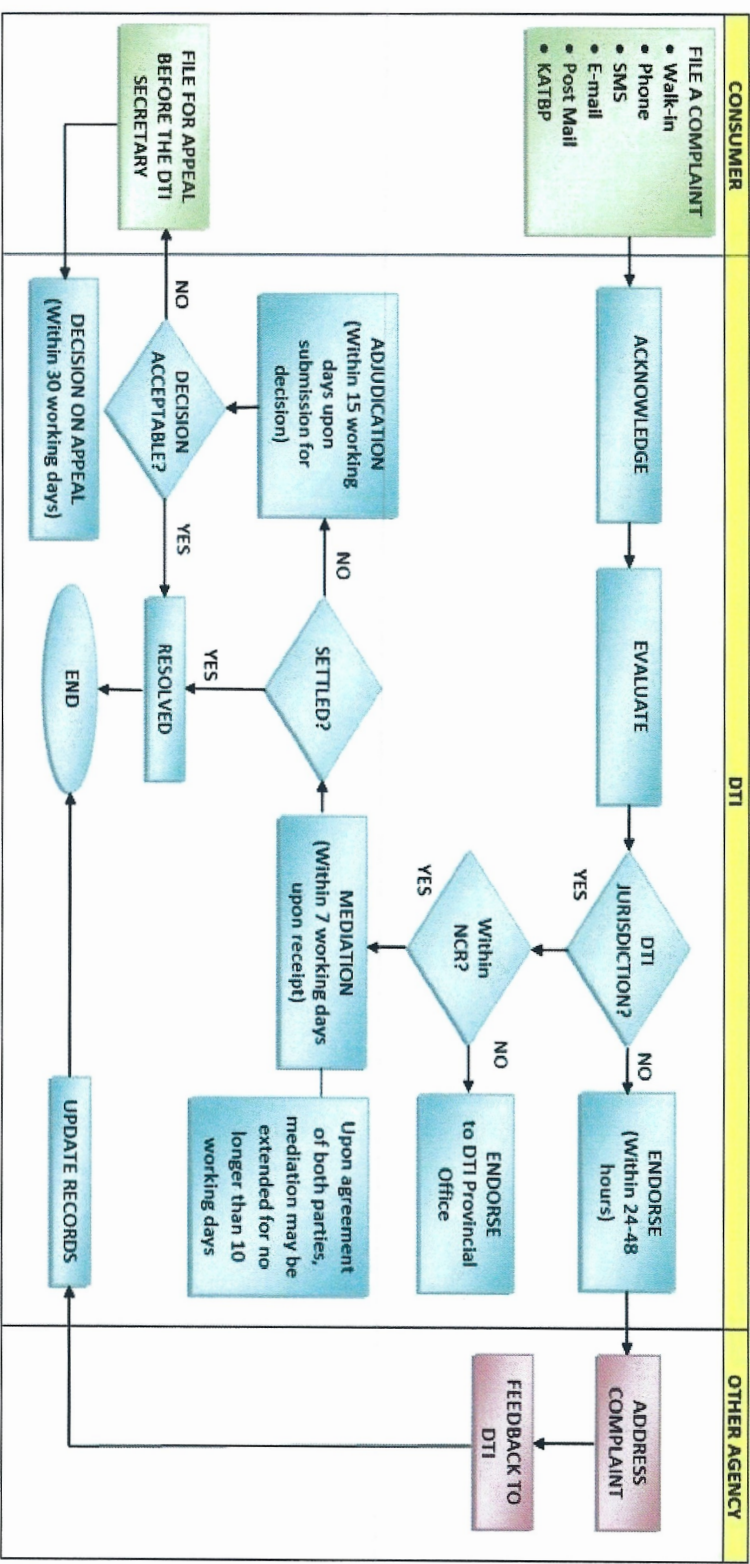
ANNEX C: NON-EXHAUSTIVE LIST OF THE PROHIBITED OR RESTRICTED ITEMS

- a. Relate to campaigns, elections, political issues, or issues of public debate;
 - b. Advocate for or against, or attack a politician or political party; or
 - c. Promote or encourage any form of hate, crime, prejudice, rebellion or violence;
- xxviii. Any other items that are, or that contain components that are:
- a. Illegal or restricted in the jurisdiction of the Buyer and/or the Seller or which otherwise encourage illegal or restricted activities, or
 - b. Determined by any governmental or regulatory authority to pose a potential health or safety risk.
- xxix. Wildlife, species (flora and fauna) whether live, stuffed, preserved, by-products and derivatives which are regulated by the Wildlife Act (RA 9147)
- a. Live animals whether domestic or wild (exotic or indigenous) animals which may be found producing, companion, aquatic, laboratory, including birds, worms, bees and butterflies, its products and by-products, veterinary feed premixes and biologics, laboratory specimen of animal origin, feeds and feed ingredients that may be carriers of communicable animal diseases
 - b. Terrestrial wildlife species whether live, stuffed, preserved, by-products & derivatives, including:
 - i. All wildlife species (fauna and flora) bred in captivity or propagated
 - ii. All exotic species (fauna and flora)
- xxx. Fishery and aquatic products:
- c. All fish and fishery/aquatic products (live, fresh, dried and/or processed, frozen and chilled)
 - d. Live Mud crab ("Alimango"-*Scylla serrata*), carapace length of 10cm or over and weight of 200 grams or over
 - e. Seasnakes whether live, skin or products from the skin or meat
 - f. Shells such as:
 - i. Black lip pearl ("Concha Negra"-*Pinctada margaritifera*), with a minimum size of 11cm, maximum outside long axis measurement, taken at right angle to the base.
 - ii. Gold lip pearl ("Concha blanca"-*Pinctada maxima*), with a minimum size of 19cm, maximum outside long axis measurement, taken at right angle to the base.
 - iii. Semi-finished or Semi-processed Capiz shells ("Kapis"), 8cm or over in diameter measured from the base perpendicular towards the top edge of the shell
 - iv. Hirose shell ("Babae"-*Trochus noduliferus*), with a minimum size of 5cm across the least diameter of the base, taken at right angles to the axis
 - v. Rough top shell or trochus shell ("Simong"; trocha rough

ANNEX C: NON-EXHAUSTIVE LIST OF THE PROHIBITED OR RESTRICTED ITEMS

