

# THE 2023 COMPENDIUM OF NPC ISSUANCES



# **TABLE OF CONTENTS**





# ADVISORY

---

- 11**            NPC Advisory No. 2023-01  
Guidelines on Deceptive Design Patterns

# CIRCULAR

---


- 16**            Circular No. 2023-01  
Schedule of Fees and Charges of the National Privacy  
Commission
- 22**            Circular No. 2023-02  
Data Privacy Competency Program - FAQ Data Privacy  
Competency Program
- 27**            Circular No. 2023-03  
Guidelines on Identification Cards
- 30**            Circular No. 2023-04  
Guidelines on Consent
- 44**            Circular No. 2023-05  
Prerequisites for the Philippine Privacy Mark Certification  
Program
- 47**            Circular No. 2023-06  
Security of Personal Data in the Government and the Private  
Sector
- 56**            Circular No. 2023-07  
Guidelines on Legitimate Interest - FAQ Guidelines on  
Legitimate Interest
- 80**            Circular No. 2024-01  
Amendments to Certain Provisions of the 2021 Rules of  
Procedure of the National Privacy Commission -  
2021 Rules of Procedure of the NPC




# ADVISORY OPINION

---

- 105**      **Advisory Opinion No. 2023-001**  
Re: Disclosure of Condominium Unit Owners' Personal Data and Related Documents.
  
- 112**      **Advisory Opinion No. 2023-002**  
Re: Disclosure of Tax Declarations of Real Properties and other Related Documents
  
- 117**      **Advisory Opinion No. 2023-003**  
Re: Disclosure of Property Information through the Land Registration Authority's Geo-spatial Query Service
  
- 120**      **Advisory Opinion No. 2023-004**  
Re: Disclosure of Subscribers' Data Pursuant to Revenue Regulation No. 09-2022
  
- 124**      **Advisory Opinion No. 2023-005**  
Re: Barangay Inventory of Vaccinated Population
  
- 129**      **Advisory Opinion No. 2023-006**  
Re: Request for Membership Details by a Spouse of a Missing Philhealth Member
  
- 133**      **Advisory Opinion No. 2023-008**  
Re: Blocking SMS with Clickable Links
  
- 136**      **Advisory Opinion No. 2023-009**  
Re: Data Sharing Agreement with a Specialized Agency of the United Nations
  
- 142**      **Advisory Opinion No. 2023-010**  
Re: Recording of Telephone Conversation through Voice Over Internet Protocol (VoIP) System
  
- 149**      **Advisory Opinion No. 2023-011**  
Re: Request for Information from Labor Unions

- 
- 154**      **Advisory Opinion No. 2023-012**  
Re: Collection of Information of Customers, Delinquent Borrowers, and Loan Applicants of CIBI Members
- 159**      **Advisory Opinion No. 2023-013**  
Re: Proposed Ordinance on the Establishment of a Barangay Database of all Households and Individuals in the Province of Palawan.
- 164**      **Advisory Opinion No. 2023-014**  
Re: Transfer Of Personal Data Among Personal Information Controllers
- 167**      **Advisory Opinion No. 2023-015**  
Re: Disclosure to the National Bureau of Investigation of the Record of Barangay Inhabitants
- 172**      **Advisory Opinion No. 2023-016**  
Re: Applicability of Soft Opt-in Approach in the Philippines
- 175**      **Advisory Opinion No. 2023-017**  
Re: Request of Government Agencies to Access Pnp’s Crime Information, Reporting and Analysis System (Ciras) and other Databases
- 180**      **Advisory Opinion No. 2023-018**  
Re: Request for Personal Data of Condominium Tenants by Philippine Drug Enforcement Agency (PDEA)
- 185**      **Advisory Opinion No. 2023-019**  
Re: Disclosure of an Individual Customer’s Personal Information Upon the Request of Another Individual Customer
- 189**      **Advisory Opinion No. 2023-020**  
Re: Use of Breath Analyzer on Employees and Service Providers
- 193**      **Advisory Opinion No. 2023-021**  
Re: Access to Documents Relative to a Business Permit Application.

- 
- 196**      **Advisory Opinion No. 2023-022**  
Re: Media Access to Police Blotters
- 200**      **Advisory Opinion No. 2023-023**  
Re: Request by a Third-party for Access to the Supporting Documents Relative to her Father’s Application for a Marriage License.
- 204**      **Advisory Opinion No. 2023-024**  
Re: Disclosure of Vessel Records from Regulatory Agency Thru Request Letter.
- 206**      **Advisory Opinion No. 2023-025**  
Re: Multi Face ID Initiative for Fraud Prevention.
- 212**      **Advisory Opinion No. 2023-026**  
Re: Creation of a Shared Employee Fraud Database
- 218**      **Advisory Opinion No. 2023-027**  
Re: Employer’s Data Privacy Obligations Concerning its Financial Services Benefit to its Employees.
- 220**      **Advisory Opinion No. 2024-001**  
Re: Request for Access to Personal Data for Audit Purposes
- 222**      **Advisory Opinion No. 2024-002**  
Re: Request for Comments/Insights Regarding the use of Artificial Intelligence (AI) in the Civil Service Commission’s (CSC) Correspondence
- 224**      **Advisory Opinion No. 2024-003**  
Re: Random Surveillance of Telecommuting Employees and Consent to the Recording of Virtual Meetings



# DECISION

---

- 229** NPC SS 22-001 and NPC SS 22-008  
In re: Commission on Elections
- 250** NPC 21-167  
MAF v. Shopee Philippines, Inc.
- 262** NPC 21-010 to NPC 21-015  
MVC, et al. v. DSL
- 272** NPC 20-317 and 20-318  
GBA v. SBG and LPL v. SBG
- 280** NPC 22-012  
RJC v. DL
- 286** NPC 20-026  
JBA v. FNT and NNT
- 302** NPC 19-1273  
NFM v. BPI
- 312** NPC 21-111  
EG v. JI, RO, and RR
- 326** NPC 21-054  
RGC v. JK Incorporated and Recovery, Inc.
- 337** NPC 21-122  
JBZ v. Metropolitan Bank & Trust Company
- 351** NPC 19-758 and NPC 19-1846  
Spouses MCD, JJD v. Victorias Milling Company, et al



# RESOLUTION

---

- 372**      CID BN 17-039  
In re: Sun Life of Canada
  
- 376**      NPC BN 20-208  
In Re: Commission On Elections (Comelec)
  
- 382**      NPC 17-K-001  
JCR vs. GLOBE TELECOM, INC.
  
- 386**      CID BN 17-021  
In re: Breach Notification Report of Sun Life of Canada
  
- 392**      NPC BN 20-157  
In re: Batangas Bay Carriers, Inc.
  
- 397**      NPC BN 18-179  
In re: ABS-CBN Corporation
  
- 403**      NPC BN 18-045  
In re: University of the Philippines - Visayas
  
- 407**      NPC BN 18-006  
In re: Business World Inc.
  
- 412**      NPC BN 22-094  
In re: Equicom Savings Bank
  
- 417**      NPC BN 18-085  
In re: La Salle Greenhills School
  
- 426**      NPC 22-180 and 22-181  
DVL v. Alamat Crewsers Motorcycle Club and LAE v. Alamat Crewsers Motorcycle Club
  
- 434**      NPC 22-012  
RJC v. DL



- 442** NPC 20-026  
JBA v. FNT and NNT
- 452** NPC BN 18-229  
In Re: LEAPFROGGR, Inc.
- 455** NPC BN 18-200  
In Re: Cardinal Health International Philippines, Inc.
- 460** NPC BN 18-115  
In Re: REMIT, Inc.
- 465** NPC BN 18-213  
In Re: Manufacturers Life Insurance Co.
- 476** NPC BN 18-033 and NPC BN 18-076  
In Re: AIG Shared Services-Business Processing Inc. and AIG Shared Services Corporation – Management Services (ROHQ), and In Re: Medicaid Philippines, Inc. - Festival Alabang Clinic

## ORDER

---

- 492** NPC 16-004  
CBP v. Orani Water District
- 497** NPC 21-010 to NPC 21-015  
MVC, et al. v. DSL
- 500** NPC BN 18-179  
In re: ABS-CBN Corporation
- 506** NPC BN 21-097  
In re: PowerVision EAP Inc
- 514** NPC BN 21-180  
In Re: Enchanted Kingdom Inc.
- 519** CID CDO 22-001  
CID vs. PH-Check.com



# ADVISORY



# NPC Advisory No. 2023 - 01

**DATE :** 07 November 2023

**SUBJECT :** GUIDELINES ON DECEPTIVE DESIGN PATTERNS

**WHEREAS,** Section 7 (g) of the Data Privacy Act of 2012 (DPA) provides that the National Privacy Commission (NPC) is empowered to publish, on a regular basis, a guide to all laws relating to data protection;

**WHEREAS,** the NPC issued a Circular on the “Guidelines on Consent” to elaborate on the processing of personal data based on consent and to emphasize the fair processing of personal data in a manner that is neither manipulative nor unduly oppressive to data subjects;

**WHEREAS,** Section 7 (A) of the Guidelines on Consent provides that the use of deceptive methods, such as deceptive design patterns, results in vitiated consent for not being freely given;

**WHEREAS,** consent is not freely given in instances where 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;

**WHEREAS,** the utilization of deceptive design patterns in personal data processing activities is tantamount to deception and coercion which may result in the vitiation of the consent given by data subjects and the infringement of their data privacy rights;

**WHEREAS,** data subjects must be made aware of the nature and common examples of deceptive design patterns in order to prevent them from being victimized;

**WHEREAS,** a personal information controller (PIC) must avoid such practices on their analog and digital interfaces as they have a responsibility to adhere to the general privacy principles at all times and ensure that mechanisms are in place for the exercise of data privacy rights;

**WHEREAS,** as deceptive design patterns are already rampant, guidelines are necessary to uphold data subject rights to maintain trust in transactions in analog or digital interfaces;

**WHEREFORE,** in consideration of these premises, the NPC hereby issues this Advisory on deceptive design patterns.

**SECTION 1. Purpose.** — This Advisory provides guidance on PICs on the nature of deceptive design patterns, and its impact on the lawful processing of personal data based on the data subject’s consent and in line with the general privacy principles. This Advisory aims to prevent the usage of deceptive design patterns on analog and digital interfaces.

**SECTION 2. *Definition of Terms.*** — Terms used in the DPA and its Implementing Rules and Regulations (IRR), as amended, are adopted herein. In addition, whenever used in this Advisory, the following terms are defined as follows:

A. “Deceptive Design Patterns” refer to design techniques embedded on an analog or digital interface that aim to manipulate or deceive a data subject to perform a specific act relating to the processing of their personal data.

B. “Analog Interface” refers to an offline point of interaction between two or more users;

C. “Appearance-Based Deceptive Design Pattern” refers to a design pattern that manipulates or deceives a data subject through the display or presentation of information;

D. “Content-Based Deceptive Design Pattern” refers to a design pattern that manipulates or deceives a data subject through the actual contents, including the language and context, of the information made available to them;

E. “Digital Interface” refers to any software, including a website or a part thereof, or computer or mobile application;<sup>1</sup>

F. “User Experience” or “UX” refers to the overall experience of a data subject using an analog or digital interface in relation to its convenience, accessibility and credibility;

G. “User Interface” or “UI” refers to the means by which a data subject interacts with a website, a computer or mobile application, or offline points of interaction.

**SECTION 3. *Deceptive Design Patterns.*** – Deceptive design patterns undermine general data privacy principles and the rights of data subjects. The following is a non-exhaustive list of prevalent deceptive design patterns:

A. Appearance-Based Deceptive Design Patterns are those, but are not limited to, that:

1. prohibit a data subject from categorically disallowing the processing of their personal data, or repeatedly prompt a data subject to take an action to share more information than what is necessary or originally intended;

2. present control settings that confuse a data subject such that it leads them to inadvertently consent to the processing of their personal data;

3. make it easy to consent to the processing of their personal data but make it difficult to withdraw their consent by requiring the data subject to undertake tedious, complex, and time-consuming processes;

4. accentuate a choice that results in the processing of more personal data, while blurring or obfuscating the option that enables data minimization;

---

<sup>1</sup> REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), Article 3 (m) (19 October 2022).

5. purposely complicate or muddle a data subject's choices relating to the processing of their personal data;

6. bombard a data subject with excessive information that is not essential to the processing of their personal data;

7. present default options that benefit the PIC but may be detrimental to the data subject, such as (1) maximizing the amount of personal data that will be processed; or (2) unnecessarily bundling the purposes for processing;

8. use style and design techniques to distract a data subject from the information provided by a PIC: (1) to acquire the data subject's consent for the processing of their personal data; or (2) for the data subject to provide more information than what is required or necessary for the specified purpose declared; or

9. use characters that children know and trust to influence them into providing more information than what is necessary for the declared purpose.

B. Content-Based Deceptive Design Patterns are those, but are not limited to, that:

1. use ambiguous, complex, or confusing language or sentence structures to steer a data subject into making a choice that is detrimental or violative of their rights as a data subject;

2. provide contradicting, fabricated, or misleading information, or omitting relevant information when acquiring the data subject's consent for the processing of their personal data; or

3. frame choices as better alternatives to shame or steer a data subject from making a choice that better adheres to the general principles of privacy or respects their rights as a data subject.

**SECTION 4. *Transparency.*** – A PIC shall ensure transparency in the presentation of information to the data subject by avoiding deceptive design patterns. In accordance with the DPA and the Guidelines on Consent, a PIC shall ensure that the data subject is aware of the nature, purpose, and extent of the processing of personal data.

The user interface must provide a concise statement in clear, plain, consistent, and straightforward language on the personal data to be processed, nature, purpose, extent, duration, and scope of processing for which consent is used as basis, risks and safeguards involved, the identity of the PIC, the existence of data subject rights, and how these rights can be exercised.

**SECTION 5. *Fairness.*** – A PIC shall ensure that personal data is processed in a manner that is neither manipulative nor unduly oppressive to a data subject. As such, an analog or digital interface must be designed and operated in a way that the processing of information will not be detrimental, discriminatory, unexpected, or misleading to a data subject. The use of deceptive design patterns on analog or digital interfaces violates fairness and may result in vitiating the consent of the data subject.

**SECTION 6. *Accountability.*** – A PIC is responsible for the personal data it processes through an analog or digital interface. The user interface and user experience may be used as evidence to show that the data subject has read and understood the information that the PIC has given on the processing that the data subject consented to.

**SECTION 7. *Effects on Consent.*** – The use of Deceptive Design Patterns contravenes the principle of Fairness as provided in Section 5 of this Advisory. As such, its use may result in invalidating the consent given by a data subject for a specific processing activity and renders the processing undertaken without valid lawful basis.

**SECTION 8. *Privacy by Design.*** – A PIC’s use of Appearance-Based Deceptive Design Patterns or Content-Based Deceptive Design Patterns is inconsistent with its obligation to adopt a Privacy by Design approach in the processing of personal data.

**SECTION 9. *Interpretation.*** – Any doubt in the interpretation of any provision of this Advisory shall be liberally interpreted in a manner mindful of the rights and interests of the data subject.

**Approved:**

**SGD.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**SGD.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

**SGD.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner



# CIRCULARS



# NPC Circular No. 2023-01

**DATE :** 17 May 2023

**SUBJECT :** SCHEDULE OF FEES AND CHARGES OF THE NATIONAL PRIVACY COMMISSION

**WHEREAS**, Executive Order No. 292, otherwise known as the “Administrative Code of 1987”, authorizes all agencies to charge fees, including honoraria, and other reasonable allowances, as compensation for consultation, seminars or training programs, or technical services rendered to other government agencies or private parties;

**WHEREAS**, the National Privacy Commission (NPC) was created under Republic Act No. (R.A.) 10173, otherwise known as the “Data Privacy Act of 2012” (DPA), in order to discharge the duty of the State to protect individual personal information in information and communications systems in the government and the private sector;

**WHEREAS**, the Administrative Code of 1987 provides that heads of bureaus, offices, or agencies, upon approval of the concerned department head, have the continuing authority to revise their rates of fees and charges to recover the cost of the service rendered;

**WHEREAS**, Administrative Order No. 31 series of 2012 states that the rates of fees and charges collected must be just and reasonable to enable the government to provide services without straining the National Government’s resources effectively;

**WHEREAS**, Administrative Order No. 31 allows the collection of fees to reduce or minimize government spending while allowing the continued performance of services to the public through efficient resource management and in recognition of the cost recovery principle;

**WHEREAS**, DOF-DBM-NEDA Joint Circular No. 1-2013 provides the procedures in imposing new fees in all departments, bureaus, commissions, agencies, offices and instrumentalities of the National Government;

**NOW, THEREFORE**, the **NATIONAL PRIVACY COMMISSION**, by virtue of the authority vested by law, hereby adopts the following schedule of rates of fees:

SECTION 1. **Schedule of Fees** – Hereunder is the list of all the fees and charges to be imposed and collected by the NPC



PARTICULARS	Rates
<b>Complaints and Investigation</b>	
Filing Fee for Complaints	Php 500.00
Additional Fee for Claims of Damages	
a. Not more than Php 20,000.00	Php 150.00
b. More than Php 20,000.00 up to Php 100,000.00	Php 500.00
c. For every succeeding Php 100,000.00, or a fraction thereof	Php 500.00
Motion for Reconsideration	Php 500.00
Application for Cease-and-Desist Order (CDO)	Php 1,000.00
Cease and Desist Order Bond	<p>If the CDO is included in the complaint, the bond shall be computed as follows:</p> <p style="text-align: center;">(total amount of filing fees) × (number of affected data subjects)</p> <p style="text-align: center;">Sample: Php 500.00 × 1 = Php 500.00</p> <p>If the CDO is filed separately, the bond shall be computed as follows:</p> <p style="text-align: center;">(total amount of filing fees) × (number of affected data subjects based on the application filed)</p> <p style="text-align: center;">Sample: Php 1,000.00 × 1 = Php 1,000.00</p> <p>* In no case shall the amount of the bond exceed Php 100,000.00.</p>
Certificate of No Pending Case	Php 500.00
Temporary Ban Bond	<p>The amount of bond shall be computed as follows:</p> <p style="text-align: center;">(total amount of filing fees) × (number of affected data subjects based on the complaint filed)</p> <p style="text-align: center;">Sample: Php 500.00 × 1 = Php 500.00</p>

	* In no case shall the amount of the bond exceed Php 50,000.00
Legal Research Fee	1% of the filing fee but not less than Php 10.00
<p><i>Indigent Litigants are exempt from payment of legal fees:</i></p> <ol style="list-style-type: none"> <li>a. <i>Those whose gross income and that of their immediate family do not exceed an amount double the monthly minimum wage of an employee; and</i></li> <li>b. <i>Those who do not own real property with a fair market value as stated in the current tax declaration of more than Three Hundred Thousand Pesos (Php 300,000.00)</i></li> </ol> <p><i>To be entitled to the exemption herein provided, the litigant shall provide all documents enumerated below:</i></p> <ol style="list-style-type: none"> <li>a. <i>Certificate of Indigency from the Barangay where he or she resides.</i></li> <li>b. <i>Notarized affidavit that the litigant and his or her immediate family do not earn a gross income abovementioned, nor they own any real property with the fair value aforementioned, and supported by a notarized affidavit of a disinterested person attesting to the truth of the litigant's affidavit.</i></li> <li>c. <i>The current tax declaration, if any, shall be attached to the litigant's affidavit.</i></li> </ol>	
<i>Government agencies and its instrumentalities are exempt from paying fees and bonds.</i>	
<i>Local government and government-owned and controlled corporations with or without independent chapters are exempt from paying fees and bonds.</i>	
<b>Mediation</b>	
<p><b>Mediation Fee</b></p> <p><i>The cost of the mediation fee of Php 500.00 shall be shared equally among the parties applying for mediation (both complainant/s and respondent/s).</i></p> <p><i>The Mediation Fee shall cover the entire mediation process regardless of the number of scheduled mediation conferences.</i></p> <p><i>In case the parties re-apply for mediation after a previously terminated mediation, the parties shall again pay the mediation fee.</i></p>	<b>Php 500.00</b>
<p><i>Indigent Litigants are exempt from payment of legal fees:</i></p> <ol style="list-style-type: none"> <li>a. <i>Those whose gross income and that of their immediate family do not exceed an amount double the monthly minimum wage of an employee; and</i></li> <li>b. <i>Those who do not own real property with a fair market value as stated in the current tax declaration of more than Three Hundred Thousand Pesos (Php 300,000.00)</i></li> </ol>	

To be entitled to the exemption herein provided, the litigant shall provide all documents enumerated below:

- a. Certificate of Indigency from the Barangay where he or she resides.
- b. Notarized affidavit that the litigant and his or her immediate family do not earn a gross income abovementioned, nor they own any real property with the fair value aforementioned, and supported by a notarized affidavit of a disinterested person attesting to the truth of the litigant's affidavit.
- c. The current tax declaration, if any, shall be attached to the litigant's affidavit.

Government agencies and its instrumentalities are exempt from paying mediation fees.

Local government and government-owned and controlled corporations with or without independent chapters are exempt from paying mediation fees.

### Online Data Processing System /Data Protection Officer Registration

#### Initial Registration Fees

Individual/Professional	Php 500.00
Public and Private Organization	
1. Multinational/ National/ Foreign Branch	Php 2,500.00
2. Regional/ Provincial/ Metro Manila areas/ Cities	Php 1,000.00
3. Municipalities	Php 500.00

#### Registration Renewal Fees

Individual/ Professional	Php 350.00
Public and Private Organization	
1. Multinational/ National/ Foreign Branch	Php 1,000.00
2. Regional/ Provincial/ Metro Manila areas/ Cities	Php 500.00
3. Municipalities	Php 350.00

#### Major Amendments

(a) Name of PIC/PIP

(b) Principal Office Address of PIC/PIC/Individual Professional

1. Multinational/ National/ Foreign Branch	Php 2,500.00
2. Regional/ Provincial/ Metro Manila areas/ Cities	Php 1000.00
3. Municipalities	Php 500.00
4. Individual Professional	Php 500.00

#### Other Registration Fees

Validation/ Authentication/ Certified True Copy of Certificate of Registration (COR)	Php 100.00
-----------------------------------------------------------------------------------------------	------------

Recovery of Inaccessible DPO Accounts	Php 5,000.00
<b>Advisory Opinion and Legal Research</b>	
Request for Advisory Opinion	Php 7,500.00
Legal Research Fee for issuance of Advisory Opinions	Php 75.00
<b>Enforcement</b>	
Certified True Copies (CTC) of any paper, record, decree, judgment, or entry thereof	Php 10.00 per page plus Php 50.00 authentication fee per document
Request for issuances of clearances and certifications	Php 50.00 per document
Legal Research Fee for issuance of clearances and certifications.	1% of the filing fee imposed but in no case lower than Php 10.00

SECTION 2. **Fees Payable in Advance** – All fees shall be collected in advance of any service to be rendered or materials to be furnished. Upon the filing of a complaint or other application which initiates a service to be rendered or materials to be furnished, the fees prescribed therefor shall be paid in full. The NPC shall not act on any pending transaction or request unless the prescribed fee is paid in full on or before the due date.

In case of indigent litigants as stated under Section 1, all requirements for exemption shall be submitted and attached with the application or request form.

SECTION 3. **Date of Payment** – Fees shall be considered to have been paid as follows:

- a. For Cash Payment: The date of receipt in cash of the amount due in full.
- b. For Check Payments: The manager’s check shall be payable to the National Privacy Commission. The date of receipt is honored upon first presentment and provided that the payment covers the amount due in full.
- c. For Online Payment: The date of proof of online transfer or payment.

SECTION 4. **Time and Place of Payment** – Payment transactions shall be made during regular working days and business hours, from Monday to Friday 8:00 a.m. to 5:00 p.m. to the NPC Cashier.

Online payments, if applicable, shall be coursed through an official online payment partner of the NPC.

Section 5. **Error or Mistake in Payments** - In case of excess amount paid, the payor may file with the concerned division a request for refund within thirty (30) working days from the date of payment. All requests for refund of the excess amount paid shall be endorsed by the concerned division to Finance and Administrative Office (FAO) within five (5) working days from the receipt of the request.

The FAO shall evaluate the request, and if meritorious, the excess amount shall

be processed in accordance with the established guidelines of the Department of Budget and Management and Bureau of Treasury. The refunded amount shall be released to the payor within five (5) working days from the receipt of its corresponding Notice of Cash Allocation.

In case the request is not meritorious, the payor shall be informed at the contact information indicated in the request for refund.

SECTION 6. **Non-refundable payments** – Fees paid pursuant to Section 1 hereof, shall be non-refundable, except in cases wherein Section 5 is applicable.

SECTION 7. **Annual Review** – Pursuant to Sec 5.1 and 5.2 of DOF-DBM-NEDA Joint Circular No. 1 series of 2013, and Executive Order Nos. 159 and 197, this Commission shall review the adopted fees annually from the date of its approval.

SECTION 8. **Separability Clause** – If any provision of this Circular be declared invalid or unconstitutional, other provisions hereof which are not affected thereby shall continue to be in full force and effect.

SECTION 9. **Effectivity** - This Circular shall take effect fifteen (15) days after its publication in a newspaper of general circulation.

Approved:

**SGD.**  
**ATTY. JOHN HENRY D. NAGA**  
Privacy Commissioner

**SGD.**  
**ATTY. LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

*On official leave*  
**ATTY. NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

# NPC Circular No. 2023-02

**DATE :** 26 September 2023

**SUBJECT :** Data Privacy Competency Program

**WHEREAS,** Republic Act No. 10173 or the Data Privacy Act (DPA) mandates the National Privacy Commission (NPC) to administer and implement the provisions of the law, and implement plans and policies that strengthen the protection of personal data formulate in the country;

**WHEREAS,** Section 9 of the Implementing Rules and Regulations of the DPA (IRR) provides that the NPC shall develop, promulgate, review, or amend rules and regulations for the effective implementation of the DPA;

**WHEREAS,** Section 9 of the IRR states that the NPC shall undertake the necessary or appropriate efforts to inform and educate the public on data privacy, data protection, and fair information rights and responsibilities;

**WHEREAS,** the NPC, through the NPC PHIL-DPO Program, initiated the DPO Accountability, Compliance, and Ethics (DPO ACE) training to capacitate Data Protection Officers with the knowledge and skills necessary to effectively manage the compliance of their respective organizations with the DPA;

**WHEREAS,** the NPC, through the PHIL-DPO Program, launched its Training the Trainers (T3) Program to grant provisional accreditation to Institutional Privacy Trainers (IPT) and Accredited Privacy Trainers (APT) to expand the breadth and scope of public education and training on data privacy throughout the Philippines;

**WHEREAS,** the DPO ACE training and T3 Program were mere ad hoc programs not covered by any formal issuances of the NPC and are being discontinued;

**WHEREAS,** there is a need to institutionalize the NPC's public education and training programs on data privacy through the issuance of a Circular;

**WHEREAS,** the NPC seeks to enhance the accessibility and quality of data privacy and protection trainings available in the Philippines in line with the recent developments in the application and interpretation of the DPA;

**WHEREAS,** the NPC shall develop a Data Privacy Competency Program (Program), which shall be composed of courses on the fundamental and operational aspects of the DPA essential for anyone who seeks to have a better understanding of the DPA and its application to actual situations, and other projects geared towards data privacy education;

**WHEREAS,** the Program shall neither result in a specialized accreditation or certification, such as those carried out by an independent third-party body, nor as a qualification to act or perform the functions of a data privacy professional;

**WHEREAS,** Executive Order No. 292, s. 1987, as amended, or the Administrative Code

of 1987 authorizes all agencies to charge fees as compensation for seminars or training programs rendered to other government agencies or private parties;

**WHEREAS**, the Republic Act No. 8293, as amended, or the Intellectual Property Code provides that while the work of a government agency or office is not protected by copyright, a government agency or office may require prior approval and impose as a condition the payment of royalties for use of such work for profit;

**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 prescribing the guidelines for the courses, including a Data Privacy Foundational Course, under the Program

**SECTION 1. *Scope and Purpose.*** Through the Program, the NPC shall develop uniform curricula and modules on the legal framework of privacy law and regulations (Curriculum) and learning outcomes to train and capacitate the public. The NPC shall license the use of a prescribed Curriculum to qualified Training Providers to enhance the quality of education on Philippine data privacy law. Qualified and licensed Training Providers shall design and conduct Training Courses based on the prescribed Curriculum covered by the specific License granted by the NPC.

This Circular shall apply to the Data Privacy Foundational Course, which shall cover fundamental concepts and principles of Philippine data privacy law, and other courses developed by the NPC under this Program.

