



THE 2020-2021 COMPENDIUM OF NPC ISSUANCES

MESSAGE



The release of the Compendium of the National Privacy Commission's issuances remains a vital element in the Commission's efforts, not only in its campaign to raise awareness on data subject rights, but also to guide various stakeholders in effectively complying with Republic Act No. 10173, or the Data Privacy Act of 2012.

During 2020 and 2021, the Commission experienced the unprecedented challenge of balancing the two priorities of supporting public health measures brought about by the COVID-19 pandemic and upholding data privacy. Nonetheless, the Commission prevailed in protecting the data privacy rights of our citizens while recognizing the right of the people to health in the midst of a public health emergency.

In enforcing data protection and privacy laws to protect Filipinos in the new normal, the Commission released a variety of issuances, including Joint Memorandum Circulars with the Department of Health (DOH), Public Health Emergency (PHE) bulletins, Advisory Opinions, Memoranda, Decision, Resolutions, and Orders. This Compendium presents these issuances to empower data subjects and guide the public health authorities, local governments and other stakeholders, in terms of data privacy and protection.

The Compendium is consistent with the continued intensive awareness campaigns of the Commission. It believes that the Compendium will support the efforts of businesses, government agencies, and other stakeholders in implementing intensive data privacy security measures in protecting our citizens' personal data. The Commission continues to urge our stakeholders in leveraging data privacy and protection to establish trust with their customers.

A key thrust of the NPC is to empower the data subjects by arming them with knowledge in protecting their data. With the Commission's issuance of this Compendium, we hope to better guide our citizens and stakeholders. May this Compendium expand the knowledge on data privacy of our citizens, policymakers, privacy professionals, and allies. Likewise, may it ignite their enthusiasm in joining the Commission on the road towards strengthened data privacy policies and regulations.

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

MESSAGE



Since the start of the COVID-19 pandemic, the National Privacy Commission has worked harder to promote the fundamental human right to privacy. This is in response to the increasing concerns on the potential tradeoff between public health and data privacy. Some parties even advocated that privacy should take a backseat to enable the efficient sharing and disclosure of personal data as part of the measures to mitigate the impact of this pandemic.

The Commission remains firm that data privacy should neither be seen as an obstacle to saving lives nor as a barrier to the free flow of information. Instead, privacy serves as an enabler for the continued use of various technologies primarily developed to defeat this pandemic. After all, people need to trust these technologies before they will use it.

The Commission has ensured that the significant role of privacy, particularly in the context of this pandemic, is clear to all Filipinos through its various Circulars, Advisories, and Advisory Opinions. More importantly, the Commission hopes that the public, and those who involved in the processing of personal data, will refer to its Decisions, Resolutions, and Orders to gain a deeper understanding of the fundamental principles of the Data Privacy Act of 2012. These Decisions, Resolutions, and Orders provide clarity and guidance based on actual experiences of data subjects, personal information controllers and personal information processors on issues relating to, among others, breach management, privacy impact assessments, reasonable expectation of privacy, penalties, the necessary lawful criteria of processing, and the general privacy principles of transparency, legitimate purpose, and proportionality.

On a personal note, I hope we begin to realize that privacy, as expounded in the Commission's issuances, is not detached from our own human experiences. When we share our personal data, it is expected that the context, purpose, and relationship in that disclosure will be treated with utmost respect. After all, personal data, when shared, still belongs to us. Everyone else is just a custodian.

Finally, I hope that these issuances will help people develop a more profound appreciation of the importance of privacy, and ultimately, renew the country's commitment to build a culture of privacy, one reader at a time.

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

TABLE OF CONTENTS





14 ADVISORY OPINION

- 14 Advisory Opinion No.2019-049**
Facial Recognition for ID System
- 16 Advisory Opinion No.2019-050**
Request for the Last Known Address
of a Former Employee
- 21 Advisory Opinion No.2019-051**
Right to Delete Account through
E-mail
- 25 Advisory Opinion No.2019-052**
Teenage Pregnancy Registry
- 28 Advisory Opinion No.2020-001**
Use of Body-worn Camera Pursuant
to a PEA Tollway Corporation Policy
- 32 Advisory Opinion No.2020-002**
Publication of the Full Content of
Bureau of Internal Revenue (BIR)
Rulings in the BIR Website
- 37 Advisory Opinion No. 2020-003**
Information on Vehicle Ingress and
Egress

- 40 Advisory Opinion No. 2020-004**
Request for the Guidance on the
Disclosure of List of Deceased
Barangay Officials (DBOs) from 2002
to 2011

- 44 Advisory Opinion No. 2020-005**
Verification of Pre-Employment
Document

- 48 Advisory Opinion No. 2020-006**
Collection Agency Communicating
with Human Resource Department

- 60 Advisory Opinion No. 2020-007**
Request for Copies of Statement of
Assets, Liabilities, and Net Worth
(SALN) from the Bureau of Treasury

- 52 Advisory Opinion No. 2020-008**
Video Documentation of Mandatory
Training for Safety Officers

- 59 Advisory Opinion No. 2020-009**
Deletion of Electronic Medical Records

- 63 Advisory Opinion No. 2020-010**
Philippine Health Insurance
Corporation Inspection and
Monitoring Activities

- 68 Advisory Opinion No. 2020-011**
Access to Sibling's Birth Certificates
for Obtaining Tax Identification
Numbers

- 72 Advisory Opinion No. 2020-012**
Disclosure of Insurance Policy
Details to the National Bureau of
Investigation

- 75 Advisory Opinion No. 2020-013**
Access to Information in Relation
to Disciplinary Records and/or
Administrative Cases of Students and
School Personnel
- 80 Advisory Opinion No. 2020-014**
Obtaining Address of Accused
through Learner Reference Number
(LRN)
- 83 Advisory Opinion No. 2020-015**
Collection of Personal Data by the
Bureau of Internal Revenue for Tax
Compliance Purposes
- 88 Advisory Opinion No. 2020-016**
Audit Procedures of the Commission
on Audit
- 92 Advisory Opinion No. 2020-017**
Termination of Services due to
Corporate Dissolution
- 97 Advisory Opinion No. 2020-018**
Outsourcing the Processing of
Personal Data
- 100 Advisory Opinion No. 2020-019**
Public Disclosure of the List of Social
Amelioration Program Beneficiaries
- 106 Advisory Opinion No. 2020-020**
Collection of Fees Relative to Right to
Correction of Data Subjects' Personal
Information
- 109 Advisory Opinion No. 2020-021**
Automated Retrieval of Bank
Transaction History

- 115 Advisory Opinion No. 2020-022**
Public Disclosure of Identities of
COVID Patients for Contract Tracing
- 120 Advisory Opinion No. 2020-023**
Public Posting of Listahan Respondents
- 124 Advisory Opinion No. 2020-024**
Disclosure of Lot Buyers’/
Homeowners’ Contact Information
for Collection of Monthly Association
Dues
- 128 Advisory Opinion No. 2020-025**
Conflict of Interest on a Data
Protection Officer Designated as a
Compliance Officer
- 133 Advisory Opinion No. 2020-026**
Public Disclosure of Pertinent Data
Needs in the time of COVID-19
- 141 Advisory Opinion No. 2020-027**
Admissibility of Personal Data Sheet
in an Administrative Investigation
- 144 Advisory Opinion No. 2020-028**
Collection and Encoding of
Information on COVID-19 Related
Deaths
- 148 Advisory Opinion No. 2020-029**
Request for Personal Information of
Complaints under the Katarungang
Pambarangay Process for Thesis
Purposes
- 153 Advisory Opinion No. 2020-030**
Reporting to the Department of the
Interior and Local Government of
COVID-19 related Hospital Deaths

- 156 Advisory Opinion No. 2020-031**
Access to Files and Records of Anti-Illegal Drugs Operations of the Philippine Drug Enforcement Agency

CIRCULARS

- 161 Joint Memorandum Circular
No. 2020-01**
Department of Health - National Privacy Commission (DOHNPC)
Joint Memorandum Circular No. 2020-0001 entitled “Guidelines on the Use of Telemedicine in COVID-19 Response”
- 168 Joint Memorandum Circular
No. 2020-02**
Privacy Guideline on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response
- 179 Joint Memorandum Circular
No. 2020-03**
Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response
- 206 NPC Circular No. 20-01**
Guidelines on the Processing of Personal Data for Loan-Related Transactions
- 212 NPC Circular No. 20-02**
Cease and Desist Orders

- 226 NPC Circular No. 20-03**
Data Sharing Agreements

DECISIONS

- 238 NPC Case No. 18-152**
MRS v National Conciliation
and Mediation Board (NCMB)
and Department of Labor and
Employment (DOLE)
- 244 NPC Case No. 18-155**
HNT v Eastwest Bank
- 252 NPC Case No. 19-498**
JBA v U-Peso.ph Lending Corporation
(UPESO)
- 263 NPC Case No. 19-1221**
RBD v Fcash Global Lending, INC.
(FAST CASH)
- 266 NPC Case No. 18-103**
ECA v XXX
- 273 NPC Case No. 19-653**
BGM v IPP
- 283 NPC Case No. 19-910**
In Re: FL Operating ABC Online
Lending Application
- 325 CID Case No. 17-K-001**
JCR v Globe Telecom, Inc
- 330 CID Case No. 18-D-012**
JBD v JI and VVV

ORDER

339 IN RE: LISENSYA.INFO

CEASE AND DESIST ORDER

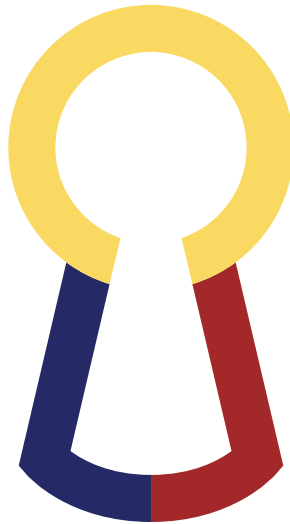
Initiated as an Independent NPC Investigation into the Possible Data Privacy Violations Committed by the website LISENSYA.INFO.

353 IN RE: LISENSYA.INFO

ORDER Re: Extension of Cease and Desist Order

Initiated as an Independent NPC Investigation into the Possible Data Privacy Violations Committed by the website LISENSYA.INFO.

359 NPC 2021 COMPENDIUM OF ISSUANCES



NATIONAL PRIVACY COMMISSION

5th Floor Delegation Building, PICC Complex, Roxas Boulevard

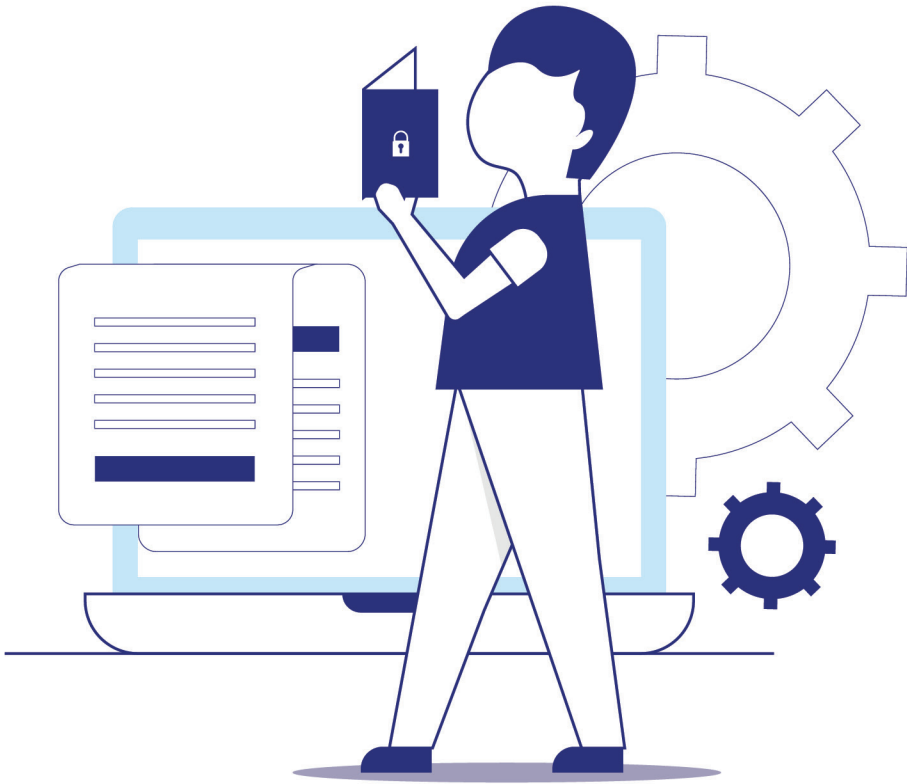
NPC Trunk line No: 8234-2228

For registration & compliance concerns– 118

For complaints– 114

For advisory opinions– 110

For other inquiries– 117



ADVISORY OPINIONS

ADVISORY OPINION NO. 2019-049¹

11 December 2019

[REDACTED]

Re: **FACIAL RECOGNITION FOR ID SYSTEM**

Dear [REDACTED],

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) via email. You inquire on whether the NPC has recommended or approved any procedure on written, electronic and recorded means in obtaining the express consent of the individual prior to conducting facial recognition for the entry of individual to a private building in lieu of presenting identification cards. If in the negative, you request guidance on the use of facial recognition for identification.

Section 3(d) of Republic Act No. 10173,² otherwise known as the Data Privacy Act of 2012 (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.” Accordingly, images of an individual are personal information and fall under the protection of the DPA.

The NPC has yet to issue official guidelines on the use of facial recognition in lieu of identification cards, including the process obtaining consent from the data subject. However, the general data privacy principles of transparency, legitimate purpose and proportionality should prevail, and the provisions of the DPA should be upheld, including the rights of the data subjects.

¹Tags: Consent; Facial Recognition; Identification.

²An 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

Using facial recognition as a means to identify an individual entering buildings and premises must be grounded on any of the lawful criteria for processing under Section 12 of the law. In this situation, the identification of the individual is linked to ensuring the safety and security of the premises and its occupants, which may fall under “legitimate interests pursued by the personal information controller” under Section 12 (f)³ under the DPA. To comply with transparency and the right of the data subject to be informed, employees or occupants of buildings must first be apprised of the use of facial recognition as the chosen identification system, and any information related to the processing of their information in connection such system.

This opinion is based solely on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

³(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

ADVISORY OPINION NO. 2019-050¹

12 December 2019

[REDACTED]

Re: **REQUEST FOR THE LAST KNOWN ADDRESS OF A
FORMER EMPLOYEE**

Dear [REDACTED],

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) where you seek clarification on whether the Metropolitan Waterworks & Sewerage System (MWSS) may provide the last known address of its former employee at the request of the Commission on Audit (COA), pursuant to Section 7, Rule IV of its 2009 Revised Rules of Procedures.

We understand that you have denied the request of COA for having no clear indication in the said provision that compels your office to submit such information.

The 2009 Revised Rules of Procedures of the COA applies to its pleadings and practice in all matters, actions and proceedings originally acted upon by or appealed to it in the exercise of its quasi-judicial function, including administrative cases.²

Per COA's letter to your office, the request for the last known address of your former employee was made in accordance with Section 7, Rule IV of the same rules, to wit:

¹Tags: Address, Employee, Commission on Audit, COA, Government, Legal obligation, Personal information, Proportionality

RULE IV PROCEEDINGS BEFORE THE AUDITOR

XXX XXX XXX

Section 7. Service of Copies of ND/NC/NS, Order or Decision. The ND, NC, NS, order, or decision shall be served to each of the persons liable/responsible by the Auditor, through personal service, or if not practicable through registered mail. In case there are several payees, as in the case of a disallowed payroll, service to the accountant who shall be responsible for informing all payees concerned, shall constitute constructive service to all payees listed in the payroll.

From our understanding of the abovementioned provision, the purpose of the request is to be able to serve the corresponding copies of Notice of Disallowance/Charge (ND/NC) and/or Notice of Suspension (NS)³ to the person considered liable by the Auditor, either through personal service or his/her registered mail.

The Data Privacy Act of 2012⁴ (DPA) applies to all types of processing of personal data in the country or outside, subject to certain qualifications.⁵ The last known address of a former employee is considered personal information⁶ under the DPA.

Pursuant to Section 12 of the DPA, processing of personal information may only be allowed if not otherwise prohibited by law and when justified by at least one of the conditions therein, such as the following:

³ 2009 Revised Rules of Procedures of the Commission on Audit, Rule IV, § 4 - Audit Disallowances/Charges/Suspensions. - In the course of the audit, whenever there are differences arising from the settlement of accounts by reason of disallowances or charges, the auditor shall issue Notices of Disallowance/Charge (ND/NC) which shall be considered as audit decisions. Such ND/NC shall be adequately established by evidence and the conclusions, recommendations or dispositions shall be supported by applicable laws, regulations, jurisprudence and the generally accepted accounting and auditing principles. The Auditor may issue Notices of Suspension (NS) for transactions of doubtful legality/validity/propriety to obtain further explanation or documentation.

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 Id., §4.

⁶ 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.

SECTION 12. Criteria for Lawful Processing of Personal Information. – 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;
- (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.⁷

In this regard, we note COA's mandate as provided for under Section 2, Article IX-D of the 1987 Philippine Constitution, which states that:

Section 2. (1) **The Commission on Audit shall have the power, authority, and duty to examine, audit and settle all accounts pertaining to the revenues and receipts of, and expenditures or uses of funds and property, owned or held in trust by, or pertaining to the Government, or any of its subdivisions, agencies, or instrumentalities,** including government-owned and controlled corporations with original charters, and on a post-audit basis: (a) constitutional bodies, commissions

⁷ Data Privacy Act of 2012, § 12. Emphasis supplied.

and offices that have been granted fiscal autonomy under the Constitution; (b) autonomous state colleges and universities; (c) other government-owned or controlled corporations and their subsidiaries; and (d) such non-governmental entities receiving subsidy or equity directly or indirectly, from or through the government, which are required by law or the granting institution to submit to such audit as a condition of subsidy or equity. However, where the internal control system of the audited agencies is inadequate, the Commission may adopt such measures, including temporary or special pre-audit, as are necessary and appropriate to correct the deficiencies. It shall keep the general accounts of the Government, and for such period as may be provided by law, preserve the vouchers and other supporting papers pertaining thereto.

(2) The Commission shall have exclusive authority subject to the limitations in this Article, to define the scope of its audit and examination, establish the techniques and methods required therefor, and **promulgate accounting and auditing rules and regulations including those for the prevention and disallowance of irregular, unnecessary, excessive, extravagant, or unconscionable expenditures, or uses of government funds and properties.**

Considering the mandate of the COA, the Auditor may rely on Section 12(c) of the DPA as the appropriate basis for the lawful processing of personal information.

We note however that any processing of personal information shall also adhere to the principles of transparency, legitimate purpose, and proportionality.⁸ Thus, the disclosure shall be only limited to the last known address of the former COA employee for the purpose as stated by COA.

⁸ Id., § 11.

This opinion is being rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO

OLC-Director IV, Privacy Policy Office Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

ADVISORY OPINION NO. 2019-051¹

18 December 2019

[REDACTED]

Re: **RIGHT TO DELETE ACCOUNT THROUGH E-MAIL**

Dear [REDACTED],

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) where you seek clarification on the data subject's exercise of the right to withdraw his or her consent and/or have his or her data deleted from the system of a personal information controller (PIC)² in a reasonable manner such as through e-mail, which is allegedly not allowed by Cashalo unless accompanied by a signed letter of request through snail mail with two copies of valid IDs.

We understand that you sent Cashalo a request via email for deletion of your account, following the instruction provided under the Privacy Policy statement in their website. However, your request was denied until fulfillment of the requirement to submit the request to their office and provide identification, as indicated above. You claim that it is unreasonable for them to ask you to send snail mail when e-mail can be used. You further claim that you already had several cases of successful account deletion with other service providers through e-mail.

¹ Tags: Right to erasure; blocking; deletion of account; data subjects rights.

² Data Privacy Act of 2012, §3(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 information in connection with the individual's personal, family or household affairs.

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).

Data subjects' rights; withdrawal of consent; procedure for the exercise of rights

Section 16 of the Data Privacy Act of 2012³ (DPA) and Section 34 of its Implementing Rules and Regulations (IRR), provide for the rights of the data subjects. In particular, Section 34 (e) of the IRR states:

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 or 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.
2. The personal information controller may notify third parties who have previously received such processed personal information.⁴

⁴ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 34(e) (2016).

The law and the rules are silent on the procedure of the exercise the right to erasure or blocking. However, the instances wherein this right applies are enumerated, such as when the data subject withdraws consent or objects to the processing of his or her personal data.

We note that Cashalo included in its Privacy Policy posted in its website, the following procedure for the exercise of the abovementioned right of a data subject, to wit:

If you wish to exercise your right to access, correction, cancellation, portability and objection rights as described below, or for complaints and other inquiries, **please send a registered letter with return receipt to 16F World Plaza Building, 5th Avenue, Bonifacio Global City, Taguig City 1634, Philippines or email hello@cashalo.com** to the attention of Data Privacy Officer:

XXX XXX XXX

to update, correct, supplement, or delete the data, to block or render anonymous data that have been processed unlawfully, including data whose retention is unnecessary for the purpose for which such data have been collected or subsequently processed; to have a certification that the operations requested have been completed, as also related to their contents, to the entities to which the data were communicated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected; to receive the personal data concerning you and copy or transmit it to another data controller (right to data portability);⁵

XXX XXX XXX

As can be gleaned from the above, the instructions given by Cashalo indicate that the data subject has the option to send a request to the Data Privacy Officer through snail mail or e-mail in order to assert his or her rights.

⁵ Cashalo, Privacy Policy, available at <https://www.cashalo.com/privacy-policy/> (last accessed Dec. 18, 2019). Emphasis supplied.

Cashalo may institute additional policies especially when the need arises, such as requiring the submission of other documentation, i.e. signed letter, copies of valid identification/s, etc. as PICs equally have a responsibility to ensure the identity of the requestor in order to validate any requests before granting them.

Nonetheless, in keeping with the thrust of upholding data subjects' rights and enabling the free exercise of these rights, any additional submissions, if absolutely necessary, should likewise be possible to be made through electronic mail as well.

The DPA places emphasis on the PIC's compliance in addressing requests satisfactorily, without undue delay. The actual methodology to be implemented for addressing such requests, at the minimum, should be simple and not have the effect of discouraging such requests from data subjects.

This opinion is being based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-052¹

19 December 2019



RE: **TEENAGE PREGNANCY REGISTRY**

Dear ,

We write in response to your request for advisory opinion regarding the data sharing of teenage pregnancy registry between your institution, Southern Isabela General Hospital (SIGH) and the City Population Office (CPO) of Santiago City.

We understand that the CPO of Santiago City is requesting for the following personal data from your institution for the purpose of creating plans, activities, or any possible interventions in the campaign to decrease the incidence of teenage pregnancy in your city:

1. Complete name of female client;
2. Age;
3. Admission;
4. Discharge;
5. Final Diagnosis; and
6. Barangay.

The abovementioned information being requested by the CPO are health information. Health information, under the Data Privacy Act of 2012 (DPA),² is considered as sensitive personal information and processing of such information is prohibited, except if the following cases:

¹ Tags: Data sharing, Registry, Collection of Sensitive Personal Information, Teenage Pregnancy, Health Information, Transparency, Legitimate purpose, Proportionality.

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).

- 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.³

Note that we cannot confirm the basis of the proposed data sharing agreement from the information provided. It is not clearly indicated whether a law or city ordinance was issued that mandates the CPO to collect sensitive personal information for teenage pregnancy registry and the specific program or project that needs the said personal data for implementation.

³ Id. § 13.

The purpose of the collection, “to create plans and activities or any possible interventions in the campaign to decrease the incidence of teenage pregnancy in the city” is general in nature, which may be attainable even without the disclosure of personal information.

On its face, without the specific purpose and statutory basis of the CPO, the planning and execution of activities and campaigns on teenage pregnancy may be administered and implemented with the use of aggregate or statistical data.

Should the data sharing push forward, SIGH must ensure that the proposed data sharing agreement with the CPO has complied with the requirements of the DPA, must conform with the NPC Circular No. 16-02, and has met any of the abovementioned criteria for lawful processing before sharing such information with the CPO of Santiago City. Likewise, the data sharing must adhere to the principles of transparency, legitimate purpose and proportionality.

This opinion is based solely on the information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. The attached data sharing agreement was not reviewed for the purpose of clarifying the basis of the said processing.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO

OIC-Director IV, Privacy Policy Office Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

ADVISORY OPINION NO. 2020-001¹

29 January 2020



Re: **USE OF BODY-WORN CAMERA PURSUANT TO
A PEA TOLLWAY CORPORATION POLICY**

Dear ,

We write in response to your request for an advisory opinion which sought guidance regarding the applicability of the provisions of the Data Privacy Act of 2012² (DPA) to the Memorandum dated 5 August 2019 and Policy and Procedure for the Use of Body Worn Camera (BWC) (Policy) dated 9 July 2019, issued by the PEA Tollway Corporation (PEATC).

Specifically, you requested for clarification on the following:

1. Whether the use of body-worn cameras by the Patrol Officers, pursuant to the aforementioned Memorandum and Policy, will violate the DPA; and
2. What operating procedures should best be followed to be able to comply with the Memorandum and Policy while at the same time, also comply with the provisions of the DPA.

Functions of PEATC

We understand that PEATC is a wholly-owned subsidiary of the Philippine Reclamation Authority (PRA), an attached agency of the Department of Environment and Natural Resources.

¹ Tags: scope, lawful processing, legal obligation, public authority, law and regulation, 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).

Pursuant to Section 15.03 of the Toll Operations Agreement (TOA) approved by the Toll Regulatory Board (TRB), PEATC shall undertake and perform the Operations and Maintenance obligations of the PRA, specifically to manage, operate, monitor, maintain and repair the Manila-Cavite Toll Expressway Project now known as Cavitetex.³

The agreement was entered into pursuant to the power of the TRB to grant authority to operate a toll facility and to issue therefore the necessary “Toll Operation Certificate” subject to such conditions as shall be imposed by the Board, under the Toll Operation Decree of 1977.⁴ Under the granted authority, the PEATC is given the power to issue rules and regulations to carry out the purposes of the Toll Operation Decree⁵ and by this authority, the subject Memorandum and Policy was issued accordingly.

The Memorandum and Policy issued by PEATC requires Patrol/Traffic Officers to use PEATC-issued BWCs when apprehending traffic violators, rendering assistance to motorists, making an arrest, engaging in confrontational encounters with the public, or any other incidents deemed necessary by the Patrol/Traffic Officer to record.

Audio-visual recordings; lawful processing of personal data

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.⁶ Accordingly, the image of an identifiable individual captured in a photograph or video is personal information about the individual, and thus, covered by the DPA.

The collection and use of audio-visual recordings captured by these BWCs may find basis under Section 12 of the DPA, specifically where the processing is necessary for compliance with a legal obligation⁷ or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.⁸

³ PEATC official website, About PEATC, available at <http://peatc.gov.ph/about-us/about-peatc> (last accessed Jan. 30, 2020).

⁴ Authorizing the Establishment of Toll Facilities on Public Improvements, Creating a Board for the Regulation Thereof, and for Other Purposes [Toll Operation Decree of 1977], Presidential Decree No. 1112, § 3 (e) (1977).

⁵ *Ibid.*

⁶ Data Privacy Act of 2012, §20 (c).

⁷ *Id.* § 12 (c).

⁸ *Id.* § 12 (f).

In addition, Section 13 of the DPA may likewise apply where a BWC footage or image would reveal sensitive personal information. Thus, the processing of the same may be allowed if provided for by existing laws and regulations.⁹

From the foregoing, PEATC has a mandated regulatory function specifically to enforce and monitor traffic rules and regulations within Cavitex. As such, the PEATC, being a public authority acting within its mandate, is permitted under the DPA to process such personal data.

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.

General data privacy principles; data subjects' rights; security measures

The principle of transparency enshrined in the DPA 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.

PEATC must have the appropriate privacy notices to apprise data subjects that the traffic officers are equipped with BWCs that will capture audio-visual recordings in certain instances, i.e. apprehending traffic violators, rendering assistance to motorists, making an arrest, among others. These notices may be posted in conspicuous areas within the Cavitex and should likewise be available in PEATC's website.

We recognize the "Notification Spiel" under Sections 5.4.1 of the Policy which shall inform data subjects at the very outset of the activated BWC. The same may still be further improved, taking into consideration the exigencies of the actual operations on the ground and feedback from both the Patrol/Traffic Officers and the data subjects.

⁹Id. § 13 (b).

Lastly, the PEATC and its Patrol/Traffic Officers are mandated under 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. Refer to NPC Circular No. 2016-01 - Security of Personal Data in Government Agencies for further details.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2020-002¹

06 February 2020



Re: **PUBLICATION OF THE FULL CONTENT OF BUREAU
OF INTERNAL REVENUE (BIR) RULINGS IN THE BIR
WEBSITE**

Dear [REDACTED],

We write in response to your request for an advisory opinion seeking to clarify the following matters regarding the Data Privacy Act of 2012² (DPA) and the Unlawful Divulgence Rule under Section 270 of the National Internal Revenue Code of 1997³ (NIRC), as amended, in relation ease of doing business and the State's policy of public disclosure of all its transactions involving public interest embodied in Executive Order (EO) No. 02, s. 2016.⁴

Specifically, you request for clarification on the following:

1. Whether the publication of the full content of BIR Rulings may be done without violating the provisions of the DPA, as well as Section 270 of the NIRC; and
2. If publication of the full content will violate the aforementioned laws, may publication be done through redacting and masking personal or sensitive personal information as defined under the DPA and the information covered by Section 270 of the NIRC, as amended.

1 Tags: scope, lawful processing, public authority, mandate, 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).

3 AN ACT AMENDING THE NATIONAL INTERNAL REVENUE CODE, AS AMENDED, AND FOR OTHER PURPOSES [“Tax Reform Act of 1997”], Republic Act No. 8424 (1997).

4 Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies to Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor, Executive Order

Scope of the DPA; subject of advisory opinions

We wish to clarify that information of corporate taxpayers, i.e. corporate name, address, tax identification numbers, business transactions, etc. are not covered by the DPA since these pertain to information of juridical persons and does not identify an individual. As such, processing of information pertaining to such juridical entities, including publication thereof, is not governed by the DPA.

Note also that the subject of advisory opinions of the National Privacy Commission (NPC) revolves around the interpretation of the provisions of the DPA, its Implementing Rules and Regulations (IRR) and NPC issuances, compliance requirements under the DPA, enforcement of data privacy laws, and other related matters on personal data privacy, security, and protection.⁵

Thus, the interpretation of the provisions of the NIRC, particularly Section 270, are not within the purview of our mandate. For purposes of this advisory opinion, the discussion shall be limited to the application of the DPA, its IRR and NPC issuances on the publication of the full content of BIR Rulings.

Transparency; public authority; mandate

The DPA has the twin task of protecting the fundamental human right to privacy whilst ensuring the free flow of information to promote innovation and growth.⁶ For this very reason, the DPA shall not operate to hinder the BIR from adopting measures that it may deem necessary and crucial to promote transparency in its transactions involving public interest, to bolster the Constitutional right of every citizen to information on matters of public concern, and to comply with EO No. 2. The DPA is not meant to prevent government institutions from processing personal data when necessary to fulfill their mandates.⁷

The above must be harmonized with the protection of the fundamental human right to privacy. The DPA dictates that any person or entity who processes personal and/or sensitive personal information (collectively, personal data) shall still be subject to its provisions.

⁵ National Privacy Commission, Rules of Procedure on Requests for Advisory Opinions, Circular No. 18-01 [NPC Circular 18-01] (September 10, 2018).

⁶ Data Privacy Act of 2012, § 2.

⁷ National Privacy Commission, NPC Advisory Opinion No. 2018-083 (Nov. 26, 2018).

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

(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

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

(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. (Underscoring supplied)

We acknowledge the fact that BIR is a public authority tasked with the duty, among others, to ensure compliance with the NIRC and other tax laws, rules, and regulations. We also understand that BIR Rulings are official positions of the BIR on inquiries of taxpayers who request clarification on certain provisions of the NIRC, other tax laws or other implementing regulations, usually for the purpose of seeking tax exemption.⁸

The publication of BIR rulings is a matter of public concern as it aims to apprise taxpayers of essential information on how the BIR treats various transactions and the corresponding tax implications.

⁸ Bureau of Internal Revenue, Revenue Memorandum Order No. 9-2014 [RMO No. 9-2014] (February 6, 2014).

This may help uninformed taxpayers on how to avail of the benefits provided under the NIRC, such compromise and abatement of tax liabilities, tax credits and refunds, among others.

Broader dissemination of BIR rulings through the BIR website may even possibly prevent tax evasion as such rulings will give taxpayers a better understanding of the tax laws and regulations and their concomitant responsibility filing the proper tax returns and paying the correct amount of taxes.

General data privacy principles; proportionality

While there may be a lawful basis for the publication of BIR rulings, the BIR, as a personal information controller, must still adhere to the general data privacy principles, particularly the principle of proportionality. This principle dictates that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.⁹ Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.¹⁰

We understand that the BIR collects various personal data for a better understanding of the materials facts surrounding a transaction for which a BIR ruling has been requested. These may include names, addresses, tax identification numbers, among others.

As these rulings will be published in the BIR website, it is recommended that the same be formulated in such a manner whereby only the factual circumstances of the transaction and how the BIR interprets and applies the NIRC in relation to such circumstances shall be included in the ruling, without necessarily disclosing personal data, especially sensitive personal information.

If a particular ruling cannot otherwise be crafted in the above manner, the BIR may opt to redact the ruling to be posted on the BIR website. This is similar to our previous pronouncement in Advisory Opinion No. 2018-018 ¹¹ regarding the online publication of PhilHealth decisions, where we advised PhilHealth to consider posting a redacted or pseudonymized version of the decision or case digests which may be sufficient for public information.

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

¹⁰ Ibid.

¹¹ National Privacy Commission, NPC Advisory Opinion No. 2018-018 (12 April 2018).

From the foregoing, the publication of the full content of BIR Rulings may be done without violating the provisions of the DPA, considering the discussions above on the BIR's mandate. However, bearing in mind the principle of proportionality, it is recommended that as a best practice, the BIR should endeavor to formulate these rulings without necessarily disclosing personal data, especially sensitive personal information, if feasible. In all cases, the BIR always has the option to redact the rulings to be posted on the BIR website.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2020-003¹

3 February 2020

[REDACTED]

Re: **INFORMATION ON VEHICLE INGRESS AND EGRESS**

Dear [REDACTED],

We write in response to your inquiry received by the National Privacy Commission (NPC) seeking to clarify the nature of vehicle ingress and egress information in light of the Data Privacy Act of 2012² (DPA).

We understand from your letter that your company, Serendra Condominium Corporation (SCC), received a letter from one of your residents (“A”) through a certain law office requesting SCC to release the record of ingress and egress of the resident’s vehicle on 23 July 2018 (“Subject Information”). However, as confirmed from your records, A is married to B, the latter also a registered SCC resident. Thus, you opined that the vehicle may be conjugal property and SCC cannot determine who used and was in possession of the car on the said date.

In its reply to the law firm, SCC requested a sworn-affidavit from A stating that she was in actual use and possession of the vehicle. The purpose of the affidavit is to ensure that A is the owner and driver of the subject vehicle at that time. However, the law firm responded that the Subject Information is neither privileged nor confidential and does not contain sensitive personal information and thus is not covered by the DPA.

¹ Tags: personal information, data subject, data subjects’ rights

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Govern-

You now seek clarification on the following questions:

- (a) Whether the vehicle ingress and egress of the resident is considered as personal information under the DPA; and
- (b) Assuming that it is personal information, is the Subject Information owned by the registered owner of the vehicle or the actual possessor/driver of the vehicle during the requested period?

Vehicle ingress and egress as personal information; access; disclosure; legitimate interest

As defined under the DPA, personal information is any information 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

Taking from the definition, the exact location of an individual at a certain date and time when put together with other information may directly and certainly identify an individual. Thus, the ingress and egress of a vehicle driven by an individual, which point to the individual's location at a certain time and date is considered personal information.

As to the second inquiry, the vehicle ingress and egress may pertain to both the personal information of the registered owner of the vehicle and/or the driver or the possessor of the vehicle at that specific moment. The details of an individual's movement or whereabouts are considered personal information. At the same time, because the vehicle is registered to a natural person, information on the vehicle's movement may also be considered as an identifier which relates to the registered owner.

Given the foregoing, details on a vehicles ingress and egress are considered as personal information under our law. SCC, as the personal information controller (PIC), has the responsibility to process, which includes disclosure, said personal information in accordance with the provisions of the DPA and its implementing rules and regulations,

³ Data Privacy Act of 2012, § 3 (g).

including the implementation of reasonable and appropriate security measures for the protection of personal information, adherence to the general data privacy principles, and upholding data subjects' rights.

We wish to clarify that while this particular request may be treated as an exercise of a data subject's right to access, where the registered owner of the car is the one requesting for information, the same is not the only manner by which disclosures of personal information can be made.

In the case at hand, SCC may also consider Section 12(f) of the DPA on legitimate interest which allows processing (i.e. disclosure) that is necessary for the purposes of the legitimate interests pursued by the PIC 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 order to use legitimate interest as basis for lawful processing, PICs must consider the following: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 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 should not be overridden by the legitimate interests of the PICs, considering the likely impact of the processing on the data subjects.⁵

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

⁴ 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-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/> [last accessed on Feb. 12, 2020].

ADVISORY OPINION NO. 2020-004¹

3 February 2020



Re: **REQUEST FOR GUIDANCE ON THE DISCLOSURE OF
LIST OF THE DECEASED BARANGAY OFFICIALS (DBOs)
FROM 2002 TO 2011**

Dear ,

We write in response to your letter received by the National Privacy Commission (NPC) regarding academic research in relation to the Data Privacy Act of 2012² (DPA).

This is in relation to the 18 June 2019 letter of a certain researcher requesting for purposes of his dissertation the list of Deceased Barangay Officials (DBOs) from 2002 to 2011 who were able to claim death benefits as provided under Executive Order No. 155, Series of 2002.³ We understand from your letter that the Department of Interior and Local Government (DILG) has been administering the payment of the death and burial claims to the beneficiaries of the deceased barangay officials who died during their incumbency pursuant to DILG M.C. 2008- 124,⁴ the implementing guidelines of E.O. 115.

We further understand from the annexes attached to your letter that the researcher is requesting such information based on the list posted in the DILG website entitled “Consolidated List of Death Benefit Claims and Amount Paid to All Barangay Officials,” which disclosed the

¹Tags: scope, research, special cases, public officials, barangay officials, death benefit

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 Authorizing Payment of Death Benefits to Barangay Officials Who Die During Their Term of Office, Executive Order No. 115, [E.O. 115] (2002).

⁴ Revised Rules and Regulations Implementing Executive Order No. 115 Entitled “Authorizing Payment of Death Benefits to Barangay Officials Who Die During Their Term of Office, Department of Interior and Local Government Memorandum Circular No. 2008-124 [DILG MC 2008-124] (2008).

following information about the barangay officials: name, position, region, province, city/municipality, barangay, date of death and amount of benefit.

In denying the request for information, it is the position of your good office that the data being requested contains personal information and is covered by the DPA. You now inquire whether the release of the information requested to the researcher is allowed under the DPA.

Scope of the Data Privacy Act of 2012; special cases; public officials

The DPA is applicable to the processing of all types of personal information and to any natural and juridical person involved in such processing. 5 The list of DBOs contain personal information as it includes, among others, the names of the deceased barangay officials, their addresses, date of death, and amount of death and burial claims to beneficiaries. Thus, the disclosure of the list should be in accordance with DPA, existing laws, rules and regulations.

However, the Section 4 of the DPA further provides for the specific information which are outside of its scope and which the Implementing Rules and Regulations⁶ (IRR) classifies as special cases. Two special cases are pertinent to the subject of the researcher's request, to wit:

1. Information about any individual who is or was an officer or employee of the government that relates to his or her position or functions, including:
 - a. The fact that the individual is or was an officer or employee of the government;
 - b. The title, office address, and office telephone number of the individual;
 - c. The classification, salary range, and responsibilities of the position held by the individual; and
 - d. The name of the individual on a document he or she prepared in the course of his or her employment with the government.⁷

⁵Data Privacy Act of 2012, § 4.

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

⁷Data Privacy Act of 2012, § 4 (a).

2. Information relating to any discretionary benefit of a financial nature such as granting of a license or permit given by the government to an individual including the name of the individual and the exact nature of the benefit.⁸

Given the above, the information requested by the researcher falls under the above quoted provisions. As such, the list of DBOs and other details requested may be disclosed to the researcher as this information are considered special cases and are outside of the scope of the DPA.

We reiterate however that the exemption is not absolute, and not an exemption on the entity or agency but on the type of information processed under such special cases. Further, it is not a blanket exemption but is limited only to the minimum extent of processing necessary to the purpose of the function or the activity concerned.⁹

The provisions on special cases are interpreted to the effect that personal data may be lawfully processed (i.e., disclosed) by a personal information controller (PIC) under the special cases, but the processing shall be limited to achieving the specific purpose, function or activity, in this case, research purposes, and that the PIC remains to be subject to the requirements of implementing measures to secure and protect personal data.

Data privacy; freedom of information; research

The DPA has the twin task of protecting the fundamental human right to privacy and ensuring the free flow of information to promote innovation and growth.¹⁰ Free flow of information necessarily protects the people's right to information as well as research for public purposes.

We take this opportunity to emphasize that while the right to access public information, official acts, records and documents may be limited by the DPA in protection of the personal information of individuals, the law should not be used as justification to deny requests concerning matters of public concern. More so that the law already specifies information that fall outside the scope of the DPA.

⁸ Id. § 4 (c).

⁹ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (2016).

Further, it is the intent of our data privacy law to grant processing of personal information for research purposes with much flexibility but still within the bounds of the DPA and other existing laws. It recognizes that research is critical to nation-building and serves the interest of the public.

It is for this reason that the DPA will not operate to hinder the DILG to disclose certain information which are within its power to disclose, taking into consideration the applicable provisions of law, rules and regulations, and the data privacy principles enunciated in the DPA.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) **RAYMUND ENRIQUEZ LIBORO**
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2020-005¹

4 February 2020

[REDACTED]

Re: VERIFICATION OF PRE-EMPLOYMENT DOCUMENTS

Dear [REDACTED],

We write in response to your inquiry received by the National Privacy Commission (NPC) seeking to clarify the lawfulness of document verification in relation to the requirements under Data Privacy Act of 2012² (DPA).

We understand that your company, Dataflow Verification Services Limited (Dataflow), confirms the authenticity of the documents submitted by applicants of government agencies, regulators and organizations as part of their pre-employment or pre-licensing requirements, such as, education and employment certificates, passports, practice licenses. Under your normal operations, you ask the applicants to sign a Letter of Consent/Authorization which you present to the different agencies and entities who issue the documents to be verified.

You now seek clarification on the following issues:

1. In cases where some applicants do not submit a Letter of Consent or Authorization, can Dataflow still proceed with the processing under Sections 12 (b) and 12 (f) of the DPA?
2. In cases where the applicants signify their intent to be licensed by government regulators, Dataflow is instructed by the regulator, through a letter of advice, to initiate their Primary Source Verification. Can Data flow proceed with the verification requests under Section 12 (b) and 12 (e) of the DPA?
3. There are some universities and employers who require a specific format for Consent Letters. The format which Dataflow uses states the scope and legitimate purpose for data processing. How can Dataflow best address the situation?
4. As to evidence of consent defined under Section 3 (b) of the law, are digital signatures acceptable? Can the act of applicants in sending their documents for processing be evidence of consent to the processing of their personal information?

¹ Tags: criteria for lawful processing, consent, contract, 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).

Verification documents; personal information; sensitive personal information; lawful criteria for processing

The data privacy principle of legitimate purpose requires 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.³ The DPA explicitly provides the lawful criteria for processing of personal and sensitive personal information under Sections 12 and 13, respectively.

In general, 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 DPA are met.⁴ While verification or authentication of personal information submitted by an applicant as part of the pre-employment requirements may fall under Section 12 (b) of the DPA or Section 12 (f), said legal bases only apply to personal information and not sensitive personal information.

It is worth emphasizing that the law delineates the differences in the treatment of the different types of personal data. Processing of sensitive personal information is generally prohibited unless any of the conditions provided by Section 13 are met.

Dataflow verifies or authenticates documents on education and employment certificates, passports, practice licenses, among others. By their nature, these documents contain information that may be classified as sensitive personal information under Section 3 (l) of the DPA, such as information about an individual's education or their government-issued identification numbers.

Because of the limitation provided under Section 13, Dataflow would have to evaluate if the data processing involved in the verification would fall under any of the lawful criteria for processing under Section 13. Particularly in this scenario, the consent of the data subject and/or processing which is required by existing laws and regulations may be applicable.

Verification of documents for government

²

We understand that Dataflow has clients that are government agencies. When applicants signify their intent to be licensed by these agencies, the latter instructs Dataflow to initiate Primary Source Verification through a letter of advice, a sample of which was attached to your letter.

³ Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (b) (2016).

⁴ Data Privacy Act of 2012, § 12

You inquire on whether you may proceed with the verification on the basis of Section 12 (b) on contract, or Section 12 (e), that “the processing is necessary... to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.”

Given that the documents to be verified contains sensitive personal information, Section 12 is not the proper basis for processing. As discussed above, Dataflow would have to assess the various criteria under Section 13 to determine the most appropriate basis for processing.

If consent of the data subject is the basis for processing, the same is defined under Section 3

(b) the DPA 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.”

It is apparent in the provision that it is the data subject himself or herself who gives consent, or by an agent specifically authorized by the data subject to do so.

From the attached sample letter of advice or letter of authorization, we note that there is a statement by the government agency authorizing Dataflow to verify the authenticity of documents belonging to the applicant and the details of the applicant: name, ID and description of document. While the letter of authorization clearly states the authority of Dataflow to act on behalf of the regulator for verification purposes, this does not amount to the consent of the data subject as required under the DPA.

No official format requirement for authorizations or letters of consent; evidence of consent

Consent of the data subject refers to 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.⁵ Consent shall be evidenced by written, electronic or recorded means.⁶

The DPA, its IRR and the issuances of the NPC do not require a particular format for the consent of the data subject. What matters is that the basic requirements of the law are clearly shown in the consent letter or letter

⁵ Data Privacy Act of 2012, § 3 (b).

⁶ Id.

of authorization, such that the data subject specifically agrees to the processing of his or her personal information for the purposes specified by the PIC.

Regarding evidence of consent, the law only requires that consent is evidenced by written, electronic or recorded means. Digital signatures are thus acceptable.

Lastly, since consent of the data subject needs to be explicit, implied consent is not recognized as valid under the law. Thus, the mere act of applicants in sending their documents for processing may not amount to the consent required by law.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2020-006¹

7 February 2020

[REDACTED]

**Re: COLLECTION AGENCY COMMUNICATING WITH
HUMAN RESOURCE DEPARTMENT**

Dear [REDACTED],

We write in response to your letter received by the National Privacy Commission (NPC). Upon further evaluation, the Complaints and Investigation Division of the NPC endorsed your letter to the Policy Review Division for an advisory opinion in accordance with the Rules of Procedure of the NPC. You inquired on whether the Human Resource (HR) department of your employer is allowed to communicate with the collection agency regarding your unpaid personal loan without your consent.

We understand that you are an employee of an insurance company. You further disclosed that a collection agency allegedly representing a certain bank sent an email to your employer's customer service email address regarding your unsettled loan.

After having been forwarded to two other departments, the email was eventually forwarded to the HR department, which then informed you about the same. They further informed you that two cases will be filed against you in court if you fail to communicate with collection agency. The HR department also told you to resolve the issue immediately so as not to jeopardize your employment and further requested for a copy of the settlement made with the collection agency.

You now inquire on how the HR department came to know about the two court cases that will be filed against you, since such details were not included in the email that was sent, and if the corresponding actions of the HR department are in violation of your rights under the Data Privacy Act of 2012² (DPA).

¹ Tags: Collection agency, personal loan, employment, right to privacy.

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 other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

Lawful criteria for processing; legitimate interests of the personal information controller

Under the DPA, the employment details of an individual are considered personal information.³ Information about an individual's employment, when put together with other information, would directly and certainly identify an individual.⁴ Subject to prohibition by existing law, the processing of such information shall be allowed only if at least one of the criteria provided by Section 12 of the DPA are met.

In particular, Section 12 (f) of the DPA provides that the processing of personal information is allowed when 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."

For this criterion, the personal information controller (PIC) must be able to establish that it has a legitimate interest or purpose in the processing of personal information. Legitimate interests, as discussed in our NPC Advisory Opinion No. 2018-061, are matters that are desired by or important to a PIC, which may include business, financial or other reasonable purpose.⁵ Such legitimate interest, reasonable purpose and intended outcome must be clearly identified by the PIC or a third party or parties to whom the personal data is disclosed.⁶

Furthermore, the PIC must consider the following in using legitimate interest as its basis for lawful processing:

1. Purpose test – the processing of personal information must be compatible the PIC's objectives for its business, which must be clearly determined;
2. Necessity test – the processing of personal information must be necessary for the purpose of pursuing the legitimate interests of the PIC and such purpose could not be reasonably achieved by other means; and
3. Balancing test – the data subject's interests, rights or freedoms should not be overridden by the legitimate interests pursued by the PIC.⁷

³ Data Privacy Act of 2012, § 3 (g).

⁴ Ibid.

⁵ National Privacy Commission, NPC Advisory Opinion No. 2018-061 citing 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/> (Anything illegitimate, unethical or unlawful is not a legitimate interest).

⁶ Ibid.

⁷ 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/> (last accessed Aug. 8, 2019).

Although employers are not obliged to respond to requests for confirmation of employment status, they may do so, provided it is done truthfully, in good faith and pursuant to a legitimate interest of the company or the third party to whom the data is disclosed. Hence, the HR department may confirm the employment status of its employee as long as it can establish that it was done pursuant to a legitimate interest of the company or the third party. The disclosure must be reasonable, limited only to the fact of verification of the employment status and must not include the disclosure of other personal data.

It is also worth noting that the HR department may implement policies with regard to employment confirmation requests to address similar incidents in the future. For instance, such policies may provide for the type of information to be disclosed, among others.

As to your question on whether the company may communicate with the collection agency, if the communication is for the sole purpose of confirming the employment status of an employee, the same may fall under the legitimate interest of the company and/or the collection agency, as discussed above.

We note that the collection agency, allegedly collecting on behalf of a bank, is considered a personal information processor (PIP). Hence, the collection agency must also adhere to the requirements of the DPA in the processing of personal data and must ensure the protection of personal data at all times.

Hence, if the purpose of the collection agency's communication to the employer's HR department is to discuss the alleged unsettled loan obligation and the filing of cases in court for an alleged offense/s by one of its employees then such communication/disclosure should have a basis under Section 13 of the DPA dealing with processing of sensitive personal information, the definition of which includes information about any proceeding for any offense committed or alleged to have been committed by such person. If otherwise, there may be a violation of the DPA.

Employer-employee relationship; labor matter

Lastly, you sought clarification on whether the HR Department can threaten an employee due to an unsettled obligation. As this may be a labor matter, the NPC is not the appropriate agency to address this concern.

This opinion is based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2020-007¹

3 February 2020

[REDACTED]

**Re: REQUEST FOR COPIES OF STATEMENT OF ASSETS,
LIABILITIES AND NET WORTH (SALN) FROM THE
BUREAU OF THE TREASURY**

Dear [REDACTED],

We write in response to your letter requesting for an advisory opinion received by the National Privacy Commission (NPC). We understand that the Bureau of the Treasury (BTr) is the agency authorized by law to bond accountable public officials and to issue appropriate guidelines thereof, pursuant to the Public Bonding Law.² Among the supporting documents required by the BTr in furtherance of its fidelity bonding operations, particularly in the assessment of risk of the accountable public officials, is the Statement of Assets, Liabilities and Net Worth (SALN).

As stated in your letter, a resident of Cuyapo, Nueva Ecija requested for copies of the SALN of certain municipal and barangay officials of Cuyapo, Nueva Ecija from your office, with the intent of using the SALN as evidence for the filing of falsification and malversation charges against the said officials. However, the BTr upholds its position that, although the SALN is a public document, the BTr cannot lawfully disclose copies of the SALN to a requesting third party since the BTr is not the official custodian of the said public document.

You now seek clarification on whether the BTr can furnish copies of the SALN to a third party without violating the provisions of the Data Privacy Act of 2012³ (DPA), its Implementing Rules and Regulations (IRR) and other relevant issuances of the NPC.

¹ Tags: SALN; Bureau of Treasury; elective officials; malversation; public documents; right to information; official custodian of documents.

² Office of the President, Realigning the Organization of the Bureau of Treasury, Executive Order No. 449 [E.O. No. 449], § 1 (9) (October 17, 1997).

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 other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

*Nature of the SALN; scope of the DPA;
public access to SALNs; official repository of SALNs*

Section 8 of Republic Act (RA) No. 6713, otherwise known as the Code of Conduct and Ethical Standards for Public Officials and Employees, provides that public officials and employees have the duty to accomplish and submit their respective SALNs.⁴ The SALN is a document, declared under oath, by public officials and employees which states their respective assets and liabilities, including their business and financial interests, that of their spouses, and of their unmarried children under eighteen (18) years of age living in their households.⁵ RA No. 6713 further mandates that the public has a right to know the foregoing information.

There is a common misconception the public documents fall outside the scope of the DPA. On the contrary, the processing of public documents containing personal data is still governed by the DPA as read together with other applicable laws on the matter.

Section 8 (A) of R.A. 6713 provides for the guidelines on the filing of the SALN, which provides that the SALNs of regional and local officials and employees shall be filed with the Deputy Ombudsman in their respective regions. Furthermore, the Civil Service Commission (CSC) designated the Deputy Ombudsman of the respective regions of Luzon, Visayas or Mindanao as the repository agency of, among others, city and municipal elective officials and employees including mayors, vice-mayors, Sangguniang Bayan/Panlungsod members and barangay officials.⁶

On the other hand, the process of requesting for a copy of a SALN is also subject to specific guidelines.⁷ Section 3 (c.5) of Memorandum Circular No. 03, series of 2012 issued by the Office of the Ombudsman, provides that requests for a copy of a SALN should be filed with the appropriate public assistance bureau of the central office which is the official repository of the requested SALN. In the case of municipal and barangay officials, such request must be made to the concerned Deputy Ombudsmen for Luzon, Visayas or Mindanao.⁸

Given the foregoing, requests for copies of the SALNs of certain municipal and barangay officials coursed through the BTr is not the appropriate process. Although the BTr has copies of the SALNs in question, it is not the repository agency designated by the law to provide copies to requesting

4 An Act Establishing a Code of Conduct and Ethical Standards for Public Officials and Employees, To Uphold the Time-Honored Principle of Public Office Being a Public Trust, Granting Incentives and Rewards for Exemplary Service, Enumerating Prohibited Acts and Transactions and Providing Penalties for Violations Thereof and for Other Purposes [Code of Conduct and Ethical Standards for Public Officials and Employees], Republic Act No. 6713, § 8 (1989).

5 The Official Gazette, The basics: Statement of Assets, Liabilities, and Net Worth, available at <https://www.officialgazette.gov.ph/saln/> (last accessed September 5, 2019).

6 Civil Service Commission, Statement of Assets, Liabilities and Net Worth (SALN) Re: Amendment to the CSC Resolution No. 1300173 (January 24, 2013); Revised SALN Form, Resolution No. 150008 [CSC Resolution No. 1500088] (January 23, 2015).

7 Office of the Ombudsman, Guidelines on Public Access to Statements of Assets, Liabilities and Net Worth (SALNs) Filed with the Office of the Ombudsman, [Memorandum Circular No. 03], § (September 11, 2012).

8 Id.

parties. Furthermore, the BTr's possession of the requested SALNs is only incidental to its duty to implement the Public Bonding Law.

information such as RA No. 6713 on the obligations of public officials and employees to file their respective SALNs and the right of the public to obtain the information contained therein. However, given that the law itself explicitly provides the process for requesting SALNs of certain public officials and the repository agency responsible for the same, then such procedure must prevail and be complied with.

The DPA has the twin task of protecting the fundamental human right to privacy and ensuring the free flow of information.⁹ We emphasize that the DPA should not be a hindrance to the people's right to know. The DPA respects existing laws that mandate the disclosure of certain

This opinion is based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2020-008¹

4 February 2020

[REDACTED]

ADVISORY OPINION
2020-008

Re: VIDEO DOCUMENTATION OF MANDATORY TRAININGS FOR SAFETY OFFICERS

Dear [REDACTED],

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) which sought clarify whether the requirement set by the Occupational Safety and Health Center (OSHC) mandating Occupational Safety and Health Training Organizations (OSHTOs) to submit video documentation of mandatory trainings for safety officers violates the Data Privacy Act of 2012² (DPA).

OSHC as public authority

The OSHC was created by virtue of Executive Order No. 307.³ Its primary mission is to develop effective, responsive, and sustainable Occupational Safety and Health (OSH) programs, policies and services; promote excellent management of resources and foster mutually beneficial linkages that will create a healthy and safe work environment for workers in all industries.⁴ Under Section 2 of the EO, the OSHC have the following powers and functions, among others:

- a. To undertake continuing studies and researches on occupational safety and health, including those relating to the establishment of causal connection between diseases and occupations and the development of medical criteria in determining the nature and extent of impairment or diminution in health, functional capacity or life expectancy of the employees as a result of their work and working conditions;

¹ Tags: lawful processing; personal information; public authority; general 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).

³ Establishing the Occupational Safety and Health Center in the Employees' Compensation Commission, attached agency of the Department of Labor and Employment [Executive Order No. 307] (1987).

⁴ Occupational Safety and Health Center, About OSHC available at <http://www.oshc.dole.gov.ph/transparency-seal/history> (last accessed December 4, 2019).

- b. To plan, develop and implement training programs in the field of occupational safety and health, and related interests;
- c. To serve as a clearing house of information and innovative methods, techniques and approaches in dealing with occupational safety and health problems and institute a mechanism of information dissemination to the general public;
- d. To monitor the working environment by the use of industrial hygiene, field and laboratory equipment and conduct medical examinations of workers exposed to hazardous substances for the ready detection of occupational diseases;
- e. To act as the duly recognized agency to undertake practical testing for safe use and set standard specifications of personal protective and other safety devices;
- f. To assist government agencies and institutions in the formulation of policies and standards on occupational safety and health and other matters related thereto and issue technical guidelines for the prevention of occupational diseases and accidents;
- g. To adopt annually a budget of expenditures of the Center and its staff chargeable against the State Insurance Fund: Provided, That the SSS and GSIS shall advance on a quarterly basis the remittances of allotment of the loading fund for this Center's operational expenses based on its annual budget as duly approved by the Department of Budget and Management; Provided, further, That such budget shall not exceed 4% of the 12% loading fund based on the total of the State Insurance Fund and its earnings as of December 31st of the preceding years;
- h. To perform such other acts as it may deem appropriate for the attainment of the purposes of the Center and proper enforcement of the provisions of this Executive Order; and
- i. To enlist the assistance of government agencies and private organizations in carrying out the objectives of the Center.

Additionally, the OSHC is also mandated under the Department of Labor and Employment (DOLE) Administrative Order No. 56 series of 2011 to conduct spot check/audit/inspection of accredited organization's office including the actual conduct of training and to take measures that will ensure the maintenance of standards on the conduct of training by

OSHTO. From the foregoing, the OSHC is a public authority exercising regulatory functions within the purview of the DPA.

Scope of the DPA; video as personal information; criteria of lawful processing; general data privacy principles

The DPA applies to the processing of all types of personal information and to any natural and juridical person in the government or private sector involved in personal information processing.⁵ 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.⁶ Accordingly, the image of an identifiable individual captured in a photograph or video is personal information about the individual, and thus, covered by the DPA.⁷

In your letter, you mentioned that OSHC received several complaints regarding the quality of trainings being conducted by the OSHTOs. To address the said complaints, the OSHC issued a Memorandum requiring OSHTOs to submit video documentation of the five (5)-day training. While some OSHTOs complied with the said Memorandum, many OSHTOs did not, and claim that the said Memorandum violates the DPA. Some OSHTOs also mentioned that training participants refused to be video-recorded invoking their privacy rights.

The DPA allows the processing of personal data subject to compliance with the law and adherence to the principles of transparency, legitimate purpose, and proportionality. Consequently, the processing activities being required by the OSHC may find support under Section 12 (e) of the DPA where processing is necessary in order to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.

From the foregoing, the OSHC may review its existing accreditation requirements and may include video documentation as an additional requirement for accreditation and/or renewal of the OSHTOs, upon its determination that this is necessary to carry out its mandate in ensuring that the safety officers are provided with core knowledge and skills in the prevention of work-related injuries and illnesses.²

Nonetheless, in view of the proportionality principle and taking into

⁵ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 4 (2016).

⁶ Data Privacy Act of 2012, § 20 (c).

⁷ See: National Privacy Commission, Advisory Opinion No. 2018-053 (26 November 2018).

account that the main purpose of the video documentation is merely to ensure whether the trainings being conducted remain within the prescribed standards, the OSHC should consider the location of the camera and/or camera angle to capture relevant images or videos only, i.e. videos may be filmed from the back of the room whereby the training participants' faces are not captured.

Moreover, the OSHC should require all OSHTOs to have a standard privacy notice on the application form and the training facilities for purposes of informing the training participants of the nature and purpose of the video documentation.

This opinion is based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2020-009¹

4 February 2020

[REDACTED]

Re: DELETION OF ELECTRONIC MEDICAL RECORDS

Dear [REDACTED]

We write in response to your inquiry regarding the electronic medical records from pre-employment medical examination of job applicants and the concern on its removal or deletion from the database of Healthway Medical Inc. (Healthway) upon the request of its corporate clients who paid for such service.

We understand that Healthway is a network of mall-based clinics that offers medical examination and healthcare consultations. Healthway provides pre-employment medical examination services to the corporate clients' potential employees.

It is stipulated in Healthway's contract with such corporate clients that in case of termination of service, all records obtained or generated through the contract shall be returned to the corporate client. Such corporate clients likewise have the right to have the records removed and deleted from Healthway's records or database.

You now request for clarification on the following matters:

1. Is it allowable under the Data Privacy Act of 2012 (DPA) to have the medical records removed/deleted without the consent of the job applicants?
2. Does the legitimate purpose principle have a period of effectivity, meaning that the purpose of the pre-employment examination has been served, therefore the corporate client has the discretion/right to have the personal data removed/deleted?
3. Is Section 19(d)(1) of the Implementing Rules and Regulations (IRR) of the DPA applicable in this case?

¹ Tags: personal information controller, personal information processor, health information, electronic medical record

Scope of the DPA; personal information controller and processor; role of a PIC

The Data Privacy Act of 2012² (DPA) applies to the processing of all types of personal information and to any natural and juridical person involved in the processing of personal information.³

A personal information controller (PIC) refers to a person or organization who controls the collection, holding, processing or use of personal information,⁴ while a personal information processor (PIP) refers to any natural or juridical person to whom a PIC may outsource the processing of personal data pertaining to a data subject.⁵ 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.⁶

In this scenario, the processing of personal data for the pre-employment medical examination of job applicants has been outsourced to Healthway by the corporate clients. The clinic thus acts under the instructions of its corporate clients as to the purpose of processing personal data, as well as the data subjects qualified to undergo the pre-employment medical examination.

However, in its truest sense, Healthway cannot be considered a mere PIP solely because the medical examination was outsourced and paid for by the corporate client. Nor will it make the corporate client the owner of the medical record for the fact remains that the medical record is still personal information pertaining to the job applicant.

Rather, between the job applicant and Healthway, the latter is a PIC since it determines what information from the job applicant is collected and determines the processing and extent of use of the job applicant's personal information to effectively conduct the medical examination, depending on the specific medical purposes only the clinic may identify.

Rights of a data subject; retention of personal information for the fulfillment of the declared, specified, and legitimate purpose and in cases provided for by law

Each being a separate PIC in its own right, Healthway and the corporate

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 Data Privacy Act of 2012, § 4.

⁴ Id., § 3 (h).

⁵ Id., § 3 (i).

⁶ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 3 (m) (2016).

client are both mandated by law to uphold the rights of data subjects as provided for in Section 16 of the DPA. This includes among others, the right to access and the right to withdraw or order the blocking, removal or destruction of a data subject's personal information if the same is no longer covered by any other grounds for lawful processing. Non-compliance will each make Healthway and the corporate client liable to the data subject.

Considering that Healthway and the corporate client may have different and separate purposes for the collection, use and retention of a data subject's information, each PIC then must assess the period within which it is necessary for them to maintain health records, hinging its assessment on the legitimate purpose for which the data subject's information was processed and not merely based on who commissioned or paid for the service.

In the case of the corporate clients, the determination of the retention period of health records and the decision to delete the same may stem from Section 19 of the IRR of the DPA which provides as follows:

“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 xxx xxx

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 approved by appropriate government agency.
2. Retention of personal data shall be allowed in cases provided by law.
3. Personal data shall be disposed 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.”

On the other hand, aside from the circumstance provided for in Section 19 (d) of the IRR of the DPA, Healthway, a healthcare facility, may also anchor their retention period to the applicable provisions of the Departments of Health’s Department Circular No. 70 series of 1996,⁷ providing for the retention period of various health records.

Thus, while it is ideal to get the consent of the data subject prior to deletion of their information, such consent is not a requisite if the PIC determines that retention falls within any of the circumstances under Section 19 (d) of the IRR. What the law mandates is for each PIC to inform its data subjects through appropriate means the time frame for the retention and deletion of the health records in order to ensure that the latter’s right to access and erasure are upheld.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For you reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

⁷ Department of Health, The Revised Disposition Schedule of Medical Records Amending Ministry Circular 77 s. 1981, [Department Circular No. 70 s. 1996] (1996).

ADVISORY OPINION NO. 2020-010¹

10 February 2020

[REDACTED]

**Re: PHILIPPINE HEALTH INSURANCE CORPORATION
INSPECTION AND MONITORING ACTIVITIES**

Dear [REDACTED],

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify several matters in relation to the inspection and monitoring activities conducted by the Philippine Health Insurance Corporation (Philhealth).

We understand that a representative of the Philhealth Regional Office VII visited your hospital to inspect and monitor the hospital's compliance with Philhealth circulars on fraud prevention. Part of the process includes access to hospital logbooks containing patient information of both Philhealth and non-Philhealth members, Integrated Hospital Operations Management Information System (iHOMIS) and patients' charts containing personal and sensitive personal information (collectively, personal data).

We further understand that per the hospital's organizational security measure, the Philhealth employee was requested to sign a non-disclosure agreement (NDA) but was advised by Philhealth's legal counsel not to sign the same.

¹ Tags: Philhealth inspection and monitoring, public authority, regulatory mandate, special cases, general data privacy principles, non-disclosure agreement, data sharing agreement.

From the foregoing, you seek clarification on the following:

- 1) Are the inspection and monitoring activities of the Philhealth an exemption from the applicability of Section 5 (d) and the last paragraph thereof of the Implementing Rules and Regulations² (IRR) of the Data Privacy Act of 2012³ (DPA);
- 2) Is Philhealth exempt from signing an NDA if their staff performs monitoring and inspection; and
- 3) Is Philhealth exempt from entering into a data sharing agreement (DSA) with the hospital.

Processing of sensitive personal information; regulatory function of the public authority; statutory mandate

The DPA and its IRR provide for a list of specific information or special cases wherein the law and the rules are not applicable. Section 5(d) and the last paragraph of said section provides:

“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 authority, subject to restrictions 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; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA).

XXX XXX XXX

Provided, that the non-applicability of 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

² Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).

³ An Act Protecting the 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 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.⁴

In order to apply, the following must be established:

1. Information is necessary in order to carry out the law enforcement or regulatory function of a public authority;
2. Processing is for the fulfillment of a constitutional or statutory mandate;³
3. Applies only to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose; and
4. Strict adherence to all substantive and procedural processes.⁵

Republic Act (RA) No. 10606, otherwise known as the National Health Insurance Act of 2013, provides that Philhealth has the power to visit, enter and inspect facilities of health care providers and where applicable, secure copies of their medical, financial and other records and data pertinent to the claims, accreditation, premium contributions of the health care provider's patients and employees.⁶ This is read together with the Philhealth's power to supervise the provision of health benefits and to set standards, rules, and regulations necessary to ensure quality of care, appropriate utilization of services, fund viability, among others.⁷

Given the above, the inspection and monitoring of the hospital's logbooks and patient records may be necessary in the exercise of Philhealth's regulatory mandate. The information necessary for such mandate is outside of the scope of the DPA but only to the minimum extent necessary to achieve Philhealth's purpose, i.e. fraud prevention.

General data privacy principles; security measures; non-disclosure agreement; data sharing agreement

⁴ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (d) and last ¶ (2016).

⁵ See generally: National Privacy Commission, NPC Advisory Opinion No. 2018-079 (Oct. 23, 2018).

⁶ An Act Amending Republic Act No. 7875, Otherwise Known as the "National Health Insurance Act of 1995", As Amended, And for Other Purposes [National Health Insurance Act of 2013], Republic Act No. 10606, § 10 (2013).

⁷ Id.

Although Philhealth is allowed to process personal data pursuant to its mandate, as a personal information controller, it is still subject to the requirements of implementing security measures to protect personal data, adhering to the general data privacy principles of transparency, legitimate purpose and proportionality, and upholding data subjects' rights.

While we are not privy to the provisions of the NDA of the hospital, we understand that this is part of its organizational security measures. With this, Philhealth and its authorized representatives are not prohibited from signing an NDA which ensures the confidentiality of the patients' personal data as between the hospital and Philhealth.

As to whether or not Philhealth is exempt from entering into a data sharing agreement, NPC Circular No. 2016-02 provides that nothing in the Circular shall be construed as prohibiting or limiting the sharing or transfer of any personal data that is already authorized or required by law.⁸

For this purpose, we understand that there is already a Philhealth issuance on the matter – Philhealth Circular No. 013 – 2015 (Revisions in the Performance Commitment for Health Care Institutions and Professionals).⁹ You quoted the 2018 version of the Performance Commitment form, specifically Item E (35), to wit:

“E. REGULAR SURVEYS/ADMINISTRATIVE INVESTIGATIONS/ DOMICILIARY VISITATIONS ON THE CONDUCT OF OPERATIONS IN THE EXERCISE OF THE PRIVILEGE OF ACCREDITATION

35. That we shall extend full cooperation with duly recognized authorities of PhilHealth and any other authorized personnel and instrumentalities to provide access to patient records and submit to any orderly assessment conducted by PhilHealth relative to any findings, adverse reports, pattern of utilization and/or any other acts indicative of any illegal, irregular and/or unethical practices in our operations as an accredited

⁸ National Privacy Commission, Data Sharing Agreements Involving Government Agencies, Circular No. 16-02 [NPC Circular 16-02], § 1 (October 10, 2016).

⁹ Philippine Health Insurance Corporation, Revisions in the Performance Commitment for Health Care Institutions and Professionals, Philhealth Circular No. 013 – 2015 [Circular No. 013-2015] (June 15, 2015).

HCI of the NHIP that may be prejudicial or tends to undermine the NHIP and make available all pertinent official records and documents including the provision of copies thereof; provided that our rights to private ownership and privacy are respected at all times.”

Thus, the existing transfers or submissions of personal data from the hospitals to Philhealth is already authorized or required by this circular and commitment form, and thus, Philhealth is not constrained or compelled into signing any NDAs nor DSAs.

Nonetheless, the DPA, its IRR, and issuances of the NPC do not prohibit Philhealth from entering into a separate DSA or a similar agreement with any hospital under its supervision, as may be necessary and appropriate in certain circumstances, i.e. in order to document other terms and conditions of the sharing or transfer arrangement which is not reflected in the current Philhealth issuance.

This opinion is based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts. For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

ADVISORY OPINION NO. 2020-011¹

11 February 2020

[REDACTED]
[REDACTED]
[REDACTED]

Re: ACCESS TO SIBLINGS' BIRTH CERTIFICATES FOR OBTAINING TAX IDENTIFICATION NUMBERS

Dear [REDACTED],

We write in response to your letter requesting for an advisory opinion from the National Privacy Commission (NPC) on whether you can be allowed to secure the birth certificates of your seven siblings from the Philippine Statistics Authority (PSA), pursuant to Section 12 (c) and (f) and Section 13 (f) of the Data Privacy Act of 2012² (DPA).

You require the said birth certificates in order to apply for the tax identification numbers (TINs) of your siblings for the payment of estate taxes and the transfer of the respective allotted portions of the estate of your deceased parents to you and each of your siblings as heirs, pursuant to the compromise agreement approved by the Regional Trial Court Branch 30 of Surigao City in Civil Case No. for Partition dated March 10, 2011.

We understand that the PSA denied your request for the birth certificates citing the provisions of the DPA as the reason for the denial.

*Birth certificate contains sensitive
personal information; lawful basis for processing*

¹

A birth certificate contains the following information of an individual, among others: name, sex, date of birth, place of birth, type of birth,

¹ Tags: birth certificate, PSA, personal information, sensitive personal information, lawful processing, law or regulation

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for

birth order, weight at birth, parents' details (name, citizenship, religion and occupation), among others. Most of the information contained in a birth certificate are considered sensitive personal information under Section 3(l) of the DPA.

²

The processing or disclosure of a birth certificate, which contains sensitive personal information, is generally prohibited except in certain cases enumerated under Section 13 of the law.

One of those exceptions, which was included in your query is under paragraph (f) which applies when 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.

But in this case, there is actually a law regarding the issuance of birth records. It is of significance to discuss Section 13(b) of the DPA in relation to Presidential Decree (PD) No. 603³ and the 2019 issuance of the Philippine Statistics Authority (PSA).

Section 13(b) 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:

xxx xxx xxx

(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”

³ The Child and Youth Welfare Code, Presidential Decree No. 603 (1974).

Article 7 of PD No. 603⁴ provides for the rules on disclosure of birth records, to wit:

“Article 7. Non-disclosure of Birth Records. – The records of a person’s birth shall be kept strictly confidential and no information relating thereto shall be issued except on the request of any of the following:

3

- (1) The person himself, or any person authorized by him;
- (2) His spouse, his parent or parents, his direct descendants, or the guardian or institution legally in-charge of him if he is a minor;
- (3) The court or proper public official whenever absolutely necessary in administrative, judicial or other official proceedings to determine the identity of the child’s parents or other circumstances surrounding his birth; and
- (4) In case of the person’s death, the nearest of kin.”

And lastly, we refer to the PSA’s Memorandum Circular No. 2019-15 dated 11 June 2019 on the Guidelines on the Issuance of the Civil Registry Documents (CRDs)/Certifications including Authentication. Said issuance provides for the basic requirements for the issuance of CRDs, which includes Certificate of Live Birth, to wit:

1. Presentation of a valid Identification (ID) Card of the document owner.
2. If the requesting party is a duly authorized representative, the original copy of the Authorization Letter or Special Power of Attorney (SPA) must be presented together with a valid ID of the document owner. The duly authorized representative should also show his/her valid ID and must provide the PSA with photocopies of all the IDs presented for its file.

With this, you are constrained to follow the above PSA requirements for purposes of obtaining the birth certificates of your siblings.

Transfer of ownership of real property

As the final objective is the transfer of the ownership of the real property to each of the heirs after the payment of all the requisite

⁴ Id.

taxes, the competent authority to resolve the matter is the Bureau of Internal Revenue (BIR).

We recommend that you coordinate with the BIR Revenue District Office having jurisdiction over the subject property and request for proper guidance over your reported concern given that there is a difficulty in acquiring the birth certificates of your siblings.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2020-012¹

19 February 2020

[REDACTED]
[REDACTED]

RE: DISCLOSURE OF INSURANCE POLICY DETAILS TO THE NATIONAL BUREAU OF INVESTIGATION

Dear [REDACTED]

We write in response to your letter which sought clarification on whether the disclosure of insurance policies of several government officials to the National Bureau of Investigation (NBI) by the Philippine Life Insurance Association, Inc. (PLIA) in connection with the investigation for graft and corruption being conducted by the NBI is allowed under the Data Privacy Act of 2012² (DPA).

We understand that the NBI National Capital Region (NBI-NCR), through a letter signed by the NBI-NCR Regional Director, provided a list of names and dates of birth of certain government officials, and requested for the following details from the Insurance Commission (IC):

1. List of insurance policies;
2. Face value;
3. Monthly premiums; and
4. Corresponding beneficiaries.

Since the IC does not maintain a database of insurance policyholders and/or insurance policies issued by insurance companies, it endorsed the request to PLIA for appropriate action. The latter is of the opinion that complying with the NBI request may be a violation of the DPA, while the IC submits that there will be no violation as the processing is necessary to fulfill the functions of the NBI as a public authority under Section 12 (e) of the DPA.

¹ Tags: public authority, mandate, lawful 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).

Public authority; mandate; investigatory functions of the NBI

The NBI has the mandate to undertake investigation and detection of crimes and offenses pursuant to Republic Act (RA) No. 10867 or the National Bureau of Investigation Reorganization and Modernization Act.³ Section 5 of said law provides that the NBI shall have primary jurisdiction to undertake investigations in cases referred by the Inter-Agency Anti-Graft Coordinating Council (IAGCC), among others.

We understand that the IAGCC was created pursuant to Administrative Order No. 79, s. 1999,⁴ upon the recognition that in the fight against graft and corruption in government, the Commission on Audit, Civil Service Commission, Office of the Ombudsman, Department of Justice, NBI, and Presidential Commission Against Graft and Corruption have taken the initiative to formulate and develop concerted techniques and strategies in the prevention, detection, investigation and prosecution of graft cases.⁵

From the foregoing, NBI's request for personal information falls squarely within its mandate to investigate government officials for graft and corruption.

Processing of personal
information by a public
authority under the DPA

The NBI is requesting for the details of the insurance policies of several government officials. These constitute personal information, the processing of which should be in accordance with any of the criteria for lawful processing under Section 12 of the DPA. Section 12 (e) provides as follows:

“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

(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

³ An Act Reorganizing and Modernizing the National Bureau of Investigation (NBI) And Providing Funds Therefor [NBI Reorganization and Modernization Act], Republic Act No. 10867, § 4 (2016).

⁴ Recognizing the Establishment of the Inter-Agency Anti-Graft Coordinating Council and Directing Government Agencies to Extend Support and Assistance to it, Administrative Order No. 79, s. 1999 (1999).

⁵ Id., Fourth Whereas Clause.

fulfillment of its mandate;" (underscoring supplied)

From the foregoing, it is evident that the NBI has a statutory mandate to investigate crimes and other offenses, including violations of the Anti-Graft and Corrupt Practices Act,⁶ and such investigation would necessarily include the processing of personal information. Hence, the disclosure of the requested details to the NBI is allowed under the DPA.

We wish to remind the IC, PLIA, and the NBI that while such disclosure may be allowed under the law, the same should be done in a secure manner and with strict adherence to all existing protocols and standard operating procedures, which includes the issuance of a subpoena, where appropriate in the circumstances and as may be determined by the NBI under Section 4 (b) of the National Bureau of Investigation Reorganization and Modernization Act.

This opinion is rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

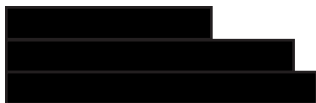
Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

⁶ Anti-Graft and Corrupt Practices Act, Republic Act No. 3019 (1960).

ADVISORY OPINION NO. 2020-013¹

21 February 2020



Re: ACCESS TO INFORMATION IN RELATION TO DISCIPLINAR RECORD AND/OR ADMINISTRATIVE CASES OF STUDENTS AND SCHOOL PERSONNEL

Dear [REDACTED],

We write in response to your inquiry received by the National Privacy Commission (NPC) seeking guidance and clarification in relation to the Ateneo de Manila University's ("University") protocols for the disclosure and sharing of information in relation to disciplinary records and administrative cases of students and school personnel.

We understand that the University receives, processes, and resolves complaints involving its students, faculty members and administrative personnel. We understand further that in the course of such proceedings and up until their conclusion, various parties would attempt to obtain – in some cases, demand – access to some or all information relating to such proceedings.

¹

Thus, the University now seeks clarification on the following questions in relation to the Data Privacy Act of 2012² (DPA):

1. Is the University required to disclose or share information (including personal data) about a particular administrative case to the following:
 - a. parties to the case (i.e. complainant, respondent, and/or witnesses);
 - b. other parties who may be affected by the case and/or its outcome (e.g. other students of a teacher who is the respondent in a case filed by one student, parents or guardian of an adult student, etc.); and

¹ Tags: administrative cases, education sector, 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).

- c. public (e.g. other students/University personnel, other students' parents, etc.)

If the University is not required to make any such disclosure or to share any such information, is it at least allowed by the DPA to do so? If the answer is in the affirmative, on what possible ground/s in the law?

- 2. In relation to Questions #1 and #2, would it matter if a case is still pending or has already been concluded?
- 3. Regardless of the answers to Questions #1 and #2, may the University issue public reports that provide statistical information in relation to specific offenses, such as, but not limited to the following: (a) number of cases filed; (b) number of cases resulting in suspension or termination; (c) number of cases dismissed. In this wise, would the number of cases be relevant insofar as determining whether such information may constitute personal data?
- 4. In relation to sexual harassment cases in particular, what is the implication of Sections 22 and 26 of Republic Act (RA) No. 11313, also known as the Safe Spaces Act, on the right to privacy of the accused or respondent, especially under the DPA? Of particular importance are the following provisions:
 - a. Section 22(8). It provides that school heads have the duty to create an independent internal mechanism to investigate and address complaints of gender-based sexual harassment which shall guarantee to the greatest extent possible;
 - b. Section 26 (on Confidentiality). It states that, at any stage of the investigation, prosecution and trial of an offense under the Safe Spaces Act, the rights of the victim and the accused who is a minor shall be recognized.

Disclosure of information related to administrative cases; procedural due process requirements; administrative proceedings as sensitive personal information

As the above items 1, 2 and 3 are related, these will be collectively discussed.

The disclosure or sharing of personal and sensitive personal information (collectively, personal data) is considered as processing under the DPA. Hence, the same should be based on any of the lawful criteria for processing under Sections 12 and 13 of the law, depending on the nature of personal data being disclosed or shared.

In this case, information about any proceeding for any offense committed or alleged to have been committed by an individual, the disposal of such proceedings, or the sentence of any court in such proceedings are classified as sensitive personal information.³

In our Advisory Opinion No. 2019-011,⁴ the term “proceedings” has been interpreted to also include those non-judicial in nature, including administrative proceedings, to wit: “...case files of every data subject, in all types of proceedings, shall be provided a higher degree of protection ‘as the context of their processing could create significant risks to the fundamental rights and freedoms.’” Administrative cases in an educational institution are then included in such proceedings protected by the DPA.

Generally, the processing of sensitive personal information is prohibited, except in certain instances, i.e. when the processing is provided for by existing laws and regulations⁵ or necessary for establishment, exercise or defense of legal claims.⁶

In the given scenario, we refer to the Manual of Regulations for Private Higher Education (MORPHE) issued through Commission on Higher Education (CHED) Memorandum Order No. 40, s. 2008. Section 142 of the MORPHE states that, “In all matters that may result in the imposition of any sanction or penalty to a higher education institution, or to any personnel or student, administrative due process shall in all instances be observed.”⁷

Jurisprudence has provided for the procedural rights of students in disciplinary cases and the minimum standards to be followed in the imposition of disciplinary sanctions in academic institutions, to wit:

1. The students must be informed in writing of the nature and cause of any accusation against them;
2. They shall have the right to answer the charges against them, with the assistance of counsel, if desired;
3. They shall be informed of the evidence against them;
4. They shall have the right to adduce evidence in their own behalf; and
5. The evidence must be duly considered by the investigating committee or official designated by the school authorities to hear and decide the case.⁸

³ Data Privacy Act of 2012, § 3 (l) (2).

⁴ National Privacy Commission, NPC Advisory Opinion No. 2019-011 (14 January 2019).

⁵ Data Privacy Act of 2012, § 13 (b).

⁶ *Id.*, § 13 (f).

⁷ Commission on Higher Education, Manual of Regulations for Private Higher Education (MORPHE), available at <https://ched.gov.ph/manual-regulations-private-higher-education-morphe/> (last accessed 7 January 2020).

⁸ See: *Guzman v. National University*, G.R. No. L-68288 (11 July 1986), cited in *Spouses Go v. Colegio de San Juan de Letran*, G.R. No. 169391 (10 October 2012) and *Ateneo De Manila University v. Capulong*, G.R. No. 99327 (27 May 1993).

Hence, as can be gleaned from the above, the parties involved in the administrative proceeding, specifically the complainant and respondent, have the right to be informed of the details of the case, including personal data, as a matter of procedural due process. This holds true whether the party to the case is a student, faculty or school personnel.

Meanwhile, third parties to the proceeding, including witnesses, other individuals who may be affected by the case and its outcome, and the public, are not accorded the same right.

With respect to item number 3, the above interpretation will apply whether the administrative case is pending or already concluded.

Statistical data not considered personal information

As to whether the University may issue public reports that provide statistical information in relation to specific offenses, the University may do so considering that purely statistical data falls outside the ambit of the DPA as the same does not identify a person.

However, the number of cases to be reported may be relevant in the determination of whether the same may constitute personal data when for instance, other data may be used or may allow a statistical unit to be identified.⁹ To determine whether a statistical unit is identifiable, account shall be taken of all relevant means that might reasonably be used by a third party to identify the statistical unit.¹⁰ With this, caution should be exercised in releasing reports on specific offenses to ensure that no personal data is inadvertently released.

Safe Spaces Act vis-à-vis the DPA

Lastly, the University seeks clarification on the implication of the Safe Spaces Act (SSA)¹¹ on the right to privacy of the accused or the respondent.

We understand that the SSA requires school heads to create an independent internal mechanism to investigate and address complaints of gender-based sexual harassment which shall guarantee confidentiality to the greatest extent possible.¹² Further, the law requires confidentiality at any stage of the investigation, prosecution and trial of an offense under the SSA, where the rights of the victim and the accused who is a minor shall be recognized.¹³

⁹ See: Eurostat, Statistical Confidentiality and Personal Data Protection, available at <https://ec.europa.eu/eurostat/web/microdata/statistical-confidentiality-and-personal-data-protection> (last accessed Feb. 21, 2020).

¹⁰ Ibid.

¹¹ An Act Defining Gender-Based Sexual Harassment in Streets, Public Spaces, Online, Workplaces, and Educational or Training Institutions, Providing Protective Measures and Prescribing Penalties Therefor [Safe Spaces Act], Republic Act No. 11313 (2019).

¹² Id., § 22 (8).

¹³ Id., § 26.

Upon a reading of both laws, the SSA and the DPA do not contradict each other. While Section 22 (8) of the SSA provides that the institution shall guarantee confidentiality to the greatest extent possible and Section 26 of the same law states that the rights of a minor, who may either be the victim or accused, shall be recognized in all stages of the proceedings for an offense under the SSA, these provisions do not contradict the provisions of the DPA which protects the data privacy of all individuals regardless of age.

In effect, the SSA complements the DPA's requirement of having proper safeguards to ensure confidentiality of personal data being processed.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2020-014¹

24 February 2020

[REDACTED]

Re: OBTAINING ADDRESS OF ACCUSED THROUGH LEARNER REFERENCE NUMBER (LRN)

Dear [REDACTED],

We write in response to your inquiry received by the National Privacy Commission (NPC) seeking clarification on the disclosure of the present address of certain individuals who are the accused in an ongoing criminal case through the Learner Reference Numbers (LRNs) of their children.

We understand that your Office received an Indorsement from the Department of Education (DepEd) Office of the Assistant Secretary for Legal Affairs relative to the letter of one of the two complainants in a pending criminal case for estafa. In his letter, the complainant requested for the present address of the accused spouses in the criminal case currently with Branch 58 of the Regional Trial Court (RTC) in Angeles City.

We further understand that the present address is expected to be obtained through the LRN of the children of the accused, the records of which are currently in the possession of the DepEd Planning Division.

The complainant attached the following in his letter request:

¹

1. Certification dated 20 August 2019 issued by the Branch Clerk of Court of Branch 58, RTC of Angeles City stating to the effect that “[case title - redacted]” docketed as , has been filed and raffled to this court on 15 April 2019 and a

¹ Tags: personal information, address of accused, learners LRN, warrant of arrest, confidentiality

warrant of arrest has been issued for the apprehension of the accused on 16 April 2019; and

2. Copy of the Warrant of Arrest for the accused spouses issued by the Judge in Branch 58, RTC of Angeles City, endorsed for immediate service and return to the following:
 - a. The Chief of Police, Batangas City
 - b. National Bureau of Investigation (NBI), Manila
 - c. Director, PNP Criminal Investigation Command, Camp Crame, QC
 - d. NBI Regional Office, San Fernando, Pampanga
 - e. CIDG Office, Angeles City
 - f. CIDG Pampanga
 - g. Bureau of Immigration, Manila

Thus, your Office now seeks clarification on the lawfulness of disclosure of the present address of the accused in relation to the provisions of the Data Privacy Act of 2012² (DPA).

Disclosure prohibited under DepEd Order 22, s. 2012

The DepEd Order No. 22 dated 20 March 2012 (D.O. 22, s. 2012) mandated the issuance of the unique LRN to all public school pupils, students and Alternative Learning System (ALS) learners to facilitate their tracking and performance.³ Schools are responsible in incorporating the LRN in all documents, forms, examinations, surveys and databases which refer to a pupil, student or learner.⁴

Under our data privacy law, the processing of personal information shall be permitted only if not otherwise prohibited by law and subject to conditions provided by the DPA.⁵ On the other hand, item 9 of D.O. 22, s. 2012 explicitly states, “The identity or other information that may reasonably identify the pupil, student or learner shall be kept confidential.”⁶

The present address of the pupil, student or learner may be considered as information made to be kept confidential. Hence,

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 Department of Education, Adoption of the Unique Learners Reference Number, Department Order No. 22, s. 2012 [D.O. 22, s. 2012] (March 20, 2012).

⁴ Ibid.

⁵ Data Privacy Act of 2012, § 12.

⁶ Ibid, Footnote 4.

the DepEd may not disclose the present address of the children of the accused spouses requested through a mere letter by the complainant in the criminal case.

Nonetheless, it is worth noting that although obtaining the present address of the accused through the school files of their children through a mere letter request of the complainant is prohibited under the current DepEd regulation, the complainant and/or the proper law enforcement or investigative agency as listed in the Warrant of Arrest may still make use of all other available and proper administrative or judicial processes and/or remedies to obtain the address, for the purpose of executing said warrant.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2020-015¹

24 February 2020



Re: COLLECTION OF PERSONAL DATA BY THE BUREAU OF INTERNAL REVENUE FOR TAX COMPLIANCE PURPOSES

Dear 

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify whether the Bureau of Internal Revenue (BIR) may process personal and sensitive personal information (collectively, personal data) such as the list of names and Taxpayer Identification Numbers (TINs) pursuant to its mandate, specifically Section 5 of the National Internal Revenue Code (NIRC) of 1997, as amended.

In your letter, you stated that the BIR issued Revenue Memorandum Circular (RMC) No. 31-2013 to resolve and correct the wrong impression that Filipinos employed by resident foreign missions, such as embassies and consulate offices, in the Philippines are exempt from tax on salaries and emoluments received from their foreign mission employers. For years, the local hires of foreign missions did not file and pay their income tax. RMC No. 31-2013 reiterated the obligation of such Filipino employees to file and pay the corresponding income taxes.

You further stated in your letter that the BIR requested for assistance from the Department of Foreign Affairs (DFA) in the course of its investigation and verification of the Filipino employees' compliance

¹ Tags: scope; special cases; public authority; lawful processing; foreign diplomatic missions.

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).

with the RMC. In particular, the BIR asked the DFA to obtain the list of names and the corresponding TINs of the locally hired employees of the foreign missions, citing Sections 4 and 19 of the Data Privacy Act of 2012 (DPA) as legal bases for the request. Despite the foregoing, some of the embassies still refused to cooperate and claimed that the information being requested is sensitive and protected.

Scope of the DPA; special cases; general data privacy principles; security measures

The DPA and its Implementing Rules and Regulations (IRR) provide for a list of specified information that are not covered by the law, which includes information necessary to carry out functions of a public authority, 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, use, disclosure or other processing necessary to the purpose, function, or activity concerned:

xxx xxx xxx

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 authority, subject to restrictions 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; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);

xxx xx xxx

Provided, that the non-applicability of 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.”³ (Underscoring supplied)

Based on the above, information necessary to carry out regulatory functions of a public authority, in accordance with a constitutional or statutory mandate, are outside the scope of the DPA. This exemption, however, is to be strictly construed:

1. Applies only to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned. The processing for a regulatory function must be in accordance with a constitutional or statutory mandate, and strictly adheres to all required substantive and procedural processes; and
2. Only the specified information is outside the scope of the DPA. The public authority remains subject to its obligations as a personal information controller (PIC) under the DPA of implementing security measures to protect personal data, upholding the rights of data subjects, and adhering to data privacy principles.⁴

Public authority; regulatory mandate; limitations on data subjects’ rights

The BIR is a public authority tasked with the duty to, among others, ensure compliance with the NIRC, as amended, and other relevant tax laws and issuances. Under Section 5 of the NIRC, as amended, the BIR Commissioner has the following powers:

“SEC. 5. Power of the Commissioner to Obtain Information, and to Summon, Examine, and Take Testimony of Persons. - In ascertaining the correctness of any return, or in making a return when none has been made, or in determining the liability of any person for any internal revenue tax, or in collecting any such liability, or in evaluating tax compliance, the Commissioner is authorized:

³ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (d) (2016).

⁴ See: National Privacy Commission, NPC Advisory Opinion No. 2019-022 (May 7, 2019).

(A) To examine any book, paper, record, or other data which may be relevant or material to such inquiry;

(B) To obtain on a regular basis from any person other than the person whose internal revenue tax liability is subject to audit or investigation, ... any information such as, but not limited to costs and volume of production, receipts or sales and gross income of taxpayers,...

xxx xxx xxx

(C) To summon the person liable for tax or required to file a return, or any officer or employee of such person, or any person having possession, custody, or care of the books of accounts and other accounting records containing entries relating to the business of the person liable for tax, or any other person, to appear before the Commissioner or his duly authorized representative at a time and place specified in the summons and to produce such books, papers, records, or other data, and to give testimony; xxx xxx xxx.”

From the foregoing, the BIR Commissioner is authorized by law to obtain information in the evaluation of the tax compliance of any person, specifically in this case where the BIR has already identified an issue with respect to compliance of local hires of foreign diplomatic missions in the Philippines with the NIRC and specifically, RMC No. 31-2013.

While the BIR may have a lawful basis for processing, the same should be done in a secure manner and with strict adherence to all existing rules and regulations, which may include the issuance of tax verification notices, letter notices, letter of authority, subpoena duces tecum, etc., where appropriate in the circumstances and as may be determined by the BIR.

We note that there may be some limitations with respect to the rights of the data subjects where the processing of personal data is for the purpose of investigations in relation to any tax liabilities of the data subject.⁵

Nonetheless, in all other cases, the BIR is expected to uphold and have mechanisms in place for the exercise of these rights.

⁵ Data Privacy Act of 2012, § 19.

We reiterate that the DPA is not meant to prevent government agencies from processing personal data when necessary to fulfill their mandates. Rather, the law aims to protect the right to data privacy while ensuring free flow of information. It promotes fair, secure, and lawful processing of such information.⁶

This opinion is based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner and Chairman

⁶ See: National Privacy Commission, NPC Advisory Opinion No. 2018-083 (Oct. 29, 2018).

ADVISORY OPINION NO. 2020-016¹

12 March 2020



Re: AUDIT PROCEDURES OF THE COMMISSION ON AUDIT

Dear 

We write in response to your request for an advisory opinion seeking guidance vis-à-vis the Commission on Audit (COA) Memorandum which states that the Data Privacy Act of 2012² (DPA) does not absolutely prohibit access to information since the law itself has exceptions, and that auditees cannot validly deny the COA access to information/details based on the DPA.

In your letter, you stated that although you acknowledge the functions of the COA, pursuant to its constitutional mandate to examine, audit, and settle all accounts pertaining to the revenue, receipts, and expenditures or uses of funds and property owned or held in trust by, or pertaining to, the government,³ you have reservations regarding the manner to be employed by COA in the acquisition of personal information, specifically if the same will be done through remote access or database cloning which may pose risks and may lead to personal data breach.

Public authority; constitutional or statutory mandate

¹ Tags: COA; processing of public authorities; constitutional or statutory mandate; presumption of regularity; general 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, § 4 (e) (2012).

³ Phil. Const. art. IX § 2 ¶ D.

⁴ Commission on Audit website, Commission on Audit Mission, available at https://www.coa.gov.ph/coa_at_a_glance/index.html#mission (last accessed 11 March 2020).

The COA is a constitutional commission, created precisely to be one of the pillars of the State's system of checks and balances. As a public authority, it has the mission to ensure accountability for public resources, promote transparency, and help improve government operations, in partnership with stakeholders, for the benefit of the Filipino people.⁴

We must be reminded that the processing of 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, is one of the instances where the application of the Data Privacy Act of 2012⁵ (DPA), and of the DPA's Implementing Rules and Regulations⁶ (IRR), is qualified or limited.

This means that when the personal information is needed to be processed by a public authority, such as the COA, pursuant to its constitutional mandate, the processing of such personal data is generally allowed by the aforementioned enactments.

The DPA shall not be used to hamper, or interfere with, the performance of the duties and functions of duly constituted public authorities. Pursuant to the 1987 Constitution, the COA shall have exclusive authority, subject to certain limitations, to define the scope of its audit and examination, establish the techniques and methods required therefor, and promulgate accounting and auditing rules and regulations, including those for the prevention and disallowance of irregular, unnecessary, excessive, extravagant, or unconscionable expenditures or uses of government funds and properties.⁷

With this in mind, the COA in carrying out its mandate, enjoys the presumption of regularity in the performance of its duties. The determination of what methods to utilize in the collection or gathering of personal data in performing its auditing functions shall be left to the COA's sound discretion.

The Supreme Court, in the case of *Yap v. Lagtapon*, held that "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.”⁸

Applying such ruling in this case, absent any proof that the methods adopted by the COA in gathering personal data may be violative of the provisions of the DPA, the presumption of regularity in the carrying out of its official duties stands.

General data privacy principles; proportionality; obligations of personal information controllers

On the other hand, the foregoing does not relieve the COA, as a personal information controller (PIC), of its duties as such under the DPA. The constitutional provision allowing the COA to determine the scope, method and extent of auditing, including the gathering of personal data from its auditees, shall not be construed to have waived the application of the DPA.

As your office correctly pointed out, the COA must still abide by the general data privacy principles provided under the DPA and its IRR, particularly the principle of proportionality. This means that in the processing of personal data, the COA must see to it that the personal data collected and processed shall be adequate, relevant, suitable, necessary, and not excessive in relation to its declared and specified purpose, and that personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.⁹ Thus, the methods to be used in conducting audits may be further assessed if the same are proportional methods vis-à-vis the purposes as well as risks these may pose.

Nonetheless, we trust that the COA, as a PIC, is aware of its obligations under the DPA, its IRR, and issuances of the NPC, specifically NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies, which includes the implementation of physical, organizational and technical security measures for the protection of personal data, among others, and NPC Circular No. 16-03 on Personal Data Breach Management.

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, § 4 (e) (2012).

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

⁷ PHIL. CONST. art. IX-D § 2.

⁸ Yap v. Lagtapon, 803 PHIL 652, (2017).

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.
Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

⁶⁻⁹ Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (c).

ADVISORY OPINION NO. 2020-017¹

31 March 2020



Re: TERMINATION OF SERVICES DUE TO CORPORATE DISSOLUTION

Dear [REDACTED],

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify matters in relation to the termination of the Software Implementation Agreement (SIA) entered into by and between The Bayleaf, Lyceum of the Philippines (Bayleaf) and HDI System Technologies, Inc. (HDI) vis-à-vis the provisions of the Data Privacy Act of 2012² (DPA).

We understand that Bayleaf and HDI executed a SIA for the latter to provide human resource software modules to the former.

However, in anticipation of the forthcoming corporate dissolution of HDI, the parties drafted a Letter of Agreement (Letter) detailing the terms for the termination of the SIA. In the Letter, it was stated among others, that:

“In consideration of complete and proper disposal of the above enumerated data/information conducted by HDI Systech in the presence of and under the supervision of [REDACTED] on January 28, 2020, TBM hereby release, discharge and waive any and all actions of whatever nature which Bayleaf may have against HDI Systech,

¹ Tags: personal information controller, personal information processor, corporate dissolution; accountability; data subjects' rights; liability.

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).

its directors, officers, employees and agents by reason of or arising from any data/information regarding transactions and dealings of HDI Systech with Bayleaf and its employees, such as but not limited to electronic mail (e-mail), physical and digital copies of documents, codes, and database that HDI Systech acquired under the Software Implementation Agreement with Bayleaf executed in January 28, 2020.”

In line with the forgoing provision in the Letter, Bayleaf would now like to seek clarification on the following matters:

1. Is the stipulation in the Letter cited above tenable? Should Bayleaf require HDI to issue a certification of complete and proper disposal in lieu of the Letter? What instrument should be prepared which will best uphold the data privacy of the data subjects in this case?
2. Who shall be made liable for any negligence or punishable acts under the DPA if the responsible party is a dissolved corporation? Based on the facts, who should be made liable?

Relationship between Bayleaf and HDI

An examination of the SIA executed between the parties would reveal that Bayleaf is the customer and HDI is the supplier of the software. In this scenario, Bayleaf is the personal information controller (PIC) while the latter may be considered a personal information processor (PIP), depending on whether or not Bayleaf authorized HDI to process personal and sensitive personal information (collectively, personal data) on its behalf.

Looking at the SIA's provisions on Implementation Services and Technical Services, it seems that HDI's role is limited only with respect to assisting and preparing Bayleaf to implement the new system, guide and provide input for the converting of data, assist Bayleaf in designing the integration of the software, provide Bayleaf specific knowledge on how to configure the software and train Bayleaf's trainers and/or users on the operations of the software.

But as stated in your letter request, “in the course of performing the services, HDI processed personal data.” With this, we therefore

assume that HDI is a PIP who had the occasion to process personal data during the implementation of the SIA.

Disposal of information upon termination of agreement

The determination of the appropriate security measures to be undertaken by the parties with regard to the disposal and turnover of confidential information is best left with the parties as they are more competent in determining the needs of their organizations. This includes determining whether or not there is a need to issue a certification of complete and proper disposal or any other instrument to ensure that proper safeguards were put in place.

In this case, Paragraph 11.4 of the SIA provides for the proper and full turnover of confidential information upon termination of the Agreement between the parties. While there is a provision providing for the proper and full turnover of confidential information, the parties may also be guided by Section 27 (d) of the Implementing Rules and Regulations (IRR) of the Data Privacy Act of 2012³. Said provision mandates the parties to implement policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of personal data.

On the other hand, in determining the appropriate level of security that should be implemented, the parties may be guided by Section 29 of the IRR. As such, the parties should take into account the nature of the personal data that requires protection, the risks posed by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation.

Waiver of actions; liability for punishable acts under the DPA; dissolution; Revised Corporation Code

We note that the Letter of Agreement provides for the release, discharge and waiver of all actions of whatever nature which Bayleaf may have against HDI in connection with any data/information which HDI acquired under the SIA. However, basic is the principle that the law is deemed written into every contract, such that while a contract is the law between the parties, the provisions of positive law which regulate contracts shall limit and govern their relations.⁴

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

We note that pursuant to the principle of accountability under the DPA, PICs are expected to be responsible for any personal data under its control or custody, including the processing of information that have been outsourced to a PIP by the use of contractual or other reasonable means. With this, PIPs may still be held contractually liable to the PIC for violations of their agreement despite the provision on waiver in the Letter of Agreement.

In any case, a data subject may file a complaint in case of violation of his or her rights. Section 3 of NPC Circular No. 16-04 provides that 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.⁵

With respect to the dissolution of a corporation and the concomitant obligations and liabilities of its directors, officers, and/or employees, the same shall be governed by its Articles of Incorporation and By-Laws, and the provisions of the Revised Corporation Code (RCC).⁶

Particularly, Section 139 of the RCC provides that a corporation shall remain a body corporate for three (3) years for purposes of prosecuting and defending suits by or against it and enabling it to settle and close its affairs, dispose of and convey its property, and distribute its assets, and at any time within the said period, the corporation is authorized to convey all its property to trustees to which legal interest vests in, for the benefit of its stockholders, members, creditors and other persons in interests.

In case all of the corporation's properties are conveyed to trustees within the said three (3) year period, the trustees may sue and be sued as such in all matter connected with the liquidation. The trustees become the legal owners of the property conveyed, subject to the beneficial interest therein of creditors and stockholders.⁷

Such being the case, the liability of HDI's directors, officers, employees, agents or representatives as stated in paragraphs 15.5 and 15.6 of the SIA will remain until the time provided for under the RCC and existing rules and jurisprudence, to enable it to defend any suit against it.

⁴ Heirs of Severina San Miguel v. CA, 416 Phil. 943, 954 (2001).

⁵ National Privacy Commission, NPC Advisory Opinion No. 2017-058 (October 3, 2017).

⁶ An Act Providing for the Revised Corporation Code of the Philippines [Revised Corporation Code of the Philippines], Republic Act No. 11232 (2019).

In addition, the dissolution of the company will not affect its liability because the clauses in the SIA, by nature and intent, are intended to survive the termination of the agreement, as provided for in paragraph 11.5 of the same. Thus, the obligation for confidentiality as stated in paragraph 13.2 as well as the liability of responsible officers, who participated in, or by their gross negligence, allowed the commission of the crime, shall remain.

While we make no determination on the rights of the parties, the nature of their agreement, or possible liabilities, what is clear is that reasonable and appropriate safeguards must be put in place to protect the rights of data subjects.

This advisory opinion is based on the information provided and may vary based on additional information or when the facts are changed or elaborated.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

ADVISORY OPINION NO. 2020-018¹

31 March 2020

[REDACTED]

[REDACTED]

[REDACTED]

RE: OUTSOURCING THE PROCESSING OF PERSONAL DATA

Dear [REDACTED]

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify on whether it is permissible to relax or if there are alternatives to the requirement of an outsourcing agreement in instances where a stringent application of the Data Privacy Act of 2012 (DPA)² and its Implementing Rules and Regulations (IRR)³ is operationally or relationally not feasible.

In your letter, you disclosed that the University of the Philippines (UP) outsources the processing of personal data to various personal information processors (PIPs). Among others, UP is currently using Google's Gmail services for its email, Microsoft's OneDrive for the storage of data files, Facebook and Twitter for the process of posting information to the public and local couriers and logistic providers for delivery needs.

¹Tags: outsourcing; outsourcing agreements; personal information controllers; personal information processors.

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 Id. § 3 (f).

Outsourcing; personal information controllers and personal information processors

Outsourcing is defined as the disclosure or transfer of personal data by a personal information controller (PIC) to a service provider, considered as a personal information processor (PIP).⁴ The purpose of such disclosure is for the PIP to perform processing activities on the personal data upon the instructions of the PIC.⁵ Under an outsourcing agreement, the PIP has no other purpose for the personal data and it cannot amend or process the same outside the bounds of its agreement with the PIC.⁶ The PIP's processing of the personal data is merely to carry out the instructions given by the PIC in accordance with their agreement.

Hence, the PIC remains to be responsible for any personal data that have been outsourced or transferred to a PIP.⁷ Among others, the PIC is responsible for determining the purpose and means for the processing of the personal data. The PIC shall also ensure that the personal data transferred to a PIP for processing must not be used by the latter for other purposes and that the PIP has physical, technical and organizational security measures in place to ensure protection of the personal data.

Legal obligations of the PIC and PIP

To reiterate, the DPA allows a PIC to outsource the processing of personal data to a PIP provided proper safeguards are in place to ensure the security of such personal data.⁸ One way of ensuring both parties' compliance with the DPA is through a contract or other legal act that binds the PIP to the PIC.⁹

Based on the wording of the law, the DPA does not require every outsourcing arrangement to be governed by an outsourcing agreement. In fact, it provides that such arrangement may also be governed by any other legal act that clearly indicates the legal obligations of the parties. This way, the PIC can ensure that the PIP is legally bound to it and may be held accountable in case of breach of the agreement.

In view of the foregoing, although there is an arrangement wherein the processing of personal data is outsourced to a service provider, the wording of the DPA must not be construed literally to the effect that an outsourcing agreement must be entered into by the parties.

For instance, the applicable terms and conditions indicated when availing of the email services of Google or the engagement letter with the terms and conditions provided by a local courier shall suffice for as long as proper safeguards in the protection of personal data are in place, as required by the DPA.

We note that UP, as a PIC, is still accountable for complying with the requirements of the DPA and shall use reasonable means to provide a similar level of protection while personal data is being processed by a service provider.

This opinion is provided based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

⁵ See: National Privacy Commission, NPC Advisory Opinion No. 2018-015 (April 12, 2018).

⁶ Ibid.

⁷ Rules and Regulations Implementing the Data Privacy Act of 2012, § 50.

⁸ Id. § 43.

⁹ Id. § 44.

ADVISORY OPINION NO. 2020-019¹

28 April 2020

[REDACTED]

[REDACTED]

RE: PUBLIC DISCLOSURE OF THE LIST OF SOCIAL AMELIORATION PROGRAM BENEFICIARIES

Dear [REDACTED]

We write in response to your letter requesting for an advisory opinion from the National Privacy Commission (NPC) on whether the public disclosure of the list of beneficiaries of the Social Amelioration Program (SAP) would be considered a violation of the Data Privacy Act of 2012² (DPA).

We understand that the Department of Social Welfare and Development (DSWD) was tasked by the Inter-Agency Task Force for the Management of Emerging Infectious Diseases (IATF-EID) to spearhead the implementation of the SAP as provided for under the Bayanihan to Heal As One Act.³

Pursuant thereto, the DSWD entered into a Memorandum of Agreement and Data Sharing Agreement (DSA) with local government units (LGUs) to lay down the terms and conditions in the conduct of the physical profiling of and payout to the target beneficiaries.

¹Tags: DSWD, DILG, Social Amelioration Program, Emergency Subsidy Program, COVID-19, lawful processing, law or regulation, transparency, public funds, right to information, matters of public concern

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 An Act Declaring The Existence Of A National Emergency Arising From The Coronavirus Disease 2019 (Covid-19) Situation And A National Policy In Connection Therewith, And Authorizing The President Of The Republic Of The Philippines For A Limited Period And Subject To Restrictions, To Exercise Powers Necessary And Proper To Carry Out The Declared National Policy And For Other Purposes [Bayanihan to Heal As One Act], Republic Act No. 11469 (2020).

As instructed by the Secretary of the Department of the Interior and Local Government (DILG), some LGUs publicly posted physically or electronically, the list of said beneficiaries.

Lawful processing of personal and sensitive personal information

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 Under the law, the names of the beneficiaries of the SAP are considered personal information,⁵ and its disclosure to the public constitute processing⁶ which should comply with the requirements specifically on the criteria for lawful processing of personal information found under Section 12 thereof.

For sensitive personal information,⁷ Section 13 of the DPA generally prohibits its processing, except in certain cases enumerated therein. Furthermore, the processing should adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.⁸

While we understand that there is no formal issuance as of yet from the DILG, the public disclosure of the list may find basis for processing under Section 12 of the DPA, specifically paragraphs (c) and (e), to wit:

- The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;⁹ and
- 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.¹⁰

⁴Data Privacy Act of 2012, § 4.

⁵ Id. § 3 (g) - Personal information pertains to any information 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 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 Id. § 3 (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.

⁸ Id. § 11.

⁹ Id. § 12 (c).

¹⁰ Id. § 12 (e).

1. Facilitate the execution of the required MOA and abide by their roles and responsibilities;
2. Provide the list of target beneficiaries/clients;
3. Facilitate distribution, accomplishment and encoding of Social Amelioration Card (SAC) forms;
4. Facilitate the preparation and approval of the payroll;
5. Ensure the timely delivery of payment to the beneficiaries based on the approved payroll;
6. Monitor the delivery of assistance;
7. Submit liquidation reports within fifteen (15) working days from the completion of the distribution; and
8. Perform other actions or undertake activities consistent with the provisions of the guidelines.¹¹

In addition, the DILG Secretary directed all barangays to post the list of the beneficiaries in conspicuous public places within their communities in response to reports from field offices on the lack of transparency in the distribution of SAC forms and assistance to target beneficiaries.¹² Aside from ensuring transparency, the public disclosure was also intended to guarantee the completeness and accuracy of the list received by the barangays.¹³

The DILG further claims that the disclosure enables the residents to be adequately informed if they will receive the financial assistance from the government.¹⁴ Similarly, they are able to provide feedback if they think that they should be part of the list, following the procedures for the appeal system provided under the Memorandum.¹⁵

¹¹ Department of Social Welfare and Development, Memorandum Circular No. 09, series of 2020: Omnibus Guidelines in the Implementation of the Emergency Subsidy Program (ESP) of the DSWD, April 9, 2020, available at https://www.dswd.gov.ph/issuances/MCs/MC_2020-009.pdf (last accessed April 28, 2020).

¹² See: Department of the Interior and Local Government, DILG to Punong Barangays: Post list of SAP beneficiaries in barangay hall for transparency, April 18, 2020, available at <https://www.dilg.gov.ph/news/DILG-to-Punong-Barangays-Post-list-of-SAP-beneficiaries-in-barangay-hall-for-transparency/NC-2020-1100> (last accessed April 28, 2020).

¹³ Ibid.

¹⁴ Ibid.

¹⁵ Ibid.

Hence, it is meant to enable the LGUs to comply with their legal obligation as indicated above in an efficient and transparent manner. Consideration must also be made of the fact that the entire country is currently under the state of national emergency arising from the COVID-19 pandemic, where such public disclosure of personal information may be necessary to fulfill the respective LGUs' mandate.

Right to information on matters of public concern; COVID-19 pandemic response; utilization of public funds

We emphasize that the DPA has the twin task of protecting the fundamental human right of privacy and ensuring the free flow of information.¹⁶ As such, the DPA will not operate to hinder the LGUs in disclosing information which it deems essential for the public to know, especially when there is an increasing public demand for transparency on the distribution of the financial assistance.

The right of the people to information on matters of public concern is a constitutionally vested right. Thus, the public disclosure may also be anchored on the LGU's compliance with Section 7, Article III of the 1987 Constitution,¹⁷ in conjunction with Section 28, Article II of the same which states that, "Subject to reasonable conditions prescribed by law, the State adopts and implements a policy of full public disclosure of all its transactions involving public interest."

It is worth mentioning that in the case of *Akbayan v. Aquino*,¹⁸ the Supreme Court held that:

"In determining whether or not a particular information is of 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. xxx" (underscoring supplied)

Considering the serious threat of the COVID-19 pandemic not just to

¹⁶ Data Privacy Act of 2012, § 2.

¹⁷ PHIL. CONST. art. 3 § 7 - The right of the people to information on matters of public concern shall be recognized. Access to official records, and to documents, and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development, shall be afforded the citizen, subject to such limitations as may be provided by law.

¹⁸ G.R. No. 170516, July 16, 2008.

¹⁹ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).

the citizens' health and safety but also to their means of livelihood, they would naturally want to know any information about the government's actions in these extraordinary times. Consequently, information about the utilization of public funds for the implementation of the Emergency Subsidy Program in accordance with Bayanihan Act is a matter of public concern, especially for the target beneficiaries who may suffer the greatest impact of the enhanced community quarantine (ECQ).

General data privacy principles; proportionality

Note, however, that said public disclosure of personal information should strictly adhere to the principle of proportionality. This principle requires 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 purpose of the processing could not reasonably be fulfilled by other means.”¹⁹

In this case, uploading the list of SAP beneficiaries online may be deemed to be the only way to achieve the purpose of ensuring the meaningful exercise of the public of their right to access information of public concern. This is mainly because of the physical limitations imposed by the ECQ where the posting in barangay halls and other areas may be pointless or ineffective.

Nonetheless, the LGUs are equally urged to apply the proportionality principle in determining the types of personal data that they will disclose, particularly when the original list of SAP beneficiaries contains sensitive personal information.

For this reason, LGUs are reminded that releasing sensitive personal information may be excessive and no longer be considered as necessary for the purpose of the disclosure and may constitute an unwarranted invasion of privacy. Sensitive personal information includes but is not limited to the following:

- Marital status
- Date of birth/age
- Religion
- Government-issued ID numbers, i.e. GSIS, Passport, PhilHealth, PRC, SSS, UMID, or Senior Citizen ID number, etc.

We reiterate that the processing of sensitive personal information is prohibited, except for the instances provided for under Section 13 of the DPA, i.e., the data subject has given consent, processing is provided for by existing laws and regulations, 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, among others.²⁰

In view of the foregoing, the public disclosure of the list of SAP beneficiaries by the LGUs may not constitute a violation of the DPA insofar as it complies with the requirements established by law and jurisprudence for allowable public disclosures of information on matters of public concern.

While the processing may be justified, the DILG and the LGUs should be mindful of its concomitant responsibilities as personal information controllers. They should consider posting a privacy notice in their respective websites and other official channels to properly inform the SAP beneficiaries and the general public of the rationale for such public disclosure of personal data, their rights of data subjects, appropriate security measures being implemented to protect their personal data, among others.

This opinion is rendered based on the information you have provided. It does not adjudicate issues between parties nor impose any sanctions or award damages, and shall not be used in the nature of a standing rule binding on the NPC when evaluating other cases regardless of the similarity of the facts and circumstances. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

²⁰ Data Privacy Act of 2012, § 13.

ADVISORY OPINION NO. 2020-020¹

26 May 2020



Re: COLLECTION OF FEES RELATIVE TO RIGHT TO CORRECTION OF DATA SUBJECTS' PERSONAL INFORMATION

Dear 

This pertains to your request for advisory opinion received by the National Privacy Commission (NPC) which sought to clarify whether a personal information controller (PIC), such as an airline company, which collects personal information of its passengers for purposes of booking a flight, may charge and collect reasonable fees for accommodating a data subject's request to rectify or correct his or her personal information, particularly his or her name in a passenger ticket.

We understand that the fees collected shall be used to defray administrative costs that will be incurred by the PIC in manually amending the personal data of the data subjects, and in reissuing a new ticket with the corrected personal information.

Right to rectification; charging of fees

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 Data Privacy Act of 2012, § 16 (d).

³ 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, Art. 12 (5) (2016).

The Data Privacy Act of 2012¹ (DPA) recognizes the data subjects' right to dispute the inaccuracy or error in his or her personal data and have the PIC correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable.²

The DPA has no provisions regarding the charging of fees relative to a data subject's request for rectification. Nevertheless, the EU General Data Protection Regulation (GDPR),³ the successor of the EU Data Protection Directive (Directive 95/46/EC) which heavily influenced the DPA, provides guidance on the matter:

"5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- (b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request." (underscoring provided)

From the foregoing, requests to correct or rectify clerical or typographical errors in the records of the data subject, particularly his or her name, should be processed free of charge. It is only when such request is manifestly unfounded or excessive that reasonable fees may be charged. And where such fees are thus charged, the same shall not be so prohibitive as to have the effect of discouraging the exercise of data subjects' rights.

As applied in the case of an airline company, we understand that these proposed fees shall defray costs to accommodate the increasing number of requests by passengers for rectifying their names, and will be charged only to those passengers whose bookings were made through the website of the airline company.

With this, it seems that such requests from individual passengers are not in the nature of being “manifestly unfounded or excessive.” Moreover, as these requests pertain to bookings made online, there should likewise be some form of mechanism whereby data subjects may also easily exercise their right to rectification online as well, without necessarily imposing much administrative costs on the part of the airline company with regard to correcting names and reissuing tickets.

The foregoing considered, passenger requests for simple name corrections should be carried out free of charge.

This opinion is based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2020-021¹

26 May 2020



Re: AUTOMATED RETRIEVAL OF BANK TRANSACTION HISTORY

Dear 

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify issues on the rights of data subjects and compliance requirements under the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR) and other relevant issuances of the NPC in relation to automated retrieval of data.

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify issues on the rights of data subjects and compliance requirements under the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR) and other relevant issuances of the NPC in relation to automated retrieval of data.

You further disclosed that ING intends to ease the loan application process by shortening the period of assessment and at the same time, ascertaining the authenticity of the documents submitted. ING, through its mobile app, aims to automate the manual process of requesting for copies of a potential borrower's bank statements from other banks for a faster approval process. The proposed automated retrieval process shall enable potential borrowers to retrieve their transaction history (e.g. date, description of transaction, debit and credit entries and account balance) from other online banking accounts and facilitate immediate submission of the same to ING.

¹ Tags: personal information; lawful criteria for processing; consent; automated retrieval; bank transaction history; loan application; right to access; right to data portability; right to be informed; security measures.

As illustrated in your letter, during the loan application process, potential borrowers can select the specific bank/s from which to retrieve their transaction history by entering the respective online banking account log-in credentials for the said selected bank/s in the ING mobile app.

The ING mobile app shall then access the respective online bank account/s for the sole purpose of extracting the potential borrower's name, account number and transaction history over a twelve-month period or a shorter period, whichever is allowed by the other bank/s. ING shall engage a service provider to provide the technology that will enable the automated retrieval feature of the mobile app. However, the decision on whether a potential borrower's loan application will be granted shall still be done manually by a bank officer, based on the standards set by ING.

You now seek clarification on the following issues:

- 1) Is authorization under the automated retrieval process an exercise of the rights of the data subjects?; and
- 2) What are the compliance requirements under the DPA and related issuances of the NPC applicable to the automated retrieval process?

Nature of personal data; processing of personal data; automated retrieval

The DPA defines personal information as any information, whether recorded in a material form or not, from which the identify 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

On the other hand, processing of personal information and sensitive personal information, collectively referred to as personal data, is any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.³ Given its broad definition, it includes anything that can be done with personal data in any form, including by automated means.

² 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, § 3 (g) (2012).

³ Id. § 3 (j).

Hence, the name, account number and the bank account transaction history of a potential borrower are considered personal information since it directly identifies a specific individual. The automated retrieval thereof, considered a form of processing, must comply with the standards provided by Section 12 of the DPA.

Exercise of the rights of a data subject; right to access; right to data portability

The rights of a data subject pertaining to access and portability correspond with each other. The right to access allows a data subject reasonable access to, upon demand, the following:

1. Contents of his or her personal information that were processed;
2. Sources from which personal information were obtained;
3. Names and addresses of recipients of the personal information;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal information to recipients;
6. Information on automated processes where the data will or likely to be made as the sole basis of any decision significantly affecting or will affect the data subject;
7. Date when his or her personal information concerning the data subject were last accessed and modified; and
8. The designation or name of identify and address of the personal information controller.⁴

On the other hand, the right to data portability is referred to as the right of a data subject to obtain from a personal information controller a copy of his or her personal data that was processed or undergoing processing by the latter, in an electronic or structured format, which is commonly used and allows for further use by the data subject.⁵ This right primarily takes into account the right of the data subject to have control over his or her personal data being processed by the personal information controller based on consent or contract, for commercial purpose, through automated means.⁶

Based on the foregoing, data subjects are entitled to have reasonable access to their respective personal data. Upon being given such access, data subjects may request to be given a copy of the data in a

portable format where such personal data is being or was processed in an electronic or structured format.

Potential borrowers are considered data subjects not only of ING but also that of other bank/s where they have accounts with. To illustrate, a person applying for a loan with ING who wishes to use his or her bank statements from Bank A to fulfill ING's loan application requirement is a data subject of both ING and Bank A. As a data subject of Bank A, the potential borrower is entitled reasonable access to his or her bank transaction history for a given time period and can also request for copies of his or her transaction history.