variety-trochus maximus), with a minimum size of 7.5cm across the least diameter of the base, measured at right angles to the axis

- xxx. All plants, planting materials, plant, and wood products:
 - g. Pest specimen, including wood packaging materials capable of harboring plant pests
 - h. Lumber, logs, poles, piles, log core and flitches/railroad ties produced from planted trees from both the forestlands and private lands
- xxxii. Coffee
- xxxiii. All sugarcane-based sugar such raw sugar, white sugar, and muscovado, and Molasses
- xxxiv. Leaf Tobacco such as Virginia, Burley, Native tobacco strips, tobacco stems, expanded tobacco and tobacco refuse/scrap/dusts, etc.
- xxxv. Tobacco products such as cigarettes, cigars, heated tobacco products, pipe tobacco, chewing tobacco, snuff, homogenized tobacco, reconstituted tobacco, cut fillers, cut rags, snus, etc.
- xxxvi. Tobacco-related materials such as packaging materials, filters, flavorings, adhesives, collagens, machines and spare parts, etc.
- xxxvii. Crushed and/or sized sand gravel and/or other unconsolidated materials
- xxxviii. Iron, manganese and/or chromium ore(s), whether unprocessed or processed
- xxxix. Mine wastes and/or mill tailings
- xl. Unprocessed, raw, or run-of-mine mineral(s)
- xli. Controlled chemicals
- xl. Legal tender Philippine notes and coins, checks, money order and other bills of exchange drawn in pesos against banks operating in the Philippines in an amount exceeding PHP 50, 000.00
- xl. Cultural properties such as archaeological materials, traditional ethnographic materials, antiques, historical relics, natural history specimens, including holotypes, endangered, irreplaceable specimens, and fossils
- xl. Optical and magnetic media, its manufacturing equipment, parts and accessories and manufacturing materials
- xl. Firearms and ammunition, parts, and components thereof, accessories of firearms, tools, machinery, or instruments used or intended to be used in the manufacture of firearms and ammunition or parts thereof, bullet proof vests, airguns, airsoft guns, and taser guns.
- xl. Chainsaw, including its parts and accessories. Chainsaw refers to any portable saw or similar cutting implement rendered operative by an electric or internal combustion engine or similar means, that may be used for, but is not limited to, the felling of trees or the cutting of timber;
- xl. Nuclear and radioactive material having specific activity greater than 70kBq/kg
- xl. Nuclear related dual use items
- xl. Explosive/Explosive ingredients
- l. Firecrackers and Pyrotechnic devices