**SECTION 2. *Definition of Terms.*** Terms used in the DPA and its IRR, as amended, are adopted herein. In addition, whenever used in this Circular, the following terms are defined as follows:

A. “Commission” refers to the Privacy Commissioner and the two (2) Deputy Privacy Commissioners;

B. “Curriculum” refers to the syllabus, modules, and other materials that the NPC develops to set a minimum standard for the conduct of courses under the Program;

C. “Enrollee” refers to a person who shall avail themselves of a Training Course offered by a licensed Training Provider;

D. “License” refers to the non-exclusive, non-assignable, and non-sublicensable authority granted by the NPC to a Training Provider to use a specific prescribed Curriculum under the Program;

E. “NPC” refers to the National Privacy Commission created under the DPA;

F. “Training Course” refers to the course designed by a Training Provider pursuant to a specific prescribed Curriculum under the Program;

G. “Training Provider” refers to any natural or juridical person that is qualified under this Circular and licensed by the NPC to conduct a Training Course to an Enrollee based on a specific prescribed Curriculum;

**SECTION 3. *Nature of the License.*** The NPC shall issue a License to a qualified Training

Provider to design a Training Course based on a specific prescribed Curriculum. In all cases, the License granted to a Training Provider shall be non-exclusive, non-assignable, and non-sublicensable. The NPC shall issue the License to a qualified Training Provider after the execution of a formal written agreement prescribing the terms and conditions on the matter (Agreement). S

**SECTION 4. *Term and Renewal of License.*** The License shall be valid for one (1) year and may be renewed within thirty (30) days prior to its expiration, subject to continuing compliance with Section 5 of this Circular and the terms of the Agreement stated in Section 3 of this Circular.

Upon termination of a License for any reason as may be provided in the Agreement or in any provision of law, a Training Provider is prohibited from conducting a Training Course, using the applicable prescribed Curriculum covered by the specific License granted by the NPC, and representing itself as licensed by the NPC, in any way, to provide courses on data privacy.

**SECTION 5. *General Qualifications of a Training Provider.*** A Training Provider must be duly organized, validly existing, and in good standing with the Department of Trade and Industry for sole proprietorships, or the Securities and Exchange Commission for partnerships and corporations. A Training Provider must have no pending civil, criminal, or administrative action, investigation, or suit nor conviction of any offense before any courts or other quasi-judicial agencies.

**SECTION 6. *Training Course.*** A Training Provider shall design a Training Course based on the applicable prescribed Curriculum covered by the specific License granted by the NPC. Before a Training Course is offered to the public, a Training Provider shall submit the Training Course materials to the NPC for approval. The NPC shall determine if the Training Course is consistent with the applicable prescribed Curriculum covered by the specific License and prescribed learning outcomes.

**SECTION 7. *Training Course Fee.*** A Training Provider may charge a fee when offering the Training Course. The fee, however, shall not exceed the maximum amount set out in the Agreement stated in Section 3 of this Circular. The maximum amount of the fee shall be subject to periodic adjustments by the NPC.

**SECTION 8. *Royalties.*** The NPC may collect royalties from a Training Provider who shall use the prescribed Curriculum under the Program. The amount of royalties, if any, and the use and management of the prescribed Curriculum for a specific course shall be set out in the respective terms of the Agreement stated in **Section 3** of this Circular.

**SECTION 9. *Examination.*** For specific Training Courses, the NPC may conduct an examination to determine the competency of an Enrollee who has completed that Training Course with a licensed Training Provider. The successful completion of the Training Course for which the examination is administered with a licensed Training Provider shall be a requisite to take the examination.

The NPC may collect a fee when administering an examination. A Training Provider shall not collect additional fees from an Enrollee to take an examination administered by the NPC.

**SECTION 10. *Completion; Effects.*** Completion of a Training Course or successful pass-



ing of an examination administered by the NPC shall only measure the competency proficiency of an Enrollee. It shall in no case be construed as a professional certification on Philippine data privacy law. In this regard, no certification is necessary for a person to act as or perform the functions of a data privacy professional, including a Data Protection Officer or Compliance Officer for Privacy. A Training Provider may issue a Certificate of Attendance, Completion, or its equivalent, to Enrollees who have successfully completed a Training Course.

**SECTION 11. *Monitoring and Reporting.*** The NPC shall, in the manner provided in the Agreement, periodically monitor and determine if a Training Course designed by the Training Provider is in line with the prescribed Curriculum covered by the specific License granted by the NPC.

**SECTION 12. *Consultative Body.*** The NPC may form a Consultative Body to assist in formulating the prescribed Curriculum and learning outcomes for a specific course, including the Data Privacy Foundational Course, under the Program.

A Consultative Body for a specific course shall be composed of five (5) member-volunteers from outside the NPC. The member-volunteers shall be appointed by the Commission for a term of two (2) years, based on a favorable endorsement by the Chairperson of the Program, who concurrently serves as a member of the Commission.

No person shall be appointed as a member of a Consultative Body, unless they are a citizen of the Philippines, of good moral character, of proven integrity and competence, and with at least five (5) years of experience in the field of data privacy or such other fields relevant to the specific course for which that particular Consultative Body was formed.

**SECTION 13. *Qualification under the DPO ACE Program.*** Any qualifications acquired under the DPO ACE training shall remain valid for a period of one (1) year from the effectivity of this Circular.

**SECTION 14. *Separability Clause.*** If any portion of this Circular is declared null and void, or unconstitutional, the other portions not affected thereby shall continue to be in force and effect.

**SECTION 15. *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 16. *Effectivity.*** This Circular shall take effect fifteen (15) days after its publication in the Official Gazette or a newspaper of general circulation.

Approved:

**SGD.**  
**ATTY. JOHN HENRY D. NAGA**  
Privacy Commissioner

**SGD.**  
**ATTY. LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

**SGD.**  
**ATTY. NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

# NPC Circular No. 2023-03

**DATE :** 07 November 2023

**SUBJECT :** GUIDELINES ON IDENTIFICATION CARDS

**WHEREAS**, personal information controllers (PICs) issue physical or digital identification cards (ID cards) to their respective data subjects for identity verification in relation to the provision of goods and services as well as the implementation of safeguards for electronic systems and physical premises, among others;

**WHEREAS**, the National Privacy Commission (NPC) recognizes that such processing activity may have a legitimate purpose and a lawful basis for processing under Sections 12 and 13 of the Data Privacy Act of 2012 (DPA);

**WHEREAS**, Section 11 of the DPA allows the processing of personal and sensitive personal information (collectively, personal data) subject to compliance with the requirements of the DPA and other laws allowing disclosure of information to the public, and adherence to the general principles of privacy;

**WHEREAS**, 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 that personal data shall be processed only if the purpose of the processing could not be reasonably fulfilled by other means;

**WHEREAS**, pursuant to Section 7 of the DPA, the NPC is charged with the administration and implementation of the provisions of the law, which includes ensuring the compliance by PICs with the provisions of the DPA, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal data in the country, in coordination with other government agencies and the private sector;

**WHEREAS**, Section 9 of the Implementing Rules and Regulations of the DPA (IRR) provides that the Commission shall, among its other functions, develop, promulgate, review or amend rules and regulations for the effective implementation of the law;

**WHEREFORE**, in consideration of the foregoing premises, the NPC hereby issues this Circular that prescribes the guidelines for PICs on the issuance of ID cards.

**SECTION 1. Scope.** — This Circular shall apply to all PICs that issue ID cards to their respective data subjects: provided, that ID cards issued by government agencies pursuant to their respective regulatory mandate, such as but not limited to, driver's license, passport, Professional ID card of a Registered Professional, including for this purpose the Integrated Bar of the Philippines (IBP) Lawyers ID, Tax Identification Number (TIN) card, shall be excluded from the scope of this Circular.

For purposes of this Circular, ID cards are understood to be any physical or digital ID<sup>1</sup>

<sup>1</sup> See: International Telecommunication Union, Recommendation ITU-T X.1251, A framework for user control of digital identity, "3.2.3 digital identity: The digital representation of the information known about a specific individual, group or organization", available at <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=9619> (last accessed 5 July 2023) and United Nations Conference on Trade and Development, Policy Brief No. 96, March 2022, Digital identity refers to the set

card that identifies a data subject. ID cards include, but are not limited to, company IDs, school IDs, insurance cards, membership cards, and rewards or loyalty cards.

**SECTION 2. *Definition of Terms.*** —Terms used herein shall have the respective meanings provided in the DPA, its IRR, as amended, and other issuances of the NPC.

**SECTION 3. *Contents of ID cards; proportionality.*** — All PICs issuing ID cards shall ensure that only the necessary personal data are indicated therein in relation to the primary purpose of identifying the data subject.

A. In the case of ID cards with additional functionalities, PICs shall ensure that all other personal data that will be included are reasonable and necessary for the specified and declared purposes of that specific ID card.

B. Nothing in this Circular shall be construed as prohibiting the inclusion of any personal data that is explicitly required by law or regulation to be indicated in an ID card issued by PICs.

C. PICs shall implement reasonable and appropriate safeguards to protect personal data on ID cards and shall ensure that such security features are at par with technological advances, best practices, and industry standards. PICs shall also educate data subjects on the appropriate physical security measures for ID cards already issued and in the possession of such data subjects.

D. In all cases, ID cards shall not contain information that is excessive. PICs shall bear the burden of demonstrating that the inclusion of a particular category of personal data is proportionate to the legitimate purpose.

**SECTION 4. *Penalties.*** — Subject to the provisions of Section 3 (A) above, the processing of personal data in violation of this Circular shall carry criminal, civil, and administrative liability pursuant to the provisions of the DPA and related issuances of the Commission.

**SECTION 5. *Interpretation.*** —Any doubt in the interpretation of any provision of this Circular shall be liberally interpreted in a manner mindful of the rights and interests of the data subjects.

**SECTION 6. *Transitory Provision.*** — PICs shall be given a period of one hundred twenty (120) calendar days from the effectivity of this Circular to comply with the requirements provided herein.

**SECTION 7. *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 8. *Repealing Clause.*** — All other rules, regulations, and issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified accordingly.

of electronically captured and stored attributes and credentials used to uniquely identify a person, which can include biographic data (e.g. name and date of birth), biometric data (e.g. fingerprints and facial features) and/or government-issued identification, available at: [https://unctad.org/system/files/official-document/presspb2022d4\\_en.pdf](https://unctad.org/system/files/official-document/presspb2022d4_en.pdf) (last accessed 5 July 2023).

**SECTION 9. Effectivity.** — This Circular shall take effect fifteen (15) calendar days after its publication in the Official Gazette or a newspaper of general circulation.

Approved:

**SGD.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**SGD.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

**SGD.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

# NPC Circular No. 2023-04

**DATE :** 07 November 2023

**SUBJECT :** GUIDELINES ON CONSENT

**WHEREAS**, Section 7 of the DPA provides that the National Privacy Commission (NPC) is charged with the administration and implementation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), which includes ensuring the compliance by personal information controllers (PIC) with the provisions of the Act, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal information, sensitive personal information, and privileged information (collectively, personal data), in the country in coordination with other government agencies and the private sector;

**WHEREAS**, under Section 9 of the Implementing Rules and Regulations of the DPA (IRR), the NPC is mandated to, among others, develop, promulgate, review, or amend rules and regulations for the effective implementation of the DPA;

**WHEREAS**, Sections 12 and 13 of the DPA enumerate the various criteria for lawful processing of personal data which includes the consent of the data subject;

**WHEREAS**, consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the processing of personal data about or relating to him or her, and evidenced by written, electronic, or recorded means. Consent may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so;

**WHEREAS**, consent is the most commonly used criterion for processing personal data and the NPC has determined the need to further elaborate on its concept and usage;

**WHEREFORE**, in view of the foregoing, the NPC hereby issues this Circular to provide guidelines on the use of consent as a lawful basis for processing personal data.

**SECTION 1. Scope and Purpose.** — This Circular shall apply to all personal information controllers (PICs) engaged in the processing of personal data based on the consent of the data subject.

This Circular shall provide guidance on what constitutes valid consent, and how it shall be obtained and managed in compliance with the DPA and its IRR.

This Circular is limited to the requirements of consent in relation to the processing of personal data. Nothing in this Circular shall be construed as modifying the existing general legal framework on obligations and contracts under the provisions of the Civil Code of the Philippines and other applicable laws and regulations.

**SECTION 2. Definition of Terms.** — Terms used in the DPA and its IRR, as amended, are adopted herein. In addition, whenever used in this Circular, the following terms are defined as follows:

A. “At set-up notice” refers to a privacy notice shown before a data subject installs a mobile application or a software;

B. “Consent fatigue” refers to a situation where consent questions are no longer read, as a result of multiple consent requests received by a data subject on a daily basis that require answers or decisions;<sup>1</sup>

C. “Context dependent notice” refers to a privacy notice activated by certain aspects of the data subject’s context, such as location or persons who will have access to the information or warnings about potentially unintended settings;

D. “Deceptive Design Patterns” refer to design techniques embedded on an analog or digital interface that aim to manipulate and deceive a data subject to perform a specific act relating to the processing of their personal data. This includes “Dark Patterns”;

E. “Just-in-time notice” refers to a privacy notice that provides information on how personal data will be processed at the point in time when the PIC is about to process such information;

F. “Layered Privacy Notice” refers to a short privacy notice that provides key privacy information and directs the data subject to more detailed information on the personal data required by the PIC, as well as the processing of such information, in accordance with Section 34(a)(2) of the IRR, as amended;

G. “Minimum specific information” refers to the least amount of information specific to a particular processing activity that must be disclosed to the data subject at the point where they are asked to give consent. This pertains to key information such as the identity of the PIC, its Data Protection Officer (DPO), and a brief description of how the information will be processed;<sup>2</sup>

H. “Research” refers to 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.<sup>3</sup>

## GENERAL DATA PRIVACY PRINCIPLES

**SECTION 3. Transparency.** — A PIC shall ensure that the data subject is aware of the nature, purpose, and extent of the processing of personal data. This includes the risks and safeguards involved, the identity of the PIC, the rights of the data subject, and how these rights can be exercised. Transparency empowers the data subject to make informed choices, and where applicable, to have reasonable control over the processing of their personal data, and to hold a PIC accountable based on the information provided at the time the data subject gave their consent.

<sup>1</sup> Article 29 Working Party, Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017. See also European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Adopted on 4 May 2020, available at: [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf) (last accessed on 2 February 2023).

<sup>2</sup> *Id.*

<sup>3</sup> 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).

A. *Specific information.* At the minimum, the following information should be provided in a concise statement: description of the personal data to be processed, the purpose, nature, extent, duration, and scope of processing for which consent is used as basis, the identity of the PIC, the existence of the rights of the data subject, and how these rights can be exercised.

B. *Timing.* Such concise information should be provided at the moment when consent is obtained (e.g., at set-up, just-in-time, context-dependent). Further information or additional details should be made available to the data subject by means of a Layered Privacy Notice (i.e., use of a link to the detailed information on the processing).

C. *Clarity.* A PIC shall use clear, plain, consistent, and straight-forward language when providing information to the data subject. A PIC must not use vague<sup>4</sup> or blanket wording, convoluted information, technical jargon, confusing terminologies, double negatives, and deliberately providing information in a circuitous manner. Providing the data subject with information that is difficult to understand, long-winded, or complex is inconsistent with informed consent.

D. *Form.* The following clarifications and distinctions are made on these forms or statements:

1. *Privacy Statement.* It is a general statement on a PIC’s personal data processing practices across the entire organization.

2. *Privacy Policy.* It is a set of policies that governs a PIC’s personal data processing practices. It provides guidance to internal relevant parties (e.g., officers, employees) involved in any personal data processing activity. It is also referred to as a “Privacy Manual.”

3. *Privacy Notice.* It is a unilateral statement that contains essential information on a specific processing activity of a PIC that involves the data subject.

a. A PIC should use clear and plain language in its privacy notice.<sup>5</sup> Information on how the personal data will be processed must be easily apparent to the data subject. The information should be provided in the simplest manner possible and avoid using complex sentences or language structures.<sup>6</sup>The use of layman’s terms is encouraged to ensure that the data subject understands the processing, but not at the risk of miscommunicating the technical and complex concepts.<sup>7</sup> In cases where consent is obtained manually, the notice may be presented in a comprehensive manner, taking into account the medium used for presentation (e.g., printed notices). For electronic processing of personal data where the surrounding circumstances and particular medium utilized may limit the manner in which a notice is presented, a link to a more comprehensive notice should be readily available.

b. The information provided in a privacy notice should be concrete and definite.

<sup>4</sup> JVA v. UXXX, NPC Case No. 19-498, 9 June 2020, *available* at: <https://www.privacy.gov.ph/wpcontent/uploads/2022/01/Decision-NPC-Case-No.-19-498-JVA-v.-UXXX.pdf> (last accessed: 2 February 2023).

<sup>5</sup> See JRG v. CXXX Lending Corporation, NPC Case No. 19-450, 9 June 2020, *available* at: [https://www.privacy.gov.ph/wp-content/uploads/2022/01/Decision\\_NPC-19-450-JRG-v.-CXXX.pdf](https://www.privacy.gov.ph/wp-content/uploads/2022/01/Decision_NPC-19-450-JRG-v.-CXXX.pdf) (last accessed: 2 February 2023).

<sup>6</sup> NPC Case No. 19-531, 21 May 2020, (NPC 2020) (Unreported).

<sup>7</sup> JRG v. CXXX Lending Corporation, NPC Case No. 19-450, 9 June 2020, *available* at: [https://www.privacy.gov.ph/wpcontent/uploads/2022/01/Decision\\_NPC-19-450-JRG-v.-CXXX.pdf](https://www.privacy.gov.ph/wpcontent/uploads/2022/01/Decision_NPC-19-450-JRG-v.-CXXX.pdf) (last accessed: 2 February 2023).



It should not be phrased in abstract or ambivalent terms, or leave room for different interpretations. Provisions that use vague, circuitous, or overbroad language do not conform with the principle of transparency. Thus, a PIC should examine if an average member of the target audience will understand the information in the privacy notice provided to them.

c. A PIC shall convey the appropriate privacy notice for the specific processing activity before the processing takes place or at the next practical opportunity. The information must be provided in a manner that is easy to access, taking into consideration user experience and user interface. This shall be done by posting a Layered Privacy Notice that embodies the minimum specific information for purposes of transparency. The privacy notice embodying the minimum specific information should direct the data subject to additional and detailed information relevant to the particular processing activity that will be done at that point in time;

d. A PIC may use creative options such as dynamic or interactive infographics, auditory notices through announcements or pre-recorded audios, or short videos. The information may also be delivered by a scripted spiel delivered on or before entry into the system. A PIC may also use any similarly creative options that can help the data subject easily understand the processing of their personal data.

4. *Consent Form.* It should contain all the information required in a privacy notice and indicate that consent is the lawful criteria for processing relied on. Consequently, it must contain a PIC's proposal to the data subject asking the latter to consent to the processing of personal data pursuant to the terms stated in the consent form. The data subject's acceptance of the provisions of the consent form creates a contract between the data subject and a PIC on the terms of processing of the personal data.

5. *When required.* The requirement of having a privacy statement and notice is separate and distinct from obtaining the consent of the data subject in an appropriate consent form or its equivalent for the lawful processing of personal data.

a. *General rule.* A privacy notice is required in any instance of processing, whether based on consent, other lawful criteria for processing under Sections 12 or 13 of the DPA, or where processing is under a special case pursuant to Section 4 of the DPA.

b. *Exception.* When a consent form already provides the essential information relating to the specific processing activity that enables the data subject to make an informed decision, a separate privacy notice on that specific processing is no longer necessary.

E. *Accessibility of information.* Information on the processing of personal data must be easy to access and understandable. The information must be readily available, and in a language or dialect that an average member of the target audience can understand.

F. *Accountability.* A PIC shall be held responsible for the information it provides to the data subject to obtain consent for the processing of personal data. Insufficiency of the information provided by a PIC to the data subject may render the consent given invalid.

**SECTION 4. Legitimate Purpose.** — Prior to the commencement of the processing activity, a PIC shall determine and declare the specific purpose of processing and shall ensure that such purpose is not contrary to law, morals, good customs, public order, or

public policy.

A. A PIC shall identify at the outset all the purposes for the processing of personal data which must not be contrary to law, morals, or public policy. In communicating these purposes to the data subject, a PIC commits that these specified and declared purposes define the bounds of the consent given.<sup>8</sup>

B. When a PIC revises its terms and conditions, retaking of consent is not necessary if the purpose, scope, method, and extent of processing remains to be

the same as that disclosed to the data subject at the time consent was given.

**SECTION 5. Proportionality.** — A PIC must ensure that the proposed processing of personal data is adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

A. As a general rule, personal data shall be processed only if the purpose of the processing could not be reasonably fulfilled by other less intrusive means.

B. A PIC may process additional personal data if the data subject validly consents to the additional processing prior to the collection of the personal data or as soon as practicable and reasonable.

1. Processing additional personal data for the purpose of availing goods or services or enhancing services is allowed when such additional personal data and act of processing is proportional to the additional purpose.

2. Consent for processing additional personal data for additional purposes must be embodied in the appropriate agreements that clearly indicate all the elements of valid consent.

C. When the processing is based on another lawful criteria, a PIC need not obtain the consent of the data subject for such processing: *provided*, that the requirements of such other lawful criteria are met under Section 12 or 13 of the DPA.

D. A PIC must limit the collection of personal data to what is directly relevant and necessary to accomplish a specified purpose. Thus, a PIC must only ask for consent to process personal data that is directly relevant and necessary for the specified and declared purpose.

**SECTION 6. Fairness.** – A PIC shall ensure that personal data is processed in a manner that is neither manipulative nor unduly oppressive to the data subject.

A. To determine fairness in processing of personal data based on consent, the following factors must be considered:

1. The purpose of the processing;
2. The amount of personal data collected;
3. The specific processing to be conducted on the personal data;

<sup>8</sup> JV v. JR, NPC Case No. 17-047, 13 August 2019, available at: <https://www.privacy.gov.ph/wpcontent/uploads/2020/10/CID-17-047-JV-v.-JR-Decision-PSD-10Aug2020.pdf> (last accessed on: 2 February 2023).

4. The manner by which the information on the processing is conveyed to the data subject;

5. The manner of collection of the personal data;
6. The free will of the data subject when providing consent;
7. The manner by which the data subject gives their consent; and
8. The retention period of the personal data processed.

B. The processing of personal data for purposes other than those for which the personal data were initially collected may be allowed.

1. Consent for processing of personal data for other purposes shall not be required when (i) the further processing is within the data subject's reasonable expectation on the purpose, scope, manner, and extent of the processing of personal data; and (ii) the purpose of further processing is compatible with the original purpose for which the personal data were initially collected and communicated to the data subject.

2. In assessing the compatibility of the purpose of the further processing with the original purpose, a clear and reasonable link between the further processing with the original purpose should be established. In addition, the impact of the further processing to the data subject should be considered.

C. Consent for processing for additional purposes is required when the purpose is incompatible with the original purpose for which the personal data were initially collected, or is beyond what a data subject may reasonably expect in relation to the purpose, scope, manner, and extent of the processing of personal data.

## ELEMENTS OF CONSENT

**SECTION 7. *Freely given.*** — A data subject must have a genuine choice and control over their decision to consent to the processing of their personal data.<sup>9</sup>

Consent is not freely given in instances where 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.

*A. Deceptive Design Patterns.* A PIC shall not use deceptive methods or any form of coercion, compulsion, threat, intimidation, or violence in obtaining the consent of the data subject. In accordance with Section 5(B) of this Circular, however, incentivizing consent by offering benefits to the data subject and similar actions of a PIC shall not be automatically construed as a deceptive method, coercion or compulsion that renders the consent as not freely given. The Commission may make such determination on a case-to-case basis.

*B. Public authorities.* Generally, public authorities process personal data based on the applicable provisions of Section 4 on special cases, and Sections 12 (c), (d), (e) and 13 (b), (c), (f) of the DPA which relate to the performance of their public functions, or the provision of public services based on law or regulation. Where the processing falls under the aforementioned bases, the consent of the data subject is not necessary.

1. Public authorities cannot undertake additional processing contemplated by law or

---

<sup>9</sup> MNL C, Inc. v. IKP, NPC Case No. 19-528, 29 October 2020, available at: [https://www.privacy.gov.ph/wpcontent/uploads/2022/01/Decision\\_NPC-19-528-MNL C-v.-PXXX-Corporation.pdf](https://www.privacy.gov.ph/wpcontent/uploads/2022/01/Decision_NPC-19-528-MNL C-v.-PXXX-Corporation.pdf) (last accessed: 2 February 2023).

regulation by obtaining consent if the primary basis for the processing of personal data is compliance with law or regulation.

2. The use of consent as a lawful basis for processing by public authorities is permissible under the DPA and may be appropriate when the processing activity is not related to, or an extension of any processing required by law or regulation. In such cases, the requisites for valid consent must be complied with.

C. *Contract of adhesion.* A contract of adhesion is a contract where one party imposes a ready-made form of contract on the other party.<sup>10</sup> A contract of adhesion is valid under the Philippine legal system. Thus, consent given to a contract of adhesion that contains provisions on the processing of personal data shall likewise be valid for such processing:<sup>11</sup> *provided*, that all of the following conditions are complied with:

1. The contract of adhesion must contain all the information necessary to demonstrate transparency;
2. The processing of personal data must be necessary and for a legitimate purpose;
3. The processing should not be excessive in relation to the fulfillment of obligations contemplated in the contract; and
4. The manner of the processing is fair and lawful.

**SECTION 8. *Specific.*** — A PIC must ensure that the data subject provides specific consent to the specific and declared purposes of the processing of personal data.

Consent must be granular. In cases where personal data is processed for multiple but unrelated purposes, a PIC shall present to the data subject the list of purposes and allow the data subject to select which purposes they consent to, instead of requiring an all-inclusive consent to the processing for multiple purposes.

A. If processing personal data is necessary to provide the goods or services sought to be availed of, a PIC must provide information about that specific processing and include such in the terms and conditions for the provision of the goods or service. Such information should form part of what the data subject consents to.<sup>12</sup>

B. Consent to processing that is not necessary for the provision of goods or services should not be bundled with or made a condition for the provision of the goods or the services. In cases where there is additional processing on the collected personal information for an additional purpose, a PIC must ensure that the consent for such processing is given by the data subject separately.

C. Vague or blanket consent is prohibited. Consent given based on vague or blanket statements is invalid consent.

**SECTION 9. *Informed.*** — A PIC should provide to the data subject all relevant informa-

<sup>10</sup> Dia v. St. Ferdinand Memorial Park, Inc., as cited in Cabanting v. BPI Family Savings Bank, Inc., G.R. No. 201927, 17 February 2016.

<sup>11</sup> VVC v. CJB, NPC Case No. 19-134, 10 Dec. 2021, *available* at: <https://www.privacy.gov.ph/wp-content/uploads/2022/04/NPC-19-134-VVC-v.-CJB-Decision-2021.12.10.pdf> (last accessed: 7 February 2023).

<sup>12</sup> In re: FLI Operating ABC Online Lending Application, NPC Case No. 19-910, 17 December 2020, *available* at: <https://www.privacy.gov.ph/wp-content/uploads/2021/02/NPC-19-910-In-re-FLI-Decision-LYA-Final-pseudonymized-17Dec2020-.pdf> (last accessed: 6 February 2023).

tion that is necessary for the data subject to make an informed decision.<sup>13</sup> Such information must be easily understood by an average member of the target audience to ensure that the data subject has sufficient understanding of what they are consenting to.<sup>14</sup>

A. *Appropriate information.* Prior to obtaining consent, a PIC shall ensure that it provides the appropriate information to the data subject, taking into account the most suitable language or dialect for the intended data subject, in accordance with Section 3(E) of this Circular. It shall explain such information in detail to the data subject if the same is unclear.

The information to be provided to the data subject shall be such information that is appropriate and relevant at that point in time, in relation to the personal data processing activity requiring consent.

B. *Consent fatigue.* If the data subject finds themselves overwhelmed by numerous and lengthy forms and notices, then there is a risk that the consent will be improperly given. Consent fatigue undermines the purpose of obtaining consent as it desensitizes the data subject and causes them to ignore the requisites for valid consent.

1. In order to avoid consent fatigue, a PIC must properly identify the lawful basis for processing prior to the collection of personal data. If the processing falls under.

2. A PIC shall minimize the risk of consent fatigue of its target data subjects.

C. *Just-in-time and Layered Notices.* The usage of just-in-time and layered notices in presenting the relevant information to the data subject shall be the default format.

**SECTION 10. An indication of will.** – Consent must be expressly given through a clear assenting action that signifies agreement to the specific purposes of the

processing of personal data as conveyed to the data subject at the time consent was given.<sup>15</sup>

A. *Implied consent.* Consent can never be assumed. Non-response or implied consent does not constitute valid consent. “Implied consent,” for the purposes of this Circular, refers to consent given by action or inaction which is only inferred from the surrounding circumstances when it was given.

B. *Action of the data subject.* Assenting actions are those that indicate agreement to processing activity as described in the information provided by the PIC. A PIC must provide clear information to the data subject on what a particular action means prior to requesting for the data subject’s consent.

C. *Continued use of service.* Provided that all the elements of consent are present, and the PIC provides the data subject with information on the processing of personal data for a specific service, the continued use of the PIC’s specific service is an assenting action signifying consent.

<sup>13</sup> AMP v. HXXX Lending Inc., NPC Case No. 19-621, 19 November 2020, available at: [https://www.privacy.gov.ph/wpcontent/uploads/2022/01/Decision\\_NPC-19-621-AMP-v.-HXXX-Lending.pdf](https://www.privacy.gov.ph/wpcontent/uploads/2022/01/Decision_NPC-19-621-AMP-v.-HXXX-Lending.pdf) (last accessed: 6 February 2023).