In your query, the rights to access and data portability shall be exercised by the data subject through the ING mobile app by entering his or her log-in credentials for the selected bank, Bank A. The mobile app shall then access the said online banking account and retrieve the potential borrower's name, account number and transaction history. ING, through its authorized bank officers, shall then use such information to assess the potential borrower's capacity to pay the loan.

The automated retrieval feature may be considered as an exercise of data subject rights through the ING platform, pursuant to the authority given by the data subjects themselves.

Additionally, ING should take into consideration the requirements under the DPA and related issuances of the NPC which may be applicable to the automated retrieval process. Specifically, the requirements on obtaining consent, the right of data subjects to be informed, adherence to the general data privacy principles, and the safeguards to be implemented to protect personal data against any unauthorized processing.

Consent; right to be informed; general data privacy principles; security measures

A data subject is entitled to make an informed decision when it comes to the processing of his or her personal information. Under the DPA, consent should be 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.⁷ It may be evidenced by written, electronic or recorded means.⁸

4 Id. § 16 (c).

5 Id. § 18.

6 Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 36 (2016).

A data subject shall also have the right to be informed whether personal information pertaining to him or her will be, are being, or were processed and pertinent details related thereto.⁹

Hence, a potential borrower must be adequately informed of the processing activity involving his or her personal information and provide consent to ING to access his or her online banking accounts with other banks. As disclosed in your letter, ING shall obtain the consent of potential borrowers in the automated retrieval of their respective personal information.

We note that the act of merely entering the log-in credentials for a particular online banking account does not necessarily equate to the consent required by the DPA. To be considered as valid consent, the potential borrower must be fully informed, among others, of the type of personal information to be processed, how it will be processed, person/s or organization/s in charge of processing and the purpose thereof, prior to entering his or her log-in credentials in the ING mobile app. The data subject shall also have the right to be notified and furnished with the particulars on, among others, the methods utilized for automated access and the extent to which such access is authorized, before the entry of his or her personal information.

In addition, ING's mobile app must have mechanisms to enable the exercise of data subject rights, including the right to object to the processing of their personal data and/or to withdraw consent, where applicable.

We also note that, as mentioned in your letter, all the extracted data will be encrypted, whether the same is at rest or in-transit. Log-in credentials will also be encrypted and shall not be stored. With this, ING should also provide information to the data subjects regarding the storage and retention of the extracted data, details on what will happen to the same should the loan application be denied, and other pertinent information.

Although ING may have legal basis for the lawful processing of the potential borrowers' personal information, it remains subject to the requirements of implementing security measures to protect personal information.

⁷ Data Privacy Act of 2012, § 3 (b).

⁸ Ibid.

⁹ Id. § 16 (a-b).

As a personal information controller, ING must still adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. As you already mentioned in your letter, ING shall ensure that the general data privacy principles are complied with by informing potential borrowers of the purpose for the processing of their personal information, how such data shall be processed, collecting only what is necessary for the purpose of such processing and that there are no other means to achieve such legitimate purpose.

ING must implement reasonable and appropriate organizational, technical, and physical security measures to ensure the protection of personal information against any accidental or unlawful destruction, alteration or disclosure and against any other unlawful processing.¹⁰ Considering that ING will be engaging the services of a personal information processor, such arrangement must be covered by an outsourcing agreement or similar agreement to clearly define the legal obligations and liabilities of each party with regard to each other and the data subjects. The service provider must also demonstrate compliance with the DPA.

ING must also take into consideration issues which may be encountered with the proposed automated retrieval system, i.e. access controls, limitations as to accessing the transaction history for the past twelve-month period (or shorter) only, the retention of personal information of potential borrowers who were not approved for the loan application, etc.

Moreover, ING should also conduct a privacy impact assessment to identify and provide an assessment of various privacy risks, and propose measures intended to address and mitigate the effect of these risks on the data subjects.

We emphasize that the DPA, its IRR and other issuances of the NPC do not prohibit banks from implementing innovations to ease banking transactions, provided that the rights of the data subjects are always given paramount consideration.

This opinion is provided based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

¹⁰ Data Privacy Act of 2012, § 20.

ADVISORY OPINION NO. 2020-022¹

8 June 2020

ADVISORY OPINION
2020-022



Re: PUBLIC DISCLOSURE OF IDENTITIES OF COVID PATIENTS FOR CONTACT TRACING

Dear 

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify issues on contact tracing and the public disclosure of identities of COVID-19 patients vis-à-vis the provisions of the Data Privacy Act of 2012² (DPA) and other relevant issuances of the NPC and the Department of Health (DOH).

Specifically, you ask what would be the measures to address patient tracking without publicly announcing or reporting the name, sex, and residence or barangay as well as the places where the probable patients travelled to for the past two (2) weeks, and those with whom he or she had been in contact with.

You further ask if it is appropriate for the concerned local government unit (LGU), through their health personnel, to allow the public to assess their own risks by sharing the above information.

Finally, you ask the limit in terms of what information to collect and disclose, whom to disclose, method or process of information gathering, and data storage and retention so it will not be used in the future for malicious reasons.

¹ Tags: processing; public disclosure; public authority; statutory mandate; law; Department of Health; COVID-19; contact tracing; privacy guidelines.

² 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).

Processing of health information; contact tracing; COVID-19 data; lawful basis for processing; public authority; mandate

Contact tracing as defined under recent regulations of the DOH refers to the identification, listing, and follow-up of persons who may have come into close contact with a confirmed COVID-19 case.³ It has three (3) goals:

1. To interrupt ongoing transmission and reduce spread of infection;
2. To alert close contacts to the possibility of infection and offer preventive counselling or care; and
3. To understand the epidemiology of a disease in a particular population.⁴

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.

We wish to emphasize that the DPA has never been a hindrance to contact tracing activities of the government as the law does not prevent government institutions from processing personal data when necessary to fulfill their mandates.

We reiterate our 2018 Advisory Opinion issued to the DOH on the processing of health information pursuant to its mandate of conducting disease surveillance, epidemic investigation, contact tracing, survey research and disease registry, among others, at the national and regional level:

“... In this case, the DPA does not prohibit the DOH from collecting and processing personal data for purposes necessary to its mandate, with the concomitant responsibility of complying with the requirements of the DPA, its Implementing Rules and Regulations (IRR), and other issuances of the National Privacy Commission (NPC).

The processing of personal data by DOH finds support in the DPA. The DOH is a public authority performing regulatory functions, and is permitted to process personal data to the extent necessary for the fulfillment of these functions.”⁵

The DPA recognizes that the government can perform its functions in this pandemic while still guaranteeing the data privacy rights of our citizens. The law requires that all government agencies involved in the COVID-19 response, i.e. the DOH, agencies authorized by the DOH, and other agencies or entities authorized by law, specifically on contact tracing, shall adhere to the general data privacy principles, implement safeguards to protect personal data they process, and uphold data subjects’ rights at all times.

Disclosure of personal data; limitations; risks of publicly disclosing personal data

As to disclosure of COVID-19 personal data by the DOH, this may be made in a limited manner pursuant to the Annex A of the DOH Updated Guidelines on Contact Tracing:

“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.

³ Department of Health, Updated Guidelines on Contact Tracing of Close Contacts of Confirmed Coronavirus Disease (COVID-19) Cases [Department Memorandum No. 2020-0189], § II (A) (April 17, 2020).

⁴ Id. § III (B).

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.”⁶

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*,⁷ which contains a similar provision under Section VI (D) (2) thereof on the Specific Guidelines on Use and Disclosure of Health Information.

Further, the JMC provides that aggregate health information, or pseudonymized or anonymized detailed health information may be disclosed for a legitimate purpose, i.e. public information or purpose.⁸ This is also consistent with the DOH Updated Guidelines on Contact Tracing provisions on Protecting Data Privacy of COVID-19 Cases and Close Contacts,⁹ where it was declared that “the DOH reserves the right to release information on COVID-19 cases that are relevant for public health interventions without full disclosure of the case’s identity.”

Hence, the general public will not be kept in the dark as to the government’s contact tracing efforts since aggregate, pseudonymized, or anonymized data may still be made available.

This may include details on a patient’s sex, age, barangay, travel history, etc., taking caution that a COVID-19 suspected, probable, or confirmed case should not be capable of being identified from the data that is released following the DOH guidelines. These pseudonymized data may thus allow the public to assess their own risks without necessarily compromising the COVID-19 patients’ privacy rights.

We stand firm against any form of unbridled disclosure of patients’ personal data to the public that has been proven to cause a real risk of severe harm to patients, i.e. physical assaults, harassments, discrimination, among others.¹⁰

⁶ National Privacy Commission, NPC Advisory Opinion No. 2018-083 (Nov. 26, 2018).

⁷ DOH Department Memorandum No. 2020-0189, Annex A - Guidelines for Processing and Disclosure of the Personal Information of Patient/Data Subject.

⁸ Department of Health and National Privacy Commission, Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response [Joint Memorandum Circular No. 2020-0002] (April 24, 2020).

⁹ *Id.* § VI (D) (3).

¹⁰ DOH Department Memorandum No. 2020-0189, § IV (I) (3).

Storage and retention; further processing

As to the limit in terms of personal data storage and retention, the general rule is that personal data may be retained as necessary to fulfill the purpose for which these were collected, pursuant to the laws, rules and regulations and other protocols on the matter. After achieving the intended purpose/s, personal data shall be disposed in a secure manner that would prevent any unauthorized processing and disclosure.

The above shall likewise apply to all personal data processed in relation to all contact tracing efforts, be it manual or through the use of online applications or any other emerging technologies.

As to any further processing activities, the JMC provides that only aggregate health information or pseudonymized health information shall be shared by public health authorities to stakeholders for the purpose of business intelligence and policy and biomedical researches.¹¹ Further, all policy and biomedical researches related to COVID-19 surveillance and response shall secure an Ethics Board approval prior to implementation.¹²

This opinion is provided based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

¹⁰ See: NPC PHE Bulletin No. 11: Joint Statement of the Department of Health (DOH) and National Privacy Commission (NPC) on Processing and Disclosure of COVID-19 Related Data, April 30, 2020 (available at <https://www.privacy.gov.ph/2020/04/npc-phe-bulletin-no-11-joint-statement-of-the-department-of-health-doh-and-national-privacy-commission-npc-on-processing-and-disclosure-of-covid-19-related-data/>).

¹¹ DOH and NPC Joint Memorandum Circular No. 2020-0002, § VI (F) (1).

¹² Id. § VI (F) (2).

ADVISORY OPINION NO. 2020-023¹

11 June 2020



Re: PUBLIC POSTING OF LISTAHANAN RESPONDENTS

Dear 

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify whether the public display of personal information by the Department of Social Welfare and Development (DSWD) of the respondents for its program, the National Household Targeting System for Poverty Reduction (NHTS -PR), also known as Listahanan, is in accordance with the Data Privacy Act of 2012² (DPA).

We understand that the Listahanan was established by virtue of Executive Order (EO) No. 867, series of 2010 with the mandate of establishing a system of identifying who and where the poor households are in the country. The DSWD, through the National Household Targeting Office (NHTO), is mandated to maintain and update the Listahanan database.

We understand further that the DSWD will be posting an initial list of the poor households at the barangay office and other designated public places. The purpose for such posting is to enable the households to review and validate the information and at the same time, provide the opportunity for the community, especially those who were not assessed during the data collection phase, to file grievances for non-inclusion in the list, and appeals and complaints on possible errors such as family information, classification and non-assessment. All grievances shall then be evaluated by the Barangay Verification Committee and Local Verification Committee at the municipal level.

¹ Tags: personal information; sensitive personal information; DSWD; Listahanan; privacy notice.

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 public posting of the initial list of poor households may find basis under Section 12 of the DPA – where the processing of personal information is necessary to fulfill the functions of the public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.³

The DSWD is the primary government agency mandated to develop, implement and coordinate social protection and poverty-reduction solutions for and with the poor, vulnerable and disadvantaged.⁴ E.O. No. 867 requires all national government agencies to adopt the NHTS-PR as a mechanism in identifying who and where the poor households are who will be the recipients of the social protection programs.⁵ Consequently, E.O. 867 also mandated DSWD to maintain the system and serve as the repository of the data on poor households and update the same every four (4) years.⁶

We note that, although there may be legal basis in displaying the initial list of poor households in public places, DSWD is still obligated under the DPA to comply with the general data privacy principles of transparency, legitimate purpose and proportionality.

Adherence to the general data privacy principles; sensitive personal information

In posting the list, DSWD must ensure that the data subjects are informed about the details of the processing of their personal data. This may be achieved through a privacy notice, preferably in Filipino and/or the dialect being spoken in a particular area, to explain to the data subjects the purpose for posting the list, i.e. to review and validate information, for those not assessed to file grievances, appeals, complaints on possible errors, and non-assessment, etc. It should also state the means for them to access information previously collected, correct any inaccurate information and other details which will help them exercise their rights as data subjects.

DSWD must also consider the proportionality principle in determining the personal information that will be publicly displayed.

³ Data Privacy Act of 2012, § 12 (e).

⁴ Official Gazette, Department of Social Welfare and Development, available at <https://www.officialgazette.gov.ph/section/briefing-room/department-of-social-welfare-and-development/> (last accessed May 18, 2020).

⁵ Office of the President Providing for the Adoption of the National Household Targeting System for Poverty Reduction as the Mechanism for Identifying Poor Households Who Shall Be Recipients of Social Protection Programs Nationwide, Executive Order No. 867 [E.O. No. 867], Section 1 (March 9, 2010).

⁶ Id. § 2.

⁷ Data Privacy Act of 2012, § 11 (c).

In particular, the principle requires that the processing of information shall be adequate, relevant, suitable, necessary and not excessive in relation to the declared and specified purpose.⁷ Hence, there is a need to determine if the public posting of the names of the potential beneficiaries is proportional to the purpose of reviewing and validating the accuracy of such list and after considering all other means that may result in less exposure to the data subjects.

It is worth noting that the inclusion of any sensitive personal information in the list to be publicly posted should be carefully evaluated if the same is indeed necessary and proportional to the purpose. Note that generally, the processing (which includes public posting/disclosure) of sensitive personal information is prohibited, except for the instances provided by Section 13 of the DPA.

Hence, if the birthday (a variation of the information on “age”) and/or other sensitive personal information of the data subjects (i.e. marital status, religion, etc.) are not indispensable to achieve the stated purpose, the DSWD should consider removing this field of information in the list to be posted.

Since sensitive personal information will be maintained by DSWD, a government agency, such sensitive personal information shall be secured with the use of the most appropriate standard recognized by the information and communications technology industry and as recommended by NPC.⁸

Household Assessment Form; comments; recommendations

In order to ensure that the respondents understand the Household Assessment Form (HAF) including the Declaration and Certification portions on how their personal data will be used, it is recommended that the form be translated into Filipino or the language or dialect commonly used in the respective area.

On the Declaration portion, the third paragraph states that the respondent authorizes DSWD to “... allow processing and controlled disclosure or transfer of data to its development partners and other stakeholders...” There is a need to clarify who these development partners and other stakeholders are and the purpose/s, nature and extent for the controlled disclosure or transfer to their of data.

If this controlled disclosure or transfer to third parties is for purposes outside of “determining poverty status and serve as basis for research and in the development and implementation of social protection programs and services to promote the interest of the poor”, it may be advisable to provide a separate tick box in order to obtain consent from the respondents for DSWD to share data with third parties, if consent is the most appropriate basis for such processing activity.

On the Certification portion, we recommend stating that the enumerator has explained to the respondent the uses for the information collected, the opportunity provided for them to access information previously collected, to correct any errors or inaccuracies upon posting of the initial list, and to which entities the said information will be shared, if any.

This opinion is provided based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

⁸ Id. § 22.

ADVISORY OPINION NO. 2020-024¹

16 June 2020



Re: DISCLOSURE OF LOT BUYERS'/HOMEOWNERS' CONTACT INFORMATION FOR COLLECTION OF MONTHLY ASSOCIATION DUES

Dear {



We write in response to your letter request on whether the disclosure of the contact information of lot buyers/homeowners to the homeowner's association, for purposes of collection of monthly association dues, is allowed under the provisions of the Data Privacy Act of 2012² (DPA), its Implementing Rules and Regulations (IRR)³ and relevant issuances of the National Privacy Commission (NPC).

In your letter addressed to [REDACTED] of the Housing and Land Use Regulatory Board (HLURB) which was subsequently endorsed to the NPC, you stated that the newly elected presidents of Royal Villas West Homeowners, Inc. and Ashiyana Tagaytay Classics Homeowners', Inc. (collectively, HOAs) requested for the contact information of the lot buyers/homeowners of Anhawan Development, Inc. and Royal Asia Multi Properties, Inc. (collectively, Developers), respectively. The purpose for such requests was to facilitate the collection of the monthly association dues.

Contact information; disclosure; data privacy principles; legitimate interest

¹ Tags: contact information; disclosure; 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 Other Purposes, "Data Privacy Act of 2012" (15 August 2012).

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

It is worth noting that under the DPA, contact information of individuals are considered as personal information.⁴ The Developers, as personal information controllers (PICs), have the responsibility of ensuring the lawful processing of its clients' personal information in accordance with Section 12 of the DPA.

In particular, Section 12 (f) provides that the processing of personal data may be allowed if the processing is necessary for the purposes of the legitimate interests pursued by the PIC or by a third party 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.⁵

To determine if there is legitimate interest in processing personal information, PICs must consider the following: ⁶

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.⁷

Although a personal information controller may have lawful basis for the processing of information, it must still adhere to the basic data privacy principles of proportionality, transparency and legitimate purpose. The processing of personal information must be limited only to the extent that is necessary for the stated purpose and that there are no other means to achieve such legitimate purpose.

⁵ Id. § 12(f).

⁶ 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-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>.

⁷ 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/> (last accessed July 13, 2019).

⁸ An Act Providing for a Magna Carta for Homeowners and Homeowners' Associations, and for Other Purposes [Magna Carta for Homeowners and Homeowners' Associations], Republic Act No. 9904, § 5 (2009).

⁹ Id. § 12 (b).

Monthly association dues; membership; Magna Carta for Homeowners and Homeowners' Associations

We note that it is among the rights and duties of every homeowner to enjoy the basic community services and facilities, provided that he or she pays the necessary fees and other pertinent charges.⁸ It is also among the duties and responsibilities of the Board of Directors or Trustees of a HOA to collect the fees, dues and assessments that may be provided for in the by-laws, as approved by a majority of its members.⁹

From the foregoing, the disclosure by the Developers of its clients' contact information to the HOAs depends on the determination of what the term "monthly association dues" pertain to and the type of membership in the said HOAs.

It is important to establish the definition of the term "monthly association dues" referred to in your letter, in accordance with the provisions of the by-laws of the corresponding HOAs. For instance, the fees included in the monthly association dues and if such association dues are required to be paid by all homeowners or limited only to HOA members. It is worth noting that the term "association dues" has not been defined under the Magna Carta for Homeowners and Homeowners' Association and its IRR. Instead, the said laws provide that the association by-laws shall provide the dues, fees and special assessments to be imposed and its manner of imposition.¹⁰

If the HOAs can confirm that the payment of monthly association dues applies to all homeowners regardless of whether or not they are members of the HOAs, then the HOAs, as third parties, have legitimate interests in the disclosures of the homeowners' contact information.

On the other hand, if payment of the monthly association dues only applies to members of the HOAs, then it is imperative to determine if membership in the HOAs is automatic for all homeowners. Membership in a HOA is optional, unless otherwise provided in the instruments of conveyance or as annotated in the title of the property.¹¹ Hence, if such documents signed by the said homeowners provide for automatic membership in the HOAs by mere ownership, then they are indeed HOA members and are thus obliged to pay the fees, as may be imposed by the HOA officers in accordance with the by-laws.

The Developers and HOAs may also consider entering into a data sharing agreement (DSA) among themselves, considering that they are all personal information controllers under the DPA and with different purposes in the processing of the homeowners'/landowners' personal information. The DSA shall clearly indicate details, such as but not limited to, the purpose of the sharing, the personal information to be shared and the respective rights and obligations of each party to the agreement.

Given the foregoing, we note that the Developers may lawfully disclose the contact information of the homeowners, provided that the two salient points have been established.

This opinion is based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

¹⁰ Id. § 15 (o).

¹¹ Rules and Regulations Implementing the Magna Carta for Homeowners and Homeowners' Associations, Republic Act No. 9904, § 9 (2011).

ADVISORY OPINION NO. 2020-025¹

16 June 2020



Re: CONFLICT OF INTEREST ON A DATA PROTECTION OFFICER DESIGNATED AS A COMPLIANCE OFFICER

Dear 

We write in response to your request for an advisory opinion seeking clarification on matters relating to the role of a data protection officer (DPO) vis-à-vis the department reorganization within your company. Essentially, you ask whether there will be an independence issue and conflict of interest if the DPO who is currently under the Executive Department and reports to the highest officer in the plant, will be transferred to the Risk and Assurance Department (Risk Department), and will be assigned to function as the Compliance Officer at the same time.

We understand that the Compliance Officer handles the monitoring of the company's various compliance requirements and activities, i.e. renewal of permits, licenses, third party contracts, working visas, alien employment permits, health insurance of expatriate employees, etc. You claim that the tasks of a Compliance Officer would require processing the personal data of employees which gives rise to a conflict of interest vis-à-vis the duties as a DPO.

Data protection officer; independence; autonomy

It is true that a DPO must be independent in the performance of their functions and shall be afforded a significant degree of autonomy by the personal information controller (PIC) or personal information processor (PIP).² However, this principle must be harmonized with the employer's right to fully manage and control his or her business, subject only to the limitations provided by law.

¹Tags: data protection officer; compliance officer; independence; conflict of interest.

² National Privacy Commission, Designation of Data Protection Officers [NPC Advisory No. 2017-01] (March 14, 2017).

You mentioned that it is proposed that the Risk Department will facilitate the overall implementation of the Compliance Management System that covers Data Privacy Compliance. From cursory reading of the facts, it seems that the Risk Department will only be overseeing Data Privacy Compliance and may not necessarily interfere with the functions of the DPO. Further, being placed under the direct supervision of any of the company's departments does not necessarily entail the loss of the DPO's independence and autonomy.

NPC Advisory No. 2017-01 is clear in its requirement that a DPO shall be allowed to enjoy a sufficient degree of autonomy, and that for this purpose, he/she must not receive instructions from the PIC or PIP regarding the exercise of his/her tasks. A DPO is not required to have total or complete autonomy as the independence required only pertains to the exercise of his/her tasks.

Direct supervision of a company department can pertain to various aspects of employment such as monitoring and implementing compliance with company rules and regulations, or the setting of qualitative and quantitative parameters for accomplishments. These, however, does not necessarily encroach on the performance of a DPO's functions and/or tasks and the DPO can still perform each task independently without any interference from the department he was assigned to.

Furthermore, under the doctrine of management prerogative, every employer has the inherent right to regulate, according to his own discretion and judgment, all aspects of employment, including hiring, work assignments, working methods, the time, place and manner of work, work supervision, transfer of employees, lay-off of workers, and discipline, dismissal, and recall of employees.³

Nonetheless, if based on your assessment, there will indeed be an independence issue if the DPO would made to report to the Risk Department, you are not precluded from formally communicating the same to the pertinent officers in your company and documenting the outcome.

Simultaneous designation as DPO and Compliance Officer; conflict of interest

Another related concern you raised is the seeming conflict of

interest with the designation of the DPO as the Compliance Officer simultaneously. You stated that the conflict of interest arises mainly because of the functions to be performed by a Compliance Officer conflicts with the functions of a DPO.

Specifically, you pointed out that the function of monitoring company compliance for the operations and maintenance makes a Compliance Officer a process owner, and thus creates the conflict vis-à-vis a DPO's functions.

To backtrack, conflict of interest refers to a scenario wherein a DPO is charged with performing tasks, duties, and responsibilities that may be opposed to or could affect his performance as DPO, i.e. holding a position that leads him to determine the purposes and the means of the processing of personal data.⁴

Further, we note the pertinent discussions under Article 29 of the Data Protection Working Party of the European Commission - Guidelines on Data Protection Officers ('DPOs')⁵ on the matter of conflict of interest, to wit:

"... This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing."

We understand the concern about processing personal data by the DPO as a Compliance Officer.

³ Rural Bank of Cantilan, Inc. v. Julve, 545 Phil. 619 (2007).

⁴ NPC2017-01, Definition of Terms.

⁵ European Commission, Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017, page 16, available at <https://ec.europa>.

Nevertheless, we note that this will essentially entail monitoring compliance with a predetermined or set compliance requirements with various government agencies or other third parties, i.e. submission of reportorial requirements, securing permits, renewing business licenses, reviewing contracts, etc. These are recurring and standard tasks that are accomplished on a regular basis.

In a sense, a Compliance Officer does not technically have much discretion or flexibility to actually determine the purposes and the means of the processing personal data as most, if not all, of the compliance requirements are pursuant to a specific law or regulation.

Nevertheless, a DPO can make his or her opinion on the matter known to management to help the latter in identifying the positions which would be incompatible with the function of a DPO. Pursuant to the Article 29 of the Data Protection Working Party of the European Commission - Guidelines on DPOs, internal rules may be drafted to avoid conflict of interests, where such rules may provide for the following, to wit:

- Identification of the position/s which would be incompatible with the function of DPO;
- Draft internal rules to avoid conflicts of interests;
- Provide an explanation about conflicts of interests;
- Declare that the DPO has no conflict of interests with regard to his/her function as a DPO, as a way of raising awareness of this requirement;
- Include safeguards in the internal rules of the organization and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests.⁶

As provided in NPC Advisory 2017-01, the “opinion of the DPO or the Compliance Officer for Privacy(“COP”) must be given due weight. In case of disagreement, and should the PIC or PIP choose not to follow the advice of the DPO or COP, it is recommended, as good practice, to document the reasons therefor.”

This opinion is provided based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

⁶ See: European Commission, Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017, page 16, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (last accessed: 17 June 2020).

ADVISORY OPINION NO. 2020-026¹

26 June 2020

[REDACTED]

[REDACTED]

[REDACTED]

Re: PUBLIC DISCLOSURE OF PERTINENT DATA NEEDS IN THE TIME OF COVID-19

Dear [REDACTED]

We write in response to your request for an Advisory Opinion received by the National Privacy Commission (NPC) to clarify whether or not the public disclosure of pertinent information of beneficiaries of the different government programs related to COVID-19 response is a violation of the Data Privacy Act of 2012² (DPA).

In particular, you seek guidance on the legality of disclosing information involving but not limited to the following:

1. General Data Requests

- Release (to private requesters) of information related to government programs granting various forms of benefits or incentives; and
- The publication of such information in an open data machine-readable format (e.g. XLSX, CSV, JSON) in official government and civil society tracking websites.

¹ Tags: right to privacy; freedom of information; disclosure of beneficiary data; special cases; accountability; transparency; proportionality; pseudonymization; statistics

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).

2. Data relevant to benefits granted/received in line with the Government's COVID-19 response and operations, including but not limited to the following:

- DSWD Social Amelioration Program, e.g. Emergency Subsidy Program (ESP), Assistance to Individuals in Crisis Situations (AICS), Social Pension for Senior Citizens (SocPen), Livelihood Assistance Grants (LAG): program name, beneficiary names, amounts received, barangay, city/municipality, province;
- DOLE COVID-19 Adjustment Measures Program (CAMP)/Tulong Panghanapbuhay sa Ating Disadvantaged/Displaced Workers (TUPAD)/AKAP: business name, beneficiary names, amounts received, barangay, city/municipality, province of business and beneficiary;
- DA Financial Subsidy to Rice Farmers (FSRF), DA Rice Farmer Financial Assistance (RFFA), Expanded Survival and Recovery (SURE) Aid and Recovery Program: beneficiary names, amounts received, barangay, city/municipality, province;
- DOF-SSS Small Business Wage Subsidy: business name, beneficiary names, amounts received, barangay, city/municipality, province of business and beneficiary; and
- PhilHealth Advisory No. 2020-022, and Circular Nos. 2020-0009, 2020-0011, and 2020-0012: Number of recipients of full financial risk protection, and total amount disbursed, by hospital/health facility, between February 1 and April 14, 2020; Number of cases and total claims approved per hospital/health facility, no. of claims and total amount disbursed per patient and per benefit package under each circular.

3. Data relevant to the Balik-Probinsya Program: beneficiary names; origin and destination barangay, city/municipality, province; types and amounts of benefits received;

4. Data relevant to the National Food Authority's Palay Procurement Program: beneficiary names; barangay, municipality, province; volumes procured and total amounts paid; and

5. Data relevant to fiscal incentives granted: name and location of establishments receiving fiscal incentives, the type and amounts of

Furthermore, you seek clarification on the level of detail that can be released without violating the DPA. For Item Nos. 2-4 above, you inquired whether disaggregation by gender and the inclusion of age groups is allowable.

The Data Privacy Act of 2012, not a hindrance to transparency in government; right to information

The constitutional right to information and the right to privacy are not contradictory. Both are essential human rights that feature prominently in society and are necessary in a democracy. These rights are complementary, especially in ensuring government's accountability, and are forms of protection that constantly attempt to restore the balance between the citizen and the State.

The fundamental human right to privacy is protected by the 1987 Constitution as well as the DPA. This is the right of an individual to control the collection of, access to, and use of personal information about him or her that are under the control or custody of the personal information controllers, be it the government or the private sector.

Likewise, the right to information on matters of public concern is a constitutional right afforded to every citizen.³ This constitutional guarantee is a recognition of the importance of the free flow of ideas and information in a democracy; it enables citizens to cope with the exigencies of the times.⁴ The government must provide the public sufficient access to information that is of public concern, and it is not exempted by law from the operation of the constitutional guarantee to information.

While a freedom of information (FOI) law has yet to be enacted, the right to information is operationalized in the Executive Branch through Executive Order (EO) No. 2, 2016.⁵

Protection of personal information as an exception to FOI; DPA special cases; criteria for lawful processing under Section 12

Pursuant to the Inventory of Exceptions to EO No. 2 (S. 2016),⁶ information deemed confidential for the protection of the privacy of persons is an exception to the general rule of disclosure in the right of access to information.⁷

³ PHIL. CONST. art. 3 § 7.

⁴ Baldoza v. Dimaano, A.M. No. 1120-MJ (1976).

While a freedom of information (FOI) law has yet to be enacted, the right to information is operationalized in the Executive Branch through Executive Order (EO) No. 2, 2016.⁵

Protection of personal information as an exception to FOI; DPA special cases; criteria for lawful processing under Section 12

Pursuant to the Inventory of Exceptions to EO No. 2 (S. 2016),⁶ information deemed confidential for the protection of the privacy of persons is an exception to the general rule of disclosure in the right of access to information.⁷ Thus, informational privacy is recognized and the personal information of individuals are protected.

However, the DPA expressly provides under Section 4(c) thereof that information relating to any discretionary benefit of a financial nature given by the government to an individual, such as granting a license or permit, including the name of the individual and the exact nature of the benefit, is classified as a special case, where the provisions of the DPA and its Implementing Rules and Regulations (IRR) do not apply, subject to the qualification that such non-application of the law is only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned.⁸

Therefore, the DPA itself recognizes that the minimum extent of disclosure of personal information of those granted discretionary financial benefits by the government may be allowed.

For other benefits granted by the government which are given in the course of an ordinary transaction or as a matter of right, the minimum extent of disclosure of personal information of beneficiaries may still find basis under any of the various criteria for lawful processing under Section 12 of the DPA.

Public disclosure of pertinent data in relation to COVID-19 response programs; general data privacy principles; proportionality; release of statistical data

We now respond to the specific items mentioned above:

On Item no. 1 on the general data requests of private requesters for information related to government programs granting various forms of benefits, and the publication of such information in an open data machine-readable format in official government and civil society tracking websites, in keeping with the principles of transparency and accountability, government agencies in charge of implementing such programs may disclose or release to private requesters such information relating to the government program. Where such requests pertain to personal information of beneficiaries, as discussed above, the minimum extent of disclosure may be allowed.

Nonetheless, such disclosure should strictly adhere to the principle of proportionality, which requires 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 Hence, the disclosure or release should only be limited to those personal information which are necessary to the purpose. Data minimization should be employed in all cases of public disclosure. Further, pseudonymization of names or even the exclusion of the “name” field altogether may be considered before these lists are released to the public, if it is possible that the stated purpose can be achieved just the same.

We reiterate that releasing sensitive personal information may be excessive, no longer considered as necessary, and may constitute an unwarranted invasion of privacy.¹⁰

As to the manner of publication, the DPA nor the Commission does not require a specific form. While government agencies are encouraged to disclose these information in way that enhances the ability of the citizens to access such information, this is with the strong reminder that such disclosure is strictly for the purpose of promoting transparency and public participation. It should not be construed as a basis for unbridled processing that undermines the rights and freedoms of these beneficiaries, considering that they may be vulnerable data subjects.

On Item Nos. 2-4 on data relevant to benefits granted in line with the government's COVID-19 response and operations, i.e. for the DSWD, DOLE, DA, DOF-SSS, Balik Probinsya, NFA programs, etc., personal information relating to the beneficiaries' names, amounts received, and the pertinent barangay, city/municipality and province, may be disclosed but always taking into account the principles of transparency, legitimate purpose, and proportionality, as well as other applicable provisions of the DPA. Thus, if the purpose may be achieved by omitting personal information or through the use of pseudonymization, this may be considered.

On the release of information which are not personal information, such as:

- information of juridical persons (i.e., establishment/business names and addresses, amounts received, etc.);
- aggregate or statistical data relating to PhilHealth Advisory No. 2020-022, and Circular Nos. 2020-0009, 2020-0011, and 2020-0012 (i.e., number of recipients of full financial risk protection, total amount disbursed (by hospital/health facility) between February 1 and April 14, 2020, number of cases and total claims approved per hospital/health facility, and number of claims per benefit package under each circular); and
- disaggregated data on sex and age groups under Item Nos. 2-4 (i.e. statistics on the number of males and females and applicable age groups of those who availed of benefits),

the above do not involve personal information where an individual is identifiable, hence, these are outside the scope of the DPA. The release of such information may be governed by other laws or regulations.

Pseudonymization; health information

However, in relation to the Philhealth issuances and the request for the “total amount disbursed per patient,” we recommend that the information be de-identified or pseudonymized prior to release or disclosure.

Pseudonymization has been defined as “the processing of personal data in a manner that the

⁹ Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (c) (2016).

¹⁰See: National Privacy Commission, NPC Advisory Opinion No. 2020-019 (April 28, 2020).

personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.”¹¹

Actual patient names should not be released, considering that these may already be deemed as health information which is sensitive personal information, in relation to the fact that these patients who availed of Philhealth benefits or assistance are COVID-19 suspected, probable, or confirmed cases.

Personal information controllers; accountability in processing personal data

Finally, we remind government agencies, civil society organizations (CSO), and the private requesters that while personal information of beneficiaries may be disclosed to fulfill the requirements of transparency, accountability and good governance, the data privacy principle of proportionality dictates that only those information relevant, suitable, necessary, and not excessive may be processed. Further, these personal information shall only be used for the specified and legitimate purpose indicated.

Once such personal data are released to the CSOs and the private requesters, they automatically become personal information controllers, having obligations and responsibilities under the DPA, its IRR, and other issuances of the NPC.

These would include, but is not limited to, implementing reasonable, appropriate and adequate safeguards to protect personal data (i.e. having a data protection officer, providing privacy notices, conducting privacy impact assessments, having a privacy manual, managing personal data breaches, etc.), upholding data subject rights, and in general, being accountable for all personal data processing activities that they undertake.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

¹See: 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 [EU GENERAL DATA PROTECTION REGULATION], Article 4(5) (2016).

ADVISORY OPINION NO. 2020-027¹

2 July 2020



Re: ADMISSIBILITY OF PERSONAL DATA SHEET IN AN ADMINISTRATIVE INVESTIGATION

Dear 

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify matters relating to an official/faculty member's Personal Data Sheet (PDS) to be used as evidence in an administrative investigation vis-à-vis the provisions of the Data Privacy Act of 2012² (DPA) and NPC Advisory No. 2017-02.³

We understand that a complaint was filed with the Civil Service Commission (CSC) by the Head of Human Resource Management Office (HRMO) of your University against the Vice President of Academic and Student Affairs, for alleged misrepresentation of the contents of and false statement of material facts in the daily time record (DTR). Attached to the complaint was the PDS as evidence that respondent was attending various trainings and seminars contrary to his claims in his DTR that he was in the University's premises.

Given the forgoing, you sought resolution for the following matters:

- 1) Whether or not the PDS (which was obtained without observing the procedures and protocols prescribed in NPC Advisory No.

¹ Tags: Personal Data Sheet; NPC Advisory No. 2017-02; administrative investigation; admissibility; evidence

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 National Privacy Commission, Access to Personal Data Sheets of Government Personnel [NPC Advisory No. 2017-02] (3 April 2017).

2017-02 dated 3 April 2017) can be accepted as an admissible evidence to the administrative investigation to be conducted by the Appointing/Disciplining Authority; and

2) Whether or not the circumstances and issues surrounding the instant case are within or outside the coverage of NPC Advisory No. 2017-02 dated 3 April 2017.

Personal Data Sheet; access; NPC Advisory No. 2017-02 A PDS is an official document required of a government employee and official and is the repository of all information regarding his or her personal background, qualification, and eligibility.⁴ Because the PDS contains sensitive personal information, its processing, which includes disclosure, may find basis under Section 13 of the DPA, particularly Section 13(b), which recognizes the processing that is provided for by existing laws and regulations, and Section 13(f) when such personal information is provided to government or public authority.

While access to the PDS may be allowed, the same may still be regulated, taking into consideration a government official or employee's right to data privacy. Thus, in NPC Advisory No. 2017-02, the NPC laid down the guidelines in resolving requests for access to a PDS as follows:

1. The information requested falls under matters of public concern;
2. The individual requesting for personal data has declared and specified the purpose of his or her request;
3. The declared and specified purpose is not contrary to law, morals, and public policy; and
4. The personal data requested is necessary to the declared, specified, and legitimate purpose.

However, the above NPC Advisory contemplates the situation where the request for access is coming from a third party or the public.

In this case, the PDS is already under the custody of the Head of the HRMO of the University, presumably since the HRMO maintains these employee files as part of its core function and as required under the applicable CSC rules and regulations. Thus, the NPC Advisory is not squarely applicable to the case at hand.

⁴ *Advincula v. Dicen*, G.R. No.162403 (2005).

⁵ Civil Service Commission, 2017 Rules on Administrative Cases in the Civil Service (July 3, 2017).

⁶ *Id.* § 3.

Instead, what will be controlling in this scenario is the University's own internal policies and procedures on access to employee files in relation to the handling of administrative investigations, as well as any other pertinent CSC rules on the matter.

Admissibility of the PDS; administrative investigation; evidence

We note that in the 2017 Rules on Administrative Cases in the Civil Service⁵ (2017 RACCS) it is provided that “administrative investigations shall be conducted without strict recourse to technical rules of procedure and evidence applicable to judicial proceedings.”⁶

With this in mind, the determination of admissibility of documentary evidence such as the PDS, should be made by the University's Appointing/Disciplining Authority based on the University's internal rules and regulations governing administrative investigations and the 2017 RACCS of the CSC.

We reiterate our previous Advisory Opinion that the determination of the admissibility of evidence is not within the purview of NPC's mandate.⁷

This opinion is rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

⁷ National Privacy Commission, NPC Advisory Opinion No. 2019-023 (June 13, 2019).

ADVISORY OPINION NO. 2020-028¹

15 July 2020



Re: COLLECTION AND ENCODING OF INFORMATION ON COVID-19 RELATED DEATHS

Dear 

We write in response to your request for an advisory opinion seeking guidance on the propriety of complying with the series of memoranda and other communications issued by the Department of Interior and Local Government (DILG) requesting your office to do the following:

1. Encode the details of confirmed COVID-19 related deaths on <https://tinyurl.com/R4A-Death-Report>;
2. Upload the respective death certificates on <https://tinyurl.com/R4A-COVID19-DCert>; and
3. Provide the CALABARZON Disaster Risk Reduction Management (DRRM) Focal Persons – Management of Human Remains, through their Viber group, a daily update on the number of COVID-19 related deaths starting 27 June 2020.

Specifically, you ask whether accommodating the requests would result in possible violation/s of the provisions of the Data Privacy Act of 2012² (DPA) and its Implementing Rules and Regulations³ (IRR).

Death Certificate; sensitive personal information

A Death Certificate is an official document setting forth particulars relating to a deceased

¹ Tags: processing; sensitive personal information; COVID-19; public authority; mandate; statistics.

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).

person.⁴ It contains details such as (a) date and place of death, (b) full name, (c) age, (d) sex, (e) occupation or profession, (f) residence, (g) status as regards marriage, (h) nationality of the deceased, and (i) probable cause of death.⁵

Section 3 of the DPA specifically enumerates sensitive personal information, which includes information about an individual's marital status, age and health, among others. Thus, certain personal data found in the Death Certificate are sensitive personal information which must be processed in accordance with the DPA.⁶

Providing the DILG with electronic copies of death certificates; encoding details and uploading of the certificates; mandate

Under Section 13 of the DPA, processing of sensitive personal information is generally prohibited, unless it falls under any of the criteria for processing, specifically, when such processing is provided for by existing laws and regulations.⁷

In connection with this, we understand that there are several issuances of the DILG and the Department of Health (DOH) which deals with the handling of human remains and standard coding and reporting of deaths in relation to COVID-19:

1. DILG and DOH Joint Memorandum Circular No. 01 Series of 2020 (JMC)⁸ - Supplementary Guidelines on the Management of Human Remains for Patient Under Investigation (PUI) and Confirmed COVID-19 Cases;
2. DILG Memorandum Circular No. 2020-0639 - Interim Guidelines on the Management of Human Remains for Patient Under Investigation (PUI) and Confirmed COVID-19 Cases; and
3. DOH Department Circular No. 2020-0067-A10 - ICD-10 code for COVID-19.

⁴ See: Philippine Statistics Authority, Death Certificate, available at <https://psa.gov.ph/civilregistration/requesting-civil-registry-document/death-certificate> (last accessed July 16, 2020).

⁵ See: National Privacy Commission, NPC Advisory Opinion No. 2019-045 (Nov. 6, 2019) citing Law on Registry of Civil Status, Act No. 3753, § 6 (1930).

⁶ Id.

⁷ Data Privacy Act of 2012, § 13 (b).

⁸ Department of the Interior and Local Government and Department of Health, Supplementary Guidelines on the Management of Human Remains for Patient Under Investigation (PUI) and Confirmed COVID-19 Cases [Joint Memorandum Circular No. 01 Series of 2020] (April 16, 2020).

⁹ Department of the Interior and Local Government, Interim Guidelines on the Management of Human Remains for Patient Under Investigation (PUI) and Confirmed COVID-19 Cases [Memorandum Circular No. 2020-063] (March 27, 2020).

¹⁰ Department of Health, Amendment to Department Circular No. 2020-067 re ICD-10 code for COVID-19 (previously known as 2019-nCoV Acute Respiratory Disease).

¹¹ Data Privacy Act of 2012, § 13 (b).

¹² Id. § 13 (f).

In relation to these issuances, the DILG further issued an Advisory and Memoranda from the DILG REGION IV-A and Rizal Province, to cascade the guidelines to the regional and provincial levels and provide specifics of what is required.

With the foregoing considered, the requests made by the DILG for encoding the details surrounding the COVID-19 related deaths and uploading the corresponding death certificates on a secure site may fall under the criteria for lawful processing under Section 13 of the DPA; more specifically, processing that is provided for by existing laws and regulations¹¹ and when sensitive personal information is provided to the government or a public authority.¹² These issuances should be duly complied with. Compliance to the same is recognized under the DPA, its IRR, and issuances of the NPC. We reiterate that the DPA should be read together with other laws and regulations and should not be used as an excuse for non-compliance with the same.¹³

We trust also that the DILG, as a personal information controller (PIC), is well aware of its obligations, specifically NPC Circular No. 16-014 on the Security of Personal Data in Government Agencies, which requires all government agencies engaged in the processing of personal data to observe various duties and responsibilities for the protection of personal data, which includes the implementation of adequate and reasonable security measures to protect personal data against unauthorized access and disclosure.

In addition, we also note that the DILG, as a PIC, must adhere to the general data privacy principles, specifically in this case the principles of legitimate purpose and proportionality. The principle of legitimate purpose requires 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.¹⁵ On the other hand, the principle of proportionality requires that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose, and that personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.¹⁶

Updates on the number of COVID-19 related deaths; statistics

As to the requirement for providing daily updates on the number of COVID-19 related deaths, these only involve the disclosure of aggregate

data which are statistical in nature, and hence, the provisions and principles under the DPA may not necessarily apply.

Statistical information which does not include information from which the identity of an individual is apparent or can be reasonably and directly ascertained, is not personal information, and thus, not covered by the provisions of the DPA and its IRR.

This opinion is rendered based solely on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

¹³ See: National Privacy Commission, NPC Advisory Opinion No. 2018-035 (July 20, 2018).

¹⁴ NPC Circular No. 16-01 dated 10 October 2016, § 4.

¹⁵ Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (b).

¹⁶ Data Privacy Act of 2012, § 13 (c).

ADVISORY OPINION NO. 2020-029¹

20 July 2020

[REDACTED]

[REDACTED]

Re: REQUEST FOR PERSONAL INFORMATION OF COMPLAINANTS UNDER THE KATARUNGANG PAMBARANGAY PROCESS FOR THESIS PURPOSES

Dear [REDACTED]

We write in response to your letters requesting for an advisory opinion from the National Privacy Commission (NPC) on whether a particular barangay could provide certain information on the Katarungang Pambarangay² process to an individual as part of her data collection for her thesis without violating Republic Act (R.A.) No. 10173, or the Data Privacy Act of 2012³ (DPA).

We understand that an individual who is currently taking her master's degree is requesting for the following information:

1. Names of all the complainants in 2019;
2. Complainants' addresses;
3. Date of filing the complaint; and

¹ Tags: DILG, Katarungang Pambarangay, barangay, research, exemption, special cases, lawful processing, disclosure, thesis, dissertation, general data privacy principles, transparency, legitimate purpose, proportionality, data subject's rights, limitation on rights, ethical standards.

² An Act Providing for a Local Government Code of 1991 [Local Government Code of 1991], Republic Act No. 7160 (1991), Book III, Title I, Chapter VII.

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. Date when the decision was made.

We understand further that the barangay officials are hesitant to provide the information for fear of committing a violation of applicable laws.

Scope of the DPA; processing for research purposes; special case
The DPA applies to all types of processing of personal information and to any natural and juridical person involved in personal information processing, subject to certain qualifications.⁴ Under the law, the names of the complainants and their addresses are considered personal information, and its disclosure constitutes processing which should meet the requirements such as the criteria for lawful processing of personal information found under Section 12 thereof.

However, the law provides for special cases where the processing of certain personal information is excluded from its scope. These include personal information processed for journalistic, artistic, literary or research purposes.⁵ The Implementing Rules and Regulations (IRR) of the DPA states that personal information that will be processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards, is outside of the scope of the law.⁶

Nevertheless, this exemption is not absolute. This is interpreted to the effect that there is a presumption that personal information may be lawfully processed under such special cases.⁷ Specifically in this case, a researcher may lawfully process personal information even without meeting the conditions under Sections 12 or 13 of the DPA, but the processing shall be limited to that which is necessary to achieve the specific purpose, function, or activity, and the researcher, as a personal information controller, is still required to implement measures to secure and protect personal information.⁸

Stated simply, researchers are still obliged to implement reasonable and appropriate security measures for the protection of personal information, uphold the data subject rights, and adhere to the data privacy principles and other provisions of the DPA.

⁴ Id. § 4.

⁵ Data Privacy Act of 2012, § 4 (d).

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

⁷ See: National Privacy Commission, NPC Advisory Opinions No. 2017-035 (July 27, 2017), 2018-054 (Dec. 4, 2018), 2019-017 (March 5, 2019), and 2020-004 (Feb. 3, 2020).

⁸ Id.

9 National Privacy Commission, NPC Advisory Opinion No. 2019-017 (March 5, 2019).

Nature of research; obligations of researchers

In determining whether the release of the abovementioned personal information may be allowed under the DPA, it is necessary to understand the nature of research which is contemplated by the DPA and its IRR.

As stated in NPC Advisory Opinion No. 2019-0179 which discussed the implications of the DPA to the conduct of academic research vis-à-vis access to documents and records in the custody of government, “research is an activity that aims to develop or contribute to knowledge that can be generalized (including theories, principles, relationships), or any accumulation of information using scientific methods, observation, inference, and analysis.”¹⁰ This includes data gathering for thesis or dissertations.

We reiterate the discussion on the aforesaid Advisory Opinion, to wit:

“...apart from the laws and regulations on privacy, any code of ethics or any rules and regulations on research issued and implemented by institutions involved in research must be complied with by the researchers. After all, personal information used for research remains to be subject to a range of policies, including internal ones maintained by organizations, and other laws, as enacted or issued by the appropriate legislating authority.

xxx xxx xxx

...researchers should always keep in mind that though the DPA recognizes that the processing of personal data is critical to quality research, the rights and freedoms of individuals is likewise of utmost importance. This view is consistent with Section 38 of the DPA, which calls for an interpretation of the law that is mindful of the rights and interests of data subjects.”¹¹

Moreover, the DPA “recognizes that research is critical to nation-building and serves the interest of the public.”¹² It bears stressing that the DPA offers flexibility on processing for research purposes as long as it is in consistent with ethical and legal standards, meaning that there may be instances when the consent requirements may be waived if such waiver is consistent with legal and ethical principles.¹³ Likewise, the rights of data subjects may also be limited where such limitation is necessary to maintain research integrity.¹⁴

Data subject’s rights; limitation on rights

We note, however, that Section 19 of the DPA provides for the non-applicability of the rights of data subjects where the processing of personal information is only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject. At the same time, the personal information shall be held under strict confidentiality and shall be used only for the declared purpose.

Nonetheless, we reiterate that any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research.¹⁵

General data privacy principles; proportionality; evaluation of request

While personal information processed for research purposes is a special case, PICs are still obliged to adhere to the data privacy principles of transparency, legitimate purpose, and proportionality. Specifically for this request, the principle of proportionality requires that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.¹⁶ Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.¹⁷

Considering the foregoing, the request should be evaluated carefully in terms of whether the specific information requested is indispensable in achieving the research purpose.

¹⁰ Philippine Health Research Ethics Board Ad Hoc Committee for Updating the National Ethical Guidelines, National Ethical Guidelines for Health and Health Related Research, Introduction, p. 5 (2017).

¹¹ Ibid.

¹² National Privacy Commission, NPC Advisory Opinion No. 2019-017 (March 5, 2019).

¹³ National Privacy Commission, NPC Advisory Opinion No. 2018-054 (Dec. 4, 2018).

¹⁴ Id.

¹⁵ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 37 (2016).

In relation to such evaluation, the barangay officials, or even the Lupong Tagapamayapa (Lupon), created for the implementation of the Katarungang Pambarangay, pursuant to Section 399, Chapter VII of the Local Government Code of 1991, has the obligation to examine the particular request, keeping in mind their functions under the governing law, applicable rules and regulations, and data privacy principles enunciated in the DPA.

These barangay officials are not precluded from seeking further clarification from the researcher as to the details of her thesis, such as the exact purpose for collecting the names of the complainants and their addresses in relation to the study, whether such personal information is indispensable to the purpose, if statistics or aggregated data will suffice, whether redacting the personal information in the documents to be provided may be acceptable, among other considerations.

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

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

¹⁶ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §18 (c) (2016).

¹⁷ Ibid.

ADVISORY OPINION NO. 2020-030¹

5 August 2020



Re: REPORTING TO THE DEPARTMENT OF THE INTERIOR AND LOCAL GOVERNMENT OF COVID-19 RELATED HOSPITAL DEATHS

Dear 

We write in response to your request for an advisory opinion seeking guidance on the requirement of the Department of Interior and Local Government – VII (DILG-VII) in a Memorandum dated 3 July 2020 and the corresponding Memorandum from the Provincial Director of the DILG Cebu Province, requiring hospitals to submit a daily report of COVID-19 related deaths.

We understand from your email that the report requested will contain the following:

- a. Registry number;
- b. Patient's complete name;
- c. Sex;
- d. Date of death;
- e. Cause of death;
- f. Classification (Suspect/Probable/Confirmed COVID-19 case);
- g. Address;
- h. Local government unit (LGU) involved; and
- i. Whether the cadaver has been released or not.

Processing of sensitive personal information; public authority; mandate; proportionality

¹ Tags: sensitive personal information; COVID-19; DILG; public authority; reportorial requirement

Under the Data Privacy Act of 2012 (DPA), personal information about an individual's health is considered as sensitive personal information (SPI), the processing of which is generally prohibited, unless it falls under any of the criteria for processing pursuant to Section 13. Specifically applicable in this scenario is when such processing 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,³ and when information is to be provided to government pursuant to a constitutional or statutory mandate.⁴

We understand that Section 9.2 of Joint Memorandum Circular No. 01 (JMC)5, issued by the DILG and the Department of Health, in relation to the DILG MC No. 2020-063, provides that “the hospital, through a designated point person, shall immediately inform the nearest kin of the deceased and/or the Local MDM Cluster Focal Person of the city/municipality of residence once a suspect, probable (PUI), or confirmed COVID-19 patient dies...”

In view of the foregoing and all the related DILG issuances, compliance with the reportorial requirement may be warranted under the law.

Nonetheless, it is worthy to note that the processing of SPI, even if allowed under specific circumstances under the DPA, must always adhere to the general data privacy principles, specifically in this case the principles of legitimate purpose and proportionality. The principle of legitimate purpose requires 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. As mentioned above, the legitimate purpose for the intended processing is provided for under the DILG issuances which were made in response to the current public health emergency.⁶ On the other hand, the principle of proportionality requires that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.⁷

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 Id. § 13 (b).

⁴ Id. § 13 (f) and Rules and Regulations Implementing the Data Privacy Act of 2012, § 22 (f).

⁵ Supplementary Guidelines on the Management of Human Remains for Patient Under Investigation (PUI) and Confirmed COVID-19 Cases (DILG Memorandum Circular No. 2020-063).

⁶ Rules and Regulations Implementing the Data Privacy Act of 2012, § 17 (b).

⁷ Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (c).

We note that the purpose of DILG requirement is to ensure that COVID-19 related hospital deaths within the region are reported in a timely manner. We advise that the reports should contain only the information requested and that reasonable and appropriate safeguards should be implemented to protect all personal data collected against any unauthorized access, disclosure, or processing, given that Section 4.4 of DILG MC No. 2020-063 is clear in stating that the identity and other personal details of the deceased shall be respected at all times and remain confidential, unless otherwise provided by law.

We likewise emphasize Section 22 of the DPA which requires that all sensitive personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the Commission.

This opinion is rendered based solely on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

ADVISORY OPINION NO. 2020-031¹

6 August 2020



Re: ACCESS TO FILES AND RECORDS OF ANTI-ILLEGAL DRUGS OPERATIONS OF THE PHILIPPINE DRUG ENFORCEMENT AGENCY

Dear 

We write in response to your letter which sought the opinion of the National Privacy Commission (NPC) on whether the request for access by the Inter-Agency Review Panel, and the Department of Justice (DOJ) Panel of Prosecutors as stated in your letter, to files and records involving negation operations of the Philippine Drug Enforcement Agency (PDEA) is allowed under the Data Privacy Act of 2012 (DPA).

DOJ; Inter-Agency Review Panel; public authority

The DOJ derives its mandate primarily from the Executive Order No. 292.3 Under EO 292, the DOJ is the government's principal law agency, and serves as the government's prosecution arm and administers the government's criminal justice system by investigating crimes, prosecuting offenders, and overseeing the correctional system.⁴

¹Tags: lawful processing of personal data; special cases; public authority; mandate.

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 Instituting the Administrative Code of 1987 [Administrative Code of 1987], Executive Order No. 292, BOOK IV, Title III, Chapter 1-General Provisions (1987).

⁴ Department of Justice, About, available at <https://www.doj.gov.ph/vision-mission-and-mandate.html> (last accessed 6 August 2020).

⁵ 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 [The Comprehensive Dangerous Drugs Act of 2002] Republic Act No. 9165 (2002).

In particular, Section 90 of Republic Act No. 9165 as amended, otherwise known as the Comprehensive Dangerous Drugs Act of 20025 (CDDA) provides that:

Section 90. Jurisdiction. – The Supreme Court shall designate special courts from among the existing Regional Trial Courts in each judicial region to exclusively try and hear cases involving violations of this Act. The number of courts designated in each judicial region shall be based on the population and the number of cases pending in their respective jurisdiction.

xxx xxx xxx

The DOJ shall designate special prosecutors to exclusively handle cases involving violations of this Act. (underscoring supplied).

From the above, the DOJ is a public authority mandated by the law to investigate the commission of crimes such as, among others, violations of the CDDA and to prosecute offenders through the National Bureau of Investigation and the National Prosecution Service, respectively.

As to the Inter-Agency Review Panel (Panel), we understand that the same was *“formed to evaluate the over 5,000 operations of law enforcers against illegal drugs which resulted in the death of suspects involved in the drug trade.”*⁶

We understand further that the Panel is chaired by the Secretary of Justice, and composed of representatives from the Department of the Interior and Local Government (DILG), Presidential Human Rights Committee Secretariat (PHRCS), Presidential Management Staff (PMS), DOJ-National Prosecution Service (NPS), Department of Foreign Affairs (DFA), Presidential Communications Office (PCOO), PDEA, Dangerous Drugs Board (DDB), Philippine National Police (PNP) and the National Bureau of Investigation (NBI).⁷

With this, such Panel composed of various government agencies, is likewise acting based on their respective mandates which includes the investigation and evaluation of anti-illegal drugs operations.

Scope of the DPA; criteria for lawful processing of personal and sensitive personal information; mandate; law; security measures

⁶ Department of Justice letter addressed to the PDEA dated 17 July 2020, attached to the PDEA letter request.

⁷ Id.

Section 4 of the DPA states that the law is applicable to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.

The processing of personal and sensitive personal information (collectively, personal data) by the DOJ and the Panel finds support in the DPA, specifically Sections 12 and 13 thereof providing the criteria for lawful processing, 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

(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 xxx xxx

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

(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

(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.(underscoring supplied)

We are mindful of the mandates of the DOJ and the Panel and the necessity of examining the pertinent files and records of the PDEA in order to “determine whether administrative and/or criminal complaints should be filed/re-filed against law enforcement agents arising from their operations and, if warranted, recommend changes in the protocols in law enforcement operations against illegal drugs.”⁸

We reiterate that the DPA is not an obstacle to the collection and processing of personal data by the various government agencies as long as the same is necessary for the fulfillment of their respective mandates.⁹ This is with the concomitant responsibility of complying with the requirements of the DPA, its Implementing Rules and Regulations, and other issuances of the NPC.¹⁰

Finally, any personal data processing should always adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. Government agencies, as personal information controllers, must implement reasonable and appropriate safeguards to secure and protect personal data, considering the provisions of NPC Circular No.16-01 on the Security of Personal Data in Government Agencies.

This opinion is rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

⁸ Department of Justice letter addressed to the PDEA dated 17 July 2020, attached to the PDEA letter request.

⁹ See: National Privacy Commission, NPC Advisory Opinion No. 2019-040 (Oct. 17, 2019), citing National Privacy Commission, NPC Advisory Opinion No. 2018-083 (Nov. 26, 2018).

¹⁰ Id.



CIRCULAR



Republic of the Philippines
Department of Health
OFFICE OF THE SECRETARY

7 April 2020

JOINT MEMORANDUM CIRCULAR
2020-001

MEMORANDUM CIRCULAR

No. 2020- 0016

TO: ALL UNDERSECRETARIES, ASSISTANT SECRETARIES, DIRECTORS OF BUREAUS, REGIONAL OFFICES AND SERVICES; EXECUTIVE DIRECTORS OF SPECIALTY HOSPITALS, AND NATIONAL NUTRITION COUNCIL; CHIEFS OF MEDICAL CENTERS, HOSPITALS, SANITARIA AND INSTITUTES; PRESIDENT OF THE. PHILIPPINE HEALTH INSURANCE CORPORATION; DIRECTORS OF PHILIPPINE NATIONAL AIDS COUNCIL AND TREATMENT AND REHABILITATION CENTERS; AND OTHERS CONCERNED

SUBJECT: Department of Health - National Privacy Commission (DOHNPC) Joint Memorandum Circular No. 2020-0001 entitled “Guidelines on the Use of Telemedicine in COVID-19 Response”

Attached for your information and guidance is a copy of the DOH-NPC Joint Memorandum Circular No. 2020-0001 entitled “(Guidelines on the Use of Telemedicine in COVID-19 Response dated March 28, 2020.

Dissemination of the information to all concerned is requested.

By Authority of the Secretary of Health:

A handwritten signature in black ink, appearing to be "Lilibeth C. David", is written over the printed name.

LILIBETH C. DAVID, MD, MPH, MPM, CESO III

Undersecretary of Health

Health Facilities and Infrastructure Development Team

I. SCOPE AND COVERAGE

This Joint Memorandum Circular shall apply to all patients vulnerable to the COVID-19 health situation; all public and private, national and local healthcare providers regulated by DOH and Philippine Health Insurance Corporation (PhilHealth); and telemedicine providers.

IV. DEFINITION OF TERMS

For the purpose of this Joint Memorandum Circular, the following terms are defined:

- 1. Electronic Medical Record (EMR)** refers to a computerized medical record used to capture, store, and share information of a patient between healthcare providers in an institution or organization;
- 2. Electronic Prescription (ePrescription)** refers to either (a) *“optical electronic data (captured image in pdf, jpeg, or other photo file format) issued by or made by a licensed physician which is generated, sent, received or stored through email and messaging applications”* as defined under the Food and Drug Administration (FDA) Circular 2020-007 on Guidelines in the Implementation of the Use of Electronic Means of Prescription for Drugs for the Benefit of Individuals Vulnerable to COVID-19, or (b) a complete medical prescription with date, generic name and strength and dosage form and total amount of each prescribed drug, and directions issued by a physician to a patient, sent from a mobile number under the possession and control of the physician or his/her hospital or clinic as shall be authenticated by the local pharmacy
- 3. Healthcare Providers** refer to any of the following:
 - a. **Physician** refers to all individuals authorized by law to practice medicine pursuant to Republic Act No. 2382, or the “Medical Act of 1959,” as amended;
 - b. **Health facility** refers to a public or private facility or institution devoted primarily to the provision of services for health promotion, prevention, diagnosis, treatment, rehabilitation and palliation of individuals suffering from illness, disease, injury, disability, or deformity, or in need of medical and nursing care;
- 4. Processing** refers to any operation or any set of operations performed upon patient’s data including, but not limited to, the collection, recording, organization, storage, updating or modification, extraction, retrieval, consultation, use, consolidation, blocking, submission, erasure or destruction of data; and
- 5. Telemedicine** refers to the practice of medicine by means of electronic and telecommunications technologies such as phone call, chat or short messaging service (SMS), audio- and video-conferencing to deliver healthcare at a distance between a patient at an originating site, and a physician at a distant site.



Republic of the Philippines
DEPARTMENT OF HEALTH
NATIONAL PRIVACY COMMISSION OFFICE

28 March 2020

JOINT MEMORANDUM CIRCULAR

No. 2020- 001

I. BACKGROUND

Due to the alarming coronavirus disease (COVID-19) health situation in the country and pursuant to Republic Act No. 11332, the President issued Proclamation No. 922, s. 2020 declaring a State of Public Health Emergency throughout the Philippines, and consequently, Proclamation No. 929 s. 2020 placing the entire Luzon under enhanced community quarantine.

The serious threat to health, safety, security, and lives of the Filipinos, the long-term adverse effects on their means of livelihood, and the severe disruption of economic activities arising from this health situation prompted further issuance of Republic Act No. 11469 that placed the entire country in a state of national emergency.

II. OBJECTIVES

The overall aim of this Joint Memorandum Circular is to enable patients to receive health services even while staying at home except for serious conditions, emergencies, or to avail of COVID-19-related health services as per standing protocols.

Specific objectives are:

1. Alleviate surge and minimize risks posed by unnecessary patient traffic in health facilities;
2. Support implementation of community quarantine by providing access to primary care providers through the use of telemedicine, or medical consultation services being provided through online and/or mobile platforms; and
3. Ensure efficient, safe and secure use of telemedicine by healthcare providers.

V. DECLARATION OF PRINCIPLES

The following principles govern the implementation of this Joint Memorandum Circular:

1. Telemedicine services shall follow the standards of practice of medicine as defined under Republic Act No. 2382, its Implementing Rules and Regulations, and other applicable policies and guidelines, taking into account the absence of physical contact. While telemedicine is encouraged, the gold standard for clinical care remains to be face-to-face consultation.
2. The patient-physician relationship shall be based on full knowledge of the patient's medical history and a physical examination given the circumstances of a lack of physical contact (i.e., by inspection only). Telemedicine shall be employed when a licensed physician is physically inaccessible (e.g. such as during a national emergency with community quarantine in effect, among others), in the management of chronic health conditions, or follow-up check-ups after initial treatment.
3. The patient-physician relationship shall be founded on mutual trust and respect in which they both identify themselves reliably during a telemedicine consultation. In case the patient is referred to a health facility, the physician who initially sees the patient shall be responsible for the coordination of care.
4. Emergency and serious conditions, where face-to-face assessment and physical contact are most essential, should not be managed via telemedicine.
5. The use/implementation of telemedicine shall respect the universal principles of ethics, legal standards, and guiding principles on primacy of human rights and protection of health privacy as defined by Philippine laws, international instruments, rules, and other applicable policies.
 - a. All healthcare providers and telemedicine partners shall implement the minimum organizational, physical and technical security standards and measures as set by the National Privacy Commission (NPC) and the Department of Information and Communications Technology (DICT).
 - b. Proper informed consent must be established with all the necessary information regarding the features of the telemedicine visit fully discussed with the patient, including, but not limited to:
 - i. How telemedicine works;
 - ii. How referral is to be done;
 - iii. Privacy concerns;
 - iv. Risk of technology failure including confidentiality breach; and
 - v. Policy on care coordination.

VI. GUIDELINES

A. Healthcare Providers

1. 1. All healthcare providers shall help unburden local health systems and health facilities by engaging in telemedicine practices with a DOH telemedicine partner to provide essential primary care consultations, both for COVID-19 and non-COVID-19 healthrelated concerns.
2. 2. All healthcare providers are encouraged to subscribe to a DOH telemedicine partner which can augmenta health facility's medical services like health promotion services, triaging for both COVID-19 and non-COVID-19 health-related consultations, medical advice, referral to a doctor for home visit as necessary, and others. Medical consultations that require physical contact shall be handled by the local health office upon referral from a telemedicine consultation.
3. 3. All healthcare providers shall be given fifteen (15) days to engage with a DOH telemedicine partner from the date of effectivity of this Joint Memorandum Circular. Additional cost for setting up shall be charged using their own administrative funds.
4. All healthcare providers are authorized, in the interim, to issue documents like electronic clinical abstract, consultation summary, and/orreferral form (if applicable) to the patient. These documents must be suitable for optical character recognition (OCR) by being typewritten. The documents shall be issued via email or acceptable modes under Republic Act 8792, or the "Electronic Commerce Act of 2020." All clinical abstract/consultation summaries shall have the following content:
 - a. Patient Information (Name, Age, Birthdate, Sex, Address)
 - b. Brief Clinical History and Physical Examination (i.e., notes from inspection by video camera, if applicable)
 - c. Travel and Exposure History (for COVID-19 screening)
 - d. Diagnosis/Assessment
 - e. Plan of Management
5. All healthcare providers shall recognize and deem equivalent the electronic clinical abstract, consultation summary, prescription, and referral form issued by the physician for all intents and purposes.
6. All physicians whose services are sought through telemedicine shall keep records of all electronic clinical abstracts/consultation summaries, prescriptions and/or referral forms issued pursuant to this Joint Memorandum Circular in coordination with the DOH telemedicine partner
7. All licensed physicians shall issue electronic prescriptions in accordance with FDA
8. Circular No. 2020-007 and any subsequent FDA guidelines. All healthcare providers shall, at all times, ensure that patient confidentiality, privacy, and data integrity are not compromised.

B. Telemedicine Partners

Telemedicine Partners shall:

1. Provide an information or application system that can securely store and/

- or process patients' data according to established rules and regulations on confidentiality, privacy, and data integrity.
2. Comply with the requirements of the DOH to be able to link and/or interoperate with electronic medical record (EMR) systems or applicable health systems.
 3. Secure clearance from the DOH on all policy decisions affecting processing as regards to COVID-19-specific triaging algorithm, and the data collected in a telemedicine consultation.
 4. Allow physicians to sign up, and in the interim, volunteer their services with safety and security assurances for them to operate.
 5. Define or establish mechanisms to refer patients to appropriate health care providers in coordination with the Local Government Unit (LGU) in a network set-up, and following DOH and PhilHealth policies.
 6. Forge a memorandum of agreement with an LGU for the deployment of health professionals for home visit from a primary care facility, should it be deemed necessary.
 7. Receive calls escalated from the DOH COVID-19 hotlines as follows: 02-894-COVID (02-894-26843) and 1555, and any other iteration henceforth.
 8. In coordination with the LGU, report a suspected COVID-19 patient identified during the consult to the respective Regional or City Epidemiology and Surveillance Unit (RESU/CESU).
 9. Submit reports to DOH as shall be defined to monitor performance of this Joint Memorandum Circular.
 10. Provide these services free of charge until the enhanced community quarantine is lifted.

C. Monitoring and Evaluation Framework

1. The DOH and NPC shall regularly undertake monitoring and evaluation activities to assess the quality of implementation, including adequacy of control mechanisms to ensure confidence and acceptance of telemedicine services by healthcare providers, patients, and those in authority.
2. Dimensions for monitoring and evaluation shall be as follows:
 - a. Outcome measures (safety, effectiveness, efficiency, and quality of care)
 - b. Performance measures (access, functionality, quality and cost of service)
 - c. Summary measures (cost comparison)
 - d. Operational measures (access, acceptability, provider satisfaction, patient satisfaction, data privacy and cybersecurity)

VII. REPEALING CLAUSE


All previous issuances that are inconsistent with any provisions of this Joint Memorandum Circular are hereby amended, modified, or repealed accordingly.

VIII. SEPARABILITY CLAUSE

In the event that any provision or part of this Joint Memorandum Circular is declared unauthorized or rendered invalid by any court of law, those provisions not affected by such declaration shall remain valid and in effect.

IX. EFFECTIVITY

This Joint Memorandum Circular shall take effect immediately for the duration of the declared Enhanced Community Quarantine for the management of COVID-19 health situation, and the effectivity of this Order shall likewise be automatically lifted once the imposed quarantine is lifted.



FRANCISCO T. DUQUE III, MD, MSc
Secretary
Department of Health



RAYMUND E. LIBORO
Privacy Commissioner and Chairman
National Privacy Commission



Republic of the Philippines
DEPARTMENT OF HEALTH
NATIONAL PRIVACY COMMISSION OFFICE

24 April 2020

JOINT MEMORANDUM CIRCULAR

No. 2020- 0002

SUBJECT: Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response

I. BACKGROUND

In pursuit of disease surveillance and response against the coronavirus disease 2019 (COVID-19) in the country, and pursuant to Republic Act (RA) 11332 (Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act), the Department of Health (DOH), being the principal health agency in the country, collects, processes and disseminates COVID-19-related data; requires the reporting of such data from appropriate sources; and undertakes apropos epidemiologic investigations and biomedical researches.

The collection and processing of COVID-19-related data consists of both personal and sensitive personal information. The confidential nature of these data only underscores the primacy of right of the patient to health privacy. This right is articulated in RA 10173 (Data Privacy Act of 2012 [DPA]), which specifically provides for health privacy, establishes the directive for data protection, and reinforces the right of the patient to data privacy.

In response to the growing privacy concerns raised by various stakeholders during this current COVID-19 health situation, and in upholding RA 11332 and RA 10173, the Department of Health and the National Privacy Commission (NPC) hereby issue these guidelines on the application of data protection and privacy principles in the collection, processing and disclosure of COVID-19-related data in pursuit of disease surveillance and response.

II. OBJECTIVE

This Joint Memorandum Circular implements the guidelines for the collection, processing and disclosure of COVID-19-related data in pursuit of disease surveillance and response, while protecting the data privacy rights of patients and individuals and ensuring the confidentiality, integrity, and availability of their personal data.

III. SCOPE AND COVERAGE

This Joint Memorandum Circular shall apply to the implementation of the COVID-19 disease surveillance and response; and shall cover all public and private, national and local healthcare providers regulated by DOH and Philippine Health Insurance Corporation (PhilHealth); national and local public health authorities; DOH partner agencies involved in the collection and processing of COVID-19-related data; all COVID-19 cases; and all individuals identified as close contacts.

IV. DEFINITION OF TERMS

For the purpose of this Joint Memorandum Circular, the following terms are defined:

1. **Anonymization** is 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. (ISO/IEC 29100:2011)
2. **Case** refers to an individual who is either a COVID-19 suspect, probable, or confirmed patient.
3. **Close contact** — a person who may have come into contact with the probable or confirmed case two days prior to onset of illness of the confirmed COVID-19 case (use date of sample collection for asymptomatic cases as basis) until the time that said cases test negative on laboratory confirmation or other approved laboratory test through:
 - a. Face-to-face contact with a probable or confirmed case within 1 meter and for more than 15 minutes;
 - b. Direct physical contact with a probable or confirmed case;
 - c. Direct care for a patient with probable or confirmed COVID-19 disease without using proper personal protective equipment; OR
 - d. Other situations as indicated by local risk assessments.
4. **COVID-19-related data** refers to all types of information related to COVID-19 disease surveillance and response, including personal health information of COVID-19 cases and identified close contacts.
5. **Data Protection Officer (DPO)** is an individual who is accountable for ensuring compliance with applicable laws and regulations relating to data privacy and security. (DPA)

- 6. Data Sharing** is the disclosure or transfer to another government agency of personal data and/or information under the control or custody of a Personal Information Controller (PIC); Provided, that a PIC may be allowed to make such disclosure or transfer if it is upon the instructions of the PIC concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor. (Implementing Rules and Regulations of the DPA)
- 7. Data Subject** refers to an individual whose personal information is processed. (DPA)
- 8. Healthcare Providers** refer to any of the following:
- a. Health care professional refers to doctor of medicine, nurse, midwife, dentist, or other skilled allied professional or practitioner duly licensed to practice in the Philippines; and
 - b. Health facility refers to a public or private facility or institution devoted primarily to the provision of services for health promotion, prevention, diagnosis, treatment, rehabilitation and palliation of individuals suffering from illness, disease, injury, disability, or deformity, or in need of medical and nursing care.
- 9. DOH partner agency** refers to a DOH-designated/deputized public health authority to collect and process COVID-19-related data for purposes specified under Section V.2. of this Guidelines.
- 10. Personal data** refers to all types of personal information such as follows:
- a. 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. (DPA)
 - b. Sensitive personal information** refers to personal information:
 - i. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
 - ii. 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;
 - iii. 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
 - iv. Specifically established by an executive order or an act of Congress to be kept classified. (DPA)
- 11. Personal health information** refers to the individual's past, present or future physical or mental health or condition, including demographic data, diagnosis and management, medication history, health financing record,

cost of services and any other information related to the individual's total well-being. (DOH-DOST-PhilHealth Joint Administrative Order No. 2016-0002)

- 12. Personal information controller or “PIC”** 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: a person or organization who performs such functions as instructed by another person or organization; or an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs. 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. (DPA)
- 13. Personal information processor or “PIP”** refers to any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject. (DPA)
- 14. Processing** refers to any operation or any set of operations performed upon patient's data including, but not limited to, the collection, recording, organization, storage, updating or modification, extraction, retrieval, consultation, use, consolidation, blocking, submission, disclosure, erasure or destruction of data. (DPA)
- 15. Pseudonymization** refers to replacing one attribute (typically a unique attribute) in a record by another. The natural person is therefore still likely to be identified indirectly; accordingly, pseudonymization when used alone will not result in an anonymous dataset. (Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques).
- 16. Public Health Authority** refers to the DOH, specifically the Epidemiology Bureau, Disease Prevention and Control Bureau, Bureau of Quarantine, Food and Drug Administration, Regional Offices of DOH, Regional Epidemiology and Surveillance Unit (RESU), local health offices (provincial, city, or municipality); or any person directly authorized to act on behalf of the DOH or the local health office. (DOH Administrative Order [AO] 2020-0013)

V. GENERAL GUIDELINES

1. The implementation of COVID-19 disease surveillance and response shall promote public health action to contain and/or prevent the spread of COVID-19 and help mitigate the effects and impact of the disease to the people and communities, while safeguarding the data privacy rights of every individual.
2. The processing of personal health information of COVID-19 cases and identified close contacts for disease surveillance and response shall be to the extent necessary for the following purposes:
 - a. To outline a true picture of the country's COVID-19 health situation in terms of status and extent of local and community transmission.

- b. To build a repository of real-time COVID-19-related data as basis of evidence informed health policy and intervention measures.
 - c. To support case investigation and management, contact tracing and monitoring, quarantine and isolation, mandatory reporting to national and local public health authorities, and other disease surveillance-related activities.
 - d. To improve response activities, including the quality and accessibility of health services and other related interventions for COVID-19.
 - e. To allow information sharing and exchange between and among healthcare providers, public health authorities and other government authorities for treatment and care coordination, and/or surveillance and response purposes.
- 3. The right to privacy of health information shall be protected at all times. The processing of personal health information of COVID-19 cases and identified close contacts shall be in accordance with RA 10173, its IRR and other relevant issuances from the NPC, and shall adhere to the principles of transparency, legitimate purpose, and proportionality:
 - a. Patients/close contacts (data subjects) shall have a right to adequate information on matters relating to the processing of their health information, including the nature, purpose, and intended use of processing.
 - b. Health information shall be processed fairly and lawfully.
 - c. The processing of health information shall involve only the minimum extent of personal data necessary to the declared and specified purpose at the time of collection.
- 4. All national and local public health authorities, concerned healthcare providers and DOH partner agencies involved in the collection and processing of COVID-19-related data shall put in place the minimum organizational, physical and technical security measures and standards for data protection as set by NPC and the Department of Information and Communications Technology (DICT), and shall uphold and protect the data privacy rights of every individual at all times.
- 5. This policy shall serve as the privacy notice of national and local public health authorities, and DOH partner agencies in the collection, processing, and disclosure of COVID-19-related data in pursuit of disease surveillance and response.

VI. SPECIFIC GUIDELINES

A. Implementation Governance

- 1. The Interagency Task Force for the Management of Emerging Infectious Diseases — Task Group on Strategic Communications, in coordination with the DOH — Epidemiology Bureau, the DOH Data Protection Officer and the National Privacy Commission, shall set policy directions and oversight on all matters relating to privacy and data protection of COVID-19-related data.
- 2. The National eHealth Program Management Office (NEHPMO) in KMITS

of the DOH shall act as the overall technical and administrative secretariat for all activities related to ensuring privacy and data protection of COVID-19-related data.

B. Processing of Health Information

1. The processing of personal health information of COVID-19 cases and identified close contacts shall be allowed in any of the following cases:
 - a. The processing of personal health information is done by national and local public health authorities, pursuant to its constitutional or statutory mandate as provided under RA 11332, Sections 4(e), 12 and 13 of RA 10173, and other applicable laws, rules, and regulations.
 - b. The processing of personal health information by a healthcare provider is allowed if necessary for the purposes of case investigation and management, contact tracing and monitoring, quarantine and isolation, mandatory reporting to public health authorities, or treatment and coordination purposes.
 - c. The processing of personal health information by DOH partner agencies and their authorized personnel shall be allowed, pursuant to a Data Sharing Agreement (DSA) as provided under NPC Circular 16-02 (Data Sharing Agreements Involving Government Agencies).
 - i. All personnel who will be authorized by the DOH partner agencies to collect and process personal health information shall sign a Non-Disclosure Agreement (NDA) beforehand to prevent any unauthorized processing.
 - d. Personal information are pseudonymized or anonymized.
2. In the processing of personal health information, the following must be observed:
 - a. In all cases where processing of personal health information is allowed, the patient/close contact (data subject) shall be informed of the nature and purpose for the collection and processing of his/her personal health information by public health authorities and the DOH partner agencies, which shall include the purposes specified under Section V.2.
 - b. The manner of processing of personal health information shall be in accordance with the guidelines set forth under DOH AO 2020-0013 (Revised AO 2020-0012 "Guidelines for the Inclusion of COVID 19 in the List of Notifiable Diseases for Mandatory Reporting to the DOH dated March 17, 2020), and the DOH DM 2020- 0189 (Updated Guidelines on Contact Tracing of Close Contacts of Confirmed COVID-19 Cases).
 - c. Personal health information of all COVID-19 cases and close contacts as identified by concerned healthcare providers, public health authorities and DOH partner agencies during the conduct of respective case investigation and contact tracing must be reported to the DOH and its designated/deputized public health authorities serving as partner agencies.

C. Access of Health Information

1. Only concerned healthcare providers, public health authorities, and DOH partner agencies and their authorized personnel shall be allowed to access the personal health information of the COVID-19 cases and/or identified close contacts, pursuant to the guidelines set forth under DOH AO 2020-0013, and the DOH DM 2020-0189.
2. All entities and individuals with access to the personal health information shall be bound by legal duty to protect the personal health information pursuant to this Guidelines.

D. Use and Disclosure of Health Information

1. The use of personal health information by national and local governments shall be limited to the purposes specified under Section V.2.
 - a. All concerned healthcare providers, public health authorities, and DOH partner agencies and their authorized personnel shall be responsible for limiting the use of personal health information stored within their location to the purpose specified at the time of collection.
 - b. Use for other purposes not indicated under Section V.2. shall be prohibited.
2. Disclosure of personal health information shall be limited to authorized entities, officers, personnel and concerned individuals only, pursuant to the purposes specified under Section V.2.
 - a. 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 prohibited.
 - b. Any disclosure by the national and local public health authorities to third parties shall be embodied in a DSA.
 - c. The DOH partner agencies must first secure the written consent of the DOH before they can disclose any personal health information to third parties, and the said disclosure shall likewise be embodied in a DSA.
3. The following information may be disclosed for a legitimate purpose:
 - a. Aggregate health information, or pseudonymized or anonymized detailed health information for public communication; and
 - b. Mandatory reporting requirements, including personal health information, to national and local public health authorities, and DOH partner agencies.

E. Use of Information and Communications Technologies (ICTs) for Collection and Processing of Health Information

1. All ICT solutions and technologies used for collection and processing of personal health information of COVID-19 cases and/or identified close contacts shall be registered to the NPC, and comply with the DOH COVID-19 surveillance and response protocols and data requirements.
2. All entities who are interested to develop and implement ICT solutions and technologies for COVID-19 surveillance and response should be

registered to the NPC, and follow the minimum ICT standards set by DICT and Knowledge Management and Information Technology Service (KMITS) of the DOH.

F. Business Intelligence and Health Research

1. Only aggregate health information or pseudonymized or anonymized detailed health information shall be shared by public health authorities to stakeholders for the purpose of business intelligence and policy and biomedical researches.
2. All policy and biomedical researches related to COVID-19 surveillance and response shall secure an Ethics Board approval prior to implementation.

VII. ROLES AND RESPONSIBILITIES

A. Data Subjects (COVID-19 Cases, Close Contacts, and Other Informants)

1. Owner of the data.
2. Disclose truthful and accurate information regarding their health condition and exposure to public health authorities and/or DOH partner agencies.

B. Department of Health

1. Provide policy directions and oversight, together with NPC, on all matters relating to privacy and data protection, and processing and disclosure of COVID-19-related data.
2. Evaluate, monitor and direct activities relating to processing and disclosure of COVID-19-related data in pursuit of surveillance and response as provided under RA 11332, its IRR, and other issuances from the DOH.
3. Observe and comply with RA 10173, its IRR, and other issuances from NPC in the processing and disclosure of COVID-19-related data as a personal information controller.

C. National Privacy Commission

1. Provide policy directions and oversight, together with DOH, on all matters relating to privacy and data protection, and processing and disclosure of COVID-19-related data.
2. Evaluate, monitor and direct activities relating to privacy and data protection of COVID-19-related data in pursuit of surveillance and response as provided under RA 10173, its IRR, and other issuances from NPC.

D. Healthcare Providers

1. Report to the DOH and its designated/deputized public health authorities personal health information of identified COVID-19 cases and/or close contacts.
2. Act as personal information controller.
3. Comply with the DOH COVID-19 surveillance and response protocols and standards, including guidelines on privacy and data protection, and processing and disclosure of COVID-19-related data.

E. Public Health Authorities

1. Act as personal information controller.
2. Comply with the DOH COVID-19 surveillance and response protocols and standards, including guidelines on privacy and data protection, and processing and disclosure of COVID-19-related data.

F. DOH Partner Agencies (including Local Government Units)

1. Report to the DOH personal health information of identified COVID-19 cases and/or close contacts.
2. Protect and preserve identities of COVID-19 cases and identified close contacts, and their families to the extent that this does not result in undue discrimination, or physical or emotional harm or distress.
3. Act as both personal information controller and processor.
4. Comply with the DOH COVID-19 surveillance and response protocols and standards, including guidelines on privacy and data protection, and processing and disclosure of COVID-19-related data.

VIII. PENALTY CLAUSE

1. Non-cooperation of any individual to disclose truthful and accurate information regarding their health condition and exposure to COVID-19 to public health authorities and/or DOH partner agencies, or of any individual or entity that should report and/or respond to COVID-19 surveillance and response, or any similar action insofar as they relate to the provisions of this Joint Memorandum Circular shall be penalized in accordance with RA 11332 (Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act), RA 11469 (Bayanihan to Heal as One Act), and other applicable laws, rules and regulations.
2. Any privacy violation, or personal data breach, or security incident shall be penalized in accordance with RA 10173 (Data Privacy Act of 2012), or other applicable laws, rules, and regulations. Exemptions for privacy violation include disclosures of personal health information that is publicly known or becomes publicly known for causes not due to any unauthorized act of any concerned implementer of these Guidelines, or public disclosure made by the data subject himself/herself.

IX. REPEALING CLAUSE


All previous issuances that are inconsistent with any provisions of this Joint Memorandum Circular are hereby amended, modified, or repealed accordingly.

X. SEPARABILITY CLAUSE


In the event that any provision or part of this Joint Memorandum Circular is declared unauthorized or rendered invalid by any court of law, those provisions not affected by such declaration shall remain valid and in effect.

XI. EFFECTIVITY

This Joint Memorandum Circular shall take effect immediately.



FRANCISCO T. DUQUE III, MD, MSc
Secretary
Department of Health



RAYMUND E. LIBORO
Privacy Commissioner and Chairman
National Privacy Commission



Republic of the Philippines
Department of Health
OFFICE OF THE SECRETARY

6 May 2020

MEMORANDUM CIRCULAR

No. 2020- 0024

TO: ALL UNDERSECRETARIES, ASSISTANT SECRETARIES, DIRECTORS OF BUREAUS, REGIONAL OFFICES AND SERVICES; EXECUTIVE DIRECTORS OF SPECIALTY HOSPITALS, AND NATIONAL NUTRITION COUNCIL; CHIEFS OF MEDICAL CENTERS, HOSPITALS, SANITARIA AND INSTITUTES; PRESIDENT OF THE. PHILIPPINE HEALTH INSURANCE CORPORATION; DIRECTORS OF PHILIPPINE NATIONAL AIDS COUNCIL AND TREATMENT AND REHABILITATION CENTERS; AND OTHERS CONCERNED

SUBJECT: Department of Health - National Privacy Commission (DOHNPC) Joint Memorandum Circular No. 2020-0003 entitled “Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response”

Attached for your information and guidance is a copy of the DOH-NPC Joint Memorandum Circular No. 2020-0003 dated April 14, 2020 entitled “Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine i COVID-19 Response

Dissemination of the information to all concerned is requested.

By Authority of the Secretary of Health:

A handwritten signature in black ink, appearing to be "Lilibeth C. David".

LILIBETH C. DAVID, MD, MPH, MPM, CESO III
Undersecretary of Health
Health Facilities and Infrastructure Development Team



Republic of the Philippines
DEPARTMENT OF HEALTH
NATIONAL PRIVACY COMMISSION OFFICE

28 March 2020

JOINT MEMORANDUM CIRCULAR

No. 2020- 003

SUBJECT: Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-29 Response

I. BACKGROUND

Due to the rise of COVID-19 cases in the country and pursuant to Republic Act No. 11332, the President issued Proclamation No. 922, s. 2020 declaring a State of Public Health Emergency throughout the Philippines, and consequently, Proclamation No. 929 s. 2020 placing the entire Luzon under enhanced community quarantine. Simultaneously, a number of local government units (LGUs) have implemented Community Quarantine in their respective jurisdiction.

In the implementation of the Enhanced Community Quarantine, one of the critical measures identified to curb the spread of COVID-19 is the suspension of public transportation. This, however, resulted in missed appointments, missed filling prescriptions, and poor disease management, particularly among individuals with chronic illnesses that require ongoing active care, even when care is readily available.

To help address this gap, under the Joint Memorandum Circular (JMC) # 2020-0001, the Department of Health (DOH) and the National Privacy Commission (NPC) have institutionalized the use of telemedicine as a supplemental and complementary method to enable patients to still receive health services even while staying at home except for serious conditions, emergencies, or to avail of COVID 19-related health services as per standing protocols.

II. OBJECTIVES

The objectives of this Joint Memorandum Circular are to provide actionable information for accountability and performance improvement for

telemedicine services, and create evidence for informed decision-making for the DOH and NPC at policy level on the possible long-term use of telemedicine for service delivery.

III. SCOPE AND COVERAGE

This Joint Memorandum Circular shall apply to the program implementation of the telemedicine services during the period of Enhanced Community Quarantine; and shall cover all public and private, national and local healthcare providers regulated by DOH and Philippine Health Insurance Corporation (PhilHealth) providing telemedicine services; DOH-engaged telemedicine partners; the Department of Health; and the National Privacy Commission.

IV. DEFINITION OF TERMS

For the purpose of this Joint Memorandum Circular, the following terms are defined:

1. **Evaluation** refers to an objective and systematic assessment of an ongoing completed program to determine its effectiveness, outcome, impact and sustainability.
2. **Healthcare Providers** refer to any of the following:
 - a. **Physician** refers to all individual authorized by law to practice medicine pursuant to Republic Act No. 2832 or the “Medical Act of 1959” as amended;
 - b. **Health facility** refers to a public or private facility or institution devoted primarily to the provision of services for health promotion, prevention, diagnosis, treatment, rehabilitation and palliation of individuals suffering from illness, disease, injury, disability, or deformity, or need of medical and nursing care;
3. **Monitoring** refers to regular and routine collection and analysis of information to track progress of implementation of telemedicine services. It is conducted to ensure that this interim initiative is being implemented in accordance with its intent and to make informed decisions for policy and strategic management.
4. **Processing** refers to any operations performed upon patient’s data including, but not limited to, the collection, recording, organization, storage, updating or modification, extraction, retrieval, consultation, use, consolidation, blocking, submission, ensuring or distraction of data; and
5. **Telemedicine** refers to the practice of medicine by means of electronic and telecommunication technologies such as phone call, chat or short messaging service (SMS), audio-and-video-conferencing, among others, to deliver healthcare at a distance between a patient at an originating site, and a physician at a distant site.
6. **Telemedicine partner** refers to a telemedicine company that has registered with the DOH telemedicine program in COVID-19 response

and met the requirements for engagement as set forth under JMC 2020-0001 and its offshoot policies.

V. DECLARATION OF PRINCIPLES

The following principles shall govern the implementation of this Joint Memorandum Circular:

1. **Results-based.** Program management of telemedicine services shall have defined and measurable results that indicate the success of implementation. This contributes to better performance and accountability. It shall focus on activities, outputs, and short-term outcomes.
2. **Effectiveness.** Evidence of effectiveness, equity and sustainability shall be the basis for long-term use/implementation.
3. **Alignment.** The results of the monitoring and evaluation shall be interpreted together with existing agency management tools such as the Performance Governance System, and other relevant monitoring and evaluation tools or solutions to ensure strategic alignment and performance improvement.

VI. GUIDELINES

A. Implementation Governance

1. The interagency National eHealth Technical Working Group (NEHTWG) shall set policy direction and program oversight for the implementation of telemedicine services across the country.
2. The NEHTWG shall organize the Sub-Committee in Telemedicine that will:
(a) review and monitor the progress of implementation of telemedicine services; (b) conduct the necessary consultations and coordination with concerned stakeholders; and (c) submit monthly assessment and accomplishment reports to the NEHTWG for performance monitoring evaluation.

The Sub-Committee on Telemedicine shall be composed of policy and technical experts on telemedicine from relevant agencies and organizations as defined by the NEHTWG.

3. The National eHealth Program Management (NEHPMO) in KMITS of the DOH shall act as the overall technical and administrative secretariat for all activities related to the program implementation of telemedicine services.

B. Situational Analysis, Goal-Setting and Planning

1. The Sub-Committee on Telemedicine shall prepare strategic and operational plans and endorse them to the NEHTWG for review and approval.
2. These plans shall include a monitoring and evaluation framework, Initial

dimensions for monitoring and evaluation shall be as follows:

- a. Outcome measures (safety, effectiveness, efficiency and quality of care);
 - b. Performance measures (access, functionality, quality and cost of service);
 - c. Summary measures (cost comparison); and
 - d. Operational measures (access, acceptability, provider satisfaction, patient satisfaction, data privacy and cybersecurity.)
4. A list of indicators and corresponding targets shall guide implementers to improve performance and results. (annex 1.0)

C. Monitoring

1. Healthcare Providers

- a. All healthcare providers who have registered with DOH telemedicine partner shall provide relevant information will enable the telemedicine partners to provide timely reports to DOH.
- b. Any other healthcare providers in telemedicine are encouraged to use secure non-public-facing platforms for the conduct of the teleconsultation while inputting consult data using the DOH data entry platform which can be accessed at telemmed.doh.gov.ph. Reports will be extracted by DOH from the platform.

Required documentation for submission to DOH shall be the signed performance commitment (Annex 2.0)

2. Telemedicine Partners

- a. All telemedicine partners shall submit (1) signed performance commitments; and (2) required documentations and reports to DOH through nationalhealthprogram@gmail.com in timely manner (Annex 3.0)
- b. Telemedicine partners can adopt their own monitoring tools and solutions apart from the DOH requirements.

3. NEHPMO

- a. The NEHPMO shall: (i) receive and consolidate all submitted documentation and reports from telemedicine providers and those submitted from the DOH data entry platform; and (ii) provide the Sub-Committee on Telemedicine a summary result of findings and recommendations.
- b. Feedback from the Sub-Committee on Telemedicine shall result appropriate and timely actions to address issues in program implementation.

4. Sub-Committee on Telemedicine

- a. The Sub-Committee shall provide guidance on monitoring and evaluation, and recommend relevant policies to the NEHTWG as necessary.
- b. Random audits to verify compliance with applicable DOH and NPC guidelines on implementation of telemedicine services shall be decided by the Sub-Committee.

D. Evaluation

1. A formative evaluation shall be conducted at an appropriate time.
2. The results of the formative evaluation shall be used to determine if the program is effective in attaining its goals and objectives for COVID-19 response, and consequently, at the policy level on the possible long-term use of the telemedicine for service delivery.

VII. REPEALING CLAUSE


All previous issuance that are inconsistent with any provisions of this Joint Memorandum Circular are hereby amended, modified, or repeated accordingly.

VIII. SEPARABILITY CLAUSE


In the event that any provisions or part of this Joint Memorandum Circular is declared unauthorized or rendered invalid by any court of law, those provisions not affected by such declaration shall remain and in effect.

IX. EFFECTIVITY

This Joint Memorandum Circular shall take effect immediately for the duration of the declared Enhanced Community Quarantine for the management of COVID-19 health situation, and the effectivity of this Order shall likewise be automatically lifted once the imposed quarantine is lifted.



FRANCISCO T. DUQUE III, MD, MSc
Secretary
Department of Health



RAYMUND E. LIBORO
Privacy Commissioner and Chairman
National Privacy Commission

Annex 1.0. Monitoring and Evaluation Indicators

Dimensions	Indicators for Monitoring	Source/Method	Frequency of Collection	Unit Responsible for Monitoring
Outcome & Summary Measures	<i>Output</i>			
	Average patient satisfaction rating of the telemedicine services provided by the healthcare provider	Submitted telemedicine reports	Monthly	NEHPMO, KMITS
Performance Measures	<i>Input</i>			
	# of physicians engaged as providers of telemedicine services	Submitted telemedicine reports	Weekly	NEHPMO, KMITS
	# of unique individual patients who sought health services through telemedicine per healthcare provider (disaggregation: individual health facility vs individual physician; daily vs weekly)	Submitted telemedicine reports	Weekly	NEHPMO, KMITS
	<i>Output</i>			
	# of telemedicine consultations received per healthcare provider (disaggregation: companion-assisted patient consultation vs non-companion-assisted/individual patient consultation; individual health facility vs individual physician; daily vs weekly)	Submitted telemedicine reports	Weekly	NEHPMO, KMITS
	Type of telemedicine consultations received per healthcare provider (disaggregation: COVID-19 vs non-COVID-19 health concerns; individual health facility vs individual physician; daily vs weekly)	Submitted telemedicine reports	Weekly	NEHPMO, KMITS
	Reasons for consultations (disaggregation: COVID-19 vs non-COVID-19 health concerns; individual health facility vs individual physician; daily vs weekly)	Submitted telemedicine reports	Weekly	NEHPMO, KMITS

	Clinical classification (disaggregation: COVID-19 vs non-COVID-19 health concerns; individual health facility vs individual physician)	Submitted telemedicine reports	Weekly	NEHPMO, KMITS
	Type of disposition per telemedicine consultation received (disaggregation: COVID-19 vs non-COVID-19 health concerns; individual health facility vs individual physician)	Submitted telemedicine reports	Weekly	NEHPMO, KMITS
Operational Measures	<i>Input</i>			
	# of telemedicine providers engaged by DOH	Signed performance commitment & MOA	Weekly	NEHPMO, KMITS
	# of LGUs with engaged telemedicine providers	Signed MOA	Weekly	NEHPMO, KMITS
	# of health facilities engaged per telemedicine provider	Signed performance commitment & MOA	Weekly	NEHPMO, KMITS
	Presence of a Data Protection Officer	Submitted telemedicine reports	One time/as updated	NEHPMO, KMITS
	Privacy policy for telemedicine providers	Telemedicine privacy policy	One time/as updated	NEHPMO, KMITS
	Privacy management program in place for telemedicine providers	Privacy management program implementation plan or privacy manual	One time/as updated	NEHPMO, KMITS
	<i>Activities</i>			
	Telemedicine program implementation plan in place for telemedicine providers	Telemedicine program implementation plan	One time/as updated	NEHPMO, KMITS
	<i>Output</i>			
	# of patient complaints received by healthcare providers	Submitted telemedicine reports	Weekly	NEHPMO, KMITS
	# of patient complaints closed by healthcare providers	Submitted telemedicine reports	Weekly	NEHPMO, KMITS
	Types of complaints (i.e. privacy and security breach, medical errors, cost for access, provider disengagement, etc.) - built in monitoring and feedback mechanism in the platform for customer service	Submitted telemedicine reports	Weekly	NEHPMO, KMITS
	# of security incidents and personal data breaches reported within NPC protocols (incident reporting mechanism)	Submitted telemedicine reports	Weekly	NEHPMO, KMITS

Annex 2.0. Performance Commitment for Healthcare Providers who are Unable to Register with a DOH Telemedicine Partner

(Date)

DEPARTMENT OF HEALTH

San Lazaro Compound, Rizal Avenue, Sta. Cruz, Manila

SUBJECT: Performance Commitment

Sir/Madam:

To guarantee our commitment to support the fight against COVID-19, I respectfully submit this Performance Commitment. And for the purposes of this Performance Commitment, I hereby warrant the following representations:

1. That I agree to be enrolled in a sandbox implementation program for the utilization of telemedicine in response to COVID-19. The overall goal is to use telemedicine as a medium to deliver health services to patients in a safe environment following established treatment algorithms and guidelines while utilizing current technology capabilities.
2. That I shall only use a secure platform for medical consultation and referral of patients to the nearest health facility, if necessary.
3. That I shall ensure that the privacy settings of the platform being used is compliant with the minimum legal and regulatory laws and frameworks in the Philippines.
4. That I shall not use public-facing platforms like Youtube or Facebook Live, and such other similar public-facing platforms, for telemedicine consultations.
5. That I shall first obtain the informed consent of the patient prior to the collection of any personal data and the offering of any telemedicine service.
6. That I shall uphold the data privacy rights of patients using the platform, and shall provide mechanisms for the effective exercise of these rights. Patients should be: (a) informed that the platform being used entails privacy risks and that a telehealth consultation may not be equivalent to a face-to-face consult; (b) allowed to discuss their privacy and other related concerns, if any; and (c) be given the option not to proceed with the consult.
7. That I shall ensure that reasonable and appropriate security measures are implemented to safeguard the patients' data collected, used, stored, or otherwise processed using the platform, against any accidental or unlawful destruction, alteration or disclosure as well as unlawful access, fraudulent misuse, or any other unauthorized processing.
 - 7.1. Patients should be informed that any personal data obtained in the course of the consult shall be used for medical treatment, kept confidential, and only those involved in patient's care shall have access.
 - 7.2. That I shall choose a place to conduct the telemedicine consultation beforehand, i.e. conducive to communicating with the patient, and where interruptions or potential unwarranted disclosures are avoided.
8. That I shall comply with all pertinent DOH COVID-19 and non-COVID-19 treatment algorithms and guidelines, including patient surveillance.

9. That I recognize that DOH and I shall be the controller of patients' data, which remains to be owned by the individual patients.

10. That I shall comply with the necessary protocols for data sharing, monitoring and evaluation activities.

11. That I shall render telemedicine services without cost either to the DOH or to the patients receiving the services.

12. That I shall be held liable for any security incident, or privacy violation, or personal data breaches, and other related issues and concerns arising from the conduct of telemedicine consultation, and which are attributable to me or my acts.

13. Nothing in this document shall be interpreted or construed as creating or establishing an Employer-Employee relationship between the DOH and the healthcare provider.

We commit to extending our full support in order to effectively and appropriately deliver primary care teleconsultations to those who are in need.

Very Truly Yours,

Name of Healthcare Provider

License Number

Contact Details (i.e. address, phone number & email)

Telemedicine platform being used

Reference: Patdu, Ivy D. (19 March 2020). Privacy should not be an obstacle to telemedicine. Newsbytes.PH. Retrieved from <http://newsbytes.ph/2020/03/patdu-privacy-should-not-be-an-obstacle-to-telemedicine/>.

Annex 3.0. Program Documentations and Reports for Submission by Telemedicine Partners

3.1. Telemedicine Program Implementation Document

Minimum Content Requirements	Frequency of Submission
<ol style="list-style-type: none"> 1. Signed performance commitment (telemedicine company) 2. Signed performance commitment (for engaged healthcare providers) 3. Accomplished ICT service provider request form 4. Accomplished telemedicine program profile 5. Certified true copy of signed MOA with LGU (if applicable) 6. Telemedicine platform, including data and solutions architecture 7. Health human resource recruitment and management protocol 8. Telemedicine consultation protocol 9. Data privacy and cybersecurity measures 10. Risk and issue management protocol 11. Marketing protocol 	One-time/As updated

3.2. Telemedicine Privacy Management Program Document

Minimum Content Requirements	Frequency of Submission
<ol style="list-style-type: none"> 1. Contact details of data protection officer 2. Privacy policy 3. Documentation of privacy impact assessment 4. Privacy management program implementation plan or privacy manual 	One-time/As updated

3.3. Weekly Status Reports (to be submitted every Monday of the following week)

- a. Demographics
 - Name of telemedicine provider
 - Total #, names, and contact details of LGUs engaged
 - Total #, names and addresses of health facilities engaged as providers of telemedicine services
 - Total #, names and contact details of physicians engaged as providers of telemedicine services
- b. Summary of telemedicine consultations
 - Total # of unique individual patients who sought health services through telemedicine per healthcare provider per day (disaggregation: individual health facility vs individual physician)
 - Total # of telemedicine consultations received per healthcare provider per day (disaggregation: companion-assisted patient consultation vs non-companion-assisted/individual patient consultation; individual health facility vs individual physician)
 - Type of telemedicine consultations received per healthcare provider (disaggregation: COVID-19 vs non-COVID-19 health concerns; individual health facility vs individual physician)
 - Reasons for consultations received per healthcare provider (disaggregation: COVID-19 vs non-COVID-19 health concerns; individual health facility vs individual physician)
 - Clinical classification (disaggregation: COVID-19 vs non-COVID-19 health concerns; individual health facility vs individual physician)

- Type of disposition per telemedicine consultation received (disaggregation: COVID-19 vs non-COVID-19 health concerns; individual health facility vs individual physician)

Name of Telemedicine Provider:														
Name and Address of Health Facility														
Name of Physician														
Case #	Age	Residence	Date of Consultation	Patient was accompanied by a companion during consultation (Y/N)	Reason for Consultation	COVID-19 Health Concern (Y/N)	Non-COVID-19 Health Concern (Y/N)	Diagnosis	Plan of Management	Issued ePrescription (Y/N)	Issued Referral to Health Facility (Y/N)	Clinical Classification	Disposition	

c. Feedback

- Average patient satisfaction rating of the telemedicine services provided by the healthcare provider
- # of patient complaints received by healthcare providers
- # of patient complaints closed by healthcare providers
- Types of complaints (i.e. privacy and security breach, medical errors, etc.)

Name of Telemedicine Provider:						
Name and Address of Health Facility						
Name of Physician						
Case #	Patient Satisfaction Rating	Complaints/Issues (Y/N)	If yes, nature of complaint.	Action Taken	Closed (Y/N)	If no, indicate reason.

- # of telemedicine provider complaints received from healthcare providers
- # of telemedicine provider complaints from healthcare providers closed
- Types of telemedicine provider complaints (i.e. disengagement, etc.)
- # of security incidents and personal data breaches reported within NPC protocols (incident reporting mechanism)

Name of Telemedicine Provider:						
Total # of LGUs engaged						
Total # of health facilities engaged						
Total # of physicians engaged						
Name of Health Facility	Address	Complaints/Issues (Y/N)	If yes, nature of complaint.	Action Taken	Closed (Y/N)	If no, indicate reason
Name of Physician		Complaints/Issues (Y/N)	If yes, nature of complaint.	Action	Closed (Y/N)	If no, indicate reason

3.4. Performance Commitment for DOH Telemedicine Partners

(Letterhead of Telemedicine Company)

(Date)

DEPARTMENT OF HEALTH

San Lazaro Compound, Rizal Avenue, Sta. Cruz, Manila

SUBJECT: Performance Commitment

Sir/Madam:

To guarantee our commitment to support the fight against COVID-19, we respectfully submit this Performance Commitment. And for the purposes of this Performance Commitment, we hereby warrant the following representations:

1. That we agree to be enrolled in a sandbox implementation program for the utilization of telemedicine in response to COVID-19 where telemedicine companies are enjoined to conform to a minimum set of standard regulation for the practice of telemedicine. The overall goal is to test telemedicine as a medium to deliver care to individuals in a safe environment, utilizing current technology capabilities.
2. That we are a duly recognized telemedicine company abiding by the legal and regulatory framework of the country.
3. That all professional health care providers in our company possess proper credentials and given appropriate privileges in accordance with our policies and procedures.
4. That we shall render telemedicine services without cost either to the Department of Health or to the patients receiving the services.
5. That we shall ensure that all operations are compliant with all appropriate legal and regulatory frameworks in the Philippines.
6. That we shall provide a mechanism for physicians or medical doctors to sign up for this initiative and in the interim, for the latter to volunteer their medical services to the public at no charge to the patient.
7. That we shall provide a form of safety assurance for physicians to operate Telemedicine services to the patients or individuals.
8. That we shall provide a secure and user-friendly platform which shall be made available for medical consultation. The physicians or medical doctors will be able to make use of the process of this platform to record and maintain patient data and refer the patient to the nearest health facility, if necessary.
9. That we shall ensure that reasonable and appropriate security measures are implemented to safeguard the patients' and doctors' data collected, used, stored, or otherwise processed using the platform, against any accidental or unlawful destruction, alteration or disclosure as well as unlawful access, fraudulent misuse, or any other unauthorized processing.

10. That we shall train volunteer physicians to handle telemedicine consultations.
11. That we shall first obtain the informed consent of the patient prior to the collection of any personal data and the offering of any telemedicine service.
12. That we shall uphold the data privacy rights of patients and physicians or medical doctors using the platform, and shall provide mechanisms for the effective exercise of these rights.
13. That we shall comply with all pertinent DOH guidelines on COVID-19 responses and patient surveillance.
14. That we recognize that the DOH shall be the controller of patients' data, which remains to be owned by the individual patients.
15. That we shall comply with the necessary protocols for data sharing, monitoring and evaluation activities.
16. That we shall act as the processor of patient data for and on behalf of the DOH.
17. That we shall be held liable for any security incident, or privacy violations, or personal data breaches, and other related issues and concerns arising from the use of our platform, and which are attributable to our platform or our company.
18. Nothing in this document shall be interpreted or construed as creating or establishing an Employer-Employee relationship between the DOH and telemedicine partner.

We commit to extending our full support in order to effectively and appropriately deliver primary care teleconsultations to those who are in need.

Very Truly Yours,

Authorized Representative of the Telemedicine Company

3.5. Performance Commitment for Engaged Healthcare Providers by DOH Telemedicine Partners

(Date)

DEPARTMENT OF HEALTH

San Lazaro Compound, Rizal Avenue, Sta. Cruz, Manila

SUBJECT: Performance Commitment

Sir/Madam:

To guarantee our commitment to support the fight against COVID-19, I respectfully submit this Performance Commitment. And for the purposes of this Performance Commitment, I hereby warrant the following representations:

1. That I agree to be enrolled in a sandbox implementation program for the utilization of telemedicine in response to COVID-19. The overall goal is to use telemedicine as a medium to deliver health services to patients in a safe environment following established treatment algorithms and guidelines while utilizing current technology capabilities.
2. That I shall only use a secure platform for medical consultation and referral of patients to the nearest health facility, if necessary.
3. That I shall ensure that the privacy settings of the platform being used is compliant with the minimum legal and regulatory laws and frameworks in the Philippines.
4. That I shall not use public-facing platforms like Youtube or Facebook Live, and such other similar public-facing platforms, for telemedicine consultations.
5. That I shall first obtain the informed consent of the patient prior to the collection of any personal data and the offering of any telemedicine service.
6. That I shall uphold the data privacy rights of patients using the platform, and shall provide mechanisms for the effective exercise of these rights. Patients should be: (a) informed that the platform being used entails privacy risks and that a telehealth consultation may not be equivalent to a face-to-face consult; (b) allowed to discuss their privacy and other related concerns, if any; and (c) be given the option not to proceed with the consult.
7. That I shall ensure that reasonable and appropriate security measures are implemented to safeguard the patients' data collected, used, stored, or otherwise processed using the platform, against any accidental or unlawful destruction, alteration or disclosure as well as unlawful access, fraudulent misuse, or any other unauthorized processing.
 - 7.1. Patients should be informed that any personal data obtained in the course of the consult shall be used for medical treatment, kept confidential, and only those involved in patient's care shall have access.
 - 7.2. That I shall choose a place to conduct the telemedicine consultation beforehand, i.e. conducive to communicating with the patient, and where interruptions or potential unwarranted disclosures are avoided.

8. That I shall comply with all pertinent DOH COVID-19 and non-COVID-19 treatment algorithms and guidelines, including patient surveillance.
9. That I recognize that DOH and I shall be the controller of patients' data, which remains to be owned by the individual patients.
10. That I shall comply with the necessary protocols for data sharing, monitoring and evaluation activities.
11. That I shall render telemedicine services without cost either to the DOH or to the patients receiving the services.
12. That I shall be held liable for any security incident, or privacy violation, or personal data breaches, and other related issues and concerns arising from the conduct of telemedicine consultation, and which are attributable to me or my acts.
13. Nothing in this document shall be interpreted or construed as creating or establishing an Employer-Employee relationship between the telemedicine partner and healthcare provider, and between the DOH and the healthcare provider.

We commit to extending our full support in order to effectively and appropriately deliver primary care teleconsultations to those who are in need.

Very Truly Yours,

Name of Healthcare Provider

License Number

Contact Details (i.e. address, phone number & email)

Reference: Patdu, Ivy D. (19 March 2020). Privacy should not be an obstacle to telemedicine. Newsbytes.PH. Retrieved from <http://newsbytes.ph/2020/03/patdu-privacy-should-not-be-an-obstacle-to-telemedicine/>.

3.6. ICT Solutions Provider Request Form



Republic of the Philippines
Department of Health
**KNOWLEDGE MANAGEMENT AND
INFORMATION TECHNOLOGY SERVICE**

ICT Solutions Provider Request Form

Date Submitted: _____

Company Details	
Name of Provider	
Main Office Address	Address: _____ City: _____ Region: _____ Zip Code: _____
Website (if none, attach company/business profile)	
Years of Operation	<input type="checkbox"/> Please check if start-up (pending business registration)
Company Ownership	<input type="checkbox"/> Sole Proprietorship (Company) <input type="checkbox"/> Partnership <input type="checkbox"/> Sole Proprietorship (Consultant) <input type="checkbox"/> Corporation <input type="checkbox"/> Government agency or GOCC <input type="checkbox"/> Non-Profit Organization <input type="checkbox"/> Others (please specify): _____
Type of Provider	<input type="checkbox"/> Manufacturer <input type="checkbox"/> Systems Integrator <input type="checkbox"/> Distributor <input type="checkbox"/> Reseller
Details of ICT Solution	
Commercial Name/s of ICT Solution (if applicable)	
Category	<input type="checkbox"/> Service/ICT Consultancy <input type="checkbox"/> Mobile Health Applications <input type="checkbox"/> Electronic Health/Medical Record System <input type="checkbox"/> Telehealth Applications <input type="checkbox"/> Hospital Information System <input type="checkbox"/> ICT-based Biomedical Device <input type="checkbox"/> Systems Software <input type="checkbox"/> Other Software Application <input type="checkbox"/> Cybersecurity Solutions <input type="checkbox"/> Hardware, including computer peripherals and telephony <input type="checkbox"/> Others (please specify): _____

Building 9, San Lazaro Compound, Rizal Avenue, Sta. Cruz, 1003 Manila • Trunk Line 651-7800 Local 1947, 1926, and 1923
URL: <http://www.doh.gov.ph>

Health System Dimensions that the ICT Solution aims to address/support <i>(select whichever is appropriate)</i>	<input type="checkbox"/> Data warehousing and business intelligence. <input type="checkbox"/> Disease prevention and control, and health protection. <input type="checkbox"/> Epidemiological surveillance and response. <input type="checkbox"/> Supply chain management. <input type="checkbox"/> Procurement and financial management. <input type="checkbox"/> Health promotion and communications. <input type="checkbox"/> Data privacy and cybersecurity. <input type="checkbox"/> Alternative models of service delivery (e.g. telehealth) <input type="checkbox"/> Electronic medical/health records management. <input type="checkbox"/> Interoperability, electronic health information exchange, and service referral. <input type="checkbox"/> ICT capacity building and management. <input type="checkbox"/> Corporate ICT infrastructure.			
Brief Description of ICT Solution				
Request Details				
Nature of Partnership Requested	<input type="checkbox"/> For government procurement under RA 9184 (GPRA) <input type="checkbox"/> For public-private partnership for health under RA 7718 (BOT Law) or JV Guidelines <input type="checkbox"/> For pilot implementation <input type="checkbox"/> For health technology assessment <input type="checkbox"/> Others (please specify): _____			
Indicative Cost of Partnership (in PHP) <i>(Indicate "0" if none)</i>	<table border="1"> <tr> <td data-bbox="404 994 727 1120"> Government (DOH) Indicative Cost Upfront Cost: _____ Subscription Cost: _____ Maintenance Cost: _____ </td> <td data-bbox="727 994 1063 1120"> Provider Indicative Cost Upfront Cost: _____ Subscription Cost: _____ Maintenance Cost: _____ </td> </tr> </table>		Government (DOH) Indicative Cost Upfront Cost: _____ Subscription Cost: _____ Maintenance Cost: _____	Provider Indicative Cost Upfront Cost: _____ Subscription Cost: _____ Maintenance Cost: _____
Government (DOH) Indicative Cost Upfront Cost: _____ Subscription Cost: _____ Maintenance Cost: _____	Provider Indicative Cost Upfront Cost: _____ Subscription Cost: _____ Maintenance Cost: _____			
Nature of Presentation <i>(if applicable)</i>	<input type="checkbox"/> N/A <input type="checkbox"/> Company Profile Presentation <input type="checkbox"/> ICT Solutions Demonstration <input type="checkbox"/> Proof of Concept <input type="checkbox"/> Others: _____			
Contact Details				
Primary Contact Person	Name: _____ Position: _____ Mobile No.: _____ Email: _____			
Visiting Party Details <i>(Name & Position)</i>	1. _____ 2. _____ 3. _____			
Other Details	<input type="checkbox"/> Yes <input type="checkbox"/> No - Is this your first time to send this request form? <input type="checkbox"/> Yes <input type="checkbox"/> No - Do you have any government procurement experience? <input type="checkbox"/> Yes <input type="checkbox"/> No - Is your organization a past or current DOH contractor?			

	<input type="checkbox"/> Yes <input type="checkbox"/> No - Does your organization have a Data Protection Officer? If yes, please indicate name and contact details: _____ <input type="checkbox"/> Yes <input type="checkbox"/> No - Any conflict of interest? If yes, please indicate: _____
(For Knowledge Management and Information Technology Service use only)	
Reference Number	
Date Received	
KMITS Focal Person/s	
Actions Taken	<input type="checkbox"/> Presentation date Date: _____ <input type="checkbox"/> Officially relayed recommendation Date: _____ <input type="checkbox"/> Endorsed to _____ Date: _____
Findings and Recommendations	<input type="checkbox"/> For proof of concept study <input type="checkbox"/> For pilot demonstration <input type="checkbox"/> For health technology assessment <input type="checkbox"/> For participation in an ongoing DOH procurement <input type="checkbox"/> For endorsement to PPPH-Program Management Unit <input type="checkbox"/> For endorsement to another DOH Office/Agency: _____ <input type="checkbox"/> Duplication with an existing DOH solution <input type="checkbox"/> With conflict of interest <input type="checkbox"/> Others: _____
Noted by	_____ DR. ENRIQUE A. TAYAG, PHSAE, FPSMID, CESO III Director IV

Instructions:

E-mail a scanned copy of this form and presentation to nationalehealthprogram@doh.gov.ph

For more information, you may access FAQ's for ICT Solutions Provider: bit.ly/DOHictspFAQ

3.7. Telemedicine Program Profile Template

TELEMEDICINE PROGRAM PROFILE

[Telemedicine Company]	
SHORT PROFILE OF COMPANY	
INSTRUCTION FOR PUBLIC TO ACCESS THE PLATFORM (e.g. hotline, mobile app, etc).	
OPERATING HOURS	
DESCRIPTION OF TELEMEDICINE SYSTEM FUNCTIONALITIES	
PATIENT FLOW (ALGORITHM INTEGRATING DOH COVID-19 PROCESS FLOWS)	
DESCRIPTION OF MANPOWER OR REQUIREMENTS FOR VOLUNTEER PHYSICIANS	
AUTHORIZED REPRESENTATIVE AND CONTACT INFORMATION	
MONITORING AND EVALUATION MECHANISMS FOR PERFORMANCE/QUALITY	

Annex 4.0 Recommended Templates

4.1. Clinical Abstract/Consultation Summary Template

Name of Physician:			Date & Time of Teleconsultation:		
Name and Address of Health Facility (if applicable):			Name of Telemedicine Partner (if applicable): If none, indicate telemedicine platform being used:		
Prior to teleconsultation proper, obtain patient consent: () Yes () No					
Is patient accompanied/assisted by another person during the consultation: () Yes () No					
A. DEMOGRAPHIC PROFILE					
1. Patient Profile				Case #	
Last Name	First Name	Middle Name	Birthdate (yyyy-mm-dd)	Age	Sex
Occupation	Civil Status	Nationality	PhilHealth No.	Passport No.	
Name of Companion: (if patient is assisted/accompanied during the teleconsultation)			Relationship:	Phone No.	
2. Philippine Residence					
House No./Lot/Bldg.	Street	Municipality/City		Province	
Region	Home Phone No.	Cellphone No.		Email address	
B. CLINICAL HISTORY AND PHYSICAL EXAMINATION					
3. Clinical History					
Reason for Consultation					
Date of Onset of Illness		Name of Referral Health Facility (if applicable)		Date of Referral (if applicable)	
Known Medical Condition/s and Medical History					
Current Medications				Blood Type	
4. Physical Examination (Inspection)					
Clinical Status at the time of Consult					
Specific Findings					
C. COVID-19 SCREENING					
5. Overseas Employment Address (for Overseas Filipino Workers)					
Employer's Name:			Place of Work:		
House #/Bldg. Name	Street	City/Municipality		Province/State	
Country	Office Phone No.		Cellphone No.		
6. Travel History					

History of travel/visit/work in other countries with known COVID-19 transmission 14 days prior to onset of signs and symptoms: () Yes () No						Port of exit:	
Airline/Sea vessel:		Flight/Vessel Number		Date of Departure		Date of Arrival in Philippines:	
7. Exposure History							
Known COVID-19 Case: () Yes () No () Unknown				If yes: Date of Contact with Known COVID-19 Case:			
Accommodation () Yes () No () Unknown Specify type: Address:				Date of Last Exposure: Name: () Guest () Hotel worker			
Food Establishment () Yes () No () Unknown Specify type: Address:				Date of Last Exposure: Name: () Diner () Crew			
Store () Yes () No () Unknown Specify type: Address:				Date of Last Exposure: Name: () Customer () Worker			
Health Facility () Yes () No () Unknown Specify type: Address: Significant Other				Date of Last Exposure: Name: () Patient () Health Worker ()			
Event () Yes () No () Unknown Specify type:				Date of Last Exposure: Event Place:			
Workplace () Yes () No () Unknown Company Name:				Date of Last Exposure: Address:			
List of names of persons in contact with during any of this occasion, and their contact numbers:							
8. Clinical Assessment							
Symptomatic: A. 14 days PRIOR to first date of exposure () Yes () No B. Anytime during date of exposure () Yes () No			If yes, date of onset of illness: Name of referral health facility: Date of referral:		If no, place of quarantine: () Home () Quarantine Facility: _____		
Fever ____ °C	Cough ()	Colds ()	Sore throat ()	Diarrhea ()	Shortness/difficulty of breathing ()		
Other symptoms, specify			Is there any history of other illness? () Yes () No If YES, specify: _____				
Chest X-Ray done? () Yes () No If yes, when? _____			Are you pregnant? () Yes LMP _____ () No				
CXR Results: Pneumonia () Yes () No () Pending			Other Radiologic Findings:				
9. Specimen Information							
Specimen Collected	If YES, Date Collected	Date sent to RITM or any accredited laboratory		Date received in RITM		Virus Isolation Result	RT-PCR Result

			or any accredited laboratory						
() Serum	____/____/____	____/____/____	____/____/____						
() Oropharyngeal/ Nasopharyngeal swab	____/____/____	____/____/____	____/____/____						
() Others	____/____/____	____/____/____	____/____/____						
10. Classification									
<input type="checkbox"/> Suspect Case <input type="checkbox"/> Probable Case <input type="checkbox"/> Confirmed Case									
11. Outcome									
Date of Discharge:		Condition on Discharge:							
		() Died () Improved () Recovered							
		() Transferred () Absconded							
D. DIAGNOSIS/ASSESSMENT									
Summary of Assessment Findings									
Diagnosis									
Clinical Classification: () COVID-19 Case () Non-COVID-19 Case									
If COVID-19 Case, () Suspected Case () Probable Case () Confirmed Case									
E. PLAN OF MANAGEMENT									
Plan of Management:									
Prescription:									
Referral:									
Disposition:									
Name & Digital Signature of Physician:		License #		Professional Tax Receipt (if applicable):					

COVID-19 Case Classification

1. **Suspect case** – is a person who is presenting with any of the conditions below.
 - a. All Severe Acute Respiratory Infection (SARI) cases where NO other etiology fully explains the clinical presentation.
 - b. Influenza-Like Illness (ILI) cases with any one of the following:
 - i. with no other etiology that fully explains the clinical presentation AND a history of travel to or residence in an area that reported local transmission of COVID-19 disease during the 14 days prior to symptom onset OR
 - ii. with contact to a confirmed or probable case of COVID-19 in the two days prior to onset of illness of the probable/confirmed COVID-19 case until the time the probable/confirmed COVID-19 case became negative on repeat testing.
 - c. Individuals with fever or cough or shortness of breath or other respiratory signs or symptoms fulfilling any one of the following conditions:
 - i. Aged 60 years and above
 - ii. With a comorbidity
 - iii. Assessed as having a high-risk pregnancy
 - iv. Health worker
2. **Probable case** – a suspect case who fulfills anyone of the following listed below.
 - a. Suspect case whom testing for COVID-19 is inconclusive
 - b. Suspect who tested positive for COVID-19 but whose test was not conducted in a national or subnational reference laboratory or officially accredited laboratory for COVID-19 confirmatory testing
3. **Confirmed case** – any individual, irrespective of presence or absence of clinical signs and symptoms, who was laboratory confirmed for COVID-19 in a test conducted at the national reference laboratory, a subnational reference laboratory, and/or DOH-certified laboratory testing facility.