SCHEDULE OF PENALTIES UNDER R.A. 8792, THE ELECTRONIC COMMERCE ACT

VIOLATIONS	FINE (Php)	IMPRISONMENT
Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communication system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic documents	MINIMUM of 100,000 and a MAXIMUM commensurate to the damage incurred.	MANDATORY imprisonment of 6months to 3years
Piracy or the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature or copyrighted works including legally protected sound recordings or phonograms or information material on protected works, through the use of telecommunication networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights	MINIMUM of 100,000 and a MAXIMUM commensurate to the damage incurred.	MANDATORY imprisonment of 6 months to 3 years
Other violations of the provisions of this Act	MAXIMUM of 1,000,000 OR	6 years

SCHEDULE OF PENALTIES UNDER R.A. 4109, THE PRODUCT STANDARDS LAW /AS PROVIDED FOR UNDER DAO NO. 02, S. 2007]

NATURE OF OFFENSE	FREQUENCY OF VIOLATION	MANUFACTURER / IMPORTER / SERVICE PROVIDER						WHOLESALE / RETAILER / DEALER / AGENT				
		Basic fines	Only Mitigating	Outnumber Aggravating	Outnumber Mitigating	Only Aggravating		Basic fines	Only Mitigating	Outnumber Aggravating	Outnumber Mitigating	Only Aggravating
A. License Related 1. Distribution, sale, or offer for sale of any product covered by Philippine Standard Certification Mark Schemes which does not conform to the required and applicable PNS quality or safety standards 2. Providing repair, requalification, and installation services without the required license, accreditation, and/or recognition 3. Distribution, sale, offer for sale, or manufacture of any products with PS Mark but without valid PS license or permit 4. Manufacture, importation, distribution, sale, or offer for sale of any product covered by mandatory product certification	1 st Offense	50,000	35,000 to 42,500	42,500 to 50,000	50,000 to 65,000	65,000 to 75,000		25,000	17,500 to 21,250	21,250 to 25,000	25,000 to 32,500	32,500 to 37,500
	2 nd Offense	75,000	52,500 to 63,750	63,750 to 75,000	75,000 to 97,500	97,500 to 112,500		50,000	35,000 to 42,500	42,500 to 50,000	50,000 to 65,000	65,000 to 75,000
	3 rd Offense	150,000						150,000				

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

without the required BPS license or permit 5. Importation, distribution, sale, or offer for sale of imported products covered by mandatory product certification without required ICC	4 th Offense	150,000						150,000					
B. Product Related 1. Importation, distribution, sale, offer for sale, or manufacture of any product covered by mandatory product certification which does not bear the BPS required identification and product markings 2. Importation, distribution, sale, offer for sale, or manufacture of any product covered by mandatory product certification under a fake,	1 st Offense	50,000	35,000 to 42,500	42,500 to 50,000	50,000 to 65,000	65,000 to 75,000	25,000	17,500 to 21,250	21,250 to 25,000	25,000 to 32,500	32,500 to 37,500		
	2 nd Offense	75,000	52,500 to 63,750	63,750 to 75,000	75,000 to 97,500	97,500 to 112,500	50,000	35,000 to 42,500	42,500 to 50,000	50,000 to 65,000	65,000 to 75,000		

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

withdrawn, suspended, or cancelled BPS license or permit																
	3 rd Offense		150,000								150,000					
3. Importation, distribution, sale, or offer for sale of imported products with ICC Marks but without valid ICC	3 rd Offense		150,000								150,000					
	4 th Offense		150,000								150,000					
4. Importation, distribution, sale, or offer for sale of imported products although bearing the required BPS identification and product markings but such markings are not place in the manner provided	4 th Offense		150,000								150,000					
C. Implementation Related	1. Mandatory products released from the Bureau of Customs without the necessary conditional release or with falsified documents purportedly from the BPS or DTI Provincial or Regional Office		1 st Offense	50,000	35,000	to	42,500	50,000	to	65,000	17,500	to	21,250	25,000	to	32,500
					42,500	50,000	65,000	75,000	97,500	21,250	25,000	32,500	37,500			
				52,500	63,750	75,000	97,500	112,500	35,000	42,500	50,000	65,000	75,000			
	2 nd Offense		75,000	to	63,750	75,000	97,500	112,500	50,000	42,500	50,000	65,000	75,000			
	3 rd Offense		150,000													
2. Refuse access to or copying of pertinent records, to permit entry of or inspection in the establishment's premises or	3 rd Offense		150,000								150,000					