<sup>14</sup> JVA v. UXXX, NPC Case No 19-498, at 8.

<sup>15</sup> JVA v. UXXX, NPC Case No 19-498, at 8.

**SECTION 11. *Evidenced by written, electronic, or recorded means.*** — A PIC must ensure that the consent obtained from a data subject is evidenced by written, electronic, or recorded means. Any of the three formats may be adopted by a PIC. There is no preference among the different formats.

## OBTAINING CONSENT

**SECTION 12. *General Considerations.*** — A PIC shall obtain the consent of the data subject in a manner that complies with all the requisites for valid consent.<sup>16</sup> A PIC may also acquire consent from a data subject’s lawful representative, or an agent specifically authorized for that specific purpose.

A. A PIC must be able to demonstrate, with sufficient evidence, that the data subject has consented to the processing of personal data for the particular purpose. While there is a requirement to be able to demonstrate that the PIC has obtained consent, this should not in itself lead to additional or excessive personal data processing. A PIC should only keep enough data to show that consent was obtained in relation to a specific processing.<sup>17</sup>

B. Any evidence, in accordance with the Rules of Court, shall be sufficient, provided that the following are established:

1. The information on the processing of personal data presented to the data subject;
2. The PIC provided the data subject with the information on personal data processing at the time the consent was given; and
3. The data subject performed an act to signify their consent in relation to the information they were provided.

## WITHDRAWAL OF CONSENT

**SECTION 13. *General Considerations.*** — Consent can be withdrawn at any time and without cost to the data subject, subject to certain limitations as may be provided for by law, regulation, or contract. Should a data subject choose to exercise the right to withdraw consent to the processing and if there is no other lawful basis justifying the continued processing, a PIC is obliged to stop the processing without undue delay, terminate any processing activity including the provision of services relying on that consent, and delete the personal data.

A. A PIC shall ensure that withdrawing consent is as easy as, if not easier than, giving consent. A PIC is obliged to implement simple procedures to enable the data subject to exercise the right to erasure, including to suspend, withdraw or order the blocking, removal, or destruction, of personal data from the PIC’s repository. When the right to erasure is exercised, a PIC may employ manual or technical means for the effective management of the consent withdrawal across all its personal data processing systems.

B. A PIC shall avoid utilizing or switching to another interface for the sole purpose of

<sup>16</sup> *Id.*

<sup>17</sup> See: European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, Adopted on 4 May 2020, available at [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf) (last accessed 2 February 2023).

consent withdrawal since this would require undue effort from the data subject unless it will result in an easier manner to withdraw consent.<sup>18</sup> Where consent is obtained or recorded via electronic means through a mouse-click, swipe, or keystroke, the data subject should be able to withdraw the consent as easily as, if not easier than, it was given.<sup>19</sup> The use of a service-specific user interface for obtaining consent (e.g., application or a log-in account) should also be the one used for withdrawing consent.<sup>20</sup>

C. A PIC shall provide the data subject with adequate information on the scope and consequences of the withdrawal of consent at the beginning of the processing and at that point when the consent is to be withdrawn. This includes informing the data subject of any further processing of personal data, its purposes, and the corresponding lawful bases relied on for those other purposes.

D. Where consent is withdrawn by the data subject, the withdrawal shall not affect the lawfulness of the processing before the withdrawal of such consent.

E. A PIC shall determine and implement a reasonable retention period for personal data after the data subject withdraws consent, taking into account the other lawful bases for processing, industry best practices or standards, and other relevant factors.

## **GUIDELINES ON SPECIFIC PROCESSING ACTIVITIES**

**SECTION 14. *Direct Marketing.*** — Processing for direct marketing purposes may require consent in certain instances.

A. When processing is limited to personal information, a PIC may consider direct marketing as a legitimate interest under Section 12 (f) of the DPA and the processing will not require the consent of the data subject. The PIC must conduct an assessment whether direct marketing falls under its legitimate interest. If the result of the assessment reveals otherwise, the PIC may process personal information based on consent.

B. A PIC shall obtain the consent of the data subject for direct marketing in cases where the nature of the processing would significantly affect the rights and freedoms of the data subject.

C. If the basis for processing is consent and the consent is withdrawn, a PIC cannot claim legitimate interest to continue processing. The rights of the data subject to withdraw consent and to object to the processing, in this case, is absolute.

**SECTION 15. *Data sharing.*** Where data sharing is based on consent, a PIC shall ensure that the data subject is provided with specific information regarding the data sharing arrangement and that the data subject specifically and knowingly consents to such data sharing and the purpose of the data sharing arrangement.

A. Each affected data subject shall be provided with the relevant information before their personal data is shared or at the next practical opportunity, through a consent form or its equivalent, including the identities of the PICs who are parties to the data sharing arrangement, when already known. Otherwise, the categories of recipients should be

<sup>18</sup> *Ibid*

<sup>19</sup> See: European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Adopted on 4 May 2020.

<sup>20</sup> *Ibid*

provided at the outset: provided, that further details should be made available to the data subject through an appropriate privacy notice.

B. Where consent was obtained by one PIC who is a party to a data sharing arrangement, the other PIC may rely on such consent given: provided, that all parties to the sharing arrangement shall be accountable for upholding the exercise of the rights of the data subjects.

C. The records related to the data sharing arrangement shall contain the

proof of consent obtained from the data subject, including the date and time it was obtained or withdrawn, where applicable.

**SECTION 16. *Research.*** Processing of personal data for research purposes shall comply with the requirements of applicable laws, regulations, and ethical standards,<sup>21</sup>including but not limited to, obtaining an informed consent from the data subject, unless the processing may be justified by other lawful criteria provided under the DPA or as a special case under Section 4 of the DPA.

A. The DPA grants the processing of personal data for research purposes with flexibility, as the law recognizes that research is critical to nation-building and serves the interest of the public, especially if the same is conducted by government agencies, non-governmental organizations, academic institutions, or similar entities.

B. If obtaining consent before the gathering of information will affect the results of the research, a PIC should obtain the consent of the data subject within a reasonable time from the conclusion of the gathering of relevant information. The consent should be to validate the prior collection of information and for the further processing of the information collected.

C. The conduct of research does not always require obtaining of consent in the following instances:

1. Research conducted through observation of public behavior does not require consent unless the research will disclose the personal data of the observed research subjects.

2. The conduct of research where the end results will be anonymized and will only disclose the general demographic of the research subjects does not require the consent of the data subject.

D. Certain rights of the data subject may also be limited according to the standards prescribed by the PIC where such limitation is necessary to maintain research integrity.

**SECTION 17. *Publicly available information.*** The fact that the data subject provided

---

<sup>21</sup> See among others: (1) Philippine Health Research Ethics Board, National Ethical Guidelines for Research Involving Human Participants 2022, *available* at <https://ethics.healthresearch.ph/index.php/2012-04-19-05-10-10/451-the-advancecopy-of-the-2022-national-ethical-guidelines-for-research-involving-human-participants-is-now-available> and National Ethical Guidelines for Health and Health-Related Research 2017, *available* at <https://ethics.healthresearch.ph/index.php/references>; (2) DOST, DOH, CHED, and UP Manila, Joint Memorandum 2012-001 - Requirement for Ethical Review of Health Research Involving Human Participants, *available* at <https://ethics.healthresearch.ph/index.php/2012-0419-05-10-10/170-joint-memo-2012-001>.



personal data in a publicly accessible platform does not mean that blanket consent has been given for the use of their personal data for whatever

purposes. Any processing of publicly available information must still find basis under Sections 12 and 13 of the DPA.

**SECTION 18. *Profiling and automated processing.*** A PIC shall inform the data

subject of the existence and specific details of the profiling or automated processing of personal data before its entry into the processing system of the PIC, or at the next practical opportunity.

A. PICs engaged in any wholly or partly automated processing operations are required to notify the Commission, pursuant to the Circular on the notification regarding automated decision-making or profiling, and the data subject, in accordance with Section 16(c)(6) of the DPA;

B. A PIC shall ensure that there are safeguards against the harms of extensive profiling such as discriminatory outcomes and infringement on the right to fair treatment; and

C. A PIC shall obtain the consent of the data subject when automated processing is the sole basis for a decision that produces legal effects on or may significantly affect the data subject.

## MISCELLANEOUS PROVISIONS

**SECTION 19. *Consent as an essential element of contracts.*** — The processing of sensitive personal information through a contract between a PIC and a data subject is understood to be processing based on consent of the data subject under Section 13 (a) of the DPA as long as the contract entered into complies with the requirements for consent under the DPA.

**SECTION 20. *Waiver of the rights of the data subject.*** — A waiver by a data subject of his or her data privacy rights, including the right to file a complaint, is void.

**SECTION 21. *Period for validity of consent.*** — Generally, consent remains valid as long as the information communicated in relation to the scope, purpose, nature, and extent of the processing remains and still holds true.

A. If the scope, purpose, nature, and extent of the processing involved changes or evolves considerably, then the original consent given is no longer valid. A PIC shall obtain new consent in accordance with the revised or updated information on the processing of personal data.

B. A PIC shall determine whether it is still reasonable to treat the consent as an ongoing indication of the data subject's current choices based on the context in which consent was originally given and the nature of its relationship

with the data subject. However, consent that is clearly only intended to cover a certain period of time or a particular context will not be equivalent to an ongoing consent for all future processing of personal data.

C. The validity of consent shall depend on the PIC's compliance with the general data privacy principle of transparency for the processing. The sufficiency of the disclosures made by a PIC shall be examined based on what an average member of its target audience can understand, taking into consideration the language that was used.

D. Obtaining consent shall not be a one-time compliance on the part of a PIC. Consent should be an actively managed choice on the part of the data subject. A PIC must offer the data subject a mechanism to exercise ongoing preference and control over the consent given.

E. Where a data subject enters into a contract and subsequently cancels, terminates, or unsubscribes from it, the consent given to process personal data for that purpose shall also be terminated.

1. Processing of personal data may continue should there be another lawful basis for processing the personal data based on Section 12 and 13 of the DPA, except for direct marketing.

2. A PIC shall have the burden of determining and proving the appropriate lawful basis to continue such processing and inform the data subject of the lawful basis for continued processing.

**SECTION 22. 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 23. 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, its IRR, and related issuances of the Commission.

**SECTION 24. Transitory Provisions.** — All affected PICs shall be given a period of one hundred eighty (180) calendar days from the effectivity of these Guidelines to comply with the requirements provided in Sections 3(D), 9(C), and 13 of this Circular.

**SECTION 25. 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 26. Repealing Clause.** — All other rules, regulations, and issuances contrary to or inconsistent with the provisions of this Circular are deemed re

pealed or modified accordingly.

**SECTION 27. Effectivity.** — This Circular shall take effect fifteen (15) calendar days after its publication in the Official Gazette or a newspaper of general circulation.

**Approved:**

**SGD.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**SGD.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

**SGD.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

# NPC Circular No. 2023-05

**DATE : 25 October 2023**

**SUBJECT : Prerequisites for the Philippine Privacy Mark Certification Program**

**WHEREAS**, Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), provides that it is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications in nation-building and its inherent obligation to ensure that personal data in information and communications systems in the government and the private sector are secured and protected;

**WHEREAS**, pursuant to Section 7 of the DPA, the National Privacy Commission (NPC) is charged with the administration and implementation of the provisions of the law, which includes monitoring and ensuring compliance of the country with international standards set 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;

**WHEREAS**, the National Privacy Commission (NPC) is developing the Philippine Privacy Mark (PPM) Certification Program, a voluntary certification program, to assess public and private organizations that implement data privacy and protection management systems, to ensure the secure and protected processing of personal information;

**WHEREAS**, the PPM Certification Program shall evaluate the processing activities of organizations and the implementation of proper data protection measures and policies through a management system. It will enable organizations to reduce risks and demonstrate compliance with the DPA, its IRR and other Commission's issuances, and data subjects to identify organizations they can trust with their personal data;

**WHEREAS**, organizations and Certification Bodies who wish to voluntarily participate in the PPM Certification Program shall comply with the pre-requisites for certification or accreditation;

**WHEREFORE**, in consideration of these premises, the NPC hereby issues this Circular governing the pre-requisites for both organizations and Certification Bodies (CBs) who will participate in the PPM Certification Program.

**SECTION 1. Scope.** This Circular shall apply to all personal information controllers (PICs) or personal information processors (PIPs) that will seek certification under the PPM Certification Program, and to all Certification Bodies (CBs) that will seek accreditation under the PPM Certification Program.

**SECTION 2. Purpose.** This Circular provides the prerequisites for certification of PICs or PIPs and accreditation of CBs under the PPM Certification Program.

**SECTION 3. Definition of Terms.** The definition of terms in the DPA and its IRR, as

amended, are adopted herein. In addition, whenever used in this Circular, the following terms are defined as follows:

- A. “Accreditation” refers to a third-party attestation related to a conformity assessment body conveying a formal demonstration of its competence to carry out specific conformity assessment tasks.
- B. “Certification” refers to a third-party attestation related to an object of conformity assessment (e.g., product, process, service, system, installation, project, data, design, material, claim, person, body, or organization) with the exception of accreditation.
- C. “Certification Body (CB)” refers to a third-party conformity assessment body;
- D. “International Electrotechnical Commission (IEC)” refers to an organization that prepares and publishes international standards for all electrical, electronic and related technologies;
- E. “International Organization for Standardization (ISO)” refers to an independent, nongovernmental international organization with a membership of one hundred sixtyseven (167) national standards bodies that share knowledge and develop voluntary, consensus-based, and market relevant international standards that support innovation and provide solutions to global challenges;

**SECTION 4. Requirements for PIC or PIP.** Prior to applying for certification under the PPM Certification Program, a PIC or PIP must be certified with the following standards:

- I. ISO/IEC 27001 - information security management system (ISMS): specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization; and
- II. ISO/IEC 27701 – privacy information management system (PIMS): specifies the requirements and guides for establishing, implementing, maintaining, and continually improving a PIMS in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 (which provides a reference set of generic information security controls including implementation guidance) for privacy management within the context of the organization.

**SECTION 5. Requirements for CB.** Prior to applying for accreditation under the PPM Certification Program, a CB must be certified with the following standards:

- I. ISO/IEC 27001 - information security management system (ISMS): specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization;
- II. ISO/IEC 27701 – privacy information management system (PIMS): specifies the requirements and guides for establishing, implementing, maintaining, and continually improving a PIMS in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 (which provides a reference set of generic information security controls

including implementation guidance) for privacy management within the context of the organization; and

III. ISO/IEC 17021-1: Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements.

A CB shall complete the following accreditation stages:

I. Stage 1: Obtained a foreign or local accreditation to conduct audit or conformity assessment based on the ISO/IEC 27001 standard;

II. Stage 2: Obtained a foreign or local accreditation to conduct audit or conformity assessment based on the ISO/IEC 27701 standard; and

III. Stage 3: Obtained accreditation to conduct audit or conformity assessment against the PPM Certification Program based on the ISO/IEC 17021-1 standard.

**SECTION 6. *Failure to Comply.*** PICs, PIPs, or CBs that fail to comply with the pre-requisites for certification or accreditation stated in this Circular shall not be qualified to apply for certification and accreditation under the PPM Certification Program, respectively.

#### **ADDITIONAL MISCELLANEOUS PROVISIONS**

**SECTION 7. *Amendments.*** These Rules shall be subject to regular review by the Commission. Any amendment thereto shall be subject to the necessary consultations with the concerned stakeholders.

**SECTION 8. *Separability Clause.*** If any portion or provision of these Rules is declared null and void or unconstitutional, then the other provisions not affected thereby shall continue to be in force and effect.

**SECTION 9. *Effectivity.*** These Rules shall take effect immediately after publication in one newspaper of general circulation.

Approved:

**SGD.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**SGD.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

**SGD.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

# NPC Circular No. 2023-06

**DATE : 01 December 2023**

**SUBJECT : Security of Personal Data in the Government and the Private Sector**

**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 the 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 the private sector are secured and protected;

**WHEREAS**, pursuant to Section 7 of the DPA, the National Privacy Commission (NPC) is charged with the administration and implementation of the provisions of the law, which includes ensuring the compliance of personal information controllers (PICs) with the provisions of the Act and with international standards for data protection, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal data in the country, in coordination with other government agencies and the private sector;

**WHEREAS**, Rule III, Section 9 of the Implementing Rules and Regulations of the Data Privacy Act of 2012 (IRR) provides that the NPC’s functions, among others, are to develop, promulgate, review or amend rules and regulations for the effective implementation of the DPA;

**WHEREAS**, pursuant to Section 20 of the DPA, the PIC must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal data;

**WHEREAS**, under Section 22 of the DPA, the head of each government agency or instrumentality is responsible for complying with the security requirements mentioned in the law. This includes ensuring all sensitive personal information maintained by his or her agency is 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 NPC;

**WHEREAS**, under Section 23 of the DPA, the NPC may issue guidelines relating to access by agency personnel to sensitive personal information;

**WHEREFORE**, the abovementioned premises considered, the NPC hereby issues this Circular governing the security of personal data.

## **RULE I.**

### **GENERAL PROVISIONS**

**SECTION 1. Scope.** - This Circular shall apply to all natural or juridical persons engaged in the processing of personal data within and outside of the Philippines, subject to the applicable provisions of the DPA, its IRR, and other relevant issuances of the NPC.

**SECTION 2. Purpose.** - This Circular aims to provide updated requirements for the security of personal data processed by a PIC or Personal Information Processor (PIP). Due to the general nature of this Circular, a PIC or PIP may implement more detailed or stricter policies

and procedures that reflect industry-specific operating requirements.

**SECTION 3. Definition of Terms.** – Terms used in the DPA and its IRR, as amended, are adopted herein. In addition, whenever used in this Circular, the following terms are defined as follows:

- A. “*Acceptable Use Policy*” refers to a document or set of rules stipulating controls or restrictions that personnel of a PIC or PIP must agree to for access to the network, facilities, equipment, or services of such PIC or PIP;
- B. “*Access Control Policy*” refers to a document or set of rules that defines how access to information is managed, including who may access specific information and under what circumstances;
- C. “*Automated Processing*” generally refers to the use of automated means, such as algorithms or computer systems, in carrying out processing activities without human intervention;
- D. “*Business Continuity*” refers to the capability of a PIC or PIP to continue the delivery of products or services at acceptable pre-defined levels following disruptive events;
- E. “*Business Continuity Plan*” refers to documented procedures that guide a PIC or PIP to respond, recover, resume, and restore systems and processes to a pre-defined level of operation following disruptive events;
- F. “*Control Framework*” refers to a set of security measures that is a comprehensive enumeration of the controls intended to address the risks, including organizational, physical, and technical measures to maintain the availability, integrity, and confidentiality of personal data and to protect it against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, or contamination;
- G. “*Data Center*” refers to a centralized repository for the storage, management, and dissemination of data including personal data. This may be physical or virtual, analog or digital, or owned and controlled by the PIC or not;
- H. “*Disruptive Events*” refer to any anticipated or unanticipated occurrence or change which interrupts planned activities, operations, or functions;
- I. “*Encryption*” refers to the reversible transformation of data by a cryptographic algorithm to produce ciphertext in order to hide the information content of the data;
- 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, and state colleges and universities;
- K. “*National Computer Emergency Response Team (NCERT)*” refers to the highest body for cybersecurity-related activities;
- L. “*Off-The-Shelf Software*” refers to a software product that is ready-made and commercially available for sale, lease, or license to the general public;
- M. “*Password Policy*” refers to a document or set of rules that passwords must satisfy to increase the security and privacy of electronic devices;
- N. “*Privacy Engineering*” refers to the integration of privacy concerns into engineering practices for systems and software engineering life cycle processes;
- O. “*Privacy-by-Design*” refers to an approach to the development and implementation of projects, programs, and processes that integrate into the design or structure safeguards that are necessary to protect and promote privacy unto the design or structure of a processing activity or a data processing system;
- P. “*Privacy-by-Default*” refers to the principle according to which the PIC/PIP ensures that only data necessary for each specific purpose of processing is processed by default, without the intervention of the data subject;
- Q. “*Privacy Management Program (PMP)*” refers to a holistic program towards privacy and data protection and is important for a PIC or PIP involved in the processing of



personal data. It is intended to embed privacy and data protection in the strategic framework and daily operations of a PIC or its PIP;

- R. “*Security Clearance*” refers to the permission granted to an individual to access information based on the given level of access;
- S. “*System Management Tool*” refers to a software system that facilitates the administration of user passwords and access rights;
- T. “*Telecommuting*” refers to work from an alternative workplace with the use of telecommunications or computer technologies.

**SECTION 4. *General Obligations.*** – A PIC and its PIP shall fulfill the following responsibilities:

- A. Designate and register its Data Protection Officer (DPO) with the NPC, taking into account the provisions of the DPA, its IRR, its amendments, and any other issuances of the NPC on the designation and registration of a DPO;
- B. Register its data processing systems with the NPC according to the provisions of the DPA, its IRR, its amendments, and any other issuances of the NPC on the registration of data processing systems;
- C. Create an inventory of all its data processing systems and activities taking into account Section 26 (c) and (e) of the IRR;
- D. Conduct a Privacy Impact Assessment (PIA) on the processing of personal data: Provided, that such assessment shall be updated as necessary (e.g., new features or major changes in processing, new regulations, new contracts entered by the PIC, or changes in its PIP). Both previously assessed controls and those newly identified through recent PIAs shall be monitored, evaluated, updated, and incorporated as a component of a PIC’s Privacy Management Program;
- E. Set a Privacy Management Program, taking into account the following:
  - 1. Organizational commitment and leadership responsibilities for data privacy;
  - 2. Control framework for the development of privacy policies and implementation of data protection measures; and
  - 3. Oversight and continuous improvement of controls.
- F. Periodically train employees, agents, personnel, or representatives on privacy and data protection policies;
- G. Comply with the NPC’s orders when the PIC and its PIP’s privacy and data protection policies are subject to review and assessment in terms of compliance with the requirements of the DPA, its IRR, and all relevant issuances of the NPC.

**SECTION 5. *Privacy Impact Assessment (PIA).*** - A PIA should be undertaken for every processing system of a PIC or PIP that involves personal data.

The PIA shall include the following:

- A. a data inventory identifying:
  - 1. the amount and type of personal data held by the PIC and its PIP, if any, including records of its own personnel;
  - 2. list of all information repositories holding personal data, including location;
  - 3. type of media used for storing the personal data;
  - 4. risks associated with the processing of personal data; and
  - 5. processing operations for the entire personal data life cycle, from collection to disposal or destruction;
- B. a systematic description of the personal data being processed or to be processed, including the purposes for such processing, anticipated purposes, and their corresponding lawful bases;
- C. an assessment of the general data privacy principles in relation to the processing;
- D. a holistic assessment of the risks to the rights and freedoms of a data subject; and

- E. an assessment of risks to the confidentiality, integrity, and availability of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.

The PIA need not be submitted to the NPC, but it shall be made available by the PIC upon the NPC's request arising from investigations or compliance checks.

**SECTION 6. Control Framework for Data Protection.** - The risks identified in the PIA must be addressed by a Control Framework.

The contents of a Control Framework shall take into account, among others, the following:

- A. Nature of the personal data to be protected;
- B. Risks represented by the processing, the size of the organization, and the volume of personal data being processed;
- C. Current data privacy best practices in a specific industry;
- D. Cost of security implementation; and
- E. Purpose and extent of data sharing or outsourcing agreements and their attendant risks.

## **RULE II. EMBEDDING PRIVACY-BY-DESIGN AND PRIVACY-BY-DEFAULT**

**SECTION 7. Privacy-By-Design and Privacy-By-Default.** - A PIC or PIP shall consider Privacy-By-Design principles in its processing activities and enable Privacy-By-Default in its data processing systems without requiring any action from its data subjects.

Further, a PIC or PIP must also conduct a PIA on its Off-The-Shelf Software, solutions, or data processing systems, as outlined in Section 5 of this Circular.

Any functions that lack a lawful basis for processing or are incompatible with the general data privacy principles, must be switched off or deactivated.

**SECTION 8. Privacy Engineering.** - A PIC or PIP should incorporate data privacy requirements throughout the development and implementation of data processing systems.

## **RULE III. STORAGE OF PERSONAL DATA**

**SECTION 9. General Rule.** - A PIC or PIP must store personal information in a form that permits the identification of data subjects for only as long as necessary for the specific purpose for which it was initially processed.

In order to ensure that personal data is not kept longer than necessary, the PIC should establish and document retention periods in a policy. This Retention Policy, which defines retention periods, must be reviewed periodically and amended as necessary. The PIC should inform data subjects about the Retention Policy, including its changes.

**SECTION 10. Service Provider as Personal Information Processor.** - When a PIC engages a service provider for the purpose of storing personal data under the PIC's control or custody, the service provider acts as a PIP. It is the responsibility of the PIC to ensure that its PIP has implemented appropriate security measures for the protection of personal data and is able to demonstrate compliance with all the requirements of the DPA, its IRR, and all applicable

issuances of the NPC.

**SECTION 11. *Protection of Personal Data.*** - All personal data that are processed must be adequately protected through industry standards and best practices.

Passwords or passphrases used to access personal data should be of sufficient strength and uniqueness to deter password attacks. Each PIC or PIP shall issue and enforce a Password Policy.

#### **RULE IV.**

#### **ACCESS TO PERSONAL DATA**

**SECTION 12. *Access to or Modification of Databases.*** - Personal data stored in databases under the control of the PIC may only be accessed or modified using authorized software programs either by the PIC or by its PIP. Authorized software programs are those that are either licensed or owned by the PIC or PIP. Such restriction is necessary to protect the confidentiality, integrity, and availability of personal data.

**SECTION 13. *Restricted Access.*** - A PIC or PIP shall implement an Access Control Policy to ensure that only authorized personnel can access personal data on a “need to know” basis. Further, a PIC or PIP shall provide other mechanisms, such as authentication methods and regular monitoring, to limit access to only authorized personnel.

A PIC must ensure that access to personal data is strictly regulated by issuing a security clearance or its equivalent only to its authorized personnel. Any processing performed by a PIP must be covered by the appropriate and necessary agreement that contains an equivalent of this provision as well as other provisions required under the IRR.

A copy of the appropriate security clearance or its equivalent must be filed with the DPO of the PIC.

**SECTION 14. *PIP Access.*** - Access to personal data by a PIP engaged by a PIC shall be governed by strict procedures contained in formal contracts or other legal acts, and the provisions of such must comply with the DPA, its IRR, and all applicable issuances by the NPC. The contractual terms and undertakings stated may be considered by the NPC when evaluating the security measures implemented by the PIC.

**SECTION 15. *Acceptable Use Policy.*** - A PIC or PIP shall have an updated Acceptable Use Policy regarding the use by PIC or PIP’s personnel of information and communications technology. The PIC or PIP shall explain the policy to all personnel who use such technology in relation to their functions. Each user shall agree to the policy and, for this purpose, sign the appropriate agreement before being allowed access to and use of the technology.

**SECTION 16. *Online Access to Personal Data.*** - A PIC or PIP shall implement secure authentication mechanisms, such as multifactor authentication or secure encrypted links, when providing personnel online access to sensitive personal information, privileged information, and a high volume of personal data. Such user access rights and authentication mechanisms must be defined and controlled by a System Management Tool.

**SECTION 17. *Authorized Devices.*** - A PIC or PIP shall ensure that only known devices, properly configured to the PIC’s or PIP’s security standards, are authorized to access personal data. The PIC or PIP shall also establish solutions that only allow authorized media to be used on its computer equipment. These measures include but are not limited to the following:

1. Setting a group policy to allow certain types of devices to be connected<sup>1</sup>;
2. Use of endpoint security solutions;<sup>2</sup> and
3. Restricting access to USB ports.<sup>3</sup>

**SECTION 18. *Remote Disconnection or Deletion.*** A PIC shall employ technology solutions that enable remote disconnection or data deletion on mobile devices owned by the PIC when they are lost or compromised. In addition, PICs shall establish a notification process in cases of mobile device loss to ensure swift and appropriate actions toward safeguarding personal data contained therein.

**SECTION 19. *Physical Filing System.*** - If personal data is stored in any physical media, such as a paper-based filing system, a PIC or PIP shall maintain a log, from which it can be ascertained which file was accessed, including when, where, and by whom. Such log shall also indicate whether copies of the file were made. The PIC or PIP shall regularly review the log records, including all applicable procedures.

**SECTION 20. *Personal Data Sharing Agreements.*** - Access by other parties to personal data under the control or custody of a PIC shall be governed by the DPA, its IRR, and the NPC's relevant issuances on Data Sharing Agreements.

## RULE V.

### BUSINESS CONTINUITY

**SECTION 21. *Business Continuity Management.*** - A PIC or PIP must have a Business Continuity Plan to mitigate potential disruptive events. It must consider the following:

- i. Personal data backup, restoration, and remedial time;
- ii. Periodic review and testing of the business continuity plan which takes into account disaster recovery, privacy, business impact assessment, crisis communications plan, and telecommuting policy, among others; and
- iii. Contact information and other business-critical matters, e.g., electrical supply, building facilities, Information and Communications Technology (ICT) assets.