4.2. Patient Satisfaction Survey Form

Name of Patient: _____

Case # _____

Name of Provider: _____

Date of Consultation: _____

Questions	Rating					Remarks
1. How comfortable did you feel?	1 (not at all comfortable)	2	3	4	5 (very comfortable)	
2. How convenient was the encounter?	1 (not at all convenient)	2	3	4	5 (very convenient)	
3. Was the lack of physical contact acceptable?	1 (not acceptable)	2	3	4	5 (very acceptable)	
4. Concerns about privacy?	1 (no concerns)	2	3	4	5 (very concerned)	
5. Overall satisfaction?	1 (not at all satisfied)	2	3	4	5 (very satisfied)	
6. Would you do a teleconsultation again?	Yes			No		
7. Suggestions and recommendations						

4.3. Sample Informed Consent

**AUTHORIZATION AND CONSENT TO PARTICIPATE IN TELEMEDICINE
CONSULTATION
PAGPAPAHINTULOT AT PAGSANG-AYON NA LUMAHOK SA KONSULTASYONG
TELEMEDICINE (SAMPLE CONSENT)**

The purpose of this form is to obtain your consent to participate in a telemedicine consultation with the following physician: _____

Ang layunin ng form na ito ay makuha ang inyong pahintulot upang lumahok sa isang konsultasyong telemedicine ni Dr. _____.

Purpose and Benefits. The purpose of this service is to use telemedicine to enable patients to still receive health services even while staying at home during the enhanced community quarantine, except for serious conditions, emergencies, or to avail of COVID-19-related health services as per standing protocols.

Layunin at Benepisyo. *Ang layunin ng serbisyong ito ay gumamit ng telemedicine para mabigyan ng pagkakataon ang mga pasyenteng apektado ng enhanced community quarantine na nasa bahay na patuloy na makapagkonsulta at makatanggap ng serbisyong medical, maliban na lamang kapag ang pasyente ay may malubhang sakit o may medical emergencies na nangangailangan ng agarang atensiyong medical, o makakuha ng COVID-19-related na serbisyong medical alinsunod sa mga umiiral na protocol.*

Nature of Telemedicine Consultation: During the telemedicine consultation:

Anyo ng Konsultasyong Telemedicine: *Sa inyong konsultasyong telemedicine:*

- a) Details of you and/or the patient's medical history, examinations, x-rays, and tests will be collected and discussed with other health professionals through the use of interactive video, audio and telecommunications technology if needed.
Ang mga detalye mo at/o ng pasyente tungkol sa kasaysayang pang-medikal, mga ginawang pagsusuri at x-ray ay kokolektahin at tatalakayin kasama ng ibang mga eksperto sa pamamagitan ng interactive video, audio, at telecommunications technology kung kinakailangan.
- b) Physical examination of you or the patient may take place.
Ang pisikal na pagsusuri sa iyo o ng pasyente ay maaaring gawin.
- c) Nonmedical technical personnel may be present in the telemedicine studio to aid in video transmission, if needed.
Maaaring may makasamang mga kawani sa telemedicine studio upang magbigay ng serbisyong teknikal at umagapay sa video transmission kung kakailanganin.
- d) Video, audio, and/or digital photo may be recorded during the telemedicine consultation visit.
Maaaring i-record ang video, audio, at/o kumuha ng larawan habang isinisagawa ang konsultasyong telemedicine.

Medical Information and Records. All existing laws regarding your access to medical information and copies of your medical records apply to this telemedicine consultation. Additionally, dissemination of any patient-identifiable images or information from this telemedicine interaction to researchers or other entities shall not occur without your consent, unless authorized by existing law, policies and guidelines on privacy and data protection.

Impormasyong Pang-medikal at Mga Talaan. *Lahat ng mga umiiral na batas tungkol sa inyong pagkuha ng impormasyong pang-medikal at ng inyong mga talaang pang-medikal ay naaangkop sa konsultasyong telemedicine na ito. Bukod dito, ang pagpapakalat ng mga larawan ng pasyente at impormasyon sa pakikipag-ugnayang telemedicine na ito sa mga mananaliksik at ibang tao ay hindi*

mangyayari nang wala ang inyong pagsang-ayon, maliban na lamang kung ito ay pinahihintulutan ng mga umiiral na batas, polisiya at alintuntunin tungkol sa privacy and data protection.

Confidentiality. Reasonable and appropriate efforts have been made to eliminate any confidentiality risks associated with the telemedicine consultation. All existing law, policies and guidelines on privacy and data protection apply to information disclosed during this telemedicine consultation.

Confidentiality. Isinagawa ang mga makatwiran at naaangkop na hakbang upang alisin ang anumang panganib sa confidentiality ng gagawing konsultasyong telemedicine. Lahat ng umiiral na batas, polisiya at alintuntunin tungkol sa privacy and data protection ay nakapaloob at naaangkop sa mga ibibigay na impormasyon sa konsultasyong telemedicine na ito.

Risks and Consequences. The telemedicine consultation will be similar to a routine medical office visit, except interactive video technology will allow you to communicate with a physician at a distance. At first you may find it difficult or uncomfortable to communicate using video images. The use of video technology to deliver healthcare and educational services is a new technology and may not be equivalent to direct patient to physician contact. Following the telemedicine consultation, your physician may recommend a visit to a health facility for further evaluation.

Nakaambang Panganib at Kahihinatnan. Ang konsultasyong telemedicine na ito ay kahalintulad ng isang tipikal na konsultasyon sa isang opisinal pang-medikal, maliban sa may gagamitin ditong interactive video technology na magagamit upang makipag-usap sa isang doctor mula sa malayo. Sa simula ay maaaring mahirapan ka o maging hindi ka komportable na makipag-usap gamit ang video images. Ang paggamit ng video technology upang ibigay ang mga serbisyong pang-medikal at pang-edukasyon ay isang makabagong teknolohiya at maaaring hindi matumbasan ang direktang pakikipag-ugnayan ng isang pasyente sa kaniyang doktor. Gamit ang isang konsultasyong telemedicine, ang inyong doktor ay maaaring irekomenda ang pagpunta sa isang pasilidad na pangkalusugan gaya ng RHU o ospital upang masuri nang mas maigi.

Rights. You may withhold or withdraw consent to the telemedicine consultation at any time without affecting your right of future care or treatment, or risking the loss or withdrawal of any program benefits to which you would otherwise be entitled. You have the option to consult with the physician in person if you travel to his or her location.

Mga Karapatan. Maaari mong itigil o bawiin ang iyong pagsang-ayon sa konsultasyong telemedicine sa anumang oras nang hindi naapektuhan ang iyong karapatan sa pangangalaga o magamot sa hinaharap, o malagay sa panganib o pagbawi ang anumang benepisyo na maaari mong makamtan. Ikaw ay may karapatang kumonsulta sa doktor nang harapan kung ikaw ay pupunta sa kaniyang klinika.

Financial Agreement. You and/or your insurance company will not be billed for this visit.

Kasunduang Pinansyal. Ikaw at/o ang iyong insurance company ay hindi sisingilin sa konsultasyong ito.

I have been advised of all the potential risks, consequences and benefits of telemedicine. The physician of this telemedicine consultation has discussed with me the information provided above. I have had an opportunity to ask questions about this information and all of my questions have been answered. I understand the written information provided above.

Ako ay pinayuhan sa lahat ng maaaring panganib, kahihinatnan, at benepisyo ng telemedicine. Ang doctor sa konsultasyong telemedicine na ito ay tinalakay sa akin ang mga impormasyong inilahad sa itaas. Ako ay binigyan ng pagkakataong magtanong tungkol sa impormasyong ito at lahat ng aking mga tanong ay nasagot. Nauunawaan ko ang mga impormasyong nakasulat sa itaas.

Signature:
Lagda

Patient (or person authorized to give consent)
Pasyente (o taong itinalaga upang magbigay ng pagsang-ayon)

Date: _____
Petsa: _____

If signed by person other than patient, provide relationship to patient: _____
Kung nilagdaan ng ibang tao bukod sa pasyente, ibigay ang kaugnayan sa pasyente: _____

Witness: _____
Saksi: _____

Date: _____
Petsa: _____

NPC Circular No. 20-01

DATE: 14 September 2020

SUBJECT: GUIDELINES ON THE PROCESSING OF PERSONAL DATA FOR LOAN-RELATED TRANSACTIONS

WHEREAS, the National Privacy Commission (NPC) has received numerous complaints against some lending entities operating online lending applications (online apps) which can be downloaded and installed in mobile phones;

WHEREAS, these online apps are used to facilitate loan transactions between these lending entities and their clients. The online apps provide a platform for the processing of personal data relating to their clients, which includes access to their clients' phones' contact list, camera, location, and storage, among others;

WHEREAS, the complaints claimed that these lending entities, through the online apps, processed personal data of their clients without lawful basis under the law, and used such personal data about their clients and other individuals in their contact list causing damage to their reputation, in violation of their rights and freedoms as data subjects;

WHEREAS, Section 2 of Republic Act No. 10173 otherwise 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 recognizes the vital role of information and communications technology in nationbuilding 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;

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 compliance with the provisions of the DPA and with international standards for data protection, 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;

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 processing of personal data for loan transactions.

SECTION 1. Scope. — This Circular shall apply to, among others, the processing of personal data for purposes of loan processing activities,¹ through any modality, by lending or financing companies, as defined under the Lending Company Regulation Act of 2007 and Financing Company Act of 1998, respectively, or by any natural or juridical person who acts as such, whether or not granted with the requisite authority from the Securities and Exchange Commission (SEC). It shall likewise apply to personal information processors (PIP) or third-party service providers engaged by the lending or financing company, or any natural or juridical person who acts as such, whenever such PIPs or third-party service providers are engaged in the processing of the personal information of the latter's clients.

For purposes of this Circular, a lending company (LC) shall refer to a corporation engaged in granting loans from its own capital funds or from funds sourced from not more than nineteen (19) persons. It shall not be deemed to include banking institutions, investment houses, savings and loan associations, financing companies, pawnshops, insurance companies, cooperatives and other credit institutions already regulated by law.²

Financing companies (FC) are corporations, except banks, investments houses, savings and loan associations, insurance companies, cooperatives, and other financial institutions organized or operating under other special laws, which are primarily organized for the purpose of extending credit facilities to consumers and to industrial, commercial, or agricultural enterprises, by direct lending or by discounting or factoring commercial papers or accounts receivable, or by buying and selling contracts, leases, chattel mortgages, or other evidences of indebtedness, or by financial leasing of movable as well as immovable property.³

While some entities are excluded from the definition above of lending and financing companies, these entities remain to be within the jurisdiction of the NPC with respect to all other obligations under the DPA, its Implementing Rules and Regulations (IRR), and applicable issuances of the NPC.

SECTION 2. Obligations of personal information controllers. — All entities engaged in the processing of personal data for purposes of granting loan facilities are personal information controllers (PICs). As PICs, they shall process personal and sensitive personal information (collectively, personal

data) of borrowers in accordance with any of the criteria for lawful processing provided for under Sections 12 and 13 of the DPA. They shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data and uphold the rights of data subjects.

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:

A. Borrowers shall be provided all the details required under Section 16 (b) of the DPA and Section 34 (a)(2) of its IRR, in a clear language and in the most appropriate format.

1. The details shall include all the information concerning all phases of the loan processing activity, from loan solicitation, loan origination, repayment, debt collection and remedial measures;
2. Whenever the loan processing activity entails the use of profiling, automated processing, automated decision-making, or credit rating or scoring, the borrower shall be informed of the same before the entry of his or her personal data into the data processing system or at the next practical opportunity;
3. Pursuant to the borrower's right to information and access, LCs, FCs and other persons acting as such shall disclose the categories of data considered in deciding whether to approve or disapprove a loan application. Recognizing, however, that the integrity of the evaluation process and methods used must be maintained to avoid possible manipulation or exploitation of the same, LCs, FCs and other persons acting as such may implement reasonable policies determining the minimum information and manner of disclosure to a borrower; and
4. LCs, FCs, and other persons acting as such shall adopt policies and procedures to adequately address borrowers' inquiries and clarifications.

B. In cases where a borrower's personal data will be further processed for purposes compatible with the primary purpose, the same may be allowed, provided that:

1. A direct and objective link must exist between the primary purpose for the processing of the personal data and the other compatible purposes. Such other purposes may include customer behavior analysis, system administration, service quality maintenance, customer service or support, among others; and
2. Should information be used for marketing, cross-selling, or sharing to third parties for purposes of offering other products or services not related to loans, LCs, FCs and other persons acting as such must have a separate lawful criterion for such processing pursuant to Sections 12 and/or 13 of the DPA.

C. LCs, FCs, and other persons acting as such shall limit the collection of personal data from the borrowers to those which are adequate, relevant, suitable, necessary, and not excessive in relation with the applicable know your customer (KYC) policies, rules and regulations, as well as those necessary for determining creditworthiness and preventing fraud.

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.

1. Application permissions shall only be allowed when suitable, necessary, and not excessive for the purpose of KYC, determining creditworthiness, preventing fraud, and collecting the debt in accordance with applicable provisions of law.
2. When such purpose has already been achieved, such online apps shall prompt the data subject to turn off or disallow these permissions.
3. Where an online app requires access to the borrower's phone camera to take a photo of the borrower and/or the photo gallery to choose a photo for the exclusive purpose of KYC and preventing fraud at the beginning of the loan application, permission for such access may be allowed at that stage in the loan application process.

Where the photo has already been taken and saved in the application, the application should already turn off such permission by default, or at the very least, prompt the borrowers through appropriate means, i.e. just-in-time, pop-up notices, etc. that they 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.

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.

E. LCs, FCs, and other persons acting as such shall bear in mind that they are at all times accountable for personal data under its control or custody. They shall not use any personal data to engage in unfair collection practices as defined under SEC Memorandum Circular No. 18 series of 2019. Such practices may also be construed as a punishable act under the DPA; and

F. LCs, FCs, and other persons acting as such shall adopt and implement reasonable policies regarding the retention of the personal data of those its

whose loan applications were denied and of borrowers who have fully settled their loans. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined. Otherwise, applicable penalties as provided for in the DPA may be imposed.

SECTION 4. *Character references.* — Borrowers may be required to provide names and contact numbers of character references to support the evaluation of the loan application and/or the loan collection process. To this end, it shall be the responsibility of the borrower to inform their character reference regarding the latter's inclusion as character reference.

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.

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 option of having their personal data removed as a character reference, if the same is feasible.

SECTION 5. *Credit data.* — Where the credit data of a borrower is required to be disclosed or submitted pursuant to law or regulation, the relevant provisions of the DPA shall apply. All other instances where LCs, FCs, and other persons acting as such either share credit data to a third party or obtain personal data from other entities that may help determine creditworthiness of their borrowers, must also be authorized under the DPA. LCs, FCs, and other persons acting as such shall, at all times, ensure the protection of the rights and freedoms of the individual about whom the personal data is processed in accordance with the DPA, its IRR and relevant NPC issuances.

SECTION 6. *Outsourcing.* — LCs, FCs, and other persons acting as such may outsource any personal data processing activity it may deem appropriate. Details of the authorized PIPs or third-party service providers shall be made available to borrowers to ensure that they are transacting only with authorized individuals or entities.

Parties to such outsourcing arrangements shall be guided by the provisions of the IRR of the DPA on Outsourcing and Subcontracting Agreements. Pursuant to the principle of accountability under the DPA, PICs are expected to be responsible for any personal data under its control or custody, including the processing of information that have been outsourced to a PIP.

LCs, FCs, and other persons acting as such shall ensure, through contractual or other reasonable means, that the PIPs are aware of their obligations under the DPA, its IRR and issuances of the NPC, and may be held contractually

liable to the PIC for violations of their agreement.

SECTION 7. *Rights of the data subject.* — All borrowers shall be accorded their rights as provided for under the DPA. Similar rights as may be provided for under other applicable laws, i.e. Section 4 (o) of the Credit Information System Act (CISA), shall be available to the borrower.

LCs, FCs, and other persons acting as such shall adopt policies and procedures which enables borrowers to exercise their rights under the DPA. In all cases, loan processing activities shall be consistent with the relevant provisions of the DPA, its IRR and relevant issuances of the NPC. LCs, FCs, and other persons acting as such who shall fail to do so shall be liable under the applicable provisions of the DPA.

SECTION 8. *Transitory Provisions.* – Upon effectivity of this Circular, all LCs, FCs, and other persons acting as such who are in possession of their borrowers' contact list in whatever form, in contravention of Section 3 (D) (4) shall dispose of the same in a secure manner that would prevent further unauthorized processing, access, or disclosure to any other party or the public.

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 two newspapers of general circulation.

Approved:

Sgd.
RAYMUND E. LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

NPC Circular No. 20-02

DATE: 06 October 2020

SUBJECT: CEASE AND DESIST ORDERS

Pursuant to the authority vested in the National Privacy Commission through Section 7(c) of Republic Act No. 10173, otherwise known as the “Data Privacy Act of 2012,” (DPA) to issue cease and desist orders on the processing of personal data, the following Rules on the Issuance of Cease and Desist Orders of the National Privacy Commission are hereby prescribed and promulgated:

RULE I

PRELIMINARY PROVISIONS

Section 1. Title. - These Rules shall be known as the Rules on the Issuance of Cease and Desist Orders of the National Privacy Commission, or the “Rules”.

Section 2. Scope and Coverage. - These Rules shall apply to all applications for a Cease and Desist Order on the processing of personal data and other matters cognizable by the National Privacy Commission.

Section 3. Definition of Terms. -

A. “Adverse Party” refers to a party against whom a Cease and Desist Order is sought.

B. “Aggrieved Party” refers to a data subject who claims to be the subject of a privacy violation or personal data breach, including the latter’s duly authorized representative: Provided, that the circumstances of the authority were established.

C. “Applicant” refers to any of the following (i) the aggrieved party, (ii) the Complaints and Investigation Division, or (iii) the Compliance and Monitoring Division of the NPC.

D. “Cease and Desist Order” or “CDO” refers to a type of injunction that requires a natural or juridical person to stop its complained act of processing personal information or the conduct of any act or practice in violation of the Data Privacy Act of 2012 (DPA).

E. “Commission” refers to the Privacy Commissioner and the two (2) Deputy Privacy Commissioners, acting as a collegial body.

F. “Complaints and Investigation Division” or “CID” refers to the Division of the National Privacy Commission whose function is to receive complaints and conduct investigations regarding violations of the DPA, its Implementing Rules and Regulations (IRR) and other related issuances, including violations of the rights of data subjects and other matters affecting personal data.

H. “Compliance Check” refers to the systematic and impartial evaluation of a PIC or PIP, in whole or any part, process or aspect thereof, to determine whether activities that involve the processing of personal data are carried out in accordance with the standards mandated by the DPA and other issuances of the Commission. It is an examination, which includes Privacy Sweeps, Documents Submissions and On-Site Visits, as defined under NPC Circular 18-02, Guidelines on Compliance Checks, intended to determine whether a PIC or PIP is able to demonstrate organizational commitment, program controls and review mechanisms intended to assure privacy and personal data protection in data processing systems.

I. “Data Subject” refers to an individual whose personal, sensitive personal, or privileged information is processed.

J. “NPC” refers to the National Privacy Commission as a government agency.

K. “Rules of Procedure” refers to NPC Circular 16-04 or the “Rules of Procedure of the National Privacy Commission”, as may be amended.

L. “Sua Sponte Investigation” shall refer to an investigation initiated by the NPC itself for possible violation of the DPA by one or more entities.

RULE II

CEASE AND DESIST ORDER

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.

Section 5. Filing of Application. – An action for the issuance of a CDO may be commenced upon the filing with the Commission of an application in writing, verified and under oath, by any of the following applicants:

A. the CID, through its sua sponte investigation or the CMD through its conduct of compliance checks and handling of breach notifications, if there is a finding that the grounds for the issuance of the CDO are present; or

B. the Aggrieved Party, either attached to a complaint or as an independent action, with payment of filing fees in accordance with the Rules of Procedure of the NPC, and upon recommendation by the CID after its assessment that the application is sufficient in form and substance.

Section 6. Contents of a Verified Application. - The application for the issuance of a CDO must specify the following:

A. the material facts establishing the grounds for such issuance;

B. the name, contact information and address of the respondent where the orders, issuances, or communications from the NPC may be served; and

C. the relevant documentary, testimonial, and object evidence supporting the issuance of a CDO.

If the application is filed by an Aggrieved Party, it shall also specify the Aggrieved Party's name, contact information and address where the orders, issuances, or communications from the NPC may be served, including a secure electronic mail address when available.

An application that does not comply with the foregoing requirements may still be acted upon at the discretion of the Commission 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.

The Commission may require the submission of additional information and/or evidence when it deems it necessary for the resolution of the application for CDO.

Until the Commission issues the CDO, the fact that an application

has been initiated or a complaint has been filed, including the contents of the application and complaint, shall be confidential.

The rules on filing and service of processes under the Rules of Procedure of the NPC shall apply.

Section 7. Cease and Desist Order Bond. – Unless the Aggrieved Party is exempted from the payment of filing fees under the Rules of Procedure of the NPC, upon filing of the application for the issuance of a CDO, the Aggrieved Party shall also file a bond in the form of cash deposit or surety bond executed to the Adverse Party in an amount fixed by the CID after its assessment. The bond is to answer for whatever damages that the adverse party may sustain by reason of the order, if it should be later decided that the applicant is not entitled thereto.

Section 8. Issuance of Cease and Desist Order. - Upon its conduct of verification and investigation, the Commission may issue an ex-parte CDO, without the necessity of a prior hearing, when in its determination the grounds relied upon exist. The CDO shall specifically state the act or practice complained of and require the person to immediately cease and desist from the commission or continuance thereof.

The Commission shall ensure that a copy of the CDO be immediately furnished to each party subject thereto. The CDO shall be immediately executory and enforceable upon receipt of the Adverse Party.

Section 9. Order to Comment. – The CDO shall also include an order for the Adverse Party to comment on its issuance and file the same within ten (10) days from receipt thereof. The order shall include a copy of the application for CDO, the annexes thereto, and receipt of the bond, if applicable.

Section 10. Implementation of the CDO. – The Commission shall ensure the implementation of the CDO no later than seventy-two (72) hours from receipt thereof by the Adverse Party. The NPC unit tasked by the Commission to implement the order shall submit to the Commission a report within forty-eight (48) hours after the completion of the implementation, stating therein the actions taken. Should the CDO be implemented beyond seventy-two (72) hours or in case it cannot be implemented, the concerned NPC unit shall submit a written report to the Commission stating the causes of delay or non-execution.

Section 11. Clarificatory Hearing. – After the submission of the Comment by the Adverse Party, the Commission may order the conduct of a clarificatory hearing, whenever in its discretion, additional information is needed to make a decision on the issued CDO. In case the Commission finds that a clarificatory hearing is necessary, it shall issue a notice of hearing addressed

to all the parties concerned which shall indicate the scheduled time and date for the hearing.

Section 12. Decision on the Issued CDO. – If after giving the Adverse Party the opportunity to be heard, it appears that the applicant is entitled to have the act or practice enjoined and that there is a need for the extension of the issued CDO, the Commission shall extend its effectivity, otherwise, the same shall be lifted.

The decision whether to extend or lift the issued CDO shall be made no later than thirty (30) days from the expiration of the period for the Adverse Party to file a comment or the termination of the clarificatory hearing if one is held. In the event that the Commission fails to render its decision within the said period, the CDO shall be deemed automatically lifted.

Section 13. When CDO is Extended. - The extension of the CDO issued by the Commission shall also include an order to submit the necessary compliance report within the time prescribed for monitoring purposes. The concerned NPC unit shall ensure that a copy of such order be immediately furnished to each party subject thereto.

The extended CDO shall remain in force and effect until the same is modified or lifted by the Commission upon showing that the factual or legal basis for which it was issued no longer exists.

Section 14. Not Stayed by Appeal. - The CDO shall not be stayed by an appeal taken therefrom or by a petition for certiorari, unless otherwise ordered by the appropriate court, upon such terms as it may deem just.

RULE III

MOTION TO LIFT EXTENDED CEASE AND DESIST ORDER

Section 15. Motion to Lift Extended CDO. - At any time during the effectivity of the extended CDO, the Adverse Party may file a motion to lift said order on the ground that the factual or legal basis for which it was issued no longer exists, furnishing a copy thereof to the applicant. The motion shall contain or specify the material facts establishing the ground/s relied upon, the relevant documentary, testimonial and object evidence supporting the motion, and the proof of service of the copy of the motion to the applicant.

Section 16. Comment or Opposition to the Motion. - The applicant may file a comment/opposition to the motion to lift within ten (10) days from receipt thereof and furnishing a copy thereof to the Adverse Party. It shall contain the relevant documentary, testimonial and object evidence supporting its position, and shall specify the material dates relevant to the same and proof of service of the copy of the Comment/Opposition to the Adverse Party.

Section 17. Clarificatory Hearing on the Motion. – Whenever in its discretion, the conduct of a clarificatory hearing on the motion to lift extended CDO is necessary, the Commission shall set the motion for hearing. The notice of hearing shall be addressed to all parties concerned and shall specify the time and date of the hearing.

Section 18. Resolution on the Motion. – The motion shall be set for resolution by the Commission. If the Commission denies the motion to lift, the extended CDO shall continue to have force and effect.

Without need of filing a new application, the lifting of the extended CDO shall not preclude the issuance of another CDO, if after verification and investigation by the Commission, it is determined that the same acts complained of recommence within twelve (12) months from its lifting, subject to the penalties provided in Section 22 hereof. Beyond the said period, any future violation of the same adverse party shall warrant the filing of a new application for the issuance of a CDO.

RULE IV MISCELLANEOUS PROVISIONS

Section 19. Publication. The fact that a CDO has been issued and extended, after giving the Adverse Party the opportunity to be heard, may be published when warranted by public interest as determined by the Commission.

Section 20. Separate Proceedings. - The investigation by the CID or the compliance check or breach handling by the CMD shall be treated as a separate and distinct proceeding from the CDO proceeding.

Section 21. Cumulative Remedy. – The remedy available under these Rules shall be cumulative and in addition to, not exclusive of or in substitution for, any rights or remedies available to the applicant under the DPA, its IRR or other related issuances: Provided, that when an applicant simultaneously or successively files an application for a temporary ban and for a CDO, the proceeding on the application for the temporary ban shall be suspended until the proceeding on the CDO is decided.

Section 22. Penalties for Non-Compliance. – If upon monitoring and assessment, the Commission finds evidence of non-compliance, any natural or juridical person in violation of the orders issued under this Circular shall be subjected to fines and penalties as may hereafter be prescribed by the Commission; contempt proceedings, as may be permitted by law, before the appropriate court; and/or such other actions as may be available to the Commission.

Section 23. Application of Rules of Court. – The Rules of Court shall apply in a suppletory character, and whenever practicable and convenient.

Section 24. Interpretation. – These Rules shall be interpreted in a manner mindful of the rights and interests of the data subject while ensuring the free flow of information to promote innovation and growth.

Section 25. Separability Clause. – In the event that any provision or part of these Rules is declared unauthorized or rendered invalid, those provisions not affected by such declaration shall remain valid and in force.

Section 26. Transitory Provision. - These Rules shall govern all cases brought after its effectivity and further proceedings in pending cases, except to the extent that their application would not be feasible or cause injustice to any party.

Section 27. Effectivity. – These Rules shall take effect fifteen (15) days after publication in a newspaper of general circulation.

Approved: 06 October 2020

Sgd.
RAYMUND E. LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Frequently Asked Questions on the Draft Rules on the Issuance of Cease and Desist Orders (CDO)

1. Does Section 4(B) in laying one of the requisites for the issuance of a CDO as “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,” expand Section 7(C) of the Data Privacy Act (DPA) which provides that the National Privacy Commission (NPC) shall have the following functions, among others “Issue cease and desist orders, 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.”

No. At the outset, we note that this phrase is taken from Section 9(f)(3) of the Implementing Rules and Regulations (IRR) of the DPA which provides the functions of the NPC including “Enforcement: 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.”

The IRR, in adding the phrase “or if it necessary to preserve and protect the rights of data subjects” did not expand the DPA but rather limit the national security and public interest issue involved in data privacy cases, which is the protection and preservation of the rights of a data subject. The addition of such a phrase prevents the issuance of a CDO for national security and public interest cases outside the jurisdiction of the Commission.

What the IRR does in adding the term “protection and preservation of the rights of the data subject” is to merely contextualize the public interest issue within the jurisdiction of the NPC. This is sanctioned by law and jurisprudence, which states that “[a]dministrative [a]gencies may implement the broad policies laid down in a statute by “filling in” the details which the Congress may not have the opportunity or competence to provide” (Eastern Shipping Lines, Inc. v. POEA, G.R. No. 76633, October 18, 1988).

To be clear, before a CDO may be issued, an applicant must be able to prove that the issue falls under either of the two grounds of national security or public interest. Further, the national security or public interest issue must relate to the preservation and protection of the rights of data subjects.

2. The CDO is issued ex parte. Is this not a violation of the due process rule?

No. The CDO is an extraordinary remedy reserved only for those cases wherein the commission or continuance of a certain act or practice, unless restrained, will cause grave and irreparable injury to a data subject (Section 4(C), CDO Rules).

The due process requirement is satisfied by the provision ordering the Adverse Party to comment on the issued CDO (Section 9, CDO Rules) which shall be set for adjudication by the Commission En Banc (Section 12, CDO Rules). After giving the respondent the opportunity to be heard, the Commission will decide whether to extend or lift the CDO no later than thirty (30) days from the expiration of the period for the Adverse Party to file a comment or the termination of the clarificatory hearing if one is held. In the event that the Commission fails to render its decision within the said period, the CDO shall be deemed automatically lifted (Section 12, CDO Rules).

3. How can the NPC justify an ex parte CDO when the DPA does not authorize the NPC to issue the same?

Jurisprudence has recognized the implied power of quasi-judicial agencies to issue ex parte cease and desist orders in accordance with its mandate. While it is a fundamental rule that an administrative agency has only such powers as are expressly granted to it by law, it is likewise a settled rule that an administrative agency has also such powers as are necessarily implied in the exercise of its express powers. Otherwise, it may well be reduced to a “toothless” paper agency (*Laguna Lake Development Authority vs Court of Appeals*, GR 110120, March 16, 1994).

4. Can you further qualify “grave and irreparable injury” or set the criteria for said injury?

Jurisprudence provides that damages are irreparable when “there is no standard by which their amount can be measured with reasonable accuracy.” An irreparable injury which a court of equity will enjoin includes that degree of the wrong of a repeated and continuing kind which produces hurt, inconvenience, or damage that can be estimated only by conjecture, and not by any accurate standard of measurement. An irreparable injury to authorize an injunction consists of a serious charge of or is destructive to, the property it affects, either physically or in the character in which it has been held and enjoined, or when the property has some peculiar quality or use, so that its pecuniary value will not fairly recompense the owner of the loss thereof (*Power Sites and Signs Inc. vs. United Neon, etc.* G.R. 163406, November 24, 2009).

5. Is this similar to a preliminary injunction under Rule 58 of the Rules of Civil Procedure?

The purpose of a CDO and a preliminary injunction is the same. According to Section 5 of Rule 58 of the Rules of Court, the court allows the issuance of an injunction ex parte if shown in a verified application, that there is a grave and irreparable injury that would result before the matter is heard on notice. The purpose of Rule 58, specifically Section 5, is of the same purpose as that of a CDO.

6. What is the difference between a CDO and a temporary or permanent ban on the processing of personal information?

The CDO is an independent action that covers the processing of personal information and the conduct of any act or practice in violation of the DPA. It is commenced motu proprio by the Complaints and Investigation Division (CID) or the Compliance and Monitoring Division (CMD), or through a verified application by the aggrieved party upon recommendation by the CID. It is issued ex parte, after the conduct of verification and investigation. Upon issuance, it is immediately executory and shall remain in force until lifted or modified by the Commission.

On the other hand, a temporary or permanent ban on the processing of personal information is a provisional remedy which only covers the processing of personal information. It is commenced upon the filing of the complaint or at any time before the finality of a decision of the Commission. It is issued after a summary hearing and notice. Upon issuance, it shall remain in effect until the final resolution of the case, or upon further orders by the Commission or lawful authority. (Section 19, NPC Circular 16-03).

7. From a practical perspective, is there still a benefit to seeking a temporary or permanent ban on processing in relation to a complaint instead of applying for a CDO?

As there are different grounds in the issuance of CDO and the issuance of a temporary or permanent ban, a party cannot apply for a CDO if only the grounds in the issuance of a temporary or permanent ban are present.

8. Should this not be merely an accessory to an original action?

The application for CDO may or may not be attached to a complaint. An aggrieved party may file an application for a CDO without a complaint in instances where the ultimate remedy desired is the issuance of the CDO against the adverse party.

9. Section 5 of the CDO Rules provide “filing with the Commission of an application in writing.” Is there a specific office where this can be filed or will it be filed with the Office of the Privacy Commissioner and the two (2) Deputy Privacy Commissioners?

The application is filed with the “Commission” composed of the Privacy Commissioner and the two Deputy Privacy Commissioners through the NPC’s General Record Unit. Upon filing by an aggrieved party, the CID will first assess if the application is sufficient in form and substance before transmitting the same with its recommendation to the Commission. The Commission will ultimately decide on the propriety of the application and the necessity of the issuance of the CDO.

10. What is the standard of proof in the issuance of the CDO?

Substantial evidence is the standard of proof in the issuance of a CDO as it is also the standard of proof for final decisions of quasi-judicial agencies. Jurisprudence provides that “substantial evidence” is such “relevant evidence that a reasonable mind might accept as adequate to support a conclusion. Complainants in administrative proceedings carry the burden of proving their allegations with substantial evidence (De Jesus v. Guerrero III, G.R. No. 171491, September 4, 2019; Office of the Ombudsman v. Loving Fetalvero Jr., G.R. No. 211450, July 23, 2018).

11. How will the bond be computed? How can CID assess or estimate any potential damage that the PIC/Adverse Party may suffer due to malicious or erroneously issued CDO? What will be their basis?

The bond will be computed based on the assessment of the CID. Further details such as rules on the assessment of bond, the period within which the bond should be posted, and the effect of non-posting of the bond will be subject to another circular on fines, fees, and penalties.

12. Is it possible for the adverse party to file a counterbond?

No. By its nature, a counterbond discharges the writ of attachment enforced against the respondent. The counterbond shall secure the payment of any judgment that the attaching party may recover in the action (Section 12, Rule 57, Rules of Court). Since the CDO is an extraordinary remedy reserved only for those cases which fall under national security and public interest, and where the continued act of the respondent, unless restrained, would cause grave and irreparable injury, a counterbond may not be filed to discharge the CDO.

Allowing the respondent to file a counterbond to discharge the CDO will go against the policy of the state to protect national security and public interest. Moreover, damages are grave and irreparable when they are incapable of pecuniary estimation. Hence, filing a counterbond will not discharge the obligation of the respondent since the possible damage to the aggrieved party is grave and irreparable which is incapable of pecuniary estimation.

13. What is the rule on filing and service?

Rules on filing and service shall follow NPC Circular 16-04 or the Rules of Procedure of the NPC as may be amended. Currently, filing may be made personally or electronically while service may be made by personal or substituted service. If personal or substituted service is impossible, by private courier.

14. Explain the rationale behind the phrase “The lifting of the CDO shall not preclude the issuance of another CDO based on the same acts complained of, should such acts after lifting of the CDO, would then continue within twelve (12) months from its lifting.”

The phrase means that the Commission may issue another CDO only upon verification and investigation, without the need for a new application. This is to provide an immediate remedy in cases wherein the respondent will stop the acts complained of to lift the CDO, then resume the acts complained of shortly thereafter.

15. What happens if there is a CDO that refers to the same processing lodged as a complaint, breach notification, or compliance check, and the CID or CMD process is not yet done but the CDO has been executed already?

If there is a pending complaint or investigation under CID or if a compliance check or breach notification is pending with the CMD, and if there is an application for a CDO on the same matter, both can proceed independently of one another. They are separate proceedings.

16. Will a CDO be proper after a mere privacy sweep or document submission? Will a Data Breach Notification by itself be a good cause for the issuance of a CDO?

Every application will be decided on a case to case basis after the conduct of verification and investigation. A CDO may issue after or during the conduct of a compliance check or a data review breach notification if the Commission finds that the CDO is proper under the circumstances.

17. At which stage will the Complaints and Investigations Division (CID) recommend the issuance of a CDO? Is it possible the CID will recommend a CDO even before the order to confer for discovery?

The CID will not recommend the issuance of a CDO. Once an application is filed by an aggrieved party, the CID will only make a preliminary assessment to determine if the application is sufficient in form and substance. Ultimately, it is for the Commission to decide whether to grant the CDO or not.

18. What is the remedy if the CID does not recommend the filing of the application?

CID will only recommend whether the application is sufficient in form and substance. Upon its assessment, it will forward the application to the Commission together with its recommendation. Ultimately, it would still be the Commission that will decide on the propriety of the application and the necessity of issuing a CDO. If the application is then denied, the remedy is still against the decision of the Commission.

19. Does the rule on exhaustion of administrative remedies apply in this case?

No. Since an application for a CDO may proceed independently of a complaint, Section 4 of NPC Circular 16-04 does not apply. The CDO is an extraordinary remedy that will give an applicant immediate relief in cases where the stringent criteria under the law are met. Requiring the applicant to comply with the rule on exhaustion will defeat the main purpose of the application, which is to prevent a grave or irreparable injury.

20. What will be the basis of the CID for conducting a sua sponte investigation?

The NPC initiates an investigation of the circumstances surrounding a possible data privacy violation or personal data breach in cases of, but not exclusive to, matters that arose from pending cases before the NPC, reports from the daily news, trends or academic studies, information gathered from corroborated and substantiated anonymous tips or reports from other offices of the Commission.

21. The CDO also talks about “future action,” or “threatening to do something.” In this case, how will this fall under the jurisdiction of the NPC if there is no violation, to begin with?

The CDO is an extraordinary remedy and by its nature a remedy to prevent grave and irreparable injury. Since the purpose is to prevent said injury, future actions, by implication, are covered by the Rules. Future actions that, if not prevented, will cause grave or irreparable injury are actions which the CDO ultimately intends to enjoin.

22. Can a CDO be immediately published regardless of the public interest or public education?

For publication of Decisions, the Commission has released NPC Advisory 2020-01 on “Protocols for the Publication of Decisions, Resolutions, and Orders On the NPC Website.” Section 1, “Scope of Publication” provides,

a) These guidelines shall cover all Commission Decisions, Resolutions, and Orders issued by the Commission En Banc.

b) The following shall not be published on the NPC website:

(i) Cases decided based on compromise agreements, mediated settlement agreements, quitclaims, and other modes of alternative dispute resolutions as these are not decided based on merit and therefore lack teaching value for the public

(ii) Interlocutory Decisions, Orders, and Resolutions that do not dispose of the case or breach notification with finality.

(iii) Decisions, Orders, and Resolutions that may be subject of a Motion for Reconsideration, unless the reglementary period to file such has lapsed.

c) Notwithstanding the enumeration in paragraph (b), the Commission may, at its discretion, publish Decisions, Orders and Resolutions where public interest warrants or for the education of the public.

However, in the case of a CDO, the publication is only after allowing the Adverse Party to be heard and is only limited to instances of public interest as determined by the Commission.

23. Does the “Aggrieved Party” include a juridical person? May the corporation file a petition for issuance of CDO on behalf of its employees?

No, an aggrieved party or a data subject as contemplated by the DPA only refers to a natural person, privacy being a fundamental human right. (Advisory Opinion No. 2017-006) However, according to NPC Circular 16-04, a natural person may be represented by a juridical person (Section 3).

24. May the aggrieved party be represented by counsel?

Yes, based on the suppletory application of the Rules of Court as well as NPC Circular 16-04.

25. Does this apply to online sellers, who due to the quarantine restrictions are maximizing mobile banking and online transactions?

Yes, these Rules apply to every personal information controller or processor.

26. How will the penalties or fines be imposed? Will there a table of penalties to be included in this circular or referred to?

The penalties, fees, fines, as well as the determination of the bond will be subject to a separate Circular.

NPC Circular No. 2020-03

DATE: 23 December 2020

SUBJECT: DATA SHARING AGREEMENTS

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, 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 secured and protected;

WHEREAS, Section 21(a) of the Data Privacy Act of 2012 states that a personal information controller 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, Section 20 of the Implementing Rules and Regulations of the Data Privacy Act of 2012 provides that further processing of personal data collected from a party other than the data subject shall be allowed under certain conditions;

WHEREAS, pursuant to Section 7 of the Data Privacy Act of 2012, the National Privacy Commission is charged with the administration and implementation of the provisions of the law, which includes ensuring the compliance by personal information controllers with the provisions of the Act, 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 Data Privacy Act of 2012 provides that, among the Commission’s functions, is to develop, promulgate, review or amend rules and regulations for the effective implementation of the Act;

WHEREFORE, in consideration of these premises, the National Privacy Commission hereby issues this Circular governing data sharing agreements.

SECTION 1. Scope.— The provisions of this Circular apply to personal data under the control or custody of a personal information controller (PIC) that is being shared, disclosed, or transferred to another PIC. The Circular likewise applies to personal data that is consolidated by several PICs and shared or made available to each other and/or to one or more PICs.

It excludes arrangements between a PIC and a personal information processor (PIP).

SECTION 2. Definition of Terms. — For the purpose of this Circular, the following terms are defined, as follows:

A. “Act” or “DPA” refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012;

B. “Commission” or “NPC” refers to the National Privacy Commission;

C. “Compliance Check” refers to the systematic and impartial evaluation of a PIC or PIP, in whole or any part, process or aspect thereof, to determine whether activities that involve the processing of personal data are carried out in accordance with the standards mandated by the Data Privacy Act and other issuances of the Commission. It is an examination, which includes Privacy Sweeps, Documents Submissions and On- Site Visits, intended to determine whether a PIC or PIP is able to demonstrate organizational commitment, program controls and review mechanisms intended to assure privacy and personal data protection in data processing systems.

D. “Consent of the data subject” refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent is evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so;

E. “Data Protection Officer” or “DPO” refers to an individual designated by the head of agency or organization to be accountable for its compliance with the Act, its IRR, and other issuances of the Commission: provided, that

a government agency or private entity may have more than one DPO;

F. “Data sharing” 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 controller/s.

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;

G. “Data Sharing Agreement” or “DSA” refers to a contract, joint issuance, or any similar document which sets out the obligations, responsibilities, and liabilities of the personal information controllers involved in the transfer of personal data between or among them, including the implementation of adequate safeguards for data privacy and security, and upholding the rights of the data subjects: provided, that only personal information controllers should be made parties to a data sharing agreement;

H. “Data subject” refers to an individual whose personal, sensitive personal, or privileged information is processed;

I. “Encryption method” refers to the technique that renders data or information unreadable, ensures that it is not altered in transit, and verifies the identity of its sender;

J. “Government Agency” refers to a government branch, body, or entity, including national government agencies, bureaus, or offices, constitutional commissions, local government units, government-owned and controlled corporations, government financial institutions, state colleges and universities;

K. “IRR” refers to the Implementing Rules and Regulations of Republic Act No. 10173;

L. “Middleware” refers to any software or program that facilitates the exchange of data between two applications or programs that are either within the same environment, or are located in different hardware or network environments;

M. “Personal data” refers to all types of personal information and sensitive personal information;

N. “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;

O. “Personal information controller” or “PIC” refers to a natural or juridical person, or any other body, who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
2. A natural person who processes personal data in connection with his or her personal, family, or household affairs;

There is control if the natural or juridical person or any other body decides on what information is processed, or the purpose or extent of its processing.

P. “Personal information processor” or “PIP” refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data;

Q. “Private entity” refers to any natural or juridical person, or any other body that is not a unit of the Philippine government or any other foreign government entities, such as but not limited to, stock and non-stock corporations, foreign corporations, partnerships, cooperatives, sole proprietorships, or any other legal entity.

R. “Privileged information” refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication;

S. “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 individual, 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 is 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.

T. “Subcontracting” refers to the outsourcing, assignment, or delegation of the processing of personal data by a personal information controller to a personal information processor. In this arrangement, the personal information controller retains control over the processing.

U. “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 principles. — Data sharing arrangements are executed between or among PICs only, and are governed by the following principles:

A. Adherence to the data privacy principles of transparency, legitimate purpose, and proportionality;

B. Fulfilment of all applicable requirements prescribed by the Act, its IRR, and other issuances of the Commission;

C. Recognition of and upholding the rights of affected data subjects, unless otherwise provided by law;

D. Ensuring that the shared and collected data are accurate, complete, and where necessary for the declared, specified, and legitimate purpose, kept up to date; and

E. Implementation of 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.

SECTION 4. Parties. — Only PICs can be parties to data sharing arrangements. This is the case even where the actual sharing will transpire between a PIC and a PIP acting on behalf of, or upon the instructions of, another PIC.

SECTION 5. Transparency. — Each affected data subject should be provided with the following information before personal data is shared or at the next practical opportunity, through an appropriate consent form or privacy notice, whichever is applicable or appropriate to the lawful basis relied upon:

A. Categories of recipients of the personal data: provided, that PICs shall

provide a data subject with the identity of the recipients, upon request;

B. Purpose of data sharing and the objective/s it is meant to achieve;

C. Categories of personal data that will be shared;

D. Existence of the rights of data subjects; and

E. Other information that would sufficiently inform the data subject of the nature and extent of data sharing and the manner of processing involved.

In cases where consent is not required, a privacy notice is sufficient. Where the PIC has already collected the personal data, it should provide the data subjects with the information above as soon as it decides that personal data will be shared or as soon as possible afterwards.

It is a good practice for PICs to review their privacy notice regularly to ensure that it continues to reflect accurately the data sharing arrangement they are engaged in.

SECTION 6. Authorized processing. — Data sharing may be based on any of the criteria for lawful processing of personal data in Sections 12 and 13 of the Act: provided, that nothing in this Circular shall be construed as prohibiting or limiting the sharing, disclosure, or transfer of personal data that is already authorized or required by law.

SECTION 7. Special cases. — Data sharing may also be allowed pursuant to Section 4 of the Act, which specifies the special cases wherein the law and the rules are not applicable, but such data sharing should only be to the minimum extent necessary to achieve the specific purpose, function, or activity, and subject to the requirements of applicable laws, regulations, or ethical standards.

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.

SECTION 9. Contents of a Data Sharing Agreement.— The following constitute the contents of a DSA:

A. Purpose and lawful basis. It specifies the purpose/s of the data sharing and the appropriate lawful basis.

B. Objectives. It identifies the objective/s that the data sharing is meant to achieve.

C. Parties. It identifies all PICs that are party to the DSA and, for each party, specifies the following:

1. Type of personal data it will share, if any;
2. Whether the personal data processing will be outsourced, including the types of processing PIPs or service providers will be allowed to perform;
3. Method to be used for the processing of personal data; and
4. Designated data protection officer.

D. Term. It specifies the term or duration of the data sharing arrangement which will be based on the continued existence of the purpose/s of such arrangement. Perpetual data sharing or DSAs that have indeterminate terms are invalid. Parties are free to renew or extend a DSA upon its expiration. The DSA should be subject to the conduct of periodic reviews which should take into consideration the sufficiency of the safeguards implemented for data privacy and security.

E. Operational details. It provides an overview of the operational details of the data sharing, including the procedure the parties intend to observe in implementing the same. If the recipient will be allowed to disclose the shared data, or grant public access to the same, this must be established clearly in the DSA, including the following details:

1. Justification for allowing such access;
2. Parties that are granted access;
3. Types of personal data that are made accessible; and
4. Estimated frequency and volume of such access.

Where disclosure or public access is facilitated by an online platform, the program, middleware, and encryption method that will be used should also be identified.

Any other information that would sufficiently inform the data subject of the nature and extent of data sharing and the manner of processing

involved should also be provided.

F. Security. It includes a description of the reasonable and appropriate organizational, physical, and technical security measures that the parties intend to adopt to ensure the protection of the shared data. The parties should also establish a process for data breach management.

G. Data subjects' rights. It provides for mechanisms that allow affected data subjects to exercise their rights relative to their personal data, including:

1. Identity of the party or parties responsible for addressing: information requests, complaints by a data subject, and/or any investigation by the NPC: provided, that the NPC shall make the final determination as to which party is liable for any violation of the Act, its IRR, or any applicable NPC issuance; and
2. Procedure by which a data subject can access or obtain a copy of the DSA: provided, that the parties may redact or prevent the disclosure of trade or industrial secrets, confidential and proprietary business information, and any other detail or information that could endanger or compromise their information systems, or expose to harm the confidentiality, integrity, or availability of personal data under their control or custody.

H. Retention and Data Disposal. It includes rules for the retention of shared data and identify the method that will be adopted for the secure return, destruction, or disposal of the shared data and the timeline therefor.

The parties may specify any other stipulations, clauses, terms and conditions as they may deem appropriate: provided, that they are not contrary to law, morals, public order, or public policy.

SECTION 10. Record of data sharing arrangements. — Each PIC should establish and maintain a record of its data sharing arrangements, including the following:

- A. Contact details of all parties, including their respective data protection officers;
- B. Legal bases for the data sharing arrangement/s;
- C. Copy of the DSA/s, if executed;
- D. Written, recorded, or electronic proof of the consent obtained from data subjects, where applicable; and
- E. Date and/or time consent was obtained and withdrawn, where applicable.

Such record will allow the effective management of the PIC's third-party engagements. It should be kept accurate and up to date to allow the PIC to address any related inquiries and to demonstrate its compliance with the DPA.

SECTION 11. Security of shared personal data. — Adequate safeguards to protect personal data should be put in place in every data sharing arrangement, subject to the conditions set forth under Section 9 above.

Where online access to personal data is granted, the parties should ensure that said access is secure through the use of any appropriate program, software, or any other appropriate means, such as the use of a secure encrypted link or a middleware.

SECTION 12. Accountability. — All parties to a data sharing arrangement should comply with the Act, its IRR, this Circular, and all applicable issuances of the Commission. Subject to the terms of the DSA, each party will be responsible for any personal data under its control or custody, including those where the processing has been outsourced or subcontracted to a PIP. This extends to personal data each party shares with or transfers to a third party located outside the Philippines, subject to cross-border arrangement and cooperation.

The DPOs of the parties will sign as witnesses to the DSA.

SECTION 13. Review by the Commission.— Data sharing, whether or not covered by a DSA, may be subject to review by the Commission, on its own initiative or upon a verified complaint by an affected data subject.

SECTION 14. Periodic review. — Parties to data sharing, whether or not covered by a DSA, should subject the same to periodic reviews to determine the propriety of continuing the data sharing, taking into account the sufficiency of the safeguards implemented for data protection and any data breach or security incident that may have occurred affecting the shared data.

The terms and conditions of a DSA may be subject to review by the parties thereto upon the expiration of its term, and any subsequent extensions thereof. In reviewing the DSA, the parties should document and include in its records:

- A. the reason for terminating the agreement or, in the alternative, for renewing its term; and
- B. in case of renewal, any changes made to the terms and conditions of the agreement.

SECTION 15. Revisions and amendments.— Changes to DSAs while it is still in effect should follow the same procedure observed in the creation of a new agreement.

SECTION 16. Termination. — A data sharing may be terminated:

- A. upon the expiration of its term, or any valid extension thereof;
- B. upon the agreement by all parties;
- C. upon breach of any provisions of the DSA by any of the parties;
- D. upon dissolution or death of the PIC;
- E. upon a finding by the Commission that data sharing is:
 - 1. no longer necessary for the specified purpose/s and its objective/s has already been achieved; or
 - 2. detrimental to national security, public interest or public policy, or the termination of the same is necessary to preserve and protect the rights of a data subject.

Nothing in this Section prevents the Commission from ordering *motu proprio* the termination of any data sharing, whether or not covered by a DSA, when a party is determined to have violated the Act, its IRR, or any applicable issuance by the Commission.

SECTION 17. Return, destruction, or disposal of transferred personal data. — Unless otherwise provided by the DSA, all personal data transferred to other parties by virtue of a data sharing, whether or not covered by a DSA, should be returned, destroyed, or disposed of, upon the termination of the arrangement.

SECTION 18. Transitory period. — Where an existing data sharing is not covered by any written contract, joint issuance, or any similar document, the parties thereto may execute or enter into an appropriate agreement, subject to the considerations set forth under Section 8 of this Circular.

All existing DSAs should be reviewed by the concerned parties to determine compliance with the provisions of this Circular and make the necessary revisions or amendments, as may be appropriate.

In all cases, the PIC that collected the personal data directly from the data subjects should, at the soonest practicable time, notify and provide the data subjects whose personal data were shared, transferred, or disclosed with all the information set out in Section 5 of this Circular: provided, 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: provided further, that the PIC should establish means through which the data subjects can exercise their rights and obtain more

detailed information relating to the DSA.

SECTION 19. Separability Clause. — If any portion or provision of this Circular is declared invalid or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 20. Repealing Clause. —This Circular supersedes in its entirety NPC Circular No. 16-02. 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 21. Effectivity. —This Circular takes effect fifteen (15) days after its publication in the Official Gazette or two newspapers of general circulation.

Approved:

Sgd.
RAYMUND E. LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner



DECISIONS

MRS,
Complainant,

-versus-

NPC Case No. 18-152
For: Violation of the Data
Privacy Act of 2012

**NATIONAL CONCILIATION
AND MEDIATION BOARD
(NCMB) AND DEPARTMENT
OF LABOR AND
EMPLOYMENT (DOLE)**
Respondents.

X-----X

DECISION

AGUIRRE, D.P.C.:

Before this Commission is a Complaint filed by Complainant MRS against Respondents National Conciliation and Mediation Board (NCMB) and Department of Labor and Employment (DOLE) for an alleged violation of Republic Act No. 10173 (“Data Privacy Act”).

The Facts

Sometime in August 2013, Complainant filed a complaint against her employer for nonpayment of her 13th month pay upon termination of her employment. With the help of Respondents, the settlement between Complainant and her employer was completed in her favor.

In her complaint, Complainant narrates:

I had the impression that this mediation effort of DOLE was private until I searched my name on Google and my name appearing on the search in this link describing my alleged constructive dismissal. x x x The article describes my complaint to DOLE and how it was resolved. Although the term “alleged” was used, it is still damaging to me because it has affected my job applications after that because all they understand is I have a bad record when I thought this was resolved when I was asked to file a resignation instead.¹

She attached to her Complaint the article entitled “NCMB settles labor issues; 10 workers receive P215K thru SENA”. The pertinent portion of the article reads:

“These worker-complainants were attended to by our conciliator mediators, acting as single entry assistance desk officers find mutually acceptable and beneficial solutions to their complaints,” [NCMB Executive Director] said.

He specifically cited [Complainant], senior analyst of Phinma/Trans-Asia Oil who came to complain of alleged constructive dismissal. She also sought assistance for the collection of her unpaid overtime pay and service incentive leave.² xxx

Complainant thereafter filed this complaint with the National Privacy Commission (NPC) for the removal of the article, stating:

I am currently employed but would like this article taken out of then (sic) internet because it might affect my future career plans should I choose to search for a new job. I understand that the DOLE would like to make known their credentials in being effective mediators but this has been five (5) years ago and believe this is already irrelevant.³

¹ Complaint dated 02 October 2018

² <https://co.ncmb.ph/ncmb-settles-labor-issues-10-workers-receive-p-215-kthrusena/?print=pdf>, cited in Note 1

³ Supra at Note 1

Upon the filing of the complaint, Complainant was advised by the Complaints and Investigation Division (CID) to give Respondent the opportunity to address her complaint by informing them of her data privacy concern.

Complainant subsequently sent letters to Respondents informing them of her concerns and requesting for the removal of the article from their website.

In the meantime, the case was scheduled for Discovery Conference on 15 November 2018.⁴

Respondent NCMB promptly replied to Complainant's letter on 08 October 2018. They stated that:

In line with this, please be informed that said article has already been deleted in our website. We apologize on (sic) the anxieties this matter caused you specifically on your concern that it might taint your reputation in the eyes of potential employers. The Board does not intend to cause you any distress nor to malign your name. The article was written merely to highlight the success stories in our program implementation. However, we overlooked the aspect of consulting and seeking your permission in posting the article.⁵

On 8 November 2018, Complainant sent an email to the NPC stating:

DOLE has already removed the information they posted online. I will forward their official communication tomorrow. The situation has been resolved. There is no need for further action. Thank you for your assistance!

Consequently, none of the parties appeared at the Discovery Conference on 15 November 2018.

A few months after, Respondent NCMB furnished NPC with a letter that it sent to Google requesting for the permanent removal of the link to the published article from Google's search engine.

Issue

Whether or not Respondent NCMB and DOLE are liable for a violation of the Data Privacy Act of 2012. Discussion

⁴ Order to Confer for Discovery, n.d.

⁵ Letter from the NCMB dated 08 October 2018.

Discussion

Respondents are not liable for a violation of the Data Privacy Act of 2012.

NPC Circular 16-04 (“Rules of Procedure”) provides that complaints may be dismissed outright for the following grounds:

1. The complainant did not give the respondent an opportunity to address the complaint, unless failure to do so is justified;
2. The complaint is not a violation of the Data Privacy Act or does not involve a privacy violation or personal data breach;
3. The complaint is filed beyond the period for filing; or
4. There is insufficient information to substantiate the allegations in the complaint or the parties cannot be identified or traced.⁶

At the time Complainant filed her complaint with the NPC, she had not yet exhausted her remedies with Respondent. Prior to seeking assistance from the NPC, she had not made any communication with Respondent to request the deletion of the article that mentions her name.

The Commission emphasizes 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. This is in line with a separate provision in the NPC Rules of Procedure that states thus:

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 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 controller within fifteen (15) days from receipt of information from the complainant; xxx ⁷

⁶ Section 12, NPC Circular 16-04. Dated 15 December 2016. Emphasis supplied.

⁷ Ibid at Section 4.

In this case, it can be seen that as soon as Complainant communicated her request, Respondent promptly acted thereon and caused the deletion of the article from their website and even coordinated with Google Philippines to facilitate the permanent removal of the link from their search engine.

The resolution of the Complaint among the parties is confirmed with the Complainant's email to NPC stating "the situation has been resolved. There is no need for further action."

WHEREFORE, all the above premises considered, the Commission hereby resolves to **DISMISS** the complaint filed by MRS against Respondent National Conciliation Mediation Board and Respondent Department of Labor and Employment.

SO ORDERED.

Pasay City, 8 June 2020.

(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

MRS

Complainant

**NATIONAL COMMISSION AND
MEDIATION BOARD**

Respondent

4th-6th Floor, Arcadia Building, 860 Quezon
Avenue,
Brgy. Paligsahan, Quezon City 1103
ncmbco@yahoo.com
ncmbco@gmail.com

DEPARTMENT OF LABOR & EMPLOYMENT

Respondent

(DOLE) Building, Muralla Wing cor.
General Luna St., Intramuros, Manila,
1002, Philippines

COMPLAINTS AND INVESTIGATION DIVISION

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

HNT

Complainant,

-versus-

NPC 18-155

For: Violation of the Data
Privacy Act of 2012

EASTWEST BANK

Respondents.

X-----X

DECISION

Before this Commission is a complaint filed by Complainant HNT against Respondent Eastwest Bank for an alleged violation of the Data Privacy Act of 2012.

In his complaint, Complainant states:

I applied for an Eastwest Bank credit card through x x x their credit card sales agent. The application was approved when I got my card. My biggest problem now is that he has been using my name to encourage applications from my Facebook friends and colleagues, and worst, to our HR employees who are my Facebook friends too. I called his attention already but he continuously used it as a practice to get the customers attention and he uses and drops my name to associate it with him x x x My application was for myself and not for other people. I am depressed, humiliated and I feel really bad about this incident.¹

The parties were ordered to appear at a Discovery Conference on 06 June 2019, 2 but both parties failed to appear.³ The Discovery Conference was reset to 18 July 2019. Only Respondent, through counsel, appeared and manifested that they are willing to reschedule for a possible mediation.⁴ The Discovery Conference was reset to 22 August 2019.⁵

¹ Complaint dated 04 October 2018.

² Order dated 13 April 2019.

³ Order dated 13 June 2019.

⁴ Order to Confer for Discovery dated 18 July 2019.

⁵ Ibid.

On 6 August 2019, Complainant filed an Urgent Motion for Postponement stating that he failed to receive the Order setting the conference on 18 July 2019, and that he was not available for the forthcoming one on 22 August. He prayed for the Conference to be reset on either 28 or 29 August.⁶

The Discovery Conference was held on 28 August, where both parties appeared. Each party manifested their willingness to explore the possibility of settling their dispute through mediation.⁷

The complaint proceedings were thus suspended and the parties were ordered to appear before the mediation officer for the preliminary mediation conference.⁸ Due to the parties' failure to appear for two (2) consecutive mediation conferences, the mediation officer issued a Notice of Non-Settlement of Dispute on 31 October 2019. The parties were then ordered to appear for the resumption of the complaint proceedings.⁹

On 6 December 2019, Complainant appeared for the Discovery Conference and manifested that the parties already executed a Settlement Agreement dated 17 October 2019. He attested, verified and confirmed that he knowingly, willingly and voluntarily entered into the settlement.¹⁰ After examining the document, however, the investigating officer noted that the Settlement was not sworn before an administering officer. The parties were then given fifteen (15) days to submit a notarized Settlement Agreement.¹¹

On 22 January 2020, the parties submitted a notarized settlement agreement where they agreed to the following terms:

1. Complainant agrees to accept payment in the form of a personal check...in the amount of Fifty Thousand Pesos (Php50,000.00), which check will be given by respondent Bank within ten (10) days from notice of the confirmation of this Agreement by the Honorable Commission;
2. Complainant hereby acknowledges that he has no cause of action, complaint, claim or case, whether alone or jointly with one another, against the Bank, in respect to any matter relative or

⁶ Urgent Motion for Postponement dated 30 July 2019.

⁷ Application for Mediation dated 28 August 2019.

⁸ Order to Mediate dated 28 August 2019.

⁹ Order for Resumption of Complaint Proceedings dated 31 October 2019.

¹⁰ Order dated 06 December 2019.

¹¹ Ibid.

incident to or arising out of the incident which leads to the filing of this Complaint. Complainant further warrant that he will not instate any action, whether alone or jointly with one another, and will not continue to prosecute any pending action, if any, against the Bank, its principals, affiliates, subsidiaries and related companies, their stockholders, directors, agents, officers or employees;

3. Complainant hereby remise, release and forever discharge, and by these presents do, for himself, is heirs, successors and assignees, remise, release, and forever discharge the Bank and ECR Card Marketing Inc., and its principal, affiliates, subsidiaries and related companies, its stockholders, directors, officers, agents, or employees xxx
6. Complainant agrees that the Bank may bring action to seek an award for damages resulting from his breach of this Mediated Settlement Agreement;
7. Complainant further declares that he has read and fully understood this entire document and the Mediated Settlement Agreement hereby given is made by the Complainant willingly and voluntarily and with full knowledge of his rights under the law;
8. With the signing of this Compromise Agreement, parties jointly pray that CID Case 18-J-155 be dismissed and terminated;
9. Parties jointly move that the Honorable Commission approve this Mediated Settlement Agreement and respectfully pray that a judgment based on the Mediated Settlement Agreement be rendered by the Honorable Commission in the above entitled case.¹²

It is the mandate of the Commission to settle disputes through the use of alternative dispute resolution processes.¹³ The Commission also recognizes the policy of the State to actively promote party autonomy in the resolution of disputes and the freedom of the parties to make their own arrangements to resolve their disputes.¹⁴

In this case, it was Complainant himself who appeared before the Commission to manifest and submit the Settlement Agreement executed by and between the parties and to attest to the voluntariness

¹² Mediated Settlement Agreement filed on 22 January 2020.

¹³ Section 7(b), R.A. 10173.

¹⁴ Section 2, Republic Act No. 9285 (Alternative Resolution Dispute Act of 2004)

of its execution. The Commission finds the document to have been willingly and voluntarily executed, without any indication of fraud, deception, or misrepresentation.

The Commission also notes that a voluntary settlement between parties is considered as one of the grounds for a Motion to Dismiss under the Rules of Court, thus:

Section 1. Grounds. Within the time for but before filing the answer to the complaint or pleading asserting a claim, a motion to dismiss may be made on any of the following grounds:

xxx

(h) That the claim or demand set forth in the plaintiff's pleading has been paid, waived, abandoned, or otherwise extinguished.¹⁵

WHEREFORE, all these premises considered, this Commission resolves to **DISMISS** the complaint filed by HNT against Respondent Eastwest Bank.

SO ORDERED.

Pasay City, 8 June 2020.

(sgd)

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

WE CONCUR::

(sgd)

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

(sgd)

JOHN HENRY DU NAGA

Deputy Privacy Commissioner

¹⁵ The 1997 Rules of Procedure, Rule 16

BEM,
Complainant,

-versus-

NPC 18-046
For: Violation of the Data
Privacy Act of 2012

GFC
Respondents.

X-----X

DECISION

LIBORO, P.C.:

Before the Commission is a Complaint filed by BEM (“Complainant”) against respondent GFC (“Respondent”) dated 01 June 2018 for alleged violations of the Data Privacy Act of 2012.

Facts of the Case

In her Complaints-Assisted Form,¹ Complainant alleged that on 09 May 2018, she submitted her resignation letter through the Respondent, a work colleague. However, instead of forwarding this letter to the management, the Respondent allegedly took a picture of the resignation letter and circulated said photo in a Facebook Messenger group chat where the members were Complainant’s coemployees.

Complainant further alleged that she received from an unnamed individual a screenshot of the said group chat where members ridiculed the contents of Complainant’s resignation letter. This incident caused her anguish and humiliation which affected not

only her work environment, but also her daily life.

Aggrieved, Complainant filed this instant complaint on 01 June 2018, alleging, among others, that the unauthorized distribution of the contents of her resignation letter, a confidential document, was in violation of the Data Privacy Act, its implementing rules and regulations, and relevant issuances.

Facts of the Case

In her Complaints-Assisted Form,¹ Complainant alleged that on 09 May 2018, she submitted her resignation letter through the Respondent, a work colleague. However, instead of forwarding this letter to the management, the Respondent allegedly took a picture of the resignation letter and circulated said photo in a Facebook Messenger group chat where the members were Complainant's coemployees.

Complainant further alleged that she received from an unnamed individual a screenshot of the said group chat where members ridiculed the contents of Complainant's resignation letter. This incident caused her anguish and humiliation which affected not only her work environment, but also her daily life.

Aggrieved, Complainant filed this instant complaint on 01 June 2018, alleging, among others, that the unauthorized distribution of the contents of her resignation letter, a confidential document, was in violation of the Data Privacy Act, its implementing rules and regulations, and relevant issuances.

On July 4, 2018, the Commission's Complaints and Investigation Division (CID) issued to both parties an Order to Confer for Discovery² pursuant to Section 13 of NPC Circular 16-04.

Only the Respondent appeared during the Discovery Conference Hearing on 14 March 2019. Pursuant to Section 15 of NPC Circular 16-04, Respondent was ordered to submit her responsive comment to the complaint which she failed to comply. Consequently, the complaint was endorsed before this Commission for adjudication.

Issue

The sole question to be answered is whether or not the Respondent violated any provisions of the Data Privacy Act of 2012, its implementing rules and regulations, and relevant issuances in light of the foregoing circumstances.

Discussion

Upon consideration of the totality of evidence presented, this

Commission rules in the negative.

In our jurisdiction, basic is the rule that allegation is not tantamount to proof.³ Hence, the burden is on the Complainant to prove the allegations in her complaint.⁴ Moreover, in cases filed before quasi-judicial bodies, the quantum of proof required is substantial evidence⁵ which 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.⁶

In the instant case, the Complainant merely filed her complaint without introducing documentary or testimonial evidence as attachments. She was given an ample opportunity to be heard, to gather evidence, and to substantiate her complaint by attending Discovery Conference Hearings. Despite this, Complainant failed to appear without any reason.

The Commission is bound to adjudicate complaints based on the evidence presented pursuant to Section 22 of NPC Circular No. 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 this case, Complainant did not adduce material pieces of evidence that would reasonably establish liability on the part of the Respondent. She was not able to prove the existence of the group chat where the photo was supposedly circulated, nor was she able to prove the existence of the alleged photo of her resignation letter.

In the case of *Agdeppa vs Ombudsman*⁷ it was held that “Charges based on mere suspicion and speculation 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”.

Guided by the foregoing postulates, this Commission finds that there exists no substantial evidence establishing that Respondent committed the alleged violations of the Data Privacy Act. Accordingly, the complaint should be dismissed for lack of merit. Finally, the Commission reminds all employers to have a clear policy on the proper handling of confidential documents

² Id. at p. 9

³ *Alcedo v. Sagundang*, G.R. No. 186375, June 17, 2015.

⁴ *Miro v. Mendoza*, G.R. Nos. 172532 172544-45, November 20, 2013.

⁵ *Philippine National Bank v. Gregorio*, G.R. No. 194944, September 18, 2017.

⁶ *Montemayor v. Bundalian*, G.R. No. 149335, July 1, 2003.

⁷ *Agdeppa v. Office of the Ombudsman*, G.R. No. 146376, April 23, 2014. (Emphasis supplied.)

such as resignation letters to prevent the occurrence of similar incidents. Data protection and security, or the lack thereof, have profound effects on the lives of individuals. Hence, employers should always promote privacy protection as an organizational value for the mental, emotional, and professional wellbeing of its personnel.

WHEREFORE, premises considered, the instant case is hereby **DISMISSED** for failure of Complainant BEM to substantiate and prove the allegations in her complaint, without prejudice to the filing of appropriate civil, criminal or administrative cases against the Respondent GFC before any other forum or tribunal, if any.

SO ORDERED.

Pasay City, Philippines;
09 June 2020.

(Sgd.)

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner
Deputy

(Sgd.)

JOHN HENRY D. NAGA
Deputy Privacy Commissioner

JVA,
Complainant,

-versus-

NPC Case No. 19-498
(Formerly CID Case No. 19-498)
For: Violation of the Data
Privacy Act of 2012

**U-PESO.PH LENDING
CORPORATION (UPESO)**
Respondents.

X-----X

DECISION

AGUIRRE, D.P.C.:

Before this Commission is a Complaint filed by Complainant JVA against Respondent U-PESO.PH Lending Corporation (“UPESO”) for an alleged violation of R.A. 10173 (“Data Privacy Act”).

The Facts

Complainant is a borrower who obtained a loan from UPESO through their online lending application. Prior to this complaint, Complainant had settled three (3) previous obligations. On 11 April 2019, Complainant successfully obtained his fourth loan from respondent and has made several partial payments. However, Complainant was not able to fully settle his obligation and after several follow-ups, he could no longer be contacted.¹

Complainant alleges harassment, threats, and damage to his reputation

¹ Comment dated 15 November 2019, p. 2.

caused by the Respondent.² He alleges that he learned about the violation from his friends who received messages from Respondent, thus:

Nagmessage po yung mga kasama ko na hinahanap ako at may warrant na daw ako at makukulong na daw po ako.³

Explaining how these messages affected him, the Complainant states:

Apektado po ako ng sobra. Hindi po ako makatulog at hindi ako makapasok sa trabaho dahil sab anta nila na sasampahin ako ng warrant at ipihiya [sic] sa trabaho ko.⁴

The Complainant indicates in the Complaint that he is seeking an Order to temporarily stop the processing of his data, because “his life and his work is affected.”⁵

The parties were ordered to appear on 19 August 2019 for a Discovery Conference.⁶ During the Discovery Conference, both parties manifested their willingness to explore the possibility of amicable settlement through mediation. The investigating officer caused the parties to sign an application for mediation and issued an order to mediate. The parties were endorsed to the mediation officer to commence the mediation proceedings.

Since the Complaint included an application for a temporary ban on the processing of his personal information, an order for summary hearing was issued on the same date. The initial date of the summary hearing was, however, rescheduled due to the pendency of the mediation proceedings

During mediation, Complainant failed to appear without prior notice and justifiable reason for two (2) consecutive conferences. Thus, mediation was terminated without the parties arriving at a settlement and the complaint proceedings were resumed.⁷

At the Discovery Conference held on 06 November 2019, only Respondent appeared. They manifested that they will not be requiring any document or evidence from Complainant. Respondent was thus ordered to submit their responsive comment.

On the same day, a second Order for Summary Hearing was issued requiring the parties to appear on 29 November 2019 in connection with Complainant’s application for a temporary ban on the processing

of his information. Despite this Order, none of the parties appeared. An Order

² Complaints-Assisted Form dated 8 July 2019, p. 3.

³ Ibid., at p. 4.

⁴ Ibid., at p. 6.

⁵ Ibid., at p. 7.

⁶ Order to Confer for Discovery dated 23 July 2019.

⁷ Order for Resumption of Complaint Proceedings dated 06 November 2019.

was thereafter issued requiring Respondent to submit its memorandum stating why a temporary ban should not be issued but Respondent failed to submit. There being no other submissions made, the investigation of the case was terminated and all pending matters were endorsed for adjudication.

Arguments of the Parties

In their Comment, Respondent argues for the dismissal of the Complaint due to the repeated non-appearance of Complainant during mediation proceedings, applying the Rules of Court provisions on the dismissal of cases due to the fault of plaintiff.⁸ Respondent also avers that Complainant has not exhausted administrative remedies prior to the filing of the Complaint, as required under NPC Circular 16-04.⁹

Respondent further argues that there is no violation of the Data Privacy Act of 2012. In their Comment, they state:

The Step-by-Step Process in Loan Application of UPESO shows that it is the Complainant herself who entered the personal information required by UPESO in order to process the loan including the information of the Contact Person/s as the case may be. Furthermore, the said process flow also shows that the Complainant has consented for UPESO to have access to her contacts on her phone.¹⁰

The Respondent cites several portions of the Terms and Conditions and Loan Agreement to illustrate Complainant's consent as their lawful basis to process.¹¹ Among those they cite are the provisions on Waivers and Data Privacy:

38) Finally the Loan Agreement with UPESO provides:

12. Waivers. 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 the terms and conditions of this Loan Agreement.

⁸ Rules of Court, Rule 17, Section 3, Rule 17.

⁹ NPC Circular 16-04 ("Rules of Procedure of the National Privacy Commission") dated 15 December 2016, Section 4.

¹⁰ Comment dated 15 November 2019, p. 6.

¹¹ *Ibid.*, at pp. 6-11.

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 affiliates, subsidiaries, agents, service providers, as well as any prospective assignee or transferee, rating agency, insurer, any such person, entity or regulatory body that may be required by law or competent authority.

The Borrower holds the Lender free and harmless from any and all liabilities, claims and demands of whatever kind or nature in connection with or arising from the aforementioned disclosure or reporting.

xxx

14. Data Privacy. The Borrower hereby acknowledges, agrees and consents that the Lender or its authorized officer may collect, store, process and dispose data about the Borrower by the Lender. Any information and data received from the Borrower by the Lender may be used and utilized by the Lender, either directly or indirectly in the performance of the terms under this Agreement. The Lender shall take reasonable precautions to preserve the integrity and prevent any corruption or loss, damage, or destruction of the said data of the Borrower.¹²

The Respondent also denies any liability for the alleged harassment and threats to Complainant stating that:

48) The text messages shown by Complainant as proof of the alleged harassment or threats cannot be said to have come from the Respondent because they are not from the Respondent and the Respondent does not authorize and even prohibits its collectors from using such collection methods. As discussed above, [Respondent] does not authorize and even prohibits its collecting agents from making threats and harassing customers.

¹² Comment dated 15 November 2019, pp. 8-9. Emphasis supplied.

Despite this, they ultimately maintain their main argument that hinges on their Terms and Conditions, thus:

49) Furthermore the allegations that the Respondent contacted the contacts of the Complainant and other contacts to ask them to remind the Complainant of her loan which are all within the terms and conditions that the Complainant has agreed and consented to.

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

Discussion

It is necessary for the Commission to delineate the two (2) issues alleged by Complainant in his Complaint. The first one relates to his claims of harassment and threats based on the text messages he received. Copies of these messages were attached to his Complaint as evidence.¹³ The second issue is his claim that he was not the only one who received messages about his failure to pay, but that other people also learned about his loan and his corresponding default. He alleges that his contacts relayed to him that the messages said that he could be arrested.¹⁴

On the first issue, it bears stressing that the Commission is not the competent authority to determine the allowable practices in debt collection by financing companies and lending companies. These are governed by other laws and regulations and not the Data Privacy Act.

The second issue raised, however, falls squarely within the scope of the Data Privacy Act. The fact that Complainant was told by his acquaintances that he was being hunted to be arrested indicates that Complainant's name and fact of having obtained a loan were disclosed by Respondent to third parties. This is considered processing of personal information under the Data Privacy Act.¹⁵ The right to data privacy or informational privacy, after all, is the right of individuals to control information about themselves.¹⁶ It is this control, exercised by persons and entities other than the data subject, that the Data Privacy Act seeks to regulate.

As Respondent recognizes in its Comment, there is a set of criteria provided in the Data Privacy Act for the lawful processing of personal information.¹⁷

¹³ Complaints-Assisted Form dated 8 July 2019, pp. 9-18.

¹⁴ Supra note 3.

¹⁵ See Republic Act No. 10173, Section 3(j).

¹⁶ Vivares v. STC, GR No. 202666, 737 SCRA 92, 29 September 2014.

¹⁷ See Republic Act No. 10173, Section 12.

In justifying its contacting of Complainant's contacts, Respondent cites consent as its lawful basis to process, stating:

39) The above-quoted provisions of the Loan Agreement shows that the Complainant, by agreeing to loan from UPESO, has also waives (sic) 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 the terms and conditions of this loan agreement. This means that the Complaint has consented for UPESO to contact her (sic) contact references and her contacts in case she continues to fail to pay her obligations with UPESO and answer the calls and messages of UPESO.

40) Furthermore, the Complainant has given her consent for UPESO to access her contacts especially the reference contacts. It was even the Complainant who provided her contact references. These information also help UPESO make sure that the Complainant can be contacted in case she fails to pay her obligation with UPESO and refuse to answer the calls or reminders of UPESO.¹⁸

To determine whether the consent given by the data subject is proper, an examination must be made whether such consent was freely given, specific, informed, and an indication of will.¹⁹ Respondent points to the fact that it was Complainant himself who provided his personal information to UPESO as proof of consent. While this may show that there was a positive act showing an indication of will on the part of the Complainant and that such act was freely given, it is not enough to show that the given consent was specific or informed. These two (2) requirements relate to the obligation of personal information controllers such as UPESO to comply with the general privacy principle of transparency.

As the Implementing Rules and Regulations of the Data Privacy Act explains:

The data subject must be aware of the nature, purpose, and extent of the processing of his or her

¹⁸ Comment dated 15 November 2019, p. 10. Emphasis supplied.

¹⁹ See Republic Act No. 10173, Section 3(b).

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.²⁰

In this case, Respondent's Loan Agreement provides that the borrower "willingly, voluntarily, and with full knowledge of his right under the law, waives the right to confidentiality of information and authorizes 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 the terms and conditions of this Loan Agreement."²¹

The Loan Agreement also provides that "[a]ny information and data received from the Borrower by the Lender may be used and utilized by the Lender, either directly or indirectly in the performance of the terms under this Agreement."²²

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.²³ The information provided should be concrete and definitive; it should not be phrased in "abstract or ambivalent terms or leave room for different interpretations."²⁴

Applied to the present case, one is hard-pressed to identify the extent of what the Respondent is allowed to disclose and when. The cited provision not only allows Respondent to disclose any information relating to Complainant's loan availment but the purposes enumerated, which normally would limit the type of and the instances when information can be disclosed, are so different from each other and open ended that they cease to provide any

²⁰ Implementing Rules and Regulations of the Data Privacy Act, Section 18(a).

²¹ Comment dated 15 November 2019, p. 8.

²² *Ibid.*, at p. 9

²³ See Guidelines on transparency under Regulation 2016/679 of the Article 29 Working Party (2017).

²⁴ *Ibid.*

meaningful limits.

This is all the more true when the provisions of the loan agreement are read together with the information provided in the application itself when it asks for permission to access and use the contacts of borrowers. The screenshot attached to Respondent's Comment states:

Hello! Upeso needs to safely process your data so that you are qualified for loan... Upeso should be authorized for contact person and text message. We will process information for build your network with your financial record. Without your permission, we won't reach any of your contact.²⁵

From this, access to the borrower's contacts seem to be only for client evaluation or verification and not for the purpose of debt collection which is what Complainant alleges.

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.

Aside from this, the authorization given to the Respondent to disclose should be read in the context of related provisions in the Loan Agreement: the borrower's waiver of his right to the confidentiality of his information and the borrower holding Respondent "free and harmless from any and all liabilities, claims and demands of whatever kind or nature in connection with or arising from the aforementioned disclosure or reporting."²⁶

Without being informed of their rights under the Data Privacy Act, borrowers are asked to not only waive their rights under the Act but also, as to them, the obligations of Respondent as a personal information controller to, among others, ensure that there is lawful basis for its disclosures and to comply with the general privacy principles. Read in this light, the extent of Respondent's authority to general privacy principles. Read in this light, the extent of Respondent's authority to disclose becomes not just broader but seemingly without any legal consequence as well.

²⁵ Comment dated 15 November 2019, Annex "B".

²⁶ Ibid., at p. 9.

While the Commission recognizes the principle of autonomy of contracts which allow parties to stipulate the terms of their agreement, this doctrine, however, comes with a qualification. Such stipulations, clauses, terms and conditions may be agreed upon by parties, as they may deem appropriate, provided only that they are not contrary to law, morals, good customs, public order or public policy.²⁷ This is not met in this case.

The Data Privacy Act declares it the policy of the State to protect the fundamental human right of privacy.²⁸ This classification by law of privacy as a human right – as opposed to property rights, or civil and political rights – necessitates a corresponding treatment and protection in law. The 1987 Constitution includes as a State Policy that “the State values the dignity of every human person and guarantees full respect for human rights.”²⁹ The very first premise of the Universal Declaration of Human Rights, to which the Philippines is a signatory to, characterizes such human rights to be “inalienable.”³⁰ All of these indicate that no entity can subject an individual’s right to privacy – a fundamental human right - to a contractual waiver. Similar to other human rights, such as the right to life, it cannot be treated as property that is subject to the rules of ownership and trade. Respondent, in their Comment, manifest such misconceptions. It is the mandate of the Commission to clarify this issue and prevent the future commodification of this declared human right.

Hence, contrary to what Respondent claims, they cannot rely on consent as its lawful basis to process the names and mobile numbers of Complainant’s contacts for purposes of disclosing to them the status of his loan.

Despite this, however, the Commission is constrained to rely on the facts proven by Complainant in determining whether there is sufficient basis to warrant a recommendation for criminal prosecution.

The Supreme Court has held that in administrative proceedings such as this case, it is the complainant who carries the burden of proving their allegations with substantial evidence or such “relevant evidence that a reasonable mind might accept as adequate to support a conclusion.”³¹

In this case, an examination of the records shows that Complainant failed to sufficiently prove that Respondent processed and disclosed his personal information to his companions.

Although Complainant attached screenshots of his conversations with agents of Respondents showing how he was harassed as a result of his failure to pay his outstanding loan, as discussed previously, these go

²⁷ Bricktown Development Corp. v. CA, G.R. No. 112182, 12 December 1994.

²⁸ Republic Act No. 10173, Section 2.

²⁹ CONST. art. II, § 11.

³⁰ United Nations, Universal Declaration of Human Rights (nd) available at <https://www.un.org/en/universal-declaration-human-rights>

³¹ Ombudsman v. Fetalvero, G.R. No. 211450, 23 July 2018.

into the allowable practices in debt collection and are not under the jurisdiction of this Commission.

What is relevant to the discussion on disclosure is Complainant's allegation that he received messages from other people informing him that he is being hunted and that he has a pending warrant of arrest. In his Complaint, he said "*Nagmessage po yung mga kasama ko na hinahanap ako at may warrant na daw ako at makukulong na daw po ako.*"³² Aside from this statement, however, Complainant has not presented any other piece of evidence that would show much less prove the existence of the messages that he received from his companions, the contents of the messages, and, more importantly, the actions of Respondent in relation to them.

From the records, it is unclear how Respondent disclosed Complainant's personal information to his companions and what personal information, if any, was disclosed to them, whether Respondent communicated with them through calls or messages, or whether an actual person came to his workplace or residence looking for him armed with a warrant. Complainant did not even identify his companions.

The Commission cannot rely on allegations that are unsupported by fact or by law. It is bound to adjudicate 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.³³

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."³⁴

Despite being given several opportunities to provide additional information at the two mediation conferences and the Discovery Conference scheduled on 6 November 2019, Complainant failed to appear before the Commission without notice or justification.

Given this, in the absence of sufficient evidence to support Complainant's allegation that Respondent disclosed his personal information to his companions, it cannot be said that Respondent committed an act that would constitute unauthorized processing³⁵ or processing for an unauthorized purpose.³⁶

³² Complaints-Assisted Form dated 8 July 2019, p. 5.

³³ NPC Circular No. 16-04 dated 15 December 2016 ("NPC Rules of Procedure"), Section 22. Emphasis supplied.

³⁴ G.R. No. 165585, 20 November 2013, citing *Real v. Belo*, 542 Phil. 109 (2007).

³⁵ Republic Act No. 10173, Section 25.

³⁶ *Id.*, at Section 28

Section 19. 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; xxx

Considering the findings above, Complainant's application for the issuance of a temporary ban is denied.

WHEREFORE, all the above premises considered, the Complaint 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, 9 June 2020.

(sgd)

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

(sgd)

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(sgd)

JOHN HENRY DU NAGA
Deputy Privacy Commissioner

RBD

Complainant,

-versus-

NPC Case No. 19-1221

For: Violation of the Data
Privacy Act of 2012

FCASH GLOBAL LENDING, INC.

(FAST CASH)

Respondent.

X-----X

DECISION

AGUIRRE, D.P.C.:

Before this Commission is a complaint by RBD (“Complainant”) against FCash 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

¹ Records, p. 3.

² Id., at 5.

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 Fast Cash online lending company. After careful consideration, I decided not to take any action against them in order to have peace on both sides.

Decision

NPC Case No. 19-1221

Page 2 of 4

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 FCash 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.

³ Id., at 9.

⁴ Id., at 10.

⁵ Id., at 11.

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.

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 the NPC Rules of Procedure which provides:

WHEREFORE, all premises considered, the Commission hereby resolves to DISMISS the Complaint of RBD against Respondent FCash 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

(sgd)

JOHN HENRY DU NAGA
Deputy Privacy Commissioner

⁶ NPC Circular No. 16-04 dated 15 December 2016 ("NPC Rules of Procedure"), Sec. 2

ECA,
Complainant,

-versus-

NPC Case No. 18-103
For: Violation of the Data
Privacy Act of 2012

XXX,
Respondent,

X-----X

DECISION

NAGA, D.P.C.:

This refers to the complaint filed by ECA (Complainant) against XXX. (Respondent) for violation of several provisions of the Data Privacy Act (DPA) due to mishandling of the Complainant's Visa Credit Card and company Identification Card (Company ID).

The Facts

On 14 August 2018, the Complainant bought several units of Bluetooth headsets from the Respondent's store branch at Cebu City. She then paid using her Visa Credit Card and presented her Company ID as proof of identity. During the processing of payment, the Complainant noticed that the Respondent's staff took a picture of her Visa Credit Card and Company ID and sent it to the Respondent's Officer-in-Charge (OIC) through an online messaging system, the Complainant stated:

But looking to (sic) her, she posed for a moment and looking again to my two cards then (sic) covering the cards to her body and i heard the sounds of her cellphone that she's taken picture of my two cards... To my surprised i saw her phone, she sent picture of my TWO CARDS in the messenger. I asked her again, ms what makes (sic) you too long? What's the problem of my card, she said i am waiting for my Boss approval.¹

The Complainant then cautioned the staff that what she did might constitute a violation of the DPA. After processing the payment, the staff explained what happened in this wise:

That's the time she answer me, the purpose of taken (sic) picture was to ask approval to our Boss thats (sic) why i also sent (sic) to the messenger which were i communicated to (sic) the messenger.²

According to the Complainant, the staff further explained that she just followed the company's procedure. The staff also tried to allay the fear of the Complainant by telling that only the staff and the OIC have access to the Complainant's Visa Credit Card and Company ID.

Complainant alleged that the act of the Respondent's staff caused her stress, loss of time, and inconvenience since she had to report her credit card to the bank. The Complainant is also worried that she might be exposed to identity theft.

Thus, on 22 August 2018, the Complainant filed a complaint with the Commission for violation of the DPA with prayer for damages.

The parties were ordered to appear for discovery conference on 05 December 2018. After the discovery conference, the Respondent was ordered by the investigating officer to submit: 1) an explanation why no data protection officer (DPO) was appointed in their company; 2) a notarized answer to the complaint; 3) corporate papers of XXX; 4) identity of the organization's CEO; and 5) the result of the forensic examination of the mobile phone of the staff and her boss.

On 15 December 2018, the Respondent submitted its answer together with the other required documents, except the result of the forensic examination of the mobile phone of the Respondent's staff her boss and

¹ Complaints-Assisted Form, p. 3-4

² Ibid, p. 4

the explanation on why no DPO was appointed in XXX. For the purposes of forensic examination, the Respondent attached a letter to National Bureau of Investigation (NBI) seeking its assistance.

In the answer, the Respondent stated that the acts committed by its staff were not part of company's standard practice considering that they respect the rights of data subjects as provided in the DPA.

The Respondent further averred that the incident was caused by their staff's lack of knowledge on processing credit card transactions, especially if the credit card is not BDO or Eastwest, to wit:

Unfortunately, this incident occurred because the staff involved in this case is not yet very familiar with credit card transactions... She was given a one-on-one instruction on how to process BDO and Eastwest credit cards. The credit card used by complainant in this incident was an HSBC Visa Card and was therefore unsure as to how payment will be processed... The staff saw that an HSBC credit card was given to her and was not sure which POS Terminal to use to swipe the card and not knowing how to better handle the situation, took a picture of the credit card and ID and sent these to her OIC in order to be guided as to what POS Terminal will be used.³

Respondent further stated that the processing of Complainant's personal information was conducted to seek guidance from the OIC and not to commit any malicious act. However, the Respondent also acknowledged in the answer that taking photos of credit card and ID and sending those via messenger are risky processes that may cause serious inconvenience and potential damage to their customers.

Respondent then undertook to perform the following activities:

1. On-board a data privacy legal consultant who can guide them in their DPA compliance;
2. Appoint a data protection officer to execute their data privacy program and to whom the customers can direct their data privacy issues and concern;

³ Answer, p. 1

4. Conduct a credit card handling procedure training to all their staff; and
5. Publicly publish an escalation call tree in all their store branches where customers can directly escalate their issues and concerns in their dealings with their staff.

Issue

The sole issue for this Commission's resolution is whether the Respondent committed acts in violation of the DPA.

Discussion

The Complainant's contentions are meritorious.

The DPA, its Implementing Rules and Regulations (IRR), and other issuances of this Commission provide for various obligations and responsibilities for Personal Information Controller (PIC).

Among those that are relevant to this case are the following:

1. Adherence to the General Data Privacy Principles in processing of personal information⁴;
2. Upholding the Rights of the Data Subjects⁵;
3. Securing Personal Information through organizational, physical, and technical measures⁶; and
4. Appointing of a DPO⁷.

The Respondent's main argument is anchored on their staff's lack of knowledge and good faith when she took a picture of the Complainant's Visa Credit Card and Company ID. They did not provide explanation for the non-appointment of a DPO, and just enumerated several measures that they are planning to do in order to improve their data privacy compliance.

The Respondent's argument failed to persuade this Commission and finds that the Respondent had unjustifiably disregarded its abovementioned obligations and responsibilities as a PIC.

Respondent failed to adhere to the General Data Privacy Principles of Transparency and violated the Complainant's Right to be Informed

The principle of transparency provides that data subjects must be aware of the nature, purpose, and extent of the processing of his or her personal data.⁸ A related provision is the data subject's right to be informed,

⁴ R.A. No. 10173, §11

⁵ Id., §16

⁶ Id., §20

⁷ NPC Advisory 2017-01 dated 14 March 2017

⁸ DPA IRR, §17.a

which states that: “the data subject shall be notified and furnished with information indicated hereunder before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity.”⁹ (Emphasis supplied)

The timing of the provision of the information must be done before the entry of the data subject’s personal data to the PIC’s system or at the next practical opportunity. The “next practical opportunity” depends upon the surrounding circumstance of the case. However, the timing of the provision of information must always be within a reasonable period to give effect to the data subject’s right to be informed.

In this case, the Respondent failed to provide the purpose and justification as to the need of processing the Complainant’s personal information through taking pictures of her Visa Credit Card and Company ID. It took the Complainant four (4) inquiries before getting a substantial answer from the staff. Further, the needed information was only provided after the processing of payment through the credit card. The timing of the notification was not done before the entry of the Complainant’s personal data nor can it be said that it was conducted within a reasonable period given the surrounding circumstances. Indubitably, the Complainant’s right to be informed as provided by the DPA was violated.

Respondent disregarded its obligation to secure personal information and responsibility to appoint a DPO

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 its responsibility under the DPA.

The DPA IRR provides that, “the personal information controller and personal information processor shall take steps to ensure that any natural person acting under their authority and who has access to personal data, does not process them except upon their instructions, or as required by law.”¹⁰ (Emphasis supplied)

Thus, the reasoning provided by the Respondent that the conduct of its personnel was supported by the standard practice of the company must fail. It is its responsibility as PIC to secure personal information of its customers and relay the company’s privacy policies and procedures to its

⁹ Id., §34 (2)

¹⁰ Id., §25 (2)

personnel, especially to those responsible in processing personal information of customers.

Further, Respondent's gross incompliance of the DPA and other issuances of this Commission made evident on its nonappointment of a DPO, which is one of the elementary ways for companies to comply with the DPA.¹¹ The designation of a DPO is mandatory for all PICs regardless of size and nature of business.¹²

To ensure that the Respondent will make good of its stated undertakings in the submitted answer, this Commission shall require various documentation and/or proof of its compliance in line with the Commission's general power to compel any entity to abide by its orders on matters affecting data privacy.¹³

Complainant is entitled to the award of nominal damages

On the award of damages prayed for, while the Complainant claims that she suffered stress, loss of time, and inconvenience, such bare allegations would not be enough for this Commission to award moral damages without sufficient evidence for the same.¹⁴ Considering the circumstances of this case, it would be appropriate to award nominal damages to the Complainant in recognition of her violated legal right.

As provided by the Supreme Court, in Santos B. Arreola v. Court of Appeals.:

Nominal damage is 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.¹⁵

As established above, the Respondent failed to be transparent in the processing of the Complainant's personal information, which then resulted in the violation the Complainant's right to be informed.

The assessment of nominal damages is left to the discretion of the court/tribunal, according to the circumstances of the case.

¹¹ See The Five Pillars of Data Privacy Compliance and Accountability, NPC Privacy Toolkit (3rd edition)

¹² NPC Advisory 2017-01 dated 14 March 2017

¹³ R.A. No. 10173, 7(d)

¹⁴ Kierulf, et.al v. The Court of Appeals et. al., G.R. No. 99301, 13 March 1997

¹⁵ G.R. No. 95641, 22 September 1994

WHEREFORE, all these premises considered, this Commission resolves to AWARD Complainant, ECA, nominal damages in the amount of Ten Thousand (P10,000.00) Pesos for Respondent XXX's violation of her right to be informed under the Data Privacy Act. Respondent is also **ORDERED** to furnish this Commission the following documents:

1. Proof of its on-boarding a data privacy consultant;
2. Proof of registration with the NPC;
3. Copy of its Data Privacy Manuals and Privacy Notice;
4. Proof of its conduct of data privacy awareness and trainings for its employees;
5. Result of the forensic examination of the NBI on the mobile phone;
6. A sworn undertaking from both the Respondent and its agent regarding the deletion of the photos of the Complainant's credit card and identification card; and
7. Proof of payment of the awarded nominal damages.

The Respondent is DIRECTED to accomplish the foregoing within thirty (30) days from receipt of this Decision.

SO ORDERED.

Pasay City Philippines, 23 July 2020.

(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:

ECA

Complainant

XXX

Respondent

COMPLAINTS AND INVESTIGATION DIVISION

ENFORCEMENT DIVISION GENERAL RECORDS UNIT

National Privacy Commission

BGM

Complainant,

-versus-

NPC 19-653

For violation of Data
Privacy Act of 2012

IPP.,

Respondent.

X-----X

DECISION

LIBORO, P.C.:

Before this Commission is a Complaint filed by BGM (Complainant) against IPP. (Respondent) for the violation of her rights as a data subject under the Data Privacy Act of 2012 (DPA).

Facts

On 17 July 2019, Complainant filed her Complaint-Affidavit, alleging that respondent have violated her data privacy rights. In her Complaint-Affidavit, Complainant alleged that:

Complainant's sister purchased online an iPad Pro from a certain seller named LQG (Seller) via an online platform CP. One of the mode of payments in said transaction was through respondent IPP., where payments can be made through its app or its designated physical payment centers. Hence, upon the request of her sister, Complainant paid the remaining balance of the purchase price, in the amount of Twenty Thousand pesos (P20,000.00) to the Seller through the medium provided by Respondent. Complainant then proceeded to the meet up place where the Seller promised to hand over the purchased product. However, after waiting for more than three (3) hours, the Seller was nowhere to be found. Complainant

immediately called Respondent to have the Seller's account blocked and to get more information on the identity of the same for future legal actions. In the said phone call, Respondent told complainant that before they can disclose any information on the recipient of the payment, complainant must first secure a police blotter and a court order. On the same day, Complainant went to the MOA Police Community Precinct to file a police blotter of the incident. Thereafter, Complainant received a text message¹ from the seller's alleged mobile number saying that she used the money for her comatose son and that she will pay back Complainant when she receives the money from PCSO.

On 27 March 2019, Complainant sent Respondent an email informing them of the alleged incident and consequently requesting for the information of the account holder involved in the incident. Complainant invoked Section 16 (c) of the DPA 2 alleging that Respondent have violated the same for not providing them of the requested personal information of the seller/account holder who allegedly defrauded them thus prompting her to file the instant complaint.

On 12 September 2019, the parties were called for discovery conference. Both parties appeared, Atty. VTM, Mr. RCJ and Ms. UTM represented Respondent. During the scheduled discovery conference, Complainant asked from Respondent the information of the person she had the transaction with using Respondent's facility as alleged in the Complaint. However, since said information is involved in the issue of the case, Respondent was not required by the investigating

¹Records at page 10 Fact-Finding Report NPC Case No. 19-653 Page 2

"Hi good evening. I'm sorry for what happened. Thank you so much sa tulong mo malaking tulong 2 para sa anak kong comatose ngaun dito sa davao. Ibabablik q agad to pagkakuha ko sa pscso. Pinapangako ko yan sau. At dodoblehin pa 2 ni lord. Ung binayadm kc kinuha ko lang din sa remittance center. Salamat ulit. God bless."

2 Section 16 (c) of DPA provides:

(c) Reasonable access to, upon demand, the following:

- (1) Contents of his or her personal information that were processed;
- (2) Sources from which personal information were obtained;
- (3) Names and addresses of recipients of the personal information;
- (4) Manner by which such data were processed;
- (5) Reasons for the disclosure of the personal information to recipients;
- (6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
- (7) Date when his or her personal information concerning the data subject were last accessed and modified; and
- (8) The designation, or name or identity and address of the personal information controller;

officer to divulge the same. Respondent and Complainant were then ordered to submit their Responsive Comment within ten (10) days from the date of the discovery conference and Reply, respectively.

officer to divulge the same. Respondent and Complainant were then ordered to submit their Responsive Comment within ten (10) days from the date of the discovery conference and Reply, respectively.

On 14 October 2019, Respondent filed its Responsive Comment praying for the dismissal of the instant complaint because it does not involve a violation under the DPA. Further, Respondent argued that the provision under Section 16 (c) (3) of the DPA does not apply when the data subject prompted the sharing of information to the receiver due to a transaction between them. Accordingly, it cannot give the personal information requested by the Complainant without the risk of violating the data privacy rights of the data subject involved as well as violating the numerous obligations mandated by the same law to personal information controllers.

Respondent further contended that their imposition of requiring Complainant to first obtain a police blotter and a court order are mere safeguards that they have to enforce as custodians of the personal information disclosed to them.

On 24 October 2019, Complainant then filed her Reply to Respondent's Responsive Comment. In her Reply, Complainant anchored her claims on the following: Complainant contended that the act of Respondent requiring her to first secure a court order manifests the latter's disinterest in protecting its subscribers from fraudulent behavior in the usage of their online application. More so, that such acts would embolden scammers from using their service, knowing that Respondent would not divulge any information. To disclose only on the basis of a court order before Respondent divulges the information she is requesting defeats the purpose of the right of access granted to data subjects under the DPA. Further, Complainant assumes that by the time that a court order is released, the case involving said fraudulent acts would have gone stale and would also cause the complaining party great cause, expense, and effort. She argued that she has no other means to verify the name given to her by the alleged scammer aside from the information that Respondent have in their custody. Complainant believes that it is essential for her to obtain the subject information from Respondent because the scammer may have used or assumed a different identity, which might cause failure on her part to protect her property from fraud. Complainant reiterated that to allow Respondent to decline from disclosing information needed, such as in the instant Complaint, would effectively prevent other similarly situated victim of fraud to have concrete legal recourse against the scammer.

On 20 November 2019, Respondent filed its Rejoinder restating their prayer for the dismissal of the instant Complaint.

Issue

Whether or not Respondent's act of requiring Complainant to secure a court order prior to its release of the requested personal information violated the latter's data privacy rights.

Discussion

The Commission posits that the instant Complaint should prosper.

The crux of the Complaint involves the data subject's right to access, which is one of the rights conferred by the DPA under Section 16, paragraph (c) of the DPA, as follows:

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

x x x

- (c) Reasonable access to, upon demand, the following:
 - (1) Contents of his or her personal information that were processed;
 - (2) Sources from which personal information were obtained;
 - (3) Names and addresses of recipients of the personal information;**
 - (4) Manner by which such data were processed;
 - (5) Reasons for the disclosure of the personal information to recipients;
 - (6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
 - (7) Date when his or her personal information concerning the data subject were last accessed and modified; and
 - (8) The designation, or name or identity and address of the personal information controller; x x x

In the instant case, in the exercise of her right to access, Complainant merely seeks to obtain the information of the recipient of her personal information.

Section 16 (c) (3) of the DPA is clear which has no room for interpretation and should therefore be applied in its literal meaning.

Complainant, as data subject, should be entitled to access the information of the recipient of her personal information considering that the money

transfer receipts of Respondent only contains a transaction number and does not contain the name of the recipient of Complainant's personal information to enable her to identify as to whom a criminal case should be filed against.

In sum, Respondent's excessive or stringent requirement to complainant, with regard to the Complainant's request for the information of the account holder of the Respondent involved in the subject incident of alleged scam, violated the latter's right to access.

Moreover, Respondent as an entity considered as personal information controller (PIC), it is duty bound to observe and uphold the data privacy rights of Complainant, which thereby includes her right to access.

The Respondent herein should not have denied outright the request of the Complainant for the exercise of her right to access and using the DPA as a shield. Its requirement of compelling Complainant to produce a court order prior to the release of the requested information creates a high barrier that effectively impedes the rights vested by the DPA to the latter as a data subject.

Further, Respondent's assertion that the information within its custody can only be disclosed upon data subject's consent or on the basis of a lawful order is misplaced.

Section 12 of the DPA provides for the following criteria for lawful processing:

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

In order for Complainant to secure a court order, there must necessarily first be a court proceeding. However, before there can be any court proceeding

or in order for Complainant to initiate a criminal case against the Seller, the Complainant needs the information as to whom her personal data was disclosed in order to know against whom she should file a criminal case against.

Section 13 of the DPA 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).”

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.”

This Commission in the same case went on further and held 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.

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.

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 protection 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.³ 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.⁴

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.

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. 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.⁵

Lastly, this Commission finds that the award of nominal damages to Complainant is warranted.

³CID Case No. 17-K-003 dated 19 November 2019 and NPC 18-135 dated 06 August 2020

The Data Privacy Act provides that restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.⁶ 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.

As provided by the Supreme Court, in Santos B. Arreola v. Court of Appeals.:

Nominal damage is 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.⁷

As established above, the Respondent violated the Complainant's right to access which is considered as a violation of the DPA⁸. 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.⁹

As a recognition and vindication of Complainant's right that was violated by Respondent, the Commission awards nominal damages to the Complainant in the total amount of Forty Thousand (P40,000) Pesos.

⁴ R.A. 10173, Section 12(f); Ibid.

⁵ Ibid

⁶ Id., §37.

⁷ G.R. No. 95641, 22 September 1994.

⁸ SEC. 16. Rights of the Data Subject, Republic Act 10173 – Data Privacy Act of 2012

⁹ Seven Brothers Shipping Corporation v. DMC-Construction Resources, Inc. G.R. No. 193914. November 26 2014.

WHEREFORE, all premises considered, Respondent IPP. is hereby **ORDERED** to furnish the Complainant BGM the name of the recipient of her personal information in compliance with Section 16 (c) (3) of the Data Privacy Act and pay the Complainant the amount of Forty Thousand (P40,000) Pesos as nominal damages to vindicate Complainant's right to access, which was violated by Respondent. Further, Respondent is mandated by this Commission to submit proof of compliance that it complied with the orders of the Commission **within ten (10) days from the receipt of this Resolution.**

SO ORDERED.

Pasay City, Philippines;
17 December 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:

BGM

Complainant

IPP.

Respondent

LEGAL DIVISION

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

**IN RE: FLI OPERATING ABC
ONLINE LENDING
APPLICATION**

NPC 19-910

For violation of Data
Privacy Act of 2012

X-----X

DECISION

AGUIRRE, D.P.C.

This concludes the investigation conducted by the Commission following the Fact-Finding Report prepared by the NPC Task Force on Online Lending Mobile Applications¹ (Task Force) dated 29 August 2019, which serves as the Complaint (Complaint) pursuant to Rule IV of NPC Circular 16-04.² The Complaint alleged violations of Republic Act (R.A.) 10173 or the Data Privacy Act of 2012 (DPA) by FLI, operating the ABC online lending application.

The Complaint summarized its findings with the following recommendations:

On the basis of this fact finding report, there is sufficient ground to establish that FLI operating the ABC online lending application, as represented by their respective board of directors, committed acts in violation of the DPA, specifically:

1. Sections 11, 12, 13, 16, 20, and 21, for processing without complying with the requirements of the DPA and for failing to adhere to the principles of

¹ This Commission issued, on 14 May 2019, Privacy Commission Special Order Nos. 028 and 032-A, creating and reconstituting the NPC Task Force on Online Lending Mobile Applications. Said Special Orders explicitly named the seven (7) staff officers as members thereof. The Task Force is responsible to investigate the influx of complaints against several online lending companies for a potential violation 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 a fact-finding report on several online lending companies, one of which is the herein Respondents.

² NPC Circular 16-04. Rules of Procedure of the National Privacy Commission. Dated 15 December 2016.

- Transparency, Legitimate Purpose and Proportionality;
2. Sections 25, for Unauthorized Processing;
 3. Section 28, for Processing for Unauthorized Purposes;
 4. Section 31, for Malicious Disclosure;
 5. Section 32, for Unauthorized Disclosure.³

The Complaint

The Complaint made the following allegations:

From 06 July 2018 to 31 July 2019, the NPC received a total of 689 complaints against several online lending applications. This constitutes around 55% of the total complaints filed before the NPC. This does not include around 2,666 similar concerns raised through email or social media which were not formally filed as complaints. These numbers are unprecedented, potentially qualifying any violation of the DPA as large scale processing. The complaints bring to focus online lending applications, which can be downloaded and installed in mobile phones. These applications are then used to facilitate loan transactions between companies and their clients, the data subjects. The applications provide a platform for the collection of all types of personal information from various device models, which information related not just to the clients of the company, but extends to persons in their contact lists. Evident from the complaints are common statements from data subjects conveying how downloading these applications lead to a disruption in the lives of others, in violation of individual rights and freedoms.

Considering the number of data subjects involved, the seriousness of the allegations, and the risks of harm to data subjects, NPC, on its own initiative, investigated the circumstances surrounding the possible violations of ABC online lending application. Significantly, the number of complaints filed against this lending application have already reached a total of 113 complaints as of 31 July 2019.⁴

The Complaint provides that affidavits and sworn statements of the complainants against the company operating the ABC lending application were evaluated. It states that individual complainants relayed the incidents in the course of their transaction with the company based on their personal knowledge, own experiences,

³ Fact-Finding Report dated 29 August 2019, p. 23.

⁴ Id at 1 .

and supporting documents.⁵ The Complaint found that the following statements about the company have been consistently made:

1. Personal information from complainants' mobile phonebook/directory/contact list were used by ABC to contact third persons, without their consent or authority;
2. Personal information about the data subjects, both unwarranted and false information were discussed to third persons, which included friends, relatives, co-workers and superior of the data subject. These persons were often told that the data subjects named them as co-makers or character references, and there were some reports that they were even asked to settle the loan in behalf of the data subjects;
3. Agents or representatives of ABC used personal information about data subjects and others in their contact list to damage the reputation of data subjects, or to harass, threaten or coerce them to settle their loans;
4. Methods used in processing personal information were unduly intrusive, including posting in social media of personal and sensitive personal information of data subjects or even subjecting their contacts to threats and harassment; the personal information processed were excessive or otherwise used for purposes beyond what is necessary or authorized under their agreement.⁶

The Complaint cites several specific allegations from various statements in different complaints, supported by screen captures by the complainants, such as:

In CID Case No. 19-F-415, complainant reveals that prior to installing the ABC application, it required permissions to access her contact list and their phone numbers, Facebook and Google accounts, and others. Furthermore, Complainant in CID Case no. 19-G-522 alleges that ABC even hacked the photos in her phone, among other identifying information. Complainant also received the following text message:

Before you sue us, we already send (sic) a text blast to all of your contacts. Posting your uploaded picture from Loan apps to social media.

⁵ Id at 2.

⁶ Id, at 3.

We know your home address, office address, and your ugly face. But you never know us, that take times and you make effort and time for that. Right now we already send text blast with false information regarding you.

We hacked your info, and we can send false information regarding this. All your contacts, messages, and in and outcall activity we have information. You're done due to swearing with us.

Goodluck with your privacy law.⁷

XXX

While some agents make it appear that they are contacting the complainant's phone list to aid in collection, an ABC agent in CID Case No. 19-G-573 admitted that said "text blast" was for the purpose of ruining complainant's reputation:

Hello Ma'am / Sir, your loan to ABC has been overdue. We will inform your relatives and friends to urge the repayment (overdue debts) when you has been overdue. Please cherish your reputation among friends and relatives, cherish your credibility and repay as soon as possible. Do reply if you don't want us to call of your contact references. This is the special collections team.⁸

The Complaint included a Technical Report, prepared by the Information Technology Officers of the Task Force, in its Annexes to corroborate the statements of the various complainants, particularly those alleging that the application was able to access their contact lists. By extracting the AndroidManifest.xml, which describes the essential information about applications, Android build tools, the Android operating system, and Google Play, the Technical Report revealed that the ABC application required forty-four (44) permissions, seven (7) of which were classified as dangerous permissions.⁹

The Technical Report explained dangerous permissions as those that "cover areas where the app wants data or resources that involve the user's private information or could potentially affect the user's stored data or the operation of other apps. For example, the ability to read

⁷ Ibid.

⁸ Id at p. 4.

⁹ ABC App Preliminary Technical Report, 09 August 2019, P.4,
https://developer.android.com/guide/topics/permissions/overview#dangerous_permissions

the user's contacts is a dangerous permission. If an app declares that it needs a dangerous permission, the user has to explicitly grant the permission to the app. Until the user approves the permission, your app cannot provide functionality that depends on that permission. To use a dangerous permission, your app must prompt the user to grant the permission at runtime.”¹⁰

On 30 August 2019, the Commission issued an Order to File an Answer pursuant to Section 24 of the NPC Rules of Procedure, directed to Respondent FLI and its responsible officers specifically ML, CW, KF, JG, HJL, and BSJ. with its dispositive as follows:

WHEREFORE, premises considered FLI and its responsible officers specifically, ML, CW, KF, JG, HJL, and BSJ, are all instructed to file their respective Answers to the allegations in the Fact-Finding Report.

The Answer should be filed no later than ten (10) days from receipt of this Order. In cases where the respondent or respondents fail without justification to submit an Answer or appear before the National Privacy Commission when so ordered, this Commission shall render its decision on the basis of available information.¹¹

On 16 September 2019, an Appearance and Omnibus Motion was filed by the QG Law Offices for FLI and Respondents ML, CW, and BSJ., which prayed for the following:

WHEREFORE, premises considered, it is prayed unto the Honorable Office, that an Order be issued:

- a) Upon receipt of the Motion, to suspend proceedings, pending resolution of the instant Omnibus Motion; and
- b) Initiating a Mediation Proceeding

As a matter of extreme prudence, it is also prayed for the Honorable Office to issue an Order giving the Respondents an additional time of fifteen (15) days or until 30 September 2019 within which to file their respective answer or such other responsive pleading.

¹⁰ Ibid.

¹¹ Order to File an Answer, dated 30 August 2019.

On 17 September 2019, a Motion for Extension to File Answer with Entry of Appearance was filed by GNGA & Associates for Respondents KF, JG and HJL, likewise requesting for an extension, thus:

WHEREFORE, premises considered, respondents most respectfully prays unto this Honorable Commission that the Motion for Extension of Time for a period of ten (10) days from 16 September 2019 or until 26 September 2019 within which to file the necessary pleading, BE GRANTED in the interest of substantial justice and the entry of appearance of the undersigned counsel be duly noted.

Thereafter, additional Motions for Extensions were filed by counsels for both parties.

On 26 September 2019, counsel for Respondents KF, JG and HJL prayed for an additional ten (10) days or until 6 October 2019 to file their Verified Answer.

On 27 September 2019, counsel for Respondent FLI, the QG Law Offices, filed their Withdrawal of Appearance.

On 30 September 2019 the law firm of DSBMR filed an Entry of Appearance with Motion for Further Extension of Time to File Answer for Respondent FLI. They moved for an additional period of fifteen (15) days or until 15 October 2019 within which to file their answer.

On 01 October 2019, the law firm of DSBMR entered its appearance as counsel for Respondents ML, CW, and BSJ and prayed for an additional period until 15 October 2019 within which to file its Answer.

On 07 October 2019, the Commission issued a Resolution that granted all the requests of the Respondents for additional time to file their Answers, finding that these were all duly filed within the allowable period of time.

As regards the prayer of Respondents ML, CW, and BSJ for the initiation of mediation proceedings, the Commission denied this and cited NPC Circular 16-04 which states thus:

Section 26. Mediation officer. – The Commission shall assign a mediation officer to assist the complainant and respondent to reach a settlement agreement, **provided that no settlement is allowed for criminal acts.**

The Answers

On 11 October 2019, Commission received a Verified Answer from Respondents KF, JG, and HJL through their counsel.

On 15 October 2019, an Answer was filed by Respondents FLI, ML, CW, and BSJ, through their counsel.

On 08 January 2020, the Commission issued an Order stating that the Answer by Respondents FLI, ML, CW, and BSJ did not provide evidence to support the following arguments:

18. It is not true that FLI and its directors / officers have “knowledge of the practices of its agents or other people clothed with the authority to collect outstanding loans” because, in fact, the collection agents who committed debt-shaming practices did so without the knowledge of FLI and its directors/officers. It then follows that without any knowledge of FLI and its officers, the respondents could not have consented to the acts of the collection agents, whether expressly or impliedly.

19. FLI recognizes that even if the collection of loan repayments was outsourced to a third-party service provider, it was not amiss in its duty to ensure that the third-party service provider/processor and the collection agents under its employ comply with the DPA and the basic principles of personal data protection. In particular, collection agents are supposed to use only a provided computer software to contact the user/borrower of third parties. They were not allowed to use their personal phones to contact the user or other parties, which is what these collection agents did.¹²

¹² Order dated 8 January 2020

The Commission thereafter ordered the Respondents to substantiate the allegations through the submission of documents such as :

1. The official company document containing the functional statements of each director and officer of the corporation; and
2. The outsourcing agreement with the third-party service provider / processor referred to in their Answer as of 29 August (the date of the Fact-Finding Report) containing the provisions they mentioned in Paragraph 19.¹³

On 10 February 2020, the Commission received a Motion for Extension of Time to File Compliance from Respondents FLI, ML, CW, and BSJ citing communication and logistics issues arising from the ongoing outbreak in China caused by the 2019 Novel Coronavirus.

On 20 February 2020, Respondents FLI, ML, CW, and BSJ filed their Compliance with the following Annexes:

- 4.1 Annex “A”, a copy of the by-laws of FLI, as approved by the Securities and Exchange Commission.
- 4.2 Annex “B”, an original copy of the Affidavit executed by the General HR manager at FLI, detailing the actual functions of the board of directors of FLI within the organization and how members of the board of directors of FLI were not privy to the manner and method of loan collection that was being adopted by the employees of CSA.
- 4.3 Annex “C”, a copy of the Master Service Agreement executed by FLI and CSA, to whom FLI had outsourced the loan collection function on 12 October 2018.
- 4.4 Annex “D”, the Code of Conduct of CSA, issued on May 2019, which identifies “bringing in and using mobile phones by unauthorized employee in the work area or while on while on duty” as an offense under the category “acts of inefficiency, negligence, and violation of work standards or company policies”.

¹³ Ibid.

- 4.5 Annex “E” is a copy of the presentation of FLI on its ongoing efforts for data collection and usage as well as optimization of data collection systems.
- 4.6 Annex “F”, a copy of the certification issued by FLI’ external legal counsel, QG Law Offices, which states that out of 69 complaints pending against FLI before the Honorable Commission, 25 complaints have already been settled.¹⁴

On 20 August 2020, the Commission noted this submission and stated in an Order:

Under NPC Circular No. 16-04 or the NPC Rules of Procedure, the Commission may order the conduct of a clarificatory hearing if, in its discretion, additional information is needed to make a Decision.

After due consideration of the evidence presented as of the date of this Order, the Commission finds that a clarificatory hearing is needed for the proper disposition of this case.

WHEREFORE, in the interest of conducting an exhaustive investigation and pursuant to the NPC Rules of Procedure, the Commission hereby resolves to **ORDER** Respondents to appear for a clarificatory hearing on **24 SEPTEMBER 2020 at 2:00 PM**, in relation to its submissions for the case of NPC 19-910.

The Commission later received a Notice of Withdrawal filed by the law firm of DSBMR dated 21 September 2020, which stated:

The law firm of SBMR respectfully manifests it is withdrawing as counsel for FLI, ML, CW, AND BSJ (collectively, the “Respondents”) in the above-captioned case, pursuant to the instructions that it received from the RESPONDENTS.

The Commission likewise noted the Entry of Appearance with Urgent Motion to Reset Clarificatory Hearing filed by the QG Law Offices dated 22 September 2020.

Following these submissions, the Commission reset the clarificatory hearing to 01 October 2020, guided by NPC Advisory No. 2020-02 or “Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission.”

¹⁴ Compliance dated 20 February 2020.

On 01 October 2020, the Commission conducted a Clarificatory Hearing (Hearing), pursuant to Section 21 of NPC Circular No. 16-04. Respondent FLI and the individual Respondents ML, CW, and BSJ were represented by Atty. QAL and Atty. ET from the QG Law Offices, while the individual Respondents KF, JG and HJA were represented by Atty. FG from the law firm of GNGA & Associates.

Following the commitments of the counsel for Respondent FLI, ML, CW, and BSJ to submit documents to substantiate their claims during the Hearing, the Commission issued an Order dated 01 October 2020 requiring them to submit the following:

1. The diagram of the organizational structure of FLI Lending, Inc. that was supposed to be attached as Annex “A” of the Affidavit of MTA, attached as Annex “B” of the Compliance filed by FLI Lending, Inc. on 20 February, 2020;
2. Board Resolutions, if any, discussing the following matters:
 - Authorizing ML, President, on behalf of FLI Lending, Inc., to enter into the Master Service Agreement with CSA dated 12 October 2018 ; and
 - Appointing the officers of FLI Lending, Inc. or authorizing the President to make appointments for the positions of General Manager, General HR Manager, and other officers of FLI Lending, Inc.
3. Documentation on the current status of the Master Service Agreement between FLI Lending, Inc. and CSA;
4. Details surrounding the presentation attached as Annex “E” of the Compliance filed by FLI Lending, Inc. on 20 February, 2020, such as: who delivered the presentation, to whom it was delivered, when it was delivered, etc.;
5. Documentation on the number of complaints filed with FLI Lending, Inc. in relation to the collection practices of CSA;
6. Documentation on the number of CSA employees terminated as a result of the complaints filed with FLI Lending, Inc.;
7. Details on the utilization, if any, by FLI Lending, Inc. of the following provisions in the Master Service Agreement dated 12 October 2018;

- Article VI, Section 2. *Unprofessional Practices in the Performance of the Service and Breach of the Contract; Penalties.*
 - Article VIII, Section 3(d). *Duration of the Agreement and Termination; Termination; Performance evaluation yields an unsatisfactory result*
8. Documentation of the issue relayed by FLI Lending, Inc. regarding alleged scammers who represent themselves to the public as agents of ABC, including any notices issued to the public informing them of this issue; and
 9. Information on the background of individual respondents ML, CW, and Bernard BSJ.