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

warehouse facilities conducted by authorities	4 th Offense	150,000					150,000				
	3. Failure to comply with any duly served notice, summons, or subpoenas issued by authorities	1 st Offense	5,000	N/A	N/A	N/A	N/A	3,000	N/A	N/A	N/A
	4. Giving false or misleading data / information, misrepresenting a material and substantial fact, or willfully concealing a material data or fact	2 nd Offense	10,000	N/A	N/A	N/A	N/A	6,000	N/A	N/A	N/A
	5. Failure to comply with the applicable rules and regulations regarding stockpiling (as defined in R.A. 7394, the Consumer Act)	3 rd Offense	25,000					10,000			
	6. Failure to comply with the orders issued pursuant to Art. 11 of R.A. 7394, relating to a) notification requirements on; and b) recall, repair, replacement, or refund of substandard products	4 th Offense	25,000					10,000			

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

The following schedule shall be applied where the offense is related to a consumer complaint filed under R.A. 7394, or the Consumer Act

NATURE OF OFFENSE	FREQUENCY OF VIOLATION	MANUFACTURER / IMPORTER / SERVICE PROVIDER					WHOLESALE / RETAILER / DEALER / AGENT				
		Basic fines	Only Mitigating	Outnumber Aggravating	Outnumber Mitigating	Only Aggravating	Basic fines	Only Mitigating	Outnumber Aggravating	Outnumber Mitigating	Only Aggravating
A. License Related 1. Distribution, sale, or offer for sale of any product covered by Philippine Standard Certification Mark Schemes which does not conform to the required and applicable PNS quality or safety standards 2. Providing repair, requalification, and installation services without the required license, accreditation, and/or recognition 3. Distribution, sale, offer for sale, or manufacture of any products with PS Mark, but without valid PS license or permit 4. Manufacture, importation, distribution, sale, or offer for sale of any product covered by mandatory product certification	1 st Offense	100,000	70,000 to 85,000	85,000 to 100,000	100,000 to 130,000	130,000 to 150,000	50,000	35,000 to 42,500	42,500 to 50,000	50,000 to 65,000	65,000 to 75,000
	2 nd Offense	150,000	105,000 to 127,500	127,500 to 150,000	150,000 to 195,000	195,000 to 225,000	75,000	52,000 to 63,750	63,750 to 75,000	75,000 to 97,500	97,500 to 112,500
	3 rd Offense	300,000					300,000				

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

without the required BPS license or permit																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																												
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

<p>withdrawn, suspended, or cancelled BPS license or permit</p> <p>3. Importation, distribution, sale, or offer for sale of imported products with ICC Marks but without valid ICC</p> <p>4. Importation, distribution, sale, or offer for sale of imported products although bearing the required BPS identification and product markings but such markings are not place in the manner provided</p>	3 rd Offense	300,000								300,000							
	4 th Offense	300,000								300,000							
<p>C. Implementation Related</p> <p>1. Mandatory products released from the Bureau of Customs without the necessary conditional release or with falsified documents purportedly from the BPS or DTI Provincial or Regional Office</p> <p>2. Refuse access to or copying of pertinent records, to permit entry of or inspection in the establishment's premises or</p>	1 st Offense	100,000	70,000	85,000	100,000	130,000	50,000	35,000	42,500	50,000	65,000						
			to	to	to	to	to	to	to	to	to						
			85,000	100,000	130,000	150,000	42,500	50,000	65,000	75,000	97,500						
	2 nd Offense	150,000	127,500	150,000	195,000	225,000	75,000	63,750	75,000	97,500	112,500						
	3 rd Offense	300,000								300,000							