**SECTION 22. *Telecommuting.*** - The adoption of telecommuting or other alternative work arrangements is a viable strategy to continuously operate and provide essential goods and services. With this, a PIC or PIP shall set, in accordance with applicable laws, rules and regulations, its policy on alternative work arrangements, and communicate it to concerned stakeholders. Security measures in alternative work arrangements shall be considered by the PIC or PIP. These measures include:

- i. Training on the limitations on use of company-issued computing devices with secure configuration of the PIC's Information and Communications Technology (ICT) assets to protect against security risks and cyberthreats such as unauthorized access, malware, data loss, and theft;
- ii. Best password management and secured practices in managing online accounts, computers, mobile phones, and network appliances; and
- iii. Periodic trainings on data privacy, cybersecurity, and online productivity, among others.

<sup>1</sup> vinaypamnani-msft, "Manage Device Installation with Group Policy - Windows Client Management," August 10, 2023, <https://learn.microsoft.com/en-us/windows/client-management/client-tools/manage-device-installation-with-group-policy>.

<sup>2</sup> USB Security Software - USB Port Blocker & Analyzer | SolarWinds," accessed October 24, 2023, <https://www.solarwinds.com/security-event-manager/use-cases/usb-security-analyzer>.

<sup>3</sup> Azharuddin@TWC, "How to Enable or Disable USB Ports in Windows 11/10," The Windows Club, June 28, 2021, <https://www.thewindowsclub.com/disable-enable-usb-windowunlock-pen-drive-at-office-or-school-computer>.

## RULE VI.

### TRANSFER OF PERSONAL DATA

**SECTION 23. *Emails.*** - A PIC or PIP that transfers personal data by email must ensure that the data is adequately protected and use secure transmission and reception of email messages, including attachments. Where appropriate, a PIC or PIP may utilize systems that scan outgoing emails and attachments for keywords that would indicate the presence of personal data and, if applicable, prevent its transmission. **SECTION 24. *Personal Productivity Software.*** - A PIC or PIP that do not have any security or access controls when using personal productivity software, shall, when reasonable and appropriate, implement security controls to prevent its personnel from printing or copying personal data to personal productivity software such as word processors and spreadsheets.

**SECTION 25. *Removable or Portable Storage Media.*** - The use of removable or portable storage media, such as compact discs (CD), digital versatile discs (DVD), and Universal Serial Bus (USB) flash drives for processing personal data, shall be regulated: Provided, that if such mode of transfer is unavoidable or necessary, the files inside the removable or portable storage media shall be encrypted.

**SECTION 26. *Fax Machines.*** - Facsimile technology shall not be used for transmitting documents containing personal data.

**SECTION 27. *Transmittal.*** - A PIC and its PIP that transmit documents or media containing personal data by mail or post shall make use of registered mail or, where appropriate, guaranteed parcel post services and Private Express and/or Messengerial Delivery Service (PEMEDES). It shall establish procedures that ensure that such documents or media are delivered only to the person to whom they are addressed, or the authorized representative of the addressee: Provided, that similar safeguards shall be adopted relative to documents or media transmitted between offices or personnel of the PIC and its PIP.

## RULE VII.

### GUIDELINES FOR DISPOSAL OF PERSONAL DATA

**SECTION 28. *Disposal and Destruction of Personal Data.*** - In establishing policies and procedures for disposal of personal data, a PIC or PIP shall take into consideration the following:

1. Retention period of data;
2. Jurisdiction-specific laws, regulations, and existing contracts;
3. Identification of relevant de-identification, anonymization, or deletion techniques for specific types of data; and
4. Required documentation before the deletion, de-identification, or anonymization of personal information.

**SECTION 29. *Logs Retention.*** - A PIC or a PIP shall retain logs as long as deemed necessary and appropriate based on best practices and industry standards. In determining the appropriate retention period, the PIC shall consider the type of log and its corresponding use. Security logs that record information about authentication attempts and security incidents shall be retained for longer periods than general system logs:

- A. In the event of a security incident or data breach, logs may need to be retained for a longer period to support investigations and digital forensic analysis. PICs shall retain logs related to incidents for a specified period required by the NPC, even if it exceeds their retention policies; and
- B. PICs shall implement backup and archive mechanisms for their logs. Backup copies may be retained for shorter periods, while archived copies can be stored for a longer duration.

**SECTION 30. *Procedures for Disposal and Destruction.*** - Procedures must be established to ensure secure and proper disposal and destruction of personal data that would render further processing impossible. These include:

- 1. Disposing and destroying personal data, regardless of how such files are stored;
- 2. Electronically disposing or destroying personal data in storage media which involve the use of degaussers, erasers, encryption, or secure wiping programs as applicable;
- 3. Physically disposing or destroying storage media used to store personal data such as disk servers, hard or solid-state drives, portable storage drives, such as disks, flash drives and memory cards, read-only memory storage in mobile phones when they reach the end-of-life;
- 4. Disposing and destroying personal data in paper documents which involve the use of paper shredders that would render shredded paper documents into small pieces that cannot be reassembled; and
- 5. Disposing personal data stored offsite.

SECTION 31. Personal Data Disposal Service Provider. - A PIC may engage a PIP to carry out the disposal of personal data under its control: Provided, that the PIP shall contractually agree to the PIC's data protection procedures and ensure that the confidentiality of all personal data is preserved.

## RULE VIII.

### MISCELLANEOUS PROVISIONS

**SECTION 32. *Threat monitoring and vulnerability management.*** - A PIC or a PIP shall continuously adapt security measures to dynamically respond to the evolving security threat landscape. This includes identifying threats based on authoritative sources of threat information (e.g., NCERT), integrating relevant threats into the PIA to determine if these lead to new unacceptable security or privacy risks, and proposing corrective actions to such threats.

**SECTION 33. *Personal Data Breach Management.*** - In case of a data breach or security incident, a PIC shall comply with the requirements of the NPC's issuance on breach management.

**SECTION 34. *Audit.*** - In certain cases, independent verification or certification by a reputable third party of a PIC or, where applicable, its PIP, may be accepted by the NPC: Provided, that the findings of an independent verification or certification by a third-party does not preclude the NPC from performing its regulatory functions pursuant to the relevant issuances of the NPC.

**SECTION 35. *Penalties.*** - A PIC or PIP that violates the provisions of this Circular, shall, upon notice and hearing, be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent ban on the processing of personal data, or payment of fines, in accordance with the DPA, its IRR, and the NPC's issuances.

Failure to comply with the provisions of this Circular can result in criminal, civil, administrative liabilities, and disciplinary sanctions against any erring officer or employee in accordance with existing laws or regulations.

The commencement of any action under this Circular is independent and without prejudice to the filing of any action with the regular courts or other quasi-judicial bodies.

**SECTION 36. *Review.*** - This Circular shall be subject to regular review by the NPC.

**SECTION 37. *Transitory Period.*** - A PIC shall be given a transitory period of twelve (12) months from the effectivity of this Circular to comply with the requirements provided herein.

**SECTION 38. *Separability Clause.*** - If any portion or provision of this Circular is declared null and void or unconstitutional, then the other provisions not affected thereby shall continue to be in force and effect.

**SECTION 39. *Repealing Clause.*** - This Circular expressly repeals NPC Circular No. 16-01. The provisions of the IRR and all other issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified.

**SECTION 40. *Effectivity.*** - These Rules shall take effect fifteen (15) days after its publication in a newspaper of general circulation.

Approved:

**SGD.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**SGD.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

**SGD.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

# NPC Circular No. 2023-07

**DATE :** 13 DECEMBER 2023

**SUBJECT :** GUIDELINES ON LEGITIMATE INTEREST

**WHEREAS**, Section 7 of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) provides that the National Privacy Commission (NPC) is charged with the administration and implementation of the DPA, which includes ensuring the compliance of personal information controllers (PICs), 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**, under Section 9 of the Implementing Rules and Regulations of the DPA (IRR), the NPC is mandated to develop, promulgate, review, or amend rules and regulations for the effective implementation of the DPA;

**WHEREAS**, Section 12(f) of the DPA provides that personal information may be processed based on a legitimate interest pursued by the PIC or by a third party to whom the data is disclosed;

**WHEREAS**, there is a need to clarify how a PIC may establish the existence of legitimate interest, the necessity of personal information processing for such interest, and the assessment of such interest in relation to a data subject's fundamental rights and freedoms;

**WHEREFORE**, in view of the foregoing, the NPC hereby issues this Circular to provide guidelines on legitimate interest as a lawful basis for processing personal information.

**SECTION 1. *Scope and Purpose.*** — This Circular applies to all PICs and third parties engaged in the processing of personal information based on legitimate interest under Section 12(f) of the DPA. This Circular provides guidelines for PICs and third parties relying on legitimate interest as a lawful basis to process personal information for a specific processing activity.

**SECTION 2. *Definition of Terms.*** — The definition of terms in the DPA and its IRR, as amended, as well as in existing NPC issuances, are adopted herein.

**SECTION 3. *General Considerations.*** — Section 12(f) of the DPA permits the processing of personal information when the processing is necessary for the legitimate interests pursued by the PIC or a third party to whom the personal information is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject that require protection under the Philippine Constitution.

A. Legitimate interest refers to any actual and real interest, benefit, or gain that a PIC or third party may have in or may derive from the processing of specific personal information.

B. Processing based on a legitimate interest may only be relied on for the processing



of personal information. It cannot be relied upon when the processing involves sensitive personal information and privileged information.

C. The third party in Section 12(f) of the DPA refers to any natural or juridical person to whom personal information is disclosed and who is not the PIC, the personal information processor (PIP), or the data subject of the specific processing activity.

D. The fundamental rights and freedoms of data subjects protected under the Philippine Constitution and the effect and impact of the specific processing activity on such rights and freedoms shall be assessed and weighed against the legitimate interest of the PIC or third party through a legitimate interest assessment.

## **PROCESSING BASED ON LEGITIMATE INTEREST**

**SECTION 4. *Requisites for Processing Based on Legitimate Interest; Legitimate Interest Assessment.*** — Processing based on legitimate interest requires the fulfillment of the following conditions:

- A. The legitimate interest is established;
- B. The means to fulfill the legitimate interest is both necessary and lawful;  
and

C. The interest is legitimate and lawful, and it does not override fundamental rights and freedoms of data subjects. There is no prescribed form for a legitimate interest assessment. The PIC or third party is not precluded from using any existing method, structure, or form, provided that the PIC or third party applies the requisites for processing based on legitimate interest in its assessment.

**SECTION 5. *The Legitimate Interest is Established (Purpose Test).*** — A PIC shall determine the existence of a clearly established legitimate interest, including a determination of the objective of the specific processing activity.

A. The purpose of the specific processing activity must be specific, such that it is clearly defined and not vague or overbroad;

B. The purpose of the specific processing activity must not be contrary to laws, morals, or public policy following the principle of legitimate purpose; and

C. The interest established must be declared to the data subject prior to the processing or at the next practical opportunity, following the principle of transparency and the right of the data subject to be informed.

**SECTION 6. *The Means to Fulfill the Legitimate Interest is both Necessary and Lawful (Necessity Test).*** — The means or method chosen for the specific processing activity undertaken to accomplish the legitimate interest of the PIC or the third party should be necessary and lawful.

A. The means to fulfill the legitimate interest must be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose, in accordance with the principle of proportionality; and

B. The means chosen to accomplish the legitimate interest is itself lawful. The PIC cannot violate any law in the process of accomplishing its legitimate interest.

**SECTION 7. *The Interest is Legitimate and Lawful, and it does not Override Fundamental Rights and Freedoms of Data Subjects (Balancing Test)*.** — A PIC or third party relying on legitimate interest shall determine whether the processing undertaken does not override the data subject’s fundamental rights and freedoms. In doing so, the PIC or third party shall look at the effect or impact of accomplishing the legitimate interest and consider the purpose of processing the interest established and the means by which it is fulfilled.

The factors that may be considered include but are not limited to:

- A. Effect or impact of the specific processing activity on the data subject;
- B. Measures implemented to protect the personal information involved in the specific processing activity or to mitigate the effect or impact of the specific processing activity on the data subject (e.g., privacy-enhancing technologies);
- C. Availability of other means or methods to fulfill the legitimate purpose; and
- D. Reasonable expectation of the data subject on the specific processing of their personal information taking into consideration the surrounding circumstances of each case. A PIC shall consider what a reasonable person would find acceptable under the circumstances taking into consideration the interest established.

## **OBLIGATIONS OF THE PERSONAL INFORMATION CONTROLLER**

**SECTION 8. *Documentation*.** — A PIC shall document the conduct and results of its legitimate interest assessment.

A. A PIC must regularly evaluate its compliance with the requisites for legitimate interest as part of their regular process.

B. A PIC must keep the records of the legitimate interest assessment made as the basis for relying on Section 12(f) of the DPA to process personal information.

C. In case of an investigation or a compliance check, the NPC may require the submission of the records of the legitimate interest assessment.

**SECTION 9. *Further Processing of Personal Information Based on Legitimate Interest*.** — For personal information originally collected based on consent, further processing for additional purposes that constitute a legitimate interest of the PIC may be allowed in accordance with Section 6(B) of the Circular on the Guidelines on Consent.

**SECTION 10. *Legitimate Interest of Third Parties*.** — A PIC shall verify the legitimate interest of the third party to whom personal information may be disclosed, either through its own legitimate interest assessment or on the basis of the third party’s legitimate interest assessment, as stated in Section 4 of this Circular. If a third party intends to process personal information from another PIC for its own legitimate interest, such third party is considered a PIC.

**SECTION 11. *Sectoral Determination of Specific Legitimate Interest.*** — The NPC encourages industry sectors to determine common personal information processing activities within their respective industries that may be based on legitimate interest.

**SECTION 12. *Processing Carried Out by Public Authorities.*** — As a general rule, legitimate interest shall not apply to the processing carried out by public authorities in the performance of their constitutional or statutory mandates.

Legitimate interest may be considered the appropriate lawful basis for specific processing activities carried out by government agencies that are not expressly provided in their mandate and do not fall squarely on any of the other criteria for processing under Section 12 of the DPA or as a special case under Section 4 of the DPA. Legitimate interest may apply as lawful basis for ancillary processing activities performed in the ordinary course of business. In such cases, the PIC must conduct a legitimate interest assessment.

**SECTION 13. *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 14. *Penalties.*** — The processing of personal data in violation of this Circular shall carry criminal, civil, and administrative liability pursuant to the provisions of the DPA, its IRR, and related issuances of the Commission.

**SECTION 15. *Transitory Provision.*** — All affected PICs shall be given a period of ninety (90) calendar days from the effectivity of this Circular to comply with the requirements provided in Section 8(B) herein.

**SECTION 16. *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 17. *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 18. *Effectivity.*** — This Circular shall take effect fifteen (15) calendar days after its publication in the Official Gazette or a newspaper of general circulation.

**Approved:**

**SGD.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**SGD.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

**SGD.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

# Circular on Guidelines for Legitimate Interest

Questions Raised During the Public Consultation on 07 December 2023

## General Questions

Questions	Answer
<b>1. What is legitimate interest?</b>	<p>As stated in Section 3 (A) of the Circular, legitimate interest refers to any actual and real interest, benefit, or gain that a Personal Information Controller (PIC) or third party may have in or may derive from the processing of specific personal information. In simple terms, it talks about what the PIC is trying to achieve with that specific processing activity. A business purpose that is lawful and not contrary to law, morals, public order, and public policy may be a valid legitimate interest.</p>
<b>2. When does legitimate interest apply as a lawful basis for processing?</b>	<p>Legitimate interest applies as a lawful basis for processing personal information under Section 12 (f) of the Data Privacy Act (DPA). It is not a valid lawful basis when the processing involves sensitive personal information, which has been emphasized in Section 3 (B) of the Circular. The processing of sensitive personal information may be based on other lawful criteria under Section 13 of the DPA.</p> <p>The Circular applies if the specific processing of personal information is based on legitimate interest, regardless of whether other applicable lawful criteria are declared. Note, however, that the specific lawful basis that the PIC or third party is relying on for that particular processing activity should be communicated to the data subjects following the principle of transparency and the data subject's right to be informed.</p> <p>Further, the general privacy principles will continue to apply regardless of the applicable lawful basis for processing. Nothing in Section 3 (B) of the Circular gives the impression that the general privacy principles no longer apply in the processing of personal information.</p>

<p><b>3. Whose legitimate interests are considered?</b></p>	<p>The legitimate interest of a PIC or a third party or parties to whom the personal information is disclosed is considered.</p> <p>This is based on Section 12 (f) of the DPA which specifically identifies two (2) kinds of persons: (1) A PIC; and (2) a third party or parties to whom the data is disclosed.</p> <p>Under Section 3 (C) of the Circular, a third party refers to any natural or juridical person to whom personal information is disclosed and who is not the PIC, the PIP, or the data subject of the specific processing activity.</p>
<p><b>4. Does the PIC need to provide a privacy notice informing the data subject that it is processing on the basis of legitimate interest?</b></p>	<p>Yes. While this is not explicitly stated in the Circular, PICs still have the obligation to inform its data subjects of the basis for processing following the general privacy principle of transparency and the data subject's right to be informed.</p> <p>A notice will always be required, regardless of whether the basis for processing personal information is consent, legitimate interest, or another lawful basis. The content of the notice will vary depending on the declared basis for processing. If the processing is based on consent, the notice should state that. If the processing is based on legitimate interest, this should also be clearly declared. This is provided in Section 16 of the DPA and Section 34 (a) (2) (c) of its Implementing Rules and Regulations.</p> <p>To be clear, the Circular is not introducing a new basis for processing. Legitimate interest has always been provided in the DPA. The purpose of the Circular is to clarify the concept of legitimate interest to make it easier to utilize as a lawful basis for processing personal information.</p> <p>A PIC or third party must assess whether relying on legitimate interest is more suitable for its purposes than other lawful bases such as consent.</p>

<p><b>5. If legitimate interest is the lawful basis for processing personal information, is there still a need for the data subject to explicitly state that they consent to the processing through a consent form?</b></p>	<p>No, since the PIC is now relying on legitimate interest and not consent. The PIC would, however, still need to communicate the notice requirements to the data subject through the consent form, because these notice requirements still apply regardless of the lawful basis for processing that the PIC is relying on.</p>
<p><b>6. Will a PIC be given a period to ensure compliance with the provisions of the Circular?</b></p>	<p>There is a transitory period of ninety (90) days from the effectivity of the Circular to give PICs time to comply with Section 8 (B) of the Circular.</p> <p>Section 8 (B) of the Circular provides that “A PIC must keep the records of the legitimate interest assessment made as the basis for relying on Section 12 (f) of the DPA to process personal information.”</p> <p>The transitory period is limited to Section 8 (B) of the Circular because if the PIC is or has been relying on legitimate interest as its basis to process personal information, then it should have conducted some version of the legitimate interest assessment, either separately or together with its privacy impact assessment.</p> <p>Since the three (3) requisites for processing based on legitimate interest are not new and are just elaborations on what is already provided in Section 12 (f) of the DPA, the transitory period is just there to allow PICs or third parties to prepare the necessary documentation to show that they have satisfied all the requisites.</p>

<p><b>7. In a scenario where a party wishes to stop the disclosure of information, what if their basis is an assessment that they want to protect the data subject's privacy?</b></p>	<p>It is important to remember that the DPA should not be used to facilitate the perpetuation of fraud and scams. The PIC cannot refuse to disclose the name and contact information of a person involved in a scam under the guise of protecting their privacy. For instance, if a person was scammed using a digital wallet application, and the application is aware of the scammer's contact details, it would not be appropriate to withhold this information solely for privacy reasons. The interests of the person who was scammed also need to be considered. The Commission has already held that legitimate interest is a proper basis for the person that was scammed to request for the details of the scammer that are necessary for purposes of pursuing legal action.</p>
<p><b>8. What if, in our assessment, the details being requested by a party are not proportional to their legitimate interest in preventing fraud? What if they ask for more details than necessary to fulfill that legitimate interest?</b></p>	<p>There should be a discussion between the PIC and the requesting party about what is proportional, taking into account the stated purpose for their request. Proportionality should not be an arbitrary determination by the PIC. It must be based on the purpose of the request.</p> <p>If a data subject wishes to file a case, the necessary information should be provided to them, so long as it is not protected by bank secrecy law or otherwise privileged information.</p> <p>If the PIC decides not to provide certain information, it should document the reasons for this refusal.</p> <p>It is important to remember that the determination of proportionality should not solely be from the PIC's perspective but should also consider the third party's objectives and the purposes it aims to achieve with the requested information.</p>



## Legitimate Interest of Third Parties

Question	Answer
<p><b>9. May a PIC rely on the legitimate interest assessment of the third party to whom the data is disclosed without conducting its own Legitimate Interest Assessment?</b></p>	<p>Yes. The PIC can rely on the legitimate interest assessment of the third party, or a combination of the documents submitted by the third party showing the presence of all three (3) requisites as stated in the Circular.</p> <p>What is important is that the third party can show its legitimate interest, the presence of the three (3) requisites, and the PIC is able to document all of these.</p>
<p><b>10. Is it required that both the PIC and the third party to whom personal information is disclosed have a legitimate interest?</b></p>	<p>No. It is not required that both the discloser and the recipient of the personal information have a legitimate interest.</p> <p>Section 12 (f) of the DPA provides: “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.”</p> <p>What is important is that the PIC can verify the legitimate interest of the third party. It can conduct its own legitimate interest assessment or rely on the third party’s legitimate interest assessment or its equivalent.</p> <p>To clarify, it is not necessary that both the PIC (disclosing party) and the third party (receiving party) have their own legitimate interest assessment.</p> <p>For example: Person A hits Person B’s car and sped off. Person B only has the plate number of Person A’s car. Person B then goes to the LTO to ask for information, specifically the name and address of the registered owner of the car.</p> <p>Person B can demonstrate their legitimate interest, but to expect LTO to have its own legitimate interest before it discloses the information requested would be problematic because in such instances, the PIC or the disclosing party may not have a legitimate interest in disclosing.</p>

<p><b>11. Can a request for information be rejected if the requesting party has legitimate interest? Or is there a legal obligation to provide information if the requesting party has legitimate interest?</b></p>	<p>It depends on the basis for the refusal to disclose. If the refusal is based solely on a lack of legitimate interest, then that is not a proper reliance on that basis. Section 12 (f) of the DPA states that either the PIC or the third-party recipient must have a legitimate interest. If the PIC has a lawful basis outside the DPA to prevent disclosure, then it can rely on that. However, using the DPA as the sole reason to not disclose could be problematic.</p>
<p><b>12. Is there a prescribed form or procedure for the verification conducted by the PIC of the third parties' legitimate interest?</b></p>	<p>No. There is no prescribed procedure for verification of the legitimate interest of the third party under the Circular.</p> <p>Similar to Section 4 of the Circular, the PIC may use any existing method, structure, or form, to verify the legitimate interest assessment that was conducted before the specific processing activity.</p> <p>To emphasize, what is essential is that the third party can show that it has a legitimate interest in the particular processing activity with proper documentation showing the presence of all three (3) requisites.</p>
<p><b>13. Should the third party send out prior notice to the disclosing PIC concerning any subsequent processing?</b></p>	<p>No. When the third party subsequently processes the personal information it receives, the third party becomes a PIC and will be treated as such.</p>

### Requisites for Processing Based on Legitimate Interest

Questions	Answer
<p><b>14. In relation to the purpose test in Section 5 and the necessity test in Section 6, does a PIC need to fulfill all the elements of those two tests to establish its legitimate interest?</b></p>	<p>Yes. Since Sections 5 and 6 of the Circular talk about the general privacy principles of legitimate purpose and proportionality, the language is not new. As such, all the elements under the purpose test (Section 5) and the necessity test (Section 6) must be complied with.</p> <p>To demonstrate, the PIC cannot have a situation where the purpose for processing is specific but contrary to law. Thus, all three (3) elements under Section 5 and both elements under Section 6 of the Circular must be met.</p>

***B. The means to fulfill the legitimate interest is both necessary and lawful***

<p><b>15. What does “necessary” mean?</b></p>	<p>As the Commission previously held, the qualifier “necessary” refers to the general privacy principle of proportionality. Following this principle, the means must be adequate, relevant, suitable, and necessary, such that it is not excessive in relation to the declared and specified purpose.</p> <p>Since the first requisite, which is the legitimate interest is established, refers to the purpose, “necessary” in relation to the second requisite refers to the means the PIC chooses to achieve its purpose.</p>
<p><b>16. A PIC or third party must determine the “measures implemented to protect the personal information involved in the specific processing activity or to mitigate the effect or impact of the specific processing activity on the data subject (e.g., privacy-enhancing technologies).</b></p> <p><b>If the PIC or third party has implemented existing measures to protect the personal information involved, does it satisfy the second factor? Or does it still depend on the effectiveness of the implemented measures based on the privacy impact assessment and other assessments?</b></p>	<p>Yes, the PIC has to look at the effectiveness of the measures and that will depend on the good faith assessment of the PIC or third party. It is important to clarify that the enumeration in Section 7 of the Circular are factors that may be considered to determine the effect or impact of accomplishing the legitimate interest. These are not requisites.</p>

***C. The interest is legitimate and lawful, and it does not override fundamental rights and freedoms of data subjects***

**17. How is the effect or impact of accomplishing the legitimate interest determined?**

Determining the effect or impact of accomplishing the legitimate interest requires an analysis of the totality of the three (3) requisites.

The first requisite asks, “what is the PIC’s purpose?” The second requisite asks, “how is the PIC achieving that purpose?” The combination of those will give the PIC the effect or impact on the data subject.

To determine if the interest overrides fundamental rights and freedoms, the PIC or third party may consider the following factors:

- Effect or impact of the specific processing activity on the data subject;
- Measures implemented to protect the personal information or to mitigate the effect or impact on the data subject;
- Availability of other means or methods to fulfill the legitimate purpose; and
- Reasonable expectation of the data subject on the specific processing of their personal information.

The effect or impact of accomplishing the legitimate interest is viewed based on the surrounding circumstances of each case.