On 16 October 2020, FLI filed a Partial Compliance with an attached Memo from CSA. dated 01 October 2019. FLI also requested for an extension of thirty (30) days or until 15 November 2020 to produce and submit the other documents required by the Commission.

Considering the circumstances raised by FLI and in the interest of an exhaustive investigation, the Commission granted the requested extension for submission of the required documents.

The Respondents filed their Compliance dated 26 November 2020, and submitted the following documents:

- a. Disciplinary reports transmitted by CSA to FLI in relation with potential data privacy violations committed by CSA which proves that FLI mandated CSA to comply with their undertaking and obligation under the MSA;
- b. Sample employment contract between CSA and its employees showing that the collection employees undertook to comply with CSA company policies specifically data privacy policies;
- c. FLI and CSA Master Service Agreement with Confidentiality and Non-disclosure Agreement which proves that there is a contract between FLI and CSA pertaining to CSA's compliance with prevailing laws specifically data privacy laws;
- d. A sample CSA employment contract with its employees; and
- e. Master Service Agreement between FLI and CSA.¹⁵

¹⁵ Compliance dated 26 November 2020.

Issues

The issues in this case are as follows:

1. Whether procedural due process was observed;
2. Whether the proceedings should be held in abeyance during the pendency of the other complaints;
3. Whether Respondent FLI violated Sections 11, 12, 13, 16, 20, and 21 of the DPA for processing without complying with the requirements of the DPA and for failing to adhere to the principles of Transparency, Legitimate Purpose, and Proportionality;
4. Whether Respondent FLI committed Unauthorized Processing of Personal Information and Sensitive Personal Information under Section 25 of the DPA;
5. Whether Respondent FLI committed Processing for Unauthorized Purposes under Section 28 of the DPA; and
6. Whether the penalty shall be imposed upon the Board of Directors, as responsible officers who by their gross negligence, allowed the commission of the crime.

Discussion

I. Procedural Due Process was Observed

In the Answer filed by Respondents FLI, ML, CW, and BSJ, they questioned the procedure in the sua sponte investigation, thus:

43. The Fact Finding Report admits that “[e]xaminations of publicly accessible information and the initial technical evaluation on FLI and their online lending application, ABC, show that the company has failed to demonstrate compliance with the DPA.” This statement clearly shows that the Fact-Finding Report did not consider the side of FLI.¹⁶

The Commission takes the opportunity to discuss the nature of a *sua sponte* investigation.

¹⁶ Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019. Page 13.

The NPC is an independent body created to administer and implement the provisions of the DPA of 2012. As provided in Section 7 of the DPA, the NPC has Rule-Making, Advisory, Public Education, Compliance and Monitoring, Complaints and Investigation, and Enforcement powers¹⁷ to enable it to protect the fundamental human right of privacy while ensuring the free flow of information to promote innovation and growth.¹⁸

Section 7(b) of the DPA specifically states that it is the mandate of the NPC to:

(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; (Emphasis supplied)

In the exercise of its rule-making power and to flesh out the provision above, the NPC issued NPC Circular 16-0419 on 15 December 2016. Section 3 thereof provides who may file complaints with the Commission:

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.

Further, Section 23 of the NPC Circular 16-04 provides for the NPC's power of original inquiry:

¹⁷ See, RA 10173, Section 7.

¹⁸ See, *Id.*, Section 2.

¹⁹ NPC Circular 16-04. NPC Rules of Procedure. Dated 15 December 2016.

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.

The NPC Circular 16-04 provides for the procedure in instances of *sua sponte* investigations, thus:

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.²⁰

The Fact-Finding Report, therefore, serves as the Complaint in *sua sponte* investigations and is not yet a Decision by the Commission. Contrary to the claim of the Respondents that they were not afforded their right to due process, this Commission provided Respondents an opportunity to provide their side. This is precisely why the Commission, in an Order dated 30 August 2019, directed Respondents to file an Answer in response to the allegations in the Fact-Finding Report.

II. The proceedings should not be held in abeyance during the pendency of the other complaints.

In the Answer filed by Respondents FLI, ML, CW, and BSJ, they alleged that:

²⁰ Ibid, Emphasis supplied.

46. The proceedings in the instant case also appear to be premature because there are, in fact, individual complaints involving actual, individual complainants which remain pending at various stages before the Honorable Commission.

47. The Fact-Finding Report mentions that there are a “total of 113 complainants as of 31 July 2019 which have been filed with the Honorable Commission against FLI.

48. First, out of the 113 complaints, FLI has been made aware only of 54 complaints and have received files, orders, and pleadings only for 54 complaints. These 54 complaints are in different stages of proceedings and some of them have already been subject to compromise agreement that was approved by the Honorable Commission while some of them are subject precisely to mediation proceedings.

49. Second, it is possible that the Honorable Commission could even lose the basis for the instant case, which was supposedly the 113 complaints, if for example, these individual complaints are eventually dismissed. In line with due process and fairness, the Honorable Commission should have first allowed the individual complaints against FLI [to] be threshed out by the Complaints and Investigation, before creating a fact-finding committee, also from within the Honorable Commission, which would investigate the same circumstances and cases. The Fact-Finding Report has effectively prejudged the pending individual complaints.

xxx

51. Thus, the reasonable approach would be to let the individual complaints run their course and hold the instant case in abeyance.²¹

The Commission refers once more to the abovementioned Sections 3, 23, and 24 of NPC Circular 16-04 which provides the nature of a *sua sponte* investigation.

The fact that there exist hundreds of pending cases before the Commission against Respondent FLI is no bar to the filing of the present case. The Commission notes that the pending cases and the case on hand involve different parties, different causes of action with different prayers of relief.

²¹ Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019. Page 14.

The focus of this investigation is the functionality of the ABC application in relation to the categories of personal information collected upon its download and the extent of further processing vis- à-vis what is declared by Respondent FLI in their Credit Agreement and Privacy Policy. The citation of allegations from different pending cases illustrate that the effects of these functionalities coupled with the lack of transparency are not imagined but have seriously harmful effects in the lives of their borrowers, who are considered data subjects under the DPA.

III. Sections 11, 12, 13, 16, 20, and 21 of the DPA may be bases for determining violations under Chapter VIII of the DPA.

Respondents FLI, ML CW, and BSJ emphasized in their Answer that the violation of the above-captioned provisions does not give rise to criminal liability, thus:

Sections 11, 12, 13, 16, 20, and 21 of the DPA cannot be the basis for criminal prosecution. The Honorable Commission could hold respondents liable only administratively for violations of the provisions, if any, based on the provision in the DPA that the Honorable Commission shall have the power to merely “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” (Section 7(b) of the DPA).

Further, the DPA does not provide for any penalties, whether imprisonment or fine, for failure to comply with Sections 11, 12, 13, 16, 20, and 21 thereof.²²

While it may be true that these provisions do not fall under Chapter VIII of the DPA, which provides for the prohibited acts, these provisions notably cover the General Data Privacy Principles, Criteria for Lawful Processing of Personal Information, Sensitive Personal Information

²² Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019, page 2.

and Privileged Information, Rights of the Data Subject, Security of Personal Information, and Principle of Accountability. These consist of the principles and concepts in the DPA that serve as the substantive bases for determining violations under Chapter VIII which incur criminal liability.

IV. Respondent FLI committed Unauthorized Processing of Personal Information and Sensitive Personal Information under Section 25 of the DPA

In determining whether a violation of Section 25 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 and 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.²³

A. The accused processed the personal information of the data subjects.

The first two elements for Unauthorized Processing are undisputed, as Respondent FLI admits to processing personal and sensitive personal information. In their Answer, they cite their Credit Agreement in claiming that it obtained it borrowers' consent to "collect, process, and retain" personal information such as, but not limited to, the name, address, phone number, mobile phone number, financial information, credit status information, phone contacts and other related information.²⁴ It further cites its Privacy Policy which states that ABC collects personal information provided to them which may include additional information about the borrower to help ABC get to know them better, such as "gender, age, date of birth, nationality, professional associations and registration numbers, information about how [they] use [their] products, and demographic information."²⁵

²³ NPC Case No. 17-018, Decision dated 15 July 2019.

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.”²⁶ Undeniably, the name, address, phone number, financial information,

credit status information and phone contacts of the ABC borrowers, when put together, will serve to identify specific individuals. The gender, date of birth and nationality of the borrowers, on the other hand, are considered sensitive personal information under the enumeration provided in the DPA.²⁷

The DPA enumerates a series of processing activities to emphasize that this covers the different stages of a data lifecycle. Processing is defined by the DPA 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.”²⁸

Respondent FLI, through the ABC application, processed the information of the borrowers when it accessed personal information through app permissions such as READ_CONTACTS and READ_EXTERNAL_STORAGE.²⁹ The processing, however, did not end there given the apparent retention of information which made it possible for Respondent FLI, through collection agents, to inform third parties about the borrower’s outstanding debt. This will be discussed subsequently.

²⁴ Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019, at 6.

²⁵ Ibid.

²⁶ RA 10173, Section 3 (g)

²⁷ R.A. 10173, Section 3(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.

²⁸ R.A. 10173, Section 3(j).

B. The processing was done without the consent of the data subject, or without being authorized under the DPA or any existing law.

The DPA provides for lawful criteria to process personal information. For the subject personal information in this case, the lawful criteria are found under Section 12³⁰ and 13³¹ of the law.

²⁹ Pondo Peso App Preliminary Technical Report, 09 August 2019.

³⁰ 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.

³¹ 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;

Respondent FLI claims the consent from the borrowers as its lawful criteria. In its Answer, it argued that it has obtained the consent of the borrowers prior to the collection and processing of the contact list, thus:

22. First of all, FLI obtains the prior consent of the borrowers to the collection and processing of their respective contacts list.

23. It provides a Credit Agreement and Privacy Policy which data subjects need to agree to:

Credit Agreement

Part II (e)

*e) Subject to the provisions of the Privacy Policy, the User agrees, consents and authorizes ABC to collect, process and retain personal information of the User such as, but not limited to: name, address, phone number, mobile phone number, financial information, credit status information, phone contacts and other related information **in order to achieve the purpose of this Agreement.***

Part II(g)

*g) ABC ensures that personal information of the User shall be protected and secured from unauthorized access, breach, disclosure or sharing. The User agrees, consents and authorizes ABC to use, manage, disclose personal data, information, archives, data sources to Third Parties in **order to achieve the purpose of this Agreement** including but not limited to collection, data verification, use telecom operators, among others. Subject to the limitations as set forth under the Data Privacy Act and its Implementing Rules and Regulations.³²*

Privacy Policy

*ABC collects personal information you **provide us**, which may include: (i) contact information, such as your name, company name, job title, address, e-mail address, and phone number; (ii) additional information about you to help us get to know you better, such as gender, age, date of birth, nationality, professional associations and registration numbers, information about how you use our products,*

(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.

³² Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019 at 7. Emphasis supplied.

*and demographic information; (iii) comments, questions, requests and orders you make; (iv) financial information needed to process loans and payments, such as credit card or account information or other banking information; (log-in information, including, if applicable, social media account information for log-in purposes, if applicable; (vi) information about your preferences, such as your preferred methods of communication and product types in which you are interested (viii) phone contacts in your device needed **for collection purposes, if in case the information provided in the credit agreement is false, invalid or otherwise not responsive to our collection attempts.***

24. During user sign-up in the app, the user is required to click “Agree” to the Privacy Policy. Then, when the user decides to actually make a loan, the borrower is required to click “Agree” to the Credit Agreement and Disclosure Statement. Thus, the consent of the borrower to the collection and processing of his contacts list is obtained based on a specific purpose disclosed to the user. The consent is given expressly as well.³³

According to Answer of Respondent FLI, the user is required to click “Agree” to the Privacy Policy during sign up in the application. Upon making a loan, the borrower is also required to click “Agree” to the Credit Agreement. In this regard, Respondent FLI states the consent of the user or borrower is expressly given and obtained based on a specific purpose disclosed to them.

At this juncture, the Commission takes the opportunity to emphasize the difference between a Privacy Policy and a Consent Form, considering the different requirements for these under the DPA.

This issue has been clarified in the Commission’s Advisory Opinions, thus:

[T]here is also a need to determine and clarify the distinction between a privacy policy and securing the consent of the data subject for the processing of his or her personal information. **Being a mere notice, it is emphasized that the 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 the data subjects.

³³ Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019 at 7. Emphasis supplied.

The principle of transparency mandated by the DPA 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. Any information and communication relating to the processing of personal data should be access and understand, using clear and plain language.

On the other hand, obtaining consent from the data subject for the purposes of processing his or her personal data has different requirements altogether.

Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information.

When the processing of personal information is based on consent, the PIC must obtain the consent in relation to the declared purpose for processing. The consent must likewise be evidenced by written, electronic, or recorded means.

We reiterate that the mere posting of a PIC’s privacy policy or notice and requiring the consumers to agree thereon via the online platform does not equate to obtaining the consent of the data subject for purposes of processing his or her personal information as required under the law.

[T]he fact that the data subject must agree to a privacy policy or notice fails to meet the requirement of meaningful consent. A “bundled” consent, for instance, will generally not suffice as the data subject is not empowered to make a true choice.³⁴

In this case, Respondent FLI requires the borrowers to click “Agree” to the Privacy Policy, aside from the Credit Agreement, and subsequently relies on this as basis for the supposed consent obtained from the borrowers. Given this, the Commission evaluates both the Privacy Policy and Credit Agreement according to the requirements of the DPA for consent.

³⁴ Advisory Opinion 2018-013. Dated 18 April 2018. Emphasis supplied.

i. Respondent FLI committed unauthorized processing for its retention of contact lists beyond its declared purpose.

The Complaint included a Technical Report that examined the functionalities and permissions of the ABC application, in order to corroborate the collective allegations from the individual complaints.

Based on the declared permission on Google Play Store, the extracted AndroidManifest.xml file and the Google Developer definition, the Examiners concluded that ABC app is:

Capable of **COLLECTING USER'S PRIVATE INFORMATION** that potentially affect the user's stored data and the operation of other apps once installed on an Android device. Thru the android.permission.READ_CONTACTS permission, ABC app is capable in reading the user's contact data; thru the android.permission.READ_EXTERNAL_STORAGE, ABC app is capable in reading any data from the external storage of the device such as microSDs;

In its Answer, Respondent FLI gave its rationale behind all the Dangerous Permissions used in the ABC application, thus:

34. xxx

c. READ_CONTACTS permission is necessary because reference contacts are populated during the loan application with a drop- down box. The reference contacts cannot be manually typed as this would potentially give way for users to provide bogus numbers. This also prevents instances wherein potential users would use a burner phone in order to have a loan application approved. One of the verification steps undertaken by FLI is the examination of the phone contact list to see if the phone is newly purchased or if there are no or next to minimal contacts presently registered in the phonebook. If the contacts list reviewed appears to be unscrupulous or is otherwise made up, the loan application will be denied outright.

37. It may also be noted that the access of FLI to the contacts of the user allows FLI to conduct its due diligence and credit investigation on potential customers. Thus, the processing of the contacts information of the user carries a legitimate

purpose and is proportional to that purpose.³⁵

The Commission finds this explanation to be insufficient and inconsistent with actual events that have led to the numerous complaints filed with the NPC.

Respondent FLI claimed that the READ_CONTACTS dangerous permission is justified by its need to determine, at the point of loan application, whether the mobile phone was newly purchased in the event of a few entries in the contact list. This is part of their verification process which is done prior to the approval of the loan. The issue remains, however, as to why these contacts were retained and kept in a form that allowed further processing even after the loan application's approval.

Such retention is considered as a processing activity under the DPA which must also be supported by consent or other lawful criteria.

The cited Credit Agreement shows that the declared purpose for retention and other processing activities was "in order to achieve the purpose of this Agreement." This cannot be a basis for consent.

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."³⁶

The declaration "in order to achieve the purposes of this Agreement" is circuitous and is an overbroad phrase that does not conform with the general privacy principle of transparency. This cannot support a claim of validly obtained consent, hence consent cannot be FLI' basis for lawful criteria. As held by the Commission in a decided case³⁷:

³⁵ Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019. Page 11.

³⁶ R.A. 10173, Section 3(b). Emphasis supplied.

³⁷ NPC Case 19-450. Dated 09 June 2020.

[There is a need 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....³⁸ The information provided should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations.³⁹

The cited Privacy Policy in Respondent FLI’ Answer also cannot be the basis for acquiring consent to retain the borrowers’ entire contact lists. The Privacy Policy declared that its purpose for processing phone contacts was “for collection purposes.”⁴⁰

Regardless of whether Respondent FLI hinges on the purposes of verification, loan application, or debt collection, the retention of the borrowers’ entire contacts lists far exceeds these purposes.

The Data Privacy Act of 2012 states thus:

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

(d) Adequate and not excessive in relation to the purposes for which they are collected and processed;...⁴¹

This principle is further explained in the Implementing Rules and Regulations of the Data Privacy Act of 2012, which states, “personal

³⁸ See, Guidelines on transparency under Regulation 2016/679 of the Article 29 Working Party (2017).

³⁹ Ibid.

⁴⁰ Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019, at 7.

⁴¹ R.A. 10173, Section 11(d).

data shall be processed **only if the purpose of the processing could not reasonably be fulfilled by other means.**⁴²

The availability of far less intrusive measures, such as a reliance on a limited number of reference contacts provided by the borrower, demonstrates that the measures employed by Respondent FLI were disproportionate to the aim they sought to achieve.

Personal information that is processed in excess of what is proportional to the declared purpose amounts to Unauthorized Processing which is a punishable act under Section 25 of the DPA.

Lastly, the Commission notes that the Privacy Policy only refers to personal information “provided by the borrower” to the ABC application. It does not contemplate accessing the entire contact list stored in the mobile phone that was not specifically provided by the borrower. While the Privacy Policy refers to “collection purposes”, this cannot be taken as a blanket authority for excessive collection and unauthorized retention of information.

ii. Respondent FLI committed unauthorized processing in its use of the borrowers’ contacts for their debt collection.

The Complaint incorporates the findings of the Technical Report in its allegations, thus:

The READ_CONTACTS permission make it possible for their agents to call and send messages to the people in the complainant’ contacts lists.

The fact that the ABC is also able to obtain access to storage devices of complainants through READ_EXTERNAL_STORAGE permission also confirms the allegations of some complainants about the reported threats made by agents that they can view complainants; photos and can post them anywhere they want.

⁴² IRR, § 18(c), emphasis supplied.

ABC is also capable of determining the approximate and precise geographical location of the users the Global Positioning System (GPS) through cellular network information and wi-fi connection. Again, this correlates with the allegations of some complainants that collection agents knew of their work and home addresses and exact locations.

ABC is capable of manipulating information on the device through the WRITE_CALENDAR and WRITE_EXTERNAL_STORAGE dangerous permissions.

Finally, ABC is capable of manipulating application will not fully function if any one of these dangerous permissions is not approved by the user.⁴³

As summarized in the Complaint, the above dangerous permissions used by the ABC application translated into these actual experiences by data subjects:

On 6 February 2019, NPC received a complaint docketed as CID Case No. 19-B-056 filed against ABC. Complainant alleges that ABC hacked her cellphone and obtained the details of her contacts. According to complainant, she received complaints from her people and clients that ABC have (sic) been disturbing them.

xxx

Complainant in CID Case No. 19-G-613 states that persons who called her phone, some of whom were not in her phone book, were even contacted by ABC.

Complainant in CID Case No. 19-G-634 narrates that ABC contacted her team leader and sent the latter a photo of herself holding her Unified Multipurpose ID.⁴⁴

xxx

While some agents make it appear that they are contacting the complainant's phone list to aid in collection, a ABC agent in CID Case No. 19-G-573 admitted that said "text blast" was for the purpose of ruining complainant's reputation:

⁴³ Fact-Finding Report, at 11.

⁴⁴ Fact-Finding Report, at 3.

*Hello Ma'am / Sir, your loan to ABC has been overdue. We will inform your relatives and friends to urge the repayment (overdue debts) when you has been been overdue. Please cherish your reputation among friends and relatives, cherish your credibility and repay as soon as possible. Do reply if you don't want us to call of your contact references. This is the special collections team.*⁴⁵

It is worth noting that Respondent FLI has never disputed the fact that the names of their borrowers and the fact of overdue payment have been disclosed to the people in their mobile contact lists.

Instead, Respondent FLI argues in its Answer that information on the use of the borrowers' personal information for loan collection purposes was provided to the borrowers in the Credit Agreement and Privacy Policy, thus:

25. The Credit Agreement and Privacy Policy expressly provide that the borrower's contacts list on his mobile phone will be obtained by FLI and such information will be used for purposes of loan collection, in case the borrower himself is unresponsive to FLI' collection attempts.

26. Even the Fact-Finding Report quotes the foregoing provisions. While the "third parties" to whom the personal information is disclosed is not specified, the user could reasonably assume that these third parties would be engaged in activities in line with the purposes stated for the disclosure to them – "collection services, background investigation, skip tracing, among others".

27. Based on these, a user of the app who reads and agrees to the Privacy Policy could reasonably conclude and expect that first, the app will be able to collect the details on his phone's contact list, and second, FLI could communicate with those contacts for collection purposes.

The Commission disagrees. Borrowers would not have been able to reasonably expect Respondent FLI to use their phone contacts other than the reference contacts they submitted, especially because the Privacy Policy is worded this way:

ABC collects **personal information you provide us**, which may include... (vii) phone contacts in your device needed for

⁴⁵ Id. at 4.

collection purposes, if in case the information provided in the credit agreement is false, invalid or otherwise not responsive to our collection attempts.⁴⁶

The Commission, in a previous Decision, has discussed the concept of reasonable expectation of privacy in relation to informational privacy:

While the two-part test under Katz and Ople should now be construed taking into consideration the provisions of the Data Privacy Act, this concept of “reasonable expectation” may still be useful in addressing issues concerning informational privacy in relation to what controllers and processors may legitimately do. In this regard, this concept of “reasonable expectation” is considered to determine 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.**⁴⁷

Applying the foregoing concept to this case, the burden cannot be placed on the borrowers to have known what the ABC application was capable of, based on the information provided to them. The borrowers could have only expected that their entire contact lists will be utilized for collection purposes if they had known the scope, manner, and extent of Respondent FLI’ processing of their information in the first place. This is all the more true considering the broad language used in the declared purposes of the Credit Agreement, i.e. “in order to achieve the purposes of this agreement.” The declared purpose of “collection purposes” in the Privacy Policy likewise does not contemplate the indiscriminate messaging of family, friends, and acquaintances, considering the Policy referred to personal information “provided” by the borrowers. In the case of the ABC application, this pertains only to the reference contacts supplied upon the loan application.

This is bolstered by the fact that the Securities and Exchange Commission (SEC), in a Memorandum dated 19 August 2019, prohibited unfair debt collection practices of financing companies and lending companies such as the disclosure of the names and other personal information of borrowers who allegedly refuse to pay debts,⁴⁸

⁴⁶ Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019, at 6-7. Emphasis supplied.

⁴⁷ See, EU General Data Protection Regulation, Recital 47, cited in NPC Case No. 17-047.

except for circumstances provided in the same Memorandum. It also expressly provides for the confidentiality of information.⁴⁹ Given these, the Commission strongly disagrees with the claim that “the user of the app who reads and agrees to the Privacy Policy could reasonably conclude and expect that first, the app will be able to collect the details on his phone’s contact list, and second, FLI could communicate with those contacts for collection purposes”.

Respondent FLI, for good measure, states that even if there were acts of unauthorized processing, these cannot be attributed to Respondent FLI, thus:

28. If the collection agents who reach out to the borrowers’ contacts, “damage the reputation of data subjects, or harass, threaten, or coerce them to settle their loans,” as the Fact-Finding Report claims, then these acts are indeed unauthorized by the data subjects (i.e., beyond the consent they had given to FLI) but at the same time, these were neither authorized by FLI. Acts that damage the reputation of data subjects or coerce them to settle their loans are personal acts of the collection agents who, when they do these, act beyond the authority given to them by the data subjects and FLI.

Respondent FLI cannot be absolved of the violations of the DPA on the argument that the processing in relation to the collection was subcontracted to CSA.

In fact, during the Hearing, the Commission was able to elicit the actual arrangement between Respondent FLI and its collection agent, CSA. It sought clarification about one of the attachments in the Compliance submitted by FLI, specifically the slide about the “ABC Product Description.”⁵⁰ It noted that there was a department in FLI for a “Collector,” as described in their company organization structure:

⁴⁸ SEC Memorandum Circular No. 18. Prohibition of Unfair Debt Collection Practices of Financing Companies (FC) and Lending Companies (LC). Dated 19 August 2019. Section 1(d).

⁴⁹ *Ibid.*, at Section 2.

⁵⁰ Annex “E” is a copy of the presentation of FLI on its ongoing efforts for data collection and usage as well as optimization of data collection systems

Part 1.1 Company Organizational Structure

- COLLECTOR. Responsible for the collection of overdue users, sending reminders through calls and SMS.
- QUALITY ASSURANCE. Enforces rules developed with aid from the Legal Department, by checking the call recordings of the collections, and imposing sanctions when warranted.
- LEGAL. Evaluates contracts and helps QA with inspections to determine collection rules. Handles customer complaints when it comes to questions of law.⁵¹

The counsel for Respondent FLI answered that the collector is an outsourced party, CSA.⁵²

Even if it were true that the Collection Department was outsourced to a service provider, Respondent FLI's own Organizational Structure reveals that it considered debt collection as an integral part of its business, meriting its own department. During the Hearing, the counsel for Respondent FLI admitted to the Commission that the "Collector" department had a supervisor to whom reports were submitted.⁵³

The DPA defines a Personal Information Controller 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, hold, process, use, transfer or disclose personal information on his or her behalf." In this case, Respondent FLI is the corporation that operates the ABC online lending application, which is the service that collects and processes personal information of its borrowers. Thus, Respondent FLI is the Personal Information Controller. It cannot escape the fact that it was in the position to control and exercise discretion over what personal information is processed and the extent of its processing. It is likewise registered with the National Privacy Commission as a Personal Information Controller belonging to the Online Lending Sector.⁵⁴

⁵¹ Ibid. Emphasis supplied.

⁵² See, Transcript p. 8.

⁵³ See, Transcript at 23-25.

⁵⁴ Fact-Finding Report, Annex B.

The DPA provides for the Principle of Accountability and concomitant obligations for Personal Information Controllers, thus:

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. xxx

(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.

(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.⁵⁵

The arguments of Respondent FLI, therefore, must fail for lack of basis in the law.

C. Respondent FLI did not violate Section 28 (Processing for Unauthorized Purposes) of the DPA.

Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes is committed when:

1. A person processed information of the data subject;
2. The information processed is classified as personal information or sensitive personal information; and
3. The processing of personal information is for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

As discussed previously, the first and second elements are met in this case. The third element, which should differentiate Processing for

⁵⁵ R.A. 10173, Section 21.

Unauthorized Processing under Section 25, does not apply in this case.

Although seemingly similar, the application of principles in statutory construction would require a differentiation between the two (2) provisions:

Moreover, under the maxim *noscitur a sociis*, where a particular word or phrase is ambiguous in itself or is equally susceptible of various meanings, its correct construction may be made clear and specific by considering the company of words in which it is founded or with which it is associated. This is because a word or phrase in a statute is always used in association with other words or phrases, and its meaning may, thus, be modified or restricted by the latter. The particular words, clauses and phrases should not be studied as detached and isolated expressions, but the whole and every part of the statute must be considered in fixing the meaning of any of its parts and in order to produce a harmonious whole. **A statute must be so construed as to harmonize and give effect to all its provisions whenever** possible. In short, every meaning to be given to each word or phrase must be ascertained from the context of the body of the statute since a word or phrase in a statute is always used in association with other words or phrases and its meaning may be modified or restricted by the latter.⁵⁶

Applying the foregoing principle in this case, the Commission notes that the qualifier “unauthorized” attaches to “processing” under Section 25, and to “purposes” under Section 28. Thus, Section 28 contemplates processing that was initially authorized either by consent of the data subject or some other lawful basis, but subsequently became invalid when the processing went beyond the consent given or the authority provided by law.

In this case, the dangerous permissions in the ABC application allowed it to retain information without consent or other lawful basis in the DPA. Since such processing activity was never authorized either by consent or some other authority in law, it was illegal from the beginning, hence the third element does not apply in this case.

⁵⁶ Chavez v. JBC, et. al. G.R. 202242. Dated 17 July 2012.

D. The penalty shall be imposed upon the Board of Directors, as responsible officers who by their gross negligence, allowed the commission of the crime.

Having established that Respondent FLI has committed Unauthorized Processing under Section 25 of the DPA, the Commission refers to Section 34 of the law:

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.⁵⁷

Respondents FLI, CW, ML and BSJ, in their Answer, argue that they should not be liable for criminal acts unless their active participation can be proven, thus:

1. With respect to Sections 25, 28, 31, and 32 of the DPA, **a criminal offense will be committed only by individuals who actually committed the criminal act.**
2. FLI and its directors and officers such as ML, CW, and BSJ. could not be held liable for criminal violations of Sections 15, 28, 31, and 32 of the DPA because they did not at all engage or participate in, or consent to, (a) unauthorized processing; (b) unauthorized disclosure of personal information of the app users (collectively, the “Criminal Acts”).
3. If FLI, as a company, adopted policies that promoted and call for, or was aware of, the commission of the Criminal Acts, then the company and its responsible directors and officers would have been correctly impleaded as respondents.

⁵⁷ R.A. 10173, Section 34. Emphasis Supplied.

4. However, there is no showing by the Honorable Commission or the complainants that FLI observed or is observing a policy that promotes and calls for the commission of the Criminal Acts. Neither is there proof that FLI and its officers knew of the Criminal Acts;

xxx

18. It is not true that FLI and its directors / officers have “knowledge of the practices of its agents or other people clothed with the authority to collect outstanding loans” because, in fact, the collection agents who committed debt-shaming practices did so without the knowledge of FLI and its directors / officers. It then follows that without any knowledge of FLI and its officers, the respondents could not have consented to the acts of the collection agents, whether expressly or impliedly.⁵⁸

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.

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, 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.”⁵⁹

In this case, the Board of Directors of FLI did not deny the fact that a Master Service Agreement was entered into between Respondent FLI and CSA, with the President as the signatory. The Board of Directors should have been aware of the terms in this Agreement, considering that it concerns a vital aspect of their operations as a lending company.

Consequently, they should have been aware that the provisions of the Master Service Agreement contradicted the principles in the DPA.

⁵⁸ Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019 at p. 3.

⁵⁹ Fernandez v. Office of the Ombudsman, G.R. No. 193983. 14 March 2012.

It included a provision that sought to surrender its accountability as a Personal Information Controller to CSA, thus:

Article I Scope of Service

Section 5. Methods of Work. **The service shall be performed by the Contractor in accordance with means and methods of work determined solely by it**, on the understanding that the company shall exercise control over the contractor only in regard to the results of the service.⁶⁰

This provision is contrary to DPA which is very clear that the subcontracting of personal information by Personal Information Controllers cannot include the responsibility to prevent unauthorized processing, thus:

Section 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.⁶¹

Despite this provision, Respondent FLI still was not entirely powerless under the Master Service Agreement. This responsibility under law could still have been exercised by Respondent FLI through certain provisions in the Master Service Agreement which contained remedies that they should have exercised as the Personal Information Controller after voluminous complaints were filed against it, such as:

⁶⁰ Compliance dated 20 February 2020, Annex “C”. Emphasis supplied.

⁶¹ R.A. 10173, Section 14. Emphasis Supplied.

Article VI.

Unprofessional practices in the performance of the service and breach of contract.

XXX

Section 2. PENALTIES. The CONTRACTOR acknowledges that the unprofessional performance on the SERVICE may compromise and damage the goodwill and public reputation of the COMPANY. In addition to the COMPANY's remedies under this Agreement or under the general civil law for unprofessional performance of the SERVICE, the COMPANY shall likewise be entitled to be compensated for the damages caused thereby whether committed by the CONTRACTOR itself or any of its representatives, agents, or employees.

In case of suit by the COMPANY against the CONTRACTOR arising from such unprofessional practices, or any other breach or violation of any provision of this Agreement, the COMPANY shall be entitled to recover from the CONTRACTOR any and all expenses incurred by the COMPANY in investigating the matter, recovering any amounts lost to the COMPANY, or completing or rectifying defective works or service.⁶²

During the Hearing, however, the counsel for Respondent FLI stated that they were not aware of a specific instance of an action taken by FLI against CSA.⁶³

In its Compliance dated 26 November 2020, the counsel for Respondent FLI submitted supposed Disciplinary reports from CSA in relation with potential data privacy violations committed by their collection agents.⁶⁴

In the four (4) submitted Disciplinary Report Forms, however, the offenses cited were simply "using the phone" and "exploring the post loan system to get the number of the user." These do not describe the unprofessional debt collection practices that have led to the hundreds of complaints filed before the Commission. These Disciplinary Report Forms also do not state what action was taken by either CSA or FLI, either through reprimands, suspensions, or terminations. The Commission cannot consider these submissions as proof of FLI's responsibility in preventing unauthorized processing by its subcontractors.

⁶² Fact-Finding Report, Annex "B". Emphasis in the original.

⁶³ See, Transcript at 39.

⁶⁴ Compliance dated 26 November 2020, Annex 1.

The Commission likewise notes the Verified Answer of Respondents KF, JG, and HJL which claims that they should be absolved based on the supposed the fact that they are nominal directors, thus:

3.1 On 19 June 2018, respondents acted as nominee stockholders for the incorporation of respondent FLI before the Securities Exchange Commission.

xxx

3.3. Thereafter and until the present time, respondents were not involved directly or indirectly with respondent FLI management and the day to day operations of the company.

xxx

4.1. Respondents did not participate in the management of respondent FLI as well as the operation of its ABC online lending business.

xxx

a. In the case at bar, respondents although listed as board of directors and office or respondent FLI, they did not participate directly or indirectly in the management and operation of the ABC online lending business.

xxx

b. Respondents cannot also be considered to have acted in gross negligence in allowing the alleged commission of the acts for, as already emphasized, they are not involved in the management and daily operations of FLI Hence, they could not have allowed the alleged commission of the acts complained of.⁶⁵

The fact remains that all the directors were incumbent members of the Board of Directors of FLI during the date of the violations. Members of the Board are presumed to participate as such. While the individual Respondents were given opportunities to dispute this presumption, they never did so.

⁶⁵ Verified Answer dated 4 October 2020, p. 2.

The Commission has formerly ruled in the NPC Case 19-605, thus:

In the case of Alfredo Ching vs. Secretary of Justice⁶⁶, the Supreme Court held that the Board of Directors shall be held criminally liable for violations committed by the corporation when by reason of the latter's negligence to supervise its employees, it has caused the corporation to commit acts in violation of the law, viz:

“Though the entrustee is a corporation, nevertheless, the law specifically makes the officers, employees or other officers or persons responsible for the offense, without prejudice to the civil liabilities of such corporation and/or board of directors, officers, or other officials or employees responsible for the offense. The rationale is that such officers or employees are vested with the authority and responsibility to devise means necessary to ensure compliance with the law and, if they fail to do so, are held criminally accountable; thus, they have a responsible share in the violations of the law.

xxx xxx xxx

A crime is the doing of that which the penal code forbids to be done, or omitting to do what it commands. A necessary part of the definition of every crime is the designation of the author of the crime upon whom the penalty is to be inflicted. When a criminal statute designates an act of a corporation or a crime and prescribes punishment therefor, it creates a criminal offense which, otherwise, would not exist and such can be committed only by the corporation. But when a penal statute does not expressly apply to corporations, it does not create an offense for which a corporation may be punished. On the other hand, if the State, by statute, defines a crime that may be committed by a corporation but prescribes the penalty therefor to be suffered by the officers, directors, or employees of such corporation or other persons responsible for the offense, only such individuals will suffer such penalty. Corporate officers or employees, through whose act, default or omission the corporation commits a crime, are themselves individually guilty of the crime.

⁶⁶ G.R. No. 164317, February 6, 2006.

The principle applies whether or not the crime requires the consciousness of wrongdoing. It applies to those corporate agents who themselves commit the crime and to those, who, by virtue of their managerial positions or other similar relation to the corporation, could be deemed responsible for its commission, if by virtue of their relationship to the corporation, they had the power to prevent the act. Moreover, all parties active in promoting a crime, whether agents or not, are principals. Whether such officers or employees are benefited by their delictual acts is not a touchstone of their criminal liability. Benefit is not an operative fact.”

Further, the Board of Directors has the duty of diligence. As provided by the Supreme Court in one case, directors or officers of a corporation are expected to exercise reasonable care and prudence in the performance of their duties and responsibilities.⁶⁷

It is the persons behind FLI who allowed the harassment of its borrowers through the Master Service Agreement that surrendered all accountability to its subcontractor. These persons provided the approvals for the ABC application’s functionalities and dangerous permissions. They were the ones who lacked supervision over the representations it made to all of FLI’ borrowers.

Had the ABC application confined itself to the purposes FLI itself declared in the Privacy Policy, the collection agents would have only had access to the reference contacts whom the borrowers willingly indicated in their application.

Time and again, the Commission emphasizes the role that Personal Information Controllers play in ensuring that the innovation and growth that happens in the Philippines continue to abide by the laws and ethical practices, leading to products and services that are free from any doubt on their security and informational privacy.

⁶⁷ NPC Case No. 19-605.

WHEREFORE, all these premises considered, this Commission hereby:

1. FINDS that Respondent FLI and its Board of Directors, namely, ML, CW, KF, JG, HJL, as responsible officers, have violated Section 25 of the Data Privacy Act; 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 under Section 25 of the Data Privacy Act, for its further actions.

SO ORDERED.

City of Pasay, 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:

QG LAW OFFICES

Counsel

Counsel for FLI, ML, CW, and BSJ

GNGA& ASSOCIATES

Counsel for Respondents KF, JG
and HJL

COMPLAINTS AND INVESTIGATION DIVISION

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

JCR

Complainant,

-versus-

CID Case No. 17-K-001

*For: Violation of the Data
Privacy Act of 2012*

GLOBE TELECOM, INC

Respondent.

X-----X

RESOLUTION

AGUIRRE, D.P.C.:

This Resolution refers to the Compliance Report dated 03 February 2020¹ submitted by Respondent Globe Telecom, Inc. involving a complaint filed by Complainant JCR for alleged violations of Republic Act 10173 (“Data Privacy Act”).

The Facts

On 05 December 2019, this Commission issued a Decision² with the following disposition:

WHEREFORE, all the premises considered, the Commission finds no violation of the Data Privacy Act on the part of Respondent Globe Telecom, Inc. that is sufficient to warrant a recommendation for criminal prosecution. This Commission finds, however, that Respondent failed to adopt and implement the necessary policies and procedure relating to the prevention, correction, and mitigation against security incidents that can lead to a personal data breach.

The Commission hereby ORDERS Respondent Globe Telecom to submit a complete report on the measures it has undertaken or will undertake to address the issue of delayed SIM deactivation such as in this case, including the timeline for the implementation of such

¹ Compliance Report dated 3 February 2020.

² Decision dated 5 December 2019.

measures, within thirty (30) days from receipt of this Decision. Reference may be made to the requirements provided in the Implementing Rules and Regulations of the Data Privacy Act, particularly Section 28, paragraphs (c), (d), (e), and (f).

On 05 February 2020, this Commission received the Compliance Report of Respondent which included its Policy and Procedure Manual (PPM)³ concerning the Postpaid Change SIM Process in its Globe stores. Respondent claims that the PPM, which has been effective since 2018, outlines the procedure for processing requests to replace lost and defective SIM cards as well as to upgrade the same. Stringent subscriber verification protocols are in place to ensure that lost SIM cards are deactivated, and that replacement SIM cards are issued to the account owner on record within the same day of request. As a safeguard against privacy and security risks, a replacement SIM card will not be issued in case of incomplete submission of requirements, mismatched proof between identification details and customer details in the Globe My Business Support System, and failure to provide correct answers to any of the six (6) account verification questions.⁴

On 03 August 2020, the Enforcement Division of this Commission issued an Enforcement Letter⁵ ordering the Respondent to submit a more comprehensive report on the measures it has undertaken to avoid the issue of delayed SIM deactivation in the future, within ten (10) days from their receipt of the letter. Respondent received the letter on 10 August 2020. The letter stems from the Enforcement Division's finding that while the PPM contains safeguards to prevent unauthorized persons to claim another's SIM card replacement, it did not identify possible controls to avoid delayed SIM card replacement due to human error or other technicalities.⁶

On 20 August 2020, Respondent submitted a Comprehensive Report⁷ where it outlined the steps it has taken in order to address the issue at hand, particularly the changes it has made in its PPM for both postpaid and prepaid subscribers which were cascaded to all its employees. Respondent introduced enhancements in its procedure to ensure the restoration of the availability and access to personal data in a timely manner in the event of physical or technical incident. To make sure that only the account holder or his or her authorized representative can access the account, mandatory verification questions specific to the lost phone or SIM card will be asked before the temporary deactivation of the line.⁸

³ Ibid.

⁴ Letter to the National Privacy Commission dated 3 February 2020.

⁵ Enforcement Letter dated 3 August 2020.

⁶ Ibid.

⁷ Globe's Comprehensive Report dated 20 August 2020.

Nonetheless, Respondent also stated that pursuant to the Service Level Agreement (SLA), SIM deactivation should take effect within one (1) day. The Respondent admitted that the delayed deactivation of herein Complainant's SIM went beyond the period stated in the SLA and that it is conducting an investigation on the matter in order to issue appropriate sanctions against the erring officers and employees.⁹

Discussion

This Commission hereby considers the instant case as closed. Section 28 of the Implementing Rules and Regulations of the Data Privacy Act of 2012 provides for the guidelines for technical security measures:

Where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures:

- a. A security policy with respect to the processing of personal data;
- b. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;
- c. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;**
- d. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach;**
- e. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;**
- f. A process for regularly testing, assessing, and evaluating the effectiveness of security measures;**

⁸ Ibid.

⁹ Ibid.

g. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.¹⁰

In this case, it is noteworthy that Respondent has a PPM, which has already been effective since 2018. The PPM provides for the procedure of processing requests for replacement and upgrading of SIM cards. As a privacy and security measure, Respondent implements stringent subscriber verification protocols to guarantee the timely deactivation and proper replacement of lost SIM cards. Now, it has already introduced improvements in its procedure to ensure the restoration of the availability and access to personal data in a timely manner in the event of physical or technical incidents. Moreover, it has also implemented certain mechanisms to ensure that only the account holder or his or her authorized representative can access the account through the conduct of mandatory verification process.

The foregoing technical security measures employed by Respondent are deemed sufficient to prevent, correct, and mitigate security incidents that can lead to a personal data breach in view of the previous Decision¹¹ of this Commission. However, it should be noted that Respondent should hold its personnel accountable when there is delay in the deactivation and replacement of SIM cards to ensure strict compliance with its privacy policies and procedures and prevent similar incidents in the future.

WHEREFORE, premises considered, the case of JCR v. Globe Telecom, Inc. is hereby considered CLOSED. Furthermore, Globe Telecom, Inc.'s representations to comply with its Service Level Agreements (SLAs), and Policy and Procedure Manual (PPM) are hereby NOTED for future reference and assessment.

SO ORDERED.

Pasay City, Philippines;
10 September 2020.

¹⁰ Emphasis supplied.

¹¹ Supra note 1.

(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:

JCR
Complainant

CASTELO UNGOS CASIÑO & TUBAYAN
Counsel for Respondent Globe Telecom, Inc.
28/F, The Globe Tower, 32nd St. corner, 7th Avenue
Bonifacio Global City, Taguig 1634

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

JBD

Complainant,

-versus-

CID Case No. 18-D-012

*For: Violation of the Data
Privacy Act of 2012*

JI and VVV

Respondent.

X-----X

ORDER

AGUIRRE, D.P.C.:

Before this Commission is a Complaint filed by Complainant JBD against the respondents JI and VVV for an alleged violation of R.A. 10173 (“Data Privacy Act”).

The Facts

Complainant here alleges that his Social Security System (“SSS”) Employment and Payment history were illegally obtained by Respondent JI, his common law spouse, and her lawyers. He learned about this when he received a Position Paper against him with attached print-outs from the SSS. These contained his birthdate and SSS number, as well as his employment history and actual premiums.¹ This Position Paper was filed with the Professional Regulation Commission (“PRC”) in connection with an ongoing case involving him and Respondent JI.

Complainant initially filed a complaint before the SSS. Upon inquiring with SSS, he was told by its Fraud and Legal Department that this data was not processed within the vicinity of the agency, and that an unauthorized individual accessed the SSS data portal where his work history and premiums were collected. ²

¹ Records, p. 9-10.

Upon the filing of this Complaint with the National Privacy Commission, the parties were called for a Discovery Conference. Complainant and Respondent VVV were present, but Respondent JI failed to appear.

During the Discovery Conference, the parties manifested that they were not willing to enter into an amicable settlement. They further manifested that there is no need to secure evidence from each other to further their case.

Hence, an Order was issued by the Commission on 12 July 2018 directing Respondents to file their responsive Comment until 22 July 2018. Complainant was in turn given ten (10) days from the receipt of the Comment to file his Reply.

Arguments of the Parties

In his Complaint, Complainant argues that his SSS personal information was disclosed by Respondent VVV to PRC without his consent and for unauthorized purposes. He asserts that the contents of his SSS personal data were not authorized and authenticated by the organization since the annexes are pictures only from a personal computer of a certain individual who has access to the SSS data portal. He also alleges that he gave no consent for Respondents to acquire the sensitive personal information they presented as evidence in the PRC case.³ He prays for moral damages for the anxiety, sleepless nights, and extreme emotional pain that this caused.⁴

In their Comment, Respondent VVV asserts that he and his law firm are not covered by the Data Privacy Act, stating thus:

Under [Sections 3 and 4] of the Data Privacy Act, it can be deemed that Respondent VVV and Law Firm is not covered nor violated any provisions in [The Data Privacy Act] for the reason that respondents are not considered as personal information controller and processors... It is clear that Respondent VVV and Law Firm are not involved in personal information and even not [sic] considered as personal information controller and processors.⁵

² Id., p. 59.

³ Id., p. 5.

⁴ Ibid.

He asserts that the Complaint must be dismissed outright, following the provisions of NPC Circular 16-04:

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;

xxx

d. There is insufficient information to substantiate the allegations in the complaint.⁶

They likewise argue that Complainant did not comply with the Exhaustion of Remedies provision under the same Circular:

Assuming without necessarily admitting that the complaint falls within the scope of this Honorable Commission, it is seemingly obvious that the Complainant did not comply with the exhaustion of remedies as there is no evidence showing that he informed, in writing, the personal information controller or concerned entity of the privacy violation or personal data breach to allow for appropriate action.⁷

Respondent VVV also raises the fact that Complainant attached a photocopy of pictures as his sole evidence and that it was not authenticated in accordance with the Rules on Electronic Evidence.⁸ On the same note, he cites the best evidence rule:

A photocopy, being a mere secondary evidence, is not admissible unless it is shown that the original is unavailable... Complainant cannot claimed [sic] thereafter that he was not given any time or opportunity to have his evidence authenticated as he was advised of his right to the assistance of counsel on the Order to Confer for Discovery dated 29 June 2018. Likewise, during the discovery conference dated 12 July 2018 complainant waived his right in connection to said authentication of evidence.⁹

According to Respondent VVV, lawyers act as mere agents to their clients and the pieces of evidence are provided by the client.

⁵Id., p. 48.

⁶Section 12, NPC Circular 16-04. Dated 15 December 2016.

⁷Id., p. 49-50.

⁸Id., p. 50-51.

⁹Id., p. 51.

Respondent VVV asserts he acted as a substitute counsel at the time he handled the Respondent JI's case with the PRC. Being a substitute counsel and due to time constraint, he states that he only relied on the pieces of evidence presented by his client, Respondent JI.¹⁰

Respondent JI, on the other hand, has not filed a Responsive Comment despite being copy furnished the Order to Confer for Discovery and the Order to file a Responsive Comment. It was manifested as well during the Discovery Conference that Respondent VVV is not representing Respondent JI in this case.¹¹

In the Verified Reply, Complainant asserts that the allegations constitute a violation of the Data Privacy Act:

10. [R]espondents violated the said data privacy law. The Social Security System disclosed that SSS premiums and work history of the Complainant were not processed within the vicinity of the agency. Hence, a certain individual, according to the Fraud and Legal Department, has unlawfully accessed the SSS data portal so the work history and premiums were collected.¹²

Complainant states that the Order by the Commission to the parties to confer for Discovery justified that the complaint reviewed by the Honorable Commission offers substance, hence their findings in the Order that the "allegations are sufficient."¹³

As to the issue that the evidence is a mere photocopy that was not authenticated, Complainant states:

We respectfully emphasize that the SSS employment – Work history and actual premiums presented in the Honorable Board did not come from the Complainant but from the Respondents, JI and VVV, instead.¹⁴

For Complainant, both the lawyer and his client are liable under the Data Privacy Act. He states thus:

19. In their PRC Position Paper, they [used] unlawfully and maliciously disclosed the Complainants SSS details. Their common position to use the same is unlawful under the above law. They are both bound by the same.¹⁵

¹⁰ Id., p. 51.

¹¹ Id., p. 54.

¹² Id., p. 59.

¹³ Ibid.

¹⁴ Records, p. 60.

¹⁵ Id., p. 61.

Moreover, he asserts that the lawyer should be considered as a personal information controller, to wit:

22. NPC has jurisdiction over the respondent [Respondent] VVV since he is considered as a personal information controller for instructing another person to collect, hold, process, use, transfer and disclose personal information on his behalf. As such, he should have provided the Honorable Commission on when, where, who, and how they were able to unlawfully obtained [sic] Complainant's SSS personal information.¹⁶

Issues

- a. Whether the Complaint should be dismissed for non-exhaustion of remedies;
- b. Whether Complainant violated the Best Evidence Rule, precluding the Commission from taking cognizance of the photocopies of the SSS documents;
- c. Whether the Respondent VVV should be treated as an agent and not a personal information controller;
- d. Whether the Complaint should be dismissed for insufficient substantiation of the allegations in the Complaint; and
- e. Whether Respondents committed unauthorized processing of Complainant's SSS employment history and actual premiums.

Discussion

Respondent VVV argues that Complainant failed to exhaust remedies available to him as they were not informed of the alleged violation prior to the filing of the instant case. The alleged privacy violation subject of this case supposedly resulted from the access and disclosure to the PRC of Complainant's SSS documents without his knowledge and consent. Contrary to the contention of Respondent VVV, to require Complainant to first exhaust his remedies with the Respondents would be unreasonable. First, Respondents already accessed and submitted the SSS documents of Complainant as evidence in the PRC case. These facts were never disputed. Second, there is nothing in the records or the statements and submissions of the Respondents show either their willingness or capability to provide an adequate remedy to Complainant. The requirement to exhaust available remedies does not contemplate exercises in futility that only delay justice for data subjects whose rights are violated.

¹⁶Ibid.

In addition, the Commission emphasizes that this requirement in Circular 16-04 also provides that:

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 complainant.¹⁷

Respondent VVV also claims that Complainant violated the best evidence rule, citing the fact that the evidence provided showing the alleged SSS employment history and actual premiums is a mere photocopy. The Commission reminds Respondent that the best evidence rule applies only when the subject of the inquiry is the contents of the document.¹⁸ In this case, the intent of Complainant in submitting the photocopy of the SSS employment history and actual premiums is to show that his personal and sensitive personal information was used as evidence in a PRC case without his knowledge and consent. The accuracy of the SSS premiums or the details of Complainant's employment history is not in dispute.

The Commission notes that the fact that Complainant's SSS documents were accessed and used without his consent was never disputed by Respondents.

These documents contained not just his employment history and premiums but his date of birth and SSS Number as well. These fall squarely under the enumeration of what is considered sensitive personal information under the Data Privacy Act:

I) 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;

xxx

(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;¹⁹

¹⁷Supra note 6 at Section 4.

¹⁸ Section 3, Rule 130, Rules of Court.

¹⁹Section 3 (I), R.A. 10173. Emphasis supplied.

Absent any basis to process such sensitive personal information,²⁰ the access and use of Complainant's SSS documents as attachments in a position paper may constitute unauthorized processing under Section 25 of the Data Privacy Act.

In the interest of giving due course to Complainant's claims, the Commission resolves to order Complainant to provide the following:

1. A Certified True Copy of the Position Paper containing the subject SSS documents filed with the PRC; and
2. Documents to substantiate the allegations made in Paragraph 10 of the Verified Reply which refers to the findings of the SSS Fraud and Legal Department.

The foregoing is pursuant to NPC Circular 16-04 which provides that the Commission may, on the basis of its review of the evidence, order the conduct of a clarificatory hearing if in its discretion, additional information is needed to make a Decision.²¹ ²⁰

²⁰ 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:

(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.

²¹ Supra note 6, at Section 21.

WHEREFORE, all the above premises considered, the Commission hereby **ORDERS** Complainant JBD to submit the documents enumerated above within fifteen (15) days from receipt of this Order. The failure of Complainant to submit such documents shall cause this case to be submitted for resolution.

SO ORDERED.

Pasay City, 21 May 2020.

(sgd)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Concurring:

(sgd)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(sgd)
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED

JBD
Complainant

JI
Respondent

VVV
Respondent

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission



ORDER

IN RE: LISENSYA.INFO
Initiated as an Independent NPC
Investigation into the Possible Data
Privacy Violations Committed by the
website LISENSYA.INFO.

For: Violation of the
Data Privacy Act) of
2012

X-----X

CEASE AND DESIST ORDER

LIBORO, P.C.:

This resolves the Application for Issuance of Cease and Desist Order of the National Privacy Commission (NPC)'s Complaints and Investigation Division (CID)¹ pursuant to a Sua Sponte Investigation against respondent Lisensya.Info for unauthorized processing and unauthorized access of personal information and sensitive personal information which are violations of the Data Privacy Act of 2012 (DPA).

FACTS

The website Lisensya.Info depicts itself as one connected with the Land Transportation Office (LTO).

In an effort to inform the public of the fact that this website is not related to the LTO, on 05 November 2020, the LTO posted on its Facebook page a warning to the public stating, in part, "*Ang lisensya.info website ay HINDI pinapatakbo o konektado sa ahensya ng LTO. Para sa kaligtasan ng lahat, huwag po tayong magbigay ng SENSITIBONG IMPORMASYON sa UNVERIFIED links o accounts.*"²

¹ Application For Issuance of Cease and Desist Order dated 11 November 2020.

² <https://www.facebook.com/lto.cdmpao/photos/a.1589028444448324/4945107912173677/> (last accessed 09 November 2020).

On 08 November 2020, Manila Bulletin published an online article entitled “LTO exposes thousands of information due to misconfiguration”³. The article is anchored on the independent investigation of AJ Dumanhug (Dumanhug), an independent cybersecurity analyst published on his blog⁴.

Dumanhug, on his blog dated 08 November 2020, states that the website has two (2) main features, Driver’s License Authenticator (DLA) and Motor Vehicle Authenticator (MVA). The DLA feature asks for user’s license number and birthday and once those information are submitted, the name of the license’s owner and the expiration date would be revealed. Meanwhile, the MVA asks users to submit just the Motor Vehicle File Number and would show sensitive information like the make, plate number, engine number, chassis number, registration expiry date and the name of the owner⁵.

Dumanhug also mentioned how the acquired the personal data are stored by the said website. He further stated that one can see that the website is using the Application Programming Interface (API) endpoint of LTO.net.ph, an official website of LTO, by viewing the source code of the PHP files downloaded on the git repository of Lisensya.Info⁶.

Upon knowledge, the CID commenced its investigation on the developing issue. In this initial data gathering, the CID found out that:

- 1) The website Lisenysa.Info has been in existence as early as 15 September 2019; and
- 2) It has neither a privacy notice nor any contact details of its owner⁷

CID has communicated with the registered Data Protection Officer of the LTO – Atty. Romeo G. Vera Cruz (LTO Executive Director) for them to shed light on the incident considering that the information

³<https://mb.com.ph/2020/11/08/lto-exposes-thousands-of-information-due-to-misconfiguration/>.

⁴ Ibid.

⁵ https://atom.hackstreetboys.ph/lisensya-website-and-why-you-should-never-useit/?fbclid=IwAR0meSLYGlpSib0h-WioJKo_V_94GBgrM8-bzx7gkn_uGHmHi3jlaNzQniO (last accessed 09 November 2020).

⁶ Ibid.

⁷ Preliminary Report on Lisensya.Info/ LTO dated 09 November 2020.

being provided by Lisensya.Info may be found on their database. The DPO committed to file a breach notification report with the NPC.

On 09 November 2020, the CID further conducted an in-depth investigation regarding the blog post of Dumanhug dated 08 November 2020 regarding the website Lisensya.Info.

The examiners were able to get the dump files from the website Lisensya.Info, and captured sensitive information from the captured dump file of the website.

Through the source code, the examiners found the following information⁸:

- 1) Author of the website is **Jose Minao** with email address **joseminao@pm.me**;
- 2) Project is named **ValidateDL**; and
- 3) The website is using the API endpoint from LTO.net.ph, one of the official website of LTO to retrieve some information.

Using the captured information, the examiners searched at github.com and found a repository result under user yoseminao updated on 14 September 2020. The date coincides from the gathered information on the creation of the website Lisensya.Info.

Under the _config.yml of ValidateDL, the examiners found that the owner of the URL of the website **https://lto.pinoydev.org**. is also **Jose Minao** with email address **joseminao@protonmail.com**.

The examiners checked the Whois history of the url pinoydev.org and found the owner **Billy James Jimena** from Cagayan De Oro, Misamis Oriental, Philippines with email address **billyjamesjimena@yahoo.ca**.

After full extraction of the source code of the website Lisensya.Info, the examiners have validated the following⁹:

⁸ Technical Report dated 10 November 2020.

⁹ Supplemental Technical Report dated 11 November 2020.

- 1) There are 9,953 saved driver's license information on the developer's server;
- 2) There are 19,412 saved motor vehicle file number information on the developer's server; and
- 3) The website captures the following information:

For the Driver's License Validation:

- a) License Number ;
- b) Birthdate ;
- c) Sex;
- d) First Name, Middle Name and Last Name; and
- e) Expiry Date.

For the Motor Vehicle Number Validation:

- a) Motor Vehicle Number;
- b) Plate Number ;
- c) Chassis Number;
- d) Vehicle Make;
- e) Vehicle Series;
- f) First Name, Middle Name and Last Name of owner;
- g) Registration Date; and
- h) Classification of vehicle use whether private or public.

As of 11 November 2020, the LTO.net.ph website is no longer accessible, while Lisensya.Info is still fully accessible.

On the Application for Issuance of Cease and Desist Order dated 11 November 2020, the CID prays that its request for the issuance of a Cease and Desist Order against Lisensya.Info be granted by the Commission, and consequently require Lisensya.Info to stop processing the personal and sensitive personal information in its possession in order to preserve and protect public interest and the rights of the data subjects.

Discussion

The NPC is an independent body created to administer and implement the provisions of the DPA. As provided in Section 7 of the DPA, the NPC has Rule Making, Advisory, Public Education, Compliance and Monitoring, Complaints and Investigation, and Enforcement powers¹⁰ to enable it to protect the fundamental human right of privacy while ensuring the free flow of information to promote innovation and growth.¹¹

Section 7(b) of the DPA specifically states that it is the mandate of the NPC to:

“(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;” (Emphasis supplied)

In the exercise of its rule-making power and to flesh out the provision above, the NPC issued NPC Circular 16-04 (NPC Rules of Procedure) on 15 December 2016. Section 3 thereof provides who may file complaints with the Commission:

“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.”

¹⁰ See, RA 10173, Section 7.

¹¹ See, *Id.*, Section 2.

Further, Section 23 of the NPC Rules of Procedure provides for the NPC's 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."

In addition, the DPA explicitly provides for the Commission's power to issue Cease and Desist Orders:

"Section 7 (c). Issue cease and desist orders, impose a temporary or permanent ban on the processing personal information, upon finding that the processing will be detrimental to national security and public interest."

This was reiterated in the Implementing Rules and Regulations (IRR) of the DPA:

"Section 9. Functions. The National Privacy Commission shall have the following functions:

xxx

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 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.”
(Emphasis supplied)

Furthermore, Section 4 of the recently issued NPC Circular No. 20-02 (Rules on the Issuance of Cease and Desist Orders) provides that the grounds for the issuance of Cease and Desist Order are the following:

“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.”

From the foregoing, it can be seen that three (3) elements are required for this Commission to validly exercise its power to issue a Cease and Desist Order, *to wit*:

1. There must be a finding of a practice or act that an entity is doing, threatening, or about to do, which constitute a violation of the DPA, its IRR, or other related issuances;
2. Such act or practice is or will be detrimental to national security or public interest, or the issuance is necessary to preserve and protect the rights of the data subject; and
3. The commission or continuance of such act or practice, unless restrained, will cause grave and irreparable injury to a data subject.

Based on the facts and initial result of the technical investigation, the Commission finds that substantial evidence has established the

concurrence of the grounds for the issuance of a Cease and Desist Order against Lisensya.Info.

Lisensya.Info is doing some act or practice in violation of the DPA and its IRR

In sum, there is sufficient ground to support the finding that Lisensya.Info violated the following penal provisions of law:

SEC. 25. *Unauthorized Processing of Personal Information and Sensitive Personal Information.* – (a) The unauthorized processing of personal information 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 process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

(b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

xxx

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.

The initial investigation and the technical report have clearly shown that the processing of the personal data on Lisensya.Info is without the consent of the affected data subject, or without authority under the DPA or any existing law, which is a blatant and complete violation of the DPA.

Lisensya.Info displays the logo of the LTO prominently in its website pretending to be an official government website. It processed the personal data of the data subjects, the owners of the driver's license and motor vehicle file number, by storing the unlawfully obtained information from LTO in its website and using them to "verify" entries by the public without their consent or authority of law., as defined under Section 13 of the DPA.

The license number, birthday, sex, and plate number are sensitive personal information that are generally prohibited to be processed except under the circumstances provided under Section 13 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:

(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.

As quoted above, there is a set of criteria provided in the DPA for the lawful processing of sensitive personal information. To rely on consent as the lawful basis for procession, an examination must be made whether such consent was freely given, specific, informed, and an indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her¹².

Consent is considered freely given, specific and informed when it adheres to the principles to the general data privacy principles of transparency, legitimate purpose and proportionality.

As the IRR of the DPA explains:

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.¹³

¹² See Republic Act No. 10173, Section 3(b).

¹³ Implementing Rules and Regulations of the Data Privacy Act, Section 18(a).

There is no informed consent in this instance considering that said website does not provide any specific and legitimate purpose for the collection and processing of the involved personal data.

Further, the website accessed the personal information from LTO.net.ph without authority. Through the use an Application Programming Interface (API), it acquired the personal data from LTO.net.ph, an official website of LTO and stored the same in its own database.

Lisensya.Info's act or practice is detrimental to national security or public interest, CDO is necessary to preserve and protect the rights of a data subject.

The act of accessing a government website's stored data is detrimental to national security or public interest, and the practice of storing the unlawfully collected personal data on its database without any authority or statement of purpose is in gross disregard and violation of the rights of data subjects.

As of 11 November 2020, a total of 9,953 driver's license information and 19,412 motor vehicle file number information were saved on the server of Lisensya.Info.

Until its recent discovery, it has been masquerading itself as a website of the LTO and has been unlawfully processing personal data without the consent and knowledge of data subjects.

Lisensya.Info accessed a government website LTO.net.ph., used the information stored therein without authority, and stored it in its own website. This unlawful acquisition of sensitive personal information exposes the affected data subjects to real risks of serious harm.

The protection of the data subjects from these imminent threats or harm is a matter of public interest and issuance of a cease and desist order is crucial in order to preserve and protect the rights of the data subject.

The commission or continuance of Lisensya.Info's acts or practice, unless restrained, will cause grave and irreparable injury to a data subject.

Lisensya.Info's continued operation is a palpable risk that can cause grave and irreparable injury to affected data subjects.

Lisensya.Info's website is still active as of date. Its continued existence poses a threat to unsuspecting individuals who may use its services by surrendering their sensitive personal information.

Identity theft is the most likely consequence, but there is no telling what other acts and further damage can be done to the stored data on Lisensya.Info's database as surveillance and threats to security may be among them. Allowing it to continue its operations increases the risk of exposing the personal data to identity fraud, and other grave and irreparable damage and/or injury.

As discussed by the Commission in the case of *In re: Philippine Seven Corporation (CID BN 18-081)*¹⁴, viz:

Identity theft occurs when individual/s wrongfully acquired, use, misuse, transfer, possession, alteration or deletion of identifying information without right. In Jose Disini, Jr., et al., vs. Secretary of Justice, the Supreme Court had this to say on the crime of Identity Theft:

'The usual identifying information regarding a person includes his name, his citizenship, his residence address, his contact number, his place and date of birth, the name of his spouse if any, his occupation, and similar data. The law punishes those who acquire or use such identifying information without right, implicitly to cause damage.'

The Court rightly recognizes that a **combination of personal information can be used by online imposter to access or take over existing personal accounts or open new accounts in the name of unsuspecting data subjects. x x x. A simple online search in search engines and/or social media accounts of these franchise applicants may already give enough**

¹⁴ Resolution dated 21 May 2020.

ammunition for these online wrong doers to commit the crime of Identity Theft. Thus, considering the above, this breach might entail real risk of serious harm to the affected data subjects. (Emphasis Supplied)

Hence based on the foregoing, it is clear that grounds for the issuance of a Cease and Desist Order are present in the instant case.

WHEREFORE, premises considered, **Lisensya.Info** and its owner/operator, **JOSE MINAO, BILLY JAMES JIMENA** and other responsible officers are hereby ordered to:

1) File a **COMMENT**, within ten (10) days from receipt of this Order, on the allegations in the attached Application for Issuance of Cease and Desist Order, pursuant to Section 9 of the NPC Circular No. 20-02; and

2) **CEASE AND DESIST** from the processing the personal and sensitive personal information in its possession, until the Commission issues a decision on the submission of the Comment, which shall be made no more than thirty (30) days from the expiration of the period to file a Comment or of the termination of the clarificatory hearing if one is held, pursuant to NPC Circular No. 20-02.

Furthermore, the **NATIONAL TELECOMMUNICATONS COMMISSION** is hereby enjoined to take down the website *Lisensya.Info* immediately upon receipt of this Order.

SO ORDERED.

City of Pasay, Philippines;
12 November 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

IN RE: LISENSYA.INFO
Initiated as an Independent NPC
Investigation into the Possible Data
Privacy Violations Committed by the
website LISENSYA.INFO.

For: Violation of the
Data Privacy Act) of
2012

X-----X

ORDER

LIBORO, P.C.:

On 12 November 2020, this Commission issued a Cease and Desist Order (Cease and Desist Order) against the Lisensya.Info website and its owner/operator, respondents Jose Minao and Billy James Jimena (Respondents) for unauthorized processing and unauthorized access of personal information and sensitive personal information which are violations of the Data Privacy Act of 2012 (DPA), with the following dispositive portion:

“WHEREFORE, premises considered, Lisensya.Info and its owner/operator, JOSE MINAO, BILLY JAMES JIMENA and other responsible officers are hereby ordered to:

1) File a COMMENT, within ten (10) days from receipt of this Order, on the allegations in the attached Application for Issuance of Cease and Desist Order, pursuant to Section 9 of the NPC Circular No. 20-02; and

2) CEASE AND DESIST from the processing the personal and sensitive personal information in its possession, until the Commission issues a decision on the submission of the Comment, which shall be made no more than thirty (30) days from the expiration of the period to file a Comment or of the termination of the clarificatory hearing if one is held, pursuant to NPC Circular No. 20-02.

Furthermore, the NATIONAL TELECOMMUNICATIONS COMMISSION is hereby enjoined to take down the website Lisensya.Info immediately upon receipt of this Order.

SO ORDERED. “

From the time the Cease and Desist Order was first served to the Respondents, the following were the developments¹:

1. The National Telecommunications Commission (NTC) issued a Memorandum dated 16 November 2020 directing Internet Service Providers (ISPs) to block access to Lisensya.Info and it was sent through electronic mail to various ISPs on 20 and 23 November 2020.

The Memorandum directs ISPs to submit a report to the NTC of its actions within five (5) days from receipt of the same.

As of 25 November 2020, the NTC has not yet provided a report on the response of the ISPs to the Memorandum it issued.

2. As of 24 November 2020, Lisensya.Info has already been flagged by Google and Firefox. Upon accessing the site through Google Chrome, users can see a security warning saying that Google Safe Browsing recently detected phishing activities on Lisensya.Info.

Unlike in the previous weeks when users can still access the site upon ignoring the security warning, users who choose now to proceed despite the warning will be directed to a Youtube video. The same happens when users use browsers without a security warning like Safari. Some users also reported that upon accessing the site, they are directed to a statement that “Lisensya.Info’s server IP address could not be found.”

From the above, it can be concluded that Lisensya.Info is no longer easily accessible to the general public.

¹Memorandum dated 17 and 25 November and 15 December 2020 of the Enforcement Division.

Section 12 of NPC Circular 20-02 or the “Rules on the Issuance of Cease and Desist Order” provides:

Section 12. *Decision on the Issued CDO.* – If after giving the Adverse Party the opportunity to be heard, it appears that the applicant is entitled to have the act or practice enjoined and that there is a need for the extension of the issued CDO, the Commission shall extend its effectivity, otherwise, the same shall be lifted.

The decision whether to extend or lift the issued CDO shall be made no later than thirty (30) days from the expiration of the period for the Adverse Party to file a comment or the termination of the clarificatory hearing if one is held. In the event that the Commission fails to render its decision within the said period, the CDO shall be deemed automatically lifted.

The Cease and Desist Order was first served to the Respondents through electronic mail on 12 November 2020, while the revised Cease and Desist Order² was sent through email the following working day on 16 November 2020.

The requirements of due process were complied with when the Respondents were apprised, through their last known email addresses, of the results of the Commission’s investigation and were given a reasonable opportunity to present their defense.³

In administrative proceedings, the filing of charges and giving reasonable opportunity for the person so charged to answer the accusations against him constitute the minimum requirements of due process. The essence of due process is simply to be heard, or as applied to administrative proceedings, an opportunity to explain one’s side, or an opportunity to seek a reconsideration of the action or ruling complained of.⁴

² Copy furnished portion of the Cease and Desist Order was amended to reflect personal information of recipients.

³ Memorandum dated 17 November 2020 of the Enforcement Division.

⁴ *Primanila Plans, Inc. vs. SEC* (G.R. No. 193791, August 6, 2014).

Nonetheless, following the Complaints and Investigation Division's Supplemental Report which provided for a possible physical address of one of the respondents, Billy James Jimena, the physical copy of the Cease and Desist Order was also served to Respondent Jimena's physical address on 26 November 2020. As of this writing, there is still no registry return receipt. On the other hand, Jose Minao's address is still left unknown because of limited information on the said person.

From the foregoing, the Respondents had until 22 November 2020 to file a Comment. From that period, the Commission has thirty (30) days or until 22 December 2020 to decide whether to extend or lift the issued Cease and Desist Order.

This Commission hereby resolves to extend the Cease and Desist Order against the Respondents as owner/operator of the Lisensya.Info website, as the Respondents failed to counter the allegations made therein.

Furthermore, the Commission orders the publication of the Cease and Desist Order and this Order extending the same in the NPC website and its social media channels in order to apprise the public regarding the said website and further protect the rights of the data subjects.

Section 12 of NPC Circular 20-02 provides:

Section 19. Publication. – The fact that a CDO has been issued and extended, after giving the Adverse Party the opportunity to be heard, may be published when warranted by public interest as determined by the Commission.

WHEREFORE, premises considered, the Cease and Desist Order dated 12 November 2020 issued against **Lisensya.Info** and its owner/operator, **JOSE MINAO, BILLY JAMES JIMENA** and other responsible officers is hereby extended until modified or lifted by the Commission upon showing that the factual or legal basis for which it was issued no longer exists.

The Enforcement Division of NPC is hereby ordered to submit the necessary compliance report within the time prescribed in NPC Circular 20-02 for monitoring purposes on the enforcement action on Lisensya.Info and its owner/operator.

SO ORDERED.

City of Pasay, Philippines;
17 December 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



THE 2021 COMPENDIUM OF NPC ISSUANCES

TABLE OF CONTENTS





368 ADVISORY OPINION

369 ADVISORY OPINION NO. 2021-001
REQUEST OF AN OVERSEAS FILIPINO WORKER
(OFW) TO DELETE RECORDS STORED IN THE BALIK
MANGGAGAWA ONLINE SYSTEM

372 ADVISORY OPINION NO. 2021-041
POSTING OF NAMES OF PASSPORT APPLICANTS
ON THE WEBSITE OF THE OFFICE OF CONSULAR
AFFAIRS OF THE DEPARTMENT OF FOREIGN
AFFAIRS

377 ADVISORY OPINION NO. 2021-042
DISCLOSURE OF LIST OF FRONTLINE WORKERS
AFFECTED BY COVID-19

381 ADVISORY OPINION NO. 2021-043
DATA SHARING WITH THE PHILIPPINE NATIONAL
POLICE

389 ADVISORY OPINION NO. 2021-044
DISCLOSURE OF ACADEMIC RECORDS IN SUPPORT OF
ADMINISTRATIVE AND CRIMINAL COMPLAINTS

394 ADVISORY OPINION NO. 2021-045
ACCESS TO SUBSCRIBER RECORDS FOR INTERNAL
REVENUE TAX PURPOSES



400 ADVISORY OPINION NO. 2021-002
DISCLOSURE OF SUMMARY OF EVALUATION AND
RATINGS FORM

403 ADVISORY OPINION NO. 2021-003
INFORMATION SHARING AND THE PHILIPPINE
MARITIME MANPOWER FACTBOOK

- 406 ADVISORY OPINION NO. 2021-004**
REQUEST FOR PERSONAL DATA BY HMO BROKERS
- 410 ADVISORY OPINION NO. 2021-005**
CONFLICT OF INTEREST IN THE DESIGNATION OF A
DATA PROTECTION OFFICER
- 413 ADVISORY OPINION NO. 2021-006**
DATA CLASSIFICATION FOR THE DISCLOSURE OF
PROCUREMENT-RELATED DOCUMENTS
- 417 ADVISORY OPINION NO. 2021-008**
REQUEST FOR OFFICIAL LIST OF LEGITIMATE TAXI
OPERATORS
- 422 ADVISORY OPINION NO. 2021-009**
FORENSIC AUDIT ON COMPANY-ISSUED ASSETS AND
COMPANY-RELATED ACCOUNTS
- 425 ADVISORY OPINION NO. 2021-010**
PRIVATE DETECTIVE SERVICES
- 434 ADVISORY OPINION NO. 2021-011**
REQUEST OF A VOTER FOR THE ERASURE OF NAME
FROM THE CERTIFIED LIST OF OVERSEAS VOTERS
POSTED IN PHILIPPINE EMBASSIES
- 439 ADVISORY OPINION NO. 2021-012**
DOCUMENTARY REQUIREMENTS FOR ACCREDITATION
AS FINANCIAL INSTITUTION
- 446 ADVISORY OPINION NO. 2021-013**
REQUEST FOR INFORMATION IN AID OF
IMPLEMENTING THE HAGUE CHILD ABDUCTION
CONVENTION

- 451 ADVISORY OPINION NO. 2021-014**
POSTING OF PHOTO IN A SOCIAL MEDIA PLATFORM
WITHOUT CONSENT
- 453 ADVISORY OPINION NO. 2021-015**
TRANSFER OF EMPLOYEE RECORDS FROM SSS TO GSIS
- 458 ADVISORY OPINION NO. 2021-016**
DATA PRIVACY IMPLICATIONS OF UPLOADED
CONTRACTS IN THE DEVELOPMENT BANK OF THE
PHILIPPINES' WEBSITE
- 462 ADVISORY OPINION NO. 2021-017**
INTELLECTUAL PROPERTY INVESTIGATION AND
ENFORCEMENT AGENCIES' RIGHTS TO INQUIRY AND
REQUEST FOR PERSONAL INFORMATION
- 466 ADVISORY OPINION NO. 2021-018**
PNP REQUEST FOR PERSONAL INFORMATION FROM
EMPLOYERS
- 470 ADVISORY OPINION NO. 2021-019**
ACCESS TO DOCUMENTS IN AN ADMINISTRATIVE CASE
- 474 ADVISORY OPINION NO. 2021-020**
INSTALLATION AND USE OF GLOBAL POSITIONING
SYSTEMS (GPS) ON MOTORCYCLE UNITS
- 477 ADVISORY OPINION NO. 2021-021**
DISCLOSURE OF ADDRESSES OF TERMINATED
EMPLOYEES TO THE OFFICE OF THE PROSECUTOR
FOR A CRIMINAL CASE
- 480 ADVISORY OPINION NO. 2021-022**
PROCESSING PERSONAL DATA FOR ELECTRONIC
KNOW-YOUR-CUSTOMER (eKYC)

- 483 ADVISORY OPINION NO. 2021-023**
PROCESSING OF PERSONAL DATA FOR RESEARCH
WITHOUT ETHICS CLEARANCE
- 489 ADVISORY OPINION NO. 2021-024**
PUBLIC DISCLOSURE OF INFORMATION ON SOCIAL
WELFARE AND DEVELOPMENT AGENCIES, SERVICE
PROVIDERS, AND CIVIL SOCIETY ORGANIZATIONS
- 495 ADVISORY OPINION NO. 2021-025**
MANDATORY PSYCHIATRIC EVALUATION OF ALL
NATIONAL COUNCIL ON DISABILITY AFFAIRS
PERSONNEL
- 500 ADVISORY OPINION NO. 2021-026**
DATA PRIVACY IMPLICATIONS FOR FINANCIAL SERVICES
INDUSTRY INITIATIVES ON DATA SHARING
- 507 ADVISORY OPINION NO. 2021-027**
ACCESS TO DOCUMENTS BY SAN MIGUEL AEROCITY
INC. PURSUANT TO ITS LEGISLATIVE FRANCHISE
- 515 ADVISORY OPINION NO. 2021-028**
DISCLOSURE OF PERSONAL INFORMATION OF TENANTS
BY A CONDOMINIUM CORPORATION TO THE BUREAU OF
INTERNAL REVENUE
- 519 ADVISORY OPINION NO. 2021-029**
PROCESSING OF PERSONAL DATA CONTAINED IN
ABANDONED SERVERS OR COMPUTERS
- 524 ADVISORY OPINION NO. 2021-030**
PUBLICATION OF COPYRIGHT REGISTRATIONS
- 528 ADVISORY OPINION NO. 2021-031**
PROCESSING FOR DUE DILIGENCE, QUALITY CONTROL,
AND COMPLIANCE CHECKS PURSUANT TO THE
REQUIREMENTS OF THE GOVERNMENT PROCUREMENT
REFORM ACT

- 532 ADVISORY OPINION NO. 2021-032**
DISCLOSURE OF PHOTOGRAPHS OF ACCUSED IN
CRIMINAL CASES
- 536 ADVISORY OPINION NO. 2021-033**
INTERNAL DISSEMINATION OF INFORMATION REGARDING
BANK-RELATED CRIMES
- 539 ADVISORY OPINION NO. 2021-034**
REQUESTS FROM GOVERNMENT AGENCIES FOR THE
DEPARTMENT OF FOREIGN AFFAIRS TO PROVIDE
PERSONAL INFORMATION
- 544 ADVISORY OPINION NO. 2021-035**
DATA SHARING AGREEMENT BETWEEN PHILHEALTH
AND CITY CIVIL REGISTRAR ON REPORTING OF
REGISTERED DEATHS
- 548 ADVISORY OPINION NO. 2021-036**
DISCLOSURE OF LOAN DOCUMENTS PURSUANT TO A
LEGAL CLAIM
- 553 ADVISORY OPINION NO. 2021-036**
REQUEST FOR THE STATUS OF APPLICATION AND THE
LIST OF BENEFICIARIES OF THE SITIO ELECTRIFICATION
PROGRAM (SEP)
- 556 ADVISORY OPINION NO. 2021-038**
DATA SHARING FOR THE NATIONAL HEALTH
WORKFORCE REGISTRY
- 560 ADVISORY OPINION NO. 2021-039**
DATA SHARING OF INCIDENT/DISASTER DATA

568 DECISIONS

569 CID Case No. 18-D-012

JBD v JI VVV

582 NPC 18-109

(Formerly CID Case No. 18-H-109)

ACN v DT

595 NPC 18-010

(Formerly CID Case No. 18-D-010)

RLA v PXE

615 NPC Case No. 19-043

(Formerly CID Case No. 19-A- 043)

FAT v XXX

622 NPC 19-134

VVC v CJB

638 NPC 21-086

RTB v EAST WEST BANKING CORPORATION

646 ORDERS

647 CID 18-J-162

GC, INC. FORCED LOGOUT

657 CID BN 19-034

ROKKO & ASSOCIATES, INC.

662 CID-CDO-21-003

PILIPINAS2022.PH

668 NPC BN 20-044

RESEARCH INSTITUTE FOR TROPICAL MEDICINE

672 NPC BN 20-116
SAINT LOUIS UNIVERSITY

679 NPC BN NO. 21-054
BPI PHILAM LIFE ASSURANCE CORPORATION

684 RESOLUTIONS

685 NPC 18-010
RLA v PLDT ENTERPRISE

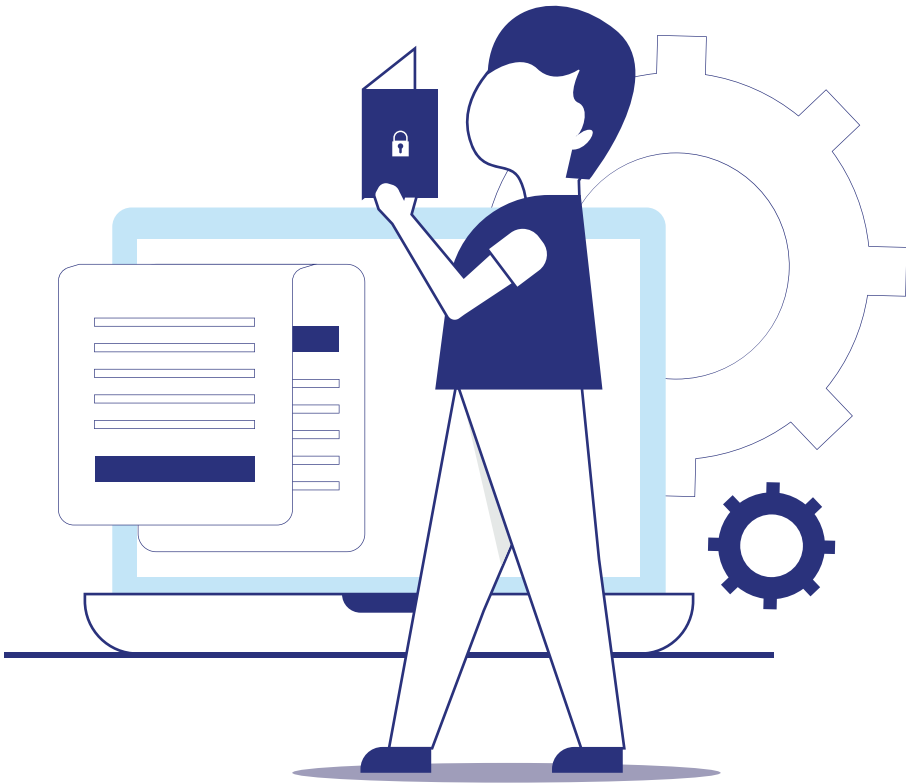
741 CID BN 18-183
SUNLIFE OF CANADA (PHILIPPINES) INC.

746 NPC 19-1201
D.N.T v K.K and X.F

752 CIRCULARS

753 NPC CIRCULAR
NO. 2021-01

781 NPC CIRCULAR
NO. 2021-02



ADVISORY OPINIONS

ADVISORY OPINION NO. 2021-001¹

19 January 2021



Re: **REQUEST OF AN OVERSEAS FILIPINO WORKER (OFW)
TO DELETE RECORDS STORED IN THE BALIK MANGGAGAWA
ONLINE SYSTEM**

Dear [REDACTED]

We write in response to your request for an Advisory Opinion seeking clarification on the request of an OFW for the deletion or erasure of his or her records stored in the Balik Manggagawa Online System (BM Online System).

We understand that the BM Online System is a web-based service that allows vacationing or returning OFW to get their Overseas Employment Certificate (OEC) without having to go the Philippine Overseas Employment Administration (POEA) Office or Philippine Overseas Labor and Office (POLO) Centers.² This system is a collaboration between the Department of Labor and Employment (DOLE) and the POEA to expedite the application and processing of the OECs allowing the OFWs to make relevant OEC transactions online.³

Given the foregoing, you seek clarification on the data subjects' right to erasure as well as the proposal for the POEA to anonymize personal information of OFWs in the BM Online system, and whether this falls within the scope of the Data Privacy Act of 2012 (DPA).

¹ Tags: data subject rights; right to erasure; retention; anonymization

² Department of Labor and Employment, DOLE's POEA issues Q & A on Balik-Manggagawa online processing system, available at <https://www.dole.gov.ph/news/does-poea-issues-q-a-on-balik-manggagawa-online-processing-system/> (last accessed 11 January 2021).

³ Id.

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)

Rights of the data subject; right to erasure; retention

Section 16 (e) of the DPA clearly sets forth the right of every data subject to suspend, withdraw or order the removal or destruction of personal information from the filing system of a personal information controller (PIC) upon discovery and substantial proof that the personal information are outdated or is no longer necessary for the purposes for which they were collected, among other conditions.

In relation to the above, we note that POEA Memorandum Circular No. 6, Series of 2016 provides:

“Pursuant to POEA Governing Board Resolution No. 12, Series of 2016 and in line with the thrust of the Administration to streamline the processing of documents of Overseas Filipino Workers (OFWs) and to address the clamor of Balik-Manggagawa (BM) workers to further enhance the online system of processing their exit clearance prior to their return to their employer, the Administration hereby exempts certain categories of BM workers from securing Overseas Employment Certificate (OEC) and paying any POEA processing fee...”

Likewise, POEA Governing Board Resolution No. 04 Series of 2018 provides, among others:

“FURTHER, the POEA is directed to enhance the existing system for the Balik-Manggagawa to ensure compliance with herein issuance and to include those exempted from securing the Overseas Employment Certificate. Relevant advisory should be issued to all the stakeholders subject of the above policies. xxx xxx xxx.”

From the foregoing, we understand that the primary purpose of the BM Online System is to streamline the processes in the deployment of OFWs, facilitate the issuance of the OEC to vacationing OFWs, and to determine exemption from securing the OEC prior to departure.

After the said purpose/s have been achieved, the retention of such personal data may no longer be necessary, such as when an OFW retires or ceases to work abroad. Thus, an OFW may rightfully request for the deletion of his or her former records stored in the BM Online System, subject to other existing laws and regulations governing the retention period of employment documents or records.

Anonymization of personal data

We understand that the POEA plans to have labor migration data and other personal information under the BM Online system anonymized for policy formulation and the conduct of long-term economic research studies.

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 is no longer identifiable.”⁵

But for information to be truly anonymized, the same must be irreversible, and done in such a way that it is impossible (or extremely impractical) to identify a data subject. There must be no way for the POEA or any other person to single out an individual in a given data set, from connecting two records within a data set (or between two separate data sets) and from any information in such data set.⁶

Where information is anonymous, the provisions and principles under the DPA does not apply. Both the EU General Data Protection Regulation, which repealed the 1995 EU Directive⁷ which highly influenced the DPA, recognizes that “the principles of data protection should not apply to anonymous information.”⁸

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 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) 2016 O.J. (L 119), Recital 26.

⁶ See: European Commission, Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, § 2.1.

ADVISORY OPINION NO. 2021-041¹

24 November 2021



**Re: POSTING OF NAMES OF PASSPORT APPLICANTS ON THE
WEBSITE OF THE OFFICE OF CONSULAR AFFAIRS OF THE
DEPARTMENT OF FOREIGN AFFAIRS**

Dear 

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) which sought confirmation from the NPC whether the Department of Foreign Affairs- Office of Civilian Security and Consular Affairs (DFA-OCSCA) can publicly post on the website of the DFA – Office for Consular Affairs (DFA-OCA) the names of Philippine passport applicants whose passports were unsuccessfully delivered despite repeated attempts.

We note from your letter that due to the influx of passport appointments due to the pandemic, the DFA permitted its technical service provider, APO Production Unit, Inc., to integrate a third-party service provider in the passport Online Appointment System (OAS). However, due to logistical issues and ineffectiveness of the former courier service, there are at least one thousand nine hundred sixty-four (1,964) backlogs in passport delivery.

As a solution, the DFA intends to publicly post on its website (<https://consular.dfa.gov.ph>) the names of Philippine passport applicants whose passports were unsuccessfully delivered despite repeated attempts.

This is also in consideration of the fact that the DFA's efforts in calling and emailing these applicants were equally ineffective. You now ask

¹ Tags: lawful processing of personal information; contract; mandate; general data privacy principles; transparency; proportionality; privacy notice.

whether such disclosure is permissible under the Data Privacy Act of 2012² (DPA).

*Lawful basis for processing personal information;
Section 12; fulfillment of functions; contract*

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

Under the DPA, the names of the passport applicants are considered as personal information,⁴ thus, posting of the same on the website of the DFA-OCA constitutes processing⁵ which should comply with the provisions of the DPA, particularly Section 12 of the law providing for the criteria for lawful processing of personal information, 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

(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; 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 xxx”

As applied in this case, Section 12 (e) is applicable and may be the most appropriate lawful basis for processing.

We note that the DFA has the legal mandate to enforce Republic Act No. 8239⁶ or the Philippine Passport Act of 1996.

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 Data Privacy Act of 2012, § 4.

⁴ Id. § 3 (g).

⁵ Id. § 3 (j).

⁶ Philippine Passport Act of 1996, Republic Act No. 8239 (1996).

specifically, Section 4 of the Philippine Passport Act provides for the authority of the DFA to issue passports to citizens of the Philippines in accordance with the said law.

The DFA may also consider Section 12 (b) above, taking into consideration the nature of the relationship among the DFA, the courier, and the data subjects. Posting of the names on the DFA-OCA website may be considered as processing necessary and related to the fulfilment of a contract with a data subject, i.e., delivery of passport.

We note that in your letter, you have cited Section 12 (f) on legitimate interest as a possible basis for processing:

(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.

We wish clarify that generally, government agencies cannot rely on its “legitimate interest” as its as lawful basis for processing. We refer to the restriction in the EU General Data Protection Regulation (GDPR) for guidance:

“Article 6

Lawfulness of processing”

1. Processing shall be lawful only if and to the extent that at least one of the following applies: x x x

f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.”⁷

Government agencies’ personal data processing activities should be

limited to their constitutional or statutory mandates and should not go beyond the same.

Hence, the public disclosure of the names the passport applicants with printed passports waiting for delivery may be anchored on Sections 12 (b) and/or (e) as discussed above.

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

While there may be lawful basis for processing under the DPA, the DFA must always 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.⁸ We note from your letter that the DFA intends to post the full names and the corresponding sites where the passports will be released to the applicants. The DFA must have an assessment and determination that such public posting of the full names of the applicants is the least privacy intrusive manner of processing in relation to the declared purpose, considering all attendant circumstances.

Likewise, the DFA must ensure that the data subjects are informed about the posting of their personal information on the website. This may be done through an appropriate privacy notice.

A privacy notice is “a 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.”⁹

If not already included, the DFA should include a privacy notice in its passport application form so that moving forward, its clients may be apprised of the possible posting of their names in case of unsuccessful deliveries of their passports.

⁷ 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, Art. 6 (1) (f) (4 May 2016).

⁸ Data Privacy Act of 2012, § 11 (c).

⁹ IAPP, Glossary of Privacy Terms, available at <https://iapp.org/resources/glossary/#paperwork-reduction-act-2>

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2021-042¹

16 December 2021



Re: **DISCLOSURE OF LIST OF FRONTLINE WORKERS
AFFECTED BY COVID-19**

Dear [REDACTED]

We write in response to your letter received by the National Privacy Commission (NPC) which sought clarification on whether to grant the request of a third-party organization to be given a list of frontline workers who were affected by COVID-19.

We understand that the Department of Health (DOH) received a request from the Filipino International Staff of the Asian Development Bank (ADB Fil-IS) for a list of names of frontline workers who passed away or were severely affected by COVID-19. This request is pursuant to ADB Fil-IS' initiative to raise funds to help the affected Filipino frontline workers and their beneficiaries for the fund drive, Alay Dangal sa Bayaning Lumalaban sa COVID-19.

You now ask on whether the disclosure of such information is allowed under the Data Privacy Act of 2012² (DPA).

Lawful basis for processing; health information; law;
mandate; public authority; consent

¹ Tags: lawful basis for processing; law; public authority; consent; further processing; statistical data; COVID-19 patient 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).

A list of names, by itself, is considered personal information under the DPA. However, a list of names of COVID-19 patients are considered sensitive personal information since it pertains to the health information of the said individuals. Hence, to be able to process such data, there must be lawful basis under Section 13 of the DPA.

In this scenario, the DOH, as the health authority of the country, has information on COVID-19 cases and related deaths. However, the processing of the said information is limited only for purposes of disease surveillance and response against the COVID-19 and is based on the requirements of various laws, rules, and regulation on notifiable diseases and the pandemic response of the government. On the other hand, the ADB is a private international financial institution that provides assistance to, among others, developing member countries and the private sector.

For further processing of the said health information which includes disclosure to third parties, such as the proposed disclosure by the DOH of the personal data of frontline workers who passed away or were severely affected by COVID-19 to the ADB Fil-IS, pursuant to the latter's initiative to extend financial assistance, there must be lawful basis under Section 13 which is distinct from the original lawful basis for processing relied upon by the DOH as a public authority.

Section 13 of the DPA provides that the processing of sensitive personal information is generally prohibited unless it falls under any of the criteria for processing. In particular, processing may be allowed when the data subject has given his or her consent, specific to the purpose prior to the processing.⁴

In the current matter, although the disclosure of data will be used for a good cause and legitimate purposes in extending assistance to frontline workers and/or their families, the requirements of the DPA must still be complied with.

The DOH, as the personal information controller, must obtain the consent of the affected frontline workers or their heirs for those who are deceased, prior to the disclosure of their identities to the ADB Fil-IS.

³ Department of Health and National Privacy Commission, Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response, Joint Memorandum Circular No. 2020-0002 [DOH-NPC JMC No. 2020-0002] (April 24, 2020).

⁴ 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, § 13(a) (2012).

⁵ DOH-NPC JMC No. 2020 – 0002, § VI (D).

Public health authorities such as the DOH, their partner agencies and authorized personnel must limit the use and disclosure of health information to the purpose specified at the time of collection.⁵ Further, the processing of COVID-19-related personal data by public authorities should be limited to the pandemic response, specifically the following as stated in the DOH and NPC JOINT MEMORANDUM CIRCULAR No. 2020-0002:

“V. GENERAL GUIDELINES

X X X

2. The processing of personal health information of COVID-19 cases and identified close contacts for disease surveillance and response shall be to the extent necessary for the following purposes:

- a. To outline a true picture of the country’s COVID-19 health situation in terms of status and extent of local and community transmission.
- b. To build a repository of real-time COVID-19-related data as basis of evidence- informed health policy and intervention measures.
- c. To support case investigation and management, contact tracing and monitoring, quarantine and isolation, mandatory reporting to national and local public health authorities, and other disease surveillance-related activities.
- d. To improve response activities, including the quality and accessibility of health services and other related interventions for COVID-19.
- e. To allow information sharing and exchange between and among healthcare providers, public health authorities and other government authorities for treatment and care coordination, and/or surveillance and response purposes.⁶

We note that the proposed disclosure of the requested personal data to ADB Fil-IS does not fall under any of the foregoing purposes and circumstances. Hence, the consent of the affected frontline workers and the heirs of the deceased must be obtained prior to the disclosure of such information.

We also note that the rights of the data subjects must be considered under the current circumstance. For instance, there may be some frontline workers and/or the heirs of the deceased who may not want their personal data, specifically their health information, disclosed to third parties.

⁶ Id. § V (2).

Statistical data; further processing

For purposes of the fundraising, the DOH may opt to provide statistical data only rather than providing the personal data of the frontline workers. However, we emphasize that the foregoing condition on further processing must be strictly construed. This means that the data must be purely statistical and free from any factors that will enable others to reasonably identify the individuals involved.

We note that under this option, the identities of the affected frontline workers and their heirs remain confidential. As to how the financial assistance from the funds raised by ADB Fil-IS will eventually be distributed, the DOH and the ADB Fil-IS may devise such mechanisms which are less privacy-intrusive, i.e., make announcements as to how affected frontline workers may apply for assistance, etc., thereby making any further personal data processing consent-based in this instance.

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2021-043³

16 December 2021



Re: **DATA SHARING WITH THE PHILIPPINE NATIONAL POLICE**

Dear 

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC or the Commission) on whether the personal and sensitive personal information (collectively, personal data) of drug surrenderers undergoing drug rehabilitation may be shared by the Iloilo City Health Office (CHO) with the Philippine National Police (PNP).

We understand that the Iloilo City Police Office (CPO) sent a letter to the CHO requesting for the data of drug surrenderers who are presently undergoing drug rehabilitation under the Iloilo City Community Change Center dubbed as “The Crossroads” (Community-based Drop-in Center).

The CHO denied the request citing Sections 11 (a) and 13 of the Data Privacy Act of 2012 (DP A), stating that the CPO did not provide the specific purpose for which the requested data will be utilized, and it was not shown that the circumstance fits any of the exceptions under Section 13 that would warrant the processing of sensitive personal information.

Further, we understand the PNP Legal Service reiterated the request for the production of the necessary data on the following grounds:

¹ Tags: data sharing; data sharing agreement; general data privacy principles; law and regulation; consent; statistics.

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).

- a. The PNP aid the DILG, where the CHO belongs, are part of the nucleus of the interagency membership in the Dangerous Drugs Board and the drug rehabilitation program is one of the thrusts of the government's anti-illegal drugs campaign. Being in the same inter-agency cooperation cluster, the PNP is not a third party, x x x. The legitimacy of the use of such data is inherent in the PNP's function to collaborate with other government agencies to perform its duty. The collaboration and sharing of these data are essential in the government's anti-illegal drugs campaign without further need for the PNP to justify the legitimacy of its purpose;
- b. Section 4 (e) of the DPA excludes from its coverage information necessary in order to carry out functions of public authority x x x. These cases must be likewise distinguished from those which are purely private matters and does not involve public interest; and
- c. The information from the CHO is essential for the accurate inventory of these cases as compared to those already available at hand and information gathered will be exclusively used for a legitimate purpose only and nothing else.

We understand that the PNP is requesting for the following to be submitted:

Format No. 6A

A. INVENTORY OF RECOVERY AND WELLNESS PROGRAM(RWP)/COMMUNITY-BASED REHABILITATION PROGRAM (CBRP) GRADUATES
As of October 8, 2021 (cumulative since the implementation of CBRP/RWP)

Office/Unit	Total Number of Drug Surrenderers	Total Number of Drug Surrenderers Completed RWP/CBRP	Unemployed	Total Number of RWP/CBRP Graduates				
				Employed		Self Employed	Arrested/d/Detain	Deceased/d/Dead
				Local	Abroad			
TOTAL								

B. INVENTORY OF REMAINING DRUG SURRENDERER WHO HAVE NOT UNDERGONE RWP/CBRP
As of October 8, 2021 (cumulative since the implementation of CBRP/RWP)

Office/Unit	Total Number of Drug Surrenderers	Total Number of Drug Surrenderers Completed RWP/CBRP	Unemployed	Total Number of not Undergone RWP/CBRP					Cannot be
				Employed		Self Employed	Arrested/d/Detain	Deceased/d/Dead	
				Local	Abroad				
TOTAL									

C. INVENTORY OF ONGOING PNP IMPLEMENTED RWP/CBRP
As of October 8, 2021 (cumulative since the implementation of CBRP/RWP)

Office/Unit	Total Number of Drug Surrenderers	Total Number of Ongoing RWP/CBRP			
		Currently Enrolled	Methodology Adopted	Date Started	Date of Graduation
TOTAL					

Figure 1: Form requiring statistics

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.³

On the other hand, a data sharing agreement or 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.⁴

We wish to clarify that the execution of a DSA under the latest NPC issuance is not mandatory.⁵

“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 not mandatory, it is still advisable to execute one as it is a best practice and a demonstration of accountability amongst the parties to the data sharing. It is best to consult the respective data protection officers (DPOs) of the local government unit (LGU) and the PNP for a better understanding of the data sharing arrangement and whether the agencies should pursue the execution of a DSA.

We also wish to emphasize that the Circular clarified that data sharing may be based on any of the criteria for lawful processing of personal data in Sections 12 and 13 of the DPA⁶

³ National Privacy Commission, Data Sharing Agreements [NPC Circular No. 2020-03], § 2 (F) (December 23, 2020). ⁴ Id. § 2 (G).

⁵ Id. § 8.

⁶ Id. § 6.

and may also be allowed pursuant to Section 4 of the law which specifies the special cases.⁷ The Circular further provides that it does not prohibit or limit the sharing, disclosure, or transfer of personal data that is already authorized or required by law.⁸ of personal data that is already authorized or required by law.⁸

In relation to the above, as sensitive personal information is required by the PNP based on the sample forms provided, the processing, which includes sharing, of the same may fall under any of the instances provided for in Section 13 of the DPA, one of which is when processing is provided for by existing laws and regulations.⁹

Adherence to general data privacy principles; legitimate purpose; proportionality; purpose limitation; statistics

Regardless of whether the CHO and the PNP executes a DSA, as personal information controllers (PICs), both must adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality in all personal data processing activities.

Specifically for legitimate purpose, this principle requires that the processing shall be limited to and compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.¹⁰

In addition, the principle of proportionality requires that the processing shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose and that personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.¹¹

Hence, it is incumbent upon the PNP to declare the specific purpose/s for requesting the data in accordance with Section 11 (a) of the DPA as appropriately cited by the CHO in its letter to the PNP.

It bears stressing that the blanket statement of the PNP that “The legitimacy of the use of such data is inherent in the PNP’s function to collaborate with other government agencies to perform its duty. The collaboration and sharing of these data are essential in the government’s anti-illegal drugs campaign without further need for the PNP to justify the legitimacy of its purpose;” does not conform with the requirements of purpose limitation under the DPA.

The PNP should identify the specific provisions of laws, rules, and regulations mandating it to process the personal data of drug surrenderers and communicate the same to the CHO.

We also note the statement from the PNP that “The information from the CHO is essential for the accurate inventory of these cases as compared to those already available at hand and information gathered will be exclusively used for a legitimate purpose only and nothing else.”

If the purpose is for ensuring accuracy of the inventory of cases, then the first form (see Figure 1) requiring statistics should already suffice. Collecting individual level data which includes sensitive personal information for this purpose may be deemed to be excessive and no longer relevant, suitable, or necessary as the statistics or aggregated data should be enough to meet the PNP’s requirements.

We reiterate our pronouncement in Advisory Opinion No. 2018-077 on the processing of personal data of vulnerable data subjects:

“We underscore that the interpretation of any provision of the DPA must be in a manner mindful of the rights and interests of the data subject. Processing operations performed about 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 personal information controller or personal information processor, require special protection.”¹²

In this scenario, the involved data subjects are drug surrenderers. Clearly, there exists an imbalance between such data subjects and the LGU currently processing their personal data under the pertinent rehabilitation programs and/or the PNP requesting to have access to such personal data. A judicious assessment is necessary to determine if sharing and further processing of such personal data is reasonable and appropriate, taking into account existing laws and regulations applicable on the matter.

⁷ Id. § 7.

⁸ Id. § 6.

⁹ Data Privacy Act of 2012, § 13 (b).

¹⁰ See: Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (b) (2016).

¹¹ Id. § 18 (c).

Section 4 (e); special cases

We wish to clarify that even if the PNP's processing falls under Section 4 (e) as a special case, as the PNP Legal Service discussed in its letter to the CHO, this only means that the provisions on the lawful criteria for processing of personal data under Sections 12 and 13 of the DPA does not apply and the exemption from the requirements is only to the minimum extent necessary to achieve the specific purpose, function, or activity.¹³

Further, the PNP as a PIC is still subject to the other requirements under the DPA, its IRR, and issuances of the NPC, i.e., adhering to the general data privacy principles, upholding data subject rights, implementing appropriate and reasonable physical, organizational, and technical security measures for personal data protection, among others.

Sensitive personal information; consent; processing provided for by existing laws and regulations; public authority

Generally, the processing of sensitive personal information is prohibited, unless such processing falls under the exceptions provided under Section 13. As mentioned above, Section 13 (b) recognizes the processing that is provided for by existing laws and regulations.¹⁴

In this instance, consent is not required for lawful processing as it is not the most appropriate lawful basis. PICs should choose the lawful basis that most closely reflects the true nature of the relationship with the data subject and the purpose of the processing.

In other words, the consent of the drug surrenderers is not required for the sharing of their personal data if such data sharing is anchored on laws, rules, and regulations mandating government agencies to share personal data.

¹² National Privacy Commission, NPC Advisory Opinion No. 2018-077 (Oct. 25, 2018), citing Data Privacy Act of 2012, § 38, National Privacy Commission, Registration of Data Processing Systems and Notifications Regarding Automated Decision-Making, Circular No. 17-01 [NPC Circular 17-01], § 5 (c) (3) (July 31, 2017), Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Item III (B)(a)(7), 4 April 2017, available at

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

¹³ Rules and Regulations Implementing the Data Privacy Act of 2012, § 5.

¹⁴ Data Privacy Act of 2012, § 13 (b).

It would be important to document the specific legal basis for the PNP to collect the personal data of the drug surrenderers who are presently undergoing drug rehabilitation and consider the discussion above on the sufficiency of statistics to be submitted in lieu of personal data, bearing in mind purpose limitation and data minimization requirements.

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2021-044¹

28 December 2021



Re: **DISCLOSURE OF ACADEMIC RECORDS IN SUPPORT OF ADMINISTRATIVE AND CRIMINAL COMPLAINTS**

Dear 

We write in response to your request for an Advisory Opinion received by the National Privacy Commission (NPC or Commission) regarding the release of certain academic records by Carlos Hilado Memorial State College (CHMSC) in relation to the filing of an administrative case and criminal complaint before the Ombudsman against a faculty member.

In your letter, it states that a certain faculty member of the CHMSC (“Requesting Party”) requested copies of the academic records of another CHMSC faculty member (“Data Subject”).

These academic records were to be used as evidence in support of a complaint the Requesting Party filed against the Data Subject with CHMSC and as evidence in filing a criminal case before the Office of the Ombudsman. The Requesting Party specifically asked for the following:

1. Official Transcript of Records for Master of Arts in Education Major in Educational Management issued by CHSMC;
2. Official Transcript of Records for Doctor of Philosophy in Educational Management of issued by another specified university;
3. Certification from the Office of the Registrar that the Data Subject has not completed the requirements for the MA degree as of his date of graduation and the actual date of completion;
4. Certification from Dean of College of Education of CHSMC for the Data Subject’s submission of his hardbound thesis; and

5. Approval Sheet page of the thesis of the Data Subject submitted to the Graduate School of CHSMC.

We understand that the Requesting Party is questioning the authenticity of the signature in the Approval Sheet of the thesis as well as the regularity in the issuance of Official Transcript of Records by CHMSC.

Finally, we understand that the Requesting Party in his letter-request cited multiple provisions of the Data Privacy Act of 2012² (DPA) as justification for the disclosure of the requested academic records, specifically Sections 4, 11, and 12 of the DPA.

Special cases; information about government officers or employees; information about an individual's education; sensitive personal information

The Requesting Party cited Section 4 of the DPA regarding information about an individual working for the government as justification for the release of the academic records. Section 4 of the DPA provides for its scope and the special cases in which the law may not be applicable.

Section 4 (a) of the DPA, as expounded in Section 5 (a) (1) of the Implementing Rules and Regulations³ (IRR) of the DPA states that:

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, use, disclosure or other processing necessary to the purpose, function, or activity concerned:

a. Information processed for purpose of allowing public access to information that fall within matters of public concern, pertaining to:

1. Information about any individual who is or was an officer or employee of government that relates to his or her position or functions, including:

a) The fact that the individual is or was an officer or employee of the government;

b) The title, office address, and office telephone number of the individual;

c) The classification, salary range, and responsibilities

of the position held by the individual; and

d) The name of the individual on a document he or she prepared in the course of his or her employment with the government;

X X X

Provided, that the non-applicability of 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.⁴

The exclusion of the above information from the scope of the law is limited to the minimum extent of collection, access, use, disclosure or other processing necessary to achieve the specific purpose, function or activity concerned. Specifically, access to such information pertaining to government officials or employees is recognized to the extent that the same will uphold the right to information on matters of public concern.

Nevertheless, the exemption does 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

In this instance, the requested information relates to the Data Subject's position or functions in CHMSC, particularly as his academic records form part of his qualifications as a member of CHMSC faculty. This falls squarely under Section 5 of the DPA's IRR which may warrant the grant of the request, but only to the minimum extent necessary to achieve the specific purpose of the Requesting Party.

¹ Tags; disclosure of academic records; sensitive personal information; special cases; administrative and criminal complaints; Section 13 (f); legitimacy; proportionality; necessity.

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 Id. § 5 (a).

⁵ National Privacy Commission, NPC Advisory Opinion No. 2017-056 (Sept. 20, 2017) citing the Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (2016).

Filing of complaint before the Office of the Ombudsman; Section 13 (f)

In addition, we note that aside from the administrative complaint before the CHMSC, another purpose of the request is to support a complaint before the Office of the Ombudsman. This processing of sensitive personal information of the Data Subject for the complaint before the Office of the Ombudsman may also find basis under Section 13 of the DPA.

Specifically, Section 13 (f) recognizes the processing which 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.⁶

The criterion “necessary for the x x x establishment x x x of legal claims,” was interpreted by the Commission in the case of BGM vs. IPP7 citing the case of NPC 17-018, to wit:

“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.

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. 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 determining 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. In this instance, we note

that the request indicates a specific set of documents and declares a clearly defined purpose.

Considering as well that there is a pending complaint before CHMSC involving the same matter, CHMSC should have enough information to be able to make a proper determination on both the legitimacy and proportionality of the request.

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.

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

⁶Data Privacy Act of 2012, § 13 (f).

⁷National Privacy Commission, NPC 19-653 (Dec. 17, 2020)

ADVISORY OPINION NO. 2021-045¹

28 December 2021



Re: **ACCESS TO SUBSCRIBER RECORDS FOR INTERNAL
REVENUE TAX PURPOSES**

Dear 

We write in response to your letter requesting for an Advisory Opinion received by the National Privacy Commission (NPC or the Commission) on the legality of providing the Bureau of Internal Revenue (BIR) subscriber records of certain individuals in view of the provisions of the Data Privacy Act of 2012 (DPA).

We understand that the BIR, through its Regional Director for Revenue Region No. 8A- Makati City, sent a letter dated 16 September 2021 (BIR letter), requesting Globe Telecom, Inc. (Globe) to allow the attorneys of its Regional Investigation Division access to the records of and/or be furnished with the registered addresses of 782 persons enumerated in Annex A of the same. The BIR further stated that the request is made pursuant to Section 5 (b) of the National Internal Revenue Code (NIRC), as amended, and in consonance with Revenue Memorandum Circular (RMC) No. 97-2021, otherwise known as “Taxation of Any Income Received by Social Media Influencers.”

Furthermore, in the copy of the letter provided to the Commission, the BIR stated that any information or documents furnished will be kept strictly confidential and used for Internal Revenue Tax purposes only.

¹ Tags: subscriber records; address; social media influencers; Bureau of Internal Revenue; internal revenue tax purposes; special cases; public authority; proportionality.

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 from the NPC on the legality of providing the requested information given that the same pertains to natural persons identified as “social media influencers” whose personal data are protected by the DPA and not of “corporations, mutual fund companies, insurance companies, regional operating headquarters of multinational companies, joint accounts, associations, joint ventures of consortia and registered partnerships, and their members,” as stated in Section 5 (b) of the NIRC, as amended.

In the same vein, you brought up the concern that the request may be inconsistent with the principle of proportionality embodied in the DPA because the list enumerated in Annex A of the BIR letter may or may not be Globe customers and may include entities, not just natural persons.

Special cases under the DPA; public authority

The DPA provides specific kinds of information deemed as special cases, particularly under Section 4 of the law. The situation at hand involves the BIR as a public authority with a regulatory function. We reiterate our position in NPC Advisory Opinion No. 2021-28:

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

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.’ (Underscoring supplied)

The above exemption must be strictly construed. For the exemption to apply, the following are considered:

- The information is necessary in order to carry out the law enforcement or regulatory function of a public authority;
- The processing is for the fulfillment of a constitutional or statutory mandate;
- There is strict adherence to all due process requirements;
- Applies only to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned; and
- Only the specified information falls outside the scope of the DPA. The public authority, considered as a personal information controller under the DPA, must still comply with the other requirements of the DPA such as the implementation of reasonable and appropriate physical, organizational and technical security measures, uphold the rights of data subjects and adhere to the data privacy principles of transparency, legitimate purpose, and proportionality.”³

The BIR is tasked to, among others, ensure compliance with the NIRC, as amended, and other relevant tax laws, rules, and regulations. The DPA recognizes the authority of the BIR Commissioner under Section 5 of the NIRC, to wit:

“SEC. 5. Power of the Commissioner to Obtain Information, and to Summon, Examine, and Take Testimony of Persons. - In ascertaining the correctness of any return, or in making a return when none has been made, or in determining the liability of any person for any internal revenue tax, or in collecting any such liability, or in evaluating tax compliance, the Commissioner is authorized:

(A) To examine any book, paper, record, or other data which may be relevant or material to such inquiry;

To obtain on a regular basis from any person other than the person whose internal revenue tax liability is subject to audit or investigation, or from any office or officer of the national and local governments, government agencies and instrumentalities, including the Bangko Sentral ng Pilipinas and government-owned or -controlled corporations, any information such as, but not limited to, costs and volume of production, receipts or sales and gross incomes of taxpayers, and the names, addresses, and financial statements of corporations, mutual fund companies, insurance companies, regional operating headquarters of multinational companies, joint accounts, associations, joint ventures of consortia and registered partnerships, and their members; Provided, That the Cooperative Development Authority shall submit to the Bureau a tax incentive report, which shall include information on the income tax, value added tax, and other tax incentives availed of by cooperatives registered and enjoying incentives under Republic Act No. 6938, as amended: Provided, further, That the information submitted by the Cooperative Development Authority to the Bureau shall be submitted to the Department of Finance and shall be included in the database created under Republic Act No. 10708, otherwise known as “The Tax Incentives Management and Transparency Act (TIMTA). x x x”

The above powers of the BIR Commissioner as exercised by him or as duly delegated to other BIR officials to examine any book, paper, record, or other data, and obtain from any person other than the person whose internal revenue tax liability is subject to audit or investigation any information for the limited purposes of (1) ascertaining the correctness of any return, or (2) in making a return when none has been made, or (3) in determining the liability of any person for any internal revenue tax, or (4) in collecting any such liability, or (5) in evaluating tax compliance, is broad enough to cover its request for access to records and registered addresses.

In the case of examining and investigating Social Media Influencers, the authority of the BIR is further supported by RMC No. 97-2021, otherwise known as “Taxation of Any Income Received by Social Media Influencers.”

The RMC clearly stated that Social Media Influencers are required to pay

taxes, in accordance with the law, and stated the BIR's "end goal of raising revenues from the undeclared income (of Social Media Influencers)."⁴

General data privacy principles; proportionality

Given the foregoing, it is without doubt that the BIR has authority to investigate Social Media Influencers to determine their tax liabilities and compliance with tax laws and regulations. Globe should then provide the information requested by the BIR RDO pursuant to its mandate while keeping in mind the principle of proportionality.

We note that the letter of the BIR states: "... allowed access to your records and/or furnished with the registered address/es of persons...", with no specification as to the kind of information. While it is clear that the BIR has authority to obtain necessary information for its investigation, the access to records letter, as currently worded, may not align with the principle of proportionality.

In order to comply with the request while upholding the data privacy of its subscribers, Globe may seek clarification with the BIR on what particular information of the subscribers are needed in relation to their specified purposes. Limited personal information of the subscriber concerned that is sufficient to enable the BIR to properly conduct its investigation may be provided.

As the letter gives an option to Globe to provide the registered address only, providing the same may be the least privacy-intrusive manner to comply with the request, unless the BIR provides a more specific list of personal data needed to achieve their declared purposes.

We understand that once the BIR has the requested addresses of the Social Media Influencers, it may then issue its Letter of Authority and transmit the same to the Social Media Influencers. Thereafter, the BIR can just request for the needed documents from the influencers themselves.

On the concern raised about the list containing persons who may not be Globe customers, Globe need not provide any information that it does not have under its custody. As to juridical entities, the processing of their information is well beyond the scope of the DPA, and may be subject to other applicable laws, such as the NIRC.

³ See: National Privacy Commission, NPC Advisory Opinion No. 2019-022 (07 May 2019), NPC Advisory Opinion No. 2020-015 (24 Feb 2020) and NPC Advisory Opinion No. 2021-28 (16 July 2021).

⁴ Bureau of Internal Revenue, Revenue Memorandum Circular No. 97-2021 [BIR RMC No. 97-2021] (16 Aug 2021).

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.

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. 2021-002¹

19 January 2021



Re: **DISCLOSURE OF SUMMARY OF EVALUATION AND RATINGS FORM**

Dear [REDACTED]

We write in response to the request for clarification by your office addressed to the Civil Service Commission – National Capital Region (CSC-NCR) and referred to the National Privacy Commission (NPC), seeking clarification on the applicability of the Data Privacy Act of 2012² (DPA) relative to the requests of applicants for copies of the Summary of Evaluation and Ratings Form (SERF) prepared by the Department of Public Works and Highways Human Resource Merit Promotion and Selection Board (DPWH-HRMPSB) for purposes of the screening and evaluation of applicants for a particular position.

We understand that the requesting applicants are invoking their rights to due process and information. But the DPWH-HRMPSB is also considering the privacy rights of the other applicants as the SERF contains sensitive personal information as defined under the DPA.

We also note that the SERF and other records on file with the Civil Service Commission (CSC) as well as the respective Human Resource Management Offices of various government agencies are confidential in nature.

¹ Tags: scope of the DPA; right to information; limitations; lawful processing of personal data; general 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).

³ Legaspi v. CSC, G.R. No. 72119 (1987).

⁴ Id.

Right to information; FOI vis-à-vis the DPA; limitation; general data privacy principles; CSC rules

The right to information is guaranteed by the Constitution. It is the right of every citizen to access official records, documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development.

In determining whether a particular information is of public concern, there is no rigid test which can be applied.³ Public concern like public interest is a term that eludes exact definition.⁴

It must be noted, however, that the above constitutional guarantee is not absolute. Even Executive Order (EO) No. 02 which operationalizes the Freedom of Information in the Executive Branch⁵ admits of certain limitations and/or exceptions like those that pertain to the privacy of individuals and those that may affect security. The said EO likewise provides that any disclosure of personal data should be in accordance with the principles of transparency, legitimate purpose, and proportionality enunciated under the DPA.

Also, the EO clarifies that “while providing access to information, public records, and official records, responsible officials shall afford full protection to the right to privacy of the individual.”⁶ For this purpose, it requires that each government office shall ensure that personal information in its custody or control is disclosed or released only if it is material or relevant to the subject-matter of the request and its disclosure is permissible under this EO or existing law, rules or regulations, among others.⁷

In this case, the particular purpose/s for which the requests were made are not specified. Assuming that the requested document would be used for filing a complaint or protest with the CSC to question the appointment and/or recruitment process of the DPWH, we understand that it would be the CSC itself who would request from the concerned agency the pertinent documentation to aid in its evaluation of the protest. This may inevitably include the SERF and other documents, i.e. resolutions, minutes of meetings, among others.

With this, the disclosure of the SERF to a particular applicant may not be warranted in this scenario as it may be a violation of the data privacy rights of other applicants, as well as the applicable confidentiality rules governing CSC recruitment records.

We note that a particular applicant may be informed and provided with his/her own rating/score/results considering the criteria and rating matrix used, but not that of his/her co-applicants.

Finally, we wish to emphasize that the DPWH's data protection officer as well as the FOI decision maker may also be duly consulted on this matter.

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, Operationalizing In The Executive Branch The People's Constitutional Right To Information And The State Policies To Full Public Disclosure And Transparency In The Public Service And Providing Guidelines Therefor, Executive Order No. 2 [EO No. 2] (July 23, 2016).

⁶ EO No. 2, § 7.

⁷ Id.

ADVISORY OPINION NO. 2021-003¹

9 February 2021



Re: **INFORMATION SHARING AND THE PHILIPPINE MARITIME
MANPOWER FACTBOOK**

Dear [REDACTED]

We write in response to your letter requesting for clarification on whether the sharing of information between the National Maritime Polytechnic (NMP) and the other regulatory government agencies such as the Maritime Industry Authority (MARINA), Commission on Higher Education (CHED), Philippine Overseas Employment Administration (POEA), Philippine Coast Guard (PCG), and Overseas Workers Welfare Administration (OWWA) (collectively, data source agencies) is covered by NPC Circular No. 16-02 on Data Sharing Agreements (DSAs) involving Government Agencies.

We note from your letter and the attached draft Memorandum of Agreement (MOA) and annexures on the Data Needs for the Philippine Maritime Manpower Factbook (Factbook) and the Situation Briefer on the Effects of COVID-19 (collectively, data needs) that for the regular and timely production of the Factbook, the data source agencies will share to the NMP industry-related administrative data and statistics.

National Maritime Polytechnic

We understand that the NMP is a government agency created pursuant to Presidential Decree No. 1369.² It is mandated to conduct research and studies on the latest maritime technologies and other related matters for the maritime industry.³

¹ Tags: data sharing; data sharing agreement; scope; personal data; statistics.

² Creation of a National Maritime Polytechnic, Presidential Decree No. 1369 (1978).

³ Id.3 Legaspi v. CSC, G.R. No. 72119 (1987).

⁴ Id.

Pursuant to the above, the NMP produced the comprehensive Factbook which is a consolidated country report containing relevant industry-related data and statistics. We understand that the Factbook is updated at regular intervals and data source agencies have been identified to contribute relevant information.

Data Privacy Act of 2012; scope; personal information; data sharing; NPC Circular No. 2020-03; sharing of statistics

At the outset, please note that NPC Circular No. 2020-03 on Data Sharing Agreements has expressly repealed NPC Circular No. 16-02. The new Circular may be accessed at our website at: <https://www.privacy.gov.ph/wp-content/uploads/2021/01/Circular-Data-Sharing-Agreement-amending-16-02-21-Dec-2020-clean-copy-FINAL-LYA-and-JDN-signed-minor-edit.pdf>.

To determine whether data sharing falls within the scope of the Data Privacy Act of 2012 (DPA) and NPC Circular No. 2020-03, it is important to first determine whether the subject matter of the DSA is personal information.

To clarify, Section 4 of the DPA provides 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, whereas Section 3(g) of the same 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.

Further, NPC Circular No. 2020-03 defines DSA as a contract, joint issuance, or any similar document which sets out the obligations, responsibilities, and liabilities of the personal information controllers involved in the transfer of personal data between or among them, including the implementation of adequate safeguards for data privacy and security, and upholding the rights of the data subjects.

We observed from the draft MOA and the data needs that the NMP is only requesting for the number of individuals involved in a specific situation, to wit:

- Number of seafarers deployed for CY 2018-2019 from the POEA and for CY 2017-2019 from the MARINA;
- Number of persons involved in maritime accidents from the PCG;
- Number of enrollees for Bachelor of Science in Marine Transportation (BSMT) and Bachelor of Science in Marine Engineering (BSMarE) for CY 2020-2021 from CHED;
- Number of repatriated seafarers for CY 2020 from OWWA, among others.