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

warehouse facilities conducted by authorities.	4 th Offense	300,000					300,000				
	1 st Offense	10,000	N/A	N/A	N/A	N/A	3,000	N/A	N/A	N/A	N/A
	2 nd Offense	20,000	N/A	N/A	N/A	N/A	6,000	N/A	N/A	N/A	N/A
	3 rd Offense	50,000					25,000				
	4 th Offense	50,000					25,000				
3. Failure to comply with any duly served notice, summons, or subpoenas issued by authorities											
4. Giving false or misleading data / information, misrepresenting a material and substantial fact, or willfully concealing a material data or fact											
5. Failure to comply with the applicable rules and regulations regarding stockpiling (as defined in R.A. 7394, the Consumer Act)											
6. Failure to comply with the orders issued pursuant to Art. 11 of R.A. 7394, relating to a) notification requirements on; and b) recall, repair, replacement, or refund of substandard products											

SCHEDULE OF PENALTIES UNDER R.A. 7394, THE CONSUMER ACT OF THE PHILIPPINES

The following schedule shall be the basis in the imposition of administrative fine for violation of R.A. No. 7394, otherwise known as the Consumer Act of the Philippines, particularly on the provisions on Price Tag.

SCHEDULE I

	RANGE OF CAPITALIZATION (Php)	MINIMUM	MEDIUM	MAXIMUM
RETAILER	a. Below 20,000	500	1,000	1,500
	b. 20,000 to 100,000	5,000	10,000	20,000
	c. Above 100,000 to 200,000	10,000	20,000	30,000
	d. Above 200,000	30,000	40,000	50,000

The following schedule shall be applied in cases of violation of the R.A. No. 7394 as provided in Section 1, Article IV, except (1), and its implementing rules.

SCHEDULE II

	RANGE OF CAPITALIZATION (Php)	MINIMUM	MEDIUM	MAXIMUM
RETAILER	a. Below 20,000	500	1,000	1,500
	b. 20,000 to 100,000	20,000	30,000	40,000
	c. Above 100,000 to 300,000	40,000	50,000	60,000
	d. Above 300,000 to 500,000	60,000	70,000	80,000
	e. Above 500,000 to 1,000,000	100,000	140,000	180,000

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

RETAILER	f. Above 1,000,000 to 5,000,000	120,000	160,000	200,000
	g. Above 5,000,000 to 10,000,000	240,000	260,000	280,000
	h. Above 10,000,000	280,000	290,000	300,000
WHOLESALE, DISTRIBUTOR, MANUFACTURER, IMPORTER	a. Below 500,000	60,000	70,000	80,000
	b. Above 500,000 to 1,000,000	100,000	140,000	180,000
	c. Above 1,000,000 to 5,000,000	120,000	160,000	200,000
	d. Above 5,000,000 to 10,000,000	240,000	260,000	280,000
	e. Above 10,000,000	280,000	290,000	300,000

NOTE: In the event the offender is engaged in two or more business activities, the activity to which a higher penalty corresponds shall be made the basis in imposing the appropriate penalty.

SCHEDULE OF PENALTIES UNDER R.A. 7581, THE PRICE ACT OF THE PHILIPPINES

In determining the imposable fine for violation of R.A. 7581 as amended, otherwise known as the Price Act, the following shall be taken into consideration:

SCHEDULE I

	Range of Capitalization (Php)	Minimum	Medium	Maximum
RETAILER	a. Below 20,000	500	1,000	1,500
	b. 20,000 to 100,000	5,000	10,000	20,000
	c. Above 100,000 to 300,000	20,000	30,000	40,000
	d. Above 300,000 to 500,000	40,000	50,000	60,000
	e. Above 500,000 to 1,000,000	60,000	80,000	100,000
	f. Above 1,000,000	100,000	125,000	150,000
WHOLESALE, DISTRIBUTOR, MANUFACTURER, IMPORTER	a. 300,000 and below	20,000	30,000	40,000
	b. Above 300,000 to 500,000	40,000	50,000	60,000
	c. Above 500,000 to 1,000,000	60,000	80,000	100,000
	d. Above 1,000,000	100,000	125,000	150,000

NOTE: In the event the offender is engaged in two or more business activities, the activity to which a higher fine is attached shall be imposed, subject to all other requirements of the law.