<p><b>18. COMMENT: “[T]he first sentence of Section 7 appears to be a restatement of Section 4 regarding the importance of the fulfillment of the requisites for legitimate interest. As such, we find it fitting to integrate the same in Section 4.”</b></p>	<p>The first sentence of Section 7 of the Circular is not a restatement of Section 4 of the Circular. Section 7 provides that in assessing the effect or impact of accomplishing the legitimate interest, the PIC or third party should consider the purpose of processing (first requisite) and the means by which it is achieved (second requisite). It is the combination of the first two requisites that will determine the effect or impact of the processing.</p> <p>For example: In the case of debt collection, which is a legitimate purpose, the effect to the data subject is not determined solely based on the purpose, which is debt collection, but how the PIC or third party goes about achieving debt collection. Does the PIC individually notify each person that has a debt, or does the PIC now publicize it on social media and announce to the world that this person has a debt? The purpose of collecting debt may be the same, but the means of fulfilling it can have different effects on the data subject.</p>
<p><b>19. The third factor provides that a PIC or third party must also consider the availability of other means or methods to fulfill the legitimate purpose.</b></p> <p><b>If there are other methods to fulfill the legitimate purpose and the PIC or third party fails to use the same, does that mean there is a failure to satisfy the third factor? What if both methods can fulfill the legitimate purpose?</b></p>	<p>It is the obligation of the PIC or third party relying on legitimate interest to choose the least intrusive method taking into consideration the PIC or third party’s particular circumstances.</p> <p>The Commission considers the particular circumstances of the PIC or the third party. For example, if a PIC can utilize privacy enhancing technologies to make processing less intrusive, but the implementation of that requires an investment of resources and capital that the PIC cannot reasonably shoulder at that point, then the Commission will take those into consideration in determining the applicability of the third factor.</p>

<p><b>20. What is a “reasonable expectation”?</b></p>	<p>The reasonable expectation of the data subject is understood based on what a reasonable person would find acceptable under the circumstances. This is not discretionary, rather, it is viewed based on the surrounding circumstances of each case.</p> <p>The Commission has already issued decisions explaining this and clarified that the reasonable expectation of privacy discussed here is not the same reasonable expectation of privacy in <i>Ople v. Torres</i>.</p> <p>Reasonable expectation of privacy is in terms of further processing of personal information given the specific circumstances surrounding the processing activity such as the original business arrangement between parties.</p>
<p><b>21. COMMENT: “Reasonable expectation must not be discretionary, all possible reasonable expectations must be given to the data subject upon obtaining consent to be compliant to the data subject’s right to be informed of the purposes for which they are being or will be processed, including processing for all legitimate interests of the PIC, or the data subject such as processing for direct marketing, profiling, or historical, statistical or scientific purpose.</b></p> <p><b>Also, the data subject shall be given the opportunity or the right to object to the processing of the personal data, in relation, to the other legitimate interests particularly those favorable to the PIC or the PIP.”</b></p>	<p>There may be some misinterpretation regarding the concept of a reasonable expectation of privacy in this context. There is a difference between the reasonable expectation of a data subject discussed in the previous question and what data subject can expect following the obligation of the controllers to provide them with information on the scope, purpose, nature, and extent of the processing.</p> <p>Under Section 34 (b) under the Implementing Rules and Regulations of the DPA, the right to object is also not absolute. Data subjects can exercise it in instances when the basis for processing is consent or legitimate interest.</p> <p>Therefore, the data subject should be given an opportunity to object.</p> <p>The Commission highlights that the Circular does not change the lawful basis for processing that is legitimate interest. It just provides clarifications to make it easy for people to rely on legitimate interest as basis for processing, so that they avoid over reliance on consent.</p>

## Legitimate Interest Assessment (LIA)

QUESTION	ANSWER
<b>22. What should the legitimate interest assessment contain? Are there required contents?</b>	<p>A legitimate interest assessment should contain information on how the PIC or third party fulfills the requisites for processing based on legitimate interest.</p> <p>It is important to emphasize the existence of proper documentation indicating that the PIC or third party has thoroughly assessed whether it can properly rely on legitimate interest as its basis for processing following the three (3) requirements, including being able to substantiate all of these with evidence.</p>
<b>23. Will the NPC release guidelines for the legitimate interest assessment?</b>	<p>The guidelines for fulfilling these requisites are provided in Sections 5 to 7 of the Circular.</p>
<b>24. Is there a prescribed form for a legitimate interest assessment?</b>	<p>No. There is no prescribed form for a legitimate interest assessment as stated in Section 4 of the Circular. The Commission will not release a template because each legitimate interest assessment will depend on the circumstances of the case.</p> <p>The PIC or third party may use any existing method, structure, or form, provided the PIC or third party applies the requisites for processing based on legitimate interest in its assessment. This may even be included in the conduct of a privacy impact assessment. It also doesn't even have to be in one document, it can be one document or several documents with annexes.</p> <p>The important thing is to have proper documentation showing that all three requisites are fulfilled.</p>

<p><b>25. Under Section 4, which outlines the requisites for processing based on legitimate interest, it is mentioned that there is no prescribed form for the legitimate interest assessment. In this case, is email correspondence an acceptable means?</b></p>	<p>Yes. Email correspondence is acceptable as long as it demonstrates that the three requisites for processing based on legitimate interest are fulfilled in that specific case.</p> <p>Consider a situation where someone wants to obtain the name of a person who scammed them through a payment wallet or platform. This individual paid but the goods were not delivered. Thus, the scammer’s name and contact details are being requested from the payment platforms.</p> <p>In such cases, there might not be formal documentation, but screenshots of email or message correspondence, whether through messenger or other platforms like Facebook Marketplace, can serve as evidence. As long as it clearly demonstrates the fulfillment of the three (3) requisites for legitimate interest in relation to the third party, using email correspondence should be acceptable.</p>
<p><b>26. Will the NPC require the submission of the legitimate interest assessment?</b></p>	<p>As stated in Section 8 (C) of the Circular, the NPC may require the submission of the records of the legitimate interest assessment in cases of investigations or compliance checks.</p> <p>The legitimate interest assessment is not a new requirement. Any PIC or third party relying on legitimate interest as a lawful basis for processing personal information should have conducted an assessment, whether separately or as part of its privacy impact assessment, to determine if legitimate interest is the most applicable lawful basis for a specific processing activity. Following this, a legitimate interest assessment should also be conducted on existing processing activities that involve personal information.</p>



<p><b>27. How often should a legitimate interest assessment be conducted?</b></p>	<p>A PIC or third party should regularly conduct a legitimate interest assessment. If a PIC or third party is relying on legitimate interest as its basis for a specific processing activity, then it should assess if legitimate interest continues to be the most suitable lawful basis for that specific processing activity.</p> <p>The degree of regularity depends on the circumstances of each case. We cannot provide a specific period because PICs are in a better position to know when it is needed to conduct a legitimate interest assessment. The important thing is that a PIC should regularly conduct one and that it is a continuing requirement. It is not a one-time assessment.</p>
<p><b>28. Can we incorporate a legitimate interest assessment as part of the privacy impact assessment?</b></p>	<p>Yes, it can be incorporated because it essentially forms part of the privacy impact assessment. The privacy impact assessment evaluates all the various processing activities the PIC is involved in, and the legitimate interest assessment is just one component of that. It specifically addresses situations where legitimate interests serve as the lawful basis for processing.</p>
<p><b>29. Regarding documentation under Section 8 for routinary or recurrent processes, will a one-time privacy impact assessment suffice, and how long should the documentation be kept?</b></p>	<p>A one-time privacy impact assessment may not be sufficient because regular evaluations of compliance with the requisites for legitimate interest are necessary. Just like a privacy impact assessment, legitimate interest assessments should not be treated as a one-time requirement. They assess the ongoing compliance of the PIC. If there are changes in the PIC's organization, such as launching a new project or product, or altering processes, the PIC is required to conduct a new privacy impact assessment or legitimate interest assessment for that change.</p> <p>As for how long the documentation should be kept, it should be retained as long as the particular process is in place. In the event of an investigation or compliance check, the documentation may be requested. Failure to have adequate documentation while continuing a processing activity relying on legitimate interest could pose challenges.</p> <p>Therefore, it is advisable to maintain documentation as long as the relevant process is ongoing.</p>

**Further Processing of Personal Information Based on Legitimate Interest**

QUESTION	ANSWER
<p><b>30. May further processing of personal information be based on legitimate interest?</b></p>	<p>Yes. Under Section 9 of the Circular, personal information originally collected based on consent may be processed further for additional purposes that constitute a legitimate interest of the PIC or third party.</p> <p>In doing so, the PIC or third party must conduct a legitimate interest assessment on the further processing of personal information.</p> <p>For example: A creditor collected a debtor’s personal information based on consent through the contract’s terms and conditions and consent forms; but during the course of that relationship, the creditor wanted to file a case against the debtor. His information may be further processed based on a legitimate interest.</p> <p>Hence, if one person wants to file a case against another person and he needs the personal information of the accused in order to file the case, he can use as basis for processing Section 13 (f) in relation to Section 12 (f) of the DPA even if personal information was originally collected based on consent.</p>
<p><b>31. Is consent required for further processing based on legitimate interest?</b></p>	<p>No, consent is not required since there is already a lawful basis for that further processing. The lawful basis for the further processing would be legitimate interest. I</p> <p>f the processing activity contemplated by the PIC is already covered by the consent given by the data subject, then the PIC doesn’t even need to look at legitimate interests. It can just rely on the consent. It will depend on the PIC to figure out what is the most appropriate lawful basis for that particular processing activity.</p>

<p><b>32. COMMENT: Regarding Section 9, we propose that it be revised to clarify that as long as consent has been obtained in compliance with applicable requirements (e.g. Circular on the Guidelines on Consent), further processing for additional purposes should be permitted under the legitimate interest basis. We believe that this is what Section 9 intends to convey but suggest that the reference to the Circular on the Guidelines on Consent be clearly tied to the consent originally obtained.”</b></p>	<p>This is not the intention of Section 9 of the Circular. The Commission emphasizes that Section 9 provides “may”. How the PIC goes about achieving that legitimate interest is an important consideration.</p>
<p><b>33. By what channel or means should PIC’s report the results of the legitimate interest assessment to NPC. Is it going to be a compliance report that needs to be submitted at certain times of the year?</b></p>	<p>No, PICs are not required to submit the legitimate interest assessment through a mandatory compliance report at specific times of the year. Submission is only necessary if they are the subject of a compliance check or investigation, where the Complaints and Investigation Division (CID) or the Compliance and Monitoring Division may request the submission of the legitimate interest assessment. In the absence of such circumstances, there is no obligation to submit the legitimate interest assessment.</p> <p>It is helpful to look at legitimate interest assessment in the same way as the privacy impact assessment, as it constitutes a part of the latter. Currently, the NPC does not require the submission of privacy impact assessments unless an entity is under investigation or subject to a compliance check. The same principle could apply to legitimate interest assessments.</p>

## Sectoral Determination of Specific Legitimate Interest

QUESTION	ANSWER
<p><b>34. Is it mandatory for sectors to determine common personal information processing activities within their respective industries that may be based on legitimate interest?</b></p>	<p>No. Section 11 of the Circular is not mandatory. It expressly states that the NPC encourages industry sectors to undertake this task. It is not an obligation but rather a recommendation.</p> <p>This encouragement is intended to be beneficial for both the sectors involved and the NPC. Establishing a common understanding of normal processing activities within a particular sector can streamline the process, eliminating the need for guesswork in each instance. While this is beneficial, it's important to remember that each case still needs individual consideration. Despite this, having sectoral determinations in place will be very helpful.</p>
<p><b>35. Will the NPC release a list of common legitimate interests for each sector or in general?</b></p>	<p>No, the Commission will not release such a list. The concern is avoiding a situation where individuals could claim any form of data collection or fraud prevention as a legitimate interest, enabling them to justify any action.</p> <p>The first requirement in determining legitimate interest goes into what the PIC's purpose is and whether the purpose is lawful and does not go against morals, public order, and public policy. Making such a determination is relatively straightforward; the critical aspect lies in how one goes about achieving that purpose.</p> <p>Creating a list of common legitimate interests for each sector or in general might be counterproductive, as it could overlook the specific methods and means necessary to achieve a legitimate interest in a given context.</p>

<p><b>36. Medical technology companies need to process health data both when developing new technologies and as part of their rollout to healthcare systems. In general, Medical Technology Companies act as processors. Given this scenario, can the medical technology sector work on a sectoral determination of specific legitimate interests?</b></p>	<p>Yes, the medical technology sector can work on the sectoral determination of legitimate interests. It's important to note, however, that legitimate interest applies solely to the processing of personal information and not sensitive personal information.</p> <p>Since health data likely falls under sensitive personal information, legitimate interest may not be the most suitable criteria for processing. Instead, engaging in proper research, relying on the provisions in Section 4 of the DPA, is recommended. This involves conducting proper research that is cleared by an ethics board and documented appropriately, among others.</p> <p>Given the nature of health data, legitimate interest may not be the best criteria to rely on, but the sector is free to come up with its sectoral determination of specific legitimate interests.</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Processing carried out by Public Authorities**

<b>QUESTION</b>	<b>ANSWER</b>
<p><b>37. When may public authorities rely on legitimate interest as their lawful basis for processing personal information?</b></p>	<p>When processing personal or sensitive personal information, public authorities should primarily rely on their mandate as provided by law or regulation.</p> <p>As outlined in Section 12 of the Circular, a government agency can resort to legitimate interests as basis for processing, but only for ancillary processing activities conducted in the ordinary course of its business, not to fulfill its mandate. This includes activities such as office management, employee welfare, and financial accountability.</p> <p>In such instances, a legitimate interest assessment must still be conducted to ascertain whether legitimate interest is the most appropriate and suitable legal basis for that specific processing activity.</p>

<p><b>38. In relation to Section 10, to clarify, third parties do not include the PICs with whom we have an existing data sharing agreement?</b></p>	<p>No, that is incorrect. An existing data sharing agreement is not considered a lawful basis for processing, as emphasized in our Circular on Data Sharing Agreements. A data sharing agreement outlines the process and mechanism for sharing information, specifying how it's operationalized, the duration, and other relevant details. However, it does not serve as the basis for the actual sharing.</p> <p>When sharing information with third parties, it is crucial to identify the basis for this sharing. If the basis is legitimate interest, a version of a legitimate interest assessment should be in place. If a previously executed data sharing agreement already includes the requisites for a legitimate interest assessment, it can be sufficient. However, it is essential to recognize that a data sharing agreement itself is not the lawful basis for processing.</p> <p>herefore, it is necessary to understand why information is shared with other PICs, even if there's an existing data sharing agreement. Is the sharing based on consent, contract, legal requirement, or legitimate interest? In the absence of the former, it might be that the sharing is based on legitimate interests, and in such cases, proper analysis and documentation are imperative.</p>
<p><b>39. Is the sector required to submit the sectoral determination of common legitimate interest to the NPC?</b></p>	<p>No, there is no mandatory requirement for sectors to submit the sectoral determination of common legitimate interest to the NPC. Section 11 encourages sectors to voluntarily come up with their common legitimate interests. It may, however, be beneficial for the sector to submit it to the NPC once established. This submission can provide the NPC with a clearer understanding of the common legitimate interests and means of achieving those interests within that specific sector. Consequently, this aids the NPC in analyzing and recognizing practices that regularly occur within that sector which helps enhance overall comprehension.</p>

<p><b>40. If legitimate interest is used for further processing not covered by consent, must the data subject receive fresh notification or opportunity to object?</b></p>	<p>Yes, a fresh notification is required. It is essential to clarify that the right to be informed, grounded in the principle of transparency, is a constant requirement. Even if a different lawful basis, other than consent, is utilized for processing, the obligation to provide a privacy notice persists, as consistently emphasized by the Commission. If there are new developments or changes in processing activities, the data subject must be notified.</p> <p>In the context of relying on legitimate interest as a basis, the data subject retains the right to object, and this right does not expire. However, it's important to note that the right to object is not absolute. For instance, in cases when the basis for processing is legitimate interest, the data subject can exercise their right to object. However, this will not stop the processing if another basis for processing exists such as when pursuing a legal claim under Section 13 (f) of the DPA. As always, these determinations are made on a case-to-case basis.</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

# NPC Circular No. 2024-01

**DATE : 26 January 2024**

**SUBJECT : AMENDMENTS TO CERTAIN PROVISIONS OF THE 2021 RULES OF PROCEDURE OF THE NATIONAL PRIVACY COMMISSION**

*Pursuant to the authority vested in the National Privacy Commission (NPC) through Section 7(b) of Republic Act No. 10173, otherwise known as the “Data Privacy Act of 2012” (DPA), to receive complaints and institute investigations on matters affecting any personal information, the following amendments are hereby prescribed and promulgated, repealing for this purpose certain provisions of the 2021 Rules of Procedure of the NPC dated 28 January 2021.*

**SECTION 1.** Rule 1, Sections 4 and 5 of the 2021 NPC Rules of Procedure are hereby amended and renumbered to read as follows:

**“SECTION 4. *Definition of Terms.*** – The terms defined in the DPA, and its rules, are adopted accordingly in this Circular.

- a. **AFFIRMATIVE DEFENSES** – shall refer to any defense by the respondent which, if found to be credible, will negate liability under the DPA, 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 prompted by the applicable rules promulgated by the Commission.
- c. **COMMISSION** – shall refer to the Privacy Commissioner and the two (2) Deputy Privacy Commissioners.
- 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 or her representative for violation of the DPA.
- e. **COMPLIANCE CHECK** – shall refer to the systematic and impartial evaluation of a personal information controller (PIC) or personal information processor (PIP), in whole or in 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, IRR, and NPC issuances. It is an examination that includes Privacy Sweeps, Documents Submission, and On-Site Visits, which intends 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.
- f. **COURIER** – shall refer to any private mail carrier accredited by the Supreme Court, the NPC, or by international conventions of which the Philippines is a



signatory.

- g. DIGITAL SIGNATURE** – shall refer 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.<sup>1</sup>
- h. DOCUMENTS SUBMISSION** – shall refer to a mode of Compliance Check where the NPC may require the submission of documents and additional information from a PIC or PIP that has undergone a Privacy Sweep to, among others, clarify certain findings arising therefrom and to determine the level of compliance of the PIC or PIP with respect to its obligations under the DPA, IRR, and NPC issuances.
- i. ELECTRONICALLY-STORED INFORMATION** – shall refer to any information that is received, recorded, transmitted, stored, processed, retrieved, or produced electronically. It shall include any printout or output that accurately reflects the electronically stored information.<sup>2</sup>
- j. EVALUATING OFFICER** – shall refer to a member of the Compliance and Monitoring Division (CMD), a special committee, or task force (or respective members thereof) that may or may not include members from the CMD, created by order of the Commission to evaluate documents and information submitted to the CMD pertaining to compliance requirements and personal data breach notifications.
- k. HEARING OFFICER** – shall refer to a member of the Complaints and Investigation Division (CID), a special committee, or task force (or respective members thereof) that may or may not include members from the CID, created by order of the Commission to conduct hearings.
- l. INVESTIGATING OFFICER** – shall refer to a member of the CID, a special committee, or task force (or respective members thereof) that may or may not include members from the CID, created by order of the Commission to conduct investigations, hearings, and prepare related reports.
- m. JURIDICAL PERSON** – shall refer to: (1) the State and its political subdivisions, (2) corporations, institutions, and entities that are created by law for public interest or purpose, and (3) corporations, partnerships, and associations for private interest or purpose to which the law grants a juridical personality, separate and distinct from that of each shareholder, partner, or member.<sup>3</sup>

1 Rules on Electronic Evidence, A.M. No. 01-7-01-SC, Rule 2, § 1(e) [July 17, 2001].

2 *Id.* Rule 2, § 1(h).

3 An Act to Ordain and Institute the Civil Code of the Philippines, [CIVIL CODE OF THE PHILIPPINES], Republic Act No. 386, Art. 44 (1949).

- n. **MEDIATION** – shall refer 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.
- o. **MEDIATION OFFICER** – shall refer to a member of the Legal Division (LD), a special committee, or task force (or respective members thereof) that may or may not include members from the LD, created by order of the Commission to conduct mediation.
- p. **MEDIATION SUPPORT OFFICER** – shall refer to a member of the LD, a designated person, special committee, or task force (or respective members thereof) that may or may not include members from the LD, created by order of the Commission to provide support to Mediation Officers.
- q. **NPC** – shall refer to the National Privacy Commission created under the DPA.
- r. **ON-SITE VISIT** – shall refer to a mode of Compliance Check if there are persistent or substantial findings of non-compliance of the PIC or PIP with the obligations indicated in the DPA, IRR, and NPC issuances.
- s. **PARTIES IN INTEREST** – shall refer to a real party in interest who stands to be benefited or injured by the judgment in the suit, or the party entitled to the avails of the suit. Unless otherwise authorized by law or these Rules, every action must be prosecuted or defended in the name of the real party in interest.<sup>4</sup>
- t. **PRELIMINARY MEDIATION CONFERENCE** – shall refer to the initial mediation conference after the parties mutually agree to enter into the mediation proceeding and the case is referred by the Investigating Officer to the Mediation Officer.
- u. **PRIVACY SWEEP** – shall refer to the initial mode of Compliance Check where the NPC shall review a PIC or PIP’s compliance with respect to its obligations under the DPA, IRR, and NPC issuances, based on publicly available or accessible information, such as, but not limited to websites, mobile applications, raffle coupons, brochures, and privacy notices.
- v. **PRIVATE CAUCUS** – shall refer to a private meeting with either party called by the Mediation Officer, with the consent of both parties, to discuss issues in private and to arrive at a mutually satisfactory agreement beneficial to all parties.
- w. **PUBLIC AUTHORITY** – shall refer to any government entity created by the Constitution or law.

---

<sup>4</sup> 2019 Amendments to the 1997 Rules of Civil Procedure (A.M. No. 19-10-20-SC), [RULES OF COURT], Rule 3, § 2 (May 1, 2020).

- x. **RULES** – shall refer to the 2021 NPC Rules of Procedure, including its amendments, unless otherwise stated.
- y. **SUA SPONTE INVESTIGATION** – shall refer to an investigation initiated by the NPC on its own for possible violation of the DPA.”

“**SECTION 5. Enforcement Powers.** – The Commission may use its enforcement powers under the DPA in the course of investigations to order cooperation of the subject of the inquiries or other interested individuals or entities, including public authorities, or to compel appropriate action to protect the interests of data subjects.”

**SECTION 2.** Rule II, Section 1 of the 2021 NPC Rules of Procedure is hereby amended to read as follows:

“**SECTION 1. Who may file complaints.** – Subject to Rule X of these Rules, data subjects who are affected by a privacy violation or data breach may file complaints for violations of the DPA: Provided, that a representative may file on behalf of a data subject if he or she is authorized by a special power of attorney. In the case of a minor or a person alleged to be incompetent, the pertinent provisions of the Rules of Court and its amendments shall apply. It is sufficient that proof establishing the relationship with the complainant be presented to the NPC as an attachment to the complaint. In case the minor or a person alleged to be incompetent is represented by the father or mother, the birth certificate shall be considered sufficient proof, while for the guardian, the court order designating the person as guardian shall be sufficient.”

One or more data subjects may be represented by a single juridical person: Provided, that the juridical 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 person representing the juridical person acting as the representative of one or more data subjects must be authorized to appear and act on behalf of the juridical person by a Board Resolution contained in a duly notarized Secretary’s Certificate or its equivalent in case of government agencies<sup>5</sup>

In cases where the complainant is a non-resident citizen who has no authorized representative in the Philippines or is unable to appoint such a representative, such person may submit a complaint in accordance with these Rules: Provided, that the complaint must be notarized by the Philippine Embassy or Consulate, or with an apostille certificate from the country of origin.”

**SECTION 3.** Rule III, Section 6 of the 2021 NPC Rules of Procedure is hereby amended to read as follows:

“**SECTION 6. Service of judgments, orders, or resolutions of the NPC.** – At the discretion of the Commission, judgments, orders, or resolutions shall be served either personally, by registered mail, by courier, by sending through user accounts and autogenerated notification of electronic systems implemented by the NPC, or by electronic mail. When a complaint, pleading, or any other submission is filed or submitted through electronic mail, the NPC may serve its judgments, orders, or resolu-

<sup>5</sup> This includes a department, bureau, office, instrumentality, government-owned or controlled corporation, local government, state university and college, or a distinct unit in it.

tions by electronic mail through the same electronic mail address used in the filing of the complaint or pleading, or submission of document, unless otherwise indicated in the complaint, pleading, motion, or other submissions of parties. When the NPC has opted to serve a judgment, order, or resolution by electronic mail, it shall no longer serve its issuances in the same case or matter by any other mode of service, unless circumstances warrant otherwise.

For judgments, orders, or resolutions served by electronic mail, electronic service is considered complete at the time of electronic transmission of the document, or when available, at the time that the electronic notification of service of document is sent.

For matters coursed through the electronic systems implemented by the NPC, the service of judgments, orders, or resolutions is deemed completed at the time it is successfully uploaded to the system.”

**SECTION 4.** Rule IV of the 2021 NPC Rules of Procedure is hereby amended and renumbered to read as follows:

**“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 of the following grounds:

1. The complaint is insufficient in form or does not comply with Section 3, Rule II of these Rules;
2. The complainant does 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 DPA or does not involve a privacy violation or data breach;
4. There is insufficient information to substantiate the allegations in the complaint;  
or
5. The parties, other than the responsible officers of juridical persons, cannot be identified or traced despite diligence to determine them.

**SECTION 2. *Amendment of complaint, when allowed.*** – The complainant may substantially amend the complaint once as a matter of right at any time before the 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 and with leave of the Investigating Officer.

**SECTION 3. *Permissive joinder of parties.*** – All persons in whom or against whom any right to relief in respect to or arising out of the same transaction or series of transactions is alleged to exist, whether jointly, severally, or in the alternative, may, except as otherwise provided in these Rules, join as complainants or be joined as

respondents in one complaint, where any question of law or fact common to all such complainants or to all such respondents may arise in the action; but the NPC may make such orders as may be just to prevent any complainant or respondent from being embarrassed or put to expense in connection with any proceedings in which the party may have no interest.

***SECTION 4. Compulsory joinder of indispensable parties.*** – Parties in interest without whom no final determination can be had of an action shall be joined either as complainants or respondents.

***SECTION 5. Necessary party.*** – A necessary party is one who is not indispensable but who ought to be joined as a party if complete relief is to be accorded as to those already parties, or for a complete determination or settlement of the claim subject of the action.<sup>6</sup>

***SECTION 6. Non-joinder of necessary parties to be pleaded.*** – Whenever in any complaint or pleading in which a claim is asserted a necessary party is not joined, the pleader shall set forth the party's name, if known, and shall state why the party is omitted. Should the NPC find the reason for the omission unmeritorious, it may order the inclusion of the omitted necessary party if jurisdiction over the person may be obtained.

The failure to comply with the order for a necessary party's inclusion, without justifiable cause, shall be deemed a waiver of the claim against such party.

The non-inclusion of a necessary party does not prevent the NPC from proceeding with its investigation, and any decision rendered therein shall be without prejudice to the rights of such necessary party.

***SECTION 7. Misjoinder and non-joinder of parties.*** – Neither misjoinder nor non-joinder of parties is ground for dismissal of a complaint. Parties may be dropped or added by order of the NPC by motion of any party or on its own initiative at any stage of the action and on such terms as are just. Any claim against a misjoined party may be severed and proceeded with separately.

***SECTION 8. Entity without juridical personality as respondent.*** – When two or more persons not organized as an entity with juridical personality enter into a transaction, they may be sued under the name by which they are generally or commonly known. In the answer of such respondent, the names and addresses of the persons composing the entity must be accurately stated. The address to be used shall be the last known address of the respondent.

***SECTION 9. Submission of comment.*** – Upon finding that the complaint may be given due course, the 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 the respondent does not file a comment within the period provided.

In case the respondent is a minor or a person alleged to be incompetent, the pertinent provisions of the Rules of Court and its amendments shall apply. It is sufficient that proof establishing the relationship with the respondent be presented to the NPC as an attachment to the comment. In case the minor or a person alleged to be incompetent is represented by the father or mother, the birth certificate shall be considered sufficient proof, while for the guardian, the court order designating the person as guardian shall be sufficient.

In case the respondent is a juridical person, the representative filing the comment must be authorized to appear and act on behalf of the juridical person by a Board Resolution contained in a duly notarized Secretary's Certificate, or its equivalent for a government agency<sup>7</sup>.

**SECTION 10. *Content of the comment.*** – The respondent shall raise all of his or her defenses in the comment. No motions to dismiss shall be entertained: Provided, the Investigating Officer, in his or her discretion, may treat a motion to dismiss as the respondent's comment.

**SECTION 11. *Change of physical address or electronic mail address.*** – A party who changes physical address or electronic mail address while the complaint is pending must promptly file, within five (5) calendar days from such change, a notice of change of physical address or electronic mail address with the NPC and serve the notice on all other parties. Service through the physical address or electronic mail address of a party, on record, shall be presumed valid, unless such party notifies the NPC of any change.

**SECTION 12. *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. appeals or motions for reconsideration from any interlocutory order of the Investigating Officer.

**SECTION 13. *Affirmative defenses.*** – In lieu of a motion to dismiss, the respondent may raise in the comment affirmative defenses such as but not limited to:

---

<sup>7</sup> This includes a department, bureau, office, instrumentality, government-owned or controlled corporation, local government, state university and college, or a distinct unit in it.

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 14. Authority of the Investigating Officer to rule on motions.** – The Investigating Officer may directly rule on motions that do not fully dispose of 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 5.** Rule VI of the 2021 NPC Rules of Procedure is hereby amended and renumbered to read as follows:

#### “RULE VI – ALTERNATIVE DISPUTE RESOLUTION

**SECTION 1. Willingness to mediate.** – During the preliminary conference or at any stage of the proceedings but before endorsement of the case for decision by the Legal and Enforcement Office (LEO) Director or the Commission, as the case may be, 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 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.

Parties may apply for mediation through their representatives, provided that the latter are duly authorized in accordance with Section 8 of this Rule. Otherwise, no order to mediate shall be issued by the Investigating Officer until and unless such requirements have been completed and substantiated.

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 Commission 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 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 up to

ninety (90) 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. Conduct of Mediation Officers.** – All Mediation Officers and Mediation Support Officers shall be bound by the NPC Mediation Code of Conduct.

**SECTION 6. 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 reiterate the benefits of an early settlement of the dispute and endeavor to achieve the fairest and most expeditious settlement possible.

Each party shall be allowed to make a brief statement of their respective position and preferred outcome. The Mediation Officer shall assist the parties in exploring common grounds for settlement while respecting party autonomy throughout the process.

When necessary, the parties shall agree on the schedule of the next mediation conference and the Mediation Officer shall issue an order therefor.

**SECTION 7. 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 opportunity to ventilate such interest and motivation. The Mediation Officer may call such conferences or 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 8. 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 a 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 juridical person, the representative must be authorized by a Board Resolution contained in a duly notarized Secretary's Certificate, or any equivalent written authority to offer, negotiate, accept, decide, and enter into a mediated settlement agreement.

No representative shall be allowed to appear in mediation on behalf of a party without proper authorization as verified by the Mediation Officer.

The parties shall inform the LD about changes in representation through a written statement or manifestation along with the corresponding written authority to offer, negotiate, accept, decide, and enter into a mediated settlement agreement submitted to the Mediation Officer prior to the next scheduled mediation conference. The



mediation shall not proceed until and unless the representatives are duly authorized in accordance with this Section.

**SECTION 9. *Failure of parties to appear, effect.*** – If any of the parties fail to appear without justifiable reason for two (2) consecutive mediation conferences at any stage of the proceedings, the Mediation Officer may order its termination 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 or caucuses, and be henceforth permanently prohibited from requesting mediation at any other stage of the complaint proceedings before the NPC.

**SECTION 10. *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 persons may directly attend the mediation conference with all its concomitant rights and obligations.

**SECTION 11. *Venue.*** – Mediation proceedings may either be conducted via video-conferencing technology for the remote appearance and testimony of parties, as provided under Rule XIII, Section 7 hereof, or within the NPC premises, as agreed by both parties. 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 12. *Mediation period and extension.*** – The Mediation Officer shall endeavor to achieve a mediated settlement of the dispute within sixty (60) calendar 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 Mediation Officer may extend the mediation period for another thirty (30) calendar days for good cause shown. In all instances, the mediation period shall not exceed ninety (90) calendar days.