From the foregoing, the various data source agencies will not share any personal information with the NMP. As such, the data needs subject matter of the draft MOA are aggregate data, which are statistical in nature. Consequently, the provisions, principles, and other requirements under the DPA and NPC issuances may not necessarily apply.

Statistical information which does not include information from which the identity of an individual is apparent or can be reasonably and directly ascertained, is not personal information, and thus, not covered by the provisions of the DPA.⁵ Therefore in this scenario, the execution of a DSA may not be necessary in the sharing of information related to the production and updating of the Factbook.

The above is based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. Note that this communication 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

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)

ADVISORY OPINION NO. 2021-004¹

9 February 2021



Re: **REQUEST FOR PERSONAL DATA BY HMO BROKERS**

Dear 

We write in response to your inquiry concerning MediCard Philippines (MediCard) and the various issues raised on the request for personal and sensitive personal information (collectively, personal data) by accredited HMO brokers (brokers) with respect to the utilization analysis of Medicaid's corporate clients' employees and other personal data processing activities.

We understand that the brokers are accredited by MediCard. Accreditation is merely an acknowledgment that a particular broker is recognized by Medicaid, but there is no formal agreement establishing mutual contractual obligations between them.

We understand further that the broker and the Medicaid corporate client have a service agreement, and as part of the broker's service offering to the corporate client, the brokers may conduct utilization analysis involving the corporate clients' employees. To do such activity, the brokers seek to collect utilization information of the corporate clients' employees from MediCard. Utilization information includes diagnosis, dates of confinement, place of confinement, cost of confinement, procedures done, among others.

In addition, you mentioned that these brokers share information with their branches located in other countries, perform analytics on the data obtained and publish studies on the same, and sell insurances.

¹ Tags: HMO brokers; request for personal data; sensitive personal information; health information; lawful basis; consent; general data privacy principles; statistics.

With this, MediCard expressed hesitation in providing information to the brokers. In view of the foregoing, you now seek clarification of the following:

1. Can MediCard charge the accountability of securing the consent of the data subjects to the corporate client since MediCard does not have direct contract with the corporate client's employees and dependents?
2. In relation to the corporate account, what is the role of the broker, is it a personal information controller (PIC) or a personal information processor (PIP)?
3. What can be the broker's basis for processing/receiving/sharing data since they are not a party to the agreement between MediCard and its corporate clients? Should they secure consent from the employee/data subject?

Data Privacy Act of 2012; scope; personal information controller; duties and responsibilities

The Data Privacy Act of 2012² (DPA) applies to the processing of all types of personal information and to any natural and juridical person involved in processing personal information.³ When brokers request for utilization information details and process the same, they are engaged in processing personal data and are thus covered by the provisions of the DPA.

As to whether they are PICs or PIPs, brokers may be considered as PICs based on the information provided. A PIC is defined as a person or organization who controls the collection, holding, processing or use of personal information.⁴ There is control if the natural or juridical person decides on what information is collected or the purpose or extent of its processing.⁵

As indicated in the facts provided to us, the brokers may be engaged in the processing of personal data based on their own purposes, distinct and independent from Medicards' and/or the corporate clients' purposes. The brokers control the processing of the personal data of the employees of such corporate clients, and determine what personal data to collect and how such information will be used.

Thus, as PICs, the brokers are accountable with respect to the personal data they process and must ensure adherence to the general data privacy principles of transparency, legitimate purpose, and proportionality, the implementation of reasonable and appropriate security measures for the protection of personal data, and that data subject rights are upheld at all times.

Lawful basis for processing; sensitive personal information; health information; consent; transparency

Since the brokers intend to collect and process health information, which is considered as sensitive personal information under the DPA, they must anchor their processing on any of the various lawful criteria under Section 13 of the law. A determination must be made on the most appropriate lawful basis, considering all relevant circumstances of the proposed processing, the corporate clients' employees' expectation of privacy as well as the impact on their rights and freedoms.

Should there be no other appropriate lawful basis to process such utilization information except for the consent of the employee data subject, it is incumbent upon the brokers to inform them and obtain their consent, either directly or through the corporate clients.

We wish to reiterate the definition of consent. The same must be 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, and evidenced by written, electronic or recorded means.⁶

The brokers would have to provide details on the processing for the utilization analysis, analytics, research, sharing and disclosure to third parties, and other proposed personal data processing activities, pursuant to the transparency principle and the data subjects' right to be informed.

Aggregate data; statistics; proportionality principle

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 Data Privacy Act of 2012, § 4.

⁴ Data Privacy Act of 2012, § 3 (h).

⁵ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 3 (m) (2016).

⁶ Data Privacy Act of 2012, § 3 (b).

Finally, Medicaid is not precluded from asking the brokers if the disclosure of statistical or aggregate information without necessarily including any personal data would already suffice for purposes of the utilization analysis and other proposed analytics or further processing.

This is in keeping with the proportionality principle that personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.⁷

This opinion is based solely on the limited information you have provided. No service agreements or other contracts were reviewed for purposes of this opinion. 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, § 18 (c) (2016).

ADVISORY OPINION NO. 2021-005¹

24 February 2021



Re: **CONFLICT OF INTEREST IN THE DESIGNATION OF A DATA PROTECTION OFFICER**

Dear [REDACTED]

We write in response to your letter requesting for clarification on whether there is conflict of interest in relation to the designation of the Executive Director of the Land Transportation Office (LTO) as the data protection officer (DPO) of the said agency.

Designation of DPOs; NPC Advisory No. 2017-01; independence; conflict of interest

NPC Advisory No. 2017-01 on the Designation of DPOs emphasizes the requirement that a DPO or a compliance officer for privacy (COP) must be independent in the performance of his or her functions, and should be accorded a significant degree of autonomy by the PIC or PIP.² Further, the Advisory provides that in his or her capacity as DPO or COP, an individual may perform (or be assigned to perform) other tasks or assume other functions that do not give rise to any conflict of interest.³

Conflict of interest refers to a scenario wherein a DPO is charged with performing tasks, duties, and responsibilities that may be opposed to or could affect his/her performance as DPO, i.e., holding a position that leads him/her to determine the purposes and the means of the processing of personal data.⁴

¹ Tags: data protection officer; conflict of interest; purpose and means of processing;

² National Privacy Commission, Designation of Data Protection Officers [NPC Advisory No. 17-01] (March 14, 2017).

³ Id. Independence, Autonomy and Conflict of Interest.

⁴ Id. Definition of Terms.

⁵ European Commission, Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017, page 16, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (last accessed: 23 Feb 2021).

Further, we note the pertinent discussions under Article 29 of the Data Protection Working Party of the European Commission - Guidelines on Data Protection Officers⁵ on the matter of conflict of interest, to wit:

“The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.”

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing.” (underscoring provided)

While there may be a perceived conflict given that the position of an Executive Director is a senior management position in a government agency, there is a need to further evaluate if indeed there is actual conflict of interest as the determination of the same can be made on a case-to-case basis.

We note in this scenario that generally, LTO's purposes for the processing of personal data, is already determined by law and regulation, and not by any official or employee, including the Executive Director.

Nevertheless, LTO may internally re-assess if the position of an Executive Director would be incompatible with the functions of a DPO. It can be good practice to:

- identify the other positions within the agency which would be incompatible with the function of a DPO;
- draw up internal rules to this effect to avoid conflicts of interests;
- include a more general explanation about conflicts of interests; and

- upon evaluation, declare that your DPO has no conflict of interests with regard to his/her function, as a way of raising awareness of this requirement;

where the above also takes into consideration the particular circumstances of LTO - its activities, size, and structure as a government agency.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 See generally: European Commission, Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017, page 16, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (last accessed: 23 Feb 2021).

ADVISORY OPINION NO. 2021-006¹

5 March 2021



Re: **DATA CLASSIFICATION FOR THE DISCLOSURE OF PROCUREMENT-RELATED DOCUMENTS**

Dear 

We write in response to your email inquiry received by the National Privacy Commission (NPC) seeking clarification on whether it is necessary for the Bids and Awards Committee (BAC) of the Bangko Sentral ng Pilipinas - Security Plant Complex (BSP-SPC) to have its data classification approved or enrolled with the NPC, and whether there is an established procedure for the same.

We understand that the BAC of the BSP-SPC would like to establish consistency in releasing procurement-related documents to the public and to all other relevant parties especially since requests for bidding documents are oftentimes received by the BSP-SPC from interested parties, i.e., losing bidders and uninvited non-government organizations (NGOs), in order for them to determine BSP-SPC's compliance with Republic Act No. 9184² (R.A. 9184) otherwise known as the Government Procurement Reform Act and its revised Implementing Rules and Regulations³ (IRR).

Data Privacy Act of 2012; scope; data classification approval

We wish to clarify that the Data Privacy Act of 2012⁴ (DPA) would only apply to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. Personal information is defined as any information whether recorded in a

¹ Tags: data classification; Government Procurement Reform Act; procurement documents; disclosure; transparency; general data privacy principles.

² An Act Providing for the Modernization, Standardization and Regulation of the Procurement Activities of the Government and for Other Purposes [Government Procurement Reform Act], Republic Act No. 9184 (2003). ³ Revised Rules and Regulations Implementing the Government Procurement Reform Act, Republic Act No. 9184 (2016).

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).

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.⁵

Where procurement-related documents would contain personal information, the provisions of the DPA may apply to the processing, which includes disclosure of the same, to the public and requesting parties.

Relevant to this matter, the NPC does not have a data classification approval process. As a personal information controller (PIC), the BSP can internally determine a classification of what data and/or documents are being processed, whether these involve personal and/or sensitive personal information (collectively, personal data), and whether the provisions of the DPA are applicable to the same, including the most appropriate lawful basis for processing.

Government procurement; disclosure of procurement-related documents; lawful basis for processing

We note that government procurement is governed by certain principles:

- Transparency in the procurement process and in the implementation of procurement contracts through wide dissemination of bid opportunities and participation of pertinent NGOs.⁶
- Public monitoring of the procurement process and the implementation of awarded contracts with the end in view of guaranteeing that these contracts are awarded pursuant to the provisions of the law, and that all these contracts are performed strictly according to specifications.⁷

With the above in mind, our procurement laws require that procurement opportunities and related documents, i.e., Annual Procurement Plan, Request For Quotation, Invitation to Bid, Supplemental/Bid Bulletin, Notice to Bidders, Contracts Awarded (NTP, NOA, PO, & WO), among others, are made public by the procuring entity through posting in the official agency website, Transparency Seal, the Philippine Government Electronic Procurement System (PhilGEPS), and even physically posting hardcopies of relevant documents in conspicuous places in the office premises of the procuring entity.

Hence, the disclosures above are required by a particular law or regulation

and procuring entities must comply. This is read together with the DPA provisions, particularly Section 12 (c) where the processing of personal information is necessary for compliance with a legal obligation to which the PIC is subject, or 12 (e) where personal information is processed for the fulfillment of the functions of a public authority, or Section 13 (b), where processing sensitive personal information is provided for by existing laws and regulations.

Assessment; general data privacy principles

For other procurement-related documents containing personal data the disclosure of which is not specifically stated under laws, rules, and regulations, requests for disclosure may be assessed by the procuring entity on a case-to-case basis, taking into account the general data privacy principles, specifically the following considerations:

- The purpose of the request must be legitimate and not contrary to law, morals, or public policy, and the personal data requested must be necessary to the declared, specified, and legitimate purpose;
- The document requested is not excessive in relation to the declared and specified purpose of the request;
- Redaction of personal data, where appropriate, should also be considered; and
- Determine whether abstracts, statistics, or aggregated data will suffice for the purpose of the request.

We also take note of some provisions of the revised IRR of RA No. 9184:

“Section 9. Security, Integrity and Confidentiality xxx xxx xxx

c) Confidentiality – The PhilGEPS shall ensure the privacy of parties transacting with it. For this purpose, no electronic message or document sent through the system shall be divulged to third parties unless such electronic message or document was sent after the sender was informed that the same will be made publicly available. The PhilGEPS shall protect the intellectual property rights over documents, including technical designs, submitted in response to Invitations to Bid.

⁵ Data Privacy Act of 2012, § 3 (g). 6

See: Government Procurement Reform Act, § 3 (a).

⁷ Id. § 3 (e).

Section 29. Bid Opening xxx xxx xxx

The bidders or their duly authorized representatives may attend the opening of bids. The BAC shall ensure the integrity, security, and confidentiality of all submitted bids. The abstract of bids as read and the minutes of the bid opening shall be made available to the public upon written request and payment of a specified fee to recover cost of materials.”

The above should also be considered in the assessment of whether procurement-related documents may be disclosed or not.

Finally, it is best that you consult with your data protection officer who may assist you in this endeavor.

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. 2021-008¹

15 March 2021



Re: **REQUEST FOR OFFICIAL LIST OF LEGITIMATE TAXI OPERATORS**

Dear 

We write in response to your letter forwarded by the Civil Service Commission - Cordillera Administrative Region on the request of the Association of Independent Taxi Operations and Drivers in the Cordillera (Association) for legal opinion on matters involving the Data Privacy Act of 2012 (DPA).

We understand that the Association requested from the Land Transportation Franchising and Regulatory Board – Cordillera Administrative Region (LTFRB-CAR) the list of legitimate taxi operators in the CAR in order for the Association to assist concerned government agencies in the anti-colorum drive and traffic decongestion efforts.

Specifically, the request pertains to the list of the legitimate taxi operators together with the Certificate of Public Convenience (CPC) number, number of taxi units, type of taxi units, and their corresponding plate numbers. We understand that such request was denied by LTFRB-CAR citing the provisions of the DPA.

We wish to clarify that the DPA only applies to the processing of personal information. Section 3 (g) of the DPA defines personal information as information from which the identity of an individual is apparent or can reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

¹ Tags: special cases; discretionary benefit of a financial nature; lawful basis for processing; freedom of 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).

On the other hand, the names of taxi operators, including the CPCs, the number and type of taxi units, may pertain to information of a juridical entity. Hence, such information is not considered personal information as defined under the DPA and do not fall within its scope.

But if the taxi operator is a sole proprietor, personal information may be involved since a sole proprietorship does not possess juridical personality that is separate and distinct from the personality of the individual owner of the business.

Given that the information being requested may contain personal and sensitive personal information (collectively, personal data) in cases where the taxi operator is an individual or a sole proprietor, the disclosure of such list should be in accordance with the DPA, its Implementing Rules and Regulations (IRR), and other issuances of the National Privacy Commission (NPC).

Special cases; DPA Implementing Rules and Regulations

We note that the Association argued that their request is outside of the scope of the DPA, citing as basis Section 4 which provides for specific information which are outside of the scope of the law and which the IRR classifies as special cases, specifically Section 4 (c), to wit:

“Section 4. Scope - This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing xxx.

This Act does not apply to the following: x x x

(c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit; x x x”

However, we wish to clarify that the above provision is further explained in the IRR:

“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, use, disclosure or other processing necessary to the purpose, function, or activity concerned: x x x

Information processed for purpose of allowing public access to information that fall within matters of public concern, pertaining to: x x x

3. Information relating to a benefit of a financial nature conferred on an individual upon the discretion of the government, such as the granting of a license or permit, including the name of the individual and the exact nature of the benefit: Provided, that they do not include benefits given in the course of an ordinary transaction or as a matter of right; x x x.”

From the foregoing, the above special case is not applicable in this scenario involving the list of the legitimate taxi operators and their CPCs, given that the issuance or the grant of a CPC is not discretionary on the part of the government and the same is given in the course of an ordinary transaction.³

Lawful basis for processing; law; legal claim

Nevertheless, the Association may evaluate whether its request would fall instead under Sections 13 (b) and (f) of the DPA:

“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

(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.”

For processing based on law, the Association mentioned that pursuant to Administrative Order No. 212, s. 2007,⁴ accredited transport groups have representation in the Presidential Anti-Colorum/Anti-Kotong Task Force (PACKTAF) as volunteer consultants.⁵ We likewise note that the Association also mentioned that the City of Baguio has an existing Anti-Colorum Ordinance⁶ and that anti-colorum operations are not limited to

the LTFRB enforcement unit.

We are not privy as to the actual implementation of the anti-colorum operations and other initiatives of the PACKTAF and Baguio City. Nevertheless, the Association may provide substantiation to the LTFRB-CAR that the same is a volunteer consultant under the abovementioned Administrative Order and is carrying out functions as such in relation to the request for information. Similarly, the Association may provide documentation as to its functions with respect to the enforcement of the Baguio City Ordinance.

For processing under paragraph (f) above, the Association should be able to establish that the requested information from the LTFRB-CAR is necessary, material, or indispensable for its purpose for processing, either for the protection of lawful rights and interests of the Association in court proceedings, the establishment, exercise, or defense of legal claims of the Association, or if the Association shall be providing the requested information to a government agency or public authority requiring the same based on its mandate.

Publicly available information; freedom of information

We wish to address the argument that the information sought is publicly available since the information is required to be printed on the sides of the taxi units, and that the list from LTFRB-CAR is just a summary.

In NPC Advisory Opinion No. 2017-41, we had the occasion to discuss the applicability of the DPA to the processing of publicly available personal data:

“There is no express mention that personal data which is available publicly is outside of its scope. Thus, “it is a misconception that publicly accessible personal data can be further used or disclosed for any purpose whatsoever without regulation.”

With this, we believe that the personal information controller (PIC) which collects and processes personal data from the public domain

³ See: National Privacy Commission, NPC Advisory Opinion No. 2017-20 (July 18, 2017).

⁴ Office of the President, Creating The Presidential Anti-Colorum/Kotong Task Force (PACKTAF) [Administrative Order No. 212] (2007).

⁵ Id. § 6.

⁶ See: The City Government of Baguio, Council passes anti-colorum ordinance, available at <https://baguio.gov.ph/content/council-passes-anti-colorum-ordinance> (last accessed: 14 March 2021).

must still observe the requirements under the law, specifically on the criteria for lawful processing of personal, sensitive personal and privileged information found under Sections 12 and 13 thereof.

Thus, even if the data subject has provided his or her personal data in a publicly accessible platform, this does not mean he or she has given blanket consent for the use of his/her personal data for whatever purposes.”⁷

We also take this opportunity to emphasize that the freedom of information is not absolute. The same is always harmonized with data privacy rights of individuals. The right to access personal data held by government agencies is regulated by the DPA and other applicable laws on the matter, including Executive Order No. 2, s. 2016 which provides for certain exceptions.⁸

Finally, we recognize the Association’s efforts in trying to assist government agencies in the anti-colorum drive and traffic decongestion efforts. With this, the Association may consider other less privacy-intrusive means as well to achieve its objectives.

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 See: National Privacy Commission, NPC Advisory Opinion No. 2017-41 citing the Hong Kong Office of the Privacy Commissioner for Personal Data, Guidance Note - Guidance on Use of Personal Data Obtained from the Public Domain (July 18, 2017).

⁸ Office of the President, Operationalizing in the Executive Branch the Constitutional Right to Information and the State Policies of Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor, Executive Order No. 2 [E.O. No. 2] (July 23, 2016).

ADVISORY OPINION NO. 2021-009¹

17 March 2021



Re: **FORENSIC AUDIT ON COMPANY-ISSUED ASSETS AND
COMPANY-RELATED ACCOUNTS**

Dear 

We write in response to your email received by the National Privacy Commission (NPC) which sought to clarify whether the conduct of a forensic audit on company-issued assets and company-related accounts will have any negative implications or non-compliance with the Data Privacy Act of 2012 (DPA) and if there are any specific guidelines for such audits.

We understand that the internal audit team of your company is planning to perform a forensic audit on company-issued assets such as laptops and mobile phones, and company-related accounts and accesses such as email addresses, WiFi access, browsing and download history, among others. The purpose of such forensic audit is to ensure that no confidential company information is disclosed to third parties and that the use of company-issued assets shall not cause any type of company information breach.

The NPC has limited information as to the actual scope of the forensic audit which may involve personal and sensitive personal information (collectively, personal data) stored in the company-issued assets and accounts. Nevertheless, should the processing activity involve personal data, the same should have a lawful basis under the DPA.

*Lawful basis for processing personal and sensitive personal information;
general data privacy principles*

¹ Tags: forensic audits; general data privacy principles; lawful basis for processing; data subject rights.

² 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, § 4 (2012). Tags: forensic audits; general data privacy principles; lawful basis lawful basis for processing;

The DPA provides for the various lawful criteria for processing personal data under Section 12 (personal information) and Section 13 (sensitive personal information). The company, as a personal information controller (PIC), should make a determination of the most appropriate lawful basis.

In any case, the company is expected to adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality, and should consider the following factors on the proposed activity:

- necessity and the lawful basis that may be applicable;
- fairness to the employees;
- proportionality of the processing to the concerns raised by the company; and
- transparency of the activity.³

If there are means through which the company can conduct the forensic audit without accessing and/or otherwise processing personal data contained in devices and accounts, such options should be explored and implemented.

We reiterate that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose, i.e., forensic audit. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.⁴

General guidance; transparency; data subject rights; security measures

Aside from determining the lawful basis for processing, the company should inform and notify the employees of the nature, purpose, and actual method and extent of the forensic audit, security measures to protect personal data, as well as the procedure for redress in cases where the rights of the employee as a data subject are violated.⁵ The company, as a PIC, is required to uphold data subject rights. For further guidance, you may refer to NPC Advisory No. 2021-01 - Data Subject Rights.

The company also has the obligation to implement reasonable and appropriate organizational, technical, and physical security measures for the protection of personal data which may be involved in the forensic audit. This may entail requiring persons who will be conducting the audit to sign non-disclosure agreements, where appropriate, to ensure

confidentiality. If the company will be outsourcing the forensic audit to a third-party service provider, such arrangement must be covered by an outsourcing agreement or similar document which shall clearly identify the corresponding obligations and liabilities of the parties.

We wish to emphasize that while the employees using the company-issued assets and company-related accounts may reasonably expect that the company would conduct periodic audits on said assets and accounts to ensure the security of company information and network, employers should keep in mind that employees are still entitled to their right to privacy at work.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

³ See: European Commission, Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, adopted on 8 June 2017, page 11, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 (last accessed: 16 March 2021).

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

⁵ Id. § 18 (a).

ADVISORY OPINION NO. 2021-010¹

17 March 2021



Re: **PRIVATE DETECTIVE SERVICES**

Dear 

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC). As a follow up to Advisory Opinion No. 2019-001,² you now seek further clarification on the applicability of the Data Privacy Act of 2012³ (DPA) to the specific services and engagements of your company, Eyespy Detectives and Investigators Co. (Eyespy).

From your letter, we understand that Eyespy, a duly licensed private detective agency, offers the following services:

1. Surveillance Operations – includes monitoring the activities and movements of a data subject, following the data subject in his/her day-to-day activities, and taking pictures and/or videos. Eyespy does not record conversations but only take videos or pictures of activities or interactions of the data subject in public places.
2. Undercover Operations – mostly requested by business owners or proprietors, whereby Eyespy deploys undercover personnel in the premises or areas of operation to investigate or determine liability for anomalies or irregularities including theft and fraud, preparatory to possible administrative sanctions or criminal prosecution against responsible personnel. A licensed private detective is employed by the client-company to work in their premises and discreetly observe the activities of the client's employees during working hours.

¹ Tags: Private detective services, background investigation, surveillance operations, undercover operations, lifestyle check, records check, right to privacy, lawful criteria for processing, data subject rights.

² National Privacy Commission, NPC Advisory Opinion No. 2019-001 (Jan. 3, 2019).

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).

3. Background Check – involves checking the information provided by the client on the data subject such as family, educational/professional background, and previous employment, among others, to determine whether the information provided by the data subject are truthful and accurate. Eyespy usually verifies the addresses, offices or establishment provided by the data subject and conducts discreet verification of the information provided.

4. Lifestyle Check – similar to surveillance investigation and background check except that the primary focus in the investigation is to determine whether the data subject is living within his or her means.

5. Records Check – involves checking and/or verifying with the records of private entities or government agencies any relevant information requested by the client in connection with the engagement.

Furthermore, you state that the services abovementioned are performed in connection with the following engagements:

1. Employers who request to investigate whether an employee is engaged in activities which violates employment stipulations such as non-competition clauses, exclusive employment (no moonlighting) clauses and other stipulations prohibiting employees from engaging in activities that are either in conflict or detrimental to the interest of the employer.

2. Insurance companies who ask to conduct Records Check and validate information/documents submitted by the insured or the latter's beneficiary. The Records Check usually requires validation of hospital, medical, police and/or funeral records. The insurance company would issue an authorization to Eyespy.

3. Creditors who plan to file collection suits against debtors but before doing so would ask Eyespy to perform Records Check to determine if the debtor has properties that can either be attached or used to satisfy any judgement issued for the case.

4. Foreign nationals or other individuals who request to conduct Background Check and Surveillance Operations on his/her Filipino partner in the Philippines before he/she continues to give support and/or proceed with the visa application to the foreign country.

5. A client who is either a principal, financier or business partner wants to check the general background and reputation of the subject person or company before deciding to enter into a business partnership.

6. A client who wants to check the activities of agents or employees in the Philippines to determine the latter's compliance with obligations under their contract.

7. A client whose rights to intellectual property is allegedly being infringed upon, requests Eyespy to obtain evidence of infringement and gather information about the infringer necessary for the application of a search warrant and/or prosecution.

8. A spouse who suspects marital infidelity of the other spouse, cohabiting with another person, or being engaged in any activity prejudicial to the marriage and the family. Eyespy is asked to conduct Surveillance Operations, including gathering of evidence to support cases for adultery, concubinage, annulment, legal separation, child custody, as may be applicable.

9. A client who is either the petitioner or the respondent in a guardianship case who wishes to interpose an objection to the appointment of another party as a guardian. Eyespy is asked to gather evidence which will be used in court to show that the adverse party is either disqualified or ill-suited to be appointed as guardian.

Eyespy posits it only accepts assignments that provide legal basis, i.e., protection or enforcement of the lawful rights or interest, and requires clients to accomplish a Service Request Form to provide a comprehensive background of the case and disclose the requested service. The potential client is notified beforehand that any information or report submitted should be used exclusively for the purpose indicated in the Service Request Form and should not be disclosed or shared with any third party.

You now seek guidance and clarification on the legality and propriety of the services conducted by Eyespy vis-à-vis the engagements mentioned. From your letter, we gathered these specific inquiries:

1. Are the services conducted in connection with the engagements

mentioned permissible and do not violate the DPA?

2. In the case of services performed for insurance companies: Is the authorization provided by the insurance company is already sufficient to authorize Eyespy to conduct Records Check?

3. In the case of Records Check for debt collection: Is Eyespy authorized under the DPA to gather information from pertinent government offices?

4. In the event that the data subject learns of the data gathering being conducted and demands that Eyespy cease and desist from data gathering and furnish the data subject a copy of all reports, information and data gathered, is Eyespy legally bound to comply with such demands? Is this applicable to any or all of the engagements?

5. In relation to Section 37 of the Implementing Rules and Regulations of the DPA (IRR), where the rights of the data subject “are also not applicable to the processing of personal data gathered for the purposes of investigations in relation to any criminal, administrative or tax liabilities of a data subject,” is the same applicable to any or all of the abovementioned engagements?

6. In the case of Records Checks, how can Eyespy deal with data controllers who refuse access to records on the mistaken insistence that it is prohibited under the DPA?

Legality of processing personal data by private detective services; criteria for processing personal data

On the services provided by Eyespy, you propose that the same are all permissible data gathering activities pursuant to the provisions of the DPA, specifically Section 12 (b) - processing of personal information is necessary and is related to the fulfillment of a contract with the data subject and Section 13 (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.

While the above provisions of the DPA may be applicable to certain services in relation to some aforesaid engagements, i.e., relating to

enforcement of existing contractual obligations for employment, insurance or loan-related matters, or in contemplation of or preparatory to, establishing, exercising or defending legal claims, it would be inaccurate to say that these provisions are the indeed the appropriate legal bases for Eyespy to carry out all of its services in relation to all the engagements earlier described.

Please note that the criteria for valid processing of personal and sensitive personal information (collectively, personal data) are enumerated in Sections 12 and 13 of the DPA, respectively. As discussed above, Section 12 (b) may be applicable in some instances where processing of personal information is related to or rooted on an existing contract between your client and the data subject, while Section 13 (f) may be applicable when processing sensitive personal information for legal claims or court proceedings.

With this, Eyespy should evaluate other possible lawful bases for processing, i.e., Section 12 (f) for processing personal information on legitimate interests pursued by the PIC 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, especially for those instances where there is no underlying contract involving the data subject and/or where Eyespy's client is not considering any legal action or proceeding from such personal data processing activity.

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.

Determination of DPA violation

As to the determination of whether there is a DPA violation in relation to the services provided by Eyespy, there can be no categorical statement to that effect based on the given information.

The Commission, where a complaint is filed or a sua sponte investigation is conducted, will have to take into consideration the circumstances of each situation and evidence submitted by the parties. Each case may be appreciated differently, depending on the manner of processing of personal data, whether there was adherence to the general data privacy principles, and data subject rights were upheld, among others.

We reiterate our position in Advisory Opinion No. 2019-001:

“Given the foregoing, it is for Eyespy to determine whether its acts, such as records verification and background investigation, would: (a) constitute a violation of an individual’s reasonable expectation of privacy, and (b) violate existing laws, including the DPA.

Note that the DPA dictates that its provisions shall be liberally interpreted in a manner mindful of the rights and interests of the data subject. Thus, it is the burden of Eyespy to ensure that any processing of personal data is in accordance with the law.”⁵

Conduct of Records Checks; authorization; general data privacy principles

In relation to Records Check services for insurance claims or cases, we wish to clarify that the authorization of the insurance company may just be one of the documents which may satisfy the requirements of the pertinent PIC to verify/validate the presented record or document.

Please note that the PIC being asked for the information will consider each request on a case-to-case basis, and must be satisfied that it is legitimate, within the lawful basis for processing under the DPA, and there is indeed an insurance claim or proceeding where the records validation is necessary for the purpose stated by the Eyespy.⁶ The same may hold true for the records check for debt collection.

⁴ 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-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>.

⁵ National Privacy Commission, NPC Advisory Opinion No. 2019-001 (Jan. 3, 2019).

⁶ See: UK Information Commissioner’s Office, When can I disclose information to a private investigator?, available at https://ico.org.uk/media/1556/disclosures_to_private_investigators.pdf (last accessed March 23, 2021).

In both cases, the affected data subject should have been informed at the outset, through the appropriate terms and conditions of the insurance contract, that verification of the information provided for insurance claims will be conducted when necessary, or in a loan agreement, whereby essential records will be verified/validated for purposes of debt collection.

Data subjects should therefore have an expectation that their personal data will be disclosed in relation to the aforementioned contractual obligations, subject to the general data privacy principles transparency, legitimate purpose, and proportionality.

Data subject rights in relation to private detective services; right to object; right to access; limitations

On the theoretical situation where the data subject learns of the personal data gathering conducted and demands Eyespy to cease and desist therefrom and furnish him or her a copy of all information gathered, Eyespy's compliance with such request will depend on the situation.

Note that while there may be a right to object to the processing of personal data, this applies in instances where processing is based on consent or legitimate interest. Hence, it is still possible to continue processing personal data where for example, the same is still 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.⁷

For further guidance, we refer to NPC Advisory No. 2021 – 01 on Data Subject Rights discussing the right to object, to wit:

“SECTION 7. Right to Object. — x x x

C. When a data subject objects, the PIC shall cease the processing of personal data and comply with the objection, unless the processing falls under any other allowable instances pursuant to in Sections 12 or 13, other than consent and legitimate interest.

Should there be other grounds to continue processing the personal data, the PIC shall have the burden of determining and proving the appropriate lawful basis or compelling reason to continue such processing. The PIC shall communicate and inform the data subject of said lawful basis or compelling reason to continue processing.”⁸

On the request to furnish a copy of the personal data collected, this may be anchored on the data subject right to access, and generally, may be granted by Eyespy. As an exception, this right may be limited when necessary for public interest, protection of other fundamental rights, or there exists a legitimate purpose justifying such limitation, which shall be proportional to the purpose of such limitation.⁹

Further, on the limitation provided in Section 37 of the IRR which you mentioned, the provision states in part:

“Section 37. Limitation on Rights. The immediately preceding sections shall not be applicable x x x. The said sections are also not applicable to the processing of personal data gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject. Any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research or investigation.”

The nature of investigations in the above provision pertain to those conducted by government agencies based on their respective mandates. This does not contemplate investigations made by private parties, even when it is in relation to an alleged crime such as adultery or concubinage as described in your letter. We again refer to NPC Advisory No. 2021 – 01 for further guidance:

“SECTION 13. Limitations. — x x x

B. Investigations in relation to any criminal, administrative, or tax liabilities of a data subject: provided, that:

1. The investigation is being conducted by persons or entities duly authorized by law or regulation;
2. The investigation or any stage thereof relates to any criminal, administrative, or tax liabilities of a data subject as may be defined under existing laws and regulations; and
3. The limitation applies to the extent that complying with the requirements of upholding data subject rights would prevent, impair, or otherwise prejudice the investigation. x x x”

⁷ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 34 (b) (2) (2016).

⁸ National Privacy Commission, Data Subject Rights [NPC Advisory No. 2021 – 01] § 7 (C) (January 29, 2021).

⁹ Id. § 13 and 13 (D).

Refusal of PICs to grant access to records

As mentioned above, PICs would have to make their own evaluation of the legitimacy of the requests for access and disclosure to personal data on a case-to-case basis, and must be sufficiently convinced that indeed, the personal data is necessary for the declared purpose, and that the processing is fair, lawful, may have been reasonably expected by the data subject in case of existing contractual obligations or legal claims, and/or within the legitimate interests of the client which is balanced with the rights and freedoms of the data subject.

Eyespy may likewise communicate with the data protection officers of these PICs and clarify its lawful basis for requesting records, keeping in mind that these organizations and government agencies may have already established procedures on access to personal data which should be complied with.

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. 2021-011¹

30 March 2021



Re: **REQUEST OF A VOTER FOR THE ERASURE OF NAME
FROM THE CERTIFIED LIST OF OVERSEAS VOTERS POSTED
IN PHILIPPINE EMBASSIES**

Dear 

We write in response to your request for clarification on whether the European Union (EU) General Data Protection Regulation² (GDPR) applies to the processing of personal data by Philippine embassies abroad.

The above concern is in relation to a request from a Philippine voter in the EU to have his/her name removed from the posted Certified List of Overseas Voters (CLOV) in a particular embassy. We note from your email that pursuant to Republic Act (RA) No. 9189,³ as amended by RA No. 10590, otherwise known as the Overseas Voting Act of 2013 (OVA), Philippine embassies abroad are required to post the CLOV on their premises.

COMELEC; Overseas Voting Act

The Commission on Elections (COMELEC), through the Office for Overseas Voting, oversees and supervises the effective implementation of the OVA. Under the said law, qualified citizens of the Philippines abroad may exercise their right to vote. We note the provision on Section 20 of the OVA, as amended, which reads:

¹ Tags: General Data Protection Regulation; Overseas Voting Act; Philippine Embassy; certified list of overseas voters; Vienna Convention on Diplomatic Relations; lawful criteria for processing; data subject rights; limitations.

² 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 (4 May 2016).

³ An Act Amending Republic Act No. 9189, Entitled "An Act Providing For A System Of Overseas Absentee Voting By Qualified Citizens Of The Philippines Abroad, Appropriating Funds Therefor And For Other Purposes [The Overseas Voting Act of 2013], Republic Act No. 10590 (2013).

“SEC. 20. Preparation and Posting of Certified List of Overseas Voters. - The Commission shall prepare the Certified List of Overseas Voters or CLOV not later than ninety (90) days before the start of the overseas voting period, and furnish within the same period electronic and hard copies thereof to the appropriate posts, which shall post the same in their bulletin boards and/or websites within ten (10) days from receipt thereof. x x x (underscoring supplied)

Hence, Philippine embassies, consulates, and other foreign service establishments are legally obligated to post the CLOV within ten days from receipt of such list from the COMELEC pursuant to the OVA.

EU GDPR; territorial scope; EU Data Protection Directive; Vienna Convention; Embassies; Extraterritorial Application of the DPA

To clarify, Article 3 of the GDPR enumerates the territorial scope of the law, namely:

1. The processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
 - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
 - (b) the monitoring of their behavior as far as their behavior takes place within the Union.
3. The processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

The GDPR only applies when an organization is processing personal data in the context of the activities of an establishment in the EU, or when non-EU organizations process personal data of data subjects in the EU, or in all diplomatic establishments of EU member-states located all over the world.

Conversely, the GDPR may not apply to embassies and consulates of non-EU member-states notwithstanding the fact that the non-EU embassy is within the territory of an EU member-state. In the European Data Protection Board Guidelines 3/2018 on the territorial scope of the GDPR,⁴ it was discussed in this wise:

“x x x by virtue of international law, certain entities, bodies or organisations established in the Union benefit from privileges and immunities such as those laid down in the Vienna Convention on Diplomatic Relations of 1961, the Vienna Convention on Consular Relations of 1963 or headquarter agreements concluded between international organisations and their host countries in the Union. In this regard, the EDPB recalls that the application of the GDPR is without prejudice to the provisions of international law, such as the ones governing the privileges and immunities of non-EU diplomatic missions and consular posts, as well as international organisations.”

We note that the Vienna Convention on Diplomatic Relations⁵ recognizes that while the premises of diplomatic missions remain under the jurisdiction of the host state, such are afforded special privileges and immunities.

Thus, the GDPR may not necessarily be applicable when the processing of personal data is done within the Philippine embassies in the EU. Nevertheless, the provisions of the Data Privacy Act of 2012⁶ (DPA) will apply to the same.

Data subject rights; right to erasure or blocking; limitation; lawful criteria for processing personal information

On the matter of the request for deletion of the name from the posted certified list of overseas voters, Section 16 (e) of the DPA provides that a data subject has the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system in certain instances. This may be read together with the right to object under Section 34 (b) of the Implementing Rules and Regulations⁷ (IRR) of the DPA.

These rights are further clarified in NPC Advisory No. 2021-01 on Data Subject Rights, which provides:

⁴ European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf (last accessed 31 March 2021).

“SECTION 7. Right to Object. — The data subject shall have the right to object to the processing of his or her personal data where such processing is based on consent or legitimate interest.

X X X

C. When a data subject objects, the PIC shall cease the processing of personal data and comply with the objection, unless the processing falls under any other allowable instances pursuant to in Sections 12 or 13, other than consent and legitimate interest.

Should there be other grounds to continue processing the personal data, the PIC shall have the burden of determining and proving the appropriate lawful basis or compelling reason to continue such processing. The PIC shall communicate and inform the data subject of said lawful basis or compelling reason to continue processing.

X X X

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;

⁵ Vienna Convention on Diplomatic Relations, available at https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf (last accessed 26 March 2021).

⁶ 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).

⁷ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).

3. The processing is unlawful; or
4. The PIC or PIP violated the rights of the data subject. x x x.”

However, it seems that none of the above instances is applicable in this scenario involving the posted voter list. Note that while a data subject has a right to object and request for erasure, such rights are not absolute. These may be limited, as in this instance, when the processing is in compliance with the provisions of the OVA and the COMELEC's and the embassies' legal obligation under the said law.

In this case, Section 20 of the OVA mandates the COMELEC to prepare the CLOV and furnish copies thereof to the appropriate embassies, consulates and other foreign service establishments for posting.

Thus, the COMELEC and the embassy may be justified in denying the request for erasure and may continue to post the said list. With this, the COMELEC and/or the embassy should clearly and fully inform the data subject of the reason for the denial of the request.⁸

General data privacy principles; transparency; privacy notice; proportionality

Finally, we take this opportunity to remind the COMELEC that any personal data processing should always adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.

We recommend the posting of a privacy notice which would provide information on the OVA, the CLOV, the rationale for its posting by embassies, and any other information relevant to the same. Furthermore, the CLOV should only contain such personal data that is necessary to achieve the purpose of the processing under the OVA, in keeping with the practice of data minimization.

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

⁸ National Privacy Commission, Data Subject Rights [NPC Advisory No. 2021-01] (January 29, 2021).

ADVISORY OPINION NO. 2021-012¹

30 March 2021



Re: **DOCUMENTARY REQUIREMENTS FOR ACCREDITATION AS FINANCIAL INSTITUTION**

Dear 

We write in response to your request for assistance and clarification received by the National Privacy Commission (NPC) on matters relating to the application of the Public Safety Savings and Loan Association, Inc. (PSSLAI) for accreditation as a financial institution with the Philippine National Police (PNP).

We understand that the PNP, through its Committee on Accreditation and Automatic Deduction (CAAD), certifies and accredits financial institutions who are likewise granted the privilege to avail of the PNP's Automatic Salary and Pension Deduction Scheme (ASPDS).

For PSSLAI's continued accreditation, the CAAD requested from PSSLAI the submission of, among others, a copy of PSSLAI's Credit Redemption Insurance (CRI) and the Summary List of PNP borrowers-members which includes Billing Reports containing the Schedule of Computations of Loans such as principal amount, date of grant of loan, mode of payment/terms, interest and other charges, effectivity of first billing, and maturity.

However, the PSSLAI did not submit the abovementioned requirements invoking the Data Privacy Act of 2012² (DPA) and bank secrecy laws.

You now seek clarification on whether the PSSLAI can furnish copies of the said documents to the PNP without violating the provisions of the DPA, its Implementing Rules and Regulations (IRR) and other relevant issuances of the NPC.

¹ Tags: scope; lawful criteria for processing; public authority; law or regulation; general data privacy principles; confidentiality; loans; deposits.

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 understand that the PSSLA is a non-stock savings and loan association (NSSLA) founded to uphold the best interest of the public safety sector, specifically dedicated to serving the members of the PNP and the Bureau of Fire Protection (BFP).³ The PSSLA offers loans and other investment opportunities.⁴ It is under the regulatory supervision of the Bangko Sentral ng Pilipinas (BSP).⁵

Scope; Data Privacy Act of 2012; personal information; lawful basis for processing

We wish to clarify that the DPA only applies to the processing of personal information. Section 3 (g) thereof defines personal information as any information from which the identity of an individual is apparent or can reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

We understand that the parties to the CRI are the insurer and PSSLA. We note that these are juridical persons. Thus, generally speaking, the insurance document contains information about such juridical persons, and not an individual's personal information. Hence, the submission of a copy of the same may be beyond the scope of the DPA. Nevertheless, should there be any personal information in the CRI, i.e., details of signatories, etc., the DPA may still be applicable.

In any case, it may be prudent for PSSLA to check for any confidentiality clauses and/or exceptions thereto in the insurance contract prior to submitting a copy of the CRI to the PNP.

As to the processing of personal information involving the submission of the CRI as well as the summary list and billing reports, the DPA provides for the various criteria for lawful processing.

For personal information, processing may be allowed subject to the provisions of Section 12. Particularly in this case, the following may be applicable: Section 12 (c), where the processing is necessary for compliance with a legal obligation or Section 12 (e), where processing is necessary to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.

For processing sensitive personal information in the given scenario, Section 13 (b) recognizes the processing that is provided for by existing laws and regulations, while Section 13 (f) provides for the processing for the establishment, exercise, or defense of legal claims, or when provided to government or public authority.

We note that the PNP issued Memorandum Circular No. 2014-42 which established, inter alia, the procedures and effective control measures in the accreditation of financial institutions. We likewise note the relevant provisions in PNP Memorandum Circular No. 2014-45 on documentary requirements, viz:

“IV. Policies/Guidelines xxx xxx xxx

b. Procedures

The Committee shall require the Financial Institutions/Entities to submit the following documents in their application for accreditation and/or renewal of accreditation: xxx xxx xxx

5. In addition to the aforementioned documentary requirements, all applicants for accreditation shall submit certified true copy of the following documents:

5.a For new applicants' accreditation:

5.a.1 Letter Request;

5.a.2 Copy of Credited Redemption Insurance;

5.a.3 Updated Audited Financial Statements;

5.a.4 Summary list of PNP borrowers-members which includes Billing Reports containing therein are Schedule of Computations of Loans such as Principal amount, date of loan granted, mode of payment/terms, interest and other charges, effectivity of 1st billing, and maturity;

5.a.5 Copy of the Loan Release Vouchers, Promissory Note/Policy Contract signed by PNP members;

5.a.6 List of Planholders (for insurance company), which includes amount of premium, effectivity, and maturity date of policy contract; and

5.a.7 At least 500 memberships.

³ Public Safety Savings and Loan Associations, Inc. About Us, Available At: <https://www.psslai.com/Company-Information/> (last Accessed 13 April 2021).

⁴ Id.

⁵ Bangko Sentral ng Pilipinas, Financial Stability - Directories And Lists, Directory Of Banks And Non-Bank Financial Institutions, Available At <https://www.bsp.gov.ph/Sitepages/Financialstability/Dirbanksfilist.aspx> (last

5.b For renewal of accreditation, submit the same requirements stated in para 5.a except item 5.a.5.”

We understand that these Memorandum Circulars were issued by the Chief of the PNP in the exercise of powers and functions pursuant to the provisions of Republic Act (RA) No. 6975 or the Department of the Interior and Local Government Act of 1990,⁶ as amended, and other applicable laws and regulations. Having said that, these issuances are presumed to be valid until declared otherwise by a proper court.

As applied in this case, it may be possible for PSSLAI to submit these documents, even without the consent of the data subjects, as the disclosure is not based on consent, but rather on another more appropriate lawful basis for processing, i.e., legal obligation, fulfillment of the functions of public authority, or due to a particular regulation which the PSSLAI must comply with.

General data privacy principles

However, as a personal information controller (PIC), the PSSLAI has the duty to inform its data subjects as to the nature, extent, and purpose of such disclosure pursuant to the principle of transparency.

Moving forward, PSSLAI should consider including a privacy notice in the loan agreements, explaining that personal information of the PNP member-borrowers, including the summary lists and billing reports, will be disclosed to the PNP for accreditation purposes. For existing member-borrowers, such notice should also be provided to apprise them about the required disclosure.

We acknowledge the concern on the submission of the summary list of member-borrowers and the respective billing reports. The PSSLAI’s data protection officer is not precluded from seeking dialogue with the PNP for a possible review of the 2014 Memorandum Circular requirements to evaluate if the disclosure is proportional to the purpose of the accreditation.

Revised Non-Stock Savings Loan Association Act of 1997; nature of loan records; deposits definition

⁶ An Act Establishing the Philippine National Police under a Reorganized Department of the Interior and Local Government, and for Other Purposes [Department of the Interior and Local Government Act of 1990], Republic Act No. 6975, § 26 (1990).

Another point raised in the letter is that if the PSSLA will submit to the PNP the summary list and other details, the PSSLA may run the risk of violating bank secrecy laws. We note that Section 6 of RA No. 8367 or the Revised Non-Stock Savings Loan Association Act of 1997⁷ provides as follows:

“Section 6. Prohibition against inquiry into or disclosure of deposits.
– All deposits of whatever nature with an Association in the Philippines are hereby considered as of an absolutely confidential nature and may not be examined, inquired or looked into by any person, government official, bureau or office, except upon written permission of the depositor, or in cases of impeachment, or upon order of a competent court in cases of bribery or dereliction of duty of public officials, or in cases where the money deposited or invested is the subject matter of litigation. xxx xxx xxx.”

The above-quoted provision must be read together with RA No. 3591 or the Philippine Deposit Insurance Law, as amended by RA No. 10846, which defines deposits as:

“(g) The term deposit means the unpaid balance of money or its equivalent received by a bank in the usual course of business and for which it has given or is obliged to give credit to a commercial, checking, savings, time or thrift account, evidenced by a passbook, certificate of deposit, or other evidence of deposit issued in accordance with Bangko Sentral ng Pilipinas rules and regulations and other applicable laws, together with such other obligations of a bank, which, consistent with banking usage and practices, the Board of Directors shall determine and prescribe by regulations to be deposit liabilities of the bank: Provided, That any obligation of a bank which is payable at the office of the bank located outside of the Philippines shall not be a deposit for any of the purposes of this Act or included as part of the total deposits or of insured deposit: Provided, further, That subject to the approval of the Board of Directors, any insured bank which is incorporated under the laws of the Philippines which maintains a branch outside the Philippines may elect to include for insurance its deposit obligations payable only at such branch.”

Therefore, since the summary lists and billing reports requested by the PNP pertain to loan records and not necessarily deposits, the same may not fall within the prohibition under RA No. 8367.

In addition, the BSP Manual of Regulations for Non-Bank Financial Institutions⁸ (MORNBFI) provides:

“Sec. 4312S Confidentiality of Information. NSSLAs shall keep strictly confidential the data on the borrower or consumer, except under the following circumstances:

a. disclosure of information is with the consent of the borrower or consumer;

b. release, submission or exchange of customer information with other financial institutions, credit information bureaus, lenders, their subsidiaries and affiliates;

c. upon orders of court of competent jurisdiction or any government office or agency authorized by law, or under such conditions as may be prescribed by the Monetary Board;

d. disclosure to collection agencies, counsels and other agents of the NSSLA to enforce its rights against the borrower;

e. disclosure to third party service providers solely for the purpose of assisting or rendering services to the NSSLA in the administration of its lending business; and

f. disclosure to third parties such as insurance companies, solely for the purpose of insuring the NSSLA from borrower default or other credit loss, and the borrower from fraud or unauthorized charges. (Circular No. 702 dated 15 December 2010)” (Underscoring supplied)

From our understanding, PSSLA is seeking accreditation with the PNP to avail of the automatic salary and pension deduction scheme. While we are not privy to the actual terms and conditions of the PSSLA’s accreditation and actual deduction scheme, the PNP may in effect be considered as a third-party that assists PSSLA’s lending business through the collection and remittance of loan payments.

Consequently, the disclosure of the summary list of the names of the member-borrowers and the latter’s billing reports may be allowed under the MORNBFI. However, we defer to the BSP on matters involving the proper interpretation of the above provisions of the MORNBFI.

⁷ An Act Providing For The Regulation Of The Organization And Operation Of Non-Stock Savings And Loan Associations [Revised Non-Stock Savings and Loan Association Act of 1997], Republic Act No. 8367 (1997).

⁸ Bangko Sentral ng Pilipinas, Manual of Regulations for Non-Bank Financial Institutions, available at https://www.bsp.gov.ph/Regulations/MORB/2016_01MORNBFI2.pdf (last accessed 17 April 2021).

Advisory Opinions as guidance

Finally, we take this opportunity to clarify the advisory functions of the NPC. In your letter, we noted that one of the actions requested of the Commission is to authorize PSSLAI to submit to the PNP the required documents.

We wish to emphasize the provisions on NPC Circular No. 18-01 – Rules of Procedure on Requests for Advisory Opinions,⁹ that the advisory opinions of the NPC provide guidance to the requesting party and the general public on matters relating to the interpretation of the provisions of the DPA, its IRR, and NPC issuances, compliance requirements, enforcement of data privacy laws and regulations, and other related matters on personal data privacy, security, and protection.¹⁰

As such, an advisory opinion does not operate to provide any authorization or clearance to process personal information. These are left to the sound determination of PICs, taking into consideration the provisions of the DPA, its IRR, and NPC issuances.

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

⁹ National Privacy Commission, Rules of Procedure on Requests for Advisory Opinions [NPC Circular No. 18-01] (10 September 2018).

¹⁰ Id. § 5 (a).

ADVISORY OPINION NO. 2021-013¹

26 April 2021



Re: REQUEST FOR INFORMATION IN AID OF IMPLEMENTING
THE HAGUE CHILD ABDUCTION CONVENTION

Dear 

We write in response to your request for an advisory opinion on whether the Department of Justice (DOJ) can request personal information from other Philippine government agencies in relation to the requests for assistance of Contracting States to locate the whereabouts of children and Taking Parents, in accordance with the Hague Convention on the Civil Aspects of International Child Abduction or the Hague Child Abduction Convention (HCAC), without violating the provisions of the Data Privacy Act of 2012² (DPA).

We understand that the DOJ, through the Office of the Chief State Counsel, is the designated Philippine Central Authority for the HCAC. The objects of the said convention are as follows: (1) to secure the prompt return of children wrongfully removed from or retained in any Contracting State; and (2) to ensure that rights of custody and of access under the law of one Contracting State are effectively respected in the other Contracting State. We understand that in most requests by HCAC Contracting States to the DOJ, the Taking Parents are Filipino nationals.

We understand further that when the DOJ receives an application under the HCAC, it requests the Bureau of Immigration to verify if the subject child and the Taking Parent entered the Philippines and/or if they subsequently left the country. Thereafter, the DOJ requests the assistance of the National Bureau of Investigation to locate the child and the Taking Parent.

¹ Tags: Hague Child Abduction Convention; Department of Justice; mandate; lawful criteria for processing; general data privacy principles; data subject rights; data sharing.

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).

Your present concern is in relation to a situation wherein a child and a Taking Parent's whereabouts are unknown. We note that you mentioned that Philippine passport holders are no longer required to accomplish Arrival Cards. Thus, it may be difficult to obtain lead information on the possible whereabouts of the child and Taking Parent.

In view of the foregoing, you are exploring options on possibly requesting for information from the Department of Foreign Affairs, Land Transportation Office, Commission on Elections, or the Philippine Statistics Authority, among others, to look for information on the possible whereabouts of the child and the Taking Parent, without violating the provisions of the DPA.

You likewise ask if there is a need for the DOJ to have a data sharing arrangement with the said agencies.

HCAC; DOJ; mandate; lawful basis for processing personal and sensitive personal information

Article 7 of the HCAC provides:

“CHAPTER II – CENTRAL AUTHORITIES

X X X

Article 7

Central Authorities shall co-operate with each other and promote co-operation amongst the competent authorities in their respective States to secure the prompt return of children and to achieve the other objects of this Convention.

In particular, either directly or through any intermediary, they shall take all appropriate measures –

- a) to discover the whereabouts of a child who has been wrongfully removed or retained;
- b) to prevent further harm to the child or prejudice to interested parties by taking or causing to be taken provisional measures;
- c) to secure the voluntary return of the child or to bring about an amicable resolution of the issues;
- d) to exchange, where desirable, information relating to the social background of the child;
- e) to provide information of a general character as to the law of their State in connection with the application of the Convention;
- f) to initiate or facilitate the institution of judicial or administrative

proceedings with a view to obtaining the return of the child and, in a proper case, to make arrangements for organising or securing the effective exercise of rights of access;

g) where the circumstances so require, to provide or facilitate the provision of legal aid and advice, including the participation of legal counsel and advisers;

h) to provide such administrative arrangements as may be necessary and appropriate to secure the safe return of the child;

i) to keep each other informed with respect to the operation of this Convention and, as far as possible, to eliminate any obstacles to its application.”

From the foregoing, the DOJ as the designated Central Authority to discharge the duties which are imposed by the HCAC, is mandated to take appropriate measures to discover the whereabouts of a child, among others. This is read together with the mandate of the DOJ derived from Executive Order No. 292³ or the Administrative Code of 1987.

The DPA recognizes such mandates and thus, the processing of personal and sensitive personal information (collectively, personal data) which may be necessary and appropriate for the objects of the HCAC may be allowed under the law. Sections 12 and 13 of the DPA provide for the various lawful criteria for processing, depending on the type of personal data being processed.

The DOJ may consider Sections 12 (c) where processing is necessary for compliance with a legal obligation and 12 (e) - necessary in order to fulfill functions of public authority, and/or Sections 13 (b) where the processing is provided for by existing laws and regulations, and 13 (f) where the processing 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.

General data privacy principles; data subject rights; safeguards; personal information controllers

While there may be a lawful basis for processing under the DPA in relation to the HCAC and other laws and regulations, we wish to reiterate that the DOJ, as a personal information controller (PIC), must always adhere to the principles of transparency, legitimate purpose, and proportionality.

Specifically for proportionality, 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 means.⁴

Hence, the DOJ should judiciously assess the proposal to request information from other government agencies as well as the types of information to be requested, if the same are proportional vis-à-vis the objects of the HCAC.

Data subject rights must likewise be upheld, and the DOJ should have mechanisms in place which enable the free exercise of such rights, subject to limitations under the applicable laws. The DOJ is also required to implement reasonable and appropriate security measures to protect personal data.

We remind government agencies that the processing personal data for the fulfillment of a statutory mandate should always strictly adhere to all required substantive and procedural processes and must not unreasonably infringe on the rights and freedoms of individuals guaranteed by the Constitution.⁵

Data sharing; data sharing agreement

As to your query on data sharing, the same is defined 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 (PICs).⁶ A data sharing agreement or 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.⁷

While not mandatory based on NPC Circular No. 2020-03, the DOJ may opt to execute DSAs with the identified government agencies as the same is a best practice and a demonstration of accountability amongst the parties to the data sharing:

3 Instituting the “Administrative Code of 1987” [Administrative Code of 1987], Executive Order No. 292, Title III (1987).

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

5 See: National Privacy Commission, NPC Advisory Opinion No. 2019-022 (May 9, 2019).

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

“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.”⁸

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 NPC Circular No. 2020-03, § 2 (g).

⁸ Id. § 8.

ADVISORY OPINION NO. 2021-014¹

26 April 2021



Re: **POSTING OF PHOTO IN A SOCIAL MEDIA PLATFORM WITHOUT CONSENT**

Dear 

We write in response to your email seeking advice from the National Privacy Commission (NPC) which was initially docketed as a complaint. Upon evaluation, the Office of the Privacy Commissioner endorsed the matter to the Privacy Policy Office for the issuance of an advisory opinion.

We understand that a certain individual took an intimate photo of you and your partner while dining in a restaurant and then proceeded to post it in a social media platform together with a derisive caption.

We understand further that you discovered that your photo was posted through a mutual friend who saw the same. You now ask for advice on the possibility of filing a case against the individual as you felt offended with the posting of your photo without your consent.

Privacy in a public place; privacy in the digital environment

According to the United Nations High Commissioner for Human Rights report, privacy can be considered as the presumption that individuals should have an area of autonomous development, interaction and liberty, a “private sphere” with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.²

Further, the report enunciates that in the digital environment, informational privacy covering information that exists or can be derived about a person and the decisions based on that information, is of particular importance, and the protection of the right to privacy extends to

¹ Tags: social media posts; unauthorized processing; data subject rights.

² United Nations High Commissioner for Human Rights, The right to privacy in the digital age, available at https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/AHRC_39_29_EN.docx (last accessed 26 April 2021).

public spaces and information that is publicly available.³

Accordingly, a person's data privacy rights do not cease even when one is in a public space. In NPC Advisory Opinion No. 2018-051,⁴ the following advice was given regarding persons who may have been candidly and secretly photographed and whose photos were then posted online:

“The act in the given scenario may be considered as unauthorized processing, depending on circumstances of the case. The DPA penalizes persons who process personal information without the consent of the data subject, or without being authorized under the Act or any existing law. This is subject to other provisions of the DPA. x x x

In cases like these, the affected data subject is entitled to suspend, withdraw or order the blocking, removal or destruction of his or her personal information upon discovery and substantial proof that the personal information is unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. x x x.”

As discussed above, data subjects should be able to exercise their rights under the Data Privacy Act of 2012⁵ (DPA). Kindly refer to NPC Advisory No. 2021 – 01 for further guidance on this matter.

Finally, we note that based on our records, you were not able to submit the required documentation to elevate your inquiry into a full-fledged complaint. If you wish to pursue the case and file a complaint, you may visit our website to download a copy of the Complaints-Assisted Form (CAF) available at <https://www.privacy.gov.ph/complaints-assisted/>.

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

³ Id.

⁴ National Privacy Commission, NPC Advisory Opinion No. 2018-051 (Oct. 5, 2018).

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).

ADVISORY OPINION NO. 2021-015¹

26 April 2021

[REDACTED]

[REDACTED]

Re: **TRANSFER OF EMPLOYEE RECORDS FROM SSS TO GSIS**

Dear [REDACTED]

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) to provide guidance on the legality of the disclosure or transfer of employee records without their consent to facilitate the transfer of remitted premiums or contributions from Social Security System (SSS) to the Government Service Insurance System (GSIS) considering the provisions of the Data Privacy Act of 2012² (DPA).

From your letters dated 12 April 2021 and 14 April 2021 together with the Civil Service Commission (CSC) Resolution No. 1900628³ provided, we understand that the Anti-Red Tape Authority (ARTA) is currently handling a complaint lodged by Duty Free Philippines Corporation (DFPC) employees against DFPC. One of the issues involved in the complaint is the transfer of the employees' premiums or contributions from SSS to GSIS.

We further understand that the facts and events which led to the filing of the complaint, critical to this inquiry, are as follows:

¹ Tags: lawful criteria for processing, legal obligation, government employees, premium contributions, SSS, GSIS, consent; proportionality.

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 Resolution No. 1900628 (Jun. 3, 2019).

- The DFPC is a government owned and controlled corporation (GOCC) with original charter created by R.A. No. 9563 or The Tourism Act of 2009 and a corporate body created out of Duty Free Philippines (DFP), an agency attached to the Department of Tourism (DOT). Prior to its charter, the DFPC was then a division of the defunct Philippine Tourism Authority (PTA) which was a corporate body attached to the DOT, as provided under Presidential Decree No. 564.
- On 30 June 1988, the PTA entered into a Contract of Professional Services (CPS) with the Employment Consultant of the Philippines, Inc. (ECPI) for the latter to provide DFPC with manpower requirements. On 11 May 1989, ECPI assigned its rights, duties and interests under the CPS to DFP Services, Inc. (DFPSI) through a Deed of Assignment. Deemed employees of DFPSI and not DFPC, the employee's terms and conditions of employment were governed by the Labor Code of the Philippines. Consequently, the employees' premiums or contributions were remitted to Social Security System (SSS).
- On 18 January 1998, the Department of Labor and Employment (DOLE) issued a Resolution declaring DFPC as the direct employer of the DFPSI employees, on the grounds of labor-only contracting. The Supreme Court, in its Resolution dated 7 December 1998, affirmed the DOLE Resolution. Pursuant to the DOLE Resolution, DFPC terminated the manpower services contract with DFPSI effective 31 December 1999. Accordingly, DFPC became the direct and immediate employer of the DFPSI employees. However, the employees' premiums were continuously remitted to the SSS instead of the GSIS.
- In the case of *DFP vs. Mojica*⁴, the Supreme Court declared that following: "...since DFP [Duty Free Philippines] is under the exclusive authority of the PTA, it follows that its officials and employees are likewise subject to the Civil Service rules and regulations," thus consequently affirming that DFPC employees are government employees. Accordingly, the premium contributions of the employees should have been remitted to the GSIS and not the SSS.
- On 3 June 2019, the CSC issued a Resolution ruling among others, that the period to be reckoned with in which the DFPC employees are to be considered as government

employees should be 31 December 1999, the date the manpower services contract between DFPC and DFPSI was terminated and not on 30 September 2005, when the Supreme Court rendered its decision in the Mojica case.

- It was only in 2016 that DFPC started remitting the premiums or contributions of the employees to the GSIS.

In relation to the foregoing, a complaint was filed by the DFPC employees with ARTA. We understand that the role of ARTA is to help resolve DFPC employees' issues and concerns, which include the transfer of their premiums or contributions from SSS to GSIS. The employees covered are those employed with DFPC from 31 December 1999 to 31 December 2015, whether such employees have retired, resigned, still employed or have been separated from DFPC.

In an online meeting held last 16 March 2021, the parties agreed for DFPC to coordinate with SSS to submit to ARTA a list of all covered employees together with relevant details. ARTA posits that the list would require disclosure of personal information which may have some data privacy implications.

You now seek guidance on the following queries:

1. Can the SSS directly transfer all the records of the covered employees from them directly to GSIS based only on the DOLE and CSC Resolutions?
2. Is the individual consent of all the covered employees necessary for the transfer of the SSS records?

Processing of personal information in compliance with a legal obligation

Under Section 12 (c) of the Data Privacy Act of 2012, processing of personal information is allowed when it is necessary for compliance with a legal obligation to which the personal information controller is subject, while Section 13 (b) allows the processing of sensitive personal information when the same is provided for by existing laws and regulations.

As stated in both Commonwealth Act No. 1865 and R.A. No. 8291, otherwise known as the GSIS Act of 1997⁶ (collectively, GSIS Laws),

⁴ Duty Free Philippines vs. Mojica, 471 SCRA 776 (2005).

the Government Service Insurance System covers all government employees, subject to some exceptions. According to these GSIS laws, membership is compulsory for employees while in government service.

In addition, these laws mandate covered employers and employees to pay premiums or contributions.

Through the Resolution of DOLE dated 18 January 1998 and the subsequent Supreme Court pronouncement in the Mojica case, the status of DFPC employees as government employees was affirmed. This was latter echoed by the CSC in its Resolution. It is then evident that DFPC and DFPC employees are indeed subject to the provisions of the GSIS Laws, including the payment of premiums or contributions.

From the foregoing, SSS may transfer the records of the covered DFPC employees, which may contain personal information and sensitive personal information, directly to the proper agency provided by law, GSIS.

Consent of employees, unnecessary; access of the SSS records by ARTA

Since the disclosure of DFPC employees' personal data is grounded upon law, consent from the employees is no longer necessary for the transfer of their SSS records to the GSIS. Under the DPA, consent of the data subject is only required when the same is the basis for the processing. It is worth noting that consent is only one of the lawful criteria for processing both personal information and sensitive personal information.

On the matter of ARTA obtaining the list of DFPC employees and their records, while it may be permitted by virtue of ARTA's mandate to facilitate and handle the issues and concerns subject of the complaint before it, the principle of proportionality requires that processing of personal information be adequate, relevant, suitable, necessary and not excessive in relation to the purpose of the processing.⁷

Therefore, it would be advisable for ARTA to facilitate the direct transfer of the employee records from SSS to GSIS without having to obtain the actual list or records of the employees, if possible. Limiting the number of parties having access to the records containing personal data minimizes any possible risks of data privacy violations.

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 An Act to Create and Establish a “Government Service Insurance System,” To Provide for Its Administration, And to Appropriate the Necessary Funds Therefor [Government Service Insurance Act], Commonwealth Act No. 186 (1936).

⁶ An Act Amending Presidential Decree No. 1146, As Amended, Expanding and Increasing the Coverage and Benefits of The Government Service Insurance System, Instituting Reforms Therein and For Other Purposes [The Government Service Insurance Act of 1977], Republic Act No. 8291 (1997).

⁷ See Section 11 of the DPA and Section 18 (c) of the Implementing Rules and Regulation of the Data Privacy Act of 2012.

ADVISORY OPINION NO. 2021-016¹

26 April 2021



Re: **DATA PRIVACY IMPLICATIONS OF UPLOADED CONTRACTS
IN THE DEVELOPMENT BANK OF THE PHILIPPINES' WEBSITE**

Dear 

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify the data privacy and security implications of the website posting requirements mandated by National Budget Circular No. 542² and Government Procurement Policy Board (GPPB) Circular No. 02-2020,³ issued in accordance to the requirements of Republic Act No. 9184⁴ otherwise known as the Government Procurement Reform Act and its revised Implementing Rules and Regulations⁵ (IRR), and how these can be reconciled with the provisions of the Data Privacy Act of 2012⁶ (DPA).

We understand that the Development Bank of the Philippines (DBP) is considering the implementation of various measures to mitigate possible risks that may arise in complying with the aforementioned issuances, after an assessment made that the type of information from the documents required to be posted may result into identity theft and possible falsification of documents. Among the security measures that DBP is considering are as follows:

1. Redaction of sensitive data, particularly on the acknowledgement page, in the notarized contracts including, but not limited to, actual signatures of parties, personal

¹ Tags: government procurement; procurement documents; posting requirement; security measures; redaction;

² Department of Budget and Management, Reiterating Compliance with Section 93, The Transparency Seal Provision, of the General Appropriations Act of 2012 [National Budget Circular No. 542] (August 29, 2012).

³ Government Procurement Policy Board, Guidelines in the Posting and Submission of Annual Procurement Plans, Procurement Monitoring Reports and Agency Procurement Compliance and Performance Indicator Results [GPPB Circular No. 02-2020] (May 20, 2020).

⁴ An Act Providing for the Modernization, Standardization and Regulation of the Procurement Activities of the Government and for Other Purposes [Government Procurement Reform Act], Republic Act No. 9184 (2003).

⁵ Revised Rules and Regulations Implementing the Government Procurement Reform Act, Republic Act No. 9184 (2016).

⁶ 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).

details such as identification numbers (e.g., tax identification numbers, passport numbers, driver's license numbers), and copies of actual identification cards of DBP officials and the latter's contractors/suppliers;

2. Exclusion of publishing of copies of identification cards of authorized signatories attached to signed contracts;

3. Possibility of placing the words: "[Signed]" in the published versions of the records instead of displaying the actual signatures of the official signatories – since scanned signatures may easily be copied and be manipulated to create fictitious records/documents; and

4. Exclusion of uploading documents or attachments that disclose details of the Bank's IT infrastructure and security defenses.

Scope of the Data Privacy Act of 2012; personal information

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. 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.⁷

Where procurement-related documents would contain personal information, the provisions of the DPA may apply to the processing, which includes disclosure of the same, to the public and requesting parties.

Government procurement; disclosure of procurement-related documents;

In NPC Advisory Opinion No. 2021-006,⁸ the Privacy Policy Office had the occasion to discuss some of the principles governing procurement in the government in relation to the lawful criteria for processing personal data. These same principles may be the basis for the aforementioned issuances requiring the posting of various procurement-related documents, thus:

"Government procurement; disclosure of procurement-related documents; lawful basis for processing

We note that government procurement is governed by certain principles:

- Transparency in the procurement process and in the implementation of procurement contracts through wide dissemination of bid opportunities and participation of pertinent NGOs.
- Public monitoring of the procurement process and the implementation of awarded contracts with the end in view of guaranteeing that these contracts are awarded pursuant to the provisions of the law, and that all these contracts are performed strictly according to specifications.”

Even if there is a lawful basis for processing personal data, the DPA further mandates all personal information controllers (PICs) to implement reasonable and appropriate organizational, technical, and physical security measures to protect personal data being processed, which may include the practice of redacting personal data, where appropriate.

Nevertheless, while the DPA mandates all PICs to undertake appropriate safeguards, the same must be read together with other existing laws, specifically in this case, government procurement laws and regulations, such as RA No. 9184 and its revised IRR as well as all relevant GPPB and Department of Budget and Management (DBM) issuances. As such, the security measures proposed to be undertaken by the DBP should still be consistent with the transparency and accountability principles underlying all government procurement activities, i.e., should there be specific requests for access to said procurement documents, the DBP should make such documents available for viewing or authentication purposes pursuant to the principle of transparency mandated by RA No. 9184.

Finally, the NPC recognizes DBP’s judicious assessment and efforts to implement additional safeguards which may be implemented. But in order to have a streamlined and standard process across all procuring entities as to how procurement documents are to be made public, a consultation with the GPPB, DBM, and other pertinent government agencies may be necessary.

⁷ Data Privacy Act of 2012 § 3 (g).

⁸ National Privacy Commission, NPC Advisory Opinion No. 2021-006 (March 5, 2021).

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. 2021-017¹

8 June 2021



**Re: INTELLECTUAL PROPERTY INVESTIGATION AND
ENFORCEMENT AGENCIES' RIGHTS TO INQUIRY AND
REQUEST FOR PERSONAL INFORMATION**

Dear 

We write in response to your letter received by the National Privacy Commission (NPC) seeking an opinion on the metes and bounds of intellectual property (IP) investigation and enforcement agencies' rights to an unhampered inquiry and requests for basic data, which includes personal information, from online platforms as well as financial intermediaries, in connection with the agencies' investigation of suspected intellectual property rights (IPR) violations which are within the respective agencies' legal mandates.

We understand that the National Committee on Intellectual Property Rights (NCIPR) is considering having an online investigation protocol in relation to IP investigating agencies queries on suspected IPR violators.

Scope of the Data Privacy Act of 2012; criteria for lawful processing of personal data

The Data Privacy Act of 2012² (DPA) applies to the processing of personal information, sensitive personal information, and privileged information (collectively, personal data) of natural persons by the government and private entities and individuals, within and outside the Philippines.

¹ Tags: law enforcement; investigation; mandate; due process; data sharing; data sharing agreement;

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], (2012).

The law likewise provides for the various criteria for processing personal data. Specifically in this scenario, Section 12 (e) of the DPA may be applicable. This provides for the processing of personal information necessary to fulfill functions of a public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.

In addition, for processing sensitive personal information and privileged information, Section 13 should likewise be considered. The said provision recognizes various lawful bases for processing applicable in this case, i.e., the processing is provided for by existing laws and regulations,³ or 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

Mandate of the NCIPR and member agencies; manner of requesting information; due process; general data privacy principles

In relation to the above, we understand that Executive Order (EO) No. 736⁵ created the NCIPR. The said EO provides as one of the NCIPR's mandates is to intensify regular and effective enforcement against IPR violations, and to allocate sufficient resources to ensure effective prosecution of pirates and counterfeiters.⁶

The NCIPR is composed of the following agencies:

1. Department of Trade and Industry (DTI);
2. Intellectual Property Office of the Philippines (IPOPHIL);
3. Department of Justice (DOJ);
4. Department of the Interior and Local Government (DILG);
5. Bureau of Customs (BOC);
6. National Telecommunications Commission (NTC);
7. National Bureau of Investigation (NBI);
8. Philippine National Police (PNP);
9. Optical Media Board (OMB);
10. National Book Development Board (NBDB);
11. Food and Drug administration (FDA);
12. Office of the Special Envoy on Transnational Crime; and
13. Department of Information and Communications Technology (DICT).

In this regard, the processing of personal data by the NCIPR and its member agencies, pursuant to their respective mandates, is recognized

under the DPA. The “metes and bounds” of these pertinent agencies’ rights to inquire and request for information in relation to investigations and enforcement actions are essentially defined by their own respective constitutional and/or statutory mandates.

In this scenario, requests for information from online platforms and financial intermediaries may come in various forms, i.e., courts orders, subpoenas, officially issued orders, memoranda, letters, and other communication, among others, depending on several factors, such as the stage of the investigation or enforcement action as well as the powers of the particular member agency, i.e., some may have subpoena powers and while others do not.

While the NPC is not fully cognizant of all means and methods by which government agencies can validly request for information, essentially, the NPC simply requires that all agencies processing personal data, whether for law enforcement, investigative, regulatory, or some other public function, should strictly adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.

Specifically, for the legitimate purpose principle, this presupposes that all due process requirements have been complied with in relation to any request for personal data. Likewise, for proportionality, the same requires that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

We emphasize that personal data processing activities of government agencies must not unreasonably infringe on the rights and freedoms of individuals guaranteed by the Constitution. Government agencies, as personal information controllers, are bound to uphold data subject rights provided for in the DPA.

Security of personal data; data sharing agreement

The NCIPR and its member agencies should consider the provisions of NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies, and NPC Circular No. 2020-03 on Data Sharing Agreements,

³ Data Privacy Act of 2012, § 13 (b).

⁴ Id. § 13 (f).

⁵ Office of the President, Institutionalizing Permanent Units To Promote, Protect And Enforce Intellectual Property Rights (IPR) In Different Law Enforcement And Other Agencies Under The Coordination Of The National Committee On Intellectual Property Rights (NCIPR), Executive Order No. 736 [E.O. No. 736] (June 21, 2008).

⁶ E.O. No. 736, § 4.

as may be reasonable and appropriate with respect to the personal data processing activities of each agency in relation to its duties and responsibilities under EO No. 736 and related IPR laws, rules, and regulations.

We remind government agencies that the DPA is not meant to prevent them from processing personal data when necessary to fulfill their mandates. Rather, it aims to protect the right to information privacy while ensuring free flow of information. What the DPA does is to promote fair, secure, and lawful processing of such information.⁷

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 See: National Privacy Commission, NPC Advisory Opinion No. 2019-046 (Dec. 17, 2019) citing NPC Advisory Opinion No. 2018-083 (Nov. 26, 2018).

ADVISORY OPINION NO. 2021-018¹

8 June 2021



Re: **PNP REQUEST FOR PERSONAL INFORMATION FROM
EMPLOYERS**

Dear 

We write in response to your request for advisory opinion on whether an employer may disclose the residential address, among others, of its current and/or former employees to law enforcement agencies serving warrants of arrest without violating the provisions of the Data Privacy Act of 2012² (DPA).

We understand that there have been instances wherein law enforcement agencies, such as the Philippine National Police (PNP), would come to the company premises to serve warrants of arrest on current and/or former employees.

We understand further that sometimes, these employees are not present in the company premises or not anymore connected with the company when the law enforcement officers try to serve the warrants, thus prompting the latter to request for the residential address, among others, of these employees so they may properly serve the same.

You now seek clarification whether you may disclose personal information of your current and/or former employees to the PNP without violating the DPA.

¹ Tags: law enforcement agencies; special cases; lawful processing of personal information; fulfillment of mandate; processing based on laws and regulations; general 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).

Scope of the DPA; special cases; fulfillment of mandates

Section 4 of the DPA provides that the DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. 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.³

Further, Section 4 (e) of the DPA provides that the processing of information necessary to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement, subject to restrictions provided by law, is one of the special cases where the application of the provisions of the DPA and its Implementing Rules and Regulations (IRR) is qualified or limited.

This means that when the personal information is needed to be processed by a public authority, such as the PNP, pursuant to its statutory mandate, the processing of such personal data is may be allowed under the DPA and its IRR, 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.

PNP mandate; powers and functions

We understand that the PNP has the power and function under Section 24 of Republic Act No. 6975 or the Department of the Interior and Local Government Act of 1990,⁴ to investigate and prevent crimes, effect the

arrest of criminal offenders, bring offenders to justice, and assist in their prosecution, among others.

In addition, the Chief of the PNP and the Director and the Deputy Director of the Criminal Investigation and Detection Group (CIDG) have been granted subpoena powers under Section 1 of Republic Act No. 10973⁵ to issue subpoena and subpoena duces tecum in relation to its investigation.⁶

The subpoena shall state the nature and purpose of the investigation, including a reasonable description of the books, documents, or things demanded which must be relevant to the *investigation*.⁷

Hence, as a general rule, it may be prudent for a personal information controller (PIC) to provide personal information to the PNP after it receives a formal subpoena to ensure that the PNP's request is authorized, proper, and lawful under existing laws and regulations. As previously stated, RA No. 10973 requires that the subpoena must state the personal information being requested, the reason for such request, and the relevance of the said request to the investigation being conducted.

In this case, however, although there is no subpoena from the PNP requesting for personal information, there is already an existing arrest warrant against the employees, thus, accommodating the PNP's request may be warranted under the DPA.

Nevertheless, the company is not precluded to further ask and/or confirm from the PNP additional details with respect to the validity of the warrant and the standard operating procedure to be followed in case the person to be arrested is not within the premises. The company should likewise keep documentation of such instances of disclosure of personal information in relation to law enforcement activities.

We emphasize that the DPA shall not be used to hamper, or interfere with, the performance of the duties and functions of duly constituted public authorities.

³ Data Privacy Act of 2012, § 3 (j).

⁴ An Act Establishing the Philippine National Police under a Reorganized Department of the Interior and Local Government, and for Other Purposes [Department of the Interior and Local Government Act of 1990], Republic Act No. 6975, § 24 (1990).

⁵ An Act Granting the Chief of the Philippine National Police (PNP) and the Director and the Deputy Director for Administration of the Criminal Investigation and Detection Group (CIDG) the Authority to Administer Oath and to Issue Subpoena And Subpoena Duces Tecum, amending for the Purpose Republic Act No. 6975, as amended, otherwise known as the "Department Of The Interior And Local Government Act Of 1990, Republic Act No. 10973, § 1 (2018).

⁶ Ibid.

⁷ Ibid.

The DPA 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.

General data privacy principles; proportionality

We wish to reiterate that while there may be lawful basis for processing under the DPA in this case, the company, as a PIC must always adhere to the data privacy principles of transparency, legitimate purpose, and proportionality.

Specifically, for proportionality, 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 means.⁸

In keeping with the proportionality principle of the DPA, it is prudent to determine what particular personal data should be released to the PNP to aid the latter in the execution of the warrant of arrest.

The company should judiciously assess the request for information and the types of personal information being requested, if the same are proportional to the purpose of serving a warrant of arrest. Personal information not indispensable to such purpose need not be disclosed to law enforcement agencies.

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

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

ADVISORY OPINION NO. 2021-019¹

23 June 2021



Re: **ACCESS TO DOCUMENTS IN AN ADMINISTRATIVE CASE**

Dear 

We write in response to your letter received by the National Privacy Commission (NPC) which sought clarification on whether a private complainant's request to be given copies of certain documents or case files, i.e., Answer to the Formal Charge, Decision, and Fallo, of an administrative case decided by the Philippine Postal Corporation (PHLPost) may be granted.

We understand that the PHLPost is of the opinion that based on prevailing jurisprudence, there is no private interest involved in an administrative case, and that the private complainant is only a mere witness. Further, the PHLPost follows its Revised Disciplinary Rules and Procedures on administrative cases, and suppletorily the 2017 Rules on Administrative Cases in the Civil Service (2017 RACCS), and that nothing in these rules provide for the right of private complainant to be given copies of the requested documents.

NPC Advisory Opinion No. 2019-011; sensitive personal information in proceedings; lawful criteria for processing

The Data Privacy Act of 2012 (DPA) considers information about any proceeding for any offense committed or alleged to have been committed by an individual, the disposal of such proceedings,

¹ Tags: administrative proceedings; sensitive personal information; lawful criteria for processing; Civil Service Commission 2017 Rules on Administrative Cases in the Civil Service; Code of Conduct and Ethical Standards for Public Officials and Employees;

or the sentence of any court in such proceedings, as sensitive personal information.² As a rule, the processing of sensitive personal information is not allowed except for the instances provided under the DPA. Some of these exceptions include processing which is provided for by existing laws and regulations,³ necessary for the establishment, exercise, or defense of legal claims,⁴ among others.

Thus, access to or disclosure of the above should have a lawful basis under the DPA, specifically under Section 13 of the law.

Civil Service Commission (CSC) 2017 Rules on Administrative Cases in the Civil Service (2017 RACCS); classification of offenses

We note the jurisprudence cited in your letter request and agree in principle that no private interest is involved in an administrative case.

Nevertheless, as we have very limited information as to the nature of the administrative case involved in this particular inquiry, we may have to briefly discuss and make a distinction on the classification of the administrative offense in this scenario.

We understand that based on the 2017 RACCS, there are grave, less grave, and light offenses, depending on their gravity or depravity and effects on the government service.⁵ In relation to such classification, the 2017 RACCS provides for the possibility of a settlement in administrative cases in Section 59, Rule 11, to wit:

“Section 59. Applicability. In cases of light offenses where the act is purely personal on the part of the private complainant and the person complained of and there is no apparent injury committed to the government, settlement of offenses may be considered. Provided that settlement can no longer be applied for the second offense of the same act committed by the person complained of.”⁶

The succeeding section of the above Rule 11 then proceeded to provide for the guidelines in the settlement of purely personal matters in administrative cases. This includes the execution of a Compromise Agreement between the parties if the settlement succeeds, the decision issued by the disciplining authority based on the Compromise Agreement, among others.⁷

With the above settlement in administrative cases for light offenses,

it appears that the private complainant is not merely a witness, but a party vested with the right to settlement and enter into a Compromise Agreement.

Hence, we presuppose that in this scenario, the private complainant may be entitled to be given copies of certain case-related documents, proportional to the purpose of entering into a settlement.

Rules Implementing the Code of Conduct and Ethical Standards for Public Officials and Employees

Where the above is not squarely applicable, we refer to the Rules Implementing the Code of Conduct and Ethical Standards for Public Officials and Employees⁸ (Rules) which may shed some light regarding access to case files or similar documents of such nature.

The Rules provide that every department, office, or agency shall provide official information, records or documents to any requesting public except if such information, record or document comprises drafts or decisions, orders, rulings, policy, decisions, memoranda, etc.⁹ The exception also applies if the request would disclose information of a personal nature where disclosure would constitute a clearly unwarranted invasion of personal privacy.¹⁰

The DPA is meant to be read and interpreted with other applicable laws which allow for the lawful processing of personal data. Under the current circumstances, there is a need to further evaluate the nature of the administrative case decided by the PHLPost and determine if there is categorically no appropriate lawful basis under the DPA or any other applicable law to allow the disclosure of the case files to the private complainant.

We further note that any doubt in the interpretation of any provision of the DPA shall be liberally interpreted in a manner mindful of the rights and individual interests of the individual whose personal data is processed.

² 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, § 3 (l) (2) (2012).

³ Data Privacy Act of 2012, § 13 (b).

⁴ Id. § 13 (f).

⁵ Civil Service Commission, 2017 Rules on Administrative Cases in the Civil Service [2017 RACCS], Rule 10, § 50 (July 3, 2017).

⁶ Id. Rule 11, § 59.

⁷ Id. Rule 11, § 60.

Finally, PHLPost is not precluded from seeking guidance from the CSC and its data protection officer since the said agency may have further insight on these types of requests for documents.

This opinion is based solely on the limited information you have provided. We are not privy to the provisions of PHLPost's Revised Disciplinary Rules and Procedures on administrative cases. 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

⁸ Civil Service Commission, Rules Implementing the Code of Conduct and Ethical Standards for Public Officials and Employees, Republic Act No. 6713, Rule IV, § 3 (d) (1989).

⁹ Id. Rule IV § 3 (d). ¹⁰ Id. Rule IV § 3 (e).

ADVISORY OPINION NO. 2021-020¹

25 June 2021



Re: **INSTALLATION AND USE OF GLOBAL POSITIONING SYSTEMS (GPS) ON MOTORCYCLE UNITS**

Dear [REDACTED]

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) to provide guidance on the legality of the installation of global positioning systems (GPS) tracker in your motorcycle units considering the provisions of the Data Privacy Act of 2012² (DPA).



Further, [REDACTED] seeks to implement the following privacy safeguards in case the installation of GPS trackers is allowed:

- Only the CEO, COO and IT Department will be given the administrative access rights to the said GPS Portal;
- Viewing/review access to the GPS portal will only be given when there is an urgent requirement and justifications approved by the CEO, COO and Audit Head;
- There will be time limits to viewing/review access to the GPS portal;
- There will be limits to the retention period of historical locations;
- Compliance with recommendations of external auditors regarding the usage of the GPS portal;

¹ Tags: global positioning systems, GPS devices, real-time tracking; proportionality.

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).

- Most importantly, [REDACTED] will require the lessee or borrower/mortgagor to provide his/her express consent to the installation and continuous operation of the GPS device on his/her motorcycle; and
- The GPS device will be uninstalled or removed when the motorcycle has been returned/surrendered to the company or when the loan is fully paid.

Thus, you now seek guidance on the legality and propriety of installing and using GPS devices in rented and collateralized units.

GPS device installation and use; proportionality principle

The pertinent issue in this case is whether the processing of personal information, or more particularly, the collection of location data of the lessee or borrower, through the installation of GPS devices in motorcycle units that are rented or on collateral, is warranted in the situation given. Processing, including the collection, access to and storage of an individual's location has with it various risks and threats to one's privacy and security.

Under the DPA, the processing of personal information shall be allowed upon compliance with the requirements of the law and adherence to the general data privacy principles of transparency, legitimate purpose and proportionality.³

The principle of proportionality dictates that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.⁴ Furthermore, personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.⁵

We note that the purpose sought by [REDACTED] is to prevent or deter the loss or theft of the motorcycles it has for rent or on loan may initially be seen as legitimate. However, this must be scrutinized against the possible violation of the individual's privacy and threats to security.

It is worth noting that [REDACTED], being a finance corporation, would already have in place proper procedures in the provision of motorcycles on rent or collateral, including KYC or Know-Your-Customer requirements or applications requiring the disclosure of personal data

by the client. Likewise, it is of common knowledge that this type of service requires the company and the client to come under a contractual agreement that would have provisions on penalties in case of default on loan payments or in cases of theft or loss of the vehicle.

In a broader perspective, [REDACTED] would then have the means to properly account for any damage it may incur from any loss or theft of its motorcycles on rent or collateral without having to unnecessarily intrude upon the privacy of its clients.

Consent

Even if there is a proposal to obtain consent from the individual, such consent may not be considered as freely given in the sense that the client has no other option but to accede to the requirement to be able to rent or obtain on collateral the motorcycle.

We reiterate that consent has to be freely given, specific, and an informed indication of will, whereby the data subject agrees to the collection and processing of personal data about and/or relating to him or her.⁶ In this case, if doubts are raised regarding the voluntariness of the consent obtained, the validity of the consent can be put into question as well.

While there are proposed guidelines to protect privacy and to obtain the consent of the individual, we deem that the installation of GPS devices on the motorcycles for rent or on collateral is disproportional to the purpose sought to be achieved by [REDACTED]. The company should consider other less privacy-intrusive means to achieve its objectives.

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

³ Data Privacy Act of 2012, § 11.

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

⁵ Ibid.

ADVISORY OPINION NO. 2021-021¹

30 June 2021



**Re:DISCLOSURE OF ADDRESSES OF TERMINATED
EMPLOYEES TO THE OFFICE OF THE PROSECUTOR FOR A
CRIMINAL CASE**

Dear 

We write in response to your letter seeking clarification from the National Privacy Commission (NPC) on whether the disclosure of addresses of terminated employees to the Office of the Prosecutor in connection with the criminal case filed by a company violates the Data Privacy Act of 2012² (DPA).

We understand from your letter that a certain company terminated several employees following all Department of Labor and Employment-prescribed procedures, and upon establishing factual and legal bases, the company subsequently filed a criminal case for libel against the said terminated employees.

Processing of personal data; lawful basis; Sections 12 and 13

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.

In particular, Section 12 (f) of the DPA allows the processing of personal information if the same is necessary for the purpose of the legitimate interests pursued by the personal information controller or by a third party. On the other hand, Section 13 (f) permits the processing of sensitive personal information if it 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.

¹ Tags: lawful basis for processing; personal information; sensitive personal information; establishment 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).

The decision of the Commission in the case of BGM vs. IPP,³ may apply in this scenario. The Commission cited Section 12 (f) in relation to Section 13 (f) of the DPA as a possible lawful criterion for processing personal information (as applied in this case, the addresses of the terminated employees) in relation to the protection of lawful rights and interests and legal claims (in this scenario, the criminal case for libel with the Office of the Prosecutor):

“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 protection 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.” (citing CID Case No. 17-K-003 dated 19 November 2019 and NPC 18-135 dated 06 August 2020)

From the foregoing, the disclosure by the company of the addresses of terminated employees to the Office of the Prosecutor in connection with the criminal case filed with the same may be allowed under the DPA based on the above considerations.

³ National Privacy Commission, NPC 19-653 (Dec. 17, 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 30 June 2021).

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. 2021-022¹

2 July 2021



Re: **PROCESSING PERSONAL DATA FOR ELECTRONIC KNOW-YOUR-CUSTOMER (eKYC)**

Dear 

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify the appropriate lawful basis for processing for a digitization project of a bank to ensure compliance with the provisions of the Data Privacy Act of 2012² (DPA) and the requirements of the Bangko Sentral ng Pilipinas (BSP).

We understand that the bank is currently in the process of designing its digital onboarding process will entail the processing of personal and sensitive personal information (collectively, personal data) from applicants who wish to open a bank account or apply for a bank loan online.

We understand further that the bank will obtain the applicants' consent through a tick box and/or clicking on an Agree button after reading the Data Privacy Consent/terms and that the same will be recorded in the system.

In addition to the above, you likewise mentioned that opening an account or applying for a loan will then entail prior identity verification or know-your-customer (KYC) verification in accordance with the requirements of the BSP which allows electronic KYC.

You now ask whether consent or the regulatory requirement of the BSP would be the lawful basis for processing which will allow the bank to

¹ Tags: lawful basis for processing; laws and regulations; BSP; know your customer (KYC); outsourcing.

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).

provide the captured information in the digital onboarding platform (e.g., valid ID, selfie, or liveness capture) to a third party eKYC solutions provider for the sole purpose of accurately verifying the identity of the applicant or customer. You further ask if consent is the lawful basis, will the affirmative and recorded consent via tick box or Agree button suffice as evidence of consent.

Lawful basis for processing of personal data; law or regulation; privacy notice

For this scenario, Section 13 (b) of the DPA on the processing of sensitive personal information based on existing laws and regulations is applicable and may be the most appropriate lawful basis for processing considering the bank's relationship with its customers vis-à-vis compliance requirements with the BSP Manual of Regulations for Banks (MORB).

For the digital onboarding platform, we suggest that instead of asking for consent, the bank should provide a privacy notice which is an embodiment of the observance or demonstration of the data privacy principle of transparency and upholding the right to information of data subjects.³ It is a statement made to data subjects that describes how the organization collects, uses, retains, and discloses personal information.⁴

Outsourcing; data subjects rights

For outsourcing, we note the MORB provisions you have provided. These are read together with the provisions of the Implementing Rules and Regulations⁵ (IRR) of the DPA, specifically Sections 43-45. The stipulations for outsourcing agreements indicated in these provisions should be included in the bank's agreement with its eKYC solutions provider.

We emphasize that the bank, as a personal information controller, shall use contractual or other reasonable means to ensure that proper safeguards are in place in an outsourcing arrangement, which includes ensuring the confidentiality, integrity, and availability of the personal data processed, prevent its unauthorized processing, assure that the personal information processor cooperates and coordinates with the bank in addressing any requests for the exercise of data subject rights, and generally, comply with the requirements of the DPA and other applicable issuances of the NPC.⁶

Privacy by design

Lastly, as industries shift to digital platforms, the NPC encourages the adoption of a privacy by design approach that ensures that privacy and data protection have been taken into account during the design phase of a system, project, program, and process and will continue to be taken into account throughout its lifecycle and implementation.⁷

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

³ National Privacy Commission, Data Subject Rights [NPC Advisory No. 2021 – 01] (Jan. 29, 2021).

⁴ Id. citing National Privacy Commission, NPC Advisory Opinion 2018- 013 (2018).

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

⁶ Id. § 43 and NPC Advisory No. 2021 – 01, § 5 (c).

⁷ 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 2 July 2021).

ADVISORY OPINION NO. 2021-023¹

5 July 2021



Re: **PROCESSING OF PERSONAL DATA FOR RESEARCH WITHOUT ETHICS CLEARANCE**

Dear 

We write in response to your letter received by the National Privacy Commission (NPC) which sought an assessment if there is a potential case of data sampling with unlawful collection or processing for an unauthorized purpose not specified in the consent form, in relation to a research conducted without the proper clearance and approval from the appropriate authorities and institutions.

In your letter, we understand that a study entitled “Genomic Characterization of the Filipino People” was conducted by a certain Filipino researcher currently working at the Department of Organismal Biology, Human Evolution of the Uppsala University in Sweden. You further disclosed that the said researcher applied for ethics clearance from the National Ethics Committee (NEC) in 2015 to collect, transport, and analyze saliva samples sourced from indigenous peoples/indigenous cultural communities (IPs/ ICCs) of the Philippines. However, no ethics clearance was issued since the conditions imposed by NEC were not satisfied and the researcher did not pursue his application for ethics clearance further.

We further understand from your letter and its annexes that the researcher allegedly committed the following improprieties in the conduct of his study:

1. According to the published study, the researcher reportedly collected more than one thousand ninety-four (1,094) individual biological samples from one hundred twelve (112) Filipino

¹ Tags: health data; genetic data; sensitive personal information; special cases; research; ethical and legal obligations; consent.

ethnolinguistic groups without the required research ethics clearance, as required by Joint Memorandum Order (JMO) No. 2012-001 on the Requirement for Ethical Review of Health Research Involving Human Participants;²

2. Saliva samples were collected from IPs/ICCs without observing the guidelines required by the National Commission on Indigenous Peoples (NCIP), the primary government agency mandated to protect the rights and well-being of IPs/ICCs, as required by NCIP Administrative Order (AO) No. 2012-1³ and NCIP AO No. 2012-3.⁴ In particular, the researcher and his team conducted the research without being accompanied by an NCIP team designated to monitor compliance with the Indigenous Knowledge and Systems Practices (IKSP) of the communities; and

3. The biological samples were transferred from the Philippines to Sweden without the required Material Transfer Agreement (MTA), as approved by an accredited research ethics committee. The MTAs submitted by the researcher have been disapproved, the disapproval of which was communicated to him, since the parties to the MTA must be a local Philippine institution/indigenous community and the Uppsala University. However, the researcher chose to withdraw his application for ethics clearance instead, alleging that the NEC does not have regulatory mandate on the nature of his study.

You disclosed in your letter that the researcher still proceeded with the study despite the lack of ethics clearance. Further, you discovered that the study has been published in a reputable science journal and that the researcher was among those awarded of a two-year grant by the European Commission for a project titled “Probing the Genetic Diversity and Demographic History of Ancient Seafarers in ISEA and Oceania, from Archaic Hominins to the Dispersal of the Malayo Polynesia Language Family” where the samples collected by the researcher from the Philippines will be used.

We note also that the NCIP issued a statement dated 15 April 2021 condemning the conduct of genetic/genomic research with indigenous peoples by the researcher without Free and Prior Informed Consent (FPIC) and the required ethical clearance; that the blatant disregard of policies governing scientific research in the Philippines will have far-reaching adverse impact to the governance of scientific research in the

country; and that the lack of consent offends the rights of the IPs/ICCs to self-determination, self-governance, human rights, and social justice. You now express concern over the possible unlawful processing of personal data involved in the study since this may have serious implications in scientific integrity. You now ask on the possible actions that may be taken, considering the provisions of the Data Privacy Act of 2012⁵ (DPA).

Scope of the DPA; research; special case

Research is an activity that aims to develop or contribute to knowledge that can be generalized (including theories, principles, relationships), or any accumulation of information using scientific methods, observation, inference, and analysis.⁶

Section 4 of the DPA enumerates the categories of personal information and sensitive personal information (collectively, personal data) which fall outside the scope of the law. This includes the processing of personal data for research purposes.⁷ The DPA recognizes that research is critical to nation-building and serves a public interest.⁸ It is therefore the intent of the DPA to grant a certain degree of flexibility in the processing of personal data for purposes of research.⁹ Stated differently, a personal information controller, such as a researcher, may lawfully process personal data even without meeting the criteria provided by Section 12 and Section 13 of the DPA.¹⁰

However, this exemption is not absolute. The following must be strictly complied with:

1. the processing must be only to the minimum extent necessary to achieve the specific purpose, function or activity.¹¹
2. the research must be:
 - a. intended for a public benefit;
 - b. subject to the requirements of applicable laws, regulations or ethical standards.¹²

² Department of Science and Technology, Department of Health, Commission on Higher Education and University of the Philippines Manila, Requirement for Ethical Review of Health Research Involving Human Participants, Joint Memorandum Order No. 001, Series of 2012 [Joint Memorandum Order No. 2012-001] (December 28, 2012).

³ National Commission on Indigenous Peoples, The Indigenous Knowledge Systems and Practices (IKSPs) and Customary Laws (CLs) Research and Documentation Guidelines of 2012, NCIP Administrative Order No. 1, Series of 2012 [NCIP AO No. 2012-1] (March 15, 2012).

⁴ National Commission on Indigenous Peoples, The Revised Guidelines of Free and Informed Prior Consent (FPIC) and Related Processes of 2012, NCIP Administrative Order No. 3, Series of 2012 [NCIP AO No. 2012-3] (April 13, 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).

The exemption afforded to the processing of personal data for research purposes shall only apply if the requirements of applicable laws, regulations or ethical standards are complied with. Research on human subjects, especially persons belonging to a vulnerable group such as ICCs, are bound by various ethical and legal obligations.

First, the guidelines under JMO No. 2012-001 on the Requirement for Ethical Review of Health Research Involving Human Participants must be observed in the conduct of the study. Second, the provisions of NCIP AO No. 2012-1 and NCIP AO No. 2012-3 on research and documentation guidelines and free and prior informed consent, respectively, must also be complied with since the data subjects are IPs/ICCs.

The researcher apparently failed to complete the foregoing ethical and legal standards during the conduct of his study, as determined by the NEC and the NCIP, the appropriate authorities on this matter. As a result, the processing of personal data pursuant to such study cannot be considered as a special case under the DPA since the conditions provided by the law were not fulfilled.

Health data as sensitive personal information; genetic data

Information about an individual's race, ethnic origin, health, and genetics are classified as sensitive personal information under the DPA.¹³ The processing of sensitive personal information is allowed, if not otherwise provided by law, when at least one of the criteria required by Section 13 of the DPA is complied with.

Note that the DPA does not provide a definition for the term “genetic data”. However, the EU General Data Protection Regulation¹⁴ (GDPR) may provide further insight on this matter. It defines genetic data as “personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.”¹⁵

⁶ Philippine Health Research Ethics Board Ad Hoc Committee for Updating the National Ethical Guidelines, National Ethical Guidelines for Health and Health Related Research, Introduction, p. 5 (2017).

⁷ Data Privacy Act of 2012, § 4 (d).

⁸ See NPC Advisory Opinion No. 2019-017 (March 5, 2019).

⁹ Ibid.

¹⁰ See NPC Advisory Opinion No. 2020-029 (July 30, 2020).

¹¹ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (2016).

¹² Id. § 5 (c).

¹³ Data Privacy Act of 2012, § 3 (I).

Hence, genetic data can only be considered personal data if it can directly identify a specific individual. A genetic sample by itself is not personal data unless it is analyzed to produce data which can identify a specific individual.¹⁶ Similarly, anonymized or aggregated genetic data without any identifiers or which can no longer be related to any specific genetic identity or profile shall not be considered personal data.¹⁷

Given the foregoing, the saliva samples collected from the IPs/ICCs may not be considered personal data as defined under the DPA if the same can no longer be related to the identity of the person from whom it was collected.

However, we note that the DPA still applies to the other personal data that were collected from the data subjects through the consent form.

Lawful basis for processing sensitive personal information; consent

As the research herein described failed to meet the standards provided by the DPA to be considered a special case, there must be lawful basis in the processing of sensitive personal information under Section 13 of the DPA.

In particular, Section 13 (a) provides that the processing of sensitive personal information is allowed when the data subject has given his or her consent, specific to the purpose prior to the processing.

Consent under the DPA refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal data about and/or relating to him or her.¹⁸ Consent shall be evidenced by written, electronic or recorded means and may also be given on behalf of the data subject by an agent specifically authorized by the data subject for the said purpose.¹⁹

We note that the act of the IPs/ICCs in providing personal data to the researcher, while seemingly freely given, will still not suffice. We wish to emphasize that the DPA is meant to be read and interpreted with other applicable laws on consent.

¹⁴ 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 (4 May 2016).

¹⁵ EU General Data Protection Regulation, Art. 4 (13).

¹⁶ See: Information Commissioner's Office, UK, What is special category data?, available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd3> (last accessed 5 July 2021).

¹⁷ Ibid.

¹⁸ Data Privacy Act of 2012, § 3 (b).

¹⁹ Ibid.

In the current matter, specific guidelines are applicable on how the FPIC of the IPs/ICCs as data subjects/participants in a study must be obtained. Hence, the procedural and documentary requirements on consent under JMO No. 2012-001 and NCIP AO No. 2012-3 must be strictly construed.

In addition, under the DPA, the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including among others, the risks and safeguards involved.²⁰ The test to determine whether the general data privacy principle of transparency has been complied with is to assess whether the target audience could have understood the information provided to them.²¹

In the current matter, the data subjects involved were IPs/ICCs. The researcher, as personal information controller, should have considered the use of plain and simple language in the consent form to inform them of how exactly their data will be used and the consequences of providing such data to the researcher.

Considering that there are concerns raised on the alleged lack of FPIC in relation to the absence of the required ethical clearance, the affected data subjects or their appropriate representatives may consider filing a complaint before the NPC pursuant to the provisions of NPC Circular No. 2021-01 or the 2021 Rules of Procedure of the National Privacy Commission.²²

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

²⁰ Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (a).

²¹ See: National Privacy Commission, *JVA v. U-PESO.PH Lending Corporation* (UPESO), NPC Case No. 19-498 (9 June 2020).

²² National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC Circular No. 2021-01], available at https://www.privacy.gov.ph/wp-content/uploads/2021/01/2021RULESOFPROCEDURE_VER8-Final-Sgd-1-1-1.pdf.

ADVISORY OPINION NO. 2021-024¹

7 July 2021



Re: **PUBLIC DISCLOSURE OF INFORMATION ON SOCIAL WELFARE AND DEVELOPMENT AGENCIES, SERVICE PROVIDERS, AND CIVIL SOCIETY ORGANIZATIONS**

Dear 

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) to provide guidance on the various concerns with respect to the processing of data pertaining to Social Welfare and Development Agencies (SWDAs), Service Providers (SPs), and Civil Society Organizations (CSOs) registered, licensed, and accredited by the Department of Social Welfare and Development (DSWD) considering the provisions of the Data Privacy Act of 2012² (DPA).

Specifically, you ask for clarification on the following:

1. Whether the public disclosure of pertinent information of the SWDAs, SPs and CSOs is a violation of the DPA:
 - Data for research and other purpose, in compliance to Executive Order No. 2 dated 23 July 2016 on Freedom of Information (FOI) (E.O. No. 2, s. 2016) to be released to private individuals, National Government Agencies, Local Government Units, Non-Government Organizations, Business Entities and other interested parties;
 - Data about SWDAs that were granted or received benefits, particularly those organizations who received cash incentives from the DSWD;

¹ Tags: lawful basis for processing; social welfare and development; fulfillment of mandate of public authority; consent; freedom of information; privacy notice.

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).

- Information of Blacklisted SWDAs and CSOs; and
 - Information sharing among offices under the DSWD such as Field Offices.
2. Whether consent or privacy notice is required for the following scenarios:
- Processing of application for Registration, Licensing and Accreditation of SWDAs, SPs and CSOs; and
 - Posting of general information, i.e., Name of SWDA/SPs/CSOs, address, landline number, cellphone number, email address, contact person, certificate details, programs and services, clientele, and areas of operation, at the DSWD website.
3. Various questions on consent as a lawful basis for processing in the given scenarios above.

Scope of the DPA; information of juridical entities; disclosure in accordance with governing law or regulation

We wish to clarify that the DPA only applies to the processing of personal information of natural persons and not information of juridical entities recognized under the law, such as corporations, associations, and partnerships.

From a reading of available DSWD regulations, we understand that SWDAs, SPs, and CSOs are juridical entities. Hence, information of these juridical entities is outside the scope of the DPA. Disclosure of the same is governed by some other law or regulation.

Disclosure of personal data related to juridical entities; fulfillment of mandate of public authority

We take note of the following DSWD issuances:

- DSWD Memorandum Circular No. 17, Series of 2018 on the Revised Guidelines Governing the Registration, Licensing of Social Welfare and Development (SWD) Agencies and Accreditation of SWD Programs and Services (MC 17, s.2018);
- Memorandum Circular No. 01, Series of 2020 on Policies

and Procedures on the Accreditation of Social Welfare and Development (SWD) Programs and Services of SWD Agencies Operating in One Region: Supplemental to Memorandum Circular No. 17 s2018 (MC 01, s.2020); and

- Memorandum Circular No. 13, Series of 2019 on the Guidelines on the Accreditation of Civil Society Organizations (CSOs) To Implement DSWD Programs Using DSWD Funds (MC 13, s.2019),

all of which laid out with clarity the legal bases of DSWD's power and authority to register, license and accredit SWDAs, SPs and CSOs. Pertinent to this discussion, we further cite certain objectives stated in MC 17, s.2018:

“2. This guideline likewise emphasizes the objectives of Registration, Licensing, and Accreditation, namely:

2.1 To regulate enforce SWD standards to public and private organizations in the country that are engaged or planning to engage in SWD programs and services endeavors through registration, licensing, and accreditation;

2.2 x x x

2.3 To protect the clients against abuses, exploitations and inefficiency from organizations engaging in SWD entities;

2.4 x x x

2.5 To promote transparency and accountability of SWDAs to their respective donors, clients and general public.”³

Likewise, DSWD MC 13, s.2019 mentions the regulatory power of DSWD over CSOs engaged in the delivery of social welfare and development programs and services.⁴

In relation to the above, where disclosure of personal and/or sensitive personal information (collectively, personal data) of individuals connected to the SWDA, SP, or CSO is involved, the DPA will apply.

Under the DPA, Section 12 (e) provides that the processing of personal information shall be permitted when it is necessary to fulfill the functions

³ Department of Social Welfare and Development, Revised Guidelines Governing the Registration, Licensing of Social Welfare and Development (SWD) Agencies and Accreditation of SWD Programs and Services, Memorandum Circular No. 07, Series of 2018 [DSWD M.C. 07, s.2018] (August 29, 2018).

of a public authority which includes the processing of personal data for the fulfillment of its mandate. If sensitive personal information is involved, processing may be based on Section 13 (b) which recognizes processing that is provided for by existing laws and regulations.

The DSWD may process any personal data of individuals, who may be directors, officers, employees or members of SWDAs, SPs, and CSOs which may include their names, contact information, business addresses, when such processing is necessary to fulfill its functions in the registration, licensing and accreditation of said entities, including monitoring and oversight functions.

Any processing of personal data in relation to disclosure of information of Blacklisted SWDAs and CSOs and sharing of information between DSWD offices may be anchored on the above provisions as well.

Freedom of Information requests; general data privacy principles

On Freedom of Information (FOI) requests for research purposes and SWDAs who received cash incentives, the DSWD may disclose data relating to SWDAs, SPs and CSOs following the guidelines provided by E.O. No. 2, s. 2016.

The people's right to be informed on matters of public concern is recognized in this instance, especially when the SWDAs, SPs and CSOs implement social welfare and development programs which make use of public funds. For the sake of transparency and accountability, information on the SWDAs, SPs and CSOs, as juridical entities, and even related personal data, where necessary and proportional to the purpose of the request, may be disclosed.

We underscore the principle of proportionality under the DPA which requires that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.⁵ Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.⁶

We thus advise that any disclosure or publication of personal data should

⁴ Department of Social Welfare and Development, Guidelines on the Accreditation of Civil Society Organizations (CSOs) To Implement DSWD Programs Using DSWD Funds, DSWD Memorandum Circular No.13, Series of 2019 [DSWD MC 13, s.2019] (July 26, 2019).

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

⁶ Ibid.

only contain relevant information necessary to achieve the purpose of ensuring transparency and accountability. Keep in mind that any processing of sensitive personal information is prohibited unless allowed under the instances enumerated in Section 13 of the DPA.

Lawful basis for processing; Consent; Privacy Notice

As discussed above, the lawfulness of the processing of personal data is primarily based upon the mandate of the DSWD and its compliance to legal obligations. Hence, the consent of data subjects is not the most appropriate lawful basis for the given scenarios. Further, we wish to highlight that consent is only one of the various criteria for lawful processing and is not required in all instances.

But to assist the DSWD, we provide the following guidance for reference:

- Consent is freely given if the data subject has a genuine choice and control over whether to consent to the processing of personal data about and/or relating to him or her. It is not freely given if there is any element of pressure, intimidation, possibility of adverse consequences for refusal to give consent, or any other inability to exercise free will by the data subject.
- As to specificity, consent should be granular. Blanket consent is not sufficient. Personal information controllers (PICs) should present to the data subject a list of purposes and allow the data subject to select which purpose/s he or she consents to.
- Consent given can be withdrawn at any time. Should the data subject withdraw consent, PICs are obliged to cease the processing without undue delay.
- Where consent is withdrawn by the data subject, the same shall not affect the lawfulness of the processing before the withdrawal of such consent.
- PICs shall not obtain consent if the same is not appropriate and necessary in relation to the purpose of processing, and especially in instances where the PIC is already aware that such processing will continue despite the withdrawal of consent because of some other undisclosed lawful basis that can be relied on.

Finally, in keeping with the principle of transparency and upholding the right to be informed, DSWD should inform the data subjects or the personnel of the SWDAs, SPs and CSOs that their personal data will be

made publicly available pursuant to applicable laws and regulations.

This is made through a privacy notice which is a statement made to a data subject that describes how the PIC collects, uses, retains, and discloses personal information, the rights of a data subject and how these are exercised.⁷

This requirement is separate and distinct from having a lawful basis for processing and should not be confused with a consent form which is necessary only if consent is the basis for processing.

Finally, as to the sample privacy notice provided, we suggest that the same be modified given the discussion above.

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 See: National Privacy Commission, Data Subject Rights [NPC Advisory No. 2021 – 01], § 6 (c) (Jan. 29, 2021).

ADVISORY OPINION NO. 2021-025¹

21 July 2021



Re: **MANDATORY PSYCHIATRIC EVALUATION OF ALL
NATIONAL COUNCIL ON DISABILITY AFFAIRS PERSONNEL**

Dear 

We write in response to the request for guidance sent by the Civil Service Commission (CSC) in relation to the proposed mandatory psychiatric examination of all National Council on Disability Affairs (NCDA) personnel.

We note from the CSC letter that one NCDA personnel posted on the group chat of the NCDA two documents: 1) receiving letter for the Department of Health Secretary requesting for a psychiatric testing for all NCDA personnel, and 2) draft Memorandum of Agreement (MOA) with the National Center for Mental Health (NCMH).

We understand that the MOA includes a provision that an average of ten (10) personnel will be subject to psychiatric assessment and evaluation per week until all NCDA personnel has undergone it and that the psychiatric evaluation results will be given to the Executive Director.

In your memo to the Board Secretary and Officer-in-Charge, Finance and Administrative Division of the NCDA, copy furnished the CSC, you are invoking your right to doctor-patient confidentiality and constitutional rights if you will be forced to undergo psychiatric evaluation in the future.

We note also from the letter of the NCDA Executive Director to the Secretary of Health that the purpose of the psychiatric evaluation is to diagnose the mental, emotional, and behavioral

¹ Tags: sensitive personal information; health information; psychiatric evaluation of employees; criteria for lawful processing of sensitive personal information; consent.

attitude of the staff, analyze data and results of the assessment, and whenever necessary, develop a treatment plan and measure the progress of the plan.

We further note that the results of the psychiatric evaluation will be forwarded to the NCDA Executive Director rather than to the concerned NCDA personnel.

Sensitive personal information; health information; psychiatric evaluation of employees; lawful criteria for processing sensitive personal information by employers; consent

The Data Privacy Act of 2012² (DPA) considers an individual's health information as sensitive personal information.³ As such, the processing of the same, as a general rule, is prohibited unless the processing falls within the criteria for lawful processing enumerated under Section 13 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, 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. (Emphasis supplied)

In the above-quoted provisions as applied in this instance, consent may be the most appropriate lawful basis for the processing of the health information of the NCDA personnel. We wish to reiterate the definition of consent in Section 3 (b) of the DPA as follows:

“Consent of the data subject refers to 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.”

We also wish to clarify that the existence of the MOA with the NCMH does not vest the NCDA with a lawful basis for compelling its employees to undergo mandatory psychiatric examination and transmittal of the results thereof to the NCDA Executive Director, in relation to Section 13 (b) on processing that is provided for by law or Section 13 (e) on the processing for purposes of medical treatment carried out by a medical practitioner or treatment institution. These criteria may not be applicable in this scenario.

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 Id. § 3 (1) (2).

General data privacy principles; transparency; proportionality

We note from your letter that there was no prior consultation with the NCDA personnel regarding this personal data processing activity.

This may run contrary to the general data privacy principle of transparency which provides that a 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 (PIC), his or her rights as a data subject, and how these can be exercised.⁴

In addition, the principle of proportionality requires 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 means.⁵

If the NCDA is indeed concerned about the welfare of its personnel, particularly during this time of pandemic, it may still proceed with the proposed program of having them undergo psychiatric evaluation, but on a voluntary basis.

Moreover, instead of transmitting the results of the evaluation to the NCDA Executive Director, NCDA should consider asking for a certification from the NCMH that the said personnel have undergone psychiatric evaluation and are fit to work. With this, the NCDA can still achieve its purpose of ensuring employee wellness and work performance while upholding their privacy rights.

Finally, the NCMH, with whom the NCDA has a draft MOA, is also considered as a PIC under the DPA. Hence, the NCMH is likewise obliged to comply with the provisions of the DPA, which includes adherence to the general data privacy principles.

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.

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

⁵ Id. § 18 (c).

For your reference.

Very truly yours,

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

ADVISORY OPINION NO. 2021-026¹

21 July 2021

[REDACTED]

[REDACTED]

Re: **DATA PRIVACY IMPLICATIONS FOR FINANCIAL SERVICES INDUSTRY INITIATIVES ON DATA SHARING**

Dear [REDACTED]

We write in response to your letter received by the National Privacy Commission (NPC) which sought clarification on two proposed initiatives of the financial services industry on cybersecurity, specifically on data sharing.

We understand that the financial services industry has been shifting to digital financial and payment services in response to the COVID-19 pandemic. You disclosed further that cyberthreat actors continue to exploit the vulnerabilities of the Bangko Sentral ng Pilipinas (BSP) Supervised Financial Institutions (BSFIs) and their clients.

We further understand from your letter that the BSP's surveillance revealed that these cyber attacks and fraudulent schemes affect two or more financial institutions, such as banks and non-bank financial institutions such as e-money issuers, Virtual Asset Service Providers (VASPs) and remittance companies, simultaneously.

With this, the BSP, in consultation with industry associations, developed two key initiatives to prevent fraud incidents and uphold the customers' confidence in digital payment systems.

¹ Tags: lawful processing; sensitive personal information; legal claim; law; regulation; BSP; fraud investigation; fraud prevention; blacklists; fairness; lawfulness; accuracy; privacy impact assessment; data subject rights; limitations.

The first proposal is for a BSP regulatory issuance on data sharing among BSFIs. The said regulation would provide data sharing guiderails including definitions of permissible data gathering and sharing and the necessary controls to prevent any possible abuse in the data sharing arrangement. This will enable the open and transparent sharing of information among BSFIs to facilitate investigation and resolution of fraud incidents.

The second proposal is the establishment of a shared database of suspected and blacklisted accounts containing information on verified mule account holders such as customer name, case details, transaction details and online banking credentials, among others. BSFIs shall use the shared database in conducting Know-Your-Customer (KYC) procedures for new depositors/clients and in performing Enhanced Due Diligence (EDD) as part of the regular anti-money laundering (AML) monitoring for existing clients. This mechanism will prevent verified mule account holders to open accounts and perform financial transactions with BSFIs which would significantly enhance integrity in the financial system

You now ask whether the processing of sensitive personal information for the said proposals may fall under Section 13 (f) of the Data Privacy Act of 2012² (DPA) which allows processing of personal data for the protection of lawful rights and interests of natural or legal persons. You further ask on whether a court order is required under the said lawful basis or if a regulatory issuance by the BSP on fraud information sharing guidelines shall suffice.

Data sharing; lawful basis for processing; establishment, exercise, or defense of legal claims; sharing based on laws and regulations

The DPA allows the processing of sensitive personal information provided the requirements of the law are complied with and subject to strict adherence to the basic data privacy principles of transparency, legitimate purpose and proportionality.

Section 13 (f) of the DPA, which may be applicable to the current scenario, recognizes the processing of sensitive personal information when it is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or in the establishment, exercise of defense of legal claims, or when provided to government or public authority.³

In the case of BGM vs. IPP,⁴ the Commission had the opportunity to

clarify Section 13 (f) in this wise:

“x x x. Its requirement of compelling Complainant to produce a court order prior to the release of the requested information creates a high barrier that effectively impedes the rights vested by the DPA to the latter as a data subject.

Further, Respondent’s assertion that the information within its custody can only be disclosed upon data subject’s consent or on the basis of a lawful order is misplaced. x x x

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.”

This Commission in the same case went on further and held 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. 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. 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.

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

⁴ National Privacy Commission, BGM vs. IPP [NPC 19-653] (Dec. 17, 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 9 July 2021).

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 protection of the lawful rights and interests of the Complainant as contemplated by Section 13 (f) of the DPA.” (underscoring supplied)

Thus, the sharing of sensitive personal information for the establishment, exercise, or defense legal claims in relation to fraud investigations and fraud prevention may be allowed under Section 13 (f) of the DPA. The same does not require an existing court proceeding, and thus, such processing will not necessarily require a court order.

As we also discussed in Advisory Opinion No. 2021-017,⁵ requests for information from online platforms and financial intermediaries by government agencies may come in various forms, i.e., courts orders, subpoenas, officially issued orders, memoranda, letters, and other communication, among others, depending on several factors, such as the stage of the investigation or enforcement action as well as the powers of the particular agency, i.e., some may have subpoena powers and while others do not.⁶

For the general data privacy principle of legitimate purpose, the expectation is that all due process requirements have been complied with in relation to any request for personal data. Likewise, for proportionality, the same requires that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

We also wish to emphasize that once the proposed BSP regulatory issuance takes effect, the data sharing may then be based on such issuance, in relation to Section 13 (b) of the DPA which recognizes processing that is pursuant to existing laws and regulations.

Advisory Opinion Nos. 2020-050, 2020-039, 2019-041; credit card fraud; disclosure by online platforms, fintech, digital payment platforms, and telecommunications; sharing of bank transaction information for fraud investigations

⁵ National Privacy Commission, NPC Advisory Opinion No. 2021-017 (June 8, 2021).

⁶ Id.

We reiterate our previous pronouncements on the above captioned Advisory Opinions issued to the Credit Card Association of the Philippines in 2019 and 2020 and the Union Bank of the Philippines in 2020.

Essentially, fraud investigation may be considered as a legitimate interest under Section 12 (f), considering the legitimate interests test:

“First, it must be established that the investigation is strictly for purposes of resolving previously committed frauds and preventing possible frauds.

Second, only personal information which is necessary and proportionate to facilitate the fraud investigation may be processed pursuant to the said identified legitimate interest.

Lastly, it should be established that the fundamental rights and freedoms of data subjects are not overridden by the legitimate interests of the PIC. Hence, there should be minimal impact on the data subjects and in the exercise of their rights. To determine any potential risks, it must be assessed whether the data subjects had a reasonable expectation at the time and in the context of the collection of personal information that processing for fraud investigation purposes may take place.

Among the factors which may be considered in assessing the reasonableness of the processing are the relationship between the PIC and the data subject and the transparency of the PIC at the time of the collection of data. For a more comprehensive discussion on reasonable expectation, kindly refer to NPC Case 17-047 available at <https://www.privacy.gov.ph/wp-content/uploads/2020/10/CID-17-047-JV-v.-JR-Decision-PSD-10Aug2020.pdf>.”⁷

Hence, the disclosure of personal information, i.e., name, address, delivery address, email address, and mobile or other contact number, by online merchants, financial technology companies, digital payment platforms and telecommunications entities to credit card issuers or banks, or bank transaction details from one bank to another affected bank or electronic money issuer, for purposes of fraud investigation is allowed under Section 12 (f) of the DPA.

As to the disclosure of such personal information to law enforcement, regulatory, or investigative agencies, the same may find basis under

Section 12 (c), where processing is necessary for compliance with a legal obligation, and/or Section 12 (e) on processing that is necessary to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.

We likewise referred to the provisions of the Philippine Credit Card Industry Regulation Law which recognizes several instances where credit card issuers may disclose data of cardholders.

Shared database of suspected and blacklisted accounts; fair and lawful processing; privacy impact assessment; data subject rights; limitations

Blacklisting was discussed in our Advisory Opinion No. 2017-63,⁸ to wit:

“As a generic approach, blacklists are databases that consist of collected specific information relating to a specific group of persons, which may generally imply adverse and prejudicial effects for the individuals included thereon and which may discriminate against a group of people by barring them access to a specific service or harming their reputation.

That said, blacklisting constitutes processing of personal data and is therefore subject to the general data privacy principles set out in the Data Privacy Act of 2012 (DPA). Thus, the law mandates that a data subject must be properly informed of the nature, purpose and extent of the processing of his or her personal data.