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

VIOLATIONS	FINE (Php)	IMPRISONMENT
Illegal Price Manipulation on Basic Necessity or Prime Commodity	Not less than 5,000 nor more than 2,000,000 AND/OR	Not less than 5 years nor more than 15 years
Price Ceiling	Not less than 5,000 nor more than 1,000,000 AND/OR	Not less than 1 year nor more than 10 years
Other violations	Not more than 1,000,000 OR	Not more than 6 years

SCHEDULE OF PENALTIES UNDER R.A. 10173, THE DATA PRIVACY ACT OF 2012

VIOLATION	FINE (Php)		IMPRISONMENT	
	Personal Information	Sensitive Personal Information	Personal Information	Sensitive Personal Information
Unauthorized Processing	500,000 to 2,000,000	500,000 to 4,000,000	1 to 3 years	3 to 6 years
Accessing Due to Negligence				
Improper Disposal	100,000 to 500,000	100,000 to 1,000,000	6 months to 2 years	1 to 3 years
Processing for Unauthorized Purposes	500,000 to 1,000,000	500,000 to 2,000,000	1 year and 6 months to 5 years	2 to 7 years
Unauthorized Disclosure		1,000,000 to 5,000,000	1 to 3 years	3 to 5 years
Concealment of Security Breaches		500,000 to 1,000,000		1 year and 6 months to 5 years
Unauthorized Access or Intentional Breach	500,000 to 2,000,000		1 to 3 years	
Malicious Disclosure	500,000 to 1,000,000		1 year and 6 months to 5 years	
Combination or Series of Acts	1,000,000 to 5,000,000		3 to 6 years	
Large Scale (personal information of 100 persons harméd, affected, or involved)	Maximum provided			
Offender is a Public Officer	Regular schedule of penalties + Accessory penalty of Disqualification from Public Office (for a term double that of the criminal penalty imposed)			

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

SCHEDULES OF PENALTIES UNDER R.A. 8293, THE INTELLECTUAL PROPERTY CODE OF THE PHILIPPINES

VIOLATIONS	FINE (Php)	IMPRISONMENT
Repetition of Patent Infringement	Not less than 100,000 but not more than 300,000 AND/OR	Not less than 6 months but not more than 3 years
Trademark Infringement and Unfair Competition	50,000 to 200,000 AND	2 years to 5 years
Copyright Infringement	First Offense: 50,000 to 150,000	First Offense: 1 year to 3 years
	Second Offense: 150,000 to 500,000	Second Offense: 3 years and 1 day to 6 years
	Third Offense and Subsequent Offenses: 500,000 to 1,500,000	Third Offense and Subsequent Offenses: 6 years and 1 day to 9 years

NOTE: The criminal action for repetition of patent infringement shall prescribe in 3 years from date of the commission of the crime

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

SCHEDULE OF PENALTIES UNDER R.A. 9711, THE FOOD AND DRUG ADMINISTRATION ACT OF 2009

VIOLATION	FINE (Php)	IMPRISONMENT
ANY PERSON WHO VIOLATES SEC. 11 HEREOF	Not less than 50,000 nor more than 500,000 AND/OR	Not less than 1 year nor more than 10 years
MANUFACTURER, IMPORTER, OR DISTRIBUTOR OF ANY HEALTH PRODUCT *	Not less than 500,000 nor more than 5,000,000 AND	Not less than 5 years nor more than 10 years
CONTINUING VIOLATION	Continuing Violation: Additional fine of one (1%) of the economic value/cost of the violative product or violation or Php 1,000, whichever is higher	

NOTE: Health products found in violation of the provisions of this Act and other relevant laws, rules and regulations **may be seized and held in custody pending proceedings, without hearing or court order**, when the director-general has reasonable cause to believe from facts found by him/her or an authorized officer or employee of the FDA that such health products may cause injury or prejudice to the consuming public.

SCHEDULE OF PENALTIES UNDER P.D. 1144, CREATING THE FERTILIZER AND PESTICIDE AUTHORITY AND ABOLISHING THE FERTILIZER INDUSTRY AUTHORITY

	FINE (Php)	IMPRISONMENT
ANY PERSON WHO VIOLATES P.D. 1144	If the amount of fertilizer is undetermined: Not less than 5,000 but not more than 10,000	
	If the amount of fertilizer involved is Php 10,000 or less: Amount equal to the value involved to three times such value but which shall in no case be less than 5,000 nor more than 20,000 AND	Not less than 10 years and 1 day nor more than 15
		If the amount of fertilizer involved is more than Php50,000: Not less than 15 years and 1 day nor more than 20 years

NOTE: If falsification of a public or commercial document is committed by reasons or on the occasion of the commission of any of the acts punishable herein, the offender shall be imposed of the maximum fine and term of imprisonment as above prescribed. If the violation is committed by a corporation, firm, partnership, cooperative, association or any other entity, the penalty shall be imposed upon the guilty office or offices and such corporation, firm, partnership, association or entity.