**SECTION 13. *Mediated Settlement Agreement.*** – A mediated settlement agreement following successful mediation shall be jointly prepared and executed by the parties or their representatives, with the assistance of their respective counsels, if any. Only the parties or their authorized representatives shall have the authority to confirm the provisions of the mediated settlement agreement and execute the agreement. 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 14. Confirmation Conference.** – The Mediation Officer shall require the parties to attend a confirmation conference prior to the endorsement of their mediated settlement agreement to the Commission. The parties shall present to the Mediation Officer the signed mediated settlement agreement, as well as the evidence of compliance with the stipulation in the agreement, if applicable.

In case of failure of any of the parties to appear for two (2) consecutive confirmation conferences, the Mediation Officer may resolve to submit the parties' mediated settlement agreement to the Commission for confirmation: Provided, that the appearing party has agreed to proceed, that the parties have fully complied with all the obligations arising from the provisions of the mediated settlement agreement, that the parties have submitted all the necessary documents, and the LD has duly notified the non-appearing party. In such cases, the non-appearing party's right to amend, object, or revoke specific provisions in the mediated settlement agreement shall be deemed waived.

When the agreement involves future obligations or obligations susceptible to partial fulfillment beyond the mediation period, the party responsible shall submit proof of compliance to the Enforcement Division (EnD).

**SECTION 15. Confirmation by the Commission.** – The Mediation Officer shall issue a resolution submitting the signed mediated settlement agreement to the Commission within thirty (30) calendar days from the date of the confirmation conference. The Commission shall issue a resolution confirming the mediated settlement agreement within thirty (30) 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 16. Effect of confirmed Mediated Settlement Agreement.** – A confirmed mediated settlement agreement shall have the effect of a decision or judgment on the complaint but without prejudice to Rule X of these Rules and shall be enforced in accordance with the NPC's rules and issuances.

**SECTION 17. Failure to reach settlement.** – If the parties are unable to arrive at a settlement of their dispute, or it becomes apparent that a settlement, given the disparity of the respective positions of the parties, is not likely or achievable within the sixty (60) calendar day mediation period or the reasonable extension of such period under Section 12 of this Rule, the Mediation Officer may declare the mediation unsuccessful and terminate the proceedings by issuing a Notice of Non-Settlement of Dispute and furnishing copies to the Investigating Officer and the parties.

Parties may be allowed to re-apply for mediation despite a prior failure to reach settlement, unless otherwise permanently prohibited in accordance with Section 9 of this Rule: Provided, that the application is filed before the endorsement of the case for decision by the Commission: Provided further, that the application is done in compliance with this Rule.

**SECTION 18. Resumption of complaint proceedings.** – Upon receipt of the Notice of Non-Settlement of Dispute issued by the Mediation Officer, the Investigating Of-

ficer shall issue an order lifting the suspension of the complaint proceedings, which shall resume as a matter of course. Copies of the order, including the notice of the next hearing date of the complaint proceedings, shall be furnished to all the parties.

**SECTION 19. Confidentiality of proceedings.** – The mediation conferences shall be held in private. Persons other than the parties, their representatives, counsel, and the Mediation Officer may attend only with the consent of the parties and upon approval by the Mediation Officer. Anyone present during a mediation conference shall not disclose any information obtained during the conference to any other person, nor utter the same through other means.

The mediation proceedings and all related incidents shall be kept strictly confidential, and all admissions or statements shall be inadmissible for any purpose in any proceeding, unless otherwise specifically provided by law. However, evidence or information that is otherwise admissible or subject to discovery does not become inadmissible or protected from discovery solely by reason of its use in mediation.

No transcript or minutes of the mediation proceedings shall be taken, and the personal notes of the Mediation Officer, if any, shall likewise be inadmissible nor cognizable in any court, tribunal, or body for whatever purpose and shall be securely destroyed upon termination of the mediation proceedings.

**SECTION 6.** Rule VII, Section 3 of the 2021 NPC Rules of Procedure is hereby amended to read as follows:

**“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 to the Commission.

For cases recommended for outright dismissal under Rule IV, Section 1 of these Rules, the Investigating Officer shall submit to the LEO Director a Fact-Finding Report, including the basis and recommendation for outright dismissal of the complaint.”

**SECTION 7.** Rule VIII of the 2021 NPC Rules of Procedure is hereby amended and re-numbered to read as follows:

**“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 evidence on record. On the basis of the 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 the schedule;
- b. The Commission may require additional information and 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 its consideration;
- d. The Commission may require the parties 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. *Decision for Cases Dismissed Outright.*** – The LEO Director shall review the evidence presented, including the Fact-Finding Report and the evidence on record. Based on the review, the LEO Director may: (1) promulgate a decision dismissing the case outright based on the grounds in Rule IV, Section 1 of these Rules; or (2) remand the complaint for investigation and require the respondent to file a verified comment to the complaint and appear for preliminary conference. Provided, the dismissal shall be without prejudice to the refiling with the NPC in accordance with the Rules, or filing of appropriate civil, criminal, or administrative cases against the respondent before any other forum or tribunal, if any.

**SECTION 4. *Decision for Cases where Complainant files an Affidavit of Desistance.*** – The LEO Director shall review the evidence presented, including the Fact-Finding Report, evidence on record, and any other supporting documents. Based on the review, the LEO Director shall promulgate a decision. The dismissal shall be with prejudice to the refiling with the NPC, but without prejudice to the filing of appropriate civil, criminal, or administrative cases against the respondent before any other forum or tribunal, if any.

**SECTION 5. *Refiling of complaint or motion for reconsideration on the decision issued by the Legal and Enforcement Office.*** – The complainant may refile the complaint with the NPC or file with the LEO a motion for reconsideration of the decision dismissing the case outright. Otherwise, the decision of the LEO Director shall become final and executory within fifteen (15) calendar days from notice thereof with proof of service on the adverse party. If the complainant files a motion for re-

consideration, the motion for reconsideration shall be endorsed to the Commission for its resolution within fifteen (15) calendar days from the LEO Director's receipt of such motion.

**SECTION 6. Rendition of decision.** – The decision of the Commission shall resolve the issues on the basis of all the evidence on record and its own consideration of the law. The decision may include enforcement orders on the following: 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. a 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 DPA; d. an order to conduct a sua sponte investigation under Rule X such as in cases when the responsible officer of a juridical entity must be determined for recommendation to the Department of Justice for prosecution; e. an order to compel or petition any entity, government agency, or instrumentality to abide by its orders or take action on a matter affecting data privacy; f. an imposition of fines for violations of the DPA or NPC issuances; or g. any other order to enforce compliance with the DPA.

**SECTION 7. Motion for reconsideration on the decision issued by the Commission.** – The decision of the Commission shall become final and executory fifteen (15) calendar days from notice thereof with proof of service to the adverse party. One motion for reconsideration may be filed, which shall suspend the running of the period. Any appeal from the decision shall be to the proper courts, in accordance with law and the rules.

**SECTION 8. Entry of judgments and final orders.** – If no appeal or motion for reconsideration is filed within the time provided in these Rules, the judgment shall attain finality, and an entry of judgment shall be issued to the parties. The date when the judgment becomes executory shall be deemed as the date of its entry. The entry of judgment shall contain the dispositive portion of the judgment with a certificate that such judgment has become final and executory.”

**SECTION 8.** Rule X of the 2021 NPC Rules of Procedure is hereby amended and renumbered to read as follows:

#### **“RULE X – SUA SPONTE INVESTIGATION**

**SECTION 1. Commencement.**– The NPC, through the CID or a special committee or task force assigned for such purpose, may initiate an investigation on the circumstances surrounding a possible data privacy violation or data breach in cases of, but not exclusive to, matters that arose from pending cases before the NPC, including those that have resulted in a confirmed mediated settlement agreement, reports from the daily news, trends or academic studies, information gathered from corroborated and substantiated anonymous tips, or reports from other offices of the NPC or government agencies.

**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 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 data breach, subject to due process requirements under the law. 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, or to appear for an investigation hearing or clarificatory conference before the Investigating Officer, special committee, or taskforce, or the Commission, in accordance with Rule VIII, Section 1.

**SECTION 5. Request for case files during the conduct of a sua sponte investigation.** Within fifteen (15) calendar days upon receipt of a request for case files by the parties-in-interest subject of the investigation, or their representative, legal heirs and assigns, or successors-in-interest, the CID shall release the requested case files to the requesting party. The representative shall be authorized by a special power of attorney. In case a party is a juridical person, the representative shall be authorized to appear and act on behalf of the juridical person by a Board Resolution contained in a duly notarized Secretary’s Certificate or its equivalent for a government agency<sup>8</sup>.

The requested case files may be in the form of a physical copy or an electronic copy. For physical copies, the same be in the form of a copy only or a certified true copy, at the option and cost of the requesting party. For electronic copies, the same be issued to the requesting party and duly protected by a password.

The requested case files shall include documents and communications between the requesting party and the NPC, together with its attachments. Documents that are internal in nature, such as, but not limited to, Technical Reports, Minutes of the Meeting, and Memorandum within the NPC, shall be excluded. Third-party reports and submissions shall also be excluded.

**SECTION 6. 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. In a sua sponte investigation, the Fact-Finding Report serves as the complaint, with the CID as the nominal complainant.

**SECTION 7. 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 its annexes and given an opportunity to submit a comment or other pleadings, if necessary. In cases where

<sup>8</sup> This includes a department, bureau, office, instrumentality, government-owned or controlled corporation, local government, state university and college, or a distinct unit in it.

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 8. 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 DPA 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.”

SECTION 9. Rule XI of the 2021 NPC Rules of Procedure is hereby amended to read as follows:

#### “RULE XI – BREACH INVESTIGATION

**SECTION 1. Procedure for data breach notification.** – The procedure for data breach notification and other requirements shall be governed by the DPA, its IRR, and NPC issuances pertaining to data breach management. These Rules shall apply in a suppletory character.

**SECTION 2. Receipt of data breach notifications.** – The CMD shall be the initial recipient of data breach notifications and shall immediately assign an Evaluating Officer to review 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 recommend to resolve preliminary requests from the PIC or PIP for (a) extensions to notify data subjects or (b) extensions to file full breach report. The preliminary requests for extensions granted by the CMD shall be for a period of twenty (20) calendar days counted from the date of the request.

**SECTION 4. Preliminary requests and related Motions that must be endorsed to the Commission.** – The CMD shall endorse to the Commission the following requests from the PIC or PIP:

- a. On notification of data subjects:
  - i. Request for exemption;
  - ii. Request for postponement;
  - iii. Request for extension beyond twenty (20) calendar days; or
  - iv. Request for use of alternative modes of notification.
  
- b. On submission of full report:
  - i. Request for extension beyond twenty (20) calendar days; or
  - ii. Subsequent request for extension.

- c. Other preliminary requests not covered by the preceding Section.
- d. Motion for Reconsideration filed by the PIC or PIP on their preliminary request and other related pleadings.

The Commission may delegate to the CMD the resolution of Section 4 (a)(iii) and (b) as deemed necessary.

**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. The PIC or PIP may be directed to submit additional documents through an order.

Further, the CMD shall monitor the compliance of the PIC or PIP with the periods provided in the NPC issuances on data breach and the subsequent extensions allowed under the preceding sections.

In case of non-compliance, the CMD may apply for a Cease-and-Desist Order in accordance with the NPC issuances pertaining to the matter.

**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 based on information available on record.

The report may contain a recommendation of a possible violation of the DPA arising from the breach matter and a recommendation for the imposition of administrative fines on other infractions.

Upon the finding of a possible data privacy violation that requires further investigation, the CMD shall endorse the Final Breach Notification Evaluation Report to the Commission for the resolution of the breach case while endorsing the matter to the CID for further investigation for a possible data privacy violation.

**SECTION 7. *Conduct of breach investigation.*** – Upon receipt of the Final Breach Notification Evaluation Report, an Investigating Officer shall determine if there is a necessity to conduct an on-site or technical investigation. The Investigating Officer shall request proper authority from the NPC before conducting any on-site or technical investigation. The Investigating Officer may also request assistance from the technical personnel of the NPC. In the course of the investigation, the complainant and 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 Final Breach Notification Evaluation Report, whichever is applicable.

**SECTION 9. *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 with a copy of the Fact-Finding Report and its annexes and



given an opportunity to submit a comment or other pleadings, if necessary. In cases where the respondent fails without justification to submit a comment or other pleadings, 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 information that a possible data breach occurred but the PIC or PIP did not submit any notification to the NPC, the CID may use this information to initiate a sua sponte investigation under Rule X.

During the sua sponte investigation, if a breach notification is submitted by the PIC or PIP, the CID shall continue with its sua sponte investigation on violations of the DPA and NPC issuances for possible recommendations for prosecution with the Department of Justice or imposition of administrative fines. The CMD shall, for its part, evaluate the breach matter submitted and recommend the imposition of administrative fines, if warranted.

**SECTION 11. *Post-breach monitoring and compliance.*** – The CMD shall monitor compliance of PICs or PIPs with the orders and resolutions issued by the Commission during its evaluation of the data breach matter.

The EnD shall ensure the enforcement and monitoring of compliance of all other judgments, resolutions, decisions, or orders issued by the Commission.

**SECTION 10.** This Rule has been included to read as follows:

**“RULE XII – COMPLIANCE CHECKS**

**SECTION 1. *Procedure for Compliance Checks.*** – The procedure for Compliance Checks and other requirements shall be governed by the DPA, its IRR, and NPC issuances pertaining to Compliance Checks. These Rules shall apply in a supplementary character.

**SECTION 2. *Conduct of Privacy Sweep.*** – The CMD shall conduct a Privacy Sweep of all publicly available or accessible information, including, but not limited to websites, mobile applications, raffle coupons, brochures, privacy notices, social media pages or accounts, and physical or digital forms of a PIC or PIP.

**SECTION 3. *On-the-spot Privacy Sweep.*** – The CMD may also conduct on-the-spot Privacy Sweep on the premises, pop-up stores, kiosks, or stalls of a PIC or PIP where personal data is processed. The Privacy Sweep shall be limited to public areas and publicly available or accessible information. The CMD may verify the PIC or PIP’s compliance by examining all physical or digital forms, including, but not limited to data processing systems, logbooks, raffle coupons, brochures, and posters used in the PIC or PIP’s operations.

**SECTION 4. *Issuance of Warning Letter or Notice of Documents Submission.*** –

- a. Warning Letter: when applicable – The CMD shall issue a Warning Letter in the following instances:
  - i. If after a Privacy Sweep, the CMD discovers data privacy issues involving a

- PIC or PIP who has not yet registered or whose registration has expired in accordance with the relevant NPC Circular on Registration; or
- ii. If the CMD determines that the risk to the rights and freedoms of a data subject is present, and requires the PIC or PIP's urgent and immediate action.
- b. Notice of Documents Submission: when applicable – The CMD shall issue a Notice of Document Submission in the following instances:
- i. If after a Privacy Sweep, the CMD discovers that the PIC or PIP has failed to demonstrate substantial compliance with the DPA, its IRR, and other NPC issuances;
  - ii. If the CMD requires additional information to fully determine the PIC or PIP's level of compliance; or
  - iii. If the CMD requires further verification to determine if the PIC or PIP has embedded data privacy policies and data protection measures in its operations.

**SECTION 5. Review and assessment of documents submitted by the PIC or PIP.** – The Evaluating Officer shall review the sufficiency of the documents submitted by the PIC or PIP and determine other documents necessary to assess the PIC or PIP's compliance. The PIC or PIP may be directed to submit additional documents.

The CMD shall monitor all compliance of the PIC or PIP, including the submission within the periods provided in the NPC's issuances on compliance checks and the subsequent extensions allowed under Section 6 of this Rule.

**SECTION 6. Request for extension that shall be resolved by CMD.** – If the PIC or the PIP requests for additional time to comply with the Warning Letter, Notice of Documents Submission, Deficiency Report, or other orders issued by the CMD, the CMD may grant the request: Provided, that the PIC or PIP shall submit a formal letter with a justification for the extension, signed by the Data Protection Officer (DPO) or head of the organization, requesting for additional time which shall not exceed a cumulative period of thirty (30) calendar days counted from the date of the initial request. In case of refusal of the request for extension, the CMD shall send the denial of the request for extension and order the PIC or PIP to submit the same immediately.

**SECTION 7. Failure of the PIC or PIP to comply with the Warning Letter.** – If the PIC or PIP fails to comply within seven (7) calendar days from receipt of the Warning Letter, the CMD shall order the PIC or PIP to show valid cause why it should not be subject to the NPC's issuance on administrative fines and other actions that the Commission may deem proper to ensure compliance with the law.

**SECTION 8. Failure of the PIC or PIP to comply with the Notice of Documents Submission.** – If the PIC or PIP fails to comply within fifteen (15) calendar days from receipt of the Notice of Documents Submission, the CMD shall order the PIC or PIP to show valid cause why it should not be subject to the NPC's issuance on administrative fines and other actions the Commission may deem proper to ensure compliance with the law.

**SECTION 9. Show cause order for non-compliance with the mandatory registration requirement of the NPC.** – If based on the findings in the Privacy Sweep conducted by the CMD, the PIC or PIP is subject to mandatory registration but has failed to register, the CMD shall issue a show cause order for non-registration directing the

PIC or PIP to register its DPO and Data Processing Systems within five (5) calendar days from receipt of the order. Non-compliance with the show cause order may subject the PIC or PIP to administrative fines and other actions the Commission may deem proper to ensure compliance with the law.

**SECTION 10. Conduct of On-Site Visit (OSV).** – The CMD shall conduct an OSV to the PIC or PIP’s principal place of business or where personal data is processed in cases where there are persistent issues<sup>9</sup> or substantial findings of non-compliance with the obligations indicated in the DPA and NPC issuances.

Authorized personnel of the NPC shall conduct a focused inspection on the relevant issues within the premises of a PIC or PIP that may include presentation of documents or records, visits to selected departments or units wherein processing of personal information are undertaken, taking of photos and videos for monitoring purposes, and interviews of relevant personnel tasked to handle personal information processed by the PIC or PIP subject to the Compliance Check.

The CMD may, in its discretion, directly conduct an OSV if it determines that the totality of circumstances warrant such action, taking into account the succeeding provision.

**SECTION 11. Considerations for the conduct of Compliance Checks.** – A PIC or PIP may be subject to a Compliance Check based on any of the following considerations:

- a. Level of risk to the rights and freedoms of data subjects posed by personal data processing by a PIC or PIP;
- b. Reports received by the NPC against the PIC or PIP, or its sector;
- c. Non-registration of a PIC or PIP that is subject to the mandatory registration requirement as provided under NPC Circular on Registration of Data Processing System;
- d. Unsecured or publicly available personal data found on the premises and on the internet that may be traced to a PIC or PIP;
- e. Other considerations that indicate non-compliance with the DPA, IRR, or NPC issuances; and
- f. When, in the discretion of the CMD, there is an urgent need to ensure the protection of voluminous personal data records and the same can only be done by actual physical inspection of said records within the PIC’s or PIP’s office premises.

In cases where the CID is investigating or commencing an investigation against a PIC or PIP undergoing or scheduled for a Compliance Check, the Compliance Check shall be held in abeyance and the investigation shall be given precedence until such investigation has been concluded or submitted further for adjudication.

**SECTION 12. Service of orders.** – The CMD shall send an order to a PIC or PIP on the conduct of a Compliance Check through the electronic mail address used at the time it registered with the NPC. Such order shall be deemed received on the next business day: Provided, for unregistered organizations, the order shall be sent to any publicly available email address that may be found on websites or other social

---

<sup>9</sup> Persistent issues pertain to the inadequate implementation of security measures to address the heightened risk to the rights and freedoms of data subjects.

media pages or accounts and it shall be addressed to the head of the organization.

A PIC or PIP shall take the necessary steps to ensure that its registered e-mail address is working and able to receive the order promptly.

***SECTION 13. Notice of On-Site Visit.*** – A notice of OSV shall be issued by the CMD to the PIC or PIP at least five (5) days before such visit. The notice shall include a list of required documents to be submitted by the PIC or PIP at least three (3) days prior to the OSV.

The CMD shall present the physical copy of the notice and provide the list of authorized personnel of the NPC to conduct the OSV. The authorized NPC personnel shall wear their identification cards at all times.

***SECTION 14. Issuance of Deficiency Report.*** – The CMD shall issue a Deficiency Report based on the determination from the OSV that there are existing gaps in the PIC or PIP’s compliance with the DPA, its IRR, and NPC issuances.

***SECTION 15. Issuance of Notice of Deficiencies.*** – If the PIC or PIP fails to address the issues raised in a Deficiency Report or is determined to be non-compliant with the DPA, its IRR, and other issuances of the NPC after being subjected to any of the modes of Compliance Checks, the CMD shall issue the Notice of Deficiencies indicating the period of time within which to correct the identified deficiencies, which shall not be less than ten (10) days from receipt of the Notice.

***SECTION 16. Issuance of Compliance Order.*** – The Commission shall issue a Compliance Order in any of the following instances:

- a. After the lapse of the period provided in the Notice of Deficiencies and no action was taken by the PIC or PIP to correct the identified deficiencies;
- b. After the lapse of the period provided in the Notice of Deficiencies and such identified deficiencies persist.  
If the persistence of the deficiencies is due to the considerable period of time or resources needed to implement the necessary remediation measures, the timeline to complete such measures, as approved by the Commission, shall be embodied in a Compliance Order;
- c. In the course of the conduct of an OSV, the PIC or PIP refuses or fails to provide access to premises, records or prevents the conduct of the inspection; or
- d. In the course of the conduct of the on-the-spot Privacy Sweep, the PIC or PIP refuses or prevents the conduct of the inspection on otherwise publicly available areas or information.

Compliance Orders shall state the deficiencies remaining or actions to be taken, the period within which to undertake the corrections ordered by the Commission, and the period to report such actions.

***SECTION 17. Issuance of other orders.*** – The Commission, through the CMD, may issue pertinent orders in connection with the conduct or furtherance of a Compliance

Check or the assessment of any PIC or PIP’s compliance with any orders in relation thereto.

**SECTION 18. Refusal to undergo Compliance Check.** – A PIC or PIP who, without good reason and despite due notice, refuses or prevents the CMD from performing a Compliance Check may be subject to appropriate penalties and sanctions as may be allowed by law. In case of refusal, the following provisions shall govern:

- A. Action to be taken upon refusal or failure to comply with documents submission. Refusal or failure to submit the requested documents or policies within the period stated in the notice or order shall subject a PIC or PIP to an OSV from the CMD, enforcement actions, and imposition of fines in accordance with the NPC’s issuance on administrative fines and other actions the Commission may deem proper to ensure compliance with the law.
- B. Action to be taken upon refusal or failure to provide access to premises or records during an OSV and on-the-spot Privacy Sweep. Refusal or failure to provide access to premises or records during an OSV and on-the-spot Privacy Sweep shall subject a PIC or PIP to a Compliance Order, enforcement actions, and imposition of fines in accordance with the NPC’s issuance on administrative fines and other actions the Commission may deem proper to ensure compliance with the law.
- C. Failure or refusal to provide an explanation to Compliance Orders. Refusal or failure to submit an explanation to the order cited in the preceding paragraphs, or if the explanation does not present a compelling reason to justify such refusal or failure, may subject a PIC or PIP to contempt proceedings, as may be permitted by law, before the appropriate court, or such other actions as may be available to the Commission.

**SECTION 19. Certificate of No Significant Findings.** – The CMD shall issue a Certificate of No Significant Findings to a PIC or PIP that has undergone document submission or an OSV, where no substantial deficiencies were found, or the deficiencies identified in the Deficiency Report or Notice of Deficiencies have already been addressed to the satisfaction of the NPC

The issuance of this certificate is without prejudice to any other recommendation being made by the CMD for the improvement of the PIC or PIP’s compliance with the DPA, IRR, and NPC issuances. The issuance of this certificate does not bar an investigation for any possible liability arising from complaints and/or personal data breaches filed before the NPC.”

**SECTION 11.** Rule XII of the 2021 NPC Rules of Procedure is hereby amended and re-numbered to read as follows:

### **“RULE XIII – 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 NPC issuances pertaining to the matter.

**SECTION 3. Procedure for breach notification.** – Procedure for data breach notification to the Commission shall be governed by the NPC issuances pertaining to the matter.

**SECTION 4. Request for case files.** – Copies of the case files may be requested by any party to the complaint or their authorized representative, lawful heirs, and assigns, in accordance with Section 17 of the DPA, or successors-in-interest, by filling-out the request form before the General Records Unit of the NPC. The request for case files may be in the form of a physical copy or an electronic copy, at the option and cost of the requesting party. Provided, that the representative is authorized by a special power of attorney. Provided further, that in case where a party is a juridical person, the representative is authorized by a Board Resolution contained in a duly notarized Secretary's Certificate or its equivalent for a government agency<sup>10</sup>. Provided finally, that in case where the files are requested by the heirs, assigns, or successors-in-interest, proof of authority or relationship must be presented.

**SECTION 5. Procedure for requests for advisory opinion.** – Procedure for requests for advisory opinion shall be governed by NPC issuances pertaining to the matter.

**SECTION 6. Procedure for enforcement of administrative fines.** – Procedure for the enforcement of administrative fines shall be governed by NPC issuances pertaining to the matter.

**SECTION 7. 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 issuances pertaining to the matter.

Notwithstanding any provision of these Rules, the conduct of preliminary conferences, summary hearings, mediation conferences, investigations, clarificatory hearings, and all other hearings may be conducted through videoconferencing technology at the discretion of the concerned division or Commission.

**SECTION 8. Repealing clause.** – NPC Circulars No. 2016-04 and 2018-03 are hereby repealed. All other issuances by the Commission which are contrary to the provisions of these Rules are also hereby repealed or amended accordingly.

**SECTION 9. Amendments.** – These Rules or any of its portion may be amended or supplemented by the Commission.

**SECTION 10. Application of Rules of Court.** – The Rules of Court shall apply in a suppletory character and whenever practicable and convenient.

**SECTION 11. Effectivity.** – These Rules shall take effect fifteen (15) days after publication in a newspaper of general circulation.”

---

<sup>10</sup> This includes a department, bureau, office, instrumentality, government-owned or controlled corporation, local government, state university and college, or a distinct unit in it.

**SECTION 12. *Repealing Clause.*** – The Rules not included herein and amended accordingly shall remain in force and full effect. If any part of this issuance is declared unconstitutional or invalid, such provision/s thereof not so declared shall remain valid and subsisting.

**SECTION 13. *Effectivity.*** – These amendments shall take effect fifteen (15) days after its publication in a newspaper of general circulation.

Approved:

**SGD.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**SGD.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

**SGD.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner



# ADVISORY OPINIONS





# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-001<sup>1</sup>

17 January 2023

[REDACTED]

## **Re: DISCLOSURE OF CONDOMINIUM UNIT OWNERS' PERSONAL DATA AND RELATED DOCUMENTS.**

Dear [REDACTED]

We respond to your request for an Advisory Opinion on whether your client may compel the condominium developer and the Register of Deeds to disclose the following information without violating the Data Privacy Act of 2012 (DPA):

- 1.) Condominium Certificate of Title (CCT) numbers, purchase agreements by the condominium developer to the condominium corporation;
- 2.) Traceback of CCT numbers from the Register of Deeds; and
- 3.) Delinquent unit owners by posting via bulletin board and elevator notice their unit numbers and the amount due by a condominium corporation.

You state in your letter that The Infinity is a condominium developed by Nuvoland Philippines, Inc. (NPI). Your client, The Infinity Condominium Corporation (TICC), is the condominium corporation in charge of managing the affairs of The Infinity by virtue of a Deed of Conveyance between NPI and TICC.

Conflict arose when the unit owners/tenants of The Infinity defaulted on their payments of association dues and other assessments. You further stated that TICC is currently facing difficulties in the collection and enforcement of payments from the delinquent unit owners since their whereabouts are unknown to TICC since the owners' information previously shared by NPI are incomplete or outdated.

To enforce the collection of dues and other assessments, TICC requested the Deeds of Sale and/or Reservation Agreements of the Unit Owners and CCT numbers from NPI. The request was denied on the reasoning that the consent of the unit owners is

<sup>1</sup> Tags: lawful processing; legal claims; contractual obligation; condominium corporation.

required before the request may be granted. NPI suggested to request the said documents directly from the unit owners. As an alternative course of action, TICC requested from the Register of Deeds of Taguig City the CCT numbers of the condominium units of The Infinity, but such request was also denied on the ground of data privacy.

You now ask if the NPI and the Register of Deeds' denial of TICC's requests are in order. *Personal information; Sensitive personal information; Lawful processing*

The DPA applies to the processing of all types of personal information and sensitive personal information (collectively, personal data), and to any natural or juridical person involved in the processing of personal data.<sup>2</sup> Clearly, the scope of the DPA is limited only to the processing of personal data or data relating to natural persons or individuals. Data relating to juridical entities such as corporation name, address, etc., falls outside the scope of the DPA.