Further, it is mandatory for an organization to clearly establish procedures that allow data subjects to exercise their right to access, rectification, erasure or blocking.”

While we recognize that having a shared database for KYC, EDD, and AML purposes may enhance the integrity of the financial system, we also note that this may have significant legal effects on the rights and freedoms of data subjects included in the database.

Hence, there is a need to ensure that personal and sensitive personal information (collectively, personal data) is processed fairly and lawfully.⁹

⁷ National Privacy Commission, NPC Advisory Opinion No. 2020-039 (Oct. 30, 2020) citing NPC Case No. 17-047.

⁸ National Privacy Commission, NPC Advisory Opinion No. 2017-063 (Oct. 9, 2017) citing Article 29 of Directive 95/46/EC “Working document on Blacklists”, Adopted on 3 October 2002, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp65_en.pdf

In this particular context, we emphasize that personal data in such database must be accurate, relevant and, kept up to date – inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.¹⁰

We likewise recommend the conduct of a privacy impact assessment (PIA) to identify, assess, evaluate, and manage the risks represented by the processing of personal data in the shared database.¹¹ Guidance for conducting PIAs may be found in our website at this link: https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/NPC_AdvisoryNo.2017-03.pdf.

Finally, we remind the financial services industry that data subjects should be provided mechanism to exercise their rights. Needless to say, these rights are not absolute and may be duly limited 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.¹²

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

⁹Data Privacy Act of 2012, § 11 (b).

¹⁰Id. § 11 (c).

¹¹National Privacy Commission, Guidelines on Privacy Impact Assessments [NPC Advisory No. 2017-03] (July 31, 2017).

¹²National Privacy Commission, Data Subject Rights [NPC Advisory No. 2021-01] (Jan. 29, 2021).

ADVISORY OPINION NO. 2021-027¹



Re: **ACCESS TO DOCUMENTS BY SAN MIGUEL AEROCITY INC.
PURSUANT TO ITS LEGISLATIVE FRANCHISE**

Dear 

We write in response to your letter received by the National Privacy Commission (NPC) which sought clarification on certain data privacy issues relating to the implementation of the New Manila International Airport (NMIA) project.

We understand that San Miguel Aerocity, Inc. (SMAI) was granted a legislative franchise under Republic Act (RA) No. 115062 to construct, operate, and maintain the NMIA, an Airport City adjacent to the NMIA, and rights of way that will provide ingress and egress from the airport and the Airport City (collectively, the Projects).

We understand further that Section 15 of RA No. 11506 delegated to SMAI the power of eminent domain. Corollary to the said power, there are obligations imposed under RA No. 10752² or the Right-of-Way Act³ which require access to copies of certain documents relating to the properties which may be acquired by SMAI through purchase, negotiation, expropriation, or condemnation proceedings. These documents are held by various government agencies and may contain personal and/or sensitive personal information (collectively, personal data).

You now ask whether SMAI may be provided with these documents and process the personal data contained therein pursuant to Sections 5 (c) and (d) and Section 22 (b) of the Implementing Rules and Regulations⁴ (IRR) of the Data Privacy Act of 2012⁵ (DPA).

¹ Tags: legislative franchise; eminent domain; right of way; scope; special cases; lawful criteria for processing; legal obligation; laws and regulations; legal claims.

² An Act Granting San Miguel Aerocity Inc. A Franchise To Construct, Develop, Establish, Operate And Maintain A Domestic And International Airport In The Municipality Of Bulakan, Province Of Bulacan, And To Construct, Develop, Establish, Operate, And Maintain An Adjacent Airport City, Republic Act No. 11506 (2020)

³ An Act Facilitating The Acquisition Of Right-Of-Way Site Or Location For National Government Infrastructure Projects [The Right-of-Way Act], Republic Act No. 10752 (2016)

Scope of the DPA; special cases; lawful basis for processing; legal obligation; laws and regulations

We wish to clarify that the DPA only applies to the processing of personal data of natural persons and not information of juridical entities recognized under the law, such as corporations, associations, and partnerships.

Thus, if the requested copies of titles, tax declarations, business permits, tax identification numbers, certifications, registrations, clearances, and other documents pertain to a juridical person, the DPA does not apply.

As to those which pertain to natural persons, the processing of the same should have a lawful basis under the DPA. As mentioned in your letter, you posit that SMAI's processing is anchored on Sections 5 (c) and (d) and Section 22 (b) of the DPA's IRR, which refers to information necessary for research, for carrying out functions as a public authority, and processing that is provided for by existing laws and regulations, respectively. Moreover, as specified in your letter, the SMAI's right and authority over the requested documents refer to the exercise of its right of eminent domain for a legitimate purpose as specified under its franchise as provided for by Congress, in order to undertake a national government infrastructure project.

While we recognize SMAI's personal data processing activities based on its legislative franchise, the same is not processing under a special case, but rather is more appropriately based on Sections 12 (c) and/or Section 13 (b) and (f) of the DPA, depending on the type of personal data being processed, 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:

X X X

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

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

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).

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: 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

(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.” (underscoring supplied)

General data protection principles; proportionality; safeguards

In Advisory Opinion No. 2020-036,⁶ we discussed a similar concern of the National Grid Corporation of the Philippines (NGCP) as to their request to secure land documents, under the custody of local government units:

“x x x To further implement the above mandates, the NGCP was also granted the right of eminent domain.”

X X X

Given the foregoing mandates of NGCP under its franchise with the government, it is inevitable that some private properties may be affected by the transmission projects. It is thus necessary for NGCP to identify the current owners and possessors of the affected properties for its acquisition.

X X X

While the requested documents, such as the certificates of title

and tax declarations, are the best proof of ownership and sufficient basis for inferring possession over a parcel of land, respectively, which means that the said documents shall significantly facilitate the identification of the current owners and possessors of the affected properties, there is a need to evaluate whether releasing actual copies of the same is proportional to the purpose of identification of owners/possessors.

NGCP should consider whether it may be reasonable and acceptable for the respective Register of Deeds, the Assessors' Offices and the city or municipal planning offices of the affected LGUs to provide certifications/lists of names and contact details of the owners/possessors per official records instead, without necessarily releasing copies of the land documents.

This is in adherence to the principle of proportionality which requires that the processing, which includes disclosure, of personal information must be limited only to the extent that is necessary to achieve the stated purpose and that there are no other effective means to achieve the same.

Nevertheless, we wish to emphasize that access to copies of the requested land documents may only be allowed if NGCP has duly justified and substantiated its lawful interest over the subject properties and that denial of said request shall cause NGCP's failure to comply with its legal obligations under its franchise with the Philippine government. Such determination and assessment should be duly documented. And in this scenario, the respective Registry of Deeds, the Assessors' Offices and the city or municipal planning offices may provide the requested documents to NGCP, relying on such evaluation vis-à-vis the NGCP's mandate.

We further reiterate that compliance with legal obligations and with provisions of other existing laws and regulations, as well as processing of sensitive personal information for the establishment or exercise of legal claims may be validly done and are not necessarily violations of the DPA. The provisions of applicable laws and regulations should be read together and harmonized with the DPA. x x x.” (underscoring supplied)

⁶ National Privacy Commission, NPC Advisory Opinion No. 2020-036 (Sept. 8, 2020).

In a similar vein, there should be an evaluation if indeed the long list of documents that SMAI had identified are all relevant and necessary for its compliance with its various legal obligations, its establishment, exercise, or defense of legal claims, or as may be required under the RA No. 11506, taking into consideration that personal data shall be processed only if the purpose could not reasonably be fulfilled by other means.

Considering, however, that the grant of the power to expropriate private lands for purposes of acquiring and developing the sites for the Projects necessarily results in the obligations imposed by the Right-of-Way Act on implementing agencies now extending to SMAI, it is now said statutorily obliged to undertake the following:

1. Under Section 7 of the Right-of-Way Act, the determination of –
 - a. The classification and use for which the property is suited;
 - b. The development cost for improving the land,
 - c. The value declared by the owners;
 - d. The current selling price of similar lands in the vicinity;
 - e. The reasonable disturbance compensation for the removal and demolition of certain improvements on the land and for the value of improvements thereon;
 - f. The size, shape or location, tax declaration and zonal valuation of the land;
 - g. The price of the land as manifested in the ocular findings, oral as well as documentary evidence presented; and,
 - h. Such facts and events as to enable the affected property owners to have sufficient funds to acquire similarly situated lands of approximate areas as those required from them by the government, and thereby rehabilitate themselves as early as possible.
2. Under Sections 4, 5 and 6 of the Right-of-Way Act, the determination of –
 - a. The nature of and a detailed background on the properties that will be affected by a project's alignment (for instance, whether such properties are "patent lands;" whether such properties are alienable and disposable; and whether such properties are currently the subject of litigation);
 - b. The identities of the current occupants or tenants of the aforesaid properties;

- c. The identities of the owners, possessors, or claimants of the properties that will be affected by a project’s alignment, and whether the said persons are alive or dead or may be found;
- d. The aforesaid persons’ marital status; the identity of their heirs; and the status of their estates if the owners or occupants are already deceased; and,
- e. The payment of taxes and assessments on the properties or on the estate if the owner or occupant is already deceased.

From your letter, it was explained that the following documents are required to comply with the abovementioned statutory obligations and that these documents are the same ones required by agencies that customarily implement national infrastructure projects such the Department of Public Works and Highways and the Department of Transportation:

Government Agencies	Documents
Register of Deeds	<ul style="list-style-type: none"> • E-copy of title, including title trace-back up to Original Certificate of Title • Certification (if the office copy is on file or not for administrative/judicial reconstitution purposes)
Provincial or Municipal or City Assessor’s Office	<ul style="list-style-type: none"> • Certified true copy of tax declaration, including trace-back up to 30 years • Certificate of No Improvement • Tax map • Tax map rolls
Provincial or Municipal or City Treasurer’s Office	<ul style="list-style-type: none"> • Realty Tax Clearance • RPT assessments
Business Permits and Licensing Office	<ul style="list-style-type: none"> • Assessment/s of Business Permit
Civil Registrar’s Office	<ul style="list-style-type: none"> • Certificate of No Marriage (CENOMAR) • Marriage Certificate • Birth Certificate • Death Certificate

Department of Environment and Natural Resources and/or Bureau of Lands	<ul style="list-style-type: none"> • Cadastral map • Certification (alienable and disposable) • Lot Data Computation • Approved Survey Plan with technical description
Community Environment and Natural Resources Office	<ul style="list-style-type: none"> • Certification (lot status)
Land Registration Authority	<ul style="list-style-type: none"> • Certification (lot status)
Bureau of Internal Revenue	<ul style="list-style-type: none"> • Schedule of Recommended Zonal Value • Certificate Authorizing Registration • Taxpayer Identification Number • Certificate of Registration
Municipal Trial Court and/or Regional Trial Court	<ul style="list-style-type: none"> • Certification (No pending Case) • Decree of Annulment/Divorce/Legal Separation/Separation of properties/Pre-nuptial agreement • Copies of notarized documents
Department of Agrarian Reform	<ul style="list-style-type: none"> • Clearance • List of Registered Tenants • Certificate of Non-tenancy
Barangay	<ul style="list-style-type: none"> • Certification (Actual Possessor) • BARC Certification
Philippine Statistics Authority	<ul style="list-style-type: none"> • Certificate of No Marriage (CENOMAR) • Marriage Certificate • Birth Certificate • Death Certificate
National Archives Office	<ul style="list-style-type: none"> • Copies of notarized documents • Certification (if no record on file)
Securities and Exchange Commission and/or Department of Trade and Industry	<ul style="list-style-type: none"> • Certificate of Registration • Articles of Incorporation including amendments • By-laws including amendments • General information Sheet

Considering that all these documents being requested by SMAI are required to acquire land or expropriate the same under the Right-of-Way Act, and there is legitimate purpose for processing the same, it goes without saying that these documents are necessary and relevant in order for SMAI to be able to fulfill its mandate under the franchise provided by Congress. The DPA cannot be used by other government agencies to avoid fulfilling its obligation to provide SMAI the documents requested.

Finally, it is expected that SMAI shall ensure the implementation of organizational, physical, and technical security measures when it receives the requested documents and information and have mechanisms in place to enable the free exercise of data subject rights, where appropriate. We recommend that SMAI create its Privacy Manual or update the same

accordingly, taking into consideration the above discussions.

We are mindful of the importance of the Projects and the positive impact it will have. The DPA is not meant to hinder legitimate proceedings. Rather, the law promotes fair, secure, and lawful processing of personal data.

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. 2021-28¹

16 July 2021



Re: **DISCLOSURE OF PERSONAL INFORMATION OF TENANTS
BY A CONDOMINIUM CORPORATION TO THE BUREAU OF
INTERNAL REVENUE**

Dear 

We write in response to your email received by the National Privacy Commission (NPC) which sought clarification on whether a condominium corporation may validly refuse the request of the Bureau of Internal Revenue (BIR) to provide the list of tenants of the condominium.

In your letter, you disclosed that you are counsels for Andrea North Condominium Corporation (ANCC), incorporated to manage, administer, and operate the condominium project (Project). You further disclosed that as part of its duties, ANCC requires its unit owners to provide details about its tenants which includes personal information, government-issued identification (IDs) and contracts of lease. The purpose of such requirement is to validate the tenant-occupant's authority over the condominium unit/property.

We understand that ANCC recently received a letter from a BIR Revenue District Officer (RDO) requesting for a list of tenants of the Project. The BIR RDO also included in the letter a form, to be distributed to and filled out by all unit owners asking them to submit documents such as contracts to sell, statements of account/schedule of amortization, official receipts issued by the developer/seller for payments made and deeds of sale. The requested information will be used for BIR's Tax Verification Drive to enhance tax compliance and boost its tax collection efforts.

¹ Tags: Bureau of Internal Revenue; scope of the DPA; special cases.

You now ask for confirmation if ANCC's position to decline BIR RDO's request is appropriate. ANCC believes that providing the requested documents and information will be violative of the unit owners' and tenants' data privacy rights under the Data Privacy Act of 2012² (DPA) since the information were collected by ANCC for validation purposes only.

Scope of the DPA; special cases under the DPA

The DPA and its Implementing Rules and Regulations (IRR) provide for a list of specified information which do not fall within the scope of the law.³ In particular, information necessary to carry out functions of a public authority are considered special cases under the DPA, 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 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.”⁴ (Underscoring supplied)

The above exemption must be strictly construed. For the exemption to apply, the following are considered:

- The information is necessary in order to carry out the law enforcement or regulatory function of a public authority;
- The processing is for the fulfillment of a constitutional or statutory mandate;
- There is strict adherence to all due process requirements;
- Applies only to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned; and
- Only the specified information falls outside the scope of the DPA. The public authority, considered as a personal information controller under the DPA, must still comply with the other requirements of the DPA such as the implementation of reasonable and appropriate physical, organizational and technical security measures, uphold the rights of data subjects and adhere to the data privacy principles of transparency, legitimate purpose, and proportionality.⁵

BIR mandate under the Tax Code, as amended; powers of the BIR Commissioner

We reiterate the discussions in NPC Advisory Opinion No. 2020-015 that the BIR's processing of personal data pursuant to its mandate falls under the special cases of the DPA.

The BIR is tasked to, among others, ensure compliance with the National Internal Revenue Code (NIRC), as amended, and other relevant tax laws and regulations. The DPA recognizes the authority of the BIR Commissioner under Section 5 of the NIRC to obtain information, and to summon, examine, and take testimony of persons in determining the liability of any person for any internal revenue tax or in collecting such liability or in evaluating tax compliance.

We likewise asked for clarification from the BIR National Office as to

² 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).

³ Id. § 4 (e) (2012).

⁴ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (d) (2016).

the propriety of such letter request from a BIR RDO and received the following reply:

“Please be advised that an “access to records letter” such as the one mentioned in your letter is authorized under Section 5(B) of the National Internal Revenue Code (NIRC) of 1997 as amended [Power of the Commissioner to Obtain Information, etc.].

Lastly, said letter being a mere request, there is no need yet for the issuance of a subpoena duces tecum (SDT). However, in the event that the condominium corporation fails to comply despite notices, the district office may request for the issuance of a SDT to compel compliance. x x x.”

Hence, ANCC may provide the information requested by the BIR RDO pursuant to the agency’s mandate. Submission of the same will not necessarily be violative of data privacy rights, given that the BIR has a lawful basis for requesting such information and has followed the appropriate processes for this Tax Verification Drive activity.

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.

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 See: National Privacy Commission, NPC Advisory Opinion No. 2019-022 (07 May 2019) and NPC Advisory Opinion No. 2020-015 (24 Feb 2020).

ADVISORY OPINION NO. 2021-029¹

30 July 2021



Re: **PROCESSING OF PERSONAL DATA CONTAINED IN ABANDONED SERVERS OR COMPUTERS**

Dear 

We write in response to your request for guidance regarding a situation wherein an office lessee of Eton Properties Philippines, Inc. (Eton for brevity) has defaulted and abandoned the leased building premises.

We understand that Eton will soon be taking possession of all the items that the lessee had abandoned inside its BPO building project. One of these items is the lessee's data server which may contain personal and sensitive personal information (collectively, personal data), such as its customer database. You likewise mentioned the full extent of the contents of the server is not known as of yet.

As such, you have raised the following points for clarification:

1. Are there any guidelines issued by the National Privacy Commission (NPC) as to how to handle this situation;
2. Since these are abandoned properties, can the data be wiped, and the hardware re-used for other business purposes? Eton can archive the data, if necessary and affordable;
3. Can the lessee still require Eton to return their data on their server?
4. In case Eton ends up repossessing other workstations/computers, will these be treated the same way as the data servers; and
5. Recommendations to ensure that there are no data privacy-related issues in the future.

¹ Tags: criteria for lawful processing of personal and sensitive personal information; personal information controller; accountability; retention; compliance.

Scope of the Data Privacy Act of 2012; criteria for lawful processing of personal data

The Data Privacy Act of 2012² (DPA) applies to the processing of personal data and to any natural and juridical person involved in the processing within and outside the Philippines.

Under the DPA, processing refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.³

The processing of personal data which may be contained in the server and/or other workstations/computers of the lessees, which includes erasing and archiving, shall be allowed only upon compliance with the requirements of the law and adherence to the general data privacy principles of transparency, legitimate purpose, and proportionality.⁴

The various criteria for lawful processing of personal and sensitive personal information by personal information controllers (PICs) are provided under Sections 12 and 13 of the DPA, respectively.

Section 12 enumerates the various criteria for processing personal information, such as processing that is necessary for compliance with a legal obligation,⁵ or necessary for the purposes of the legitimate interests pursued by the PIC or by a third party or parties to whom the data is disclose,⁶ among others.

Note, however, that if the database contains sensitive personal information, the processing thereof is prohibited, except for certain instances provided under Section 13 such as when the processing is provided for by existing laws and regulations,⁷ or 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.⁸

Therefore, Eton's proposed actions as to the further processing of the personal data of its lessee shall be governed by the any of the lawful bases for processing under the DPA.

Appropriating abandoned properties; erasure or archiving of personal data of the lessee

Although the lessee has abandoned its servers, workstations, and computers in the leased premises, the same does not give the lessor the right to automatically appropriate the same and the contents thereof to satisfy the unpaid rentals or recover the leasing revenue loss it has incurred. The treatment of the abandoned properties of the lessee would then depend upon the stipulations in the lease agreement and the orders or judgement from a competent court.

To reiterate, wiping or archiving of personal data falls squarely on the above definition of processing and the appropriation of the lessee's abandoned properties by Eton in order to reuse them may likely result to processing personal data of which Eton may not be authorized.

Hence, in the meantime, it is best that Eton refrain from appropriating the abandoned properties and the contents thereof. It is recommended that Eton safekeep the same while waiting for the results of the pending case.

Duties and responsibilities of PICs; accountability; five pillars of compliance

Moreover, we wish to note that under the principle of accountability, each PIC is responsible for personal information under its control or custody.⁹

If Eton, based on the lease agreement and/or the orders or judgement from a competent court, takes control over the abandoned servers, workstations, and computers, it may be deemed to be a PIC as well and should be cognizant of the duties, responsibilities, and risks associated with having custody of personal data. In CID Case No. 18-E-040,¹⁰ the Commission elaborated on the accountability of the PIC:

“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.

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 Data Privacy Act of 2012, § 3 (j).

⁴ Id. § 11.

⁵ Id. § 12 (c).

⁶ Id. § 12 (f).

⁷ Id. § 13 (b).

⁸ Id. § 13 (f).

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.”

While the servers, workstations, and computers are properties of the lessee, the personal data contained therein cannot be treated in the same manner as with any other property given the provisions of the DPA. Since the personal data was collected by a different PIC for purposes different than that of Eton’s, any further personal data processing by Eton should be supported by lawful criterion specific to the personal data and separate from whatever action it may take against its lessee. Likewise, should Eton decide to process the personal data, it is still required to notify the data subjects regardless of the lawful basis that it may eventually rely on.

As to whether the lessee can still require Eton to return the personal data from the abandoned properties even if the latter takes control over the abandoned properties, this will depend upon the existing policies of Eton as to retention of personal data, taking into account as well any applicable provisions of the lease agreement and/or orders of a competent court. We emphasize that personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.¹¹

Finally, we wish to clarify that one can never be assured that there will be no data privacy- or DPA-related issues in the future as these may not be completely avoided. Nevertheless, we have always reminded PICs to follow the five pillars of compliance as this serves as the basic steps towards complying with the DPA and issuances of the NPC.

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. We are not privy to the terms and conditions of the lease agreement between Eton and its lessee and the same has not been reviewed for purposes of this opinion. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

⁹ Data Privacy Act of 2012, § 21.

¹⁰ National Privacy Commission, CID Case No. 18-E-040, *Rala v. Burguillos, et al.* (May 12, 2020).

¹¹ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 19 (e) (3) (2016).

For your reference.

Very truly yours,

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

ADVISORY OPINION NO. 2021-030¹

30 July 2021



Re: **PUBLICATION OF COPYRIGHT REGISTRATIONS**

Dear 

We write in response to your request received by the National Privacy Commission (NPC) asking for guidance on the publication of copyright registrations.

We understand that the Bureau of Copyright and Other Related Rights (Bureau) of the Intellectual Property Office of the Philippines (IPOPHL) plans to publish a list of copyright registrations received and processed by the Bureau. The list will contain copyright registrations by category of copyrighted work and four data elements: (1) registration number, (2) name of copyright owner, (3) title of the work, and (4) date of registration.

We understand that the new form of the Bureau contains the standard data privacy notification and consent adopted by IPOPHL.

We understand further that the purposes of publication are the following:

1. To operate as notice to the public of the fact of registration of a copyrighted work;
2. To allow aggrieved and/or contesting parties to put forward a challenge to erroneously registered works because the registrant is not the true owner, or the work is not an original creative expression of the registrant; and
3. To encourage the registration of more works.

¹ Tags: criteria for lawful processing; legal obligation; mandate; copyright; general data privacy principles.

² An Act Prescribing the Intellectual Property Code and Establishing the Intellectual Property Office, providing for its Powers and Functions, and for Other Purposes [Intellectual Property Code of the Philippines], Republic Act No. 8293 (1997).

We understand finally that the IPOPHL relies on Section 182 of RA No. 8293, also known as the Intellectual Property Code of the Philippines² mandating the publication in the IPOPHL Gazette of the fact of assignment, transfer, and exclusive licensing of copyright, which mandate extends to copyright registration by way of necessary implication.

Criteria for lawful processing of personal data; legal obligation; mandate

The Data Privacy Act of 2012³ (DPA) applies to the processing of personal and sensitive personal information (collectively, personal data) and to any natural and juridical person involved in the processing within and outside the Philippines.

Under the law, personal data processing may be based any of the various criteria for lawful processing provided under Sections 12 and 13 of the DPA, respectively.

Particularly applicable for IPOPHL's proposed processing is Section 12 (c) of the DPA which recognizes processing that is necessary for compliance with a legal obligation and/or Section 12 (e) which allows processing for the fulfillment of the functions of a public authority which necessarily includes the processing of personal data for the fulfillment of its mandate. We assume in this instance that the registration number pertains to the copyrighted work.

In this scenario, the IPOPHL posits that the basis for the publication of copyright registration is by virtue of Section 182 of the Intellectual Property Code of the Philippines, by way of necessary implication:

“SECTION 182. Filing of Assignment or License. - An assignment or exclusive license may be filed in duplicate with the National Library upon payment of the prescribed fee for registration in books and records kept for the purpose. Upon recording, a copy of the instrument shall be returned to the sender with a notation of the fact of record. Notice of the record shall be published in the IPO Gazette.”

We defer to the IPOPHL's authority on the proper interpretation of the above provision as to whether the mandate extends to copyright registration by way of necessary implication. As mentioned in the IPOPHL's letter, the above provision is applicable since there is nothing to amend, assign, transfer, or grant exclusive license on IPOPHL's records if the same has not been first registered.

Nevertheless, other provisions of the Intellectual Property Code of the Philippines support the publication of copyright registration, to wit:

“SECTION 2. Declaration of State Policy. - The State recognizes that an effective intellectual and industrial property system is vital to the development of domestic and creative activity, facilitates transfer of technology, attracts foreign investments, and ensures market access for our products. It shall protect and secure the exclusive rights of scientists, inventors, artists and other gifted citizens to their intellectual property and creations, particularly when beneficial to the people, for such periods as provided in this Act.

The use of intellectual property bears a social function. To this end, the State shall promote the diffusion of knowledge and information for the promotion of national development and progress and the common good.

It is also the policy of the State to streamline administrative procedures of registering patents, trademarks and copyright, to liberalize the registration on the transfer of technology, and to enhance the enforcement of intellectual property rights in the Philippines.”⁴

The publication of copyright registration to inform the public of such fact may be considered as lawful processing under the DPA as authorized by virtue of law or regulation.

Adherence to the general data privacy principles; transparency; privacy notice; data subject rights

Nevertheless, even if the processing of personal data has a lawful basis under the DPA, the same must still adhere to the other general data privacy principles, specifically in this case, the principle of transparency.

We recall that your letter mentioned that the new form of the Bureau contains the standard data privacy notification and consent adopted by the IPOPHL.

We wish to clarify that since the lawful basis of the IPOPHL in the processing of copyright registrations is its mandate, there is no need to obtain consent of the data subject for such processing. The standard data privacy notification, which we assume to be the privacy notice, should already suffice for this purpose.

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).

Kindly refer to Section 16 of the DPA and NPC Advisory No. 2021 – 01 on Data Subject Rights (available at this link: <https://www.privacy.gov.ph/wp-content/uploads/2021/02/NPC-Advisory-2021-01-FINAL.pdf>) for a discussion of privacy notices vis-à-vis transparency and the data subject right to be informed.

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. We are not privy to the contents of the IPOPHL form reflecting the standard data privacy notification and consent, and the same was not reviewed for purposes of this opinion. 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

⁴ Intellectual Property Code of the Philippines, § 2.

ADVISORY OPINION NO. 2021-031¹

5 August 2021



**Re: PROCESSING FOR DUE DILIGENCE, QUALITY
CONTROL, AND COMPLIANCE CHECKS PURSUANT TO THE
REQUIREMENTS OF THE GOVERNMENT PROCUREMENT
REFORM ACT**

Dear 

We write in response to your request received by the National Privacy Commission (NPC) asking for guidance on the propriety of requiring Private Security Agencies (PSA) declared as lowest bidder to submit the latest copy of their Monthly Disposition Reports (MDR) submitted to the PNP Supervising Office for Security and Investigation Agencies (PNP SOSIA) and the PNP Firearms and Explosives Office (FEO) Juridical Firearms License.

We understand that this requirement is pursuant to the conduct of Post Qualification Bid (PQB) and Technical Inspection and Acceptance (TIA) processes of the Civil Aviation Authority of the Philippines (CAAP) Security and Intelligence Service (CSIS) implementing the requirements of Republic Act (RA) No. 9184 also known as the Government Procurement Reform Act² (GPRA) and its Implementing Rules and Regulations (IRR).

We understand further that an MDR is a report indicating the names of the PSA's guards assigned to its clients and an updated summary of total number of its employed/deployed guards. On the other hand, a PNP FEO Juridical Firearms License is a document issued to PSAs by the PNP FEO that indicates the list of firearms and its specifications (calibre type, make, model and serial number), registration, and authorized ownership.

¹ Tags: criteria for lawful processing; legal obligation; mandate; copyright; general data privacy principles.

² An Act Providing For The Modernization, Standardization, And Regulation Of The Procurement Activities Of The Government And For Other Purposes. [Government Procurement Reform Act], Republic Act No. 9184 (2002).

Finally, we understand that the CSIS is requiring the aforementioned documents to determine the following:

1. Whether security guards deployed in CAAP airports and facilities are duly licensed and included in the MDRs submitted to the PNP SOSIA; and
2. Whether the personal protection equipment (firearm) they carry are authentic and duly registered and licensed by PNP FEO.

Scope of the Data Privacy Act; criteria for lawful processing of personal data; legal obligation

The Data Privacy Act of 2012³ (DPA) applies to the processing of personal information,⁴ sensitive personal information,⁵ and privileged information⁶ (collectively, personal data) of natural persons by the government and private entities and individuals, within and outside the Philippines.

We would like to highlight that while an MDR involves personal data protected under the DPA, a PNP FEO Juridical Firearms License is issued to juridical entities. We wish to clarify that the DPA only applies to the processing of personal data of natural persons and not information of juridical entities recognized under the law, such as corporations, associations, and partnerships.⁷ Thus, the DPA does not apply to the processing of information which pertains to a license issued to a juridical person.

Nevertheless, the processing of personal data in the MDR should have a lawful basis under the DPA. Section 12 and 13 of the DPA provides for criteria in processing personal data. Particularly in your case, the following provision may apply, viz:

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], (2012).

⁴ Id. § 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.

⁵ Id. § 3 (I): 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.

⁶ Id. § 3 (k) Privileged information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

⁷ National Privacy Commission, NPC Advisory Opinion No. 2021-027 (July 2021).

“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

(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: 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.”

On whether the CSIS may require PSAs to submit their latest MDRs without violating the DPA, the IRR of the GPRA is highly instructive. Section 34.3, Rule X of the same provides, to wit:

“RULE X – POST-QUALIFICATION

Section 34. Objective and Process of Post-Qualification

x x x

34.3 The post-qualification shall verify, validate, and ascertain all statements made and documents submitted by the bidder with the Lowest Calculated Bid/Highest Rated Bid, using non-discretionary criteria, as stated in the Bidding Documents. These criteria shall consider, but shall not be limited to, the following:

a) Legal Requirements. **To verify, validate, and ascertain licenses, certificates, permits, and agreements submitted by the bidder,** and the fact that it is not included in any “blacklist” as provided in Section 25.3 of this IRR. For this purpose, the GPPB shall maintain a consolidated file of all “blacklisted” suppliers, contractors, and consultants. x x x”

Considering that verification of legal requirements is part of the Post Qualification process in government procurement, the same is recognized as a legitimate purpose for processing personal data. It goes without saying that the processing of the MDR is in compliance with a legal obligation under current procurement laws and/or necessary for the fulfillment of the mandate of the CAAP. Thus, CAAP may validly require a PSA to submit the latest copy of its MDR as a post qualification requirement without violating the DPA.

Lastly, CAAP, as a personal information controller, is required to adhere to the general data privacy principles, implement reasonable and appropriate safeguards to protect personal data collected from the PSAs against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing, and uphold data subject rights.

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. 2021-032¹

9 August 2021



Re: **DISCLOSURE OF PHOTOGRAPHS OF ACCUSED IN CRIMINAL CASES**

Dear 

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) to provide guidance on the legality of obtaining photographs of accused individuals taking into consideration the provisions of the Data Privacy Act of 2012² (DPA).

From your letter, we understand that you are a party-in-interest and the counsel of the family of the victim in a murder case in 2018. The accused in the criminal case are allegedly members of the Philippine National Police (PNP) who were charged for two counts of murder. A warrant of arrest had been issued in October 2019 against the twenty (20) accused police officers, as evidenced by your attachment.

We understand further that despite the issuance of the warrant of arrest, you have not seen nor felt an earnest effort on the part of the police to locate, arrest and detain the remaining sixteen (16) accused who are still at large. You are now constrained to actively pursue the remaining accused and bring them to justice using other lawful means. We understand that you requested from the PNP the high-resolution photographs of the accused, but the latter refused to grant the request on the ground that photographs are protected under the DPA.

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

¹ Tags: social welfare and development; fulfillment of mandate of public authority; freedom of information; privacy notice.

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).

1. Whether or not the photographs submitted by the accused police officers to the PNP pursuant to their application for admission or employment constitute personal information or sensitive personal information as to come within the coverage and protection of the DPA considering the particular circumstances of the accused police officers in relation to the commission of the crimes and their current status as fugitives from the law;
2. Whether or not the submission of their photographs as part of their application for admission or employment with the PNP constitutes consent that is “freely given” as contemplated under the DPA; and
3. Whether or not the submission of their photographs as part of their application for admission or employment with the PNP constitutes compulsion, as to vitiate consent, under the admission or employment processes or procedures of the PNP.

Photographs as personal and sensitive personal information

Under the DPA, 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.³ In addition, the law provides for an exclusive list of information that are considered as sensitive personal information which includes, among others, information about any proceeding for any offense committed or alleged to have been committed by the individual.⁴

Thus, images of an individual generally fall under this category as they may reasonably or directly ascertain the identity of the data subject. However, considering the peculiar circumstances of this case where the photographs sought are connected to the crime alleged to have been committed, then the photographs of the accused may be considered as sensitive personal information. Either way, these photographs are indeed under the coverage of the DPA.

Nevertheless, the law does not absolutely prohibit the disclosure of personal information or sensitive personal information. Sections 12 and 13

of the DPA provide the criteria where processing of personal information and sensitive personal information, respectively, are allowed.

Disclosure of photographs allowed under Section 13 of the DPA

Under the DPA, 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.⁵ As applied in the instant case, we may consider the photographs of the accused as sensitive personal information, the lawful criteria for processing of which is found under Section 13 of the law.

Particularly, the case at hand may find legal ground under Section 13 (f) which provides: “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.”

While jurisprudence has settled that “the interest of the private complainant is limited only to the civil liability arising from the crime,”⁶ it is still evident that there exists a valid legal claim by the bereaved family of the victim. In order for the civil liability to arise, the crime should be judicially tried, and the accused convicted. Bringing the remaining accused who are still at large to justice is within the purview of the abovementioned Section 13 as an exercise of a valid legal claim as well as the protection of lawful rights and interests in a court proceeding.

As to the other questions on the submission of photographs as part of an application for admission or employment with the PNP, the lawful basis for the processing of the same is not consent. These photographs are most probably required by the PNP based on applicable laws and regulations of the Civil Service Commission on recruitment, selection, and placement.

³ Data Privacy Act of 2012, § 3 (g).

⁴ Id. § 3 (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.

⁵ Data Privacy Act of 2012, § 11.

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. 2021-033¹

31 August 2021



Re: **INTERNAL DISSEMINATION OF INFORMATION REGARDING BANK-RELATED CRIMES**

Dear 

We write in response to your letter request received by the National Privacy Commission (NPC) seeking guidance on the proposed processing activities of a bank in relation to strengthening the campaign against fraud.

We understand that the bank proposes the conduct of effective training for and raise awareness of its employees about the consequences of committing crimes against the bank, its depositors, and other stakeholders. You now seek opinion from the NPC on the following matters, as to whether:

1. Publication and uploading of names, photos, and other details (e.g., criminal charge that gave rise to the issuance of an arrest warrant or conviction) of erring personnel due to his/her administrative or criminal offense, through an internal e-mail dissemination or posting in an intranet (internal repository) as a measure to assist the bank's efforts to combat fraud and create a deterrent effect is permissible under the Data Privacy Act of 2012² (DPA); and
2. A caveat in the publication or email message warning its internal stakeholders that unauthorized dissemination of the information contained therein may be punishable under the DPA.

¹ Tags: sensitive personal information; anti-fraud campaign, training, and awareness; internal disclosure of sensitive personal information; proportionality.

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).

Anti-fraud campaigns; disclosure of sensitive personal information; lawful basis; general data privacy principles

While we recognize the objectives of the bank to combat fraud, raise awareness regarding the consequences of committing crimes against the bank, and create a deterrent effect vis-à-vis the publication of personal and sensitive personal information (collectively, personal data) of personnel having arrest warrants or convictions, this personal data processing activity should have a lawful basis under the DPA.

With this, we note that the details of the criminal or administrative charges, the disposal of such proceedings, and the decision rendered on the same may be considered as sensitive personal information under the DPA.

Recall that the processing of sensitive personal information, as a general rule, is prohibited, unless the processing falls under any of the instances under Section 13 of the DPA. In this instance, there seems to be no applicable lawful criteria for such processing. Further, this disclosure of personal data, even if just within the internal systems of the bank where access is limited to the employees and other internal stakeholders, and even with the caveat on unauthorized dissemination, the same may still be deemed disproportionate to the specified purposes above.

We reiterate the principle of proportionality which requires that the processing of personal data 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.³

With this, the bank should reevaluate its proposed internal anti-fraud initiatives. To our mind, these may be accomplished through other less privacy-intrusive means without necessarily exposing sensitive personal information of former or current employees of the bank. We note that the Bangko Sentral ng Pilipinas (BSP) has recently issued a directive which addresses the management of human resource-related risk, requiring banks to embed in their enterprise-wide risk management framework measures to identify, measure, monitor, and control the so-called “people risk.”⁴

Lastly, it is also necessary for the bank to assess the proposed personal data processing activity in relation to how the same may possibly affect the other fundamental rights and freedoms of the data subject, such as the right to due process.

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

³ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 17 (c) (2016).

⁴ See: Bangko Sentral ng Pilipinas, Amendments to Operational Risk Management and Internal Control Measures [Circular No. 1112, series of 2021] (April 8, 2021).

ADVISORY OPINION NO. 2021-034¹

17 August 2021



Re: **REQUESTS FROM GOVERNMENT AGENCIES FOR THE DEPARTMENT OF FOREIGN AFFAIRS TO PROVIDE PERSONAL INFORMATION**

Dear 

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to guidance on the requests for information received by the Department of Foreign Affairs (DFA) – Office of Consular Affairs (OCA) from various government agencies, specifically law enforcement agencies and financial regulatory agencies.

In your letter, you stated that the Bureau of Internal Revenue (BIR) sent a letter to OCA requesting for information about a particular taxpayer. Said request for information was hinged on Section 5 of the National Internal Revenue Code (NIRC), as amended.

You further stated in your letter that the Presidential Commission on Good Government (PCGG) likewise sent a letter to the OCA requesting for information of persons in relation to a Supreme Court case.

You now come to the NPC for guidance on whether the OCA can disclose personal information and sensitive personal information (collectively, personal data) of OCA's data subjects without violating the provisions of the Data Privacy Act of 2012² (DPA).

Scope of the DPA; special cases; fulfillment of mandate; public authority; law enforcement or regulatory functions

¹ Tags: special cases; lawful criteria for processing; public authority; fulfillment of mandate; subpoena; limitation on data subject rights.

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 DPA and its Implementing Rules and Regulations (IRR) provide for a list of specified information that are not covered by certain requirements of the law, which includes information necessary to carry out functions of a public authority, 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, use, disclosure or other processing necessary to the purpose, function, or activity 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 authority, subject to restrictions provided by law...

X X X

Provided, that the non-applicability of 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.” (Underscoring supplied)

We reiterate our discussions in NPC Advisory Opinion No. 2020-015 and 2021-028 wherein we discussed the BIR’s duty and authority to, among others, ensure compliance with the NIRC, as amended, and other relevant tax laws and regulations. Particularly, the authority of the BIR Commissioner to obtain information in the evaluation of the tax compliance of any person, specifically in this case, where the BIR has already identified a tax compliance issue with a particular taxpayer, as mentioned in your letter.

Investigative functions; lawful criteria for processing; Sections 12 and 13
As to the PCGG request, we understand from Section 3(g) of Executive Order No. 1³ that the PCGG has the power to seek and secure the assistance of any office, agency, or instrumentality of the government, in

relation to the recovery of all ill-gotten wealth by Former President Marcos, his immediate family, relatives, subordinates, and close associates,⁴ and the investigation of such cases of graft and corruption as the President may assign to the Commission from time to time.⁵

While the PCGG's purpose for requesting the addresses of certain persons in relation to the Supreme Court case was not indicated in your letter, we suppose that the said request is pursuant to the exercise of the PCGG's mandates which includes the conduct investigations, sequestrations, among others.

With this, the request for addresses and other information may then be anchored under Sections 12 and/or 13 of the DPA, depending on type of personal data involved.

Specifically, Section 12 (e) recognizes the processing that is necessary to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate and Section 13 (b) which allows the processing which is provided for by existing laws and regulations and Section (f) on the processing that 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.

Requests through letters; issuance of subpoena; subpoena powers; general data privacy principles; data subject rights; limitations

Another concern you raised is that these requests from the BIR and/or from the PCGG were made through letter requests and not through subpoenas. You proceeded to cite Section 34 (b) (1) of the IRR:

“Section 34. Rights of the Data Subject. x x x

b. Right to object. x x x

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.”

³ Office of the President, Creating the Presidential Commission on Good Government [Executive Order No. 1, s. 1986] (28 February 1986).

⁴ Id. § 2 (a).

⁵ Id. § 2 (b).

To clarify, the above provision pertains to the limitations on the exercise of the right to object, specifically when processing is based on consent and the data subject has withdrawn the same, but processing may continue if the personal data is needed pursuant to a subpoena.

We emphasize that the above does not operate to provide a limitation on how personal data can be requested by government agencies.

We also wish to clarify that the issuance of a subpoena may not always be appropriate at a particular stage of an inquiry, investigation, enforcement action, or other applicable government action. Requests for information may come in various forms, i.e., court orders, subpoena, letters, orders, other official communications, among others. It is also important to note that not all government agencies are granted subpoena powers.

We emphasize that the NPC does not presume to know all the means and methods by which government agencies can validly request for personal data. Still, the DPA requires that all agencies processing personal data, whether for law enforcement, regulatory, investigative, or some other mandate, should strictly adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality, and follow all due process requirements as provided by the applicable laws and regulations.

Having said that, the OCA is not precluded to further ask and/or confirm from the BIR and/or the PCGG additional details with respect to the validity of the letter requests and the standard operating procedures of the agencies on these types of data requests made through letters instead of subpoenas.

Finally, Section 19 of the DPA and Section 37 of its IRR provide for the limitations with respect to the rights of the data subjects where the processing of personal data is for the purpose of investigations in relation to any criminal, administrative, or tax liabilities of the data subject. This is further clarified in Section 13 of NPC Advisory No. 2021-01 on Data Subject Rights,⁶ which provides:

“SECTION 13. Limitations. — The exercise of the rights of data subjects shall be reasonable. The same may be limited when necessary for public interest, protection of other fundamental rights, or when the processing of personal data is for the following purposes:

X X X

B. Investigations in relation to any criminal, administrative, or tax liabilities of a data subject: provided, that:

1. The investigation is being conducted by persons or entities duly authorized by law or regulation;
2. The investigation or any stage thereof relates to any criminal, administrative, or tax liabilities of a data subject as may be defined under existing laws and regulations; and
3. The limitation applies to the extent that complying with the requirements of upholding data subject rights would prevent, impair, or otherwise prejudice the investigation. x x x.”

Considering the foregoing discussions, the OCA may disclose personal data to the BIR and the PCGG without necessarily violating the provisions of the DPA and the rights of the data subjects.

We emphasize that the DPA shall not be used to hamper, or interfere with, the performance of the duties and functions of government agencies. The DPA 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.

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

ADVISORY OPINION NO. 2021-035¹

23 September 2021



Re: **DATA SHARING AGREEMENT BETWEEN PHILHEALTH
AND CITY CIVIL REGISTRAR ON REPORTING OF REGISTERED
DEATHS**

Dear 

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) seeking to clarify certain data privacy issues relating to the Memorandum of Agreement for Data Sharing (MOA) proposed by Philippine Health Insurance Corporation (PHIC).

We understand based on your letter that the proposed MOA states the following:

- “1.1 Through its Office of the Local Civil Registrar, it shall transmit to PhilHealth a (monthly) report of registered deaths within its territorial jurisdiction;*
- 1.2 The said report shall contain the full names of the deceased and their circumstances such as date of death, place of death, and last known residence of the deceased;*
- 1.3 Should PhilHealth request for a certified true copy of the certificate of death in line with an investigation, the LGU shall release the same subject to the payment of corresponding fees;*
- 1.4 It expressly understands that any and all information gathered, submitted, or otherwise incorporated in the database of PhilHealth in the course of this engagement shall be exclusively owned by the Corporation; and*

¹ Tags: registered deaths; death certificate; Local Civil Registrar; PHIC; data sharing; proportionality.

1.5 Any and all information regarding PhilHealth members in relation to an investigation/inquiry, from any source and in any form (i.e., written, verbal, or electronic) shall be considered as strictly confidential.”

You raised the following concerns relative to the above:

1. Whether the intended data sharing proposed by the PHIC complies with the provision of the NPC Circular No. 16-02 in relation to the Data Privacy Act of 2012² (DPA);
2. Whether prior consent from the heirs of or next of kin of the data subject (deceased) is required for purposes of data sharing; and
3. Whether the lack of a specific term for the duration of the agreement is contrary to NPC Circular No. 16-02.

Criteria for lawful processing

Sections 12 and 13 of the DPA provides for a set of criteria in the processing of personal and sensitive personal information (collectively, personal data), respectively, apart from consent. Particularly, processing that is necessary for compliance with a legal obligation,³ provided for by existing laws and regulations,⁴ or necessary for the establishment, exercise, or defense of legal claims,⁵ may be applicable.

We understand that PHIC has been granted quasi-judicial powers which include the conduct of investigations pursuant to Section 17 of RA No. 7875, as amended by RA No. 10606.⁶ Thus, where the processing of personal data is required pursuant to its mandate, specifically for investigations, the same is recognized under the DPA.

As the basis for lawful processing is by virtue of an existing law or regulation, the consent of the deceased data subject's heirs or next of kin is not necessary before the City Civil Registrar may share the deceased's personal data with the PHIC.

General data protection principles; proportionality

Although the DPA sanctions the processing of personal data by virtue of a law, personal information controllers (PICs), such as PHIC and Civil Registrars are still required to adhere to the general data privacy principles

of transparency, legitimate purpose, and proportionality.

In this case, the principle of proportionality is of utmost concern. It requires that the processing, which includes disclosure, must be necessary and not excessive in relation to a declared and specified purpose, and that personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.⁷

Thus, the PHIC monthly reportorial requirement for all registered deaths within the territorial jurisdiction of a particular city, without any qualifications, should be reevaluated if such is still proportional to the purpose. The City Civil Registrar should seek further clarification with the data protection officer of PHIC as to the specific legal basis for requiring such extensive report on all registered deaths and whether a limited report of registered deaths for which PHIC is conducting investigations as part of its statutory mandate should already suffice.

As to PHIC's request on the release of certified true copies of death certificates in relation to investigations, access to said documents may be allowed. For this purpose, the City Civil Registrar should keep records and appropriate documentation of all PHIC requests.

Data sharing; data sharing agreements; term

We would like to note that NPC Circular No. 2020-03⁸ superseded NPC Circular No. 16-02 as the governing rule regarding data sharing.

On the term or duration of the data sharing arrangement, the current Circular provides as follows:

“D. Term. It specifies the term or duration of the data sharing arrangement which will be based on the continued existence of the purpose/s of such arrangement. Perpetual data sharing or DSAs that have indeterminate terms are invalid. Parties are free to renew or extend a DSA upon its expiration. The DSA should be subject to the conduct of periodic reviews which should take into consideration the sufficiency of the safeguards implemented for data privacy and security.”⁹

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 Data Privacy Act of 2012, § 12 (c).

⁴ Id. § 13 (b).

⁵ Id. § 13 (f).

⁶ An Act Amending Republic Act No. 7875, Otherwise Known as The “National Health Insurance Act of 1995”, As Amended, And For Other Purposes [National Health Insurance Act of 2013], Republic Act No. 10606, § 17 (2013).

⁷ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).

We recommend that that the parties revisit the proposed MOA and indicate a specific term, in compliance with the above requirement.

This opinion is based solely on the limited information you have provided. We are not privy to the other provisions of the draft MOA and the review of the same is limited to the above quoted provisions for purposes of this opinion. 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

⁸ National Privacy Commission, Data Sharing Agreements [NPC Circular 2020-03] (23 December 2020).

⁹ Id. 9 (D).

ADVISORY OPINION NO. 2021-036¹

23 September 2021



Re: **DISCLOSURE OF LOAN DOCUMENTS PURSUANT TO A
LEGAL CLAIM**

Dear 

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC or the Commission) to provide clarity on whether the release of loan documents containing personal data is allowed under the Data Privacy Act of 2012² (DPA), particularly in relation to Section 13 (f) on the establishment of legal claims.

From your letter, we understand that Atty. RAN, on behalf of his client, Mr. CGS, wrote to the Home Development Mutual Fund (Pag-IBIG Fund) Loans Origination Department – Cebu Housing Hub requesting for certified copies of the vouchers on the check payment/s made to Ms. CVG.

We understand further that Mr. CGS allegedly lent money to Ms. CVG, through her brother, Mr. RV. Allegedly, Mr. RV bought two (2) Pag-IBIG Fund acquired assets (subject lots). Atty. RAN mentioned that the intention was to re-sell the lots and the proceeds used to pay Mr. CGS. However, when Mr. CGS demanded payment, Mr. RV declared that the properties are yet to be sold. Upon verification, Mr. CGS found out that the properties were purportedly bought by a certain Mr. ZPJ through a Pag-IBIG Fund housing loan with the proceeds released to the seller, Ms. CVG. Thus, Atty. RAN stated the vouchers

¹ Tags: criteria for lawful processing; legal claims; 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).

are material evidence in his client's pursuit of justice in the event the Ms. CVG and her brother fail to settle their obligation.

Finally, we understand there is a disagreement between Pag-IBIG Fund and Atty. RAN as shown through the exchange of letters between parties. According to Pag-IBIG Fund, the requested documents pertain to personal data involving the housing loan borrower Mr. ZPJ and the seller, Ms. CVG, which are protected under the DPA and would thus require their consent prior to the disclosure of the information to third parties.

On the other hand, Atty. RAN claims the following: (1) the request falls under Section 13 (f) which states that the processing of sensitive personal information is allowed where the processing concerns the establishment, exercise or defense of legal claims..."; (2) Pag-IBIG Fund has been informed that his client, Mr. CGS, has a legal claim over the proceeds of the subject sale transaction between Mr. ZPJ and Ms. CVG who stood for her brother (or father, as alleged in his letter dated 30 April 2021) in the acquisition of the subject lots; and (3) it is simply impossible and illogical to obtain the consent of Ms. CVG who allegedly anticipates to be sued criminally for misrepresentations made to his client.

Thereafter, Pag-IBIG Fund replied citing an Advisory Opinion of this Commission (number not stated) which supposedly mentioned the EU General Data Protection Regulation (GDPR) relating legal claims to those that pertain to court proceedings, administrative or out-of-court procedure, and hence the provision referred to by Atty. RAN does not apply to the request.

We understand further that Atty. RAN reiterated his claim that the request is covered by Section 13 (f) and furnished a copy of the Memorandum of Agreement (MOA) between his client, Mr. RV, and Ms. CVG regarding their joint venture to acquire and sell Pag-IBIG Fund lots for profit.

You now come to the Commission for guidance on whether the request of Atty. RAN, on behalf of his client, falls within the exemption of the prohibition of processing of sensitive personal information under Section 13 (f) of the DPA, specifically on the "establishment, exercise or defense of legal claims." You likewise seek clarity if the release of the requested documents or information is not prohibited even without the consent of the data subject.

Lawful processing; establishment, exercise or defense of legal claims

The focal point of the query is 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: 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)

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,⁴ 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.”

...

The DPA is neither a tool to prevent the discovery of a crime nor a means to hinder legitimate proceedings.⁵

Given the above, the establishment of legal claims requiring the processing of sensitive personal information is permitted under the DPA. The term establishment may include 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).

In the situation at hand, Mr. CGS, through his counsel, Atty. RAN, seeks to obtain information relating to the proceeds of the sale of the two subject lots by virtue of the MOA between him on the one hand and Mr. RV and Ms. CVG, on the other. To establish this legal claim, certified copies of the vouchers on the check payment/s

³ Data Privacy Act of 2012, § 13 (f).

made to Ms. CVG from the alleged sale with Mr. ZPJ are deemed necessary. Section 13 (f) would be the lawful criterion for such request if such vouchers contain sensitive personal information.

If, however, only personal information is involved, the disclosure of the vouchers may still find basis under Section 12 (f) of the DPA which provides:

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. (emphasis supplied)

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.⁶

Thus, Pag-IBIG Fund may release certified copies of the requested loan documents, sans the consent of the data subjects involved, keeping in mind the purpose of the request and the data privacy principle of proportionality.

⁴ National Privacy Commission, NPC 19-653 (Dec. 17, 2020), available at <https://www.privacy.gov.ph/wpcontent/uploads/2021/02/NPC-19-653-BGM-vs-IPP-Decision-FINAL-Pseudonymized-21Dec2020.pdf> (last accessed 07 September 2021).

⁵ Citations omitted.

⁶ See footnote 4; citing CID Case No. 17-K-003 dated 19 November 2019 and NPC 18-135 dated 06 August 2020.

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. 2021-037¹

23 September 2021

[REDACTED]

[REDACTED]

Re: **REQUEST FOR THE STATUS OF APPLICATION AND THE LIST OF BENEFICIARIES OF THE SITIO ELECTRIFICATION PROGRAM (SEP)**

Dear [REDACTED]

We write in response to your request for guidance on whether the Local Government of Infanta, Quezon (Infanta LGU) can lawfully request for certain information from the Quezon II Electric Cooperative, Inc. (QUEZELCO II) in relation to the Sitio Electrification Program (SEP) without violating the provisions of the Data Privacy Act of 2012² (DPA).

We understand that the QUEZELCO II launched the SEP in 2019. The Infanta LGU supports the implementation of the SEP to ensure basic utilities are provided to far-flung communities in the Quezon Province, including Infanta.

We understand further that the LGU received concerns in relation to the SEP, specifically on matters of jurisdiction. It was raised that some households that have been energized by QUEZELCO II fall within the cadastral map of Infanta, and therefore the issuance of electrical permit and other requirements falls within the Infanta LGU's jurisdiction. It is claimed that there were instances where the necessary permits were instead issued by another LGU.

To address this, the Infanta LGU requested from QUEZELCO II copies of

¹ Tags: lawful processing of personal information; fulfillment of mandate; general 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).

of the SEP applications, including the supporting documents to verify the validity of the applications. QUEZELCO II denied the request stating that consent of the applicants was needed. The Infanta LGU just requested QUEZELCO II to provide the status of application of each target beneficiary using the List of Households provided by the QUEZELCO II to the Infanta LGU. Specifically, the following are requested: 1) whether each beneficiary already has an approved electrical permit, 2) what is the issuing LGU, and 3) the status of energization by QUEZELCO II.

You now seek clarification whether the Infanta LGU can be provided with the above information considering the provisions of the DPA.

Lawful basis for processing personal and sensitive personal information (collectively, personal data); Sections 12 and 13

The DPA provides for the various lawful bases for processing personal information under Section 12, and sensitive personal information under Section 13.

We wish to clarify that consent of the data subject is just one of the possible lawful bases for processing. In this scenario where an LGU is requesting for information relating to the exercise of its mandate, consent may not be the most appropriate lawful basis.

As defined, consent refers to “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.”³

Note that consent is not an appropriate basis for processing in instances where there is a clear imbalance of power between the data subject and the personal information controller (PIC) as it is unlikely that consent will be freely given.

Given the above, the LGU can rely on other lawful bases for processing, specifically its mandate under the Local Government Code of the Philippines⁴ or any other applicable laws, rules, and regulations in relation to Sections 12 (c) and (e) on processing for compliance with legal obligations or when necessary to fulfill functions of a public authority, for the processing of personal information. For sensitive personal information, Sections 13 (b) and (f) on processing that is based on laws as well as that

which is necessary for the establishment, exercise, or defense of legal claims may be applicable.

General data privacy principles; proportionality; safeguards

We wish to reiterate that while there may be a lawful basis for processing under the DPA, the Infanta LGU must still adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. Specifically for proportionality, 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

In keeping with the said principle, we acknowledge the concession made by the Infanta LGU when it revised and limited its request to the three items mentioned above instead of insisting on having copies of all applications and supporting documents submitted by the target beneficiaries. Making a re-evaluation of whether the original list of requested information is necessary for the declared and specific purpose is consistent with the practice of data minimization.

Lastly, as a PIC, the Infanta LGU is expected to implement the necessary organizational, technical, and physical safeguards for the protection of any personal data it collects and processes. It is bound by obligations under the DPA, its IRR, and issuances of the NPC, specifically NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies.

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

³ Data Privacy Act of 2012, § 3 (b).

⁴ An Act Providing for a Local Government Code of 1991 [Local Government Code of 1991], Republic Act No. 7160 (1991).

ADVISORY OPINION NO. 2021-038¹

21 October 2021



Re: **DATA SHARING FOR THE NATIONAL HEALTH
WORKFORCE REGISTRY**

Dear 

We write in response to your request for assistance, comments, or guidance to facilitate the finalization of the Data Sharing Agreement (DSA) between the Department of Health (DOH) and the Professional Regulation Commission (PRC) (collectively, Parties).

We understand that the Parties intend to execute a DSA pursuant to Section 25 (c) of Republic Act No. 11223, otherwise known as the Universal Healthcare Act² (UHC Act) which mandated the Parties, in coordination with the duly registered medical and allied health professional societies, to create a registry of medical and allied health professionals, indicating, among others, their current number of practitioners and location of practice (Registry). The Parties also issued Joint Administrative Order (JAO) No. 2021-0001 on the Guidelines on the Establishment, Utilization, and Maintenance of the National Health Workforce Registry.³

We understand further that the Registry will use data matching protocols across different human resources for health (HRH) data sources. The matched and assembled datasets of HRH individuals will be stored in the Registry data warehouse and will be refined into anonymized and aggregated reports which could be released to the public as requested. You now seek guidance on how the Parties can pursue sharing of personal and sensitive personal information (collectively, personal data)

¹ Tags: criteria for lawful processing; compliance with legal obligation; law or regulation; consent; general data privacy principles; privacy impact assessment; privacy-by-design.

² An Act Instituting Universal Healthcare for All Filipinos, Prescribing Reforms in the Healthcare System, and Appropriating Funds Therefor [Universal Healthcare Act], Republic Act No. 11223 (2018).

³ Department of Health and Professional Regulation Commission, Guidelines on the Establishment, Utilization, and Maintenance of the National Health Workforce Registry [Joint Administrative Order No. 2021-0001] (20 Jan. 2021).

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).

required by the UHC Act and the JAO that is aligned with the provisions of the Data Privacy Act of 2012⁴ (DPA), particularly with the general data privacy principle of proportionality.

General data privacy principles; proportionality

We understand that the PRC raised the issue of proportionality with regard to the processing of the birthdate and the sex of the health professionals. According to the PRC, the inclusion of such information are excessive and unnecessary to carry out the purpose of the Registry pursuant to the UHC Act which is to have a database of medical and allied health professionals, indicating, among others, their current number of practitioners and location of practice.⁵

The principle of proportionality 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.⁶

In keeping with the said principle, we acknowledge the position of the PRC that the inclusion of birthdate and sex in the Registry may not be indispensable to achieve the purpose of the Registry. But we also understand that the DOH plans to use birthdate and sex, being unique identifiers, for the data matching protocols of the Registry.

With this, the DOH should make an assessment on whether these personal data are indeed needed, taking into account the comments of the PRC, and the fact that the Registry will likewise include other information which may serve as the additional variables for the data matching protocols vis-à-vis the achievement of the purpose intended under the UHC Act and the JAO.

Lawful basis for processing personal data; special cases; privacy notice
If the DOH, after its judicious assessment, has determined that the birthdate and sex of the health professionals are indeed indispensable to achieve the purpose of the processing, and such purpose cannot be fulfilled by any other means, the PRC may lawfully share the same.

We wish to clarify the contention of the PRC that consent of the health professionals is needed if their sex and birthdate will be processed pursuant to the UHC Act and the JAO. We note that consent of the data subject is just one of the possible lawful bases for processing. In this scenario, consent may not be the most appropriate lawful basis considering that a government agency is requesting for personal data pursuant to existing laws and regulations.

Instead, the DOH's processing may be considered as processing under the special cases provided for in Section 4 (e) of the DPA as it is a public authority performing regulatory functions to the extent necessary for the fulfillment of its mandate.

Thus, the Parties need not secure the consent of the health professionals prior to the proposed sharing. Nevertheless, the Parties are still required to provide the health professionals adequate information that describes the nature, extent, and purpose of the processing being done pursuant to the UHC Act and the JAO. This may be done through an appropriate privacy notice.

A privacy notice is “a 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.”⁷

The Parties may post the privacy notice in their respective offices, websites, and/or other official online platforms to ensure that the data subjects will have access to it.

Privacy impact assessment; privacy by design

We recall our comment in November 2020 when we reviewed the draft DSA for the Parties to conduct a privacy impact assessment (PIA) on the Registry.

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 PIP. It takes into account 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.⁸

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.

In addition to the conduct of the PIA, it is recommended that the Parties incorporate privacy by design principles in the development of the Registry system. Privacy by design is an approach that ensures that privacy and data protection have been taken into account during the design phase of a system, project, program and process and will continue to be taken into account throughout its lifecycle and implementation.⁹

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 Universal Healthcare Act, § 25 (c).

⁶ See: Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).

⁷ IAPP, Glossary of Privacy Terms, available at <https://iapp.org/resources/glossary/#paperwork-reduction-act-2>.

⁸ NPC Advisory No. 201-03, Guidelines on Privacy Impact Assessment, 31 July 2017.

⁹ 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. 2021-039¹

22 October 2021



Re: **DATA SHARING OF INCIDENT/DISASTER DATA**

Dear 

We write in response to your letter seeking guidance from the National Privacy Commission (NPC) on the sharing of personal and sensitive personal information (collectively, personal data) among the Metro Manila Disaster and Risk Reduction and Management Council (MMDRRMC) and various agencies.

We understand that the MMDRRMC is responsible for carrying out the implementation of actions and measures pertaining to all aspects of disaster risk reduction and management in the National Capital Region.

We understand further that the MMDRRMC is structured as a Regional Disaster Risk Reduction and Management Council (RDRRMC) under the Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 10121 otherwise known as the Philippine Disaster Risk Reduction and Management Act of 2010.

As an RDRRMC, the MMDRRMC is mandated to coordinate, integrate, supervise, monitor and evaluate the functions of member agencies and the Local Disaster Risk Reduction Management Councils within its jurisdiction, and be responsible for ensuring risk-sensitive regional development plans, and in case of emergencies, convene the different line agencies and concerned institutions and authorities.

In your letter, you disclosed that it has become standard practice for the MMDRRMC to share and exchange incident/disaster data and information with other government agencies for proper monitoring and documentation of all major and minor incidents and disaster occurrences in Metro Manila on its population, properties, and environment.

¹ Tags: criteria for lawful processing; data sharing; law and regulation; general data privacy principles.

You now ask if this data sharing arrangement is in adherence with the provisions of the Data Privacy Act of 2012² (DPA).

NPC Circular No. 2020-03; data sharing; mandate; laws and regulations

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.³

Further, the said Circular clarified that data sharing may be based on any of the criteria for lawful processing of personal data in Sections 12 and 13 of the DPA⁴ and may also be allowed pursuant to Section 4 of the law which specifies the special cases.⁵ The Circular further provides that it does not prohibit or limit the sharing, disclosure, or transfer of personal data that is already authorized or required by law.⁶

In relation to the above, Sections 12 (c) and (e) allows the processing of personal information when necessary for compliance with a legal obligation or if 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. For sensitive personal information, the processing of the same is generally prohibited except in certain instances provided for under Section 13 of the DPA, one of which is when processing is provided for by existing laws and regulations.

The above provisions may be applicable to the data sharing involving the MMDRRMC and other government agencies engaged in disaster risk reduction and management since the data sharing arrangement is mandated by law or regulation.

General data privacy principles; safeguards; data sharing agreement

We would like to note that, although government agencies may have lawful basis for the processing of personal data, such processing must still adhere to the other requirements of the DPA.

As personal information controllers (PICs), government agencies are required to, among others, adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.

Specifically for proportionality, the processing of personal data 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.

PICs are also required to implement physical, organizational, and technical security measures to ensure the protection of personal data and uphold the rights of data subjects.

The MMDRRMC may consider executing a data sharing agreement (DSA) with its member agencies, where appropriate. A DSA contains, among others, 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. While the execution of a DSA is not mandatory, it is a sound recourse and demonstrates accountable personal data processing.⁷

For further guidance on DSAs, please refer to NPC Circular No. 2020-03 available at our website: <https://www.privacy.gov.ph/memorandum-circulars/>.

Statistics

Finally, should the incident/disaster data and information for the Incident and Situational Reports you mentioned pertain to statistics only, i.e., on the number of dead, missing and injured, the DPA is not applicable.

Statistical information which does not include information from which the identity of an individual is apparent or can be reasonably and directly ascertained, is not personal data, and thus, the sharing of statistics is not covered by the provisions, principles, and requirements under 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

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

⁴ Id. § 6. ⁷ NPC Circular No. 2020-03, § 8.

⁵ Id. § 7.

⁶ Id. § 6.

ADVISORY OPINION NO. 2021-040¹

8 November 2021



Re: **SUBMISSION OF COPIES OF CONDOMINIUM CERTIFICATE OF TITLE TO THE CONDOMINIUM CORPORATION**

Dear 

We write in response to your letter received by the National Privacy Commission (NPC) which sought clarification on whether the Data Privacy Act of 2012² (DPA) and its Implementing Rules and Regulations³ (IRR) allow a condominium corporation to request unit owners to submit copies of their Condominium Certificate of Title (CCT) and duplicate unit keys. If so permitted, you likewise ask about the minimum safeguards to be imposed as required by the DPA.

We understand from your letter that your client, Perla Condominium Corporation (PCC), is the condominium corporation managing the affairs of Perla Mansion. We further understand that the Master Deed of PCC provides that the amount of any assessment against a unit owner, including association dues, interest due in case of delinquency, costs of collection and/or suit including attorney's fees and penalties for delinquency shall constitute a lien on the unit. The Master Deed further allows PCC to validly foreclose on the unit as if a mortgage has been executed on it.

In addition, PCC's By-Laws allows for the enforcement of collection through any of the remedies provided by the Condominium Act and other pertinent laws, including the filing of an adverse claim with the Register of Deeds should a member default in the payment of any assessment. Given the foregoing, you stated that there is a need to identify the registered owner of the units.

¹ Tags: Condominium Certificate of Title; lawful processing; consent; establishment, exercise, or defense of legal claims; general data privacy principles; proportionality; privacy impact assessment.

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).

You also provided in your letter that Perla Mansion is an old building with minimal occupancy rate which presents a real possibility that dangerous emergency conditions inside the units will not be addressed immediately. We understand from your letter that there may be a need for PCC to do the necessary inspections given the said risks.

Lawful basis for processing; sensitive personal information; consent; establishment, exercise, or defense of legal claims

The DPA applies to the processing of all types of personal and sensitive personal information (collectively, personal data) and to any natural or juridical person involved in the processing of personal data.⁴ A CCT contains personal data of the registered owner such as the name, marital status, address, and citizenship. Hence, the processing of a CCT falls within the scope of the DPA.

The DPA provides for the various criteria for lawful processing of personal and sensitive personal information in Sections 12 and 13, respectively. As the CCT contains sensitive personal information, PCC should determine the most appropriate lawful basis for processing under Section 13 of the law, taking into account the purpose of the processing and PCC's relationship with the data subjects. In particular, the following criteria may be considered:

“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:

- (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; 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.” (underscoring supplied)

For consent-based processing, the DPA requires consent to be freely given, specific, and informed indication of will whereby the data subject

agrees to the collection and processing of his or her personal data.⁵ It must be evidenced by written, electronic or recorded means and it may be given on behalf of a data subject by a representative specifically authorized by the data subject to do so.⁶ Consent must be given prior to the processing and must be specific to the stated purpose.⁷

Hence, if consent is the most appropriate basis, PCC should obtain the consent of the unit owners prior to the collection of copies of their CCTs. The consent must be documented in a form which states the specific purpose for which the CCTs will be used and other details on, among others, the processing involved, identity of the personal information controller, rights of data subjects and ways to exercise the same. PCC must provide the adequate details to enable the data subjects to make an informed decision on the processing of their personal data.

For Section 13 (f), the Commission had the opportunity to clarify the same, specifically on the criterion of the establishment, exercise or defense of legal claims in the case of BGM vs. IPP:⁸

“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.”

This Commission in the same case went on further and held 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.

⁴ 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, § 4 (2012).

⁵ Data Privacy Act of 2012, § 3 (c).

⁶ Ibid.

⁷ Id. § 13 (a).

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. 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.” (underscoring supplied)

With the above, PCC may also consider the above criterion in relation to the mentioned liens, possible foreclosures, and other related enforcement actions against unit owners.

General data privacy principles; proportionality; privacy impact assessment

Any personal data processing activity shall adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.

Specifically for proportionality, the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.⁹ The principle also requires that personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.¹⁰

As discussed above, PCC intends to request all unit owners to submit copies of their CCTs for annotating liens and foreclosing on the units of delinquent owners, identifying registered owners to properly address correspondences, confirming whether the votes are being cast by the real registered owners during meetings, and ensuring that only authorized persons enter the building premises.

We note that although the foregoing purposes are valid concerns of a condominium corporation, PCC should also consider if there are less intrusive means by which the stated purposes may be achieved. It is advisable to conduct a privacy impact assessment (PIA) to identify and provide an assessment of various privacy risks, and propose measures intended to address and mitigate the effect of these risks on the unit owners.

⁹ National Privacy Commission, *BGM vs. IPP* [NPC 19-653] (Dec. 17, 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 9 July 2021).

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

¹⁰ *Ibid.*

Submission of duplicate unit keys

Regarding your second query on whether PCC is permitted by law to request unit owners to submit duplicate keys of their units, the NPC may not be the appropriate authority to provide an opinion on this concern as the scope of the DPA only applies to the processing of personal data and consequently, the right to informational privacy.

Kindly refer to the Civil Code provisions on Human Relations which may provide the more appropriate guidance and reference on this matter. 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



DECISIONS

JBD

Complainant,
-versus-

CID Case No. 18-D-012

For: Violation of the
Data Privacy Act of 2012

JI and VVV

Respondent.

DECISION

AGUIRRE, D.P.C.:

Before this Commission is a Complaint filed by Complainant JBD against the respondents JI and VVV for an alleged violation of Republic Act No. 10173 (“Data Privacy Act of 2012” or “DPA”).

The Facts

The Commission has previously summarized the factual antecedents in this case through an Order dated 21 May 2020, thus:

Complainant here alleges that his Social Security System (“SSS”) Employment and Payment history were illegally obtained by Respondent JI, his common law spouse, and her lawyers. He learned about this when he received a Position Paper against him with attached print-outs from the SSS. These contained his birthdate and SSS number, as well as his employment history and actual premiums.¹ This Position Paper was filed with the Professional Regulation Commission (“PRC”) in connection with an ongoing case involving him and Respondent JI.

Complainant initially filed a complaint before the SSS. Upon inquiring with SSS, he was told by its Fraud and Legal Department that this data was not processed within the vicinity of the agency, and that an unauthorized individual accessed the SSS data portal

¹Records, p. 9-10.

where his work history and premiums were collected.²

Upon the filing of this Complaint with the National Privacy Commission, the parties were called for a Discovery Conference. Complainant and Respondent VVV were present, but Respondent JI failed to appear.

During the Discovery Conference, the parties manifested that they were not willing to enter into an amicable settlement. They further manifested that there is no need to secure evidence from each other to further their case.

Hence, an Order was issued by the Commission on 12 July 2018 directing Respondents to file their responsive Comment until 22 July 2018. Complainant was in turn given ten (10) days from the receipt of the Comment to file his Reply.

In the same Order, the Commission directed the Complainant to submit additional evidence pursuant to Section 21 of NPC Circular 16- 04 (“NPC Rules of Procedure” or “Rules”),³ thus:

In the interest of giving due course to Complainant’s claims, the Commission resolves to order Complainant to provide the following:

- 1.) A Certified True Copy of the Position Paper containing the subject SSS documents filed with the PRC; and
- 2.) Documents to substantiate the allegations made in Paragraph 10 of the Verified Reply which refers to the findings of the SSS Fraud and Legal Department.

The foregoing is pursuant to NPC Circular 16-04 which provides that the Commission may, on the basis of its review of the evidence, order the conduct of a clarificatory hearing if in its discretion, additional information is needed to make a Decision.⁴

WHEREFORE, all the above premises considered, the Commission hereby **ORDERS** Complainant JBD to submit the documents enumerated above within fifteen (15) days from receipt of this Order. The failure of Complainant to submit such documents shall cause this case to be submitted for resolution.

² Id., p. 59.

³ NPC Circular 16-04. Rules of Procedure of the National Privacy Commission. Dated 15 December 2016.

⁴ Id. at Section 21.

In a Manifestation and Motion dated 29 July 2020, Respondent VVV requested the Commission to order the Complainant to furnish him a copy of the Verified Reply and allow him to file a Rejoinder. Respondent VVV also moved that his other prayers be granted, namely, to (a) note their manifestation; (b) hold in abeyance any clarificatory hearing pending the consideration of his Manifestation and Motion; and (c) note his counsel's Entry of Appearance.⁵

On 04 August 2020, Complainant filed a Motion for Extension to Comply with the Commission's Order dated 21 May 2020, citing the lockdown of the Legal Division of Professional Regulation Commission (PRC) from 20 July 2020 to 27 July 2020. Complainant specifically requested that he be given until 02 September 2020 to comply with the said Order.⁶ The Commission issued a Resolution dated 06 August 2020 stating thus:

WHEREFORE, premises considered, Complainant's Motion for Extension to Comply with the Commission's Order until 02 September 2020 is hereby GRANTED. Complainant is ORDERED to furnish the Respondents a copy his Verified Reply within ten (10) days from receipt of this Resolution.

Respondent VVV's Motion to Order the Complainant to furnish him a copy of the Verified Reply and his prayers for the Commission to (a) Note his Manifestation; (b) Hold in abeyance any clarificatory hearing pending the consideration of his Manifestation, and (c) Note his counsel's entry of appearance, are hereby GRANTED. Respondent is also ORDERED to submit his Rejoinder within ten (10) days from receipt of the Verified Reply.

On 25 November 2020, Complainant submitted a Certified True Copy from the PRC of the subject Position Paper which included the printouts of his SSS Employment History and actual premiums.

On 28 November 2020, Complainant forwarded his Reply to Respondent VVV via email. Complainant manifested that Respondent JI has not submitted a Responsive Comment, hence no Reply was prepared for her.

On 11 January 2021, the Commission received the Rejoinder from Respondent VVV.

⁵ Manifestation and Motion dated 29 July 2020, p. 2.

⁶ Motion for Extension to Comply with NPC Order filed on 4 August 2020, pp. 1-2.

On 12 January 2021, Complainant submitted to the Commission a letter from the Special Investigation Department, Investigation and Research Section.

The case is now submitted for the Commission's Resolution.

Issues

The issues in this case are follows:

- i. Whether procedural due process was observed in relation to Respondent JI; and
- ii. Whether Respondents committed unauthorized processing of Complainant's SSS employment history and actual premiums.

Discussion

i.Procedural Due Process was Observed in relation to Respondent JI.

The Commission notes that Respondent JI has not submitted any Responsive Comment to the Complaint, nor did she appear at the Discovery Conference. In that Conference, Respondent VVV manifested that he was not representing Respondent JI in this case.

According to a Certification by the courier utilized by the Commission, the Order to Submit a Responsive Comment was mailed to Respondent JI via LBC Express with a tracking number 126767817685

and consigned to JI. The address, based on the Complaint-Affidavit and the Order to Confer for Discovery, was at Laguna. The same Certification provides that on 24 July 2018, said shipment was "delivered but refused by the consignee."⁷ On 11 August 2018, the shipment was returned to the origin branch and released to the representative of the shipper on 29 August 2018.⁸

Respondent JI's refusal to accept the Order mailed by the Commission and subsequent failure to submit a Responsive Comment cannot deprive the Commission of jurisdiction over her person. The NPC Rules of Procedure⁹ provides thus:

Section 17. Failure to Submit Comment. – If the respondent does not file a Comment, the investigating officer may consider the

complaint as submitted for resolution. The respondent shall, in any event, have access to the evidence on record.

The Commission is likewise bound to dispose of cases according to its Rules of Procedure. Section 22 of its Rules provides thus:

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....

Respondent JI was given multiple opportunities to present her position against the Complaint. The Commission emphasizes that any party to a Complaint lodged in the Commission cannot refuse to accept any of its lawful Orders that were properly served to the correct address.

ii. Respondent JI Committed Unauthorized Processing Under Section 25 of the DPA.

In his Complaint, Complainant argues that his SSS personal information was disclosed by Respondent VVV to PRC without his consent and for unauthorized purposes. He asserts that the contents of his SSS personal data were not authorized and authenticated by the organization since the annexes are pictures only from a personal computer of a certain individual who has access to the SSS data portal. He also alleges that he gave no consent for Respondents to acquire the sensitive personal information they presented as evidence in the PRC case.¹⁰ He prays for moral damages for the anxiety, sleepless nights, and extreme emotional pain that this caused.¹¹

The Complainant's allegations pertain to the act of Unauthorized Processing under Section 25 of the Data Privacy Act. This Section provides thus:

SEC. 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. – (a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand thousand pesos (Php500,000.00) but not more than million pesos

⁷ LBC Certification dated 02 February 2021.

⁸ Ibid.

⁹ NPC Circular 16-04. Rules of Procedure of the National Privacy Commission. Dated 15 December 2016.

Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

(b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

As provided above, three (3) elements must be established with substantial evidence in determining whether a violation of Section 25 of the Data Privacy Act occurred:

1. The accused processed the information of the data subject;
2. The information processed was personal information and 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.¹²

A. The accused processed the personal information and sensitive personal information of the data subject.

In the Certified True Copy of the subject Position Paper submitted by Complainant JBD, printouts of his SSS Employment History and Actual Premiums are attached as Annex 2-A and Annex 2-B.¹³ In the print-out of the SSS Employment History, Complainant's full name, date of birth, and social security number are visible. There is also a list of all his previous employers, reporting dates, and employment dates.

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."¹⁴ Clearly, the Complainant's full name coupled with his employment history can reasonably and directly ascertain his identity. The Complainant's age, deduced from his displayed date of birth, and his social security number are considered sensitive personal information under the enumeration provided in

the DPA.¹⁵

In the Complaints-Assisted Form duly filled out by Complainant, he stated that he found out about the incident when he received the Position Paper last 02 March 2018. He proceeds to state that:

I have given no consent and authorization to the respondents in order for them to processed (sic) acquire these sensitive personal information presented to the Medical Technology Board as evidence. It clearly shows that they violated the Data Privacy Act of 2012- my right to secure sensitive personal information.

The DPA enumerates a series of processing activities to emphasize that it covers the different stages of the data lifecycle. Processing is defined by the DPA 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.”¹⁶

The usage of Complainant’s SSS Employment History and Actual Premiums as an attachment to a Position Paper falls within the definition of processing under the DPA.

The processing was committed by Respondent JI, but not by Respondent VVV.

In the last page of the subject Verified Position Paper is a Verification that states:

VERIFICATION

I, JI, of legal age and Filipino, after having been duly sworn to in accordance with law, depose and state THAT:

¹⁰ Id., p. 5.

¹¹ Records p. 8.

¹² NPC Case No. 17-018, Decision dated 15 July 2019.

¹³ PRC Admin Case No. 48 JBD v. JI Verified Position Paper, pp.44-45.

¹⁴ RA 10173, Section 3 (g)

¹⁵ R.A. 10173, Section 3(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 cm-rent 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.

I am the respondent in the above entitled case; I have caused the preparation of the foregoing document and I have read the same and the contents of which are true and correct of my own knowledge and / or on the basis of authentic documents.

AFFIANT SAYETH NAUGHT.

In witness whereof, I hereunto affix my signature this 2nd day of March 2018.¹⁷

(sgd)
JI
Affiant

It is clear from the foregoing that it is Respondent JI who caused the preparation of the Position Paper and determined what attachments to include to substantiate her allegations. She is the person who is considered to have processed the personal information of Complainant in this case.

The Commission likewise notes Respondent VVV's assertion in the Rejoinder, which states:

32. Respondent Atty. VVV vehemently deny (sic) any participation with regard to the subject matter being raised in the case at bar. Respondent has no means do not personally know the complainant.
xxx

34. We likewise humbly beseech this Honorable Commission that respondent Atty. VVV is not the one who caused the preparation of the pleading wherein the subject matter of this case was stemmed. Attached herewith as Annex "1" is the Verification signed by respondent JBD.

35. It should be noted that a pleading is verified by an affidavit that the affiant has read the pleading that he/she caused the preparation of the said pleading and that the allegations therein are true and correct of his/her personal knowledge or based on authentic records. Hence, it was respondent JBD who caused the preparation of the pleading which is the subject matter of the present complaint.

36. From the said discussion, the only part of respondent Atty. VVV is to be the substitute lawyer of respondent JBD and merely assist her as a normal lawyer would do. Nothing therein involves or constitutes any violation of the Data Privacy Act on the part of respondent Atty. VVV.

¹⁶ R.A. 10173, Section 3(j).

¹⁷ PRC Admin Case No. 48 JBD v. JI Verified Position Paper

The Commission finds merit in this argument by Respondent VVV. Respondent VVV merely acted under the instructions of Respondent JI as her lawyer for the PRC case. Given that it was Respondent JI who declared under oath that she is the author of the Position Paper, she was the one who committed the act of processing in this case and not Respondent VVV.

Considering that the first two (2) elements do not apply to Respondent VVV, the Complaint against him fails for a lack of cause of action.

B. The processing was done without the consent of the data subject, or without being authorized under the DPA or any existing law.

The Complainant asserts that he has “given no consent and authorization to the respondents in order for them to processed (sic) acquire these sensitive personal information presented to the Medical Technology Board as evidence.”¹⁸ Consent is defined under the DPA 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.”¹⁹

The fact that Complainant did not give his consent is not disputed by Respondent VVV, and Respondent JI did not participate nor did she submit anything to the contrary. The DPA also provides for lawful criteria other than consent to process personal information. For the subject personal and sensitive personal information in this case, the lawful criteria are found under Section 12²⁰ and 13²¹ of the law.

Respondent VVV particularly asserts that the attachment of Complainant’s SSS Employment History and Actual Claims is justified under the lawful criteria of Section 13 (f) of the DPA which allows the processing if such “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 the Rejoinder, Respondent VVV asserts thus:

41. We humbly beseech this Honorable Commission to consider that there is a case filed against respondent JBD before the

Professional Regulation Commission by the complainant for Gross Dishonorable and/or Unethical Conduct. The filing of this complaint is necessary for the protection of rights and interests of respondent JBD as she was being indicted in an administrative case. Note that the complainant claimed in his complainant (sic) before the Professional Regulation Commission that he was employed to certain companies, this is part of the complaint and being raised against respondent JBD in the said case. And this was provided by respondent JBD before the Professional Regulation Commission which is a government office. Hence, the following circumstances fall under the exception provided in Section 13(f) of RA 10173.

The Commission cannot agree with this reasoning for the benefit of either Respondent VVV or Respondent JI. While it will not go into the merits of the case in the PRC, the Commission looks into the manner the personal information was processed for its inclusion in the Position Paper.

In this case, Complainant was able to submit to the Commission a letter from the SSS Special Investigation Department – Investigation and Research Section with the following findings

¹⁸ Complaints-Assisted Form.

¹⁹ R.A. 10173, Section 3 (b).

²⁰ 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.

²¹ 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.

Initial verification from the SSS Web Inquiry (WINS) of your Actual Premiums and Employment History shows the same information provided in the questioned documents, allegedly presented by JI and VVV before the PRC.

However, the questioned documents are not certified by the PRC as the same copies as those submitted by JI and VVV. Per your assertions, these are the documents provided by JI and VVV.

Although observed to be different from SSS generated and issued printouts on its face and seems irregular, we are precluded from concluding on the matter, considering that there was no investigation conducted by this Office, as you were previously advised to file your complaint and present the questioned documents instead before the NPC, which has the proper jurisdiction on the matter.

Meantime, a careful examination of the questioned documents reveals the following, showing difference with the SSS officially issued printouts:

1. Side details are not shown as they are not fit inside the grid of the device used;
2. The font size is bigger;
3. It has shady color; and
4. Presence of the mouse cursor in one of the documents.²²

The SSS itself recognized the irregularity of the subject printouts, which puts into question the manner by which these were obtained. Underhanded or irregular processing of personal information is not what the DPA contemplates in Section 13(f).

The NPC has already ruled in a previous case that the processing of personal and sensitive personal information for the establishment or defense of legal claims under Section 13(f) must still be within the limits of the law, thus:

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.

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.²³

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.²⁴

It has been clearly established that Respondent JI processed the personal data of Complainant when she caused the inclusion of Complainant's SSS Employment History and Actual Premiums in her Verified Position Paper for an ongoing PRC case. It is undisputed that this was done without the consent of Complainant, and Respondent JI cannot rely on Section 13(f) of the DPA as her lawful criterium to process the information from the SSS because such provision contemplates processing activities that are still within the limits of the law. Such is not the case here, considering the findings of the SSS Special Investigation Department – Investigation and Research Section.

Absent any lawful criteria for the processing of Complainant's personal information in this case, Respondent JI's act of using Complainant's SSS Employment History and Actual Premiums for her Verified Position Paper in a pending PRC case constitutes Unauthorized Processing of Sensitive Personal Information under Section 25 of the DPA.

WHEREFORE, all these premises considered, this Commission hereby:

- 1. FINDS** that Respondent JI has violated Section 25 of the Data Privacy Act; and
- 2. FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice, recommending the prosecution of the Respondent for the crime of Unauthorized Processing under Section 25 of the Data Privacy Act, for its further actions.

²² Letter dated 07 January 2021. Page 1-2.

²³ Implementing Rules and Regulations of the Data Privacy Act of 2012 (hereinafter, "IRR"), § 18(b).

²⁴ Resolution, NPC Case No. 17-018. Dated 5 November 2020. Emphasis supplied.

SO ORDERED.

Pasay City, Philippines; 21 January 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

JBD

Complainant

Valenzuela City

JI

Respondent

Laguna

THE LAW FIRM BACCAY HUSSIN AND VIZCONDE

Counsel for Respondent VVV

Room 302 Cabrera Building I

130 Timog Avenue, Brgy. Sacred Heart 1103 Quezon City

ENFORCEMENT DIVISION GENERAL RECORDS UNIT

National Privacy Commission

ACN

Complainant,

-versus-

NPC 18-109

(Formerly CID Case No. 18-H-109)

For: Violation of the
Data Privacy Act of 2012

DT

Respondent.

DECISION

AGUIRRE, D.P.C.:

Before this Commission is a Complaint filed by ACN (Complainant) against DT (Respondent) for an alleged violation of the Data Privacy Act of 2012 or Republic Act No. 10173 (DPA).

The Facts

Complainant has been a licensed professional boxing judge since 22 September 2012 under the supervision and control of the Games and Amusement Board (GAB), Office of the President. He has officiated over three hundred ten (310) bouts, both local and international.¹

Complainant alleged that he has been using the name “ACN-1” on the records of Boxrec.com, an online repository and record keeper of all boxing matches around the world, including data of boxers, referees, judges, among others.² Complainant states that boxing organizations rely mainly on Boxrec.com, and this is where the experience, capacity and competence of boxing officials are assessed.

He further states that the records in Boxrec.com serve as their service record.³

¹ Records, p. 1.

² Ibid.

³ Ibid.

The Complaint-Affidavit further states:

7. On 19th August 2018, Mr. DT without my consent, modified and altered my personal details – my BOXREC name – was changed to my birth name (from ACN-1 to ACN). I did searched (sic) for it myself last Monday 20 August 2018 and it yielded a negative result....

8. I suffered sleepless nights, anxiety and panic as I thought my whole record in boxing has been lost.

9. That after this I contacted another editor to “fix” this issue as I was surprised how this has happened....

10. On Monday night I was informed that my name has been re-stored back to its original state and that the responsible person of modifying and altering my name was Mr. DT, an editor of Boxrec... and his capacity to change data within that site.

On 05 December 2018, the parties were ordered to confer for discovery at the DICT Office, Morgan Street, Port Area, Cebu City. No settlement was reached during the discovery conference.

On 17 December 2018, counsel for Respondent submitted by email its Entry of Appearance with Motion. In the same email, Respondent submitted his Position Paper dated 12 December 2018 as a responsive comment to the Complaint. A copy of the of the Entry was later filed through email and special courier.

In the Position Paper, Respondent stated that he is one of the editors of www.boxrec.com, which is responsible for keeping the records of all boxers, referees and judges updated and accurate.⁴ Respondent admitted that sometime in August 2018, in the performance of his functions, he updated several information contained in boxrec.com including that of Complainant's registered name, “ACN-1” to his birth name which is “ACN”.⁵ Respondent stated that, upon his discovery of the updating of his name to his birth name last 20 August 2018, Complainant contacted another editor of www.boxrec.com to address the issue. On the same day that Complainant discovered the update, the other editor of boxrec.com restored Complainant's registered name back to “ACN-1”.⁶

⁴ Records at. 6

⁵ Ibid.

⁶ Ibid.

Respondent refuted Complainant's allegation that "to change ACN-1 into another name will render the search negative, and will result in fewer job opportunities, as it will show that I have no officiating record." In his Position Paper, Respondent stated that:

Complainant's job assignment as boxing judge emanates from the Games and Amusement Board and the boxing bodies such as the World Boxing Organization (WBO), International Boxing Federation (IBF), World Boxing Federation (WBF), World Boxing Foundation (WBF), among others. The GAB and the boxing bodies were the ones who issued licenses to the complainant as part of their pool of boxing judges. Before he was granted licenses by these offices or associations, his credentials and boxing officiating record was evaluated and scrutinized. GAB and these boxing bodies assign the complainant as judge because he was already licensed by them. If GAB (sic), these boxing bodies and any other future boxing organization which the complainant will apply (for) a license wants to check the officiating records of the complainant, they can easily search on the same website any name of the boxers or search the date of any boxing event that he has officiated previously and he could have easily discovered that his name is still listed as one of the judges in these fights.

We also want to emphasize that GAB and all boxing bodies have a copy of the complainant's passport issued by the Philippine Department of Foreign Affairs based on the foreign travels of the complainant which GAB and these boxing bodies have endorsed and processed, as the case may be. Hence, GAB and the boxing bodies know that the birth name of complainant is "ACN".⁷

In his Reply to the Respondent's Position Paper dated 27 December 2018, Complainant emphasized that the change of his name in Boxrec.com was without his consent. He alleged that:

10. On 19 August 2018, Mr. DT without the Complainant's consent, modified and altered his personal details – his BOXREC name – was changed (sic) to his birth name (ACN-1 to ACN).

11. [T]his unauthorized changing of name is already an admission that he processed complainant's personal information WITHOUT HIS CONSENT.⁸

⁷ Position Paper dated 12 December 2018.

⁸ Records at 7.

On the basis of this, Complainant alleged that Respondent violated Section 16 of the DPA, which pertains to the Rights of the Data Subject. In his Reply, Complainant prayed for the following:

WHEREFORE, complainant ACN pray (sic) that this Honorable Commission renders judgment finding respondent DT guilty of unauthorized access or intentional breach which carries a fine of Five Hundred Thousand Pesos (Php 500,000.00).

Moral damages in the amount of Five Hundred Thousand Pesos (Php 500,000.00).

Actual damages and cost of suit in the amount of One Hundred Thousand Pesos (Php 100,000.00).

Respondents (sic) further pray for such other relief that may be deemed just and equitable under the premises.⁹

In a Rejoinder dated 11 February 2019, Complainant reiterated the same allegations stated in his Reply, thus:

BAD FAITH OR MALICE IS NOT NEEDED TO VIOLATE REPUBLIC ACT 10173 OR DATA PRIVACY ACT OF 2012

2. The data privacy act of 2012 or Republic Act 10173 particularly Sections 29 and 31 punishes both intentional and unintentional breach of the data privacy act.

3. Clearly there was malice in this case, the unauthorized change affected the livelihood of complainant, by changing the name ACN-1 to ACN will cause a negative search results on boxrec.com resulting to lost job opportunities as boxing stakeholders will not be able to find the complainant's name there.¹⁰

On 05 February 2020, Complainant filed a Motion to Render Judgment.

Issues

1. Whether the complaint may be dismissed for non-exhaustion of remedies;
2. Whether Respondent is liable for unauthorized access or intentional breach under Section 29 of the DPA; and

⁹ Id., at 21-22
¹⁰ Id., at 25-26.

3. Whether Respondent is liable for malicious disclosure under Section 31 of the DPA.

Discussion

The complaint may be dismissed for non-exhaustion of remedies.

Section 4 of NPC Circular No. 16-04 (Rules of Procedure) provides the rule for the exhaustion of remedies:

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 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 controller within fifteen (15) days from receipt of information from the complainant;...¹¹

In this case, the Complainant stated in his Complaint-Affidavit that his concern was addressed by the representatives of Boxrec.com immediately after it was raised. Respondent, in his Position Paper, even alleged that the restoration of Complainant's name from "ACN" was restored to "ACN-1" on the same day. This was not refuted by Complainant in either his Reply or Rejoinder. Based on these, Complainant's main concern of allegedly being unsearchable on Boxrec.com was addressed soon after the concern was raised.

The Commission reiterates 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.

While the same Section in the Rules of Procedure provides for exceptions to the requirement of exhaustion of remedies,¹² the Commission finds that there is neither a serious violation of the DPA nor a risk of harm to the affected data subject present in this case to warrant the waiving of the requirement.

Respondent is not liable for unauthorized access or intentional breach

under Section 29 of the DPA.

In his Complaint-Affidavit, Complainant alleged that the Respondent amended his information in the Boxrec.com website without his consent in violation of Section 16 of the DPA:

11. Having no idea about his motive/s behind this malicious act, I come to you to file this FORMAL COMPLAINT against this person.

Under the Data Privacy Act of 2012 (Republic Act 10173), specifically Chapter IV Sec 16 which partly reads “... Any information *supplied* or declaration made to the data subject on these matters *shall not be amended without prior notification of data subject...*”

12. And having done this amendment to my private confidential BOXREC record without my prior consent is in fact violative of RA 10173 and as a result have put me in a disadvantaged position basically on the thought that he can just tinker with my personal data without me knowing it? What if I haven’t known it quickly enough? I would have been “inexistent” without my knowledge? Worst, what if he decides to put it onto another name altogether? That would be a disaster to me and my career as a boxing judge.¹³

In his Reply to Respondent’s Position Paper, the Complainant alleged that the unauthorized changing of his name constitutes processing of his personal information without his consent:

10. On 19 August 2018, Mr. DT without the Complainant’s consent, modified and altered his personal details – his BOXREC name – was changed to his birth name (from ACN-1 to ACN).

11. This fact is readily admitted by respondent in paragraph 4 of his position paper where he said it was in the performance of his function as an editor of www.boxrec.com that he updated several information and updated complainant’s registered name “ACN-1” to his birth name, “ACN”. This unauthorized changing of name is already an admission that he processed complainant’s personal information WITHOUT HIS CONSENT.¹⁴

11 NPC Circular 16-04 dated 15 December 2016, Section 12. Emphasis supplied.

12 See, NPC Circular 16-04 dated 15 December 2016, Section 12.

13 Complaint-Affidavit dated 24 August 2018.

14 Reply to Respondent’s Position Paper dated 27 December 2018.

Further, in Complainant's Rejoinder, he stated thus:

5. There was never any consent from the data subject, ACN to change his personal information his name (sic) from ACN-1 to ACN.

xxx

6. It is clear that respondent modified and tampered the "Personal Information" of complainant. 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.

THERE WAS AN INTENTION TO MAKE ACN'S PROFILE
INVISIBLE TO PROSPECTIVE EMPLOYERS NO MATTER
HOW SHORT OF SPAN OF TIME

7. The complainant was not informed or consented to the change in his personal information or nickname in boxrec.com. The actions of Respondent in changing the name and start date of complainant's career as a judge is unlawful and a violation of his rights as a data subject.¹⁵

The pertinent provision on unauthorized access or intentional breach in the DPA provides:

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.

For a person to be held liable under this provision, the following elements must be met:

¹⁵ Records at 26-29.

1. The data system stores personal or sensitive personal information;
2. The accused breaks into the system; and
3. The accused knowingly and unlawfully broke into the system in a manner which violates data confidentiality and security of the same.

The allegations of both parties reveal that the second and third elements are not present in this case. Respondent did not break into the system of Boxrec.com much less did it in a manner that violates the data confidentiality and security of the same.

In his Complainant-Affidavit, Complainant admits that Respondent is an editor of Boxrec.com, thus:

On Monday night I was informed that my name has been restored back to its original state and that the responsible person of modifying (sic) and altering my name was Mr. DT, an editor or Boxrec... and has the capacity to change data within that site.¹⁶

Respondent likewise stated in his Position Paper that:

Respondent DT is an editor of www.boxrec.com, a free-of-charge and public website which keeps records of all boxing bouts worldwide including records of boxers, referees and judges. One of his functions as such is to keep records of said boxers, referees and judges. One of his functions as such is to keep records of said boxers, referees and judges, including that of complainant, update and accurate.¹⁷

It is therefore undisputed that, as an editor of Boxrec.com, Respondent's access to the database of the website is lawful. Respondent, therefore, cannot be held liable for unauthorized access or intentional breach under Section 29 of the DPA.

On the Complainant's assertions that he did not give his consent to his name being updated on the website, it must be clarified that the lack of consent did not change the nature of Respondent's access and make it unlawful all of a sudden.

¹⁶ Id., at 2, Emphasis supplied.

¹⁷ Id., at 5.

The information involved in this case is the name of the Complainant which is classified as personal information.

The Commission takes this opportunity to stress that consent is not the only lawful basis to process personal or sensitive personal information under the DPA. Even a cursory look at Sections 12 and 13 of the DPA will show that there are other lawful criteria to process personal information and sensitive personal information aside from consent.¹⁸

In describing the nature of Boxrec.com, Complainant explains that it is “an online repository, record keeper of all boxing matches around the world, including data of boxers, referees, judges, among others...”¹⁹

As the “online record keeper of the sport of boxing,” Complainant should have known that Boxrec.com updates the information on its website as a matter of course even without the consent of boxers, referees, and judges.²⁰ This is part of its legitimate interest and is an integral part of maintaining its credibility as the official record keeper for the sport of professional boxing.

¹⁸ 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.

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.

¹⁹ Records, p.1.

This is consistent with Respondent's allegations in his Position Paper, which state:

The information must at all times be accurate, relevant and updated for purposes for which it was processed and stored in the first place. The respondent, in processing complainant's personal information in the website of boxrec.com, merely updated the same to reflect the accurate and true name of the latter which is the aim of the website. There is no showing that respondent tried to tamper or to attribute the credentials of the complainant to another person or to completely delete the latter's personal information in (sic) the website.²¹

Respondent is not liable for malicious disclosure under Section 31 of the DPA.

The Complainant also alleged that Respondent should be liable for Malicious Disclosure. Section 31 of the DPA provides:

SEC. 31. Malicious Disclosure. – Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to 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).

Malicious disclosure is committed when:

1. The accused is a personal information controller or a personal information processor or any of its officials, employees or agents;
2. The accused made a disclosure of information;
3. The information disclosed was unwarranted or false information;
4. The information relates to any personal information or sensitive personal information;
5. The information was obtained by the accused; and
6. The disclosure was made with malice or in bad faith.²²

²⁰ "BoxRec About Us" page available at: [Boxrec.com/en/about](https://boxrec.com/en/about), last accessed on: 24 June 2021.

²¹ Id., at 9.

It is important to note that the Respondent altered Complainant's personal information by changing his registered nickname "ACN-1" to his birth name "ACN."

In relation to the third element, the Commission finds that the change made by Respondent involved neither unwarranted nor false information on the records of Complainant. On the contrary, it was Complainant's actual name that was made to appear on the website.

Furthermore, for Section 31 of the DPA to apply, the sixth element of malice or bad faith must be present.

The Supreme Court defines malice as one which "connotes ill will or spite and speaks not in response to duty but merely to injure the reputation of the person defamed, and implies an intention to do ulterior and unjustifiable harm."²³

In this case, Complainant did not present any evidence to support his allegations that Respondent acted with ill will, spite, or any intention to do unjustifiable harm. The Supreme Court has ruled in several occasions that mere allegations do not constitute proof:

In administrative proceedings, the quantum of proof necessary for a finding of guilt is substantial evidence, which is 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. Likewise, charges based on mere suspicion and speculation cannot be given credence.²⁴

On the other hand, Respondent sufficiently explained in his Position Paper that there was no "intention to do ulterior and unjustifiable harm," thus:

We would also want to emphasize that GAB and all boxing bodies have a copy of the complainant's passport issued by the

²² NPC 19-605, 05 November 2020.

²³ Delgado v. HRET, G.R. No. 219603, 26 January 2016.

²⁴ BSA Tower Condominium Corp. v. Reyes, II, A.C. NO. 11944, 20 June 2018.

Philippine Department of Foreign Affairs based on the foreign travels of the complainant which GAB and these boxing bodies have endorsed and processed, as the case may be. Hence, GAB and the boxing bodies know that the birth name of complainant is “ACN”.

In short, the change or update neither harmed nor caused any damage to the complainant. His record with the website is intact after all. The seeming anxiety, worry and fear of the complainant were not caused by the action of the respondent, by any stretch of the imagination.

Without the presence of the essential elements of Sections 29 and 31 of the DPA, the Complaint against Respondent must be dismissed.

WHEREFORE, premises considered, this Commission resolves that the instant Complaint filed by ACN against DT is hereby **DISMISSED**. The prayer for actual and moral damages is likewise **DENIED**.

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:

ACN

Complainant

EPE

ENRIQUEZ & QUIAMBAO

Counsel for Respondent

DT

Respondent

COMPLAINTS AND INVESTIGATION

DIVISION ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

RLA

Complainant,
-versus-

NPC 18-010
(Formerly CID Case No. 18-D-010)

For: Violation of the
Data Privacy Act of 2012

PXE

Respondent.

DECISION

LIBORO, P.C.:

Before this Commission is a Complaint filed by RLA (Complainant) against Respondent PXE for violation of the Data Privacy Act of 2012 (“DPA” or “Data Privacy Act”) when it published the Complainant’s personal information in its White Pages without the consent of the Complainant.

Facts¹

Complainant alleged that he was a regular employee of KPI (KPI) and that he was provided a PXE Digital Subscriber Line (DSL) subscription as part of his employment package. Further, that on 12 January 2016, he filled out a PXE DSL subscription application form that was submitted to Respondent to activate the DSL facility installed at his then residence at Las Piñas City.

On 12 April 2016, Complainant requested the same DSL facility to be transferred to his new residential address also at Las Piñas City.

Complainant narrated that on 21 March 2018, someone called and looked for him through his PXE-issued landline number that was bundled together with the DSL subscription.

The caller allegedly wanted to offer some products to KPI. The caller told him that she obtained his number and address from PXE’s telephone directory – the White Pages.

Alarmed, Complainant called PXE’s hotline number and sent an email to smecare@PXE.com.ph to inquire why his number and address were published in their directory without his consent.

¹ Fact-Finding Report dated 13 October 2020.

The PXE customer service representative mentioned that Complainant's telephone number was tagged as confidential in PXE's system.

Complainant sent another email to smecare@PXE.com.ph for further clarification why his personal information was published in PXE's telephone directory. The customer service representative told Complainant that the involved number has been tagged as published in PXE's telephone directory listing since it was not requested as confidential via customer information form upon application. Complainant stated that there was no such option on the application form. Acting on Complainant's concern, PXE's agent replied that his personal information would be tagged as confidential and will no longer be published in the 2018 telephone directory. Complainant avers that the agent's response supports his allegation that his personal information was originally published and was not treated as confidential.

Complainant asserted that PXE's disclosure of his personal information was done without his consent and it poses great risk to his security and to his family. He further claims that his father's life was in danger and as a proof he adduced DSWD Certificate. According to the Complainant, he must protect his father's welfare at all cost, including keeping his personal information confidential, even from their relatives and friends.

On 04 July 2018, this Commission, through the Complaints and Investigation Division (CID), conducted a Discovery Conference where both parties appeared. Both parties requested for continuance of their discussion of the case.

On 11 August 2018, another Discovery Conference was conducted. This time, the parties manifested that they are both willing to enter into an amicable settlement. Thus, they were given a period of fifteen (15) days from the date of the Discovery Conference or until 26 August 2018 to submit a notarized Compromise Agreement. However, the parties were unable to settle the case amicably within the given time.

On 05 October 2018, PXE filed its responsive Comment. PXE argued that it is mandated by law to issue a listing directory of the names, addresses, and telephone numbers of all its subscribers. The publication of Complainant's personal information was done in the performance of its mandate under existing Philippine laws.

In particular, PXE stated that under Section 149 of Commonwealth Act No. 146, otherwise known as the Public Service Act, PXE, as an

entity operating a “telephone public service” is required, at least once a year, to issue a listing directory showing therein the names of all subscribers, together with their addresses, telephone numbers and such other information as may of interest to subscriber’s everyday use of his telephone. In compliance with its obligations under the laws and regulations mentioned above, PXE implemented its internal rules that was approved by the Public Service Commission in 1970.

PXE also contended that it was merely acting upon the instructions of its customer, KPI, which was the personal information controller of the Complainant’s personal information. It explained that PXE is in the business of providing communication services to corporations. PXE transacts with corporate/group clients/customers even if the ultimate recipients of the communication services it provided are individual persons connected to the corporate clientele. In PXE’s process, the corporate clients/customers provide the required information of the end-user to facilitate the rendition of services, among others.

The relevant subscription agreements/contracts were unequivocally signed between PXE and KPI. KPI, as a corporate client of PXE, was the provider of DSL subscriptions for the benefit of its employees including the Complainant. In other words, it was KPI that applied for a corporate DSL account with PXE on behalf of Complainant. Moreover, the required application form was made in the name of KPI and from PXE’s perspective, it appeared that Complainant had no participation in accomplishing the forms. Considering that the application involved was a corporate account, PXE published the details indicated in the application form in the White pages – Government and Business Book 2017.

PXE elaborated that the terms and conditions of the application form stated that it shall provide its telephone services in accordance with the rules and regulations issued by other appropriate government agencies. It is KPI, as a corporate subscriber of PXE’s services, which has the option to decide whether to publish the names, addresses and telephone numbers provided in the DSL subscription application form.

PXE further argued that KPI as the personal information controller of Complainant, has the duty to ensure that the rights of Complainant as a data subject are upheld. KPI was responsible for ensuring that Complainant gave his informed consent to the processing of his personal information. KPI should have informed Complainant of its option not to be listed in the directory for publication and relay the chosen option to PXE as the

personal information processor. However, KPI never requested from PXE not to publish Complainant's personal information. Had KPI clarified with PXE that Complainant intended to keep his personal information confidential, PXE would have complied.

For PXE, no breach was concealed because the publication of Complainant's information was made under legal compliance and was known to KPI. PXE explained that intentional breach is committed when a person knowingly and unlawfully violates data confidentiality and security data systems or breaks into system where personal and sensitive personal information are stored. Complainant also failed to show how PXE unlawfully obtained his personal data, as it obtained his personal information under its agreement with KPI.

PXE raised that Complainant has no proof of actual threat of abduction on his father and that the publication of his whereabouts caused security risks to the safety of his family. He failed to show how the publication of directory risked the safety of his family because his whereabouts can be easily known on his and his family's posts on Facebook, all set to public mode. Such act is contrary to his claim that he and his family were in hiding from the abductors of his father.

As remedial action, PXE updated the DSL application forms for corporate accounts and the relevant internal rules in processing such accounts.

PXE took immediate action to reinforce its procedure for handling customer cases and concerns on data privacy and protection.

On 05 October 2018, Complainant in his Reply argued that PXE's statutory obligation to automatically publish their subscribers' personal information even without prior consent of the data subject is a clear violation of National Telecommunication Commission (NTC) Memorandum Circular No. 05-06-2007, known as Consumer Protection Guidelines, and the Data Privacy Act.

Complainant gave his consent to his employer, KPI, only for purpose of availing the DSL facility at his residence as part of the employment privilege. Had he known that his information will be published, he would have stopped the processing of his application.

Complainant also stated that KPI was not aware that PXE can automatically

decide to publish the subscriber's personal information since its request to PXE was only to install the DSL facility. The option not to publish its subscribers' personal information is nowhere to be found on the application form. He also alleged that the terms and conditions at the back of the application form is not readable and it is not indicated that the personal information will be processed for public disclosure.

In a meeting with PXE's Data Privacy Team on 13 July 2018, Complainant presented the police report, DSWD certifications and court cases indicating that his father's life was threatened due to the exposure of their address. During the said meeting, PXE, through its Chief Data Privacy Officer, offered an immediate option to change his telephone number or a CCTV be installed at Complainant's existing residence. Complainant perceived these offers as a recognition on the part of PXE of the severity of Complainant's situation.

Complainant justified that his posting of pictures on social media was for their friends and relatives, who were unable to visit or talk to them personally for security reasons. Furthermore, Complainant also alleged that he used aliases on his social media account to protect his identity and the pictures were taken outside

Complainant's present residence. Complainant believes that his father should neither be deprived of his liberty to enjoy life with his family nor be locked in a certain place.

Complainant alleged that he and his father relocated several times after the abduction of the latter. After some time, Complainant needed to relocate his father to a different place to secure his safety. However, when PXE published his address in its White Pages, Complainant knew that his safety and that of his father were jeopardized after somebody called his landline telephone to verify his name and residential address as seen on the PXE's White Pages. Complainant believed that the publication of his personal information can never be corrected because it can no longer be recalled from the public. The only remedy he had in mind was to relocate again to another place.

Due to such publication, Complainant accused PXE of violating the following provisions of the DPA:

- a. Section 28 for Processing of Personal Information and

Sensitive Personal Information for Unauthorized Purposes, when Complainant was not informed of the purpose for processing his personal information and to whom said information will be disclosed;

b. Section 29 for Unauthorized Access or Intentional Breach, when Complainant's personal information was published intentionally and knowingly published even with the presence of the prevailing law under National Telecommunication Commission and Data Privacy Act;

c. Section 30 for Concealment of Security Breaches Involving Sensitive Personal Information, when PXE's customer service representative told Complainant that his personal information was already tagged as confidential during his

initial inquiry in March 2018 when it only started to be confidential for their June 2018 publication; and

d. Section 32 for Unauthorized Disclosure, when Complainant's personal information was published in PXE's White Pages without his consent.

Complainant prayed for actual damages representing the cost of their several relocations to safeguard their welfare and for moral damages representing the mental anguish, fright, anxiety, sleepless nights, and emotional stress caused to the Complainant for jeopardizing the safety of his family due to the disclosure of their exact address.

Issue

Whether or not the publication of Complainant's personal information particularly, his name and residential address, in the White Pages by PXE, is in violation of Sections 28, 29, 30 and 32 of the Data Privacy Act.

Discussion

The Complainant's contentions are partly meritorious.

I. Personal data is involved and PXE is a personal information con-

troller

The facts establish that the name, telephone number and residential address were published in PXE's 2017 telephone directory, also called as White Pages.

Under the Data Privacy Act, 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

The name, telephone number and residence address of Complainant are considered personal information under the DPA because his identity is apparent based on the given information. PXE, as the entity holding his mentioned personal information, can also directly ascertain his identity therefrom.

Furthermore, under the Data Privacy Act, a personal information controller (PIC) is defined 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, hold, process, use, transfer or disclose personal information on his or her behalf."³ Meanwhile, personal information processor (PIP) is "any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject."⁴

In this case, the Complainant's personal information, as found in the PXE application form, was supplied by his employer, KPI. The subscription was named under KPI for the account of Complainant. This is also supported in the customer conforme portion of the form where Mr. BCA, President and General Manager of KPI, is the signatory in the application form. KPI's address is also indicated in the billing portion of the form. KPI, being the corporate customer of PXE, supplied to the latter the personal information of their employees who will be provided with PXE's services as part of employment benefits.

However, it is PXE that decided what information were collected from KPI's employees, including that of the Complainant, to

apply for PXE's services. KPI merely supplied the personal information of its employees to PXE, but the control over the personal information provided remained with PXE.

PXE processed the personal information of the Complainant for the purposes of DSL subscription and publishing of personal information in the White Pages. Thus, PXE, for the purposes discussed about above, is the PIC and not simply the PIP.

II. PXE's violation of the Data Privacy Act

a. Processing of Personal Information for Unauthorized Purposes

Section 28 of the DPA penalizes processing of personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws, to quote:

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.** (Emphasis and underlining supplied)

To be held liable under section 28 the PIC/PIP must process personal data in violation of the purpose consented to or authorized by the data subject, or otherwise authorized by the DPA or under existing laws.

Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the

² Republic Act No. 10173, Section 3 (g).

³ Republic Act No. 10173, Section 3(h).

⁴ Id., at Section 3(i).

collection and processing of his or her personal, sensitive personal, or privileged information.⁵

When the processing of personal information is based on consent, the PIC must obtain the consent in relation to the declared purpose for processing. The consent must likewise be evidenced by written, electronic or recorded means.⁶

In this case, the recorded means that manifest the consent of the Complainant is PXE's Application Form⁷ and the attached PXE's Terms and Conditions that was printed on the back of the Form.⁸ We note however, that while the Terms and Conditions discuss the contractual relations that govern the usage, grant and maintenance of the DSL services between the Complainant and PXE, the same does not include authority or consent to publish the list of names, contact information and address in the White Pages.

Thus, we find that the consent given by Complainant in filling up the application form relates only to the use and limitations of the DSL services offered by PXE, and not as to the publication of Complainant's personal information in the White Pages. Stated simply, the processing by PXE was done for purposes not authorized by Complainant.

This being the case, we now come into the determination on whether PXE processed Complainant's information in conformity with the DPA and other existing laws.

The Data Privacy Act, as a general rule, allows for the processing of personal information when at least one criterion for lawful processing under Section 12⁹ is present, 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:

(a) The data subject has given his or her consent;

⁵ Section 3 (b), Data Privacy Act of 2012

⁶ Id.

⁷ Records at pp. 3

⁸ Records at pp. 4

(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;

X X X

PXE argued that it is required to publish the personal information of Complainant pursuant to a legal obligation as required by Commonwealth Act No. 146, otherwise known as the Public Service Act, which has been amended by Commonwealth Act No. 454 which provides for the regulation of public services, specifically wire and wireless communication.

Revised Order No. 1 or the Public Service Commission Rules and Regulations for all Public Services was further enacted to implement the Public Service Act. Section 149 of Revised Order No. 1 clearly mandates each telephone public service to issue a listing directory at least once a year, to wit:

Telephone Directory. – Each telephone public service shall at least once a year issue a listing directory showing therein the names of all subscribers arranged in alphabetical order, their addresses and telephone numbers and such other information as may be of interest to a subscriber’s everyday use of his telephone. Each subscriber shall be entitled to a free copy of the directory.

Based on the above-cited provision, PXE as provider of telephone services to the public has authority to publish Complainant’s name, address, and telephone number. The processing of Complainant’s personal information, particularly, the publication of his personal information in the directory, is allowed under the rules and regulations issued for implementing the Public Service Act.

In relation to such directive, the NTC issued Memorandum Circular No. 05-06-2007 dated 08 June 2007, stating that the consumers or subscribers of telecommunication operators shall be given the option not to be listed in the publication:

⁹ Emphasis and underlining supplied.

Section 2.2-Any data supplied by the consumer shall be treated as confidential by the entity or service provider mentioned under Section 1.1 hereof and shall not be used for purposes not authorized by him. Upon subscription, he shall be informed of his right to privacy and the manner by which his data would be protected. In cases where a public directory listing of subscribers is regularly published by the service provider, the consumer shall be given the option not to be listed in succeeding publications.

This effectively subjected Section 149 of the Public Service Commission Rules and Regulations for all Public Services to the condition set forth by NTC Memorandum Circular No. 05-06-2007 dated 08 June 2007. While the telephone service provider has the duty to publish yearly telephone directory, it now has the correlative duty to do so in a manner that upholds the data subject's rights to data privacy.

In NPC Advisory Opinion No. 18-021, the NPC Privacy Policy Office (PPO) was sought to clarify the claim of PXE that its "base of customers whose details have been printed have not expressly provided their consent to print their details in the existing DPC White Pages that meet the standards of a valid consent as contemplated by the DPA and DPA IRR."

Upon evaluation, the NPC-PPO opined that subscribers have the right to decide whether they want their name, address, and telephone number to be listed and included in the directory for publication. Hence, the NPC recommended the strict implementation of the said NTC Memorandum Circular.

Pieces of evidence at hand, particularly the PXE Application Form¹⁰ that was submitted by KPI on behalf of Complainant on 12 January 2016 to PXE, revealed that said form did not include an option to be excluded from the public directories published by PXE.

Without such option, the data subjects such as Complainant will not have an opportunity to give their consent to the publication of their personal information in public directories.

PXE likewise argued that the processing of personal information of Complainant is necessary and is related to the fulfillment of a contract with the data subject.

A cursory reading of the Subscription Form¹¹ and PXE's Home DSL Terms

and Conditions¹² reveal that the publication of Complainant's personal information is not necessary nor related to the application and subsequent grant of the DSL services. On the contrary, the contract between PXE and its subscribers primarily relate to the use of the DSL services. This being the case, this Commission finds that PXE processed the personal information of Complainant in a manner not related to the fulfillment of a contract with the data subject.

Foregoing considered, PXE has neither obtained the consent of the Complainant to publish his personal information in the White Pages, nor it is otherwise authorized under the Data Privacy Act or any existing law. Hence, PXE is liable for violating Section 28 of the DPA.

b. Unauthorized Access or Intentional Breach

Unauthorized Access or Intentional Breach can be committed, under Section 29 of the Data Privacy Act, by 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.

The violation of this provision entails the following elements:

1. The existence of a system where personal and sensitive personal information is stored; and
2. That a person breaks in any way into the system knowingly and unlawfully, or by violating the confidentiality and security of data systems.

Here, the Complainant failed to prove that PXE or any of its agents accessed his personal information knowingly and unlawfully, or by violating the confidentiality and security of data systems. No proof was adduced showing that PXE's customer service representatives knowingly and unlawfully, or violating the confidentiality and security of data systems, broke into PXE's data storage system. Rather, the White Pages is a document that is readily available for public access.

Absent is the element of breaking into any system storing personal information. Thus, PXE cannot be found to have committed unauthorized access or intentional breach.

¹⁰ Records at pp. 3.

¹¹ Id.

¹² Records at pp. 3

c. Concealment of Security Breaches Involving Sensitive Personal Information

Concealment of security breaches involving sensitive personal information can be committed, under Section 30 of the Data Privacy Act, by persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 30 (F), intentionally or by omission conceals the fact of such security breach.

For a PIC or PIP to be liable under said section, it is necessary that the breach involved sensitive personal information, or the breach refers to a nature of breach characterized by Section 20 (F) of the DPA, to wit:

(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 (bat such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. (Emphasis supplied)

X X X

Records established that Complainant's name, telephone number and residential address are involved.

As to the first requirement: the breach concealed involves sensitive personal information. We note that the details disclosed in

the White Pages are not included in the enumeration of sensitive personal information¹³ explicitly provided by the DPA.

Corollary to this, there is likewise nothing in facts and circumstances will establish that the above-mentioned details will enable identify fraud against Complainant and warrants immediate notification by PXE.

This Commission would like to emphasize that name of Complainant, as published in the white pages is "KPI Philippines Inc Fao RLA" Read plainly, we find that the published name is not a direct and accurate representation of Complainant's full name. This circumstance, coupled with the fact that only the telephone number and residential addresses

were disclosed, are not sufficient to enable a third person to steal the identity of Complainant in this case.

In view of the foregoing, this Commission determines that PXE is not liable for violation of Section 30 of the Data Privacy Act.

d. Unauthorized Disclosure of Personal Information

Unauthorized Disclosure of Personal is punishable under Section 32 of the DPA which provides:

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 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

Section 32 of the DPA penalizes disclosure of personal information not falling within Section 31 of the DPA or due to malicious disclosure. To be liable under Section 32, the following elements must concur:

- a. The accused is a personal information controller or personal information processor or any of its officials, employees or agents;
- b. the accused made a disclosure of information;
- c. the information relates to personal information;
- d. the accused disclosed the information to a third party;
- e. the disclosure was without the consent of the data subject.
- f. That the disclosure was not malicious or done in bad faith.

¹³ Section 3 (I), R.A. 10173

The previous discussions establish the existence of the first, second, third, fifth, and sixth elements of unauthorized disclosure of personal information. Hence, we now determine whether the fourth element is present in this case.

Upon evaluation and adjudication, this Commission rules in the positive.

It must be noted that the copies of PXE's 2017 White Page or Directory is distributed to its subscribers. All the personal information found therein are disclosed to PXE's subscribers and to other persons who may be given a copy thereof. Persons who received a copy of said directory is considered a third party regarding the processing of Complainant's personal information. Thus, Complainant's personal information was disclosed to third parties.

With all the elements present, the Commission holds PXE liable for violating Section 32 of the DPA.

III. Criminal Liability of PXE's Board of Directors and Responsible Officers

Having established that PXE committed violations of the DPA particularly for the Processing of Personal Information for Unauthorized Purposes, and for Unauthorized Disclosure of Personal Information, this Commission now determines the criminal liability of PXE's board of directors and responsible officers.

For ready reference, we reproduce the pertinent violations of PXE as discussed above:

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. (Emphasis and underlining supplied)

X X X

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). (Emphasis and underlining supplied)

Pursuant to the aforesaid, Sections 28 and 32 of the DPA impose both imprisonment and fine for persons who commit the violations, including the PICs officials, employees or agents who caused the unauthorized processing and disclosure of personal data.

At the onset, this Commission stresses that the Data Privacy Act was enacted and devised to safeguard the right to informational privacy of individuals and to ensure free flow of information.

The State Policy behind the passage of the DPA is founded on nation-building through a data resilient Philippines. It also aims to enable Philippines as an internationally competitive body by participating in international engagements and other forms of commitments involving data privacy and protection.

Corollary to this, Sections 28 and 32 of the DPA were intended to impose exacting standards in the protection of data, and the penal liabilities thereon were intended to ensure compliance.

To this extent, in case of a corporation, the law may hold the Board of Directors and Corporate Officers of the PIC as criminally liable and may receive penal sanction for violations of the DPA when it is proven that because of their gross negligence, they allowed the commission of the crime explicitly provided in the DPA.. This is explicitly provided under Section 34 of the DPA itself, which provides: It provides that:

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.** (Emphasis supplied)

The same provision is also reflected in Section 30 of the Corporate Code of the Philippines which provides:

Section 30. Liability of Directors, Trustees or Officers. - Directors or trustees who willfully and knowingly vote for or assent to patently unlawful acts of the corporation or who are guilty of gross negligence or bad faith in directing the affairs of the corporation or acquire any personal or pecuniary interest in conflict with their duty as such directors or trustees shall be liable jointly and severally for all damages resulting therefrom suffered by the corporation, its stockholders or members and other persons. (Emphasis and underlining supplied)

In certain cases, this Commission held Corporate Board of Directors, Officials and Officers may be criminally liable for violating the provisions of the DPA where it was established that said Directors and/or officers participated in, or by their gross negligence, allowed the commission of the crime.