SCHEDULE OF PENALTIES UNDER R.A. 6969, THE TOXIC SUBSTANCES AND HAZARDOUS AND NUCLEAR WASTES CONTROL ACT OF 1990

	FINE (Php)	IMPRISONMENT
ANY PERSON WHO VIOLATES SEC 13 (a) to (c) of R.A. 6969	Not less than 600 nor more than 4,000 AND	Not less than 6 months and 1 day nor more than 6 years and 1 day (not covered by the Probation Law)
1. Offender is a foreigner	+	
	Deportation and barred from re-entering the Philippines after service of sentence	
2. Offender is a public officer	+	
	Dismissal and Perpetual disqualification from any Elective or Appointive position	
ANY PERSON WHO VIOLATES SEC 13 (d) of P.D. R.A. 6969		Not less than 12 years and 1 day nor more than 20 years
1. Offender is a foreigner	+	
	Deportation and barred from re-entering the Philippines after service of sentence	
2. Offender is managing partner, president, or chief executive of a corporation or other association	+	
	At least 500,000 in exemplary damages	
3. Offender is a public officer	+	
	Dismissal and Perpetual disqualification from any Elective or Appointive position	
ANY VIOLATION OF R.A. 6969	+	
	Administrative Fine of not less than 10,000 nor more than 50,000 (to be imposed by the Secretary of Natural Resources)	

SCHEDULE OF PENALTIES UNDER R.A. 9175, THE CHAIN SAW ACT OF 2002

VIOLATIONS	FINE	IMPRISONMENT
Selling, Purchasing, Re-selling, Transferring, Distributing or Possessing a Chain Saw Without a Proper Permit	Not less than 15,000 but not more than 30,000 AND/OR	Not less than 4 years, 2 months and 1 day nor more than 6 years
Unlawful Importation or Manufacturing of Chain Saw	Not less than 1,000 or more than 4,000 AND	Not less than 1 month nor more than 6 months
Tampering of Engine Serial Number	Not less than 1,000 nor more than 4,000 AND	Not less than 1 month nor more than 6 months
Actual Unlawful Use of Chain Saw	Not less than Php 30,000 but not more than 50,000 AND/OR	Not less than 6 years and one 1 day nor more than 8 years
Offender is a Public Officer	Regular schedule of penalties + Accessory penalty of Perpetual Disqualification from Public Office	

NOTE: The chain saws confiscated under this Section shall be sold at public auction to qualified buyers and the proceeds thereof shall go to the Department.

SCHEDULE OF PENALTIES UNDER P.D. 705, THE FORESTRY REFORM CODE OF THE PHILIPPINES

VIOLATIONS	FINE (Php)	IMPRISONMENT
Unlawful occupation or destruction of forest lands*	Not less than 500 nor more than 20,000 + Ten times the rental fees and other charges which would have accrued under a license agreement, lease, license, or permit AND	Not less than 6 months nor more than 2 years
Kaingin	Eight times the regular forest charges due on the forest products destroyed, without prejudice to the payment of the full cost of restoration of the occupied area as determined by the Bureau AND	Not less than 2 nor more than 4 years
Unlawful possession of implements and devices used by forest officers.	Not less than 1,000, nor more than 10,000 + Confiscation of such implements and devices, and automatic cancellation of the license agreement, lease, license or permit, if the offender is a holder thereof AND	Not less than 2 nor more than 4 years

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

Sale of wood products	Not less than 200 or the total value of the invoice, whichever is greater + Suspension of the dealer's license for a period of not less than 2 years	
------------------------------	--	--

NOTE: The Court shall further order the eviction of the offender from the land and the forfeiture to the Government of all improvements made and all vehicles, domestic animals and equipment of any kind used in the commission of the offense.