Documents such as CCTs, purchase agreements and tracebacks of CCTs, by themselves, are not automatically considered personal data. However, such documents may contain personal data such as name, address, marital status, and citizenship, among others. If the registered owner/s are natural persons, then the processing of those documents fall within the scope of the DPA. However, if the subject property is registered to a juridical person, then processing of the same does not fall within the ambit of the DPA.

We emphasize that CCT numbers, although distinct and unique, do not identify the registered owner of the property or any specific individual for that matter. Instead, the CCT number is issued to identify the property, not the individual. Hence, CCT numbers by themselves are not considered personal information. Accordingly, it also cannot be considered as sensitive personal information since under Section 3 (I)(3) of the DPA, government-issued numbers should be peculiar to an individual which is not the case with CCT numbers. However, we note that CCT numbers can only be regarded as personal informa

tion if the actual certificate of title, in its entirety, is considered. This is the only time that a CCT number can be correlated with the name of the registered owner, a natural person, and therefore, indirectly identify such person. Under this context, the lawful processing of personal information shall have basis under Section 12 (f) of the DPA:

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

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

The disclosure of the requested documents and CCT numbers are necessary in order for TICC to establish its legal claims for unpaid dues and other assessments against the unit owners concerned.

---

<sup>2</sup> 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).

Given the current scenario, Section 13(f) of the DPA may be applicable:

“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:

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

The wording of Section 13(f) of the DPA is interpreted to mean that a court order or an existing court proceeding is not required for this lawful basis to apply. NPC was able to clarify this in the case of BGM v. IPP<sup>3</sup>:

“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.” (underscoring supplied)

In the same case, the Commission had the occasion to explain that the protection of lawful rights and interests under Section 13 (f) of the DPA is considered as legitimate interest pursuant to Section 12 (f) of the DPA:

“Based on the foregoing, the disclosure to be made by the Respondent of the information of the recipient of Complainant’s personal information, for purposes of identification of the person liable for the alleged fraud, sans the latter’s consent, is necessary for the 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 dis-

<sup>3</sup> National Privacy Commission, BGM v. 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).

closed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

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

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

(Underscoring supplied)"

TICC is tasked to manage the affairs of The Infinity which includes the collection of dues and assess delinquent unit owners. Such act, along with any other enforcement actions that TICC may have against the delinquent unit owners, may be considered as an establishment or exercise of a legal claim under Section 13(f) of the DPA. As explained above, a court order or a pending court proceeding is not required. With this, the requested documents may be lawfully disclosed to TICC, subject to the respective internal policies and rules of NPI and the Register of Deeds on disclosure (e.g., verification of identity, required documents). However, we wish to emphasize that NPI and the Register of Deeds

should establish a system to ensure that the requested information shall be limited only for the legitimate interests stated by the requesting party, and not be subject to abuse. As we stated in Advisory Opinion No. 2022-05:<sup>4</sup>

"LTO must establish a system for handling these types of requests for information to avoid the possibility of abuse. As a request for personal information for the filing of a legal action falls under the legitimate interests of the requesting party, the system must assess the request if it satisfies the three aforementioned tests. It must also provide for a mechanism to ensure that the information to be disclosed will only be used for the purpose/s indicated. In Advisory Opinion No. 2021-044, it was recommended that in case a request for personal information is granted, the requesting party should be required to sign an undertaking that the information will only be used for the purpose that was declared: Should the CHMSC grant the request, it is suggested that the Requesting Party be required to sign an undertaking that the use of the documents will only be for the purpose of filing a complaint with the Ombudsman and that the proper disposal thereof is ensured if he does not push through with the filing of the complaint. Further, the undertaking must include a clause to the effect that the requestor acknowledges that he becomes a PIC by his receipt of the requested documents and therefore has the obligations of a PIC as prescribed under the DPA. Thus, LTO should similarly require a requesting party to sign an undertaking that the

information that will be acquired will only be used for the purpose which was declared and authorized."

Further, we note that documents such as Deeds of Sale and Reservation Agreements may contain information which may not be relevant to TICC's claims. The principle of proportionality provides that "the processing of information shall be adequate, rele-

<sup>4</sup> NPC Advisory Opinion No. 2022-05, 24 February 2022.

vant, 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.”<sup>5</sup>The principle of proportionality necessitates that only the information requested and necessary for the purpose indicated should be processed. With this, NPI may opt to conceal or redact such information that are not relevant to TICC’s claims upon the documents’ disclosure to TICC.

*Contractual obligation; adherence to the data privacy principles; proportionality.*

Condominium unit numbers are considered personal information under the DPA since it can directly and certainly identify the identity of the unit owner when put together with other information.<sup>6</sup>Hence, the processing or posting thereof in public spaces within the condominium must comply with the requirements of Section 12 of the DPA. We understand that TICC is contemplating on posting and/or publishing in public spaces within the condominium building the unit numbers and corresponding amounts due from the delinquent owners. While we recognize that Section 6 of the TICC By-Laws allows TICC to file an adverse claim for delinquent units,<sup>7</sup>this does not equate to a legal obligation contemplated under Section 12 (c) of the DPA. When a PIC claims lawful processing on the basis of a legal obligation, the burden is on the PIC to show that all that is required by that particular lawful criterion is present. A PIC must be able to prove that the legal obligation it cites as basis exists and applies to the processing it performed, and that the processing is necessary to comply with the legal obligation.<sup>8</sup>

Instead, Section 12 (b) of the DPA on contractual obligation may be considered as a more appropriate lawful basis, *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:

(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.

In your letter, you stated that the Amended Master Deed provides that an owner, upon acceptance of the unit or the execution of the Deed of Absolute Sale, whichever comes first, automatically becomes a member of the Condominium Association and agrees to pay to TICC the owner’s pro-rata share in the expenses of The Infinity. This creates a contractual obligation contemplated by Section 12 (b) of the DPA on the part of the unit owner and may allow for the lawful processing of personal information.

However, we note that although there is lawful basis for the processing of personal information, the other requirements of the DPA must still be complied with to ensure the protection of personal data and uphold the rights of data subjects.

This means that TICC, as a personal information controller, still has the responsibility to ensure that personal data is processed lawfully and fairly. There must be strict adher-

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

6 Data Privacy Act of 2012, 3(g).

7 Section 6 of the TICC By-Laws, as provided in the letter request of Duran & Duran-Schulze Law.

8 NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015, 03 February 2022, page 7

ence with the basic privacy principles of transparency, proportionality, and legitimate purpose.

We emphasize the principle of proportionality which requires that the processing of personal data shall be adequate, relevant, suitable, necessary and not excessive in relation to the declared and specified purpose.<sup>9</sup> In this regard, TICC should only disclose such personal data which will help in the achievement of its responsibility as condominium corporation to collect the dues and assessments from the delinquent owners. Further, TICC should consider less intrusive means of identifying and/or notifying the unit owners. As stated in an NPC Decision bearing similar circumstances:

“The PIC should only process as much information as is proportional or necessary to achieve its clearly defined and stated purposes. In this case, it is the collection of unpaid dues provided under a valid contract with its unit owners. While it is necessary to process the delinquent unit owners’ personal information in order to assess and collect payments pursuant to a contract, the processing in the form of issuing the letter was neither necessary nor proportional. The purpose of the letter was not for the collection of delinquent dues. Rather, the evidence on record shows that DSL disclosed Complainants’ personal information as delinquent unit owners to cast doubt on their capability to manage the affairs of the condominium corporation in light of the recently held election of the Board of Directors.”<sup>10</sup>

In the current scenario, publication/posting of unit numbers in public spaces within the condominium may be too intrusive for the declared purpose and may not even be a guarantee that such posting/publication will lead TICC to the unit owner.

On the other hand, the posting/publication must only be considered as a last resort if there is absolutely no way for TICC to get hold of the requested information and documents. In such instance, the processing of personal information must still adhere to the proportionality principle wherein TICC must only disclose such personal information that is adequate and necessary for the declared purpose, which is the collection of unpaid dues.

We would like to emphasize that, as a regulator, the National Privacy Commission (NPC) does not issue a “legal confirmation.” The NPC’s Advisory Opinions do not serve to confirm the legal opinions/positions of its stakeholders. Should a stakeholder already have an opinion or decision regarding its processing activities, the “confirmation” of NPC is not required nor given. Instead, NPC’s Advisory Opinions provide guidance on the interpretation of the DPA, its IRR and other issuances of the NPC.

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

Please be guided accordingly.

---

9 Data Privacy Act of 2012, 11 (d).  
10 NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015, 03 February 2022, page 8.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-002<sup>1</sup>

18 January 2023

[REDACTED]

## Re: DISCLOSURE OF TAX DECLARATIONS OF REAL PROPERTIES AND OTHER RELATED DOCUMENTS

Dear [REDACTED]

We respond to your request for an Advisory Opinion on whether the Municipal Assessor's Office may release copies of tax declarations to persons other than the registered owner, or his/her authorized representative, without the need for the registered owner's consent.

You state in your letter that the Office of the Municipal Assessor of Oton, Iloilo (Municipal Assessor) received a request from the Department of Science and Technology (DOST) to be furnished copies of tax declarations, statements of account of real property taxes, and location maps of real properties allegedly owned or mortgaged to the now defunct Technology Resource Center (TRC). The request involves thirteen (13) pieces of real property, twelve of which are allegedly registered under Polyshell Industries Philippines, Inc. (Polyshell) and one (1) registered to certain individuals.

DOST's request stems from the issuance of Governance Commission on Government-Owned and Controlled Corporations (GCG) Memorandum Order (MO) No. 2015-11 dated 27 October 2015, which states that the subject properties are now allegedly under the administration of DOST.

You also state that the counsel of Premier Islands Management Corporation (Premier), the alleged current owner of eleven (11) of the subject properties, is preventing the Municipal Assessor from releasing to the DOST copies of the requested documents. The counsel of Premier is claiming that disclosure of the requested documents to DOST would violate the Data Privacy Act of 2012 (DPA) and its Implementing Rules and Regulations (IRR) since it contains personal data.

You thus ask if the position of Premier's counsel is legally proper.

### *Scope of the DPA*

For perspective, the DPA applies to the processing of all types of personal information

<sup>1</sup> Tags: scope of the DPA; sensitive personal information; tax declarations; public documents.



and sensitive personal information (collectively, personal data) and to any natural or juridical persons involved in the processing of personal data.<sup>2</sup>

The concept of processing of personal data under the DPA is limited only to natural persons or individuals. Data pertaining to juridical entities (e.g., corporation name, address, financial information) fall outside the scope of the DPA and are not considered as personal data.

The owner of the subject real properties in this case (i.e., Premier) is a juridical entity. As such, it is not considered as a data subject entitled to protection under the DPA and its IRR. Hence, the processing of information such as tax declarations, statements of account and location maps relating to Premier, a juridical entity, does not fall within the scope of the DPA.

*Lawful processing; functions of public authority; statutory mandate*

For the property registered to natural persons, however, the tax declaration and the other requested documents contain personal data. In which case, the DPA is applicable and the processing of personal data must find lawful basis under the DPA.

The DPA allows the processing of personal data subject to compliance with the law and strict adherence to the principles of transparency, legitimate purpose, and proportionality. For the processing of personal information, Section 12 (e) 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 condition 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” (Emphasis supplied).<sup>3</sup>

In the same vein, Section 13(b) of the DPA allows for the processing of sensitive personal information, 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:

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;<sup>4</sup>

<sup>2</sup> 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).

<sup>3</sup> *Id.* 12 (e).

<sup>4</sup> *Id.* 13 (b).

GCG MO 2015-11 provides that all remaining functions of TRC shall be transferred to the DOST as its supervising agency. It further provides that the custody of assets of TRC shall be turned over to DOST to prevent their dissipation and shall take all proper and necessary steps to protect the interests of the government in the winding down of its operations including the preservation of its assets.

Taking these into consideration, the requested documents such as the tax declarations, statements of account and location maps are necessary for DOST to implement its mandate to preserve the assets of TRC. This means that a government agency, such as DOST, may process personal data pursuant to its statutory mandate, even without the consent of the data subject, in the exercise of its regulatory function. Hence, the requested documents may be released to DOST subject to the principles of proportionality or processing only such personal data necessary for the stated purpose, and the concomitant responsibility of the implementation of the appropriate and reasonable physical, organizational, and technical security measures to protect data.

We note that under the current scenario, consent may not be the appropriate lawful basis in the processing of data considering that the processing is necessary for the fulfillment of DOST's statutory mandate.

*Nature of tax declarations and Tax Identification Number (TIN); processing of sensitive personal information*

We note that while a tax declaration, in itself, is not automatically considered sensitive personal information, the Tax Identification Number (TIN) issued to an individual is classified as sensitive personal information. Thus, the processing of tax declaration of properties belonging to natural persons fall within the ambit of the DPA and may only be processed under the circumstances provided under Section 13 of the DPA.

On the other hand, a TIN issued to a juridical entity such as the TRC or DOST is not considered as sensitive personal information under the DPA. The scope of the DPA only extends to natural persons, considered as data subjects, whose personal data are sought to be protected.

As such, the classification of TIN as sensitive personal information under the DPA is not applicable in this instance since the subject properties are allegedly owned by a corporation. Consequently, the tax declarations of the subject properties will contain the name and address of the owner-corporation, including its TIN, which are not treated as personal data under the DPA. In this case, the only personal data contained in the tax declarations would be the name and signature of the government employees who prepared and approved the same.

We emphasize that the processing of sensitive personal information is allowed under the DPA, subject to compliance with the criteria provided by law. As stated earlier, Section 13(b) of the DPA recognizes the processing of sensitive personal information when it is provided for by existing laws and regulations.<sup>5</sup>

Under Section 4(a)(4) of the DPA, any information about any individual who is or was an officer or employee of a government institution that relates to the position or functions

---

<sup>5</sup> Data Privacy Act of 2012, 13 (b) (2012)

of the individual, such as the name of the individual on a document prepared by the individual in the course of employment with the government, falls outside the scope of the DPA. In this instance, the name and signature of the government employees who prepared and approved the tax declarations would fall squarely under this provision, and as such, outside the scope of the DPA.

We also emphasize that although tax declarations contain government-issued identifiers, such identifiers pertain to the lot itself and not to the registered owner/s. Since the scope of the DPA pertains to personal data, the data and its unique identifiers, if any, should be peculiar to an individual. In this case, since the identifiers refer to the lot and not to the individual, it does not fall under the ambit of personal data, as defined under the DPA. Further, the claim that since the statement of account of real property and location map emanate from the tax declaration and thus, must also be treated as sensitive personal information, is erroneous. To reiterate, tax declarations are not considered sensitive personal information in and of itself. The determination of whether the contents of a document is personal information or sensitive personal information depends on what is actually contained in a document and not where such document emanates from.

In the case of *BGM vs. IPP*<sup>6</sup>, the Commission was able to clarify that the term “processing as necessary for the establishment of legal claims” does not require an existing court proceeding.

“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.” (underscoring supplied)

Given the above citation and assuming for the sake of argument that the tax declarations and requested documents do contain personal data, DOST’s request for copies of the tax declarations and other related documents, pursuant to its mandate to preserve the real properties mortgaged to TRC, may be considered as an establishment or exercise of a legal claim. Hence, such processing may rely on Section 13(b) of the DPA as

---

<sup>6</sup> 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).

lawful basis.

We note that although there may be lawful basis in the processing or disclosure of documents containing personal data, personal information controllers such as the DOST must still comply with the other requirements of the DPA. In particular, the DOST must ensure that any disclosure of documents containing personal data should be limited strictly to fulfilling its mandate, which is to preserve the remaining assets of the TRC. Further, personal information controllers must also be mindful of the manner of disclosure of the requested documents through the implementation of reasonable and appropriate physical, organizational and technical security measures to ensure the protection of personal data, which are also stated in the DPA.

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

Please be guided accordingly.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-003<sup>1</sup>

18 January 2023

[REDACTED]

## **Re: DISCLOSURE OF PROPERTY INFORMATION THROUGH THE LAND REGISTRATION AUTHORITY'S GEO-SPATIAL QUERY SERVICE**

Dear [REDACTED]

We respond to your request for clarification on the legality of providing government and private sector clients with information on titled properties using the Land Registration Authority's (LRA) Geo-spatial Query Service (GQS).

We understand that the GQS is a service offered by the LRA primarily to other government agencies. The GQS provides information on titled properties, particularly when the requesting entity does not know the title number of the property but has an identified point-of-interest and/or alignment of interest where properties to be mapped are generally located. An example is the identification of properties that will be affected by road infrastructure projects of the Department of Works and Highways (DPWH) or transmission lines of power corporations. The information provided consists of the registered name of the owner, plan, lot, and block of the property. Recently, the GQS has been offered to the private sector undertaking government infrastructure projects. Y

You thus ask if the LRA can legally provide the information mentioned above to the requesting entity, specifically to the private sector.

*Scope of the DPA; lawful basis for processing;  
legal obligation; fulfillment of mandate.*

At the outset, we wish to clarify that the Data Privacy Act of 2012 (DPA) <sup>2</sup>only applies to the processing of personal data of natural persons, and not to information concerning

<sup>1</sup> Tags: personal data; lawful processing; titled lands; public authority mandate; legal obligation.

<sup>2</sup> 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).

juridical entities such as corporations, associations, and partnerships.

Relating the above to your query, if the property involved is registered to a natural person, then the disclosure of personal information<sup>3</sup> (i.e., the name of the individual registered owner) may be allowed under Section 12 of the DPA. In particular, if the request is made by a government entity, the disclosure of the name of the registered owner may be based on Section 12 (c) and (e) of the DPA, *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:

xxx

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

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;

(Underscoring supplied).

The DPA is not intended to hinder government agencies from fulfilling their respective mandates and legal obligations. Government entities, such as the DPWH, are tasked to deliver public services pursuant to their mandate and /or existing laws and regulations. We acknowledge that verification of information about land is necessary to enable the DPWH to deliver on its mandate effectively. Be that as it may, while the DPWH may have legal basis to process personal data, it is still required to ensure that its mandate supports the particular processing involved, and that it is accomplished within the limits of such mandate.

*Disclosure to private entities; compliance with a legal obligation; proportionality.*

As mentioned in your letter, the GQS is now offered to private entities undertaking government infrastructure projects. These private entities may likewise rely on Section 12 (c) of the DPA where the processing of personal data is necessary for compliance with a legal obligation.

We have recognized as lawful the processing of personal information by private companies pursuing government projects based on legal obligation. In *Advisory Opinion No. 2020-036*,<sup>4</sup> we recognized that the National Grid Corporation of the Philippines (NGCP) has the obligation under its legislative franchise to identify the current owners

<sup>3</sup> 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.”

<sup>4</sup> National Privacy Commission, NPC Advisory Opinion No. 2020-036 (8 September 2020).

and possessors of properties subject to acquisition.<sup>5</sup> Similarly, in *Advisory Opinion No. 2021-027*,<sup>6</sup> we confirmed that San Miguel Aerocity, Inc. (SMAI) may be provided with documents and processes, including those that pertain to personal data, due to its obligations under R.A. No. 10752 or the Right-of-Way Act.<sup>7</sup> However, we also emphasized in both instances that while NGCP and SMAI have legal grounds to process personal data, such grounds should be duly documented.

In *RLA v. PLDT Enterprise*,<sup>8</sup> the NPC discussed the elements that should exist for valid processing based on a legal obligation, viz.: “(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.”<sup>9</sup>

As long as the elements cited above are complied with, the LRA may disclose requested information from the GQS to public and private requesting entities, as long as the personal information will be used in fulfillment of a statutory mandate or fulfillment of legal obligation. As the personal information controller (PIC) providing the information, the LRA has the concurrent responsibility to assess and document whether the requesting entities truly have a legal mandate or obligation to fulfill, and if the disclosure of the names of registered owners is necessary for the fulfillment of the mandate or obligation. In its assessment, the LRA may request certain documents from the public and private entities as evidence of their mandate or obligation.

We take this opportunity to emphasize that in all instances, the principle of proportionality should still be adhered to. Proportionality requires that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.<sup>10</sup>

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

Please be guided accordingly.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

---

5

*Id.*

6

6 National Privacy Commission, NPC Advisory Opinion No. 2021-027 (17 July 2021).

7

*Id.*

8

National Privacy Commission, *RLA v. PLDT Enterprise* [NPC Resolution No. 2018-010] (10 December 2021)

9

*Id.*

10

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

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-004<sup>1</sup>

02 February 2023



## Re: DISCLOSURE OF SUBSCRIBER'S DATA PURSUANT TO REVENUE REGULATION NO. 09-2022

Dear 

We respond to your inquiry on the data privacy implication of the Bureau of Internal Revenue's (BIR) request for disclosure of the registered addresses and email addresses of Globe Telecom Inc.'s (Globe) subscribers covered by the BIR Revenue Regulation (RR) No. 09-2022.

We understand that the TRAIN Law mandates the e-Invoicing and e-Sales reporting system to be implemented on or before 01 January 2023.<sup>2</sup> Under this program, covered taxpayers are required to electronically report its sales data to the BIR through their respective electronic point of sales systems or computerized accounting systems.

By such mandate, the BIR issued RR 09-2022<sup>3</sup> to implement the Electronic Invoicing/Re-

<sup>1</sup> Tags: subscriber records; subscriber data; Bureau of Internal Revenue; internal revenue tax purposes; special cases; public authority.

<sup>2</sup> See TRAIN Law, Section 74. A new section designated as Section 237-A under Chapter II, Title IX of the NIRC, as amended, is hereby inserted to as follows:

Sec. 237-A. Electronic Sales Reporting System.— Within five (5) years from the effectivity of this Act and upon the establishment of a system capable of storing and processing the required data, the Bureau shall require taxpayers engaged in the export of goods and services, and taxpayers under the jurisdiction of the Large Taxpayers Service to electronically report their sales data to the Bureau through the use of electronic point of sales systems, subject to rules and regulations to be issued by the Secretary of Finance as recommended by the Commissioner of Internal Revenue: Provided, That the machines, fiscal devices, and fiscal memory devices shall be at the expense of the taxpayers.

The data processing of sales and purchase data shall comply with the provisions of Republic Act No. 10173, otherwise known as the "Data Privacy Act" and Section 270 of the NIRC, as amended, on unlawful divulgence of taxpayer information and such other laws relating to the confidentiality of information.

The Bureau shall also establish policies, risk management approaches, actions, trainings, and technologies to protect the cyber environment, organization, and data in compliance with Republic Act No. 10175 or the "Cybercrime Prevention Act of 2012."

<sup>3</sup> BIR Revenue Regulation No. 09-2022, entitled, Prescribing Policies and Guidelines for the Admissibility of



ceipting and Sales Reporting System (EIS). Under the EIS, the BIR will store and process the sales data of covered taxpayers using BIR's Sales Data Transmission System and issue the corresponding sales documents through its web-based issuance facility. The EIS is primarily intended to ensure the integrity and reliability of the sales and purchases data that will be generated and verified therefrom.

We note further that the implementation of the BIR EIS would require Globe to provide the following details to the BIR:

1. Buyer Information
2. Buyer TIN
3. Branch Code
4. Registered Name
5. Business Name/Trade Name
6. E-mail Address
7. Registered Address

While the above information is not explicitly enumerated in RR 09-2020, you have clarified in your 20 August 2022 email that such information is being requested in the BIR's website particularly on the "e-invoice API Guide" page that shows the different e-invoices that will be generated in the EIS.<sup>4</sup>

You thus seek guidance if the BIR's request for the submission of the information above, specifically the respective email and registered addresses of Globe's subscribers, is in accordance with the DPA and its IRR. It is your position that the inclusion of the email and registered addresses may not be consistent with the principle of proportionality under the DPA given that:

- a) the requirement under Section 5 (b) of the National Internal Revenue Code (NIRC) for the disclosure to the BIR of addresses refers to the addresses of juridical persons that have a connection with the taxpayer under audit/investigation, but not the address of natural persons identified as "buyers";<sup>5</sup> and
- b) Section 113(B)(1)(4) of the NIRC limits the scope of information to be provided to the BIR in any VAT Invoice or VAT Official Receipt, to the following:

(4) In the case of sales in the amount of One thousand pesos (P1,000) or more where the sale or transfer is made to a VAT-registered person, the name, busi-

---

Sales Documents in Electronic Format in Relation to the Implementation of Sections 237, Issuance of Receipts or Sales or Commercial Invoices, and 237-A, Electronic Sales Reporting System, of the National Internal Revenue Code of 1997, as amended by R.A. No. 10963, otherwise known as the Tax Reform for Acceleration and Inclusion or the 'TRAIN Law.

<sup>4</sup> API Guide, BIR, available at <https://eis-cert.bir.gov.ph/#/apiGuide> (last accessed 22 August 2022).

<sup>5</sup> See NIRC, as amended, 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: xxx (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, 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"

ness style, if any, address and Taxpayer Identification Number (TIN) of the purchaser, customer, or client.

*Lawful processing of personal information; compliance with a legal obligation; proportionality*

Under Section 12 (c) of the DPA, there is lawful processing of personal information when it is necessary for “compliance with a legal obligation to which the personal information controller is subject.”

It appears that the BIR’s request for information, including the registered address and email address of Globe’s buyers/subscribers, is necessary to comply with the requirements of RR 09-2022 and, ultimately, the TRAIN Law.

In NPC Advisory No. 2021-045,<sup>6</sup> we recognized the authority of the BIR in the conduct of investigation for tax purposes and confirmed that Globe may disclose the personal data requested subject to proportionality.

In the same vein, Globe must provide the personal data requested to comply with RR 09-2022. Requiring the registered address and email address of buyers/subscribers who are natural persons, is not disproportionate per se to the purpose of the tax law and BIR regulation especially since no sensitive personal information is involved.

We note that the registered address is information that is currently being required in existing paper-based documentary submissions. Furthermore, the email address serves as the taxpayer’s contact information that is reasonably necessary since the BIR shifted to a digital platform.

These are information essential for the BIR to fulfill the purpose of the EIS, that is to ensure the integrity and reliability of the sales and purchases. With the appropriate information, the BIR can check whether proper taxes are declared and paid, as well as perform its other regulatory functions.

Given the foregoing, the submission of the subscriber’s registered address and email address is considered permissible under the DPA. We note that submission of said subscriber data are necessary in compliance with the TRAIN law and BIR regulations and does not contravene the data privacy principle of proportionality.

It is worth noting that the DPA itself recognizes the necessity of personal data processing to carry out the functions of public authority. In Advisory Opinion No. 2020-16 where the Commission on Audit’s authority to process personal data in light of its constitutional mandate was duly recognized, we emphasized that the DPA shall not be used to hamper, or interfere with, the performance of the duties and functions of duly

constituted public authorities.<sup>7</sup> Thus, we take this opportunity to 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.

---

6 See: National Privacy Commission, NPC Advisory Opinion No. 2021-045 (29 December 2021).

7 National Privacy Commission, NPC Advisory Opinion No. 2020-016 (12 March 2020).

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

For your reference.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-005<sup>1</sup>

17 January 2023

[REDACTED]

## Re: BARANGAY INVENTORY OF VACCINATED POPULATION

Dear [REDACTED]

We respond to the Department of the Interior and Local Government's (DILG) request for an Advisory Opinion on the data privacy concerns regarding the proposed inventory system for the vaccinated population of barangays.

We gather that DILG Memorandum Circular (MC) No. 2022-022<sup>2</sup> was issued pursuant to the pronouncement of President Rodrigo Roa Duterte to restrain the movement of unvaccinated individuals. DILG MC 2022-02 also directs all barangays to create an inventory of vaccinated individuals within their respective barangays, which entails the collection of names, birthdays, ages and vaccination status and details. The objective is to enable the barangays to determine the number of unvaccinated individuals and restrain their movement, except to access essential goods and services.

We further understand that copies of these inventories will be provided to the DILG's City and Municipal Field Offices, while a statistical summary thereof will be submitted to the DILG Provincial and Regional Offices and the DILG Central Office. To facilitate ease and efficiency in the transfer, the DILG intends to develop an online inventory system which can be updated real time through which the barangays can upload the data collected. Summary of the same may be generated and integrated in DILG's existing online systems, accessible to DILG officials and employees which shall then be used for policy formulation.

In view of the above, your office seeks guidance on the following:

- 1.) Whether the proposed online inventory system is feasible and in line with the Data Privacy Act of 2012<sup>3</sup> (DPA);

<sup>1</sup> Tags: sensitive personal information; health data; legal mandate; proportionality.

<sup>2</sup> Entitled "Inventory of Vaccinated Population in the Barangay," issued on 18 January 2022.

<sup>3</sup> Republic Act 10173.

- 2.) On the privacy-related issues and concerns that may arise out of such system; and
- 3.) National Privacy Commission's (NPC) recommendations on how to ensure data privacy in this undertaking.