Corollary to the aforesaid, in the landmark case of *Ching v. Secretary of Justice*¹⁴ for criminal liability of corporations the Supreme Court explained that:

If the crime is committed by a corporation or other juridical entity, the directors, officers, employees or other officers thereof responsible for the offense shall be charged and penalized for the crime, precisely because of the nature of the crime and the penalty therefor. A corporation cannot be arrested and imprisoned; hence, cannot be penalized for a crime punishable by imprisonment. However, a corporation may be charged and prosecuted for a crime if the impossible penalty is fine. Even if the statute prescribes both fine and imprisonment as penalty, a corporation may be prosecuted and, if found guilty, may be fined.

A crime is the doing of that which the penal code forbids to be done or omitting to do what it commands. A necessary part of the definition of every crime is the designation of the author of the crime upon whom the penalty is to be inflicted. When a criminal statute designates an act of a corporation or a crime and prescribes

¹⁴ *Ching v. Secretary of Justice*, G.R. No. 164317, [February 6, 2006], 517 PHIL 151-178

punishment therefor, it creates a criminal offense which, otherwise, would not exist and such can be committed only by the corporation. But when a penal statute does not expressly apply to corporations, it does not create an offense for which a corporation may be punished. On the other hand, if the State, by statute, defines a crime that may be committed by a corporation but prescribes the penalty therefor to be suffered by the officers, directors, or employees of such corporation or other persons responsible for the offense, only such individuals will suffer such penalty. Corporate officers or employees, through whose act, default or omission the corporation commits a crime, are themselves individually guilty of the crime.

Since a corporation, like PXE, can only act through its Board of Directors, Corporate Officers, and employees, these DPA violations must have been committed by the Board of Directors, Corporate Officers, or employees of PXE either directly or through their gross negligence. Information necessary to identify these responsible officers / employees is usually within the control of the respondent PIC and not readily or easily available to the Complainant.

In this case, a thorough and meticulous investigation must be conducted to determine those liable officers who willfully or knowingly participated in, or by their gross negligence, allowed the commission of the crime. However, upon careful perusal of the evidence submitted and the Complaint itself, the information necessary to identify these liable officers or employees are not readily available. Thus, a further investigation is necessary.

In view of this, this Commission REMAND this case to the Complaints and Investigation Division for further investigation and

for the determination of the responsible officers of PXE, who by participation, negligence, or omission, allowed the violations of Section 28 and 32 of the DPA.

Complainant is entitled to the award of nominal damages

As established above, the Respondent processed Complainant's personal information for unauthorized purposes which resulted to unauthorized disclosure of Complainant's personal information in the White Pages without or against the consent of the Complainant.

However, this Commission notes that Complainant was not able to satisfactorily establish his loss, including the perceived threat of another abduction incident of his father. While evidence submitted by Complainant indicates that there was a previous abduction attempt against Complainant's father, it does not immediately follow that the publication in the White Pages would inevitably result in another abduction attempt. Hence, the threat may be more apparent than real.

As provided by the Supreme Court, in the case of *Arreola v. Court of Appeals*:¹⁵

Nominal damage is 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.

Since no present loss of any kind, substantial injury, or actual damages have been proved by Complainant, this Commission awards the nominal damages of Fifty Thousand Pesos (P50,000.00) to the Complainant.

WHEREFORE, all these premises considered, this Commission resolves to **AWARD** Complainant, RLA, nominal damages in the amount of Fifty Thousand Pesos (P50,000.00) for Respondent PXE Enterprise's violation of Complainant's rights under the Data Privacy Act.

Moreover, this Commission resolves to **REMAND** this case to the Complaints and Investigation Division for the limited purpose of determining and identifying the responsible persons, officers, or individuals of PXE Enterprise who caused the violations of Sections 28 and 32 of the DPA prior to recommending the matter to the Secretary of Justice for criminal prosecution.

SO ORDERED.

Pasay City, Philippines; 17 December 2020

(Sgd.)

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

¹⁵Areola v. Court of Appeals, G.R. No. 95641, [September 22, 1994], 306 PHIL 656-66

WE CONCUR:

(Sgd.)

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

(Sgd.)

JOHN HENRY D. NAGA

Deputy Privacy Commissioner

Copy furnished:

RLA

Complainant

PXE INC.

Respondent

Chief Data Privacy Officer

**COMPLAINTS AND INVESTIGATION
DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
NATIONAL PRIVACY COMMISSION**

FAT

Complainant,
-versus-

NPC Case No. 19-043
(Formerly CID Case No. 19-A- 043

For: Violation of the
Data Privacy Act of 2012

XXX

Respondent.

DECISION

NAGA, D.P.C.:

Before this Commission is a Complaint by FAT (Complainant) against XXX (Respondent) for unauthorized disclosure of Complainant's mobile number just a day after the scheduled turnover of the Complainant's condominium unit.

Facts of the Case

On 27 January 2019 at 4:07 p.m., Complainant filed a complaint to the Commission, viz:

“Right after the day of my scheduled turnover of my unit with XXXX, a certain ‘X’ of GLC, contacted me asking if I was interested to rent out my condominium unit. X mentioned that he got my number from a broker named ‘X’. I knew this was a breach because XXX have their own leasing services and I would expect a formal email from their official channels to offer their leasing services. No one from my family members would give out my number to an agent without my consent (only one of my sisters and my immediate manager at work knew that I was already scheduled for turnover last Saturday. Both of them wouldn't give out my number to others without my consent). My agent would not also disclose my number since she also gets commission from referring lessees to her clients' units to be rented out. From the Facebook group of ASS resident, numerous members also complained that a certain Richie contacted them right after their unit was turned over. It could only be someone from the turnover team because that ‘X’ or ‘X’ immediately contacts whoever has their unit been turned over.”

At the Discovery Conference set on 20 April 2019¹, both the Complainant

and Respondent failed to appear. Hence, the Discovery Conference was reset on 02 July 2019.²

During the second Discovery Conference on 02 July 2019, only the Complainant appeared. He manifested that he was willing to undergo the mediation process to settle the case amicably. However, considering that it was the second time that Respondent failed to appear, the latter was ordered to file its Responsive Comment, and Complainant to file his Reply within the period provided after receipt of the Responsive Comment.³

On 24 July 2019, Respondent, through its counsel, the Law Firm of HNSO, filed its Entry of Appearance with a request for a copy of the Complaint. Respondent claimed that it did not receive any order or notice prior to the Order dated 02 July 2019.

On 25 July 2019, Respondent, through counsel, filed a Motion For Additional Time To Rile A Responsive Comment in view of the insufficient time to draft a Comment and citing other equally important and crucial professional work of Respondent's counsel.

On 1 August 2019, Respondent filed its Responsive Comment. The Respondent contended that the Complaint should be dismissed outright for being filed prematurely and for lack of sufficient information to substantiate the allegations in the Complaint pursuant to Section 12 of the NPC Circular 16-04.⁴ It further stated that Complainant notified them of the Complaint at 6:15 p.m. of 27 January 2019, which fell on a Sunday, a day before he filed the same with the Commission on 28 January 2019. Respondent argued that there was no reasonable time and opportunity for them to take the appropriate action in response to Complainant's allegation of unauthorized disclosure of his personal mobile number.⁵

Respondent further asserted that Complainant did not give any material information which can substantiate his allegation that someone from Respondent disclosed his mobile number to a third party.⁶

Respondent stressed that it is not connected and has not transacted with a company named GLC. Respondent is also not knowledgeable of the person named X who contacted the Complainant. Despite the very

limited information provided by Complainant regarding the suspected unauthorized disclosure of his personal mobile number, Respondent conducted its internal investigation and interviewed its employees who are part of the sales and turnover team. It was further alleged by Respondent that the members of the sales and turnover team stated they did not know an X from GLC and that they did not disclose any personal data of clients to third parties. Respondent also claimed that the investigation shows no sign of unauthorized access or disclosure of client's personal data.⁷

It was manifested by Respondent that it has been observing the General Data Privacy Principles under the Data Privacy Act of 2012.⁸ It instills to its employees this obligation of confidentiality and respect for data privacy rights of clients when handling personal data as provided in Respondent's Employee Privacy Policy Handbook and the Data Privacy Policy. Respondent conducts data privacy awareness seminars for its employees and regularly sends them informative emails about their obligations under the DPA.⁹

No Reply was filed by the Complainant,. Hence, with no other pleadings to be submitted, the investigation of the Complaint is terminated.

Issues

1. Whether or not Respondent was given an opportunity to address Complainant's complaint, pursuant to Section 4 of NPC Circular No. 16-04 on Exhaustion of Remedies.
2. Whether or not Respondent committed unauthorized disclosure of Complainant's mobile number.

¹ Order dated 26 March 2019

² Order dated 30 April 2019

³ Order dated 02 July 2019

⁴ Responsive Comment, page 1 (1)

⁵ Id., page 2 (3)

⁶ Id., page 3 (7)

⁷ Id., page 4 (8)

⁸ Id., page 4 (10)

⁹ Id., page 4 (11)

Discussion

The Complaint lacks merit.

Respondent was not given an opportunity to address the complaint

As shown in the records, the incident occurred on 27 January 2019 at 4:07 p.m. The following day, the complaint was filed at 4:55 p.m. Respondent acknowledges the receipt of Complainant's concern on the day of the incident. However, the Complaint was filed with this Commission the very next day.

Section 4 of the NPC Circular 16-04 requires that Personal Information Controller (PIC) be afforded the opportunity and reasonable time to address the privacy concern in order to avoid indiscriminate filing of complaints; 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 ; 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.

In the present case, Respondent was clearly deprived of the opportunity to address the concern as the Complaint was filed immediately a day after it was brought to the attention of Respondent. Complainant did not give Respondent reasonable time to address and act on the alleged privacy concern. Complainant immediately brought his concern to this Commission without first ventilating all his concerns with the PIC.

The Commission may waive any or all of the requirements of abovementioned provision in NPC Circular 16-04, 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.¹⁰ However, no justifiable reason or substantial proof was presented by Complainant to persuade this Commission to warrant its waiver.

Nevertheless, in the interest of justice, this Commission deems it wise to still rule on the substantial issue raised by the Complainant herein, specifically whether the Respondent committed a data privacy violation.

Respondent did not commit unauthorized disclosure

Complainant claims that his personal mobile number was disclosed without his consent based on the speculation that considering the timing of the incident, it was from the Respondent's turnover team who disclosed his personal information. It could not be one of his sisters, his immediate manager, nor his agent as he was certain that they will not disclose his personal information without his consent.

However, no proof was submitted to substantiate this claim. Complainant failed to show a reasonable connection between X, the supposed agent from GLC, and the Respondent. Likewise, no evidence was presented that shows a connection between GLC and Respondent. Absent any evidence to support the Complainant's claim, allegations, conjectures and suppositions in the complaint, Respondent cannot be found to have committed unauthorized disclosure.

As provided by Section 22 of NPC Circular No. 16-04, "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)

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."¹¹

¹⁰ Section 4, paragraph 2 of NPC Circular No. 16-04

¹¹ G.R. No. 165585, 20 November 2013, citing *Real v. Belo*, 542 Phil. 109 (2007).

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.”¹²

Hence, bearing only allegations without any corresponding pieces of evidence to support Complainant’s claim that Respondent disclosed his personal information which gave X the ability to contact him cannot merit a favorable decision from this Commission.

In fine, this Commission sustains Respondent’s contention that the instant Complaint should be dismissed outright for being filed prematurely and for lack of sufficient information to substantiate the allegations in the complaint as provided by Section 12 of NPC Circular No. 16-04,¹³ viz:

SECTION 12. Outright Dismissal. – The Commission may dismiss outright any complaint on the following grounds:

- a. The complainant did not give the respondent an opportunity to address the complaint, unless failure to do so is justified;
- b. The complaint is not a violation of the Data Privacy Act or does not involve a privacy violation or personal data breach;
- c. The complaint is filed beyond the period for filing; or
- d. There is insufficient information to substantiate the allegations in the complaint or the parties cannot be identified or traced. (Emphasis Supplied)

WHEREFORE, all premises considered, the Complaint is hereby **DISMISSED** for lack of merit.

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; 17 December 2020.

¹² G,R No. 180364, 03 December 2014.

¹³ Responsive Comment, page 1 (1)

(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:

FAT

Complainant

HNSO

Counsel for Respondent

COMPLAINTS AND INVESTIGATION

DIVISION ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

VVC

Complainant,

-versus-

NPC 19-134

For: Violation of the
Data Privacy Act of 2012

CJB

Respondent.

DECISION

AGUIRRE, D.P.C.:

Before this Commission is a Complaint filed by VVC (VVC) against CJB (CJB) for an alleged violation of Section 25 or Unauthorized Processing of Personal or Sensitive Personal Information and Section 32 or Unauthorized Disclosure of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

On 26 February 2019, VVC filed a Complaint against CJB. VVC stated that she holds the position of Land Management Officer I of the Department of Environment and Natural Resources (DENR).¹ CJB is the Officer-in-Charge Provincial Environment and Natural Resources Officer (OIC-PENRO) in Compostela Valley.²

On 28 November 2018, CJB issued Special Order No. 11-067 reassigning VVC from the Land Management Sector to the Forest Protection Unit of the DENR.³ VVC requested CJB to reconsider since she was appointed by the Civil Service Commission (CSC) as a Land Management Officer.⁴ CJB denied VVC's request.⁵

¹ Affidavit Complaint, at 1, in VVC v. CJB, NPC 19-134 (NPC 2019).

² Id.

³ Id. Annex A.

⁴ Id. at 1.

⁵ Id. at 1.

On 05 December 2018, CJB issued Special Order No. 12-069 creating a team to investigate VVC's alleged irregular and improper conduct of desisting from reporting to the Forest Production Unit.⁶

On 17 January 2019, CJB issued a Memorandum to VVC with the subject "Show Cause Order to explain the inconsistency, improbability, and credibility of the official records of employment and school attendance of LMO I VVC."⁷ The Memorandum required VVC to explain within 72 hours the "inconsistency, improbability, incredibility of [her] official records of employment and school attendance."⁸ CJB stated the following allegations:

1. CJB received an anonymous text message alleging that there were inconsistencies in VVC's school records and employment in the DENR;
2. VVC's Personal Data Sheet (PDS) and school attendance based on his Official Transcript of Records show "incredible and improbable inconsistencies and spurious facts that may [be] tantamount to fraud, dishonesty, and misrepresentation";
3. The PDS states that VVC was employed by the DENR from July 2007 to April 2011 as Administrative Aide VI/ Project Monitoring Officer assigned at CENRO Panabo, Davao del Norte, from April 2011 to August 2021 as Administrative Aide VI/ National Greening Program Coordinator assigned at PENRO, Nabunturan, Compostela Valley, and from August 2012 to November 2014 as Administrative Aide XI/ National Greening Program Coordinator assigned at CENRO Nabunturan, Compostela Valley;
4. The Official Transcript of Records shows that VVC had perfect attendance in the regular semesters from 2009 to 2014, and that the school awarded her a Degree in Political Science;
5. It would have been improbable for VVC to attend her classes and report to DENR at the same time throughout the 4-year period since the school is 200 kilometers away from Davao City. Assuming that the school is proximate to the office, VVC is administratively prohibited from attending both office and classes at the same time; and
6. VVC openly declared that she is currently enrolled in a law school, which is contrary to the DENR policy that requires

⁶ Id.

⁷ Affidavit Complaint, supra note 1, Annex C.

⁸ Id. at 1.

employees to secure prior clearance from the DENR Secretary in order to pursue further studies.⁹

The following documents were attached to the Show Cause Order as annexes: CS Form 212 PDS, Transcript of Records, Diploma, Eligibility for Graduation issued by Commission on Higher Education (CHED), CHED Special Order, and Google map of the distance from Davao City to the school.¹⁰

In her Complaint, VVC alleges that CJB “wantonly” processed her personal files, including sensitive personal information, and furnished a copy to third parties thus violating her rights under the DPA.¹¹ VVC claims that CJB initiated an action to have her prosecuted for fraud and dishonesty based on her personal files. VVC maintains that her personal data was unlawfully processed and CJB committed Unauthorized Disclosure when the Show Cause Order was furnished to the following third parties, namely:

1. AMMD, DENR
2. DAT, Civil Service Commission
3. DRA, Commission on Higher Education
4. DVL, Civil Service Commission.¹²

On 27 March 2019, the Commission issued an Order to confer for discovery on 30 April 2019.¹³

On 30 April 2019, the parties conferred for discovery but failed to reach a settlement.¹⁴ The Commission issued an Order for the resumption of complaint proceedings.¹⁵

On 03 May 2019, an Order was issued to CJB to file a responsive comment ten (10) days from receipt of the Order.¹⁶

On 05 July 2019, CJB, through counsel, filed his Entry of Appearance with an Urgent Motion for Extension of Time to File his Responsive Comment.¹⁷

⁹ Id. Annex C.

¹⁰ Id.

¹¹ Id. at 1.

¹² Id. Annex B.

¹³ Order to Confer for Discovery, 27 March 2021, at 1, in VVC v. CJB, NPC 19-134 (NPC 2019).

¹⁴ Order, 03 May 2019, at 1, in VVC v. CJB, NPC 19-134 (NPC 2019).

¹⁵ Id.

¹⁶ Id.

¹⁷ Entry of Appearance with An Urgent Motion for Extension of Time, 05 July 2019, at 1, in VVC v. CJB, NPC 19-134 (NPC 2019).

On 15 July 2019, CJB filed his Responsive Comment.¹⁸ CJB alleged that the Complaint should be dismissed for lack of merit because his acts were in the performance of his official functions as VVC's direct supervisor.¹⁹ CJB stated that the act of furnishing copies to the third parties is part of the verification of contents of VVC's documents.²⁰ He emphasized that the PDS submitted by VVC contains a waiver and authority for the agency head to verify and validate the contents therein.²¹

On 07 August 2019, VVC filed her Answer to the Responsive Comment in response to the Comment.²² VVC asserted that the release of her PDS to offices outside the DENR violated her rights as a data subject because it contains sensitive personal information and made her vulnerable to identity theft.²³

On 16 August 2019, CJB submitted his Motion to Admit Rejoinder.²⁴ CJB reiterated his argument that as VVC's direct supervisor, it is his legal obligation to verify the legitimacy of the qualifications of his subordinate.²⁵

On 4 September 2019, VVC filed her Answer to the Responsive Rejoinder.²⁶ VVC stated that CJB acted with ill motive when he released her PDS without her consent.²⁷

Issues

1. Whether the case should be dismissed on procedural grounds for VVC's alleged failure to give CJB an opportunity to address the Complaint pursuant to Section 4 (a) of NPC Circular No. 16-04 (NPC Rules of Procedure);
2. Whether a PDS contains personal and sensitive personal information;

18 Respondent's Responsive Comment, 15 July 2019, at 1, in VVC vs. CJB, NPC 19-134 (NPC 2019).

19 Id. at 2 – 3.

20 Id.

21 Id.

22 Complainant's Answer to Responsive Comment, 07 August 2019, at 1, in VVC vs. CJB, NPC 19-134 (NPC 2019).

23 Id. at 2.

24 Motion to Admit Rejoinder, 16 August 2019, at 1, in VVC vs. CJB, NPC 19-134 (NPC 2019).

25 Respondent's Rejoinder, 16 August 2019, at 2, in VVC vs. CJB, NPC 19-134 (NPC 2019).

26 Answer to Responsive Rejoinder, 04 September 2019, at 1, in VVC vs. CJB, NPC 19 134 (NPC 2019).

27 Id.

3. Whether VVC consented to the processing of her personal and sensitive personal information;

4. Whether CJB is liable under Section 25 (Unauthorized Processing of Personal and Sensitive Personal Information) and Section 32 (Unauthorized Disclosure) when he released VVC's PDS to third parties

Discussion

The case should not be dismissed on procedural grounds. VVC expressly consented to the processing of her personal and sensitive personal information. As such, CJB is not liable under Section 25 (Unauthorized Processing of Personal and Sensitive Personal Information) and Section 32 (Unauthorized Disclosure) of the DPA.

I. The case should not be dismissed for VVC's alleged failure to give CJB an opportunity to address the complaint against him.

CJB alleges that the Commission should dismiss the case against him since VVC failed to provide him with an opportunity to address the complaint against him as required in Section 4 (a) of NPC Circular No. 16-04.²⁸ Section 4 (a) of NPC Circular No. 16-04 provides:

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 appropriate action on the same; 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.²⁹

Where circumstances permit, it is a condition precedent to the filing of complaints that the complainant gives the respondent an opportunity to address the complaint against him.³⁰ The Commission, however, has the discretion to waive any of the conditions precedent enumerated in Section 4 of NPC Circular No. 16-04 “upon good cause shown,

²⁸ Respondent's Responsive Comment, supra 18, at 1.

²⁹ 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).

³⁰ ACN v. DT, NPC Case No. 18-109 (2021).

or if the complaint involves a serious violation or breach of the DPA, taking into account the risk of harm to the affected data subject.”³¹ The Commission emphasizes that Section 4 of NPC Circular No. 16-04 speaks of “risk of harm” and does not require actual harm or damage to the complainant.³²

In this case, the complaint contains an allegation on CJB’s alleged wanton processing of VVC’s personal files, which contains sensitive personal information.³³ The nature of sensitive personal information and the risks involved in the processing of such information increases the risk of harm to the data subject. This serves as sufficient basis to give the complaint due course.³⁴

In any case, NPC Circular No. 21-01 (2021 Rules of Procedure) provides that the Commission may waive the conditions precedent when the respondent cannot provide any plain, speedy, or adequate remedy to the alleged violation:

Section 2. Exhaustion of remedies

...

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.³⁵

³¹ NPC Circular No. 16-04, § 4.

³² FGP v. Maersk, NPC Case No. 18-038 (2020).

³³ Answer to Responsive Rejoinder, supra note 26, at 1.

³⁴ MNLC v. PXXX, et al., NPC Case No. 19-528 (2020).

³⁵ National Privacy Commission, 2021 Rules on Procedure of the National Privacy Commission, Circular No. 01, Series of 2021 [NPC Circular No. 21-01], Rule II, § 2 (28 January 2021). Emphasis supplied.

The alleged privacy violation supposedly resulted from the disclosure of VVC's sensitive personal information to third parties without her consent. To require VVC to first exhaust her remedies with CJB would be unreasonable. CJB is not in a position to provide any plain, speedy, or adequate remedy to the alleged violation against VVC since the PDS has already been released to third parties. The Commission reiterates that the requirement to exhaust available remedies does not contemplate exercises in futility that only delay justice for data subjects whose rights are supposedly violated.³⁶

Given all these, the Commission waives the procedural technicalities cited by CJB and proceeds to determine if CJB violated Section 25 (Unauthorized Processing of Personal and Sensitive Personal Information) and Section 32 (Unauthorized Disclosure) of the DPA.

II. A PDS contains personal and sensitive personal information of a government official or employee.

A PDS is an official document that contains personal and sensitive personal information of a government employee or official.³⁷ A PDS contains a government official of employee's personal background, qualifications, and eligibility³⁸, which necessarily includes personal and sensitive personal information as defined by 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.

. . .

(l) Sensitive personal information refers to personal information:

³⁶ Declaro v. Declaro, et al., CID Case No. 18-D-012 (2020).

³⁷ National Privacy Commission, Advisory on Access to Personal Data Sheets of Government Personnel, Advisory No. 02, Series of 2017 (03 April 2017).

³⁸ Affidavit Complaint, *supra* note 1, Annex D.

- (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.³⁹

Further, the PDS contains an explicit authorization to allow the agency head or authorized representative to verify or validate its contents:

I declare under oath that I have personally accomplished this Personal Data Sheet which is a true, correct and complete statement pursuant to the provisions of pertinent laws, rules and regulations of the Republic of the Philippines. I authorize the agency head/authorized representative to verify/validate the contents stated herein. I agree that any misrepresentation made in this document and its attachments shall cause the filing of administrative case/s against me.⁴⁰

III. VVC consented to the processing of her personal and sensitive personal information in the PDS.

Personal information of a data subject may be processed when the data subject has given his or her consent to such processing. Section 12 (a) 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:

³⁹ 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), (l).

⁴⁰ Affidavit Complaint, supra note 1, Annex D.

- . (a) The data subject has given his or her consent;⁴¹

Sensitive personal information of a data subject, as a general rule, shall not be processed. It is only permitted when the data subject consents to such processing or any of the other lawful criteria of processing under Section 13 of the DPA is present. Section 13 (a) of the DPA allows the processing of sensitive personal information when the data subject has given his or her consent to the processing:

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:

- (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;⁴²

The DPA defines consent as follows:

Section 3. Definition of Terms. – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

...

- (b) Consent of the data subject refers to 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.⁴³

Consent of the data subject shall be: (1) freely given; (2) specific; (3) an informed indication of will; and (4) evidenced by written, electronic or recorded means.⁴⁴

⁴¹ Data Privacy Act of 2012, § 12 (a). Emphasis supplied.

⁴² Id. § 13 (a). Emphasis supplied.

⁴³ Id. § 3. Emphasis supplied.

⁴⁴ Id. Emphasis supplied.

Consent is freely given if the data subject was given a real choice on the processing of his or her personal or sensitive personal information.⁴⁵ The data subject should not have been deceived, intimidated, or coerced into consenting to the act of processing.⁴⁶

VVC consented to the processing of her personal and sensitive personal information when she signed the PDS. VVC freely gave her consent despite the fact that the PDS is a condition for employment in the government. Such consent is not invalidated by the mere fact that the PDS is a contract of adhesion. As held by the Supreme Court, contracts of adhesion are as binding as ordinary contracts since the party who adheres to the contract remains free to reject it:

A contract of adhesion, wherein one party imposes a ready-made form of contract on the other, is not strictly against the law. 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. Contrary to petitioner's contention, not every contract of adhesion is an invalid agreement. As we had the occasion to state in *Development Bank of the Philippines v. Perez*:

... In discussing the consequences of a contract of adhesion, we held in *Rizal Commercial Banking v. Court of Appeals*:

It bears stressing that a contract of adhesion is just as binding as ordinary contracts. It is true that we have, on occasion, struck down such contracts as void when the weaker party is imposed upon in dealing with the dominant bargaining party and is reduced to the alternative of taking it or leaving it, completely deprived of the opportunity to bargain on equal footing. Nevertheless, 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.⁴⁷

Indeed, VVC always had the option to not sign the PDS and consequently, to not accept employment with the DENR. Thus, VVC

⁴⁵ MNLSC, NPC Case No. 19-528 (2020).

⁴⁶ *Id.*

⁴⁷ *Cabanting v. BPI Family Savings Bank, Inc.*, G.R. No. 201927 (2016).

freely gave her consent to the processing of her personal and sensitive personal information stated in the PDS.

The PDS specifically provides that the data subject permits the agency head or authorized representative to verify or validate the contents of the PDS.⁴⁸ This shows that VVC was informed of the purpose behind the processing of her personal and sensitive personal information. By signing and agreeing to the conditions stated in the PDS, VVC indicated her consent to the processing of her personal and sensitive personal information.

IV. CJB is neither liable under Section 25 nor Section 32 of the DPA when he released the PDS to third parties.

CJB is neither liable for Section 25 of the DPA on Unauthorized Processing of Personal and Sensitive Personal Information nor Section 32 of the DPA on Unauthorized Disclosure.

CJB is not liable under Section 25 of the DPA on Unauthorized Processing of Personal and Sensitive Personal Information.

Section 25 of the DPA on Unauthorized Processing of Personal and Sensitive Personal Information provides:

Section 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. – (a) The unauthorized processing of personal information 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 process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

(b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more

48 Affidavit Complaint, supra note 1, Annex D.

than Four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.⁴⁹

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;
3. The processing was done without the consent of the data subject, or without being authorized under the DPA or any existing law.⁵⁰

In this case, CJB processed VVC's personal and sensitive personal information when he, as her direct supervisor, released the PDS to persons authorized to receive VVC's personal information by virtue of their functions as officials of the DENR, CSC, and CHED. Nevertheless, the processing was done with the consent of VVC since she signed and agreed to the conditions stated in the PDS. Absent the third requisite, CJB is not liable under Section 25 of the DPA on Unauthorized Processing of Personal or Sensitive Personal Information.

CJB is not liable under Section 32 of the DPA on Unauthorized Disclosure.

Section 32 of the DPA on Unauthorized Disclosure states:

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).⁵¹

⁴⁹ Data Privacy Act of 2012, § 25.

⁵⁰ MNL, NPC Case No. 19-528.

⁵¹ Data Privacy Act of 2012, § 32.

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.⁵² 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. 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 lawmakers, the spirit and reason of the statute may be examined to determine the true intention of the provision.⁵³

To require the consent of the data subject when some other lawful criteria such as law or regulation requires or justifies the processing of the personal information, including its disclosure, will result in absurdity.

Section 32 of the DPA on Unauthorized Disclosure should also not be read in isolation from the 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.⁵⁴

It should be read together with Sections 12 and 13 on the criteria for lawful processing of personal and sensitive personal information.

Sections 12 and 13 show that consent is but one of the lawful criteria for processing. The presence of any of the criteria listed in either section is sufficient to justify the processing of personal or sensitive personal

⁵² *Id.*

⁵³ *Metropolitan Bank and Trust Co. v. Liberty Corrugated Boxes Manufacturing Corp.*, G.R. No.184317 (2017).

⁵⁴ *Fort Bonifacio Development Corp. v. Commissioner of Internal Revenue*, G.R. Nos. 158885 & 170680 (Resolution) (2009).

information as the case may be. Such literal interpretation based on an isolated reading of Section 32 of the DPA will render Sections 12 and 13 of the DPA inoperative.

The rule is that a construction that would render a provision inoperative should be avoided; instead, apparently inconsistent provisions should be reconciled whenever possible as parts of a coordinated and harmonious whole.⁵⁵

Thus, Section 32 of the DPA on Unauthorized Disclosure should be read and understood 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. 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.”⁵⁶ This interpretation benefits the accused since it narrows the extent to which disclosure of personal information may be considered as Unauthorized Disclosure.

The requisites of Unauthorized Disclosure are:

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 neither relates to unwarranted or false information nor malicious or in bad faith.

Here, CJB disclosed VVC’s personal and sensitive personal information to third parties when he released VVC’s PDS to persons authorized to receive VVC’s personal information by virtue of their official functions. The disclosure does not relate to unwarranted or false information since

⁵⁵ JMM Promotions & Management, Inc. v. National Labor Relations Commission, G.R. No. 109835 (1993). Emphasis supplied.

⁵⁶ People v. Liban, G.R. Nos. 136247 & 138330 (2000).

true, correct, and complete information should be indicated in the PDS.⁵⁷ This disclosure was neither malicious nor in bad faith since it was done in the performance of his official functions as VVC's direct supervisor in order to verify or validate the contents of the PDS.⁵⁸ Finally, VVC consented to the disclosure of the information to third parties when she granted her direct supervisor and persons authorized to receive VVC's personal information by virtue of their official functions the authority to validate the legitimacy of the information in the PDS. Thus, CJB is not liable under Section 32 of the DPA on Unauthorized Disclosure.

Consent is a common requisite of Section 25 and Section 32 of the DPA.

Processing personal or sensitive personal information without the consent of the data subject or any other lawful criteria under Sections 12 or 13 of the DPA is a common requisite of Sections 25 and 32 of the DPA. If the data subject consents to or any other lawful criteria under Sections 12 and 13 of the DPA allows the processing of personal and sensitive personal information, then the perpetrator cannot be held liable for the offenses of Unauthorized Processing of Personal and Sensitive Personal Information or Unauthorized Disclosure.

As previously discussed, VVC consented to the processing of her personal and sensitive personal information by agreeing to the conditions stated in the PDS. In doing so, VVC granted CJB, her direct supervisor, and persons authorized to receive VVC's personal information by virtue of their official functions the authority to validate the legitimacy of the information she indicated in the PDS. Since the PDS was processed and disclosed to third parties with VVC's consent, then the necessary requisite of processing without the consent of the data subject or any other lawful criteria under Sections 12 and 13 of the DPA is absent. Hence, there is no violation of Sections 25 and 32 of the DPA and the Complaint against CJB must be dismissed.

WHEREFORE, premises considered, the Commission resolves that the case filed by VVC against CJB is hereby **DISMISSED**.

SO ORDERED.

⁵⁷ Affidavit Complaint, supra note 1, Annex D.

⁵⁸ Id.

Pasay City, Philippines. 10 December 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:

VVC

Complainant

CJB

Respondent

**COMPLAINTS AND INVESTIGATION
DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT**

National Privacy Commission

RTB

Complainant,

-versus-

NPC 21-086

For: Violation of the
Data Privacy Act of 2012

**EAST WEST BANKING
CORPORATION**

Respondent.

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:

Sgd.

JOHN HENRY D. NAGA

Privacy Commissioner

Copy furnished:

RTB

Complainant

³³ Id. § 16 (f).

³⁴ Data Privacy Act of 2012, § 7 (b).

³⁵ NPC 18-038, 21 May 2020 (NPC 2020) (unreported).

³⁶ Id.

OPBLO

Counsel for East West Banking Corporation

**COMPLAINTS AND INVESTIGATION
DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT**

National Privacy Commission



ORDER

ORDER

LIBORO, P.C.:

Before this Commission is the Data Breach Notification Report¹(DBNR) submitted by GC, Inc. (GC), through M.K., for and on behalf of GC. The DBNR is submitted in compliance with the Order issued by the Commission dated 17 October 2018.

Facts

On 17 October 2018, this Commission issued an Order to GC containing the following dispositive portion, to wit:

WHEREFORE, PREMISES CONSIDERED this commission hereby **ORDERS** GC to:

1. **SUBMIT** a more comprehensive Data Breach Notification Report to this Commission following rules laid down in NPC Circular No. 16-03;
2. **NOTIFY** the affected data subjects through an appropriate Data Breach Notification following rules laid down in NPC Circular No. 16-03;
3. **PROVIDE** identity theft and phishing insurance for affected Filipino data subjects, or in the alternative, ESTABLISH a dedicated helpdesk/help center for Filipino data subjects on privacy related matters concerning GC, located in the Philippines and with a local number, within six (6) months from receipt of the ORDER
4. **IMPLEMENT** a program in the Philippines or otherwise directed to Filipino data subjects to increase awareness in identity theft and phishing; and
5. **PROVIDE** evidence of compliance with the foregoing.

On 16 November 2018, acting on the aforesaid Order, a letter² was

submitted and was signed by M.K. for and on behalf of GC. The letter further discussed the communication and notification it made with the Filipino users, the steps already taken and further steps planned to take, the help services it provided, the educational campaign initiatives on issues of digital literacy, safety and privacy, and the evidence of compliance with the Order of this Commission.

On 29 September 2018, GC started sending a notification to all potentially affected Filipino users via an in-app important security update. This message set out an explanation of incident as understood by GC in its initial investigation, informed users that GC had contacted law enforcement, and explained the reasons and impact of GC's remedial step of resetting all potentially affected access tokens. This security update was also posted in the GC newsroom. GC also informed affected users of the steps they can take in relation to phishing and how to protect themselves from an attacker.

Starting 13 October 2018, GC updated the smaller subset of users who were found to be affected by the incident. It was done by way of tailored in-app notification that was written in both English and Tagalog. The Tagalog notification were sent to those Filipino users whose GC language was set to Tagalog on 17 October 2020. The in-app notification varied depending on the categories of information about the user that were potentially assessed during the attack. This was explained in the 'update' under the heading 'Personal data Potentially Involved'. Users fell into three (3) different groups and received different in-app notifications accordingly. This also explained what information the attackers were believed to have accessed in relation to such users. The notification also included hyperlinks to tailored Help Center pages where the affected users could find further details about the incident, updates about GC's investigation regarding the incident, and guidance on steps which the user could take to protect themselves from suspicious emails, text messages, or phone calls.

¹Data Breach Notification Report of GC dated 16 November 2018.

² Ibid.

According to GC, if the users have further questions pertaining to the incident, users are invited to follow a link from the Help Center to the GC Security Incident Response Form, through which they are able to submit questions to GC. Those who will submit question to GC will receive an email to which they can reply with any inquiry in their preferred language.

GC stated that it informed the affected data subjects regarding the steps they can take in relation to phishing and other matters. These are provided at the bottom of the tailored Help Center notices and link to pages dedicated for educating users in this regard. In addition to this, GC also provided information about phishing to users affected by the incident. The 'How could the attackers use this information and what can I do to protect myself' part of the tailored Help Center page contains a link to a Help Center page 'Learn more about phishing' that educates users on what phishing is as well as informing them of they may do to avoid getting phished and what they can do if they have been phished on GC.

GC also provided additional resources to assist and educate users and to allow users to report issues to GC or to contact them directly. It also provided other methods of contact available for Filipino users in relation to the aforesaid matters include, but not limited to the following:

1. Email address for phishing. GC is offering an email address from that which the people can report issues.
2. Reporting violations of Community Standards. Users may report messages, posts, and other content for violation of GC's Community Standards.
3. Data conduct form and email alias where people can contact GC with questions about its data policy through a contact form and will receive a response by email. If they have further questions users can reply to that email in a language of their choice.

GC's Help Center content, account setting pages as well as the Support Inbox contents are also available in Tagalog language. GC employed Filipino Tagalog speakers to ensure that it can continue to be responsive to its Tagalog speaking employee who supports Philippines user concerns regarding the violation of its Community Standards.

GC also participated in numerous initiatives of digital literacy, safety, privacy, and critical thinking online. Currently, GC is developing an #IAMDIGITAL campaign, aimed at encouraging responsible digital citizenship. The

content will further include phishing and spam education. Moreover, GC also have other current and upcoming initiatives aimed at Filipino users to increase awareness about digital literacy to wit: Overseas Workers Welfare, Cyber Safety for Teachers, Digital Youth Summit, Cybersecurity Caravan, NPC Privacy, Safety, Security and Trust Campaign, and Tailored Briefings on GC Products and Services.

Issues

- i. Whether the National Privacy Commission has jurisdiction over the alleged data breach incident.
- ii. Whether GC, Inc. submitted a comprehensive Data Breach Notification Report that follows the rules laid down in NPC Circular No. 16-03.
- iii. Whether GC notified the affected data subjects through an appropriate Data Breach Notification following the rules laid down in NPC Circular 16-03.
- iv. Whether GC established a dedicated helpdesk/help center for Filipino data subjects on privacy related matters concerning GC in pursuant to the Order dated 17 October 2018 of this Commission.
- v. Whether GC implemented a program in the Philippines or otherwise directed to Filipino data subjects to increase awareness in identity theft and phishing in pursuant to the Order dated 17 October 2018 of this Commission.
- vi. Whether GC provided sufficient evidence of compliance.

Discussion

National Privacy Commission has jurisdiction over the alleged data breach incident.

The National Privacy Commission is an independent body mandated to administer and implement the Data Privacy Act of 2012 (DPA), and to monitor and ensure compliance of the country with international standards set for data protection³. Section 7 (a) and (d) of the DPA specifically provides that the NPC is mandated to ensure compliance of personal information controllers with the provisions of the act and

compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy, respectively.

Corollary to the foregoing, Section 6 of the DPA explicitly provides for the extraterritorial application of the DPA to wit:

SEC. 6. Extraterritorial Application. – This Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:

(a) The act, practice or processing relates to personal information about a Philippine citizen or a resident;

(b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:

(1) A contract is entered in the Philippines;

(2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and

(3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and

(c) The entity has other links in the Philippines such as, but not limited to:

(1) The entity carries on business in the Philippines; and

(2) The personal information was collected or held by an entity in the Philippines.

Following the Extraterritorial Application provided by the Section 6 of the DPA, the processing of personal information of GC as personal information controller clearly falls within the mandate and jurisdiction of this Commission. Moreover, the Order issued by this Commission is within the ambit of its power and function, thus valid and enforceable against GC.

³ Data Privacy Act, Sec. 7(2012)

GC, Inc. submitted a comprehensive Data Breach Notification Report that follows the rules laid down in NPC Circular No. 16-03.

This Commission, upon carefully reviewing the Data Breach Notification Report submitted by GC, finds that GC has complied with the requirements laid down in NPC Circular No. 16-03.

Section 17 of the NPC Circular 16-03⁴ provides that 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.

⁴ Personal Data Breach Management, NPC Circular 16-03 (2016)

In this case, the contents of the update provided by GC to the Commission dated 13 October 2018 sufficiently complied with the rules laid down in NPC Circular No. 16-03 in relation to Section 17 of the aforesaid. The aforesaid Data Breach Notification Report and the updates submitted by GC already contains the (1) Nature of the breach; (2) Personal data possibly involved; and (3) Measures taken to address the incident.

It is also worth noting that GC, in recognition of the mandate of this Commission, voluntarily informed this Commission pertaining to the breach incident dated 29 September 2019.

GC notified the affected data subjects through an appropriate Data Breach Notification that follows the rules laid down in NPC Circular 16-03.

In the letter submitted by GC dated 16 November 2018, it is stated therein that starting 29 September 2018, GC sent notification to all potentially affected Filipino users via in-app important security update. The message contained the explanation of the incident as understood by GC in its initial investigation, informed the users that GC had contacted law enforcement, and explained the reasons and impact of its remedial step of resetting all potentially affected tokens which was also posted in the GC newsroom.

On 13 October 2018, GC started updating the smaller subset of users who the investigation showed that were affected by the incident by way of tailored in-app notification which as communicated in English

and Tagalog. Tagalog notification were sent to those affected Filipino users whose GC language was set to Tagalog on 17 October 2018.

As a proof of notification, GC, also attached the sample notifications it provided to the affected data subjects.⁵

Therefore, this Commission finds that GC notified the affected data subjects through an appropriate Data Breach Notification following the rules laid down in NPC Circular 16-03.

GC established a dedicated helpdesk/help center for Filipino data subjects on privacy related matters concerning GC in pursuant to the Order dated 17 October 2018 of this Commission.

The notification made by GC includes hyperlinks to tailored Help Center

pages where the affected users could find further details about the incident, updates about GC's investigation regarding the incident, and guidance on steps which the user could take to protect themselves from suspicious emails, text messages, or phone calls. If the users have further questions pertaining to the incident, users are invited to follow a link from the Help Center to the GC Security Incident Response Form, through which they can submit questions to GC. Those who will submit question to GC will receive an email to which they can reply with any inquiry in their preferred language.

Moreover, GC provided additional resources to assist and educate users and to allow users to report issues to GC or to contact them directly. It also provides other methods of contact available for Filipino users in relation to the aforesaid matters include, but not limited to the following:

1. Security Incident Response Form. This is where Filipino users can contact GC in respect to the aforesaid incident.
2. Email address for phishing. GC is offering an email address from that which the people can report issues.
3. Reporting violations of Community Standards. Users may report messages, posts, and other content for violation of GC's Community Standards.
4. Data conduct form and email alias where people can contact GC with questions about its data policy through a contact form and will receive a response by email. If they have further questions users can reply to that email in a language of their choice.

The Help Center may not be physically located in the Philippines, but this Commission finds that the efforts of GC, as well as the designation of its GC Philippines Head for Public Policy to oversee privacy related matters, sufficiently satisfied the Order dated 17 October 2018 of this Commission.

GC implemented a program in the Philippines or otherwise directed to Filipino data subjects to increase awareness in identity theft and phishing in pursuant to the Order dated 17 October 2018 of this Commission.

GC, through the notification it made, informed the affected data subjects regarding the steps they can take in relation to phishing and other matters.

⁵ See CID 18-J-162 Case Files at pp. 9 to pp. 15

These are provided at the bottom of the tailored Help Center notices and link to pages dedicated for educating users in this regard. In addition to this, GC also provided information about phishing to users affected by the incident. The ‘How could the attackers use this information and what can I do to protect myself’ part of the tailored Help Center page contains a link to a Help Center page ‘Learn more about phishing’ that educates users on what phishing is as well as informing them of they may do to avoid getting phished and what they can do if they have been phished on GC.

Moreover, GC also participated in numerous initiatives of digital literacy, safety, privacy, and critical thinking online. Currently, GC is developing an #IAMDIGITAL campaign, aimed at encouraging responsible digital citizenship. The content will further include phishing and span education. GC also have other current and upcoming initiatives aimed at Filipino users to increase awareness about digital literacy to wit: Overseas Workers Welfare, Cyber Safety for Teachers, Digital Youth Summit, Cybersecurity Caravan, NPC Privacy, Safety, Security and Trust Campaign, and Tailored Briefings on GC Products and Services.

Considering the foregoing, this Commission finds that GC implemented a program in the Philippines or otherwise directed to Filipino data subjects to increase awareness in identity theft and phishing.

GC provided sufficient evidence of compliance.

After thorough review of the submitted documents and adjudication of this case, this Commission finds that GC sufficiently provided proof of its compliance to the Order dated 17 October 2018.

WHEREFORE, all premises considered, the Commission resolves that the matter CID 18-J-162 - “In Re: GC, Inc. Forced Logout “is hereby considered **CLOSED**.

SO ORDERED.

Pasay City, Philippines; 19 November 2020.

(Sgd.)

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

WE CONCUR:

(Sgd.) (Sgd.)

LEANDRO ANGELO Y. AGUIRE

Deputy Privacy Commissioner

JOHN HENRY D. NAGA

Deputy Privacy Commissioner

Copy furnished:

M.K.

Representative of the PIC

GC, Inc.

Attn: Privacy Operations,

xxxxxxxxxx

xxxxxxxxxx

COMPLAINTS AND INVESTIGATION

DIVISION ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

ORDER

Before this Commission is a complete post breach report submitted by Hexel Works, Inc. (formerly Rokko & Associates, Inc.), through The Law Firm of Ingles Laurel Calderon dated 28 July 2020.

Facts

On 02 July 2020, this Commission issued a resolution granting the request for an alternative means of notifying the data subjects of Hexel Works, Inc. (Hexel) containing the following dispositive portion:

WHEREFORE, all premises considered, the requested means by Hexel Works, Inc. to notify the affected data subjects is hereby GRANTED.

The complete post breach report, including details of notification and assistance provided to the data subjects, should be submitted within fifteen (15) days from receipt of this Resolution.

On 28 July 2020, Hexel submitted through its local representative a complete post breach report, including the details of notification and the assistance provided to the affected data subject. They also attached therein the Affidavit of Compliance relating to the individual notification of the data subjects.

In the said report, Hexel informed this Commission that it received the Resolution dated 02 July 2020 of this Commission which granted their request of sending mass e-mail notification and ordering their submission of the complete post breach report only last 21 July 2020. However, while awaiting the Resolution of the Commission, on

09 July 2020, Hexel sent out individual notices through the email addresses of the affected data subjects, which contained, among others: (a) an apology from Hexel; (b) the personal data breached; (c) the nature of the breach; (d) the measures taken by Hexel to address the breach; (e) the measures taken by Hexel to reduce the harm of the breach; and (f)

the contact details of Hexel's representative for further assistance.

Since Hexel already notified all one hundred fifty-eight (158) data subjects individually last 09 July 2020, they no longer notified the affected data subjects in the mass e-mail manner stated in their previous request with the Commission.

Discussion

This Commission, upon reviewing the complete post breach report submitted by Hexel through its local representative, finds that Hexel has complied with the previous Orders and Resolution of the Commission.

The Commission finds that the complete post breach report submitted by Hexel Works, Inc. dated 28 July 2020 is sufficient and considers this matter closed.

Section 17 of the NPC Circular 16-03¹ provides that 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.

¹ Personal Data Breach Management, NPC Circular 16-03 (2016)

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.

In this case, the complete post breach report dated 28 July 2020 submitted by Hexel has already indicated the nature of the breach, the possible personal data involved, and the measures taken to address the breach.

The content and information of the complete breach report is needed by the Commission in order to determine whether Hexel has acted adequately in order to protect the rights of the affected data subject and to see if Hexel has undertaken measures to avoid further damage and prevent similar incidents from recurrence.

While it is worth noting that Hexel has notified the Commission beyond the period of seventy-two (72) hours upon knowledge as required by the Section 17(A) of the NPC Circular 16-03 which provides that 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, Hexel nevertheless implemented measures to address the breach which are indicated in its complete post breach report.

In order to secure or recover the data compromised, Hexel has duplicated the data stored on both laptops through the company server, as the original database was secured and stored in such server, before both

laptops went missing.

As to the notification of data subjects, Hexel also complied with the requirements of Section 18 of NPC Circular 16-03. An affidavit of

compliance was executed by Hexel's legal counsel, who also attached therein the copy of the apology letter and notification of breach.

To prevent recurrence of the incident, Hexel also took the following steps:

1. Retained its policy that each laptop requires a login password to be accessed; and
2. Installed a Hard Disk Drive (HDD) lock software to laptops used outside the company premises to ensure that the hard drive will be locked, and the data will be encrypted if the login password is incorrectly entered for more than a limited time

WHEREFORE, all premises considered, the Commission resolves that the matter CID BN 19-034 - - "In Re: Rokko & Associates, Inc." is hereby considered CLOSED.

SO ORDERED.

Pasay City, Philippines; 21 September 2020.

(Sgd.)

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

WE CONCUR:

(Sgd.) (Sgd.)

LEANDRO ANGELO Y. AGUIRE

Deputy Privacy Commissioner

JOHN HENRY D. NAGA

Deputy Privacy Commissioner

Copy furnished:

THE LAW FIRM OF INGLES LAUREL CALDERON

Counsel of the PIC

COMPLAINTS AND INVESTIGATION

DIVISION ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

INITIATED AS A SUA SPONTE NPC
INVESTIGATION INTO THE POSSIBLE DATA
PRIVACY VIOLATIONS COMMITTED BY
PILIPINAS2022.PH

ORDER

This resolves the Application for Issuance of Cease and Desist Order (Application) dated 11 June 2021 of the Complaints and Investigation Division (CID) of the National Privacy Commission (NPC), praying for this Commission to issue a Cease and Desist Order against the PiliPinas2022.ph (Pilipinas2022), viz:

WHEREFORE, in view of the foregoing premises, it is most respectfully prayed that the instant application for CEASE AND DESIST ORDER against PiliPinas2022.ph be GRANTED and consequently require it to stop processing the personal information in its possession in order to preserve and protect public interest and the rights of the data subjects.

Pilipinas2022 is an online political survey platform designed to gather and display data to serve as an active pulse for the upcoming 2022 elections. It collects personal information from participants, particularly their full name, complete address, and mobile phone number, to be allowed to cast a vote and participate in the survey.¹

The NPC is an independent body created to administer and implement the provisions of the Data Privacy Act of 2012 (DPA). As provided in Section 7 of the DPA, the NPC has Rule Making, Advisory, Public Education, Compliance and Monitoring, Complaints and

¹ Page 1, Application for Issuance of Cease and Desist Order

Investigation, and Enforcement powers² to enable it to protect the fundamental human right of privacy while ensuring the free flow of information to promote innovation and growth.³

Section 7(b) of the DPA specifically states that it is the mandate of the NPC to:

“(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;” (Emphasis supplied)

In addition, the DPA explicitly provides for the Commission’s power to issue Cease and Desist Orders (CDO):

Section 7 (c). Issue cease and desist orders, impose a temporary or permanent ban on the processing personal information, upon finding that the processing will be detrimental to national security and public interest.

This was reiterated in the Implementing Rules and Regulations (IRR) of the DPA:

Section 9. Functions. The National Privacy Commission shall have the following functions:

xxx

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

² See: RA 10173, Section 7.

³ See: Id., Section 2.

Decisions, including the imposition of administrative sanctions, fines, or penalties. This includes:

xxx

1. 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.

In the exercise of its rule-making power and to flesh out the provision above, the NPC issued NPC Circular 20-02, otherwise known as the Rules on the Issuance of Cease and Desist Order on 06 October 2020. Section 5 thereof provides who may apply for CDO, thus:

“Section 5. Filing of Application. – An action for the issuance of a CDO may be commenced upon the filing with the Commission of an application in writing, verified and under oath, by any of the following applicants:

A. the CID, through its sua sponte investigation or the CMD through its conduct of compliance checks and handling of breach notifications, if there is a finding that the grounds for the issuance of the CDO are present; or

B. the Aggrieved Party, either attached to a complaint or as an independent action, with payment of filing fees in accordance with the Rules of Procedure of the NPC, and upon recommendation by the CID after its assessment that the application is sufficient in form and substance.” (Emphasis supplied)

Section 4 of the same Rules provides for the grounds to be established by the applicant for the Commission to issue a CDO, viz:

1. 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;
2. 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
3. The commission or continuance of such act or practice, unless restrained, will cause grave and irreparable injury to a data subject.

The Application details that Pilipinas2022 failed to comply with the general data privacy principles of Transparency, Legitimate Purpose, and Proportionality; it committed gross disregard and violation of the rights of the data subjects; and the continuance operation of Pilipinas2022 may cause grave and irreparable injury to the affected data subjects. The Report provides:

“First, the initial investigation and the technical report have shown that PiliPinas2022.ph does not meet the lawful criteria for processing of personal information and has failed to comply with the general data privacy principles of transparency, legitimate purpose and proportionality. It’s processing of the collected personal information is not being done fairly and lawfully, which is a blatant violation of the DPA and its IRR.

Second, PiliPinas2022.ph’s processing of personal information is detrimental to national security or public interest as it masquerades as an online political survey platform but does not specify all of their purposes in collecting the data, does not provide a clear and complete privacy notice sufficient to solicit an informed consent, and does not disclose their identity as a PIC. Not only is the data subject misinformed as to the true purpose and further processing of their personal information, but they are also left in the dark as to who will be held accountable in case their personal information is used for unlawful purposes. These acts are in gross disregard and violation of the rights of the data subjects.

Third, PiliPinas2022.ph’s continued operation, given the dangers as discussed above to which the personal information in its possession is exposed to, is a palpable risk that can cause grave and irreparable injury to affected data subjects.

Hence, based on the foregoing, it is clear that the grounds for the issuance of a cease and desist order are present, pursuant to Section 4 of NPC Circular No. 20-02.”

These findings exhibit that the entity is doing, threatening, or about to do, acts and practices which constitute a violation of the DPA. Furthermore, considering that, as of the date of the Application, the Pilipinas2022 website remains to be accessible online, it is necessary for the Commission to preserve and protect the rights of the data subjects involved by restraining the continuing processing of personal data by Pilipinas2022 including personal information that Pilipinas 2022 already processed.

WHEREFORE, premises considered, PiliPinas2022.ph is hereby ordered to:

- 1) File a **COMMENT**, within ten (10) days from receipt of this Order, on the allegations in the attached Application for Issuance of Cease and Desist Order, pursuant to Section 9 of the NPC Circular No. 20-02; and
- 2) **CEASE AND DESIST** from the processing of personal data on their database until the Commission issues a decision on the submission of the Comment, which shall be made no more than thirty (30) days from the expiration of the period to file a Comment or of the termination of the clarificatory hearing if one is held, pursuant to Section 11 of the NPC Circular No. 20-02.

Furthermore, the NATIONAL TELECOMMUNICATIONS COMMISSION is hereby enjoined to take down the website of PiliPinas2022.ph immediately upon receipt of this Order.

SO ORDERED.

City of Pasay, Philippines. 16 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:

PILIPINAS2022.PH

NATIONAL TELECOMMUNICATIONS COMMISSION

COMPLAINST AND INVESTIGATION

DIVISION ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

**IN RE: RESEARCH INSTITUTE
FOR TROPICAL MEDICINE**

**NPC BN
20-044**

For violation of Data
Privacy Act of 2012

ORDER

LIBORO, P.C.:

Facts

On 22 March 2020, a 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.

On 24 March 2020, the Data Protection Officer (DPO) of RITM has sent a breach report with a request to the National Privacy Commission (NPC) for assistance to conduct a full investigation of this matter¹ and exemption for notification of affected data subjects.

On 22 June 2020², the Commission issued a Resolution denying RITM's request for assistance and exemption for notification. In the Resolution, the Commission reiterated 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." Thus, the Commission finds that compliance with the Circular must first be made before NPC extends additional assistance, if warranted.

¹ Research Institute for Tropical Medicine Initial Report dated 24 March 2020.

² Resolution, National Privacy Commission, July 16, 2020.

Further, the Commission stressed on the Resolution³ 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.

On 13 July 2020⁴, RITM submitted its full breach report in compliance with the order and expressed their hope that NPC may extend assistance to their team in investigating the case.

On 12 August 2020⁵, upon evaluation of the full breach report submitted by RITM, it is found it to be deficient due to RITM's failure to notify the affected data subjects. RITM was ordered to submit (1) proof of notification to the affected data subjects in the form of notarized affidavit; and (2) copy of the notification letter sent to the affected data subjects.

On 21 August 2020, RITM submitted its Compliance Report to which they stated that they already complied with the notification requirement under NPC Circular 16-03. In the Compliance Report, attached is the Affidavit⁶ executed by Dr. E.C.A. of RITM attesting to the fact that a notification letter was sent electronically to the affected data subjects on 20 August 2020. In the letter, RITM gave assurance that the data subjects' personal information no longer exists in any social media platform upon RITM's latest verification. Further, appropriate strengthening of controls in the RITM's Data Information System was already put into place to ensure that the same or other forms of data privacy breach shall not happen again.

³ Ibid.

⁴ Compliance with Resolution dated 22 July 2020, Research Institute for Tropical Medicine.

⁵ Enforcement Letter dated 12 August 2020.

⁶ Affidavit of Dr. E.C.A. dated 21 August 2020.

DISCUSSION

The Commission adjudged that this case can now be considered closed.

In this case, RITM had taken measures to address the breach and to reduce harm or negative consequences of the breach by implementing policies that will prevent the similar events from happening in the future. Right after the Commission's order to notify the data subjects, RITM promptly complied and sent secured notification letters⁷ to the data subjects electronically, which included, among others, the (1) nature of the breach; (2) personal data involved; (3) measures taken to address the breach; (4) measures taken to reduce the harm or negative consequences of the breach; (5) contact details of the personal information controller to whom further additional information can be obtained about the breach; and (6) assistance provided to the affected data subjects.

With the foregoing, the Commission finds that RITM satisfactorily complied with the requirements of Section 18 of NPC Circular 16-03⁸ on Personal Data Breach Management, and as well as the Commission's Resolutions and Orders.

WHEREFORE, all premises considered, the Commission resolves that the matter of NPC BN 20-044 "In re: Research Institute For Tropical Medicine" is hereby considered CLOSED.

⁷ Copy of notification letter sent, letter to Senator Richard Gordon dated 21 August 2020.

⁸ 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:

Xxxx

C. Content of Notification. The notification shall include, but not be limited to: nature of the breach; personal data possibly involved; measures taken to address the breach; 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, they may be provided in phases without undue delay.

D. Form. Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic.

With the compliance of both the Commission's Resolutions and the requirement of NPC Circular No. 16-03 for a PIC like RITM to have a data breach response team that is ready to assess and evaluate a security incident, restore integrity to the information and communications system, mitigate and remedy any resulting damage, and to comply with reporting requirements, the Commission finds it just to extend its assistance to RITM through its Public Information and Assistance Division (PIAD) for the conduct of training and seminar on implementation of privacy and data privacy implementation measure and personal data breach management. RITM may directly coordinate with PIAD through piad@privacy.gov.ph or call +63 234-2228 local 117 & 116.

SO ORDERED.

Pasay City, Philippines; 21 September 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:

O.B.O.

Representative for RITM

COMPLIANCE AND MONITORING

DIVISION ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

PUBLIC INFORMATION AND ASSISTANCE DIVISION

National Privacy Commission

ORDER

LIBORO, P.C.:

Before this Commission is the Compliance and Motion for Reconsideration dated 24 March 2021 and 29 March 2021, respectively, which was submitted by Saint Louis University (SLU) to comply with the Resolution dated 21 January 2021 issued by this Commission.

Facts

On 21 January 2021, this Commission issued a Resolution with the following dispositive portion:

WHEREFORE, premises considered, Saint Louis University is hereby ORDERED to comply with the following within five (5) days from receipt of this Resolution:

(1) SUBMIT its full breach report with the contents required under NPC Circular No. 16-03 and the Resolutions dated 23 July 2020 and 21 September 2020;

(2) NOTIFY the affected data subjects and SUBMIT proof of compliance thereof, including the proof of receipt of the data subjects of such notification; and

(3) SHOW CAUSE in writing why it should not be held liable for failure to submit a full breach report and notify the affected data subjects within the required period under NPC Circular No.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.

The Resolution dated 21 January 2021 containing a Show Cause Order was issued by the Commission because at that time, the reports submitted by SLU to NPC were not compliant with the previous Resolutions dated 23 July 2020 and 21 September 2020 issued by this Commission and

with NPC Circular No. 16-03 and SLU have not yet notified the affected data subjects despite previous orders from the Commission.

At that time, for SLU, there was no reason to believe that identity fraud could be perpetrated and that there is no reason to believe that the personal data involved have been acquired by an authorized person and that there is no real risk of serious harm to the data subjects. They have also implemented measures to address such incident and to prevent similar incidents from happening in the future. Thus, they considered the matter closed and for them, there is no more reason to inform any data subject.

In the said Resolution dated 21 January 2021, the Commission, in consideration with the likelihood of harm or negative consequences on the affected data subjects, and the number of data subjects involved, resolved that notification to the affected data subjects is necessary. This Commission emphasized that the exemption of notification to the affected data subject is not to be determined by the Personal Information Controller but by the Commission.

In compliance with the Resolution dated 21 January 2021, SLU conducted a reinvestigation of the breach and resubmitted a Final and more comprehensive breach report of the incident which is for evaluation of the Compliance and Monitoring Division.

The investigation revealed a Letter dated 02 July 2020 addressed to SLU by its Service Provider, PhilSmile, outlining the scope and the extent of the software malfunction, how to identify the data subjects affected, the data that was affected, and the recipients of the data

Based thereon, SLU was able to definitively identify those exposed and those who received the data. These were broken down into two categories: 1) The data subjects affected by the software malfunction whose data were exposed, consisting of fifty nine (59) individuals; and 2) The persons who were the recipients of the sensitive personal information who logged into the system between 22 to 25 June 2020, consisting of fifty four (54) individuals.

SLU's Data Protection Committee reached out to the affected data subjects and the recipients of the data and asked all fifty nine (59) and

fifty four (54) of them to execute non-disclosure agreements in relation to the breach.

All fifty four (54) individuals who were the recipients of the sensitive personal information, have agreed to enter and have in fact entered into a non-disclosure agreement with SLU through a Google Forms site, whereby they expressed their assent to the terms and conditions of the Non-Disclosure Agreement (NDA) through a click-wrap mechanism.

Moreover, SLU has also recognized the right to indemnification of the affected data subjects whose data were exposed to the fifty four (54) persons and has granted them indemnification by waiving their registration and IT fees in the tuition fees for AY 2020-2021 of the data subjects, also through a click-wrapped NDA through Google Forms.

According to SLU, through the execution of the NDAs, it has already ensured that the risk of harm or negative consequence to the data subjects will not materialize and the breach is now under control.

SLU also stated that it has not returned to nor activated the PhilSmile student management platform since 25 June 2020. PhilSmile ceased operations on 14 December 2020. Thus, as far as the restart or use of the PhilSmile student management system is concerned, this has become a legal impossibility.¹ As a result, informing the students about the dangers of a system that is not only no longer in use but does not exist at all only heightens fear and mistrust for an event that is no longer possible.²

In its submitted Full Breach Report,³ SLU also stated that its Data Protection Committee has also resolved to undergo a third-party audit of SLU's data privacy compliance, engaging the services of a reputable third-party provider for the same. The audit includes reviews of the policies and guidelines on data privacy; privacy impact assessments on all data processing systems within SLU; current organizational,

¹ NPC BN 20-116 In re: Saint Louis University Compliance and Motion for Reconsideration dated 29 March 2021

² Ibid.

³ NPC BN 20-116 In re: Saint Louis University Attachment A Final Breach Report dated 29 March 2021

technical, and physical measures to ensure data protection; and training for SLU students, faculty, administrators, and personnel regarding SLU's data protection policies and guidelines.

SLU also stated in its Full Breach Report that based on the results of this audit, the Data Protection Committee will update SLU's fundamental data privacy documents, including but not limited to SLU's Privacy Notices, Data Privacy Manual, Data Privacy Policies and Guidelines, and other collaterals indicating a commitment to data privacy on the part of SLU.⁴

As to the reply to the Show Cause Order, SLU stated that it entertained a good faith belief that it had taken, implemented, and applied sufficient security measures to the personal data at the time the personal data breach was reasonably believed to have occurred.

The encryption of the data at rest and the taking of the system offline was part of a good faith belief that these measures prevented the use of the personal data by any person who had no rightful access to it. Upon receiving the Resolution dated 21 January 2021 of the Commission, it then took further steps to contain the data breach. SLU has since taken steps to completely prevent the likelihood of a real risk of serious harm unto the affected data subjects.

SLU prays for the Commission to reconsider its Resolution dated 21 January 2021 and finds that the disclosure of the nature and extent of the data breach to the affected data subjects is no longer necessary and should be exempt from notification under Section 19 of NPC Circular No. 16-03.

Discussion

As to the reply to the Show Cause Order, this Commission finds the explanation of SLU to be sufficient and wants to note the efforts executed by SLU to reinvestigate and to dig deeper into the breach and identify the affected data subjects.

⁴ Id at pp. 7

As to the Compliance and Motion for Reconsideration, it mentions that the Data Protection Committee of SLU has reached out to the affected data subjects for them to execute NDAs and they have in fact executed the NDAs, but it failed to mention and give background to the Commission as to what SLU disclosed to the data subjects about the breach since they are still requesting for exemption to notify the data subjects.

The fact that the data subjects were made to execute NDAs, they necessarily should have informed them about the breach and the data subjects already should have knowledge of the breach.

As to the required contents of the notification to the affected data subjects, Section 18 (C) of NPC Circular No. 16-03 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:

x x x

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
 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. x x x

However, nowhere in the NDAs or in the other documents submitted revealed that the affected data subjects, before making them execute the NDAs, were properly apprised of the reason and consequences on why they were asked to execute them.

Furthermore, upon careful perusal of the NDAs, it shows that the NDAs did not comply with the notification requirements under Section 18 (C) of NPC Circular No. 16-03 indicated above.

This Commission would like to reiterate that SLU is not in the position to determine whether the notification to the affected data subjects is necessary or not. The determination of the aforesaid is within the ambit of the mandate of this Commission. 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.⁵

In this case, the Commission did not exempt SLU from the notification of data subjects nor did SLU request for an exemption for the notification of data subjects only until now.

The Commission had already explicitly ruled on the said issue in the Resolution dated 21 January 2021 and will no longer entertain any requests from SLU regarding the matter. Thus, SLU is expected to strictly comply with the Resolution dated 21 January 2021 of this Commission to notify the affected data subjects and submit proof of compliance thereof, including the proof of receipt of the data subjects of such notification to this Commission.

WHEREFORE, premises considered, Saint Louis University is hereby **ORDERED** to **NOTIFY** the affected data subjects in pursuant to the requirements of Section 18 (C) of NPC Circular No. 16-03 and **SUBMIT** proof of compliance thereof, including the proof of receipt of the data subjects of such notification within fifteen (15) days from Receipt of this Resolution

This Commission gives a **STERN WARNING** to Saint Louis University that any deviation of compliance with the Order of this Commission will be dealt more severely.

SO ORDERED.

City of Pasay, Philippines. 15 April 2021.

Sgd.)

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

⁵ Section 18(B), NPC Circular 16-03.

WE CONCUR:

(Sgd.)

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

(Sgd.)

JOHN HENRY D. NAGA

Deputy Privacy Commissioner

Copy furnished:

R.F.H.C.T

President

Saint Louis University

**COMPLIANCE AND MONITORING
DIVISION ENFORCEMENT DIVISION
GENERAL RECORDS UNIT**

National Privacy Commission

ORDER

AGUIRRE, D.P.C.:

This Order refers to a breach notification submitted by BPI Philam Life Assurance Corporation (BPLAC) dated 26 March 2021 and its Update Report dated 09 April 2021. The breach notification refers to an alleged data breach and suspicious activity involving its third-party call center and includes a request for extension of five (5) days to submit a full breach report and to notify the affected data subjects. The update report contains a request for an extension of additional five (5) days from the originally requested period.

Facts

On 27 March 2021, the Commission received a letter from BPLAC with the subject: “Alleged Data Breach and Suspicious Activity Involving (Its) Third Party Call Center.” In its letter, BPLAC narrated that:

On Feb. 16, 2021, a file containing 61,000 names of Citi credit cardholders together with their ages and contact numbers were uploaded by CFSI into the system of the 3rd party call center, Shore Solutions, Inc. to be used for the telemarketing campaign of BPLAC called Non-Credit Insurance Campaign. In this batch of upload, there were names of Citibank employees seeded as part of their testing activity.

On March 23, 2021, suspicion of a fraudulent activity was discovered. The employees whose names were seeded in the file received calls offering credit card services which is not part of the BPLAC official campaign. The method of the call was like a social engineering scheme whereby the conversation is being conducted in a fast-paced manner that an ordinary customer will not have a chance to ask questions and feel pressured to agree to the purchase. The details of the credit card will then be secured from the customers including the card no., expiry date and the CVV.

The activity is described as account take over.

A forensic investigation is currently ongoing to determine the extent of these activities and how many customers might have already been victimized. The investigation also aims to find out if these actions are perpetrated by the agents of the call center or it could be that the system of the call center was hacked. Our vendor, third party call center Shore Solutions, is not aware of any cyber security breach at this time.¹

BPLAC stated that it has undertaken measures to address the breach and was conducting a forensic investigation to find out the root cause of the breach and to determine who and how many customers were affected so that it can appropriately notify them.² In line with this, BPLAC requested for a five (5) day extension on the seventy two (72)- hour deadline for mandatory reporting, thus:

We also write to respectfully request for extension on the 72 hour deadline of mandatory reporting. As provided under NPC Advisory 2018-02 dated June 26, 2018, we shall provide full report within 5 days, or as soon as possible, as the result of the investigation becomes available.³

On 09 April 2021, BPLAC submitted an Update Report which stated that it is making good progress in its investigation but still needed more time to complete it. Further, it stated that based on the preliminary findings, there were no signs that would indicate any cyber-attack. Lastly, it requested for an additional five (5) working days to release the customer notification letters and to submit its full breach report:

To date, we are making good progress in our investigation but we need more time to complete this thoroughly. Material pieces of evidence have been gathered that will help us determine if there was indeed a data breach that happened, and if there was, what was the cause of said breach, the extent of damage, and who were the customers affected. Based on preliminary

¹ Letter from BPLAC dated March 26, 2021.

² Ibid.

³ Ibid.

findings, there were no signs that would indicate any cyber attack.

We are in close coordination with the third party service provider and with our business partner, Citi Financial Services Inc. (CFSI), as this investigation progresses.

As such, we would request your office to grant us an additional 5 working days for us to release customer notification letters and submission of the full breach report.

Discussion

The Commission denies the requests for extension and orders BPLAC to submit its full breach report and proof of notification within seventy-two (72) hours from receipt of this Order. The Commission further orders BPLAC to show cause as to why it should not be held liable for failure to submit its full breach report and to notify the affected data subjects within the prescribed period.

At the outset, it should be emphasized that notification of data subjects of a personal data breach is the general rule and exemptions are allowed only under specific circumstances. Section 18(A) of NPC Circular No. 16-03, provides the rule:

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.⁴

The purpose of the requirement to notify data subjects of a breach incident is to give them the opportunity to take the necessary precautions or such other measures to protect themselves against

⁴ NPC Circular 16-03, Personal Data Breach Management. Dated 15 December 2016. Emphasis supplied.

possible effects of the breach. Personal information controllers (PICs) are likewise required to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach.⁵ A delay in notification can cause harm to affected data subjects as they cannot protect themselves from the consequences of the breach.

The Commission notes that BPLAC, in its initial report, requested for an extension of five (5) days or until 01 April 2021 to comply with the mandatory requirements under NPC Circular No. 16-03 to notify the data subjects and provide the Commission with its full breach report.

Despite the fact that this extended period already ended on 01 April 2021, BPLAC neither provided proof that it notified its data subjects nor did it submit its full breach report. Instead, it submitted an Update Report on 09 April 2021 requesting for an additional extension of five (5) days without sufficient explanation as to why it failed to comply with its commitments within the period it originally requested.

Until now, no submissions have been made by BPLAC despite the lapse of the additional five (5) days it requested on 09 April 2019. Time and again, the Commission has reiterated that PICs need not wait for the Commission to grant their request for extension of time before they comply.

Since BPLAC requested for a specific period to comply with the mandatory reporting requirements, it should have complied with the requirements within that requested period. At the very least, BPLAC should have submitted its request for further extension within the period they originally requested.

Given that both periods requested for has already lapsed, the Commission denies the request for extension. BPLAC should have already complied with the mandatory requirements of notifying its data subjects and submitting the full breach report. Further, BPLAC should explain its unreasonable delay in complying with these obligations.

WHEREFORE, premises considered, the Commission hereby **ORDERS** BPI Philam Life Assurance Corporation to comply with the following **within seventy-two (72) hours** from receipt of this Order:

⁵ Ibid.

(1) SUBMIT its full breach report with the contents required under NPC Circular 16-03;

(2) NOTIFY the affected data subjects and SUBMIT proof of notification that ensures all data subjects were made aware of the breach; and

(3) SHOW CAUSE in writing why it should not be held liable for failure to submit a full breach report and notify the affected data subjects within the required period and be subject to contempt proceedings as permitted by law, before the appropriate court, and such other action as may be available to the Commission.

SO ORDERED.

City of Pasay, Philippines. 15 April 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



RESOLUTIONS

RLA,
Complainant,

versus

PLDT ENTERPRISE
Respondent.

NPC 18-010
(Formerly CID Case
18-D-010)

RESOLUTION

AGUIRRE, D.P.C.:

This Commission resolves the Motion of Reconsideration filed by PLDT Enterprise on the Decision dated 17 December 2020. Facts

FACTS

On 17 December 2020, the Commission issued a Decision and held PLDT Enterprise (PLDT) liable for violation of RLA's (RLA) rights under the Data Privacy Act of 2012 (DPA), particularly Sections 28 (Processing of Personal Information for Unauthorized Purposes) and 32 (Unauthorized Disclosure) of the DPA:

WHEREFORE, all these premises considered, this Commission resolves to AWARD Complainant[,], RLA[,], nominal damages in the amount of Fifty Thousand Pesos (P50,000.00) for Respondent PLDT Enterprise's violation of Complainant's rights under the Data Privacy Act.

Moreover, this Commission also resolves to **REMAND** this case to the Complaints and Investigation Division for the limited purpose of determining and identifying the responsible persons, officers, or individuals of PLDT Enterprise who caused the violations of Sections 28 and 32 of the DPA prior to recommending the matter to the Secretary of Justice for criminal prosecution.

SO ORDERED.¹

On 26 July 2021, PLDT received the Decision.²

On 05 August 2021, PLDT filed its Motion for Reconsideration arguing the following:

1. PLDT, in compliance with existing laws, acted under a legal obligation to process RLA's personal data, which is one of the conditions for lawful processing under Section 12 (c) of the DPA and the Implementing Rules and Regulations of the DPA (IRR)³;
2. None of PLDT's "responsible persons, officers, or individuals" should be held criminally liable for violations of the DPA, as PLDT acted under a legal obligation to process RLA's personal information⁴; and
3. For Corporate Accounts, PLDT acts as Personal Information Processor (PIP) for its Enterprise clients.⁵

PLDT asserts that it should not be held liable for violating Sections 28 and 32 of the DPA. It cites its legal obligation to process personal information under Section 149 of Revised Order No. 1, otherwise known as the Public Service Commission Rules and Regulations (Section 149 of Revised Order 1) and National Telecommunications Commission (NTC) Memorandum Circular No. 05-06-2007, otherwise known as the Consumer Protection Guidelines (NTC MC 05-06-2007):

[A]t the time the application of the Complainant was processed, through Knutsen Philippines, Inc. ("Knutsen"), Respondent was mandated by Section 149 of the Revised Order No. 1, otherwise known as the Public Service Commission Rules and Regulations ("Order No. 1") and National Telecommunications Commission Memorandum Circular No. 05-06-2007, otherwise known as the Consumer Protection Guidelines ("NTC Circular"), to issue a listing directory of the names, addresses, and telephone numbers of all of its subscribers at least once a year. Acting on such mandate, Respondent processed and published Knutsen's existing accounts in the White Pages, the listing directory for PLDT's corporate accounts ("White Pages").⁶

¹ Decision, 17 December 2020, at 26, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2020) (pending).

² Motion for Reconsideration, 05 August 2021, at 1, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

³ *Id.* at 1- 2.

⁴ *Id.* at 5.

⁵ *Id.* at 9.

⁶ *Id.* at 2. Emphasis supplied.

Section 149 of Revised Order 1 provides:

Section 149. Telephone Directory. – Each telephone public service shall at least once a year issue a listing directory showing therein the names of all subscribers arranged in alphabetical order, their addresses and telephone numbers and such other information as may be of interest to a subscriber's everyday use of his telephone. Each subscriber shall be entitled to a free copy of the directory.⁷

Section 2.2 of NTC MC 05-06-2007 states:

Section 2.2 - Any data supplied by the consumer shall be treated as confidential by the entity or service provider mentioned under Section 1.1 hereof and shall not be used for purposes not authorized by him. Upon subscription, he shall be informed of his right to privacy and the manner by which his data would be protected. In cases where a public directory listing of subscribers is regularly published by the service provider, the consumer shall be given the option not to be listed in succeeding publications.⁸

PLDT further explains its legal obligation under NTC MC 05-06-2007 as follows:

Section 2.2 of NTC [MC 05-06-2007] shows that the subscriber is given the option not to be included in succeeding public directory listings of subscribers. From this provision, it can be gleaned that the subscriber may request for his/her exclusion in the subsequent publication of the directory listing. If s/he did not exercise this right to be excluded, his/her name will be included in the directory listing. As worded, the NTC Circular did not impose an obligation to secure from subscribers the affirmative act of consenting to the publication of his/her contact information before a service provider can include the subscriber's information in the directory. Thus, while Respondent is obligated to publish a directory listing with the names, addresses, and telephone numbers of its subscribers, the Respondent must remove or refrain from publishing the details of any subscriber in the succeeding directory listing if the said subscriber opts not to be listed.⁹

⁷ Public Service Commission, Rules and Regulations for all Public Services, Revised Order No. 1, Commonwealth Act No. 146, § 149 (1941).

⁸ National Telecommunication Commission, Consumer Protection Guidelines [NTC Memo. Circ. No. 05-06-2007], § 2.2 (8 June 2007).

⁹ Motion for Reconsideration, 05 August 2021, at 3, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending). Emphasis supplied.

PLDT argues that consent is not the sole criterion for lawful processing of personal information. It maintains that its act of processing is necessary to comply with a legal obligation, which is a basis for lawful processing under Section 12 (c) of the DPA¹⁰:

Clearly, consent of the data subject is only one of the allowed bases for processing of personal information. The processing of personal information is still allowed as long as any of the other lawful conditions provided under the DPA and DPA- IRR is present. In this case, Respondent published Complainant's personal information in the 2017 directory listing in compliance with the requirement prescribed by Order No. 1 and the NTC Circular. Thus, Respondent is allowed to process and publish Complainant's information in the listing directory as authorized under, and for the purpose of complying with, its legal obligation under Order No. 1 and the NTC Circular.¹¹

PLDT asserts that it fully complied with its legal obligation under NTC MC 05-06-2007:

It must also be noted that Respondent has complied with the qualifying clause under Section 2.2 of NTC Memorandum No. 0506-2007. As will be further discussed, immediately upon receiving Complainant's request, Respondent tagged the Corporate Individual Account under Knutsen as "Confidential" and confirmed that Complainant's personal information would not be published in the succeeding directories.¹²

As to criminal liability, PLDT argues that it and its responsible persons, officers, or individuals should not be held criminally liable since it did not act with gross negligence¹³:

Assuming but without admitting that there was an unauthorized processing of Complainant's personal information, Respondent submits that such does not rise to the level of gross negligence that would merit criminal sanction. Respondent notes that it immediately instituted the following measures in respect of this case: (i) upon receiving complainant's concerns, his account was promptly tagged as

¹⁰ Id. at 3.

¹¹ Id. at 5. Emphasis supplied.

¹² Id.

¹³ Id. at 6.

confidential; (ii) application forms were revisited to ensure

compliance with the DPA; and (iii) policies and processes were redefined pursuant to the additional guidelines provided by this Honorable Commission in its Advisory Opinion No 2018-021 dated 27 April 2018 (the “Advisory Opinion”). With these measures in place, none of Respondent’s “responsible persons, officers, or individuals” should be held criminally liable for violations of the DPA, because Respondent acted based on its understanding of its legal obligation to publish listing directory of the names, addresses, and telephone numbers of all of its subscribers.¹⁴

PLDT claims that it acted in good faith and even sought the guidance of the Commission on the matter:

To be sure, Respondent’s act of securing the Advisory Opinion from the Honorable Commission evinces its good faith desire and commitment to upholding the DPA in its operations.¹⁵

...

It is also worth noting that while the DPA has been in effect since 2012, the DPA-IRR was promulgated only in August 2016 and was fully implemented in 2017, and the recommended specific provisions and detailed guidance regarding services that involve the processing of personal data had not yet been implemented at the time that the Corporate Individual DSL of the Complainant was filed in 2015. With the implementation of this new law, Respondent, in good faith, voluntarily sought the guidance of this Honorable Commission on 16 November 2017 and 15 March 2018 in respect of the handling of telephone directory requirements under [Revised] Order No. 1 and NTC Circular.¹⁶

PLDT further provides that it revised its Corporate Individual DSL Application Form on 10 September 2018 based on the guidance provided by the Commission through Advisory Opinion No. 2018-021:

With the guidance provided by this Honorable Commission, through its Advisory Opinion, Respondent issued an email advisory dated 13 July 2018 informing all teams of the Enterprise Group that directory listing in its CRM system shall be defaulted to “CONFIDENTIAL” from the previous default

¹⁴ Id. Emphasis supplied.

¹⁵ Motion for Reconsideration, 05 August 2021, at 6, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

¹⁶ Id. at 7. Emphasis supplied.

of “PUBLISHED”. Respondent revisited its forms and implemented

corresponding changes thereto. These new application forms were implemented starting 10 September 2018.¹⁷

PLDT argues that it only acted as a Personal Information Processor (PIP) for its Enterprise clients and that Knutsen Philippines, Inc. (Knutsen) is the Personal Information Controller (PIC):

The Respondent respectfully disagrees with the foregoing conclusion and reiterates that it is a PIP merely acting upon the instructions of its direct corporate customer, Knutsen, the PIC of Complainant's personal information.¹⁸

It further added that:

As averred in the Comment to the Complaint, the Enterprise Group of the Respondent, which was made a party to this case, is in the business of providing communication services to corporate clients (i.e. juridical, non-individual customers). Consequently, the Enterprise Group does not directly provide services to individual subscribers or natural persons. Although the "ultimate recipients" of the communication services provided by the Respondent are composed of natural persons connected to the corporate clientele (e.g., primarily the corporate client's designated employees), Respondent's contract and transactions are only with corporate/group clients/customers. The relevant subscription agreements/contracts are unequivocally signed between herein Respondent and the relevant corporate customer/client through its authorized officer or representative; in this case, Knutsen. In fact, the billing for services rendered is addressed to the corporate customer/client. Accordingly, it is such corporate clients/customers that provide to herein Respondent the required information to facilitate, among others, the installation of needed connectivity, equipment, and other requirements and the rendition of services, and directs Respondent as to the services to be rendered and for whom the services are to be provided.¹⁹

PLDT asserts that Knutsen provided RLA's personal information to PLDT in order to allow PLDT to provide the necessary services:

¹⁷ *Id.*

¹⁸ *Id.* at 9. Emphasis supplied.

¹⁹ *Id.*

Complainant had no participation in accomplishing the said form and that Complainant merely provided his personal information to Knutsen to allow Respondent to install the necessary connectivity for the rendition of the subscribed services. Since the application involved referred to a Corporate Individual DSL account, the details indicated therein were thereafter published by Respondent in the White Pages – Government and Business Book 2017, as required under Order No. 1.²⁰

It further justifies its position by arguing that the personal information collected from RLA is the standard information necessary for providing its services and according to the terms and conditions stated in its Corporate Individual DSL Application Form:

The information collected from the Complainant are standard information necessary for the purpose of providing the services under the DSL subscription (i.e. name, address, telephone number, and choice of plan). The provision of such services under the DSL subscription is “in accordance with the following terms and conditions and the rules and regulations issued by other appropriate government agencies, as provided in the back portion of the Application Form signed by MA. The publication of the same in the White Pages is one of the mandatory legal obligations of the Respondent which is necessarily read into the terms and conditions of the services provided by Respondent.”²¹

PLDT further reasons that it was only tasked to process the personal information that Knutsen collected to allow it to provide DSL services to specific Knutsen employees:

As the corporate client, Knutsen collected the relevant personal data of the Complainant and provided such information to Respondent to enable the latter to provide the subscribed services. As noted by the Honorable Commission in its Decision, Complainant’s personal information was supplied by his employer, Knutsen, the subscription was named under Knutsen (but for the account of Complainant), Knutsen’s President and General Manager is the signatory in the Application form, and Knutsen’s address is indicated in the billing portion of the application form. Respondent only collected the information necessary to provide the service obtained by Knutsen for its employees. All of these facts are consistent with an outsourcing

²⁰ *Id.* at 11.

²¹ Motion for Reconsideration, 05 August 2021, at 11, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

agreement for the processing of personal information between Knutsen and Respondent. Stated differently, Respondent is tasked with processing of the personal information of Knutsen's employees for the purpose of providing the DSL services which Knutsen's employees will use to perform their duties and responsibilities during their employment.²²

PLDT prays that the Commission reverse the Decision dated 17 December 2020 and dismiss the Complaint for lack of merit.²³

On 26 October 2021, RLA filed its Comment/ Opposition to PLDT's Motion for Reconsideration.²⁴

Discussion

The Commission denies PLDT's Motion for Reconsideration. The Commission finds no reason to overturn the Decision dated 17 December 2020 since PLDT has not provided any new or material allegation to justify a reversal of the Decision. Nevertheless, the Commission shall proceed to further clarify its reasons for denying PLDT's Motion for Reconsideration.

I. PLDT is a Personal Information Controller.

PLDT acted as a PIC when it processed RLA's personal information. As defined in the DPA, a PIC is "a person or organization who controls the collection, holding, processing or use of personal information."²⁵ A PIC also includes "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."²⁶

In its Motion for Reconsideration, PLDT asserts that it was acting as a PIP or a "juridical person qualified to act as such...to whom a personal information controller may outsource the processing of personal data pertaining to a data subject."²⁷ It contends that its Enterprise Group acted as a PIP since the installation and the publication of RLA's

²² Id.

²³ Id. at 12.

²⁴ Comment/ Opposition to the Respondent's Motion for Reconsideration, 26 October 2021, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

²⁵ 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 (h) (2012).

²⁶ Id.

²⁷ Id. § 3 (i).

personal information resulted from the instructions of the PIC, Knutsen.²⁸ It maintains that its Enterprise Group entered into a contract with Knutsen to provide the Corporate Individual DSL account to its employee, RLA, since it does not directly provide services to individual subscribers or natural persons.²⁹ It claims that Knutsen, as RLA's employer, outsourced³⁰ or directed the transfer of RLA's personal information to PLDT for the installation of the Corporate Individual DSL account to allow RLA to perform his duties and responsibilities during his employment.³¹ It asserts that it is Knutsen who "directs [it] as to the services rendered and for who[m] the services are provided."³²

Contrary to PLDT's assertions, PLDT is the PIC, and not the PIP. The test to determine if a person or an entity acts as a PIC or a PIP is if such person or entity controls the processing of personal information.

As discussed in the Decision dated 17 December 2020, PLDT decides the pieces of information that Knutsen collects from its employees, which Knutsen, in turn, supplies to PLDT³³:

[I]t is PLDT that decided what information were collected from Knutsen's employees, including that of the Complainant, to apply for PLDT's services. Knutsen merely supplied the personal information of its employees to PLDT, but the control over the personal information provided remained with PLDT.³⁴

The Implementing Rules and Regulations of the DPA (IRR) defines control as deciding on the information to be collected, or the purpose or extent of its processing.³⁵ Through its decision-making power, a PIC determines the purposes and means of processing personal information, the categories to be processed, and access to such personal information.³⁶ These are the very acts that PLDT performed.

²⁸ Motion for Reconsideration, 05 August 2021, at 10-11, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

²⁹ *Id.* at 10.

³⁰ National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule I, § 3 (f) (2016).

³¹ Motion for Reconsideration, 05 August 2021, at 10-11, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

³² *Id.* at 10.

³³ Decision, 17 December 2020, at 10, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2020) (pending).

³⁴ Motion for Reconsideration, 05 August 2021, at 10, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

³⁵ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule I, § 3 (m).

³⁶ EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 104-105 (2018).

In this case, PLDT maintains that “the information collected from [RLA] are standard information necessary for the purpose of providing the services under the [Corporate Individual] DSL subscription”³⁷ and that it was Knutsen who provided the required information to PLDT.³⁸ Although it was Knutsen who submitted RLA’s personal information to PLDT to facilitate the installation of the Corporate Individual DSL account, Knutsen and RLA would not have known what categories of personal information they needed to submit without PLDT’s instructions. Aside from this, it was PLDT that determined what “standard information” it will require from its prospective subscribers and the purpose for each category of personal information it collects.

To accept PLDT’s position will result in absurdity. It will shift the accountability for complying with the obligations under the DPA and absolve those that provide services of any responsibility whenever an employer submits the personal information of or pays for services for its employees.

Following PLDT’s logic, for instance, a company such as a health insurance provider, who processes a lot of sensitive personal information, will not be considered a PIC simply because it was the employer who chose which of its employees should be covered, provided their personal information to the insurance company, and paid the insurance premium. This is clearly not what the DPA contemplates.

The Terms and Conditions that PLDT requires its subscribers to consent to, further belies its claim that it is only acting as a PIP. The relevant portions of PLDT’s Terms and Conditions provide:

Acceptable Use Policy – In PLDT’s efforts to promote good citizenship within the Internet community, PLDT will respond appropriately in the event that it becomes aware of any inappropriate use of the service. PLDT reserves the right to monitor bandwidth, usage and content, and from time to time to operate the service to identify violators of the Acceptable Use Policy or any inappropriate use of its service and/or to protect the PLDT network and other PLDT subscribers.

³⁷ Motion for Reconsideration, 05 August 2021, at 11, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

³⁸ *Id.* at 10.

If the PLDT Data Services is used in a way which in PLDT's sole discretion, would be considered inappropriate, PLDT may take any action deemed appropriate, including but not limited to the temporary or permanent removal of content, cancellation of newgroup posts, filtering of Internet transmission, and the immediate suspension or termination of all or any portion of the PLDT Data Service, without incurring any liability for damages.

...

Amendment – PLDT reserves the right to amend any of the provisions of any of the foregoing terms and conditions. Any such amendment shall take effect fifteen (15) days from notice to the Subscriber, through whatever means.³⁹

Following the definition of a PIC, control of personal data is the determining factor in identifying the PIC. It is the controller that determines the purpose, scope, nature, and extent of the processing activity. In the case of PLDT's Terms and Conditions, it expressly shows that PLDT undertakes certain processing activities such as monitoring the usage and the content that its subscribers access for its own purposes and benefit, i.e. "to protect the PLDT network and other PLDT subscribers."⁴⁰ The Terms and Conditions also shows that PLDT processes all of these and can "take any action deemed appropriate" at its "sole discretion." Lastly, despite its claim that it acts as a PIP for all of its Enterprise clients, PLDT claims for itself the authority to amend any provision of the Terms and Conditions without any need to consult, much less secure the consent of anyone, including its Enterprise clients that are supposed to be its PICs. All these are clearly inconsistent with the relationship between a supposed PIP and its PICs.

PLDT further maintains that it took the necessary steps to address RLA's concerns on the publication of his personal information in the 2017 White Pages.⁴¹ Based on its representations, PLDT took steps to reclassify and tag RLA's profile as "Confidential" so that his personal information will no longer be published in future listing directories.⁴² It also implemented measures to indicate the default setting of directory listings as "Confidential" instead of "Published".⁴³

³⁹ PLDT Terms and Conditions, at 2. Emphasis supplied.

⁴⁰ *Id.*

⁴¹ Motion for Reconsideration, 05 August 2021, at 6, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

⁴² *Id.*

⁴³ *Id.*

These acts show that PLDT can change the classification of subscribers and, corollary, choose when to publish subscriber information without any input from Knutsen or any of its enterprise clients who are supposed to be its PICs. These acts not only highlight PLDT's control over the extent of the processing of its data subjects' personal information, but also show the inconsistency of its claim with the limits of what PIPs can do on their own. Section 44(b)(1) of the IRR provides that the PIP shall be contractually bound to "[p]rocess the personal data only upon the documented instructions of the personal information controller."⁴⁴ This is clearly not the case with PLDT. It would not have been able to do any of the foregoing acts had it been acting simply as a PIP.

For these reasons, it is clear that PLDT acted as the PIC. Its actions, together with its Terms and Conditions, demonstrate control over not only the types of personal information it required Knutsen and RLA to submit for the installation of the Corporate Individual DSL account but, more importantly, the purpose and extent of the processing it reserves for itself in providing DSL services to its subscribers.

II. There is no conflict between PLDT's obligations under Section 149 of Revised Order 1 and NTC MC 05-06-2007 and the DPA.

The Commission finds no conflict between the obligations imposed on PLDT by the NTC, its primary regulator, and the DPA. In its analysis, the Commission is not enforcing NTC MC 05-06-07, but rather, it is fulfilling its mandate under the DPA to examine the presence of, and the proper application of the claimed lawful criteria to the processing undertaken by the PIC.

PLDT maintains that it published RLA's personal information in the 2017 White Pages pursuant to a legal obligation stemming from its mandate under Section 149 of the Revised Order No. 1, and NTC MC 05-06-2007.⁴⁵

Section 149 of Revised Order 1 requires telephone public service providers, such as PLDT, to issue a listing directory at least once a year:

⁴⁴ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule X, § 44 (b) (1).

⁴⁵ Motion for Reconsideration, 05 August 2021, at 1-2, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

Section 149. Telephone Directory. – Each telephone public service shall at least once a year issue a listing directory showing therein the names of all subscribers arranged in alphabetical order, their addresses and telephone numbers and such other information as may be of interest to a subscriber's everyday use of his telephone. Each subscriber shall be entitled to a free copy of the directory.⁴⁶

While it is true that Section 149 of Revised Order 1 mandates PLDT to publish a listing directory, this should not be read in isolation and must be taken together with Section 2.2 of NTC MC 05-06-2007. This is something that PLDT itself recognized when it identified both Revised Order 1 and NTC MC 05-06-2007 as the source of its legal obligation to publish a listing directory.⁴⁷

NTC MC 05-06-2007 is an administrative circular issued by the NTC. The nature of an administrative circular is “to supplement provisions of law or to provide means for carrying them out, including information relating thereto.”⁴⁸ NTC MC 05-06-2007 is intended to “fill in the details”⁴⁹ of Section 149 of Revised Order 1. Section 2.2 of NTC MC 05-06-2007 supplements Section 149 of Revised Order 1. It states:

Section 2.2 - Any data supplied by the consumer shall be treated as confidential by the entity or service provider mentioned under Section 1.1 hereof and shall not be used for purposes not authorized by him. Upon subscription, he shall be informed of his right to privacy and the manner by which his data would be protected. In cases where a public directory listing of subscribers is regularly published by the service provider, the consumer shall be given the option not to be listed in succeeding publications.⁵⁰

With the issuance of NTC MC 05-06-2007, PLDT's obligation under Section 149 of Revised Order 1 is necessarily qualified by Section 2.2 of NTC MC 05-06-2007. The legal obligation to publish a listing directory at least once a year under Section 149 of Revised Order 1 still subsists but now carries with it the requirements under Section 2.2 of NTC MC 05-06-2007, as also acknowledged in the dissent.⁵¹

⁴⁶ Rules and Regulations for all Public Services, Revised Order No. 1, Commonwealth Act No. 146, § 149. Emphasis supplied.

⁴⁷ Motion for Reconsideration, 05 August 2021, at 2, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

⁴⁸ Office of the President, Instituting the Administrative Code of 1987, Executive Order No. 292, Series of 1987 [E.O. No. 292, s. 1987], Book IV Chapter 11 § 50 (25 July 1987).

⁴⁹ *Tanada v. Tuvera*, G.R. No. L-63915 (1986).

⁵⁰ NTC Memo. Circ. No. 05-06-2007, § 2.2.

⁵¹ See, *Liboro Dissenting Opinion*, 10 December 2021, at 6, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

As the Commission held in its Decision dated 17 December 2020:

While the telephone service provider has the duty to publish yearly telephone directory, it now has the correlative duty to do so in a manner that upholds the data subject's rights to data privacy.⁵²

Even a cursory reading of Section 2.2 of NTC MC 05-06-2007 will show that the obligations it imposes are not in conflict with the DPA. The obligations are clear and does not give rise to any credible or significant question that prevents PLDT from complying first with its provisions before soliciting guidance from this Commission.

In requiring public telecommunication entities to inform their subscribers of their right to privacy and how their data will be protected upon subscription, and to give their subscribers the option not to be listed in succeeding publications, Section 2.2 of NTC MC 05- 06-2007 is consistent with the general privacy principle of transparency, the rights of data subjects, and the concept of consent under the DPA.

The DPA defines consent as follows:

Section 3. Definition of Terms. – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

...

(b) Consent of the data subject refers to 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.⁵³

Contrary to PLDT's claim that "the NTC Circular did not impose an obligation to secure from subscribers the affirmative act of consenting to the publication of his/her contact information before a service

⁵² Decision, 17 December 2020, at 14, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2020) (pending). Emphasis supplied.

⁵³ Data Privacy Act of 2012, § 3 (b). Emphasis supplied.

provider can include the subscriber's information in the directory"⁵⁴, the public telecommunication entity's publication of the personal information of its subscribers in a listing directory requires consent from its data subjects.

Section 2.2 of NTC MC 05-06-2007 imposes the following obligations on public telecommunication entities:

1. It shall treat the data as confidential and shall not use such data for purposes not authorized by the subscriber;
2. It shall inform the subscriber of the right to privacy and the manner by which his or her data would be protected;
3. It shall give the subscriber the option not to be listed in succeeding publications in cases where a public directory listing is regularly published by the service provider, and
4. It shall provide these pieces of information to its subscribers upon subscription.⁵⁵

Having been issued in 2007, it is not surprising that the wording in the NTC MC 05-06-2007 does not exactly mirror the concept of consent in the DPA. Nevertheless, the obligations under Section 2.2 of NTC MC 05-06-2007 resonate with the concept of consent that is freely given, specific, and an informed indication of will.

Upon subscription, a public telecommunication entity is required to inform its subscribers of their privacy rights, how their data will be protected, and the specific option to not be listed in the listing directory. If the subscribers exercise the option and choose not to be listed, then the public telecommunication entity may not publish their names and other personal information in the listing directory.⁵⁶ If the subscriber, however, chooses not to exercise the option, the subscriber is essentially consenting to the processing of his or her personal information for purposes of publishing the listing directory.⁵⁷

Aside from the obvious fact that subscribers should be given the free choice to exercise the option, whatever option they exercise should be "evidenced by written, electronic or recorded means."⁵⁸ In the case of a subscriber who chooses not to exercise the option, evidence of that

⁵⁴ Motion for Reconsideration, 05 August 2021, at 3, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

⁵⁵ NTC Memo. Circ. No. 05-06-2007, § 2.2.

⁵⁶ *Id.*

⁵⁷ *Id.*

⁵⁸ Data Privacy Act of 2012, § 3 (b). Emphasis supplied.

may be in the form of an unticked box in a form that provides all the requisite information. Although it is not ideal given the concept of consent under the DPA, as long as the information required to be given to subscribers is clearly provided, an unticked box still suffices to show the choice exercised by the subscriber for purposes of satisfying the requisites of Section 2.2 of NTC MC 05-06-2007.

In agreeing with PLDT's position, the dissent argues that "PLDT's legal obligation to publish is the default position, while an opt-out of the consumer is required for it to remove the personal information in the succeeding publications and thereby treat the same as confidential, consistent with Section 2.2 of the NTC MC 05-06-2007."⁵⁹

Both PLDT and the dissent, however, neglected to discuss how the PLDT subscribers would even be able to exercise this opt-out considering that PLDT failed to specifically inform its data subjects of everything it needed to comply with under Section 2.2 of NTC MC 05-06-2007: 1) inform its subscribers of their privacy rights and how their data will be protected, and 2) the specific option to not be listed in the listing directory. Without fulfilling these conditions attached to its legal obligation, how would the subscribers even know that they can request this opt-out in the first place? Such an interpretation that renders useless the protections provided not just by NTC MC 05-06-2007 but also the DPA cannot be considered acceptable. It is a basic principle of statutory construction that "in interpreting a statute (or a set of rules as in this case), care should be taken that every part thereof be given effect... a construction that would render a provision inoperative should be avoided."⁶⁰

Aside from this, PLDT also failed to acquire the consent of its subscribers before proceeding with the publication of personal information in the White Pages.

The dissent itself acknowledges that PLDT failed to comply with Section 2.2 of NTC MC 05-06-2007 but attempts to downplay its significance by claiming it only resulted in a violation of the general privacy principle of transparency, thus:

⁵⁹ Liboro Dissenting Opinion, 10 December 2021, at 6, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

⁶⁰ *JMM Promotions & Management, Inc. v. National Labor Relations Commission*, G.R. No. 109835, 22 November 1993.

PLDT's failure to abide by Section 2.2 of the NTC MC can be cited to be a violation of the transparency principle of the DPA which we can hold PLDT accountable for.⁶¹

Contrary to what the dissent claims, this violation of the principle of transparency is not a small thing. It affects the lawful basis relied upon by PLDT especially considering it resulted in rendering useless the protections provided by NTC MC 05-06-07 and consequently, the DPA.

At the time of RLA's subscription in 2015, the Application Form that PLDT presented for the Corporate Individual DSL account only indicates the following statement:

The PLDT telephone service shall be provided by PLDT in accordance with the following terms and conditions and the rules and regulations as approved by the then Public Service Commission, now National Telecommunications Commission (NTC), as well as the rules and regulations issued by other appropriate government entities.⁶²

PLDT claims that the statement sufficiently complies with its legal obligation, which renders processing necessary for its compliance, simply because its Terms and Conditions, as stated in its Application Form, and its internal rules relating to the publication of directories, were approved by the then Public Service Commission.⁶³

The statement, however, is clearly not sufficient to adhere to the principle of transparency. This fact is also admitted by the dissent when it found that PLDT failed to provide "a valid and comprehensive privacy notice...."⁶⁴ Transparency requires that the information provided by the PIC, both in terms of content and the manner in which it was provided, would have allowed the data subject to understand the legitimate purpose of processing based on a legal obligation. As worded, the statement does not sufficiently make the lawful basis known to the data subject.

⁶¹ Liboro Dissenting Opinion, 10 December 2021, at 10, in RLA v. PLDT Enterprise, NPC 18-010 (NPC 2021) (pending).

⁶² Motion for Reconsideration, 05 August 2021, at 11, in RLA v. PLDT Enterprise, NPC 18-010 (NPC 2021) (pending).

⁶³ Comment to the Complaint dated 31 March 2018, 05 October 2018, at 4-6, in RLA v. PLDT Enterprise, NPC 18-010 (NPC 2018).

⁶⁴ Liboro Dissenting Opinion, 10 December 2021, at 12, in RLA v. PLDT Enterprise, NPC 18-010 (NPC 2021) (pending).

Based on the statement in its Terms and Conditions, PLDT cannot claim that its data subjects were aware of the nature, purpose, and extent of the processing of their personal information. Nowhere in the statement above does PLDT communicate its obligation to publish the personal information of its subscribers and inform RLA of his right to privacy and how his personal information would be protected. More importantly, it does not show that PLDT informed RLA of his option to not be listed in succeeding publications such as the 2017 White Pages. As stated in the Decision:

In this case, the recorded means that manifest the consent of the Complainant is PLDT's Application Form and the attached PLDT's Terms and Conditions that was printed on the back of the Form. We note however, that while the Terms and Conditions discuss the contractual relations that govern the usage, grant and maintenance of the DSL services between the Complainant and PLDT, the same does not include authority or consent to publish the list of names, contact information and address in the White Pages.⁶⁵

Despite the clear provisions of Section 2.2 of NTC MC 05-06-2007, PLDT failed to comply with the obligations provided therein from its issuance in 2007. PLDT had more than enough time to comply with its obligations and acquire its subscribers' consent before publishing their personal information in the White Pages. As discussed in the Decision:

Thus, we find that the consent given by Complainant in filling up the application form relates only to the use and limitations of the DSL services offered by PLDT, and not as to the publication of Complainant's personal information in the White Pages. Stated simply, the processing by PLDT was done for purposes not authorized by Complainant.⁶⁶

The Corporate Individual DSL Application Form for RLA's account did not contain any of the information required under NTC MC 05-06-2007, including the option to be excluded from publication. As explained by the Commission in its Decision, this not only deprived RLA of the opportunity to give his consent but also prevented him from knowing that such an option even exists:

⁶⁵ Decision, 17 December 2020, at 11, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending). Emphasis supplied.

⁶⁶ *Id.* at 11-12. Emphasis supplied.

Pieces of evidence at hand, particularly the PLDT Application Form that was submitted by Knutsen on behalf of Complainant on 12 January 2016 to PLDT, revealed that said form did not include an option to be excluded from the public directories published by PLDT.

Without such option, the data subjects such as Complainant will not have an opportunity to give their consent to the publication of their personal information in public directories.⁶⁷

PLDT only complied with its obligations when it revised its Application Form on 10 September 2018 even though the DPA and its IRR were passed in 2012 and 2016, respectively.⁶⁸ The inaction and belated actions of PLDT from the issuance of NTC MC 05-06-2007 in 2007 can hardly be considered the proactive response claimed by the dissent.⁶⁹

In its Motion for Reconsideration, PLDT asserts that it “acted in good faith and in compliance with the prevailing regulations and practice at the time in providing its services.”⁷⁰

To bolster PLDT’s assertions, the dissent claims that:

PLDT Group explained that it commenced addressing and remediating this perceived “DPA gap” since 08 July 2017 with the implementation of PLDT Home’s new Customer Information Sheet (Application Form). This remediation measure notwithstanding, printed customer information for subscribers acquired pre-08 July 2017 have been included in the directory listing by default. PLDT Group determines and recognizes this to be in conflict with the general data privacy principles of transparency, legitimate purpose and proportionality – the hallmarks of the DPA and its IRR.

PLDT requested from NTC an advisory opinion on the matter and/or guidance as to how to best approach the situation to ensure that service providers such as PLDT will be both compliant with the rules and regulations prescribed by the NTC and the requirements of the DPA and its IRR.

⁶⁷ Id. at 14. Emphasis supplied.

⁶⁸ Comment to the Complaint dated 31 March 2018, 05 October 2018, at Annex B, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2018) (pending).

⁶⁹ Liboro Dissenting Opinion, 10 December 2021, at 16, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

⁷⁰ Motion for Reconsideration by PLDT, Inc., 05 August 2021, at 8, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

In return, NTC in a letter dated 30 October 2017, requested an advisory opinion regarding the residential directory listing of PLDT and its group of affiliates to fulfill PLDT's obligations as a telephone service provider vis-à-vis its compliance with the DPA. It attached PLDT's letter dated 18 October 2017 and requested NPC to comment thereon.⁷¹

Curiously, however, none of these things claimed by the dissent can be found in the records of this case. On the contrary, the evidence on record shows that there was absolutely no action taken by PLDT from the time NTC MC 05-06-2007 was issued in 2007 until the events that gave rise to the Complaint.

PLDT hinges its claim of good faith on the measures it implemented after RLA had already filed his Complaint before the Commission on 03 April 2018. PLDT claims that it promptly tagged RLA's account as "Confidential" upon receiving his concerns, revisited its Corporate Individual DSL Application Form which it only implemented on 10 September 2018, and redefined its policies and processes based on the Advisory Opinion⁷² it requested from the Commission.⁷³

PLDT's obligation to comply with Section 2.2 of NTC MC 05-06-2007 cannot be excused simply because it sought guidance from the Commission by requesting an Advisory Opinion on the matter. Following *ignorantia juris non excusat*, "[t]hat every person is presumed to know the law is a conclusive presumption,"⁷⁴ legal obligations are not put on hold simply because those subject to it supposedly require guidance. It remains incumbent upon those subject to the law to comply with it.

Also, PLDT only sought clarification from the Commission in 2017 despite NTC MC 05-06-2007's issuance in 2007, and the DPA's effectivity in 2012.⁷⁵ In fact, PLDT only provided the option for its subscribers to be excluded from publication in the listing directory in 2018.⁷⁶

⁷¹ Liboro Dissenting Opinion, 10 December 2021, at 14, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

⁷² See National Privacy Commission, *Advisory on Telephone Directories*, Advisory Opinion No. 21, Series of 2018 (27 April 2018).

⁷³ See Liboro Dissenting Opinion, 10 December 2021, at 6, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

⁷⁴ *Villafuerte v. Cordial, Jr.*, G.R. No. 222450 (2020).

⁷⁵ See National Privacy Commission, *Advisory on Telephone Directories*, Advisory Opinion No. 21, Series of 2018 (27 April 2018).

⁷⁶ See Liboro Dissenting Opinion, 10 December 2021, at 6, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

The failure to comply with Section 2.2 of NTC MC 05-06-2007 for a period of eleven years from the issuance of this Memorandum Circular, despite knowing that the obligations provided therein applied to it, negates any claim of good faith on the part of PLDT. PLDT had sufficient time since 2007 to fulfil the obligations imposed by the NTC, its primary regulator, and yet, it failed to do so. Any claim of good faith is untenable because PLDT neither attempted nor took any action to comply with NTC MC 05-06-2007 from the time it was issued.

III. PLDT processed Personal Information for Unauthorized Purposes.

PLDT violated Section 28 of the DPA or the Processing of Personal Information for Unauthorized Purposes. Section 28 provides:

Section 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.⁷⁷

Processing for Unauthorized Purposes is committed when:

1. a person processed information of a data subject;
2. the information processed is classified as personal information or sensitive personal information;
3. the person processing the information has obtained consent of the data subject or is granted authority under the DPA or existing laws for a specific purpose; 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.

⁷⁷ Data Privacy Act of 2012, § 28. Emphasis supplied.

The first two requisites of Processing for Unauthorized Purposes have been established in this case. It is not disputed that PLDT processed its data subjects' personal information for the purpose of rendering its services. Thus, the Commission shall proceed to discuss the third and fourth requisites of Section 28 of the DPA.

A. PLDT obtained the consent of the data subject to process his or her personal information for a specific purpose.

The third requisite of Section 28 of the DPA or “the person processing the information obtained consent of the data subject or is granted authority under the DPA or existing laws” is present. PLDT obtained RLA's consent for the limited purpose of providing the services that RLA subscribed to.

In this case, PLDT obtained RLA's consent to process his personal information through the Corporate DSL Individual Application Form and the Terms and Conditions indicated therein. PLDT processed RLA's personal information to allow it to provide him with telephone and Corporate Individual DSL subscription services.⁷⁸ It is clear from the facts that PLDT processed RLA's personal information for a specific purpose:

As the corporate client, Knutsen collected the relevant personal data of the Complainant and provided such information to Respondent to enable the latter to provide the subscribed services. As noted by the Honorable Commission in its Decision, Complainant's personal information was supplied by his employer, Knutsen, the subscription was named under Knutsen (but for the account of Complainant), Knutsen President and General Manager is the signatory in the Application form, and Knutsen's address is indicated in the billing portion of the application form. Respondent only collected the information necessary to provide the service obtained by Knutsen for its employees ... Respondent is tasked with processing of the personal information of Knutsen's employees for the purpose of providing the DSL services which Knutsen's employees will use to perform their duties and responsibilities during their employment.⁷⁹

⁷⁸ Motion for Reconsideration by PLDT, Inc., 05 August 2021, at 11, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

⁷⁹ *Id.*

PLDT itself admitted in its Motion for Reconsideration that RLA provided his personal information for purposes of availing himself of the subscribed services:

Complainant merely provided his personal information to Knutsen to allow Respondent to install the necessary connectivity for the rendition of the subscribed services.⁸⁰

...

The information collected from the Complainant are standard information necessary for the purpose of providing the services under the DSL subscription (i.e. name, address, telephone number, and choice of plan).⁸¹

Without a doubt, RLA consented to the collection and processing of his personal information. RLA's consent, however, is only for the limited purpose of availing of the telephone and Corporate Individual DSL services offered by PLDT. As stated in the Decision:

Thus, we find that the consent given by Complainant in filling up the application form relates only to the use and limitations of the DSL services offered by PLDT⁸²

RLA only expected PLDT to process his personal information for the purpose of providing the subscribed services since the authority that RLA gave to PLDT and the information provided by PLDT are limited only to what are covered in the Application Form and the Terms and Conditions. Considering that PLDT obtained the consent of RLA to process his personal information for such limited purpose, the third requisite is present in this case.

B. PLDT further processed the personal information of the data subject without any authority given by the data subject or under the DPA or existing laws, and such further processing could not have been reasonably foreseen by the data subject.

The fourth requisite of Section 28 is satisfied in this case. PLDT further processed RLA's personal information by publishing his personal information in the listing directory without his authority.

⁸⁰ Id.

⁸¹ Id.

⁸² Decision, 17 December 2020, at 11, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2020) (pending). Emphasis supplied.

PLDT asserts that it lawfully processed RLA's personal information under a legal obligation when it published his personal information in the listing directory.⁸³ Processing necessary for compliance under a legal obligation is a criterion for lawful processing under Section 12 of the DPA. Section 12 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:

...

(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;⁸⁴

The law that serves as the basis for processing personal information determines the purpose of the processing, establishes specifications to determine the identity of the PIC, the categories of personal information subject to processing, the data subjects concerned, the entities to which personal information can be disclosed to, the purpose limitations, the storage measures, and other measures to ensure lawful and fair processing.⁸⁵ As such, compliance with a legal obligation as a criterion for lawful processing must be understood in relation to the law from which the purported legal obligation is derived from.

When a PIC, such as PLDT, claims lawful processing on the basis of a legal obligation, it is incumbent upon the Commission to examine (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. As such, the Commission is bound to look into the PIC's degree of compliance with the specific requirements of the legal obligation that it is relying on. In determining if the PIC is complying with the specific requirements of its legal obligations, the Commission is not enforcing the law or regulation that the PIC claims to be subjected to. Rather, the Commission is strictly enforcing the

⁸³ Motion for Reconsideration, 05 August 2021, at 2, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

⁸⁴ Data Privacy Act of 2012, § 12 (c). Emphasis supplied.

⁸⁵ EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 152 (2018).

provisions of the DPA and determining if the PIC's claim of processing as necessary to comply with its legal obligation is proper. Such is clearly within the mandate of the Commission.

1. The legal obligation which the PIC claims to be subject to exists and applies to the PIC.

PLDT argues that its mandate to publish stems from its legal obligation under Section 149 of Revised Order 1 and Section 2.2 of NTC MC 05-06-2007⁸⁶:

Respondent was mandated by Section 149 of the Revised Order No. 1, otherwise known as the Public Service Commission Rules and Regulations ("Order No. 1") and National Telecommunications Commission Memorandum Circular No. 05-06-2007, otherwise known as the Consumer Protection Guidelines ("NTC Circular") to issue a listing directory of the names, addresses, and telephone numbers of all of its subscribers at least once a year.⁸⁷

PLDT also highlights that Section 2.2 of NTC MC 05-06-2007 provides that the subscriber may request for his or her exclusion from subsequent publications of the listing directory.⁸⁸ It explains that if the subscriber does not exercise the right to be excluded, then the subscriber's name will be included in the listing directory.⁸⁹ PLDT categorically states that "[a]s worded, the NTC [Memorandum] Circular did not impose an obligation to secure from subscribers the affirmative act of consenting to the publication of [the subscriber's] contact information before a service provider can include the subscriber's information in the directory."⁹⁰

There is no question that PLDT is subject to its legal obligation under Section 149 of Revised Order 1 and Section 2.2 of NTC MC 05-06-07.

2. The processing of the data subject's personal information is necessary to comply with the legal obligation.

⁸⁶ Motion for Reconsideration, 05 August 2021, at 2, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

⁸⁷ *Id.*

⁸⁸ *Id.* at 3.

⁸⁹ *Id.*

⁹⁰ *Id.*

To consider compliance with a legal obligation as a valid criterion for lawful processing under Section 12 (c) of the DPA, there must be a clear showing that such processing is necessary.⁹¹ In determining what is considered “necessary”, the Commission takes into consideration both the processing undertaken and the legal obligation claimed by the PIC. The PIC should only process as much information as is proportional or necessary to achieve its clearly defined and stated purposes⁹², which in this case is to comply with the provisions of law and regulation. Aside from this, the processing undertaken by the PIC should relate to the fulfilment of its legal obligation.

In this case, the proportionality of the processing undertaken by PLDT is not in question. It is not claimed and no evidence has been presented to show that PLDT published more than what was required to be included in the listing directory. It is also not disputed that PLDT is required to publish a listing directory.

Even if the processing of the data subjects’ personal information is necessary to comply with its legal obligation, PLDT must still show that it fulfilled all the conditions imposed by the legal obligation it relied on.

3. All the conditions imposed by the legal obligation for the processing of personal information have not been complied with.

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.

In this case, PLDT’s compliance with a legal obligation as a valid criterion for lawful processing requires compliance with its legal obligation under both Section 149 of Revised Order 1 and Section 2.2 of NTC MC 05-06-2007. It, therefore, follows that determining the legal obligation that PLDT is required to comply with necessarily includes an examination of the obligations imposed by those two provisions. As

⁹¹ Data Privacy Act of 2012, § 12 (c).

⁹² *Id.* § 11.

previously discussed, for PLDT to say that it published the listing directory in compliance with a legal obligation under Section 149 of Revised Order 1 and Section 2.2 of NTC MC 05-06-2007, it must demonstrate that it also fulfilled the conditions under Section 2.2 of NTC MC 05-06-2007, which includes securing the consent of its subscribers before publishing their personal information in the listing directory.

The obligation to substantiate the fulfilment of the conditions that qualify the general obligation to publish the listing directory rests on PLDT. It necessarily follows that it is incumbent upon PLDT to show that first, it presented to the subscriber the option to not be listed in the directory listing; second, it presented the option at the time of subscription to PLDT's services; and third, the subscriber refused the option presented to him. It is only when these conditions are satisfied that PLDT can publish the subscriber's personal information in the listing directory.

The Commission reiterates that compliance with the legal obligation imposed by NTC MC 05-06-2007 necessitates securing the consent of the data subject, which is consistent with transparency and consent under the DPA. Stated simply, PLDT should have secured the data subject's consent before it published his or her personal information in the listing directory.

If PLDT fully complied with its legal obligation, then it can validly claim that the processing by means of publishing personal information in the listing directory was proper. It is incumbent upon PLDT to show that the actions it took resulted in its compliance with its obligation or is an integral step in getting to the point of compliance. This is something PLDT failed to do.

Although PLDT obtained RLA's consent, the authority granted to PLDT was only for the purpose of providing the telephone and Corporate DSL subscription services. It does not extend to the publication of RLA's personal information in the listing directory.⁹³

RLA could not have reasonably foreseen that PLDT intended to process his personal information by publishing it in the listing

⁹³ Decision, 17 December 2020, at 11 in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2020) (pending).

directory. In fact, the statement in the Terms and Conditions stated in the Application Form that was presented to Knutsen does not adequately declare and specify the purpose of publishing data subjects' personal information in the listing directory. Neither PLDT's Application Form nor its Terms and Conditions provided the necessary information that would have allowed its subscribers, like RLA, to reasonably foresee that their personal information would be published, much less allow them to exercise their right to be excluded from the listing directory or even know that such a right exists in the first place.

It bears stressing that the obligations and conditions provided in Section 2.2 of NTC MC 05-06-2007 are directed to PLDT as the one subject to the regulatory jurisdiction of the NTC, its primary regulator. PLDT cannot pass the responsibility to its subscribers by saying that “[i]f [the subscriber] did not exercise this right to be excluded [from the publication], his/her name will be included in the directory listing”⁹⁴ especially considering that PLDT never informed its subscribers of this option in the first place.

Subscribers such as RLA are not obligated to determine for themselves the regulations their services providers are supposed to comply with. This is all the more true considering that Section 2.2 itself imposes a positive duty on PLDT to inform its subscribers of the specifically required information and to give them the option not to be listed in the public directory listing.

PLDT had several instances to comply with its obligation to apprise its subscribers of their right to privacy, the manner by which their personal information would be protected, and inform them of their option to not be listed in succeeding publications of PLDT's listing directory. The NTC issued NTC MC 05-06-2007 as early as 2007, but PLDT failed to comply with the requirements under the Circular. Stemming from PLDT's positive obligation to secure the consent of the data subject under both NTC MC 05-06-2007 and the DPA, PLDT must show that it communicated to its subscribers the option to not be listed in the listing directory and that they refused to take the option.

Specific to this case, PLDT could have apprised RLA of his right to be excluded from publication of his personal information in the listing directory it published in 2017. The Application Form for the Corporate

⁹⁴ Motion for Reconsideration, 05 August 2021, at 3, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

Individual DSL account subject of this case was signed on 21 December 2015⁹⁵, and Knutsen requested the transfer of RLA's Corporate Individual DSL account to a new address on 12 April 2016.⁹⁶ PLDT could have informed RLA in 2015, when Knutsen opened a Corporate Individual DSL account on his behalf, and again in 2016, when Knutsen requested a transfer of his account to his new address. PLDT, however, failed to do so. Even when the IRR of the DPA was issued on August 2016, PLDT still did not do anything before it published RLA's personal information in the listing directory in 2017.

Absent a clear showing that PLDT fully complied with the obligations and conditions set out in both Section 149 of Revised Order 1 and Section 2.2 of NTC MC 05-06-2007, it failed to fulfil its legal obligation. As such, PLDT cannot rely on compliance with a legal obligation as its criterion for lawful processing. From its plain wording, this criterion necessarily requires compliance with the legal obligation claimed and, consequently, presupposes that everything required by that legal obligation has been complied with.

Considering that PLDT processed RLA's personal information without satisfying a valid criterion for lawful processing under Section 12 (c) of the DPA, and in the absence of any other basis for lawful processing that has been validly asserted by PLDT, it is liable under Section 28 of the DPA on Processing of Personal Information for Unauthorized Purposes.

IV. PLDT committed Unauthorized Disclosure.

PLDT violated Section 32 of the DPA on Unauthorized Disclosure. As held in the Decision dated 17 December 2021, all the elements of Section 32 are present in this case.⁹⁷ In particular, the Decision provides:

[T]he copies of PLDT's 2017 White Page[s] or Directory is distributed to its subscribers. All the personal information found therein are disclosed to PLDT'[s] subscribers and to other persons who may be given a copy thereof.⁹⁸

⁹⁵ PLDT Application Form for Corporate Individual DSL Account (21 December 2015).

⁹⁶ Letter from Knutsen Philippines, Inc. to PLDT, Inc. (12 April 2016).

⁹⁷ Decision, 17 December 2020, at 19, in RLA v. PLDT Enterprise, NPC 18-010 (NPC 2020) (pending).

⁹⁸ *Id.*

Section 32 of the DPA on Unauthorized Disclosure states:

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).⁹⁹

Section 32 of the DPA refers to “the immediately preceding section” or Section 31 of the DPA on Malicious Disclosure, which states:

Section 31. Malicious Disclosure. – Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to 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).¹⁰⁰

Malicious disclosure is committed when the following requisites concur:

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.