SCHEDULE OF PENALTIES UNDER R.A. 10175, THE CYBERCRIME PREVENTION ACT OF 2012

VIOLATIONS	FINE (Php)	IMPRISONMENT
Sec. 4(a) and 4(b)	Not less than 200,000 up to a maximum amount commensurate to the damage incurred AND/OR	6 years and 1 day to 12 years (Prision Mayor)
Sec. 4(a)(5)	Not more than Php 500,000 AND/OR	6 years and 1 day to 12 years (Prision Mayor)
Sec. 4 (a) if committed against Critical Infrastructure	Not less than 500,000 up to maximum amount commensurate to the damage incurred AND/OR	12 years and 1 day to 20 years (Reclusion Temporal)
Sec. 4(c)(1)	Not less than 200,000 nor more than 1,000,000 AND/OR	6 years and 1 day to 12 years (Prision Mayor)
Sec. 4(c)(2)	One degree higher than the penalties provided for under R.A. 9775, the Anti-Child Pornography Act of 2009	
Sec. 4(c)(3)	Not less than 50,000 nor more than 250,000	1 month and 1 day to 6 months (Arresto Mayor)
Sec. 5	Not less than 100,000 nor more than 500,000 AND/OR	One degree lower than the penalty prescribed
When the punishable acts are committed on behalf of or for the benefit of a juridical person by a natural person acting with authority	Double the amount of the fines imposable for any punishable act under this law that also constitutes a violation of	

ANNEX E: NON-EXHAUSTIVE LIST OF PENALTIES

	the Revised Penal Code or other special laws, up to a maximum of 10,000,000 OR 5,000,000, if the violation was due to lack of supervision or control	
--	--	--

ANNEX 1

REPUBLIC OF THE PHILIPPINES)
CITY OF _____) S.S.

**SWORN DECLARATION AND UNDERTAKING FOR EXEMPTION
 FROM REGISTRATION OF DATA PROCESSING SYSTEMS**

I [Name of Data Protection Officer/Authorized Representative], of legal age, and residing at [Address of DPO/Authorized Representative], after having been duly sworn in accordance with law, do hereby depose and state that:

1. I am the [Data Protection Officer (“DPO”) or Authorized Representative] of [Name of PIC/PIP] with the following contact details:
 - a. Office Address: _____;
 - b. DPO Name: *(if through Authorized Representative)*;
 - c. DPO Email Address: _____; and
 - d. Contact Number: _____;
2. I am duly authorized to issue this Sworn Declaration and Undertaking on behalf of [Name of PIC/ PIP] as manifested in the attached [proof of authority such as a Board Resolution embodied in a Secretary’s Certificate];
3. [Name of PIC/PIP] does not meet the registration requirements for all of the following reasons:
 - [Name of PIC/PIP] employs less than two hundred fifty (250) persons;
 - the processing by [Name of PIC/PIP] does not include sensitive personal information of at least one thousand (1,000) individuals;
 - [Name of PIC/PIP] does not process any information likely to pose a risk to the rights and freedoms of data subjects including those that involve information likely to affect national security, public safety, public order, or public health or information required by applicable laws or rules to be confidential; vulnerable data subjects like minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a PIC or PIP, especially those involving automated decision-making or profiling; and

- o [Name of PIC/PIP] is not a government agency or instrumentality;
4. I undertake that [Name of PIC/PIP] shall comply with orders of the Commission requiring the submission of additional documents and other relevant information, and that failure to comply with such orders will be subject to fines and other applicable penalties;
 5. I undertake to immediately inform the Commission by filing a new Sworn Declaration and Undertaking within ten (10) days from any change in the declarations in number 1;
 6. I undertake to immediately register with the Commission within twenty (20) days from existence of facts showing that the basis for this Sworn Declaration and Undertaking is no longer true;
 7. I am executing this Sworn Declaration and Undertaking to attest to the truth of the foregoing statements and to comply with the requirements of the Data Privacy Act, its Implementing Rules and Regulations, and other relevant issuances of the National Privacy Commission.

IN WITNESS WHEREOF, I have hereunto set my hand this _____ day of _____, 20__ at _____, Philippines.

[Name of Data Protection Officer/Authorized Representative]
Affiant

SUBSCRIBED AND SWORN to before me this ____ day of _____, 20__, Affiant exhibiting to me a competent proof of identity _____ issued at _____ on _____.

NOTARY PUBLIC

Doc No. _____;
Page No. _____;
Book No. _____;
Series of _____.



Trunkline

8234-2228

Local numbers

Compliance 118

Complaints 114

Advisory opinions 110

Other inquiries 117

Website

privacy.gov.ph

Social media

fb.com/privacy.gov.ph

twitter.com/privacyPH

Address

5th Floor Delegation

Building

PICC Complex, Roxas

Boulevard