A PIC or a PIP may be held liable for malicious disclosure if it discloses unwarranted or false personal or sensitive personal information with malice or in bad faith.¹⁰¹ A finding of Malicious Disclosure requires that first, the disclosed personal information is unwarranted or false, and

⁹⁹ Data Privacy Act of 2012, § 32.

¹⁰⁰ Id. § 31.

¹⁰¹ Id.

second, the disclosure is malicious or in bad faith. If either of these two requisites is absent, then the offense falls under Section 32 or Unauthorized Disclosure.

While it is true that criminal and penal statutes must be strictly construed,¹⁰² a strict reading of Section 32 of the DPA or Unauthorized Disclosure shows that a PIC or a PIP will be penalized if it discloses personal information without the consent of the data subject even if such disclosure is justified under some other criteria for lawful processing enumerated in Sections 12 and 13 of the DPA.

The rules of statutory construction are clear:

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.¹⁰³

If Section 32 is understood in its literal sense, then it will result in an absurd situation. A PIC or PIP will be held liable for unauthorized disclosure even if it validly processed personal information based on some other lawful criteria under Sections 12 and 13 but failed to obtain the data subjects' consent.

Further, Section 32 of the DPA on Unauthorized Disclosure should be read together with the entire 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.¹⁰⁴

¹⁰² U.S. v. Go Chico, G.R. No. 4963 (1909).

¹⁰³ Metropolitan Bank and Trust Co. v. Liberty Corrugated Boxes Manufacturing Corp., G.R. No.184317 (2017).

¹⁰⁴ Fort Bonifacio Development Corp. v. Commissioner of Internal Revenue, G.R. Nos. 158885 & 170680 (Resolution) (2009).

Section 32 of the DPA should not be read in isolation. It should be read together with the other provisions of the DPA, particularly Sections 12 and 13 on the criteria for lawful processing of personal and sensitive personal information. A plain reading of Sections 12 and 13 will show that consent is just one of the lawful criteria for processing. As such, the presence of any of the criteria listed in either section is sufficient to justify the processing of personal or sensitive personal information as the case may be. To require the consent of the data subject when some other lawful criteria such as law or regulation requires or justifies the processing of the personal information, including its disclosure, will result in absurdity. Such literal interpretation based on an isolated reading of Section 32 of the DPA will render Sections 12 and 13 of the DPA inoperative.

The rule is that a construction that would render a provision inoperative should be avoided; instead, apparently inconsistent provisions should be reconciled whenever possible as parts of a coordinated and harmonious whole.¹⁰⁵

A proper reading of Section 32 should be that Unauthorized Disclosure is committed when the perpetrator processes personal information without any of the lawful basis for processing under Sections 12 and 13. This interpretation 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.”¹⁰⁶ As such, Section 32 of the DPA is violated if none of the lawful basis of processing, consent or otherwise, supports the disclosure of personal information. This interpretation is more beneficial to the accused since it actually narrows the extent to which disclosure of personal information may be considered as unauthorized disclosure.

In this case, however, the obligation imposed by NTC MC 05-06-2007 is based on the consent of the subscribers. As previously discussed, public telecommunications entities must secure the consent of their subscribers before publishing their personal information in the listing directory. Absent any showing of consent, PLDT is not permitted to publish personal information in the listing directory. It is only when the subscribers avail themselves of the option to be included in the

¹⁰⁵ JMM Promotions & Management, Inc., G.R. No. 109835 (1993). Emphasis supplied.

¹⁰⁶ People v. Liban, G.R. Nos. 136247 & 138330 (2000).

listing directory after being informed by PLDT of such option that PLDT may publish their personal information.

Here, PLDT published the personal information of its subscribers in the listing directory without securing their consent. In fact, PLDT failed to present the option to not be included in the listing directory to any of its subscribers despite being required to do so by NTC MC 05-06-2007, which was issued as early as 2007. PLDT did not present the option and secure its subscribers' consent until 10 September 2018.¹⁰⁷ It took PLDT eleven years to revise its Application Form for the Corporate Individual DSL account to include the option to not be listed in the listing directory. PLDT failed to obtain the consent of its data subjects before it published their personal information in the listing directory.

By publishing its subscribers' personal information in the White Pages without their consent, contrary to the provisions of Section 2.2 of NTC MC 05-06-2007, and distributing free copies of the White Pages to all its subscribers, who are considered third parties under the DPA, PLDT violated Section 32 of the DPA on Unauthorized Disclosure.

V. PLDT is grossly negligent.

PLDT manifested gross negligence when it failed to acquire its subscribers' consent to publish their personal information in the listing directory since 2007. Its failure to inform its subscribers of the option to not be listed in the listing directory resulted in its violation of Section 28 of the DPA. The Supreme Court defines gross negligence as:

Gross negligence implies a want or absence of or a failure to exercise slight care or diligence, or the entire absence of care. It evinces a thoughtless disregard of consequences without exerting any effort to avoid them.¹⁰⁸

In its Motion for Reconsideration, PLDT maintains that its actions do not “rise to the level of gross negligence that would merit criminal sanction.”¹⁰⁹ PLDT, however, failed to present substantial evidence to

¹⁰⁷ Comment to the Complaint dated 31 March 2018, 05 October 2018, at Annex B, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2018) (pending).

¹⁰⁸ *Casco v. NLRC*, G.R. No. 200571 (2018).

¹⁰⁹ Motion for Reconsideration, 05 August 2021, at 6, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending). Emphasis supplied.

support its statement that its responsible officers should not be held liable for PLDT's violations of Sections 28 and 32 of the DPA.

It is established that bare allegations without evidence is neither considered as nor equivalent to clear and convincing proof.¹¹⁰ As held in the Decision dated 17 December 2020, PLDT can only act through the members of its Board of Directors, its Corporate Officers, and its employees. It would not have violated Sections 28 and 32 of the DPA without the participation of one or some of these individuals:

Since a corporation, like PLDT, can only act through its Board of Directors, Corporate Officers, and employees, these DPA violations must have been committed by the Board of Directors, Corporate Officers, or employees of PLDT either directly or through their gross negligence. Information necessary to identify these responsible officers/ employees is usually within the control of the respondent PIC and not readily or easily available to the Complainant.¹¹¹

The case has been remanded to the Commission's Complaints and Investigation Division to identify the responsible officers liable for the violations of Sections 28 and 32.¹¹²

In any case, the violation of Sections 28 and 32 arose because PLDT failed to abide by Section 2.2 of NTC MC 05-06-2007. PLDT should have been aware of the conditions stated in Section 2.2 since it was issued by NTC, its primary regulator.

Further, in its representations, PLDT made it seem that Section 149 of Revised Order 1 and Section 2.2 of NTC MC 05-06-2007 require the mandatory publication of the personal information of the data subject.

[PLDT] published [RLA's] personal information in the 2017 directory listing in compliance with the requirement prescribed by Order No. 1 and the NTC Circular.¹¹³

As previously discussed, however, while it is true that Section 149 of Revised Order 1 requires public telecommunications entities to

¹¹⁰ United Claimants Association of NEA v. National Electrification Administration, G.R. No. 187107 (2012); Cordova v. Ty, G.R. No. 246255 (2021).

¹¹¹ Decision, 17 December 2020, at 22, in RLA v. PLDT Enterprise, NPC 18-010 (NPC 2020) (pending).

¹¹² Id. at 23.

¹¹³ Motion for Reconsideration, 05 August 2021, at 5, in RLA v. PLDT Enterprise, NPC 18-010 (NPC 2021) (pending).

publish a directory listing at least once a year, such legal obligation is subject to the conditions in Section 2.2 of NTC MC 05-06-2007.

PLDT, however, made no effort whatsoever to bring its processing of personal information in line with the obligations imposed on public telecommunication entities enumerated in NTC MC 05-06-2007, much less the DPA. In fact, PLDT selectively limited its appreciation of Section 2.2 of NTC MC 05-06-2007 to the last sentence. In its Motion for Reconsideration, PLDT argues that:

Section 2.2 of NTC Circular shows that the subscriber is given the option not to be included in succeeding public directory listings of subscribers. From this provision, it can be gleaned that the subscriber may request for his or her exclusion in the subsequent publication of the directory listing. If s/he did not exercise this right to be excluded, his or her name will be included in the directory listing. As worded, the NTC Circular did not impose an obligation to secure from subscribers the affirmative act of consenting to the publication of his/ her contact information before a service provider can include the subscriber's information in the directory.¹¹⁴

The dissent noted the applicability of the principle *ut res magis valeat quam pereat* to this case and correctly explained that “care should be taken that every part thereof be given effect and a construction that could render a provision inoperative should be avoided, and inconsistent provisions should be reconciled whenever possible as parts of a harmonious whole.”¹¹⁵

Despite this, both the dissent and PLDT conveniently ignored the other sentences in Section 2.2 of NTC MC 05-06-2007. They failed to address or recognize its other obligations, which are in fact harmonious with the DPA. Contrary to PLDT's assertions, the subscriber must give his or her consent before his or her personal information may be published in the directory listing. PLDT, however, by failing to provide RLA with the proper mechanism to exercise the option, disregarded RLA's right to consent to the publication of his personal information in the 2017 White Pages.

¹¹⁴ *Id.* at 3.

¹¹⁵ Liboro Dissenting Opinion, 10 December 2021, at 8, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

In failing to fulfil its obligations according to Section 2.2 of NTC MC 05-06-2007, PLDT's acts resulted in a violation of the DPA since it processed personal information for an unauthorized purpose, and disclosed personal information without the consent of the data subject. By failing to present the option to not be listed in the directory listing to RLA, PLDT deprived RLA of his right to exercise such option. For these reasons, PLDT is grossly negligent as shown by its repeated failure to comply with the obligations imposed on it.

Any finding of gross negligence is not removed by any corrective actions taken by PLDT. It had all the opportunities to comply with its obligations under NTC MC 05-06-2007. PLDT should have complied with its obligations from the time the Circular was issued in 2007. The passage of the DPA in 2012 and the IRR in 2016 should have also prompted PLDT to conduct a closer examination of its processing activities, including the obligations imposed by its primary regulator in NTC MC 05-06-2007. Yet, PLDT failed to do so.

PLDT should have at least tried to acquire the consent of all its subscribers in order to lean towards the safe mandate of the law, and if such consent was not acquired, it should not have pushed through with publishing the personal information of the subscriber.

After all, in the event of uncertainty, a PIC must always be mindful of the rights and interests of the data subjects. Section 38 of the DPA provides:

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.¹¹⁶

The Commission reiterates that while PLDT is mandated to publish a listing directory by Section 149 of Revised Order 1, such obligation to publish necessarily requires acquiring the consent of its subscribers. The Commission cannot overlook PLDT's inaction since 2007 in failing to acquire the consent of its subscribers since the DPA mandates that doubts in the interpretation should be in favor of the rights and interests of the data subject whose personal information is processed.¹¹⁷ Had PLDT intended to act to the best of its intentions, it

¹¹⁶ Data Privacy Act of 2012, § 38. Emphasis supplied.

¹¹⁷ *Id.*

would have resolved any supposed confusion in favor of an interpretation that gives greater protection to the rights of its data subjects.

In arguing in favor of PLDT, the dissent harps on the supposed fact, “NTC did not disallow the succeeding publications of PLDT... [nor did it] admonish PLDT nor issue other orders that would indicate that PLDT has been publishing in White Pages in violation of the NTC MC 05-06-2007.”¹¹⁸

Aside from the fact that these cannot again be found in the records of this case, the argument is misplaced. To be clear, the Commission is not enforcing the provisions of NTC MC 05-06-07. Rather, it is simply fulfilling its mandate under the DPA to examine the presence of, and the proper application of lawful criteria to the processing undertaken by the PIC.

Considering that PLDT claims its compliance with a legal obligation as basis for its publishing the name of RLA in the White Pages, the Commission is mandated to look into whether all conditions imposed by the legal obligation have been complied with. After all, an essential element for any claim of valid processing under this criterion is that everything required by the claimed legal obligation as a condition for the processing has been complied with.

The dissent also claims that “the Decision dated 17 December 2020 overlooked certain aspects which, if not corrected, will cause extreme and irreparable damage and prejudice as to how the DPA should be interpreted and applied.”¹¹⁹ The Decision dated 17 December 2020 was written by the dissenting Commissioner. If he truly believed that it will cause “extreme and irreparable damage and prejudice,” he should not have written the Decision in that way. And if the Decision supposedly overlooked certain things, he only has himself to blame.

Besides, despite the dissent’s protestations that the Commission should not apply the law mechanically and must consider “fairness, equity, and judiciousness in its decisions”¹²⁰, the dissent never bothered to discuss what about the majority opinion, and

¹¹⁸ Liboro Dissenting Opinion, 10 December 2021, at 9, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

¹¹⁹ *Id.* at 9.

¹²⁰ *Id.* at 2.

consequently his own Decision, is unfair or unjust based on the law and the records of this case.

It bears stressing that the Commission's Decision cannot be overturned based simply on equity as claimed by the dissent. It also cannot be overturned based on a convenient change of mindset and a rejection of the idea that recommending an organization for prosecution will have the deterrent effect intended by the legislators in favor of some abstract notion of organizational accountability.¹²¹

The Commission does not exercise any discretion in applying the penalty provisions of DPA. As long as all the elements of the offense are met by the facts and evidence on record, then the Commission is constrained to apply the law and recommend the prosecution of the PIC and its responsible officers. It is not up to the Commissioners to arbitrarily introduce a subjective interpretation restricting the applicability of these provisions only to those "who wilfully violate the law" under the guise of "put[ting] on wider lenses" when implementing the law.¹²²

It should go without saying that any change in the Commission's Decision must be based on the law and the available evidence on record. In the case of PLDT, it has failed to present anything new or substantial to warrant a reversal of the Decision dated 17 December 2020.

Considering the foregoing, the Decision dated 17 December 2020 should be maintained. PLDT is liable for violations of the DPA, particularly Section 28 or Processing of Personal Information for Unauthorized Purposes and Section 32 or Unauthorized Disclosure. In failing to comply with the directive of its primary regulator, PLDT likewise failed to comply with its obligation under the DPA to ensure that any processing it undertakes finds basis under one of the lawful criteria provided under the law.

¹²¹ *Id.* at 17.

"Thus, the idea of imposing a penalty on "the organization" in the belief that "it" will respond as a single integrated organism and avoid some future actions that result in breaches of a rule simplistic and may not always prove true. Even now, the NPC continues to conduct awareness campaigns to guide the PICs or PIPs. NPC have been leaders and protectors. And enforcers, especially against those who wilfully violate the law. As NPC advances, the Commission is urged to put on wider lenses when adjudicating cases to enable the PICs to thrive and encourage organizational accountability without fear of being put behind bars while meting justice to data subjects."

¹²² See, *Liboro Dissenting Opinion*, 10 December 2021, at 17, in *RLA v. PLDT Enterprise*, NPC 18-010 (NPC 2021) (pending).

WHEREFORE, premises considered, the Commission resolves to DENY the Motion for Reconsideration filed by PLDT Enterprise. The Decision dated 17 December 2020 is hereby AFFIRMED.

SO ORDERED.

City of Pasay, Philippines. 10 December 2021.

Sgd.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

I CONCUR:

Sgd.

JOHN HENRY D. NAGA

Deputy Privacy Commissioner

See Dissenting Opinion.

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

Copy furnished:

RLA

Complainant

AACRC

Counsel for Respondent

COMPLAINTS AND INVESTIGATION DIVISION

ENFORCEMENT DIVISION GENERAL RECORDS UNIT

National Privacy Commission

RLA,
Complainant,

NPC 18-010

(Formerly CID CaseD-010)

versus

For: Violation of the Data Privacy Act of 2012

PLDT ENTERPRISE

Respondent.

DISSENTING OPINION

LIBORO, P.C.:

The main issue before the Commission is whether or not the Decision dated 17 December 2020 (Decision) of the Commission should be sustained.

On 17 December 2020, the Commission issued a Decision with the following dispositive portion, to wit:

WHEREFORE, all these premises considered, this Commission resolves to AWARD Complainant, RLA, nominal damages in the amount of Fifty Thousand Pesos (P50,000.00) for Respondent PLDT Enterprise's violation of Complainant's rights under the Data Privacy Act.

Moreover, this Commission resolves to **REMAND** this case to the Complaints and Investigation Division for the limited purpose of determining and identifying the responsible persons, officers, or individuals of PLDT Enterprise who caused the violations of Sections 28 and 32 of the DPA prior to recommending the matter to the Secretary of Justice for criminal prosecution.

SO ORDERED.¹²³

The majority opines that the Decision dated 17 December 2020 of the Commission should be sustained which found that PLDT Enterprise (Respondent or PLDT) is liable for violation of Sections 28 and 32 of

¹²³ NPC 18-010 Decision dated 17 December 2020.

the Data Privacy Act of 2012 (DPA), awarded nominal damages to RLA (Complainant or RLA) and remanded the case to the Complaint and Investigation Division of the National Privacy Commission (NPC) for further investigation and for the determination of the responsible officers of PLDT, who by participation, negligence, or omission, allowed the violations of Section 28 and 32 of the DPA.

With all due respect, I am constrained to dissent.

At this juncture, it must be stressed that the Commission is adjudicating not only the merits of the case, but also how present and future Commissioners of the NPC will apply the provisions of the law.

The Commission must breathe life and meaning to the law. The Commission must consider real scenarios that affect real lives and livelihood to provide guidance to present and future privacy practitioners, litigators, judges, or justices for all DPA-related cases.

Rather than applying the law mechanically or in a straight-jacket, the Commission must also factor equity, fairness, and judiciousness in its decisions to prevent unjust decisions, since each case that the Commission adjudicates has its peculiar facts which may have a bearing on the present issue at hand.

Each decision has the potential to create far-reaching implications. The Commission can set precedents that may enhance how privacy is applied or change how data privacy is practiced in the country.

Beginning with the easiest point, I agree with the majority that that PLDT is a personal information controller (PIC). Hence, PLDT's argument in its Motion for Reconsideration dated 05 August 2021 (Motion for Reconsideration) that it is a Personal Information Procession (PIP) for its enterprise clients does not warrant further deliberation.

However, I dissent to deny the Motion for Reconsideration filed by PLDT Enterprise for the following reasons:

I. PLDT has lawful basis for processing Complainant's personal information

The personal data of Complainant involved in this case is personal information, i.e. name, telephone number and residence address. Personal information is treated differently from sensitive personal information under the DPA. Processing of personal data is allowed as a general rule,¹²⁴ whereas processing of sensitive personal information is prohibited by default.¹²⁵ Section 12 of the DPA provides:

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.¹²⁶

When personal information is processed, it is enough that one (1) of the criteria for lawful processing under Section 12 of the DPA is present. Without any of these criteria, the PIC or PIP can be held liable for violation of Section 28 of the DPA.

Section 28 of the DPA penalizes processing of personal information for purposes not authorized by the data subject, or otherwise authorized under the DPA or under existing laws, to quote:

¹²⁴ Section 12 of the DPA.

¹²⁵ Section 13 of the DPA.

¹²⁶ *Supra*.

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.¹²⁷ (Emphasis and underlining supplied)

Consent, which is the main argument of Complainant, is only a criterion. To be held liable under Section 28, the PIC or PIP must process personal data in violation of the purpose consented to or authorized by the data subject, or otherwise authorized by the DPA or under existing laws.

It is crucial then to determine if aside from consent, did PLDT process Complainant's information on the basis of other lawful criteria provided for under Section 12 of the DPA?

PLDT hinges the lawfulness of its processing on the compliance with a legal obligation to which it is subjected, as required by Section 149 of the Revised Order No. 1, the Public Service Commission (PSC) Rules and Regulations, implementing Commonwealth Act No. 146 or the Public Service Act enacted in 1940.

Section 149 of Revised Order No. 1 clearly mandates each telephone public service to issue a listing directory at least once a year, to wit:

Section 149. Telephone Directory. – Each telephone public service shall at least once a year issue a listing directory showing therein the names of all subscribers arranged in alphabetical order, their addresses and telephone numbers and such other information as may be of interest to a subscriber's everyday use of his telephone. Each subscriber shall be entitled to a free copy of the directory.¹²⁸

At that time, this type of processing is necessary. People or institutions did not have access to the internet and other means to publicly look for telephone numbers and addresses. The circumstances of the times dictate the need for the publication. The wordings of Section 149 were prepared at a time where people used paper copies of telephone directories.

¹²⁷ Section 28 of the DPA.

¹²⁸ Public Service Commission, Public Service Commission Rules and Regulations for all Public Services, Revised Order No. 1, Section 149.

The most popular device to communicate back then is the telephone. Undoubtedly, being part of the telephone directory have its benefits and corresponding trade-offs. Each one of us who had landlines experienced receiving prank calls by reason of being part of the PLDT White Pages. However, the White Pages proved to be helpful when the need arises, and one needs the contact information of a friend or relative that they need to reach.

In the year 2000, there was a shift from analogue to digital in the way people communicate with each other. A technological convergence happened marked by introductions of new technologies and innovations. This created new products and services and started to blur the boundaries of platforms then used for communication. New platforms were used in entertainment and communication which undermined consumer rights and protection. There was a time when the Philippines was the texting capital of the world, and to date, it remains as home for the Top SMS Senders in the world.

In relation to Section 149 of Revised Order No. 1, the National Telecommunications Commission (NTC) issued Memorandum Circular No. 05-06-2007 dated 08 June 2007 (Consumer Protection Guidelines or NTC MC 05-06-2007), which provides:

Section 2.2-Any data supplied by the consumer shall be treated as confidential by the entity or service provider mentioned under Section 1.1 hereof and shall not be used for purposes not authorized by him. Upon subscription, he shall be informed of his right to privacy and the manner by which his data would be protected. **In cases where a public directory listing of subscribers is regularly published by the service provider, the consumer shall be given the option not to be listed in succeeding publications.**¹²⁹

Since NTC MC 05-06-2007 is a later issuance, the provisions of Section 149 of Revised Order No. 1, the PSC's Rules and Regulations for all public services, is considered amended or modified only insofar as **giving the consumer the option not to be listed in succeeding publications.**

¹²⁹ National Telecommunication Commission, Consumer Protection Guidelines [NTC Memo. Circ. No. 05-06-2007], Section 2.2 (08 June 2007).

While it is true that NTC MC 05-06-2007 effectively subjected Section 149 of Revised Order No. 1 the PSC's Rules and Regulations to the condition set forth by **NTC MC 05-06-2007, NTC MC 05-06-2007 did not remove the legal obligation of telephone public service providers to publish the telephone directory at least once a year.**

That the NTC MC 05-06-2007 did not remove the legal obligation to publish the list of names in telephone directories, is bolstered upon closer scrutiny of the NTC MC.

For everyone to benefit from these new technologies and innovations, the free flow of information needs to be ensured. Thus, the NTC MC 05-06-2007 was issued to address wider consumer protection. NTC MC 05-06-2007 is an issuance that aims to address Consumer Protection Guidelines.¹³⁰ It was issued by the NTC to curb the then proliferation of push messaging,¹³¹ spam messages,¹³² and value-added services¹³³ (VAS) by Public Telecommunications Entities (PTEs) such as PLDT, Broadcast and Cable Television Companies (CATV), and Value- Added Service (VAS) and Content Providers (CPs).¹³⁴

By way of example, common VAS encountered by subscribers included Content and Program service¹³⁵ which includes music, ringtones, logos, video clips that would expose consumers to charges without their consent. These are what the NTC Memorandum Circular sought to address.

The intent of the guidelines become more obvious when reading through Sections 2.2 to 2.12 of the NTC MC 05-06-2007 which revolve around the obligation of Telecommunications providers to prevent unauthorized charges against subscribers to protect and uphold consumer rights.¹³⁶

¹³⁰ Subject Title, Id.

¹³¹ National Telecommunication Commission, Consumer Protection Guidelines [NTC Memo. Circ. No. 03-03-2007], Section 3 (03 July 2006).

¹³² Section 4, Id.

¹³³ National Telecommunication Commission, Voice Over Internet Protocol [NTC Memo. Circ. No. 05-08-2005], Section 2 (e), (23 August 2005)

¹³⁴ National Telecommunication Commission, Consumer Protection Guidelines [NTC Memo. Circ. No. 05-06-2007], Section 1.1 (08 June 2007).

¹³⁵ National Telecommunication Commission, Voice Over Internet Protocol [NTC Memo. Circ. No. 02-05-2008], Section 2 (I), (30 May 2005).

¹³⁶ See National Telecommunication Commission, Voice Over Internet Protocol [NTC Memo. Circ. No. 02-05-2008], at Sections 2.2 to 2.11. (30 May 2005).

NTC MC 05-06-2007 did not make the publication of the telephone directory optional. Neither did the NTC Memorandum Circular mandate the telephone public service providers to stop the publication of telephone directories.

PLDT in its Motion for Reconsideration, argued that the subscriber may request for his/her exclusion in the subsequent publication of the directory listing. If he/she did not exercise this right to be excluded, his/her name will be included in the directory listing. As worded, the NTC MC did not impose an obligation to secure from subscribers the affirmative act of consenting to the publication of his/her contact information before a service provider can include the subscriber's information in the directory.¹³⁷

In effect, PLDT is introducing an interpretation that PLDT's legal obligation to publish is the default position, while an opt-out of the consumer is required for it to remove the personal information in the succeeding publications and thereby treat the same as confidential, consistent with Section 2.2 of the NTC MC 05-06-2007.

To address this contention, NTC MC 05-06-2007 must be read as a whole **applying the principle of “ut res magis valeat quam pereat”** as adequately explained by the Supreme Court in the case of Philippine International Trading Corporation v. Commission on Audit:¹³⁸

It is a rule in statutory construction that 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 the other parts, and kept subservient to the general intent of the whole** enactment. Because the **law must not be read in truncated parts**, its provisions must be read in relation to the whole law. The statute's clauses and phrases must not, consequently, 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. Consistent with the fundamentals of statutory construction, all the words in the statute must be taken into consideration in order to ascertain its meaning. (Emphasis and underlining supplied)

¹³⁷ Motion for Reconsideration filed by PLDT on NPC 18-010 dated 05 August 2021 at pp. 3.

¹³⁸ G.R. No. 183517, 22 June 2010.

Moreover, the Supreme Court held that in construing the law, care should be taken that every part thereof be given effect and a construction that could render a provision inoperative should be avoided, and inconsistent provisions should be reconciled whenever possible as parts of a harmonious whole. For taken in solitude, a word or phrase might easily convey a meaning quite different from the one actually intended and evident when a word or phrase is considered with those with which it is associated.¹³⁹

Following the foregoing postulates and construing the provisions of Section 2.2 of NTC MC 05-06-2007 in its entirety, the consumer must opt-out before he/she can be removed from the succeeding publications which remain to be the default procedure for telecommunication companies as provided by Section 149 of Revised Order No. 1.

Prior to the issuance of the NTC MC 05-06-2007, since 1958, PLDT has been publishing in the White Pages the list of names, addresses and numbers of its subscribers pursuant to Section 149 of Revised Order No. 1. Hence, all subscribers have reasonable expectation that some of their information may be published even without their consent. This processing has become an industry practice supported by a legal obligation.

When the NTC MC 05-06-2007 came to effect, the consumers were given an option to opt-out of the publication in succeeding publications. Nevertheless, publication in the White Pages remain to be the default option without the consumers opting out.

In other words, the passage of the NTC MC 05-06-2007 did not stop the publication of the personal information of subscribers in the White Pages in the absence of their consent. Otherwise, the NTC MC would have expressly stated so in its issuance.

It may be surmised that NTC's interpretation of the NTC MC 05-06-2007 treating the subscriber's personal information as confidential once they opt-out from the publication is consistent with PLDT's interpretation.

Apparently, the NTC did not disallow the succeeding publications of PLDT. It did not admonish PLDT nor issued other orders that would indicate that PLDT has been publishing in White Pages in violation of the NTC MC 05-06-2007. Neither did NTC issue succeeding issuances that would clarify the matter and enforce the standards of consumer protection in NTC MC 05-06-2007. This is how NTC enforced the NTC MC 05-06-2007.

These badges manifest that to a certain extent, PLDT has been performing its legal obligation to publish in the White Pages within the standards set by the NTC for the industry during that time.

As explained by Respondent in its Motion for Reconsideration, it has complied with the qualifying clause under Section 2.2 of NTC MC 05-06-2007. Upon receiving Complainant's request, Respondent tagged the Corporate Individual Account under Knutsen Philippines, Inc. (Knutsen) as "Confidential" and confirmed that Complainant's personal information would not be published in the succeeding directories.¹⁴⁰

Now we come to the question on the effects of the failure of PLDT to strictly comply with the provisions of NTC MC 05-06-2007 as to the validity of its processing activities after the DPA came to effect and the NPC was established.

After evaluating the context of the issuance behind the NTC MC 05-06-2007, the peculiar facts and circumstances surrounding the processing activities, and the position adopted by the NTC which is the implementing agency for both issuances, the NTC MC 05-06-2007 certainly did not remove PLDT's legal obligation to publish and process the personal data.

It must be noted that the failure of PLDT to include an opt-out option to be listed in succeeding publications is not fatal to its legal obligation to publish telephone directories. In other words, the inclusion of an opt-out function is not one that is so necessary to the processing questioned. The absence of the opt-out function would not outright remove the publication requirement in the Public Service Act since the legal obligation subsists even without this additional safeguard.

¹⁴⁰ Id. at p. 5.

Nevertheless, the opt-out function is a consumer protection mechanism under the NTC MC 05-06-2007 that is aligned with the DPA. In particular, the option not to be published in the White Pages enhances the data subject's control over how his/her data would be processed. Moreover, Section 2.2 of NTC MC 05-06-2007 also essentially requires a privacy notice that would indicate how PLDT will protect the data.

PLDT's failure to abide by Section 2.2 of the NTC MC can be cited to be a violation of the transparency principle of the DPA which we can hold PLDT accountable for.

However, the violation of the general data privacy principle of transparency does not equate to a violation of Section 28 of the DPA, which is applicable when personal information is processed without the consent of the data subject, or otherwise authorized by law.

II. There is no unauthorized disclosure of Complainant's personal information under Section 32 of the DPA

In the same vein, the Commission must revisit the interpretation and application of Section 32¹⁴¹ of the DPA. The Decision dated 17 December 2020 failed to consider the operational act that is being penalized, which is the disclosure to third parties of personal information "without the consent" of the data subject.

A plain reading of this provision would qualify the application of Section 32 in instances where consent is the sole basis for processing. However, it excludes instances where the processing is done according to other lawful bases of processing under Sections 12 and 13 of the DPA.

¹⁴¹ 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 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

Stated differently, if the alleged processing of personal and sensitive personal information is based on other lawful criteria, then such disclosure does not come within the purview of Section 32 of the DPA but under a different Section of the DPA.

To interpret otherwise would result in an absurd situation where all forms of disclosure, without the data subject's consent, would be penalized under Section 32 even if they have other bases for processing. Moreover, this interpretation would create fear on the PICs to process any form of personal information without consent, even though they may have different bases for processing under Sections 12 and 13 of the DPA.

Instead of promoting the free flow of information to promote innovation and growth – the underlying state policy behind the DPA – it will create an environment of fear and uncertainty for the PICs that impede progress.

That is not how the DPA should be implemented. Its provisions should not apply mechanically, lest it will hurt the country more than the benefits that can be reaped by maximizing the beneficial uses of data.

As previously stated, PLDT has a lawful basis for processing and publishing the list of names of its telephone and DSL subscribers in the White Pages that is founded on a legal obligation according to the Public Service Act.

Since PLDT has a lawful basis for processing other than the consent requirement, then it follows that Section 32 (which penalizes disclosure without the consent of a data subject) of the DPA is not likewise applicable.

III. PLDT's accountability

It must be reiterated that although the PLDT may not be liable for Sections 28 and 32 of the DPA, the Commission can still hold them accountable for other violations of the DPA. This is especially concerning their failure to include a transparency mechanism, mainly a valid and comprehensive privacy notice, that will caution the data

subject that their personal information would be published in the White Pages according to law.

The NPC may exact accountability through various means without necessarily resorting to the penalties under Chapter VIII of the DPA, which involve criminal liabilities.

There are two (2) sides to accountability. On the one hand, the lack of accountability demonstrated by the PIC can be considered an aggravating factor in the imposition of fines and other liabilities. On the other hand, demonstrable proof of accountability is deemed in enforcement and fining actions, often mitigating the liabilities of the PIC.

There is a global consensus that factoring privacy-enhancing measures of PIC in the enforcement actions encourage organizational accountability. As a result, data privacy regulators worldwide have begun giving organizations credit for their good faith efforts to implement accountability.¹⁴²

Data privacy regulators can use organizational accountability as evidence of good-faith efforts by organizations. Through its responsive regulatory approach, the NPC has pivoted from a deterrence-only regulatory approach (that threatens enforcement of legal requirements through sanctions) to an outcomes-based approach to regulatory oversight.¹⁴³

PLDT has been publishing in the White Pages the list of subscribers since 1958. And they have been doing so because they rely on the law – the Public Service Act – which imposes the legal obligation to publish the list of names in public directories.

It must be stressed that the PLDT itself raised the matter of the printing of customer information (name, address, and telephone number) via the Directory Listing and the need for the consent of these customers to the NTC back in October 2017. They did so to clarify the matter and ask for guidance on how to best approach and address the situation they perceived as a “DPA gap.”

The “DPA gap” may be a consequence of the imperfections in the road to compliance of companies.

In the questioned Decision, reference to NPC Advisory Opinion No. 18-021 was made wherein the Privacy Policy Office (PPO) of the NPC was sought to clarify the claim of PLDT that its “base of

¹⁴² According to Hodges (2021), “Organizational Accountability in Data Protection Enforcement” (pp. 8 to 10) [Whitepaper].

¹⁴³ Id.

customers whose details have been printed have not expressly provided their consent to print their details in the existing DPC White Pages that meet the standards of a valid consent as contemplated by the DPA and DPA IRR.”

Records from the NPC’s PPO show that in a letter dated 18 October 2017, **even before the Complaint filed by RLA against PLDT, the latter already sought guidance from NTC on the matter of printed telephone directories of PLDT and its group and affiliates and related companies in light of the DPA and its IRR.**

According to PLDT, since 1958, PLDT has been printing customer information via the Directory Listing as part of the fulfillment of its obligation as a telephone service provider. In its review, PLDT discovered that its base of customers whose details have been printed in the directory listing have not expressly provided their consent to print their details in the existing DPC White Pages that meet the standards if a valid consent as contemplated by the DPA and its IRR.¹⁴⁴

PLDT Group explained that it commenced addressing and remediating this perceived **“DPA gap”** since 08 July 2017 with the implementation of PLDT Home’s new Customer Information Sheet (Application Form). This remediation measure notwithstanding, printed customer information for subscribers acquired pre- 08 July 2017 have been included in the directory listing by default. PLDT Group determines and recognizes this to be in conflict with the general data privacy principles of transparency, legitimate purpose and proportionality – the hallmarks of the DPA and its IRR.¹⁴⁵

PLDT requested from NTC an advisory opinion on the matter and/or guidance as to how to best approach the situation to ensure that service providers such as PLDT will be both compliant with the rules and

¹⁴⁴ Paragraph 3 of PLDT letter dated 18 October 2017 at p. 1.

¹⁴⁵ Id., Paragraph 4 at p. 1.

regulations prescribed by the NTC and the requirements of the DPA and its IRR.¹⁴⁶

¹⁴⁴ Paragraph 3 of PLDT letter dated 18 October 2017 at p. 1.

¹⁴⁵ Id., Paragraph 4 at p. 1. ¹⁴⁶ Id., Paragraph 2 at p. 1.

In return, NTC in a letter dated 30 October 2017, requested an advisory opinion from NPC regarding the residential directory listing of PLDT and its group of affiliates to fulfill PLDT's obligations as a telephone service provider vis-à-vis its compliance with the DPA. It attached PLDT's letter dated 18 October 2017 and requested NPC to comment thereon.

Upon evaluation, NPC's PPO opined that subscribers have the right to decide whether they want their name, address, and telephone number to be listed and included in the directory for publication. Hence, the NPC recommended the strict implementation of the said NTC Memorandum Circular.

As facts would dictate, PLDT was able to adjust accordingly.

Again, it must be stressed that the publication requirement emanates from the exigencies of times, its context and necessity. Telephone numbers and addresses could not be accessed in a world without the internet. People had to do things manually. They had to write letters, call by telephone, and refer to these White or Yellow pages to get the information they needed to reach someone.

Nothing in the DPA prohibits *per se* the publication of personal information in the White Pages, mainly when it is rooted in law. What the DPA requires is that such processing should uphold the general data privacy principles of transparency, legitimate purpose, and proportionality, among other things. PLDT failed in this regard – failing to include the transparency mechanisms to be compliant with Section 2.2 of NTC Memorandum Circular 05-06-2007.

Recommendation

To recap, since NTC MC 05-06-2007 is a later issuance, the provisions of the provisions of Section 149 of Revised Order No. 1, the PSC's Rules and Regulations for all public services, is considered amended or modified as follows:

1. The listing of the subscribers' names, addresses and telephone numbers is mandatory pursuant to Revised Order No. 1 of the Public Service Commission (1941). All telephone public service providers are mandated to publish the telephone directory at least once a year.

2. Pursuant to Section 2.2 of NTC MC 05-06-2007, the consumer shall be given the option not to be listed in succeeding publications.

3. NTC MC 05-06-2007 did not make the publication of the telephone directory optional and neither did it stop the publication of the same. Said NTC Memorandum Circular has given the consumer the option not to be listed in succeeding publications.

4. NTC MC 05-06-2007 did not provide for the procedure or mechanism on how the consumer shall exercise his/her option not to be listed. But NTC MC 05-06-2007 is clear that when the consumer exercises his/her option not to be listed in the telephone directory, the telephone public service provider shall comply. The option appears to be initiated by the consumer.

Admittedly, PLDT in compliance with its legal obligation to publish telephone directories, failed to include an opt-out option for its subscribers to be listed in succeeding publications. Such failure to abide by Section 2.2 of the NTC MC can be cited to be a violation of the general data privacy principle of transparency but does not equate to a violation of Section 28 of the DPA, which is applicable when personal information is processed without the consent of the data subject, or otherwise authorized by law.

After a thorough re-examination of the case, the Decision dated 17 December 2020 overlooked certain aspects which, if not corrected, will cause extreme and irreparable damage and prejudice as to how the DPA should be interpreted and applied.

In good conscience, there is no qualms about imposing damages against PLDT for its failure to include a privacy notice in the application form.

However, it must be emphasized that PLDT has since responded proactively by instilling privacy-protecting measures in its DSL application forms by 2017, even before Complainant filed the instant Complaint. They also sought clarification with the NTC, culminating in NPC Advisory Opinion No. 18-021. In addition, PLDT has registered with the NPC and attempted to comply with all the requirements of NPC.

There is no perfect compliance journey. For example, back in 2016 to 2018, when the NPC has newly started, admittedly, the compliance journeys of companies with the DPA varied. This is because no one fully understood the operationalization of the DPA, even when said law became effective in 2012.

It is simplistic to believe that every action or decision within a company results from either a calculation of costs and benefits or is governed solely by maximization of profits. Events can result from mistakes, accidents, confusion, poor judgment on prioritization, and especially from the complexity that arises from integrating multiple people and systems. Thus, the idea of imposing a penalty on “the organization” in the belief that “it” will respond as a single integrated organism and avoid some future actions that result in breaches of a rule simplistic and may not always prove true.¹⁴⁷

Even now, the NPC continues to conduct awareness campaigns to guide the PICs or PIPs. NPC have been leaders and protectors. And enforcers, especially against those who willfully violate the law. As NPC advances, the Commission is urged to put on wider lenses when adjudicating cases to enable the PICs to thrive and encourage organizational accountability without fear of being put behind bars while meting justice to data subjects.

Following the previous discussions, my recommendation is for this Commission to partially grant the Motion for Reconsideration filed by PLDT.

PLDT should not be liable for violating Section 28 of the DPA since it has a lawful criterion for processing, which is a legal obligation pursuant to the Public Service Act.

PLDT should not be liable for violating Section 32, which is not applicable in this case. Again, the data subject’s consent is not the basis for the disclosure; hence, the consent requirement under Section 32 of the DPA is immaterial.

There being no violations of Sections 28 and 32, it follows that the PLDT’s “responsible persons, officers or individuals” have no criminal liability. For this purpose, the directive in the Decision dated 17 December 2020, remanding the case to NPC’s Complaints and Investigation Division for the limited purpose of determining and identifying the responsible persons, officers, or individuals of PLDT who caused the violations of Sections 28 and 32 of the DPA must be set aside.

¹⁴⁷ According to Hodges (2021), “Organizational Accountability in Data Protection Enforcement” (at p. 8) [Whitepaper].

Finally, since PLDT did not violate Sections 28 and 32 of the DPA but committed only a violation of the general data privacy principle of transparency for its failure to include a notice to the data subject that their information would be published on the White Pages, the nominal damages of Fifty Thousand Pesos (P50,000.00) awarded to RLA in the Decision dated 17 December 2020 must be reduced to just Ten Thousand Pesos (P10,000.00). It must be stressed that the damages are imposed on this occasion due to the peculiarity of the instant Complaint and its surrounding circumstances.

WHEREFORE, it is recommended that the Motion for Reconsideration dated 05 August 2021 filed by PLDT Enterprise be **PARTIALLY GRANTED**. PLDT Enterprise and its responsible officers should **NOT BE LIABLE** for violations of Sections 28 and 32 of the Data Privacy Act of 2012.

However, it is recommended that the award to Complainant, RLA of nominal damages must be **SUSTAINED but in the reduced amount of Ten Thousand Pesos (P10,000.00)** on account of PLDT Enterprise's violation of the general data privacy principle of transparency.

The remand of the case to the Complaints and Investigation Division of the National Privacy Commission (NPC) for the limited purpose of determining and identifying the responsible persons, officers, or individuals of PLDT Enterprise should be **SET ASIDE**.

Instead, the Compliance and Monitoring Division (CMD) of the NPC is hereby directed to CONDUCT A COMPLIANCE CHECK on PLDT Enterprise to determine whether the measures and standards being implemented by the company are in line with the Data Privacy Act of 2012 and upholds data subjects' rights.

Further, PLDT Enterprise is ordered to submit to the CMD its Privacy Impact Assessment particularly on data flows on the application and subscription process of its customers to PLDT Enterprise's products and services.

(Sgd.)

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

RESOLUTION

LIBORO, P.C.:

This Resolution refers to the Breach Incident Report (Report) dated 24 September 2017 submitted by Sun Life of Canada (Philippines), Inc. (“Sun Life”). The Report includes a narration of a breach incident that Sun Life discovered on 21 September 2018. It involves the disclosure of information of around nine thousand seven hundred eighteen (9,718) clients that were not necessary for the third-party vendor to process.

FACTS

In May 2016, Sun Life engaged the services of an external vendor for the development of its wellness website, SUN Fit and Well. The vendor was engaged in the end-to-end membership management of SUN Fit and Well clients.

In October 2016, the wellness website was launched. From this period until 21 September 2018, the marketing staff of Sun Life has been sending the personal information of the new SUN Fit and Well clients to the vendor. The required information for this endeavor includes the client’s Owner name, Insured name, Owner email address, Insured email address, and Insured Age. However, the assigned staff also sent the extract (in Excel form) from Sun Life’s information and management system without filtering the information. Consequently, the Excel file transmitted contained information of clients that were not necessary for the vendor to process, such as policy number, policy issue date, servicing agent name, servicing branch date, settlement date, old/new client indicator, and old/new policy indicator. The Excel files were sent weekly, which were not encrypted, nor password protected.

On 21 September 2018, Sun Life’s Marketing Department requested its Compliance Team to review the processes and procedures that were done from the year 2016. From the review process, Sun Life was able to determine the practice of sending various Excel files containing the information of clients that came from Sun Life’s information and management system.

In response to this discovery, Sun Life sent a data breach incident report on 24 September 2018. In the report, Sun Life outlined the measures it took to address the breach such as requesting the vendor to immediately

purge all the data, to submit a certificate to confirm destruction, and to certify that these have not been shared, disclosed, or further processed.

Sun Life also requested for an exemption from notification of the affected data subjects on the ground that it is unlikely that the third- party vendor will use the policy information for unauthorized purposes, or that the disclosure will give rise to a real risk of serious harm to any affected data subject.

In its Resolution dated 21 May 2020, the Commission found that Sun Life's remedial measures were sufficient to handle the incident and granted its request for exemption from notification of the affected data subjects.

The Commission held that the unauthorized disclosure of the additional information was made to Sun Life's personal information processor, whose services are governed by contract which includes a confidentiality clause. The unauthorized acquisition is not likely to give rise to a real risk of serious harm to any affected data subject. Other than these, the excessive information that was shared were not personal information: policy number, policy issue date, servicing agent name, servicing branch name, settlement date, old/new client indicator and old/new policy indicator. Thus, notification would not be in the interest of the data subjects.

Nevertheless, it is required for Sun Life to submit a post-breach report to monitor the results of the measures it adopted to address the breach and to ensure that no further similar incident occurred.

In the said Resolution, the Commission ordered Sun Life to submit the following: (1) post-breach report containing the results of each of the measures it adopted to address the breach; (2) copy of the certificate from the vendor confirming the purge and destruction of all personal data not needed to perform its obligations under the contract; and (3) copy of the certification from the vendor stating that it has not shared, disclosed, or otherwise processed information outside the scope of their contract.

After its receipt of the Resolution on 18 January 2021, Sun Life submitted its Compliance Letter on 28 January 2021. In its letter, Sun Life enumerated the steps it had undertaken, as mentioned in its post- breach report.

Discussion

Upon reviewing of the Compliance Letter submitted by Sun Life, this Commission finds that Sun Life has fully complied with the order of the

Commission in its Resolution dated 21 May 2020.

As provided in Section 9 of the NPC Circular No. 16-03 (Personal Data Breach Management), 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.¹

Sun Life has reported in detail all the measures it undertook and provided copies of certification from the vendor, as instructed by the Commission.

According to the post-breach report, Sun Life has undertaken the following remedial measures to prevent similar events from happening in the future:

- (1) Immediate cessation of transfer of data to the vendor effective 21 September 2018. Hence, the website management is now directly governed by Sunlife's marketing staff;
- (2) Immediate request for the vendor to purge all data and to submit a certificate to confirm destruction;
- (3) Revision of process flow for the wellness website member management so that it will only be done internally;

Section 9 of NPC Circular 16-03

(4) Launching of new enhanced website in November 2018 automating the upgrade of members to “Gold,” from the previous manual upgrading of member status;

(5) Requested the vendor to certify that it has not shared, disclosed or otherwise processed information other than upon instruction of Sunlife;

(6) Upon assessment of the earlier conducted Privacy Impact Assessment (PIA), Sunlife found that the PIA conducted was sufficient.

(7) Review or revise processes to ensure that only personal data needed for services to be performed are shared with Sunlife’s service providers;

(8) Sweep all arrangements where personal data are shared to ensure that required documents are executed and assessments have been made.

In its Compliance Letter, Sun Life also attached a copy of the certificate from the vendor (1) confirming the purge and destruction of all personal data not needed to perform its obligations under their contract; and (2) stating that it has not shared, disclosed or otherwise processed the personal data and that the same was used solely for the purpose required by Sun Life.

Through careful review and evaluation of the submitted report, this Commission finds that the abovementioned submissions and actions implemented by Sun Life are adequate, sufficient, and compliant to its order indicated in the Resolution dated 21 May 2020 issued by this Commission.

WHEREFORE, premises considered, this Commission resolves that the matter of CID 18-183 “In re: Sun life of Canada (Philippines), Inc.” is hereby considered **CLOSED**.
SO ORDERED.

Pasay City, Philippines; 25 March 2021.

(Sgd.)

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.) (Sgd.)

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

JOHN HENRY D. NAGA

Deputy Privacy Commissioner

Copy furnished:

ATTY. MJM

Data Protection Officer

Sun Life of Canada (Philippines), Inc.

COMPLIANCE AND INVESTIGATION

DIVISION ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission

D.N.T,
Complainant,

versus

K.K and X.F,
Respondent.

NPC 19-1201

(For violation of Data
Privacy Act of 2012)

RESOLUTION

LIBORO, P.C.:

Before this Commission is the Mediated Settlement Agreement executed by and between complainant D.N.T. (Complainant) and respondents, K.K. and X.F. (collectively referred to as Respondents).

FACTS

Record¹ shows that Complainant is among the dependent and beneficiary of a retired employee of QBM (QBM). On 07 August 2019, he was not allowed by the Respondents herein to use the previously executed authorization from his brother which gives the Complainant the authority to avail travel benefits under QBM's retirement plan. In addition to this, Complainant was also denied of his trip pass allocation information and was required by Respondent K.K. to secure a new letter of authorization in accordance with QBM's new procedure for the availment of the travel benefits. When asked to explain, Respondent K.K. cited the Data Privacy Act of 2012 (DPA) as basis for the rules on letter of authorization and the non-disclosure of the details of the trip pass allocations of the Complainant. Complainant alleged that the Respondent cannot even point out the specific provision in the DPA which is the basis for the new procedure. Instead of explaining to the Complainant the purpose for the sudden changes in the new

¹ Complaint-Affidavit dated 07 September 2019.

procedure, Respondent K.K. got upset and even allegedly said that the Complainant was not even the employee of QBM and was merely a dependent. Hence, this Complaint.

On 11 March 2020, the parties filed their Application for Mediation and on the same date, the Mediation Conference was conducted.

Through the sincere efforts of the parties to arrive at an amicable resolution of their dispute, they were able to execute a Mediated Settlement Agreement on 11 March 2020.

Discussion

Rule III, Section 9(e)(3) of the Implementing Rules and Regulations of the Data Privacy Act of 2012(DPA) provides that:

The Commission shall adjudicate on complaints and investigations on matters affecting personal data: 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. This includes:

xxx

3. Facilitating or enabling settlement of complaints through the use of alternative dispute resolution processes, and adjudicating on matters affecting any personal data; (emphasis supplied)

In this case, pursuant to the Commission's power to facilitate or to enable settlement of complaints through alternative dispute resolution processes², the parties were invited to a Mediation Conference on 11 March 2020. During the Mediation Conference, the parties agreed to settle their differences through the execution of a Mediated Settlement Agreement on 11 March 2020. Thereafter, the contents of the aforesaid have been thoroughly explained and understood by the parties.

After a thorough study and adjudication of the case on hand, the Commission finds that the Mediated Settlement Agreement dated 11 March 2020 executed by and between the Complainant and the Respondents is not contrary to law, public policy, morals, or good customs.

² Rule III, Section 9 (E) of the Implementing Rules and Regulations of Data Privacy Act of 2012.

In the case of *Municipal Board of Cabanatuan City v. Samahang Magsasaka, Inc.*,³ 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 Mediated Settlement Agreement dated 11 March 2020 by and between the Complainant and the Respondents as valid and enforceable.

However, in the instant case, this Commission would like to note the erroneous and misapplication of the DPA that was allegedly committed by the Respondents. This Commission will never get tired in calling out Personal Information Controllers (PICs) to adhere to the data privacy principles and uphold the data subject's rights as enshrined in the DPA. The Commission understands that it takes effort, creativity, and innovation to cure this imbalance and not to prescribe disproportionate measures that may be too difficult for the PICs to implement and for the data subjects to comply with.

The new procedure being implemented by QBM of requiring the Complainant to secure a new letter of authorization for the availment of the travel benefits is not supported by the DPA.

The DPA should not be used to deprive the data subjects of their rights that are guaranteed by the DPA itself without a proper justification and notice to the data subjects.

Section 34(c) of the DPA provides for the right to access which a data subject is entitled, to wit:

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

c. Right to Access. The data subject has the right to reasonable access to, upon demand, the following:

1. Contents of his or her personal data that were processed;

³ *Municipal Board of Cabanatuan City v. Samahang Magsasaka, Inc.*, G.R. No. L-25818 dated 25 February 1975, 62 SCRA 435.

2. Sources from which personal data were obtained;
3. Names and addresses of recipients of the personal data;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal data to recipients, if any;
6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
7. Date when his or her personal data concerning the data subject were last accessed and modified; and
8. The designation, name or identity, and address of the personal information controller.

Considering the foregoing, the DPA assures that a data subject is entitled to the right to access. In consonance to this, the personal data must be provided by the PIC to the data subject or his authorized representative through a written document, or by any other format practicable to the PIC.⁴ The Respondent herein should have explained the purpose of securing a new letter of authorization and should not have merely cited the DPA as a shield to withhold information from the data subject. The aforesaid new procedure defeats the purpose of the right to access which is granted to data subjects by the DPA.

Moreover, QBM as a PIC, is required to develop, implement, and review policies and procedures, to ensure that the aforesaid policies and procedures shall enforce and effectively implement the provisions of the DPA, including those pertaining to the rights of data subjects.⁵

⁴ 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 [EU GENERAL DATA PROTECTION REGULATION], Article 12 (2016)

⁵ Section 26. Organizational Security Measures. Where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for organizational security:

xxx

e. Processing of Personal Data. Any natural or juridical person or other body involved in the processing of personal data shall develop, implement and review:

xxx

4.Policies and procedures for data subjects to exercise their rights under the Act;

The data subject has been defined by Section 3(c) of the DPA as an individual whose personal information, sensitive personal information, or privileged information is processed. Record shows that the trip pass allocation contains personal information such as the name of dependents and beneficiaries, relationship, or even the personal information of the retired QBM employee himself. In this case, Complainant is considered as a data subject of QBM because his full name appears in the travel pass information. Hence, the Complainant has the right to access to his personal information as explicitly provided by the DPA and its Implementing Rules and Regulations (IRR).

WHEREFORE, premises considered, the Commission resolves to **CONFIRM** the Mediated Settlement Agreement executed by and between Complainant D.N.T. and Respondents K.K. and X.F.. The case **NPC 19-1201 - “D.N.T. VS. K.K. AND X.F.”** is hereby **CLOSED**.

SO ORDERED.

Pasay City, Philippines. 18 March 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:

D.N.T.

Complainant

xxxxxx xxxxxx

K.K.

Respondent

Employee Benefits and Services Office xxxxxx

xxxxxx

X.F.

Respondent

Employee Benefits and Services Office xxxxxx

xxxxxx

**LEGAL DIVISION ENFORCEMENT
DIVISION GENERAL RECORDS UNIT**

National Privacy Commission



CIRCULARS

NPC CIRCULAR NO. 2021-01

January 28, 2021

2021 RULES OF PROCEDURE OF THE NATIONAL PRIVACY COMMISSION

Pursuant to the authority vested in the National Privacy Commission through Section 7(b) of Republic Act No. 10173, otherwise known as the “Data Privacy Act of 2012,” to receive complaints and institute investigations on matters affecting any personal information, the following 2021 Rules of Procedure of the National Privacy Commission are hereby prescribed and promulgated, repealing for this purpose NPC Circular No. 16-04 (Rules of Procedure) dated 15 December 2016 and NPC Circular No. 18-03 (Rules on Mediation before the National Privacy Commission) dated 18 December 2018.

RULE I GENERAL PROVISIONS

SECTION 1. Title. – These Rules shall be known as the “2021 NPC Rules of Procedure”.

SECTION 2. Liberal construction. - Any doubt in the interpretation of any provision of these Rules shall be liberally interpreted in a manner mindful of the rights and interests of the data subject about whom personal information is processed.

SECTION 3. Scope. – These Rules shall apply to the receipt, investigation, alternative dispute resolution, preliminary conference, adjudication, and all other proceedings before the NPC.

SECTION 4. Definition of Terms. –

a. **AFFIRMATIVE DEFENSES** – shall refer to any defense by the respondent which, if found to be credible, will negate liability under the Data Privacy Act of 2012, even if it is proven that the respondent in fact committed the alleged acts.

b. **BREACH INVESTIGATION** – shall refer to an investigation

conducted by the NPC with respect to a data breach notification triggered by the applicable rules promulgated by the Commission.

c. COMMISSION – shall refer to the Privacy Commissioner and the two (2) Deputy Privacy Commissioners, acting as a collegial body.

d. COMPLAINT INVESTIGATION – shall refer to an investigation conducted by the NPC with respect to a formal complaint filed by a data subject or his/her representative for violation of the Data Privacy Act of 2012.

e. COURIER – shall refer to any private mail carrier accredited by the Supreme Court, the NPC, or by international conventions by which the Philippines is a signatory.

f. DATA SUBJECT – refers to an individual whose personal information is processed.

g. DIGITAL SIGNATURE - refers to an electronic signature consisting of a transformation of an electronic document or an electronic data message using an asymmetric or public cryptosystem such that a person having the initial untransformed electronic document and the signer's public key can accurately determine (1) whether the transformation was created using the private key that corresponds to the signer's public key” and (2) whether the initial electronic document had been altered after the transformation was made.¹

h. ELECTRONICALLY-STORED INFORMATION – refers to any information which is received, recorded, transmitted, stored, processed, retrieved or produced electronically. It shall include any print-out or output that accurately reflects the electronically-stored information.²

i. EVALUATING OFFICER – may refer to a member of the Compliance and Monitoring Division (CMD) or a special committee or task force that may or may not include members from the CMD created by order of the Commission.

¹ A.M. 01-7-01 (Re: Rules on Electronic Evidence)

² See *ibid.*

j. INVESTIGATING OFFICER – may refer to a member of the Complaints and Investigation Division (CID) or a special committee or task force created that may or may not include members from the CID created by order of the Commission.

k. MEDIATION - refers to the voluntary process in which a mediation officer facilitates communication and negotiation, and assists the parties in reaching a voluntary agreement regarding a dispute.

l. MEDIATION OFFICER - refers to the personnel assigned or designated by the Commission to conduct mediation.

m. NPC – shall refer to the National Privacy Commission created under the Data Privacy Act of 2012.

n. 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.

o. RULES – shall refer to the 2021 NPC Rules of Procedure unless otherwise stated.

p. SUA SPONTE INVESTIGATION – shall refer to an investigation initiated by the NPC on its own for possible violation by one or more entities of the Data Privacy Act of 2012.

SECTION 5. Enforcement Powers. – The Commission may use its enforcement powers in the course of investigations to order cooperation of the subject of the investigation or other interested individuals or entities; or to compel appropriate action to protect the interests of data subjects.

SECTION 5. Enforcement Powers. – The Commission may use its enforcement powers in the course of investigations to order cooperation of the subject of the investigation or other interested individuals or entities; or to compel appropriate action to protect the interests of data subjects.

3 Act 3326: An Act To Establish Periods Of Prescription For Violations Penalized By Special Acts And Municipal Ordinances And To Provide When Prescription Shall Begin To Run.

SECTION 6. Prescriptive Period of the Penal provision of the DPA – The Commission adopts the periods of prescription for violations penalized by specials acts as provided under Act 33263 and any amendments thereto.

SECTION 1. Who may file complaints. – Subject to Rule X of these Rules, data subjects who are the subject of a privacy violation or personal data breach may file complaints for violations of the Data Privacy Act of 2012: *Provided*, that a representative may file on behalf of a data subject if he/she is authorized by a special power of attorney.

One or more data subjects may be represented by a single juridical entity: *Provided*, that the person filing the complaint must be authorized by a special power of attorney to appear and act on behalf of the data subjects: *Provided further*, the same person must also be authorized by a Board Resolution and Secretary's Certificate to appear and act in behalf of the juridical entity.

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, 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.

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.
2. The complaint must specify the identity of the individual claiming to be the subject of a privacy violation or the person so damaged or injured by a data breach, who shall be referred to as the complainant.
3. The complaint shall include the complainant's contact information, and where the complainant or duly authorized representative may be served with orders, issuances, or communications, including an electronic mail address if available.
4. The complaint must identify the person, entity or organization complained of, who shall be referred to as the respondent: Provided, that in the case of juridical persons, the responsible officers may also be included as respondents if they participated in, or by their gross negligence, allowed the commission of the alleged violation of the Data Privacy Act of 2012. If not known, the complainant shall state the circumstances that may lead to the identity of the respondent.
5. The complainant shall also provide in the complaint, if known: (a) respondent's contact information; and (b) where respondent may be served with orders, issuances, or communications from the NPC.
6. The complaint shall include a narration of the material facts and supporting testimonial or documentary evidence, if any, all of which show: (a) the violation of the Data Privacy Act of 2012, its Implementing Rules and Regulations, or NPC issuances; or (b) the acts or omissions allegedly committed by respondent and in the case of juridical persons, employees or agents who committed the offense amounting to a privacy violation or personal data breach.

7. The complaint must include any and all reliefs sought by the complainant.

8. The complainant shall attach any and all correspondence with respondent on the matter complained of and include a statement of the action taken by respondent to address the complaint, if any, showing compliance with the immediately preceding Section.

9. The supporting documents shall consist of copies of any documentary evidence and the affidavits of witnesses, if any, including those affidavits necessary to identify the documents and to substantiate the complaint.

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.

SECTION 4. Filing fees. – No further action on a complaint shall be made unless the appropriate filing fees have been paid, except when: (a) the complainant is the government, or any agency or instrumentality, and government-owned and controlled corporations organized and existing under their own charter; excluding government-owned and controlled corporations organized and incorporated under the Corporation Code; (b) the complaint is filed by an indigent complainant as defined in the Rules of Court or as otherwise prescribed by NPC through an advisory; or (c)

the NPC, upon motion by the requesting party, waives this requirement based on discretion and for good cause shown.

SECTION 5. Where to file complaints. – A complaint may be filed at any office of the NPC.

SECTION 6. Evaluation. – Within five (5) calendar days from the receipt of the complaint, the NPC shall raffle or assign the case to an investigating officer to conduct the proceedings.

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.

RULE III FILING AND SERVICE

SECTION 1. Modes of filing. – The filing of all pleadings and other submissions shall be made through any of the following modes:

- a. Submitting personally two (2) original copies and as many copies as there are receiving parties, plainly indicated as such, to the NPC;
- b. Sending them by registered mail;
- c. Sending them by courier; or
- d. Transmitting them by electronic mail as may be authorized by the Commission.

In the first case, the receiving NPC officer or employee shall indicate on the pleading the date and hour of filing. In the second and third cases, the date of the mailing of motions, pleadings, and other submissions, as shown by the post office stamp on the envelope or the registry receipt, shall be considered as the date of their filing. The envelope shall be attached to the record of the case. In the fourth case, the date of electronic transmission shall be considered as the date of filing provided that it is sufficient in form.

All pleadings and other submissions other than the complaint must be accompanied by an affidavit of service to the other party/parties.

Illegible, erroneous, and otherwise malfunctioning submissions by electronic mail shall not be considered by the NPC.

SECTION 2. Modes of service. – Unless otherwise stated, pleadings, motions, and other submissions shall be served personally or by registered mail, courier, or electronic mail as may be authorized by the Commission.

Service by electronic mail made by one party to another may only be made if the party recipient consents to such mode of service or by order of the Commission. The party recipient, within five (5) calendar days from receipt of the electronic mail, may move ex parte that the party sender resubmit the electronic mail due to illegibility or error in the first submission.

The Commission may, in its discretion, order any party who filed and/or served by electronic mail to send the printed and/or original signed copy of the document to the NPC through conventional service.

Documents not readily amenable to electronic scanning such as but not limited to those containing object evidence must be filed and served conventionally. In no instance may filing and service be done partly by electronic means and partly by conventional means.

The investigating officer or Commission, in their discretion and on a case to case basis, may demand that the parties file and serve their submissions conventionally

SECTION 3. Presumption of service. - There shall be disputable presumptive notice to a party of a hearing or conference if such notice appears on the records to have been mailed at least twenty (20) calendar days prior to the scheduled date of hearing.

SECTION 4. Extraterritorial service by NPC, when allowed. – When the respondent does not reside and is not found in the Philippines, service may be effected out of the Philippines by personal service or as provided for in international conventions to which the Philippines is a party; or by publication in a newspaper of general circulation in such places and for such time as the investigating officer or Commission may order, in which case a copy of the order to comment shall be sent by registered mail to the last known address of the respondent, or in any other manner the investigating officer or Commission may deem sufficient. The complainant shall bear the cost referred to in this Section.

SECTION 5. Service by NPC to unknown respondent or respondent whose whereabouts are unknown. – In cases where the respondent is

unknown, or whenever his or her whereabouts are unknown and cannot be ascertained by diligent inquiry, service by the investigating officer or Commission shall be effected upon him or her by publication in a newspaper of general circulation in such places and for such time as the investigating officer or Commission may order. The complainant shall bear the cost of the publication.

In case the respondent has a known electronic mail address, service by the Commission may be effected upon him or her through electronic mail in lieu of publication.

SECTION 6. Service of judgments, orders, or resolutions of the NPC. – Judgments, orders, or resolutions shall be served either personally, by registered mail, by courier, or by electronic mail: Provided, that service by electronic mail shall only be made if the party recipient consents to such mode of service or by order of the Commission. Provided further, that when a complaint or pleading is filed through electronic mail, the Commission may serve its judgments, orders, or resolutions by electronic mail through the same electronic mail address used in the filing of the complaint or pleading, unless otherwise indicated therein.

RULE IV

PRE-INVESTIGATION PHASE

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.

SECTION 2. Amendment of complaint, when allowed. – Complainant may substantially amend the complaint once as a matter of right at any time before respondent has filed a comment, in which case the respondent shall be provided a copy and granted a fresh period to submit his or her comment. Substantial amendments after the respondent has filed a comment may only be done upon motion filed with, and with leave of, the investigating officer.

SECTION 3. Submission of comment. – Upon finding that the complaint may be given due course, respondent shall be required to file a verified comment within fifteen (15) calendar days from receipt of the order. A copy of the complaint, together with its supporting evidence, shall be attached to the order to comment.

A complaint may be submitted for resolution if respondent does not file a comment within the period provided.

SECTION 4. Content of the comment. – The respondent shall raise all of his or her defenses in his or her comment. No motions to dismiss shall be entertained: Provided, the investigating officer, in its discretion, may treat the motion to dismiss as the respondent's comment.

SECTION 5. Prohibited pleadings and motions. – The following pleadings and motions shall not be allowed in the complaint proceedings:

1. motions to dismiss the complaint;
2. motions for a bill of particulars;
3. motions to declare respondent in default;
4. dilatory motions for postponement;
5. replies or rejoinders, except if the preceding pleading incorporates an actionable document;
6. third-party complaints;
7. interventions; and
8. appeal or motion of reconsideration from any interlocutory order of the investigating officer.

SECTION 6. Affirmative defenses. – The respondent, in lieu of a motion of dismiss, may raise in his/her comment affirmative defenses such as but not limited to:

- (1) The NPC has no jurisdiction over the subject matter;
- (2) The action is barred by a prior judgment;
- (3) There is another action pending between the same parties for

the same cause;

(4) The complainant has no legal capacity to sue;

(5) That the pleading asserting the claim states no cause of action or is found to be frivolous, vexatious or made in bad faith;

(6) The action has otherwise prescribed under the statute of limitations; or

(7) That the claim or demand set forth in the complaint has been paid, waived, abandoned or otherwise extinguished.

SECTION 7. Authority of the investigating officer to rule on motions. – The investigating officer may directly rule on motions that do not fully dispose the case on the merits. No appeal or motion for reconsideration may be taken for any interlocutory order made by the investigating officer but these may be included as an issue once the case has reached the Commission for adjudication under Rule VIII of these Rules.

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.

SECTION 2. Referral to alternative dispute resolution or mediation. – If alternative dispute resolution is availed by the parties, the investigating officer shall refer the case to the mediation officer, in which case Rule VI of these Rules shall govern.

SECTION 3. Failure of the parties to appear, effect.– The failure of either of the parties to appear during the preliminary conference without justifiable reason shall cause the conference to be reset once, and upon failure of the party concerned once again to appear, said party shall be deemed to have waived his/her rights to the benefits hereto, including but not limited to mediation, discovery,

and/or stipulation of facts.

SECTION 4. Discovery of electronically-stored information, process. – If discovery of electronically-stored information is reasonably likely to be sought in the proceeding, the parties shall discuss:

1. issues relating to the preservation of the information;
2. the form in which each type of information will be produced;
3. the period within which the information will be produced;
4. the method for asserting or preserving claims of privilege or of protection of the information;
5. the method for asserting or preserving confidentiality and proprietary status of information relating to a party or person not a party to the proceeding;
6. whether allocation of the expense of production among the parties is appropriate; and
7. any other issue relating to the discovery of electronically-stored information.

The investigating officer may issue an order governing the discovery of electronically-stored information pursuant to:

- a. a motion by a party seeking discovery of the information or from which discovery of the information is sought; or
- b. a stipulation of the parties and of any person not a party from which discovery of the information is sought.

Subject to the rules on privileged information, the investigating officer may impose sanctions on a party for failure to provide electronically-stored information, except if the party proves that the information was lost as a result of the routine, good-faith operation of an electronic information system in accordance with existing policies.

Any party may move *ex parte* to request for the production of electronically-stored information and for permission to inspect, copy, test, or sample such information. The party on which the said request is served must respond within ten (10) calendar days, or in such timely manner as to preserve the integrity of the electronically-stored information. With respect to every item or category in the request, the response must state that inspection, copying, testing, or sampling of the information will be permitted; otherwise, the objection to the request and the reasons therefor.

The requesting party may specify the form in which the electronically-stored information is to be produced. Unless the parties otherwise agree or the investigating officer otherwise orders: (1) if a request for production does not specify a form for producing a type of electronically-stored information, the responding party shall produce the information in the form in which it is ordinarily maintained or in a form that is reasonably usable; and (2) a party need not produce the same electronically-stored information in more than one form.

A party may object to the discovery of electronically-stored information from sources that the party identifies as not reasonably accessible because of undue burden or expense. In its objection, the party shall identify the reason for the undue burden or expense. In a motion to compel discovery or for a protective order relating to the discovery of electronically-stored information, a party objecting to discovery bears the burden of proving that the information is from a source that is not reasonably accessible because of undue burden or expense.

Despite a showing that electronically-stored information would come from a source that is not reasonably accessible because of undue burden or expense, the investigating officer may still order discovery of such information if the party requesting shows that the likely benefit of the proposed discovery outweighs the likely burden or expense, taking into account the amount in controversy, the resources of the parties, the effect of the privacy violation to the data subject, and the importance of the requested discovery in resolving the issues. The investigating officer may set conditions for discovery of the information, including allocation of the expense.

The investigating officer shall limit the frequency or extent of discovery of electronically-stored information, even from a source that is reasonably accessible, if it is found that:

- a. it is possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive;
- b. the discovery sought is unreasonably cumulative or duplicative;
- c. the party seeking discovery has had ample opportunity by discovery in the proceeding to obtain the information sought; or
- d. the likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in

controversy, the resources of the parties, the importance of the issues, and the importance of the requested discovery in resolving the issues.

SECTION 5. Discovery of other information. - Discovery proceedings outside of the production, inspection and storage of electronically stored information are allowed and subject to the Rules of Court.

SECTION 6. Confidentiality of discovered information. - Any party who receives any information, whether electronically stored or not, by result of discovery, is mandated to preserve the confidentiality of such information. Furthermore, any information obtained during discovery may only be used by the parties for legal purposes and by NPC itself for the fulfillment of its mandate. This Section shall apply even if the party chooses not to use the information during the complaint proceedings.

SECTION 7. Preliminary conference order. - Within fifteen (15) calendar days from the termination of the preliminary conference, the investigating officer shall issue an order which shall recite in detail the matters taken up.

RULE VI ALTERNATIVE DISPUTE RESOLUTION

SECTION 1. Willingness to mediate. - During the preliminary conference or at any stage of the proceedings but before rendition of decision by the Commission, the parties by mutual agreement may signify their interest to explore the possibility of settling issues by mediation.

SECTION 2. Application for mediation. - The parties shall jointly file with the investigating officer or Commission, as the case may be, an Application for Mediation manifesting their earnest commitment to engage in a meaningful settlement process and their willingness to abide by these Rules and the orders issued by the assigned mediation officer. No application for mediation shall be approved without payment of the mediation fee.

SECTION 3. Mediation fees. - The mediation fee in an amount prescribed by the NPC in a separate issuance shall be paid by the parties upon the filing of the Application for Mediation.

Parties may be exempted from the payment of the mediation fee under

the same grounds as Section 4, Rule II of these Rules.

SECTION 4. Order to mediate, when issued. – The investigating officer or Commission, as the case may be, shall issue an Order to Mediate, which shall state the following: (a) the approval of the Application for Mediation; (b) the suspension of the complaint proceedings for sixty (60) calendar days pending the mediation proceedings; (c) the name of the assigned or designated mediation officer who shall preside over the mediation proceedings; and (d) the date, time, and place when the parties shall appear before the mediation officer for the preliminary mediation conference. Copies of the Order to Mediate shall be furnished to the mediation officer and the parties.

SECTION 5. Preliminary mediation conference. – The mediation officer shall receive the appearances of the parties and inform them of the mediation process and the manner by which the proceedings will be conducted. The mediation officer shall stress the benefits of an early settlement of the dispute and endeavor to achieve the most fair and expeditious settlement possible.

Each party shall be allowed to make a brief statement of their respective position and preferred outcome. The mediation officer shall explore common ground for settlement and suggest options for the parties to consider.

When necessary, the parties shall agree on the schedule of the next mediation conference and the mediation officer shall issue an order therefor.

SECTION 6. Separate caucuses and subsequent conferences. – The mediation officer may, with the consent of both parties, hold separate caucuses with each party to enable a determination of their respective real interest in the dispute; provided, that each party shall be afforded equal time and/or opportunity to ventilate such interest and motivation. The mediation officer may call such conferences/caucuses as may be necessary to facilitate settlement.

The mediation officer shall hold in confidence any matter disclosed during the separate caucuses and shall exercise reasonable prudence and discretion in the safeguarding of such information.

SECTION 7. Personal appearance by the parties. – Individual parties

are required to personally appear during mediation conferences. Representatives may appear on behalf of individual parties: Provided, that they are authorized by special power of attorney to appear, offer, negotiate, accept, decide, and enter into a mediated settlement agreement without additional consent or authority from the principal. If the party is a partnership, association, corporation, or a government agency, the representative must be authorized by a notarized Secretary's Certificate, Board Resolution, or any equivalent written authority to offer, negotiate, accept, decide, and enter into a mediated settlement agreement.

If the representative is not equipped with a proper special power of attorney, Secretary's Certificate, Board Resolution or their equivalent, he or she may still appear on behalf of his or her principal: Provided, that the other party consents to such appearance; Provided further, the representative undertakes to bring his or her authority to appear during the next mediation conference; Provided finally, no mediation settlement may be signed by any representative without a proper special power of attorney, Secretary's Certificate, Board Resolution or their equivalent.

SECTION 8. Failure of parties to appear, effect. – If any of the parties fail to appear without prior notice and justifiable reason for two (2) consecutive mediation conferences at any stage of the mediation, the mediation officer may order the termination of the mediation proceedings and refer the same for the resumption of complaint proceedings: Provided, in case of doubt that the party's absence is justified, the mediation officer may order for another caucus or conference. The mediation officer may require the non-appearing party to explain why said party should not be required to pay treble costs incurred by the appearing party, including attorney's fees, in attending the mediation conferences/caucuses, and be henceforth permanently prohibited from requesting mediation at any other stage of the complaint proceedings before the NPC.

SECTION 9. Presence of lawyers in mediation. – Lawyers who act as counsels, upon the discretion of the mediation officer, may attend the mediation conferences in the role of an adviser and consultant to their clients and shall cooperate with the mediation officer towards securing a settlement of the dispute. They shall help their clients comprehend the mediation process and its benefits and assist in the preparation of a mediated settlement agreement and its eventual enforcement.

Lawyers who act as duly authorized representatives of juridical entities may directly attend the mediation conference with all its concomitant

rights and obligations.

SECTION 10. Venue. – Mediation proceedings shall be conducted within the NPC premises. Upon request of both parties, the mediation officer may authorize the conduct of a mediation conference at any other venue, provided that all related expenses, including transportation, food, and accommodation, shall be borne by both parties. If a change of venue is requested by one party, it must be with the other's conformity and they shall agree on the terms of handling the expenses.

SECTION 11. Mediation period and extension. – The mediation officer shall endeavor to achieve a mediated settlement of the dispute within sixty (60) days from the preliminary mediation conference.

Upon reasonable ground to believe that settlement may yet be achieved beyond the initial mediation period of sixty (60) calendar days, the period to mediate may be extended for another thirty (30) calendar days by the mediation officer for good cause shown. Copies of the notice and/or order to extend the proceedings shall be furnished the investigation officer or the Commission, as the case may be.

SECTION 12. Mediated Settlement Agreement. – A mediated settlement agreement following successful mediation shall be jointly prepared and executed by the parties, with the assistance of their respective counsel, if any. The execution of a mediated settlement agreement shall terminate the mediation proceedings. The mediation officer shall certify that the contents of the agreement have been explained, understood, and mutually agreed upon by the parties, and that the provisions are not contrary to law, public policy, morals, or good customs.

SECTION 13. Confirmation by the Commission. – The mediation officer shall issue a resolution submitting the mediated settlement agreement to the Commission within ten (10) calendar days from signing. The Commission shall issue a resolution confirming the mediated settlement agreement within fifteen (15) calendar days from submission of the resolution and mediated settlement agreement. Copies of the resolution issued by the Commission shall be furnished to the parties, the investigating officer, and the mediation officer.

SECTION 14. Effect of confirmed Mediated Settlement Agreement. – A confirmed mediated settlement agreement shall have the effect of a decision or judgment on the complaint, and shall be enforced in

accordance with the NPC's rules and issuances.

SECTION 11. Mediation period and extension. – The mediation officer shall endeavor to achieve a mediated settlement of the dispute within sixty (60) days from the preliminary mediation conference.

Upon reasonable ground to believe that settlement may yet be achieved beyond the initial mediation period of sixty (60) calendar days, the period to mediate may be extended for another thirty (30) calendar days by the mediation officer for good cause shown. Copies of the notice and/or order to extend the proceedings shall be furnished the investigation officer or the Commission, as the case may be.

SECTION 12. Mediated Settlement Agreement. – A mediated settlement agreement following successful mediation shall be jointly prepared and executed by the parties, with the assistance of their respective counsel, if any. The execution of a mediated settlement agreement shall terminate the mediation proceedings. The mediation officer shall certify that the contents of the agreement have been explained, understood, and mutually agreed upon by the parties, and that the provisions are not contrary to law, public policy, morals, or good customs.

SECTION 13. Confirmation by the Commission. – The mediation officer shall issue a resolution submitting the mediated settlement agreement to the Commission within ten (10) calendar days from signing. The Commission shall issue a resolution confirming the mediated settlement agreement within fifteen (15) calendar days from submission of the resolution and mediated settlement agreement. Copies of the resolution issued by the Commission shall be furnished to the parties, the investigating officer, and the mediation officer.

SECTION 14. Effect of confirmed Mediated Settlement Agreement. – A confirmed mediated settlement agreement shall have the effect of a decision or judgment on the complaint, and shall be enforced in accordance with the NPC's rules and issuances.

SECTION 1. Examination of systems and procedures.– Upon termination of the preliminary conference, the investigating officer shall decide whether there is a necessity to further investigate the circumstances surrounding the privacy violation or personal data breach.

The investigating officer shall not be limited to the pleadings, allegations, issues and evidence submitted before him or her. Investigations may

include on-site examination of systems and procedures, subject to the issuance of a proper authority from the NPC. Upon request of the investigating officer, on-site examination of systems and procedures may be undertaken by technical personnel who shall be authorized by the Commission to conduct highly technical and highly sensitive forensic examinations.

In the course of the investigation, the complainant and/or respondent may be required to furnish additional information, document or evidence, or to produce additional witnesses. The parties shall have the right to examine the evidence submitted, which they may not have been furnished, and to copy them at their expense.

SECTION 2. Submission of simultaneous memoranda. – The investigating officer shall require the parties to submit simultaneous memoranda discussing and summarizing their respective causes of action, claims, and defenses within fifteen (15) calendar days from written notice. The memoranda must also include, in simple tabular form, a list of all the evidence presented by the party and purpose to his/her claim or defense. Failure to submit the memorandum within the period provided shall be considered a waiver of such opportunity.

SECTION 3. Fact-Finding Report. – Within thirty (30) calendar days from the last day of the reglementary period to file memoranda, the investigating officer shall submit to the Commission a Fact-Finding Report, including the results of the investigation, the evidence gathered, and recommendations. Within ten (10) calendar days from submission of the Fact-Finding Report to the Commission, both parties shall be furnished with a notice that the case has been submitted for decision of the Commission.

SECTION 4. Withdrawal of the complaint.– At any period before the submission of the Fact-Finding Report, the complainant may withdraw the complaint upon approval of the investigating officer and upon such terms and conditions as the latter may deem proper. The investigating officer may recommend either the dismissal of the case, with or without prejudice, or the application of the Commission's power to initiate sua sponte investigations.

RULE VIII DECISION

SECTION 1. Action on the recommendations of the Investigating Officer.

– The Commission shall review the evidence presented, including the Fact-Finding Report and supporting documents. On the basis of the said review, the Commission may: (1) promulgate a Decision; (2) issue interlocutory orders on matters affecting personal data; or (3) order the conduct of a clarificatory hearing or the submission of additional documents, if in its discretion, additional information is needed to make a Decision. No motion for clarificatory hearing shall be entertained. In case the Commission finds that a clarificatory hearing is necessary, the following shall be observed:

- a. The parties shall be notified of the scheduled clarificatory hearing at least five (5) calendar days before such schedule;
- b. The Commission may require additional information and/or compel attendance of any person involved in the complaint;
- c. The parties shall not directly question the individuals called to testify but may submit their questions to the Commission for their consideration;
- d. The parties may be required to submit their respective memoranda containing their arguments on the facts and issues for resolution.

SECTION 2. Additional issues to be raised before the Commission.

– Upon motion, both parties may raise as an issue during adjudication any interlocutory order or decision issued by the investigating officer, evaluating officer, special committee or task force as the case may be. The Commission, in its discretion, may resolve the issues separately or jointly with the merits of the case.

Once a given case has reached the Commission for adjudication, the investigating officer, evaluating officer, special committee or task force shall transmit to the Commission any pleadings, motions, and other submissions erroneously filed subsequent to the endorsement of the main case to the Commission. Subject to the discretion of the Commission, these pleadings, motions and other submissions may form part of the main case.

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. The decision may include enforcement orders, including:

- a. an award of indemnity on matters affecting personal data protection, or rights of the data subject, where the indemnity amount to be awarded shall be determined based on the provisions of the Civil Code;
- b. permanent ban on the processing of personal data;
- c. a recommendation to the Department of Justice for the prosecution and imposition of penalties specified in the 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;
- e. impose fines for violations of the Act or issuances of the NPC;
or
- f. any other order to enforce compliance with the Data Privacy Act of 2012.

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.

SECTION 5. Entry of judgments and final orders. — If no appeal or motion for reconsideration is filed within the time provided in these Rules, the judgment or final order shall thereafter be entered in the book of entries of judgments. The date when the judgment or final order becomes executory shall be deemed as the date of its entry. The record shall contain the dispositive part of the judgment or final order with a certificate that such judgment or final order has become final and executory.

RULE IX

BAN ON PROCESSING OF PERSONAL DATA

SECTION 1. Temporary ban on processing of personal data. – Upon filing of the complaint or at any time before the decision of the Commission becomes final and executory, a complainant may apply for the imposition of a temporary ban on respondent's processing of personal data through motion.

SECTION 2. Suspension of complaint proceedings. – An application for a temporary ban on processing of personal data shall have the effect of suspending the complaint proceedings until such application has been finally resolved.

SECTION 3. Requisites for temporary ban. – A temporary ban on processing of personal data may be granted only when:

1. it is necessary in order to preserve the rights of the complainant or to protect national security or public interest, or if it is necessary to preserve and protect the rights of data subjects;
2. the motion shows facts entitling the complainant to the relief demanded;
3. unless exempted from the payment of filing fees as provided for in these Rules, the complainant shall file with the NPC a bond in an amount to be fixed by the investigating officer executed in favor of the party or person so banned from processing personal data; and
4. the parties are heard in a summary hearing.

SECTION 4. Notice of summary hearing.– Upon receipt of the motion, the investigating officer shall issue a notice of hearing to the parties. The notice to respondent shall include a copy of the receipt of the bond, if applicable.

The notice of hearing shall indicate the scheduled date and venue for the hearing, and a statement that respondent may appoint a duly authorized representative to appear at the hearing in order to protect its interests. The complainant shall shoulder the cost of personal service and ensure that the notice of hearing is received by respondent at least five (5) calendar days before the scheduled date. If personal service is impracticable, the notice

of hearing shall be sent by complainant to respondent through private courier. Upon service, the complainant shall file with the investigating officer an affidavit of service attesting that service was properly made upon the respondent or respondents, as the case may be.

SECTION 5. Summary hearing. – The summary hearing shall consist of the personal submission by the parties and their witnesses of their respective judicial affidavits in accordance with Sections 3 and 4 of A.M. No. 12-8-8-SC dated 4 September 2012 (Judicial Affidavit Rule).

The parties shall identify and mark as exhibit their documentary or object evidence. Should the parties or their witnesses desire to keep the original document or object evidence in their possession, after the same have been identified, compared with the original, marked as exhibit, and authenticated, they may state for the record that the copy or reproduction attached to the judicial affidavit is a faithful copy or reproduction of the original.

SECTION 6. Submission of position papers or other pleadings as alternative to summary hearing. – The investigating officer may, upon motion or in its discretion, compel the parties to submit simultaneous position papers in lieu of a summary hearing.

SECTION 7. Decision on the temporary ban. – Within thirty (30) calendar days from the conclusion of the summary hearing, the investigating officer shall decide on the application for a temporary ban on processing of personal data.

SECTION 8. Duration of temporary ban. – When issued, the temporary ban on processing of personal data shall remain in effect until the final resolution of the main case, or upon further orders by the Commission or other lawful authority.

SECTION 9. Permanent ban on processing of personal data.– If, after the termination of the complaint proceedings, it appears that complainant is entitled to have a permanent ban on respondent's processing of personal data, the investigating officer shall include in their Fact-Finding Report a recommendation to the Commission for the issuance of an order for a permanent ban on processing of personal data.

RULE X

SUA SPONTE INVESTIGATION

SECTION 1. Commencement. – The Commission may order an investigation of the circumstances surrounding a possible data privacy violation or personal data breach in cases of, but not exclusive to, matters that arose from pending cases before the NPC, reports from the daily news, trends or academic studies, information gathered from corroborated and substantiated anonymous tips, or reports from other offices of the Commission.

SECTION 2. Temporary and permanent ban on processing of personal data. – A temporary or permanent ban on processing of personal data may be imposed on the subject of a sua sponte investigation in order to protect national security or public interest, or if it is necessary to preserve and protect the rights of data subjects, in accordance with Rule IX of these Rules.

SECTION 3. Assignment of investigating officer or special committee or task force. – The Commission may, when it deems proper, assign an investigating officer or create a special committee or task force which shall be specifically assigned by the NPC to conduct the investigation.

SECTION 4. Conduct of sua sponte investigation. – The investigating officer or special committee or task force shall investigate the circumstances surrounding the privacy violation or personal data breach. Investigations may include on-site examination of systems and procedures. In the course of the investigation, the parties subject of the investigation may be required to furnish additional information, document or evidence, or to produce additional witnesses.

SECTION 5. Sua sponte Fact-Finding Report. – Within thirty (30) calendar days from the termination of the investigation, the investigating officer or special committee or task force shall submit to the Commission a Fact-Finding Report, which shall include the results of the investigation, the evidence gathered, and any recommendations.

SECTION 6. Order to comment. – Upon receipt by the Commission of the Fact-Finding Report, the respondent identified after the conduct of the preceding investigation shall be provided a copy of the Fact-Finding Report and given an opportunity to submit a comment. In cases where the respondent or respondents fail without justification to

submit an comment or appear before the NPC when so ordered, the Commission shall render its decision on the basis of available information under Rule VIII of these Rules.

SECTION 7. Existence of a complaint during sua sponte investigation and vice versa, effect. – If, during the proceedings of a sua sponte investigation, a formal complaint relating to the same act or omission for violation of the Data Privacy Act of 2012 is filed against the respondent, the complaint proceedings shall follow the normal procedure under these Rules: Provided, that the complaint proceedings shall not suspend the sua sponte proceedings, or vice versa: Provided further, that discovery and mediation proceedings under Rule V shall be available to the parties of the complaint proceedings: Provided finally, that a mediated settlement agreement shall only terminate the complaint proceedings but not the sua sponte investigation.

The preceding paragraph shall likewise apply if the complaint proceedings occurred first and the NPC wishes to initiate a sua sponte investigation thereafter.

RULE XI BREACH INVESTIGATION

SECTION 1. Procedure for personal data breach notification. – The procedure for personal data breach notification and other requirements shall be governed by the Data Privacy Act of 2012, Implementing Rules and Regulations, and NPC Circular No. 16-03, including any of its amendments. These Rules shall apply in a supplementary character.

SECTION 2. Receipt of data breach notifications. – The CMD shall be the initial recipient of data breach notifications. The CMD shall assign an evaluating officer to evaluate the data breach notification.

SECTION 3. Preliminary requests that shall be resolved by CMD. – Upon receipt of the data breach notification, the evaluating officer shall resolve requests from the PIC or PIP for (a) extensions to notify data subjects and/ or (b) extensions to file full breach report: Provided, extensions granted by the CMD shall not exceed a cumulative period of fifteen (15) working days counted from the date of the initial request.

SECTION 4. Preliminary requests that must be endorsed to the Commission. – CMD shall endorse to the Commission the following requests from the PIC or PIP:

- a. exemption or postponement to notify data subjects;
- b. extensions to file full breach report and notify data subjects

beyond fifteen (15) working days;

c. use of alternative means of notification; or

d. other requests such as but not limited to Motions for Reconsideration involving preliminary requests.

SECTION 5. Initial breach notification evaluation and monitoring. – The evaluating officer shall review the completeness of the data breach notification and determine the other documents needed to assess the PIC or PIP’s breach management.

Moreover, the CMD shall monitor the compliance of the PIC or PIP with the periods in NPC Circular No. 16-03 and the subsequent extensions allowed under the preceding sections.

The CMD may order the submission of additional documents from the PIC or PIP; or in its discretion, apply for a Cease and Desist Order in accordance with Section 2, Rule XII of these Rules.

SECTION 6. Final breach notification evaluation. – Upon receipt of all the documents required to assess the PIC or PIP’s breach management, the evaluating officer shall prepare a Breach Notification Evaluation Report using all information available to him/her.

Upon the finding of a possible data privacy violation that needs further investigation, the CMD shall transmit the Breach Notification Evaluation Report to the CID. Otherwise, the CMD shall submit the same to the Commission for adjudication directly.

SECTION 7. Conduct of breach investigation. – Upon receipt of the Breach Notification Evaluation Report, an investigating officer shall be assigned by the CID to determine if there is a necessity to conduct an on-site or technical investigation. The investigating officer shall request a proper authority from the NPC before conducting any on-site or technical investigation. The investigating officer may also request assistance from technical personnel of the NPC. In the course of the investigation, the complainant and/or respondent may be required to furnish additional information, document or evidence, or to produce additional witnesses.

SECTION 8. Fact-Finding Report – The investigating officer shall submit to the Commission a Fact-Finding Report within thirty (30) calendar days from the termination of the on-site or technical investigation or receipt of the Breach Notification Evaluation Report, whichever is applicable.

SECTION 9. Order to comment. – Upon receipt by the Commission of the Fact-Finding Report, the respondent shall be provided a copy of such report and given an opportunity to submit a comment. In cases where the respondent or respondents fail without justification to submit a comment or appear before the NPC when so ordered, the Commission shall render its decision on the basis of available information under Rule

VIII of these Rules.

SECTION 10. Failure to submit breach notification. – Should the NPC receive news, corroborated and substantiated tip, or anonymous complaint that a breach occurred but the PIC or PIP did not submit any notification to the NPC, the latter may use this information to initiate a sua sponte investigation under Rule X.

If during the sua sponte investigation a breach notification was submitted by the PIC or PIP, the CID shall have the discretion to (1) continue the sua sponte investigation; or (2) suspend said investigation through notice to the investigating officer or special committee or task force and refer the breach notification to the CMD for evaluation under this Rule.

SECTION 11. Post-breach monitoring and compliance. – The CMD shall monitor and ensure compliance of PICs or PIPs to the judgments, resolutions or orders issued by the Commission with respect to any data breach related cases.

RULE XII MISCELLANEOUS PROVISIONS

SECTION 1. Transitory provision. – These Rules shall apply to all complaints filed after its effectivity. It shall also apply to pending proceedings, except to the extent that their application would not be feasible or would work injustice.

SECTION 2. Procedure for cease and desist orders. – Procedure for the issuance of cease and desist orders shall be governed by the appropriate circular issued and published by the NPC.

SECTION 3. Procedure for requests for advisory opinion. – Procedure for requests for advisory opinion shall be governed by NPC Circular No. 18-01 including its amendments.

SECTION 4. Procedure for compliance checks. – Procedure for the conduct of compliance checks shall be governed by NPC Circular No. 18-02 including its amendments.

SECTION 5. Procedure for videoconferencing technology. - Procedure for the use of videoconferencing technology for the remote appearance and testimony of parties before the NPC shall be governed by NPC Advisory No. 2020-02 including its amendments. Notwithstanding any provision of these Rules, the conduct of preliminary conferences, summary hearings, mediation conferences, investigations, clarificatory hearings, and all other

hearings conducted by the concerned division and/or Commission may be conducted through videoconferencing technology or through any electronic means as authorized by the Commission.

SECTION 6. Repealing clause. – NPC Circulars No. 16-04 and 18-03 are hereby repealed. All other issuances by the NPC which are contrary to the provisions of these Rules are also hereby repealed or amended accordingly.

SECTION 7. Amendments. – These Rules or any of its portion may be amended or supplemented by the Commission.

SECTION 8. Application of Rules of Court. – The Rules of Court shall apply in a suppletory character and whenever practicable and convenient.

SECTION 9. Effectivity.– These Rules shall take effect fifteen (15) days after publication in a newspaper of general circulation.

Approved:

(Sgd.)

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner and Chairman

(Sgd.)

JOHN HENRY DU NAGA

Deputy Privacy Commissioner

(Sgd.)

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

NPC CIRCULAR NO. 2021-02

November 8, 2021

GUIDELINES ON THE PROCESSING OF PERSONAL DATA DURING PUBLIC HEALTH EMERGENCIES FOR PUBLIC HEALTH MEASURES

WHEREAS, the National Privacy Commission (NPC) supports the implementation of prevention, detection, isolation, treatment, and reintegration strategies of the national government agencies and local government units for the COVID-19 response, which includes contact tracing efforts and vaccine deployment;

WHEREAS, the NPC is cognizant of the vital role of data-driven technologies such as the development of contact tracing applications and vaccine card systems and applications which inevitably involve the processing of personal information;

WHEREAS, Section 11 of the Data Privacy Act of 2012 (DPA) allows for the processing of personal information, subject to the compliance with the requirements of the law and adherence to the general principles of transparency, legitimate purpose, and proportionality, among others;

WHEREAS, Sections 12 and 13 of the DPA enumerates the criteria for lawful processing of personal information, sensitive personal information, and privileged information (collectively, personal data);

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 personal information controllers with the provisions of the Act, 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 (IRR) of the DPA provides that, among the Commission's functions, is to develop, promulgate, review or amend rules and regulations for the effective implementation of the DPA;

WHEREFORE, in consideration of these premises, the NPC hereby issues this Circular governing the processing of personal data in the implementation of public health measures during public health

emergencies.

SECTION 1. Scope. —The provisions of this Circular shall apply to all personal information controllers (PICs) and personal information processors (PIPs) engaged in the processing of personal data during the COVID-19 public health emergency within the general framework of the necessary public health measures.

The relevant portions of the following sections of this Circular shall likewise apply to all future public health emergencies: Section 3 on General Principles, Section 4 on Criteria for lawful processing and purpose, Section 5 on Further processing and limitation, Section 7 on Privacy Impact Assessment, Section 8 on Privacy Notice, Section 9 on Application (app) permissions, Section 10 on Security Measures, Section 11 on Mandatory Submission of List of CTAs and Vaccine Card Systems, Section 12 on Storage and Retention, Section 13 on Disposal of personal data and decommissioning of CTAs and Vaccine Card Systems, and Section 14 on Data subject rights.

SECTION 2. Definition of Terms. — For the purpose of this Circular, the following terms are defined, as follows:

A. “Act” or “DPA” refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012;

B. “Application Programming Interface” or “API” refers to a set of well-defined methods, functions, protocols, routines or commands which application software uses with facilities of programming languages to invoke services;¹

C. “Commission” or “NPC” refers to the National Privacy Commission;

D. “Consent of the data subject” refers to 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.;

¹ See: International Organization for Standardization, ISO/TS 23029:2020(en) Web-service-based application programming interface (WAPI) in financial services, available at <https://www.iso.org/obp/ui/#iso:std:iso:ts:23029:ed-1:v1:en> (last accessed June 19, 2021).

² Department of Health, Update Guidelines on Contact Tracing of Close Contacts of Confirmed Coronavirus Disease (COVID-19) Cases, Department Memorandum No. 2020-0189 (April 17, 2020).

³ National Privacy Commission, Registration of Data Processing Systems and Notifications regarding Automated Decision-Making Operations [NPC Circular No. 17-01], § 3 (F): “Data Processing System” refers to a structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.

E. “Contact Tracing” refers to the identification, listing, and follow-up of persons who may have come into contact with a confirmed COVID-19 case. Contact tracing is an important component in containing outbreaks of infectious diseases. Under Code Red Sublevel 2, contact tracing is aimed at mitigating the spread of the disease;²

F. “Contact Tracing Application” or “CTA” refers to data processing systems³ specifically designed to accomplish or support contact tracing;

G. “COVID-19 Vaccination Program” refers to the response of the national government in addressing the adverse impact of COVID-19 through the delivery and administration of both procured and donated COVID-19 vaccines, management of Adverse Event Following Immunization (AEFI) and indemnification as covered under the Republic Act No. 11525 or the or the COVID-19 Vaccination Program Act of 2021;⁴

H. “Data Protection Officer” or “DPO” refers to an individual designated by the head of agency or organization to be accountable for its compliance with the DPA, its IRR, and other issuances of the Commission: provided, that a government agency or private entity may have more than one DPO;

I. “Data subject” refers to an individual whose personal, sensitive personal, or privileged information is processed;

J. “Decommissioning” refers to a process by which a business application (or system) is removed from use in an organization. It requires analysis of the data in the system, identifying the data, metadata and system documentation that must be brought forward and retained, and an accountable process for deletion of residual data in the system;⁵

K. “DOH Partner Agency” refers to the Department of Health (DOH) designated/deputized public health authority to collect and process COVID-19-related data for the purpose specified under the DOH and NPC Joint Memorandum Circular No. 2020-0002;⁶

⁴ See: Department of Health and the National Task Force Against COVID-19, Rules and Regulations Implementing Republic Act No. 11525 [Joint Administrative Order No. 2021-0001], § V (E), (March 26, 2021).

⁵ See: NSW State Archives, Decommissioning systems: records and information management considerations, available at <https://www.records.nsw.gov.au/recordkeeping/advice/decommissioning-systems#:~:text=Decommissioning%20is%20a%20process%20by,from%20use%20in%20an%20organisation> (last accessed June 19, 2021).

⁶ Department of Health (DOH) and National Privacy Commission (NPC), Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response, Joint Memorandum Circular No. 2020-0002 (April 24, 2020).

L. “Government Agency” refers to a government branch, body, or entity, including national government agencies, bureaus, or offices, constitutional commissions, local government units, government-owned and controlled corporations, government financial institutions, state colleges and universities;

M. “IRR” refers to the Implementing Rules and Regulations of Republic Act No. 10173;

N. “Personal data” refers to all types of personal information and sensitive personal information;

O. “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;

P. “Personal information controller” or “PIC” refers to a natural or juridical person, or any other body, who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization;
- or
2. A natural person who processes personal data in connection with his or her personal, family, or household affairs;

There is control if the natural or juridical person or any other body decides on what information is processed, or the purpose or extent of its processing.

Q. “Personal information processor” or “PIP” refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data;

R. “Privacy by Design” is an approach that ensures that privacy and data protection have been taken into account during the design phase of a system, project, program and process and will continue to be taken into account throughout its lifecycle and implementation;

S. “Privacy enhancing technologies” or “PETs” also known as “Privacy-preserving methodologies” is a coherent system of ICT

measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the data system.⁷ PETs ranges from tools that provide anonymity to those that allow a user to choose if, when, and under what circumstances personal information is disclosed.⁸

T. “Private entity” refers to any natural or juridical person, or any other body that is not a unit of the Philippine government or any other foreign government entities, such as but not limited to, stock and non-stock corporations, foreign corporations, partnerships, cooperatives, sole proprietorships, or any other legal entity;

U. “Privacy Impact Assessment” 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 PIP. It takes into account 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;

V. “Privileged information” refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication;

W. “Processing” refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system;

X. “Public Health Authority” refers to the Department of Health (DOH), specifically the Epidemiology Bureau, Disease Prevention and Control Bureau, Bureau of Quarantine and International Health Surveillance, Health Emergency Management Bureau,

⁷ See: European Union Agency For Network And Information Security, Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies Methodology, Pilot Assessment, and Continuity Plan, available at <https://www.enisa.europa.eu/publications/pets> (last accessed October 5, 2021).

⁸ Ibid.

Food and Drug Administration, government hospitals, Research Institute for Tropical Medicine and other National Reference Laboratories, and DOH Regional Offices, the local health office (provincial, city or municipality), or any person directly authorized to act on behalf of the DOH or the local health office;⁹

Y. “Public Health Emergency” refers to an occurrence or imminent threat of an illness or a health condition that poses a high probability of a large number of deaths in the affected population; a large number of serious injuries or long-term disabilities in the affected population; widespread exposure to an infectious or toxic agent that poses a significant risk of substantial harm to a large number of people in the affected population; and international exposure to an infectious or toxic agent that poses a significant risk to the health of citizens of other countries;¹⁰

Z. “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 individual, 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 is 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.

AA. “System architecture” refers to a single, high-level, description of the major elements or objects of a system plus the inter-connections between them.¹¹

BB. “Threat modeling” refers to a systematic exploration technique to expose any circumstance or event having the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service.¹²

⁹ An Act Providing Policies and Prescribing Procedures on Surveillance and Response to Notifiable Diseases, Epidemics, and Health Events of Public Health Concern, and Appropriating Funds Therefor, Repealing for the Purpose Act No. 3573, Otherwise Known as the “Law on Reporting of Communicable Diseases [Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act], Republic Act No. 11332, § 3 (k) (2019).

¹⁰ Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act, § 3 (l).

¹¹ See: International Organization for Standardization, ISO/TR 26999:2012(en), Intelligent transport systems, § 2.15, available at <https://www.iso.org/obp/ui/#iso:std:iso:tr:26999:ed-1:v:1:en> (last accessed October 19, 2021).

¹² See: International Organization for Standardization, ISO/IEC/IEEE 24765:2017(en), Systems and software engineering, § 3.4290, available at <https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:24765:en> (last accessed October 19, 2021).

SECTION 3. General principles. — The processing of personal data in response to public health emergencies as part of a public health measure, specifically the prevention, detection, isolation, treatment, and reintegration strategies such as but not limited to testing, contact tracing, treatment, and activities relating to vaccine deployment, is recognized, and shall be governed by the following principles:

A. Transparency. PICs shall provide the necessary privacy notices at the appropriate instances in relation to all personal data processing activities for public health emergencies to adequately inform data subjects of the details of the processing of their personal data and their rights under the DPA;

B. Legitimate purpose. The specific purpose/s for personal data processing in response to public health emergencies as part of a public health measure shall be clearly determined prior to any personal data processing activities;

C. Proportionality. The processing of personal data shall be limited to the extent necessary to fulfill the identified legitimate purpose/s. Privacy enhancing technologies or privacy-preserving methodologies shall be employed to the end that personal data shall be processed only if the purpose of the processing could not be reasonably fulfilled by other means;

D. Safeguards. PICs shall implement appropriate measures, taking into account the integration of privacy by design and risk management in the development of systems and other digital tools where privacy is embedded into the design and architecture of the same and integral to the system without diminishing functionality;¹³

E. Data subject rights. PICs shall recognize and uphold the rights of affected data subjects, unless otherwise provided by law;¹⁴ and

F. Compliance and accountability. PICs shall fulfill all applicable requirements prescribed by the DPA, its IRR, and other issuances of the NPC.

¹³ 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 Jan 2021) and 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 (2012).

¹⁴ 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); Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 34-37 (2016); and National Privacy Commission, Data Subject Rights [NPC Advisory No. 2021-01] (January 29, 2021).

SECTION 4. Criteria for lawful processing; purpose. — A lawful basis for processing is necessary for all personal data processing activities as part of the response to public health emergencies:

A. Personal data processing shall be based on the applicable laws, rules, and regulations requiring the collection and use of personal data for a public health measure; and

B. Personal data collected as part of the response to public health emergencies shall not be repurposed for direct marketing, profiling, or any other analogous purpose, whether commercial or non-commercial.

SECTION 5. Further processing; limitation. — Further processing of personal data may be allowed in instances which are compatible or consistent with the response to public health emergencies as part of public health measures, such as but not limited to historical, statistical, or scientific purposes.

A. The further processing is considered incompatible when:

1. It would be very different from the original purpose of responding to public health emergencies as part of public health measures or there is no clear and reasonable link between such original purpose and the purposes of the intended further processing;

2. It would result in an unjustified consequence on the rights and freedoms of the data subject;¹⁵ or

3. It would not be reasonably expected by the data subject considering the context in which the personal data has been collected.

Further processing shall only be allowed when upon examination, it is determined to be compatible with the original 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.¹⁶

¹⁵ See generally: Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, available at <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> (last accessed 29 September 2021).

¹⁶ See: National Privacy Commission, *JV v. JR*, NPC Case No. 17-047 (August 13, 2019) available at <https://www.privacy.gov.ph/wp-content/uploads/2020/10/CID-17-047-JV-v.-JR-Decision-PSD-10Aug2020.pdf>

¹⁷ Department of Health (DOH) and National Privacy Commission (NPC), Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response, Joint Memorandum Circular No. 2020-0002, § VI (F), (April 24, 2020).

B. The processing for research purposes may be allowed only when the same is intended for a public benefit and subject to the requirements of applicable laws, regulations, and ethical standards such as those prescribed by various research ethics boards or committees of the government, academic institutions, and other similar organizations prescribing such standards: provided, that processing for health research shall involve only aggregate, pseudonymized, or anonymized data. Likewise, all policy and biomedical research related to COVID-19 surveillance and response shall secure an Ethics Board approval prior to implementation.¹⁷

C. Any authorized further processing shall have adequate safeguards for data privacy and security, such as anonymization, pseudonymization, restriction on access, and shall uphold the rights and freedoms of the data subjects.

SECTION 6. Personal data requirements. — PICs should not collect any unnecessary personal data. Subject to the applicable laws and regulations, the collection of personal data required for the implementation of public health measures, specifically for contact tracing within workplaces and establishments, and the issuance of vaccine cards by either the local government units or the private sector, shall be limited to the following:

A. Contact tracing forms, whether paper-based or electronic. Personal data and other details as indicated in the (1) Employee Health Declaration Form and (2) Client/Visitor Contact Tracing Form provided for under the Department of Trade and Industry (DTI) and Department of Labor and Employment (DOLE) Supplemental Guidelines on Workplace Prevention and Control of COVID-19, Joint Memorandum Circular No. 20-04-A Series of 2020;¹⁸ and

B. COVID-19 Vaccine Card. Pursuant to DOH and the National Task Force Against COVID-19 Joint Administrative Order (JAO) No. 2021-0001, a standardized COVID-19 vaccine card shall be issued to vaccine recipients to ensure completion of the re-quired doses by documenting details of their vaccination.¹⁹ The vaccine card shall contain the following information with a template to be issued by the DOH:

1. Basic personal information such as full name, present and/or permanent address, and birthdate;
2. Manufacturer, brand name, batch number, lot number, or other identifier of the COVID-19 vaccine;

3. Date and time of vaccination;
4. Name of the hospital, health center, or health facility where the vaccine was administered;
5. Name, signature, and license number of the duly licensed physician, nurse, pharmacist, midwife or other health worker administering the vaccine;
6. Date of the last RT-PCR testing and the name of the laboratory that conducted the last RT-PCR testing, if applicable;
7. Name and details of contact person or person to be notified, in case of emergency; and,
8. Other information which may be determined as necessary by the Secretary of Health or the IATF-EID.²⁰

SECTION 7. Privacy Impact Assessment. — PICs shall conduct a privacy impact assessment (PIA) prior to adoption, use, or implementation of any personal data processing system, such as but not limited to, contact tracing applications (CTAs) and vaccine card systems or applications (Vaccine Card Systems).

A. For existing CTAs and Vaccine Card Systems, a PIA shall be conducted within fifteen (15) days from effectivity of this Circular;

B. A PIA shall be required when there are changes in the governing law or regulations or other proposed modifications which ultimately result in changes to the nature, scope, purpose, manner, and extent of the processing of personal data through CTAs and Vaccine Card Systems; and

C. The submission of the PIA report shall be required by the Commission in case of a compliance check, personal data breach, or investigation. The report shall contain the findings identifying the gaps and risks, how these have been remediated, and the status of such remediation efforts.

SECTION 8. Privacy Notice. — PICs shall ensure transparency in all personal data processing activities through an appropriate privacy notice, which is always required regardless of the lawful basis used for the processing. A privacy notice should provide concise, intelligible, and relevant information made readily available to the data subjects.

¹⁸ Department of Trade and Industry (DTI) and Department of Labor and Employment (DOLE), Supplemental Guidelines on Workplace Prevention and Control of COVID-19, Joint Memorandum Circular No. 20-04-A Series of 2020 [JMC No. 20-04-A] (Aug 15, 2020).

¹⁹ Department of Health and the National Task Force Against COVID-19, Rules and Regulations Implementing Republic Act No. 11525 [Joint Administrative Order No. 2021-0001], § VII (J) (1), (March 26, 2021).

²⁰ Id. § VII (J) (3).

A. All CTAs and Vaccine Card Systems shall provide the following information through an appropriate privacy notice:

1. Identity of the PIC;
2. Description of the personal data to be entered into the system;
3. Permissions required by applications, including their description and purposes;
4. Purpose for which the personal data will be processed;
5. Objective/s that are meant to be achieved by the system;
6. Lawful basis for processing;
7. Scope and method of the processing, including:
 - a) methods utilized for automated access;
 - b) storage and retention period;
 - c) policy for destruction or disposal; and
 - d) general description of technical security measures and other safeguards;
8. Recipients to whom personal data are or may be disclosed or shared and the purpose for the same;
9. The rights of data subjects and how these may be exercised;
10. Contact details of the data protection officer (DPO); and
11. Other information that would sufficiently inform the data subject of the nature and extent of data processing involved;

B. Privacy notices shall use clear and plain language. PICs shall determine whether a privacy notice will be more effective if translated into Filipino or in another language or dialect to be better understood by the users;

C. PICs shall convey the privacy notices prior to the collection of data by CTAs and Vaccine Card Systems. PICs shall assess the appropriateness of the contents of the privacy notice vis-à-vis the timing when a privacy notice is displayed through the CTA or Vaccine Card System, e.g., providing information on the specific process that is relevant at a particular time such as at set-up, just-in-time, context-dependent, periodic, persistent, on demand, taking into consideration user experience and the system's interface;

D. For existing CTAs and Vaccine Card Systems, PICs shall notify the data subjects at the next practical opportunity of the information mentioned in subsection A. The timing of the provision of information must always be within a reasonable period to give effect to the data subject's right to be informed; and

E. PICs shall regularly review and update their privacy notice to ensure that it properly reflects the actual processing of personal data for the implementation of public health measures. Where there are changes in the scope, purpose, nature, or extent of the processing, PICs must ensure that the data subjects are adequately informed of the same within a reasonable time: provided, that the period shall not exceed thirty (30) business days.

SECTION 9. Application (app) permissions. — Permissions requested by CTAs or Vaccine Card Systems, where applicable, shall be governed by the following:

A. Request minimum permissions. PICs shall assess the proportionality of app permissions and only request for those that are necessary to fulfill its functions.

B. Ask in context. Apps requiring specific permissions shall request them at the most reasonable and appropriate time, such as by means of pop-up notices or just-in-time notices, or any similar manner when the app or the data subject's use requires or triggers it.²¹

C. Provide adequate user choices. Whenever possible, apps shall minimize the time or access window of permissions and provide clear choices to users in managing permissions:

1. While using the app. The app will only have access to the specific permission when the app is being actively used in the foreground or in the active window of the device;

2. Only this time. The app will have access temporarily to a specific permission sought from the user, i.e., one-time permission, where such permission shall automatically be withdrawn after the app is closed by the user; and

3. Deny. The app will be prohibited to use the requested permission. PICs are required to provide mechanisms whereby users are still able to use the app despite this choice.

D. Only access sensitive permissions when necessary and the user reasonably expects it. Apps must provide continuous visual cues, indicators, or notices that are easily understood by users, such as a small icon in the status bar for mobile phones or in the browser's toolbar for websites, that applications are actively accessing

sensitive permissions, i.e., camera, location, microphone.

E. Pay attention to libraries. Apps shall be audited with regard to personal data especially sensitive personal information accessed by third-party Application Programming Interfaces (APIs) and libraries. Such third-party APIs and libraries must also be clearly indicated in the app's privacy notice.

SECTION 10. Security Measures. — PICs shall implement adequate safeguards to protect personal data processed against accidental, unlawful, or unauthorized use or access.²²

A. Technical measures. PICs shall integrate privacy by design and secure software development at every stage of the lifecycle to ensure the protection of personal data that will be processed without diminishing functionality. PICs shall consider the following recommended measures:

1. Requirements. PICs shall determine the appropriate requirements for the CTAs and Vaccine Card Systems including, but not limited to, the types and amount of personal data to be processed, the minimum application permissions required, policies in using the personal data, system architecture, threat modeling, and programming code or language to be used.

a) The requirements should comply with the general data privacy principles of transparency, legitimate purpose, and proportionality.

b) PICs shall also inform the data subjects of the risks posed by the system's architecture based on the results of the threat modeling and privacy impact assessment activities.

2. Good practices. PICs shall ensure that both digital and manual contact tracing or processing for vaccine deployment are configured securely.

a) PICs shall deploy up-to-date software components and ensure the secure configuration thereof to mitigate the risk of personal data disclosure. Likewise, PICs shall follow good practices in developing and managing the application based on industry standards, such as secure coding principles, secure design principles, and the conduct of essential software testing.

b) For manual contact tracing or processing for vaccine deployment, PICs shall provide individual forms for the data subjects to accomplish. The use of logbooks that aggregates all their information in a single page shall be

prohibited.

c) Access controls must be in place to protect physical contact tracing forms from accidental or unauthorized disclosure.

3. Risk Management. PICs shall determine and implement appropriate risk management strategies in conducting assessments in identifying risk, threats, and vulnerabilities on the development and implementation of CTAs and Vaccine Card Systems;

4. Encryption. Personal data at rest shall be encrypted. All network communications between the application and the backend shall be encrypted. For this purpose, the Commission recommends Advanced Encryption Standard with a key size of 256 bits (AES-256) as the most appropriate encryption standard. PICs shall also use transport layer encryption to encrypt data in transit when communicating over mobile and Wi-Fi networks;

5. Tests. PICs shall test the application as the need arises, such as when there are new updates on the app or its components. For this purpose, PICs shall use both automatic and manual methods to check for any weak configurations, which may unintentionally expose personal data, endpoints, and other components that are not meant to be accessible. Testing should not be limited to functional tests but also security tests such as vulnerability scanning, code quality checks, (static and dynamic) code analysis tools, and source code scanning for libraries and developed code; and

6. Information Security Incident Management Policy. PICs shall implement policies and procedures for managing security incidents in accordance with NPC Circular No. 16-03.23 The policies and procedures shall contain a process for assessing reasonably foreseeable vulnerabilities in computer networks as well as identifying the preventive, corrective, and mitigating action necessary against incidents that can lead to a personal data breach.

B. Access. PICs shall implement an access control policy that shall identify and limit the personnel who shall be authorized to have access to the personal data collected through CTAs and Vaccine Card Systems, taking into account the applicable DOH issuances on the matter, i.e., only concerned healthcare providers, public health authorities, and DOH partner agencies and their authorized personnel shall be allowed to access health information in relation to COVID-19 cases and/or identified close contacts.²⁴

1. Authorized personnel shall be adequately trained on the proper processes in handling personal data collected and shall be required to execute a non-disclosure agreement (NDA); and

2. PICs shall be responsible for ensuring that their authorized personnel strictly abide by the provisions of the DPA, its IRR, and related issuances. PICs shall also remind its authorized personnel and the third-party service providers that processing the collected personal data for any other purpose is punishable under the DPA.

C. Disclosure. Disclosure of the personal data collected through the CTAs and Vaccine Card Systems 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.

In complying with the reportorial requirements of existing regulations, all PICs shall ensure that the same are securely transmitted, and must consider the following:

1. Keep records of all submissions/transmittals for reportorial requirements;

computer networks as well as identifying the preventive, corrective, and mitigating action necessary against incidents that can lead to a personal data breach.

B. Access. PICs shall implement an access control policy that shall identify and limit the personnel who shall be authorized to have access to the personal data collected through CTAs and Vaccine Card Systems, taking into account the applicable DOH issuances on the matter, i.e., only concerned healthcare providers, public health authorities, and DOH partner agencies and their authorized personnel shall be allowed to access health information in relation to COVID-19 cases and/or identified close contacts.²⁴

²³ National Privacy Commission, Personal Data Breach Management [NPC Circular No. 2016-03] (December 15, 2016).

²⁴ Department of Health (DOH) and National Privacy Commission (NPC), Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response, Joint Memorandum Circular No. 2020-0002, § VI (C), (April 24, 2020).

²⁵ See generally: Department of Health, Omnibus Interim Guidelines on Prevention, Detection, Isolation Treatment, and Reintegration Strategies for COVID-19 [Department Memorandum No. 2020-0439] (Oct 6, 2020).

1. Authorized personnel shall be adequately trained on the proper processes in handling personal data collected and shall be required to execute a non-disclosure agreement (NDA); and

2. PICs shall be responsible for ensuring that their authorized personnel strictly abide by the provisions of the DPA, its IRR, and related issuances. PICs shall also remind its authorized personnel and the third-party service providers that processing the collected personal data for any other purpose is punishable under the DPA.

C. Disclosure. Disclosure of the personal data collected through the CTAs and Vaccine Card Systems 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.

In complying with the reportorial requirements of existing regulations, all PICs shall ensure that the same are securely transmitted, and must consider the following:

1. Keep records of all submissions/transmittals for reportorial requirements;

2. Implement procedures to verify the genuineness of any information request made for contact tracing and vaccination status, and the response procedure for such verified request;

3. Ensure strict compliance with the protocols established by the DOH and LGUs for disclosing information through the conduct of contact tracing of those in close contact with a COVID-19 case;

4. Refer individuals for quarantine, isolation, testing, clinical management, etc. shall be in accordance with DOH guidelines;²⁵

²³ National Privacy Commission, Personal Data Breach Management [NPC Circular No. 2016-03] (December 15, 2016).

²⁴ Department of Health (DOH) and National Privacy Commission (NPC), Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response, Joint Memorandum Circular No. 2020-0002, § VI (C), (April 24, 2020).

²⁵ See generally: Department of Health, Omnibus Interim Guidelines on Prevention, Detection, Isolation Treatment, and Reintegration Strategies for COVID-19 [Department Memorandum No. 2020-0439] (Oct 6, 2020).

5. Disclosure of personal data to the public, the media, or any other public-facing platforms without the consent of the patient or vaccinee or his/her authorized representative or next of kin, shall be strictly prohibited.

SECTION 11. Mandatory Submission of List of CTAs and Vaccine Card Systems. — PICs shall submit to the Commission a complete list of all the CTAs and Vaccine Card Systems which they operate. The procedure for registration shall be in accordance with the relevant NPC issuances.

SECTION 12. Storage and Retention. — All personal data collected through CTAs and Vaccine Card Systems shall be stored in a secure manner using appropriate measures, including encryption. Personal data shall be retained only for as long as necessary when the purpose for processing still exists and in accordance with the period allowed by existing government issuances.

A. Generally, personal data collected through CTAs shall be stored only for a limited period and shall be disposed of properly after thirty (30) days from date of collection.²⁶ For CTAs involving the use of unique Quick Response (QR) Codes which are assigned to specific individuals or other similar systems, PICs shall distinguish the personal data or records for purposes of determining the retention period:

1. Names, addresses, and mobile numbers may be retained for a longer period or for as long as there is a state of public health emergency necessitating the need for such system; and

B. PICs shall ensure the deactivation or decommissioning of CTAs and Vaccine Card Systems within a reasonable period after the state of public health emergency has been lifted, adopting applicable industry standards. CTAs or Vaccine Card Systems shall not be repurposed unless otherwise provided by law and subject to the condition that all categories of personal data previously collected and stored for contact tracing and vaccine deployment are properly disposed of.

SECTION 14. Data subject rights. — CTAs and Vaccine Card Systems shall provide adequate user controls in the form of a dedicated privacy control panel, dashboard, or similar interface that enables the exercise of data subject rights under the DPA.

SECTION 15. Penalties. — The processing of personal data in violation of this Circular shall carry criminal, civil, and administrative liabilities pursuant to the provisions of the DPA, related issuances of the NPC, and other

applicable laws and regulations.

SECTION 16. 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 subject.

SECTION 17. Transitory provision. — Within fifteen (15) days from the effectivity of this Circular, all PICs shall register their DPOs and submit to the Commission a complete list of all the CTAs and Vaccine Card Systems that they operate in accordance with existing rules on NPC registration under NPC Circular No. 17-01. Within the same period, PICs shall conduct a mandatory review of all personal data processing systems related to the response to public health emergencies to determine compliance of such systems with the provisions of this Circular.

SECTION 18. Separability Clause. — If any portion or provision of this Circular is declared invalid or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 19. Repealing Clause. — All issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified accordingly.

SECTION 20. Effectivity. — This Circular shall take effect fifteen (15) days after its publication in the Official Gazette or two newspapers of general circulation.

Approved:

Sgd.

RAYMUND ENRIQUEZ LIBORO

Privacy Commissioner

Sgd.

LEANDRO ANGELO Y. AGUIRRE

Deputy Privacy Commissioner

Sgd.

JOHN HENRY D. NAGA

Deputy Privacy Commissioner

²⁶ See: DTI-DOLE JMC No. 20-04-A, § Sections II.D.I.e.v and III.C.4.d.

²⁷ See: National Privacy Commission, NPC Advisory Opinion No. 2020-054 (Dec. 28, 2020).

²⁸ See: Department of Health, The Revised Disposition Schedule of Medical Records Amending Ministry Circular 77, s. 1981 [Department Circular No. 70, s.1996] (May 8, 1996) available at [http://ehealth.doh.gov.ph/nehehrsv/sys/assets/HOSPITAL%20HEALTH%20INFORMATION%20MANAGEMENT%20MANUAL%20formerly%20HOSPITAL%20MEDICAL%20RECORDS%20MANAGEMENT%20MANUAL.pdf](https://zcwdrv320190208-dot-efoi-ph.appspot.com/requests/aglzfMvmb2ktcGhyHQsSB0NvbRlbnQIEERPSC0yNDIzOTEyNzUzMdIM; Department of Health National Center for Health Facility Development, Hospital Health Information Management Manual (2010) available at <a href=).



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