*Sensitive personal information; lawful processing; regulatory mandate.*

Under the DPA, the name of an individual is considered personal information. On the other hand, an individual's age, date of birth and vaccination status (since it relates to health information), are all considered sensitive personal information.<sup>4</sup>

The DPA provides for instances on when the processing of personal information and sensitive personal information (collectively, personal data) are allowed. In particular, the DPA allows for the processing of personal information when the same is necessary for compliance with a legal obligation to which the personal information controller is subject.<sup>5</sup>

On the other hand, the processing of sensitive personal information is allowed when such processing is provided for by existing laws and regulations.<sup>6</sup>

Section 4.2 of DILG MC 2022-02 provides:

4.2 All Punong Barangays are hereby enjoined to:

4.2.1. Cause the preparation of a monthly inventory of vaccinated population in the barangay indicating their status, whether with first dose only, fully vaccinated (with two doses), or with booster dose already (see attached template). Accomplished monthly inventory form shall be in the custody of the barangay for monitoring purposes. a copy of the said report shall be submitted to the DILG Field Office for consolidation not later than the 10th day of the ensuing month.

4.2.2. Closely monitor the mobility of persons yet to be vaccinated against COVID-19 and to advise them to stay at home to minimize the risk of COVID-19 transmission, provided that utmost respect for human rights is strictly adhered to.

As stated in the letter-request, DILG MC No. 2022-02 mandates Punong Barangays to create an inventory of the vaccinated population within their respective barangays. In turn, data collected will enable Punong Barangays to identify the unvaccinated individuals and closely monitor their mobility.

The processing of personal data by way of collection and inventory is, thus, in accordance with existing laws and regulations, specifically Section 16 of the Local Government Code and DILG MC No. 2022-02, which mandates the creation of an inventory of vaccinated population within their respective barangays.

---

<sup>4</sup> 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) & 3(l) (2012).

<sup>5</sup> Data Privacy Act of 2012, § 12 (c).

<sup>6</sup> *Id.* 13 (b).

*Adherence to the data privacy principles.*

Although there is lawful basis for the processing of personal data, the other requirements of the DPA must still be complied with to ensure the protection of personal data and uphold the rights of data subjects.

This means that the barangay, as a personal information controller (PIC), still has the responsibility to ensure that personal data is processed lawfully and fairly. In particular, there must be strict adherence with the basic privacy principles of transparency, proportionality, and legitimate purpose.

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 a PIC, 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.<sup>7</sup>

Thus, in line with the right to information of the data subject, PICs are required to apprise the data subject of the following:

1. Description of the personal data to be processed;
2. Purposes for processing, including: direct marketing, profiling, or historical, statistical or scientific purpose;
3. Basis of processing, when processing is not based on the consent;
4. Scope and method of processing;
5. Recipient/classes of recipients to whom the personal data are or may be disclosed;
6. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
7. Identity and contact details of the PIC or its representative;
8. Retention period; and
9. Existence of rights as data subjects, the right to lodge a complaint before the NPC.<sup>8</sup>

Relative to the present concern, we note that the principle of proportionality requires that the processing of personal data shall be adequate, relevant, suitable, necessary and not excessive in relation to the declared and specified purpose.<sup>9</sup> To comply with this data privacy principle, the Punong Barangay should only collect such personal data which will help in the implementation of its mandate of identifying the unvaccinated population and eventually closely monitoring their mobility to prevent the further transmission of COVID-19.

Lastly, the data privacy principle of legitimate purpose, which states that processing of personal data shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. In adherence to this data privacy principle, the barangays, as PICs should make sure that personal data to be collected from data subjects should only be used for the specific and identified purpose/s indicated in DILG MC No. 2022-02. We caution that should there be processing beyond the stated purpose, the same may be penalized under the appropriate provisions of the DPA, such

---

7 7 Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18(a) (2016).  
8 See National Privacy Commission, NPC Advisory Opinion No. 2018-031 (20 July 2018).  
9 Data Privacy Act of 2012, § 11 (d).

as Unauthorized Processing of Personal Information, Processing of Personal Information for Unauthorized Purposes or Unauthorized Disclosure.<sup>10</sup>

As stated in your letter, personal data to be collected for the said purpose are names, birthdays, ages and vaccination status and details. We note that the Punong Barangay's mandate may already be achieved through the collection of names and vaccination status and details. The collection of the birthday and age of an individual, on the other hand, appears excessive to the purpose of identifying the unvaccinated individuals, unless there are other justifications for the collection of the same.

Further, the respective barangays should also consider indicating a specific period in its inventory of vaccinated and unvaccinated individuals to ensure the accuracy of the information. This inventory should likewise be kept updated within the specified period in case some individuals may eventually get vaccinated and no longer be considered as unvaccinated individuals.

*Reasonable and appropriate security measures.*

The barangays, as PICs, should also responsible for the implementation of appropriate and reasonable physical, organizational and technical security measures to ensure the privacy of personal data. Under the DPA, implementation of these security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing. These measures shall be implemented to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.<sup>11</sup>

In relation to the present concern, we suggest that both the DILG and the barangays implement applicable organizational security measures to limit system access to authorized personnel trained for the purpose of handling such personal data. This should also be made applicable to the other DILG offices to whom personal data may be transferred or transmitted to. In line with the implementation of physical security measures, barangays must ensure that the premises and the equipment which will store the data collected from the inventory are duly protected (e.g. offices are properly secured by locks and bolts). On the other hand, technical security measures refer to the means by which a personal information controller protects its electronic system from unlawful, unauthorized and accidental access. Since the inventory system may be accessed online, we recommend looking into the technical security measures specifically stated in NPC Circular 16-01 relating to online accessible systems, for guidance and application. You may access a copy of NPC Circular 16-01 at our website or you may click on this link: <https://www.privacy.gov.ph/memorandum-circulars/npc-circular-16-01-security-of-personaldata-in-government-agencies/>

The respective barangays may also take into further consideration the conduct of a privacy impact assessment (PIA) which shall, among others, assist the barangays in the identification, assessment, evaluation and management of the risks involved in the processing of personal data through the use of the online inventory system.<sup>12</sup> For a more

<sup>10</sup> See: National Privacy Commission, NPC Advisory Opinion No. 2022-005 (24 February 2022).

<sup>11</sup> Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 25. (2016).

<sup>12</sup> National Privacy Commission, Guidelines on Privacy Impact Assessments, NPC Advisory No. 2017-03 (July 31, 2017).

comprehensive discussion on the conduct of a PIA, you may refer to NPC Advisory No. 2017-03 available at [https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/NPC\\_AdvisoryNo.201703.pdf](https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/NPC_AdvisoryNo.201703.pdf).

### *Statistical data*

You also mentioned in your letter that a statistical summary will be provided to the DILG Provincial and Regional Offices and the DILG Central Office, which shall then be used eventually for policy formulation.

We note that personal data collected for other purposes may be processed for, among others, statistical purposes.<sup>13</sup> However, we emphasize that such further processing is to be strictly construed. Data must be purely statistical and free from any factors that will enable others to reasonably identify the individuals involved. Further, it must only be used strictly for policy formulation purposes only.

We further note that the barangays are still responsible for ensuring the privacy of the raw personal data from which the statistical summary may come from. This means that all personal data initially collected from the barangay's constituents are still subject to the provisions and protection of the DPA. Therefore, even if only statistical data were submitted to the DILG, in which individuals may not be easily or reasonably identified, the raw data collected from the constituents, which remains in the barangay's custody, should remain to be protected by appropriate security measures as mandated under the DPA. Further, the raw data remains subject to the compliance with the DPA. This means that if these raw data were to be used for any other purpose or activity other than those outlined in DILG MC 2002-02, the barangay may be subjected to possible findings of non-compliance or violations under the DPA.

Considering the foregoing discussions, the feasibility and compliance of the proposed online inventory system would depend largely on the observance by the barangays and the DILG of the requirements of the DPA, its IRR and other NPC issuances and the above recommendations in the processing of personal data pursuant to DILG MC 2022-02.

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

Please be guided accordingly.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

---

<sup>13</sup> Data Privacy Act of 2012, § 11 (f).



# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-006<sup>1</sup>

30 January 2023



## **Re: REQUEST FOR MEMBERSHIP DETAILS BY A SPOUSE OF A MISSING PHILHEALTH MEMBER**

Dear 

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

We gather that the wife of a Philippine Health Insurance Corporation (Philhealth) member wrote your office to inform that her husband has been missing since 2015. To aid her in locating her husband, she requested Philhealth for information on the last payment made by her husband including the company name and address of his last employer. Included in the wife's letter is a Marriage Certificate as proof of the fact of marriage, a police blotter about her missing husband, and the Birth Certificate of the husband.

Thus, you ask whether it is lawful for Philhealth to disclose the personal information of its member to the latter's spouse.

### *Lawful processing of personal information; legitimarte interests*

The company name and business address of a person's employer, as well as the dates or amounts of payment contribution of a member to Philhealth may be considered as personal information under the Data Privacy Act of 2012 (DPA). They may be considered as such if after put together with other information, would directly and certainly identify individual.<sup>2</sup>

As far as Philhealth is concerned, the requested information is personal information since it pertains to information that can identify its member. Further, the said information also forms part of the files belonging to the missing husband and thus, is considered

---

<sup>1</sup> Tags: subscriber records; subscriber data; Bureau of Internal Revenue; internal revenue tax purposes; special cases; public authority.

<sup>2</sup> Data Privacy Act of 2012, R.A. No. 10173 (2012)

personal information. As such, Philhealth, as a personal information controller, is obliged under the DPA to process personal information of its members only when there is lawful basis and the requirements of the DPA are complied with.

A personal information controller (PIC) should determine the most appropriate lawful basis for the processing of personal information and sensitive personal information (collectively, personal data), under the given facts and circumstances. For the processing of personal information, any of the conditions under Section 12 of the DPA may be considered. In particular, the following may be appropriate under the present situation:

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

x x x

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom 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.<sup>3</sup>

The legitimate interest criteria is to be distinguished from the other lawful criteria for processing since it is not centered around a specific purpose nor is it processing to which the data subject has specifically agreed to. <sup>4</sup>In principle, it can apply to any type of processing for any reasonable purpose.<sup>5</sup>

Legitimate interests are matters that are desired or important to a PIC which may include business, financial or other reasonable purpose and which are not contrary to law, morals or public policy.<sup>6</sup> Accordingly, the PIC or third party to whom personal information is disclosed must clearly identify the legitimate interest, reasonable purpose and intended outcome.<sup>7</sup>

A PIC must be able to establish the existence of a legitimate interest in the processing of personal information or that the third party to whom the PIC has disclosed the information has a legitimate interest over the processing.

In *MAF v. Shopee Philippines, Inc.*, NPC discussed processing based on legitimate interest:

“Processing based on legitimate interest requires the fulfillment of the following conditions: (1) the legitimate interest is established; (2) the processing is necessary to fulfill the legitimate interest that is established; and (3) the interest s legitimate or lawful and it does not override fundamental rights and freedoms of data subjects.”<sup>8</sup>

3 Data Privacy Act of 2012, § 12.

4 National Privacy Commission, NPC Advisory Opinion No. 2022-005 (24 February 2022) citing United Kingdom Information Commissioner’s Office (ICO), What is the ‘Legitimate Interests’ basis?, available <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/> [last accessed on 18 January 2022]

5 Ibid.

6 National Privacy Commission, NPC Advisory Opinion No. 2020-039 (30 October 2020) citing United Kingdom Information Commissioner’s Office (ICO), What is the ‘Legitimate Interests’ basis”, available at <https://ico.org.uk/for-organisations/guideto-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>.

7 Ibid.

8 National Privacy Commission, *MAF v. Shopee Philippines, Inc.* [NPC 21-167] (Sept. 22, 2022).

In order for the lawful basis of legitimate interest to apply, the conditions under the foregoing enumeration must be satisfied. Hence, the legitimate interest of the wife must be clearly established.

First, it must be established that the processing of personal information shall be done for the sole purpose of pursuing the legitimate interest of the requesting party, which is to help her to locate her husband who has been missing since 2015. Second, only personal information which is necessary and proportionate to grant the re

quest may be processed pursuant to the identified legitimate interest of the third party to whom the personal information will be disclosed. Hence, the disclosure should only be limited to the personal information specifically requested by the wife. If the husband's account is active, then the name and address of his current employer may be provided to the wife. However, if the husband's account has become inactive, then information on the last entry made by his last known employer, and its business address may be provided to the wife in this case.

Third, it is also necessary to establish that the processing of personal information pursuant to the PIC's or third party's legitimate interest will not adversely affect the rights and freedoms of data subjects. In the determination of the balancing of rights and interests, it is important to recognize whether the data subject had reasonable expectation at the time and in the context of the collection of personal information that processing of this kind may occur (i.e., the disclosure of personal information to the requesting party/spouse of a member who is reportedly missing).<sup>9</sup>

As a PIC, Philhealth must assess the purpose and reasonableness of the disclosure to the third party (i.e., the wife), [REDACTED] (i.e., to disclose information which may be essential to locating her missing husband). This assessment includes whether or not disclosure of the spouse's information may provide a means to discovering information leading to his discovery or disappearance. Locating a spouse who has been reportedly missing since 2015 constitutes as a legitimate interest of any spouse, especially if said spouse failed to disclose his last known whereabouts. Further, allowing a third-party access to personal information to pursue his or her own legitimate interest may also be considered a legitimate interest of Philhealth since the same is not unlawful or in violation of any rules or regulations.

It is also worth noting that although this may not be one of the situations contemplated by the data subject during Philhealth's collection of personal information, it may nonetheless be reasonable in view of the extraordinary circumstances. In addition, reasonableness may also be determined from the designation of a beneficiary of Philhealth benefits in case of the data subject's death, incapacity or unavailability. In the current matter, the wife was able to present documents to establish her identity and relationship with the data subject and the reason for the request. For a more comprehensive discussion on reasonable expectation, kindly refer to NPC Case No. 17-047.<sup>10</sup>

General data privacy principles; proportionality; reasonable and appropriate security measures

<sup>9</sup> EU GDPR, Recital 49

<sup>10</sup> National Privacy Commission, JV v. JR [NPC Case No. 17-047] (Aug. 13, 2019) available at <https://www.privacy.gov.ph/wp-content/uploads/2020/10/CID-17-047-JV-v.-JR-Decision-PSD-10Aug2020.pdf>. (last accessed on 4 August 2022).

While the disclosure of personal information is supported by a lawful basis, Philhealth (as a PIC) still has the obligation to comply with the other requirements of the DPA. Personal information must be processed lawfully and fairly and with strict adherence to the basic data privacy principles of transparency, proportionality, and legitimate purpose.

Of particular significance in the current scenario, is the principle of proportionality. To reiterate, Philhealth must only disclose such personal information that is adequate and necessary for the third party's declared purpose.

In addition, PICs must also ensure the protection of the disclosed personal information and uphold the rights of data subjects through the implementation of reasonable and appropriate physical, organizational and technical security measures. For instance, Philhealth may create policies in dealing with requests of this nature and require the submission of documents necessary to prove one's relationship with a certain member. Philhealth may also require the requesting party to sign an undertaking stating that the personal information requested shall only be used for a specific purpose. Philhealth should also consider how the processing or disclosure will be done (e.g., electronically or through a hard copy personally given to the requesting party).

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

Please be guided accordingly.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-008<sup>1</sup>

17 February 2023

[REDACTED]

[REDACTED]

## RE: BLOCKING SMS WITH CLICKABLE LINKS

Dear [REDACTED]

We respond to your request for an Advisory Opinion on the data privacy implication of the temporary blocking of incoming text messages or messages sent via Short Message Service (SMS) to Globe postpaid and prepaid numbers containing Uniform Resource Locators (URLs) or website links.

You inform that since 2014, Globe Telecom, Inc. (Globe) has been progressively working on improving its capabilities to combat spam and scams in its network. In response to the recent spate of spam and scam messages, the National Telecommunications Commission (NTC) issued a directive on 12 September 2022 for Globe, Dito Telecommunity Corporation, and Smart Communications, Inc. (Telcos) to block or deactivate domains, URLs, TinyURLs, Smart Links, and/ or Quick Response (QR) Codes emanating from malicious sites.

On 4 October 2022, Globe met with the personnel of the National Privacy Commission (Commission) where it relayed its efforts to comply with the NTC directive and further explained its position that:

*First*, there is no privacy impact in the blocking of links and URLs by Globe, as it is the actual delivery of the message that is prevented from terminating at a Globe endpoint, or a Globe postpaid or prepaid mobile number. Since it is the transmission of the message that is prevented, the privacy of communications remains intact.

*Second*, Globe's blocking process does not involve the reading or storing of the contents of text messages. There is no human intervention involved, save for the setting of rules and the inputting of keywords and links to be blocked. The blocking is done

---

<sup>1</sup> Tags: Scope; general data privacy principles; law and regulation; lawful processing

through automated means in compliance with Global System for Mobile Communications Association (GSMA) Standards and Guidelines.

*Lastly*, the only way that Globe sees the contents of spam and scam text messages are through the screenshots submitted or reported by its subscribers and partner-organizations. Globe then inputs the keywords and links for blocking based on the pattern or trend observed in the screenshots.

You thus seek clarification on whether Globe’s temporary blocking of text messages pursuant to the NTC directive is in accordance with Section 3, Article III of the 1987 Constitution and with Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (DPA) and its Implementing Rules and Regulations (IRR).

To put things in perspective, it is necessary to revisit some basic principles under the DPA.

The DPA applies to any natural and juridical person involved in the processing of personal information, including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines.”<sup>2</sup> The DPA defines “processing” as any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.<sup>3</sup> On the other hand, “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.<sup>4</sup> Meanwhile, Section 3(I) of the DPA provides for an enumeration of data that are classified as sensitive personal information.

Applying the foregoing to the facts presented, it appears that there is no processing of personal data involved in Globe’s SMS-blocking activity. Hence, any determination on Globe’s compliance or non-compliance with the DPA relative to its procedures in SMS-blocking, or the constitutionality thereof, would be to engage in a purely academic discussion. Nevertheless, it is worth mentioning that Globe’s present SMS-blocking activity was triggered by a directive from the NTC. By law, the NTC is mandated to regulate the country’s telecommunications industry and issue rules and regulations to implement such mandate.<sup>5</sup> Consequently, Globe must necessarily comply with the NTC’s directive which, in turn, enjoys the presumption of constitutionality. To overthrow this presumption, there must be a clear and unequivocal breach of the Constitution.<sup>6</sup> Hence, a discourse on the constitutionality of Globe’s SMS-blocking activity is not only beyond our function, but it is also equivalent to us examining the constitutionality of the issuance of a co-equal branch of government.

Please be advised that this Advisory Opinion was rendered based solely on your provided information. Any extraneous fact that may be subsequently furnished to us may

---

2        Id, § 4  
3        Id, § 3 (j)  
4        Id, § 3 (g)  
5        Republic Act No. 7925, Public Telecommunications Policy Act of 1995.  
6        Bureau of Customs Employees Association v. Teves, G.R. No.181704 (2011)

affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

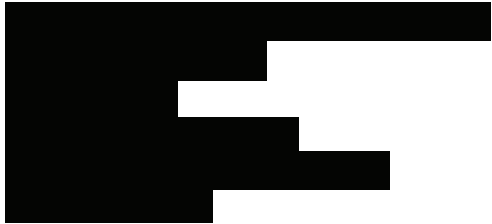
(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-009<sup>1</sup>

27 February 2023



## Re: DATA SHARING AGREEMENT WITH A SPECIALIZED AGENCY OF THE UNITED NATIONS

Dear [REDACTED]

We respond to your request for an advisory opinion on the proposed data sharing agreement (DSA) between the Department of Agriculture (DA) and the Food and Agriculture Organization (FAO).

You state that the DA is currently collaborating with the FAO for the establishment of the Rice Competitiveness Enhancement Fund- Impact Monitoring System (RCEF-IMS). The FAO is a specialized agency of the United Nations (UN) for food, nutrition, agriculture, fisheries, and forestry. Its mandate is to achieve food security for all and plays a role in interventions that support people and communities living in rural areas and those whose livelihood depend on natural resources.

One of the deliverables under the collaboration involves the integration of the components' databases and reporting platforms for seamless sharing. Since the DA maintains the Registry System for Basic Sectors in Agriculture (RBSA), which is an electronic database of basic information of farmers, farm laborers, fishermen, and target beneficiaries of agriculture-related program and services of the government, the collaboration would necessarily involve the disclosure to the FAO of confidential information about the program and the personal data of the program beneficiaries.

In its desire to comply with R.A. 10173, or the Data Privacy Act of 2012 (DPA),<sup>2</sup> and relevant issuances of the National Privacy Commission (NPC), the DA proposed to FAO that they execute a Data Sharing Agreement (DSA). Unfortunately, the FAO refused invoking their status as a Specialized Agency of the UN System which subscribes to the privileges and immunities under public international law and relevant treaties, including

<sup>1</sup> Tags: data sharing; international body, immunity from suit

<sup>2</sup> 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 immunity from all legal processes. The FAO posits that since the DSA is grounded on Philippine law, the execution thereof would equate to a waiver of its immunities.

The DA, on the other hand, recognizes its obligation to comply with the security requirements in the protection of personal data within its control under Section 22 of the DPA. Since the FAO will gain access to confidential information and personal data, including sensitive personal information of program beneficiaries, there must be a DSA to lay down the obligations and responsibilities of the parties in handling personal data.

As a middle ground, and to preserve the FAO's immunities and privileges, the DA proposed the execution of an Undertaking where the FAO will pledge to investigate and impose disciplinary action for confidentiality violations and report any incident of data breach to the DA in case of violation of Philippine data privacy laws. In support of the proposed Undertaking, the DA cited Section 6 of the DPA on the extraterritorial application of the law. FAO denied the proposal and maintained that it cannot be subject to or apply Philippine laws as it will be inconsistent with FAO's neutral character and its legal status under international law and regulations and policies that have been adopted by the Member States of the UN. Despite such stance, the FAO committed to investigate and, if appropriate, impose disciplinary action on the sole basis of their internal rules and not pursuant to the DPA or any other Philippine law. Such commitment, however, was not formalized through a written document.

Considering the opposing position of the parties, you seek guidance on the following:

1. Whether the extra-territorial application of the DPA has material application to the situation at hand;
2. Whether the execution of a DSA or an Undertaking citing data privacy laws of the Philippines shall be tantamount to waiver of immunities and privileges of the FAO; and
3. Whether the execution of a DSA or an Undertaking detailing the responsibilities and obligations of the FAO, based solely on the FAO's internal rules, and without invoking any data privacy laws of the Philippines, shall be sufficient compliance for data protection as required by the DPA.

#### *Scope of the DPA; extraterritorial application*

Section 6 of the DPA provides:

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 manage-

ment 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.

Applying the above provisions to the current situation, the extraterritorial application of the DPA applies because the personal data involved in the sharing is that of the beneficiaries who are Philippine citizens.

While we recognize the immunity and privileges accorded to the FAO pursuant to the United Nations and Convention on the Privileges and Immunities of the Specialized Agencies of the United Nations (Convention),<sup>3</sup> such privilege does not equate to a blanket exemption from compliance with Philippine law including the DPA. The Supreme Court held in *Khosrow Minucher v. Court of Appeals*,<sup>4</sup> that: "... the privilege is not an immunity from the observance of the law of the territorial sovereign or from ensuing legal liability; it is, rather, an immunity from the exercise of territorial jurisdiction." As such, the provisions of the DPA shall apply to the proposed sharing of the personal data between the DA and FAO.

*DSA not mandatory; compliance with the provisions of the DPA*

Under Section 21 (a) of the DPA, a personal information controller (PIC) is accountable for complying with the requirements of the law and shall use contractual or other reasonable means to provide a comparable level of protection while the personal data are being processed by a third party.<sup>5</sup>

The NPC previously issued NPC Circular No. 2016-02 which makes it mandatory for government agencies to execute a Data Sharing Agreement when sharing personal data to a third party. This was superseded by NPC Circular No. 2020-03,<sup>6</sup> which provides:

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 NPC 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

3 United Nations, Convention on the Privileges and Immunities of the United Nations (February 13, 1946).

4 *Khosrow Minucher v. Court of Appeals*, G.R. No. 142396, [February 11, 2003].

5 Data Privacy Act of 2012, § 21 (a).

6 National Privacy Commission, NPC Circular No. 2020-03 on Data Sharing Agreements [NPC Circular No. 202003] (23 December 2020).

thereto, as well as in the conduct of compliance checks.

(Underscoring supplied).

Thus, pursuant to NPC Circular No. 2020-03, the execution of a DSA is no longer mandatory but is considered as a best practice and a demonstration of accountability by the PIC in relation to data sharing. In the present case, the DA has other recourses besides the execution of a DSA to en

sure that it is compliant with the DPA. Section 21 (a) of the DPA does not restrict the PIC with the use of contracts to protect the personal data transferred to a third party because it also allows “other reasonable means.”

We understand that the personal data that will be shared with the FAO is under the control and custody of the DA. As the entity ultimately accountable under the DPA, the DA may opt to propose provisions relating to data sharing in the form of a policy or any similar written document. What may be included in this policy are documentation on the legitimate purpose of the data sharing with the FAO as well as the terms, conditions, and limitations of the sharing. Security measures for the protection of personal data to be shared and other details relevant to the data sharing may also be included as additional provisions. This policy may be presented to the FAO without its consent which is not an essential element in the determination of possible violations under the DPA anyway. In issuing a policy instead of insisting on the execution of a DSA, the DA is able to demonstrate accountability over the protection of the personal data subject of the data sharing.

We emphasize that the execution of a DSA does not necessarily equate to compliance with the DPA but it is only a portion of the obligations the PIC under the DPA.

*Execution of Undertaking not based on DPA;  
waiver of immunity*

We understand that the DA proposed the execution of an Undertaking detailing the responsibilities and obligations of the FAO based solely on the FAO’s internal rules, and without invoking any data privacy laws of the Philippines. As discussed above, the DA does not need to resort to contractual agreements in order to protect the personal data it shares to FAO. As to whether the execution of the DSA by the FAO amounts to a waiver of its immunit

y and privileges, we hesitate to render an opinion on this issue as the NPC’s jurisdiction is limited to the interpretation of the DPA and data privacy matters. Since that issue relates to the interpretation of international laws and its territorial application, the NPC may not be the proper authority to render a determination thereon.

*Adherence to doctrine of immunity; recourse in  
case of violation by Specialized Agency*

*In Lasco v. United Nations Revolving Fund for Natural Resources Exploration,*<sup>7</sup> the

---

<sup>7</sup> Lasco v. United Nations Revolving Fund for Natural Resources Exploration, G.R. Nos. 109095-109107, [February 23, 1995].

Supreme Court held:

As a matter of state policy as expressed in the Constitution, the Philippine Government adopts the generally accepted principles of international law. Being a member of the United Nations and a party to the Convention on the Privileges and Immunities of the Specialized Agencies of the United Nations, the Philippine Government adheres to the doctrine of immunity granted to the United Nations and its specialized agencies.

We note that in the exercise of its quasi-judicial functions, the NPC is bound to give due deference to diplomatic immunity. Subject to exemptions found in the Convention and jurisprudence, diplomatic immunity shall prevail should a scenario arise where the FAO or its members violate the DPA in relation to the data sharing.

We understand that there may be an apprehension on the part of the DA in terms of accountability in case the FAO is found liable for violating the DPA. If that happens, the NPC shall determine after investigation and hearing the liable party in cases of violations of the DPA. If the FAO is found to be liable for violating the DPA in relation to the data sharing but invokes its immunity, this does not make the DA automatically liable just because the other party may not be sued or prosecuted.

In any case, there still exists a recourse against an erring Specialized Agency. According to the Lasco case:

This is not to say that petitioners have no recourse. Section 31 of the Convention on the Privileges and Immunities of the Specialized Agencies of the United Nations states that “each specialized agency shall make a provision for appropriate modes of settlement of: (a) disputes arising out of contracts or other disputes of private character to which the specialized agency is a party.

Sections 29 and 30 of Article VIII of the Convention also provides:

SECTION 29. The United Nations shall make provisions for appropriate modes of settlement of:

(a) Disputes arising out of contracts or other disputes of a private law character to which the United Nations is a party;

(b) Disputes involving any official of the United Nations who by reason of his official position enjoys immunity, if immunity has not been waived by the Secretary-General.

SECTION 30. All differences arising out of the interpretation or application of the present convention shall be referred to the International Court of Justice, unless in any case it is agreed by the parties to have recourse to another mode of settlement. If a difference arises between the United Nations on the one hand and a Member on the other hand, a request shall be made for an advisory opinion on any legal question involved in accordance with Article 96 of the Charter and Article 65

of the Statute of the Court. The opinion given by the Court shall be accepted as decisive by the parties.

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

Please be guided accordingly.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-010<sup>1</sup>

15 February 2023



## RE: RECORDING OF TELEPHONE CONVERSATION THROUGH VOICE OVER INTERNET PROTOCOL (VoIP) SYSTEM

Dear [REDACTED]

We respond to your query about the conversation recording feature of the Voice Over Internet Protocol (VoIP) telephone system of the Philippine Merchant Marine Academy (Academy).

You explained in your letter that the VoIP phone is a hardware or software-based telephone that is designed to use VoIP technology to send and receive calls over all IP network. Through this technology, calls can be recorded entirely in the cloud or on-premises with VoIP call recording software. You mentioned that the system automatically records and saves outgoing telephone calls. The system is being managed by your Information Technology Services Unit (ITSU) which released a policy on the use of VoIP phones, as follows:

Personnel shall not use the Services for any illegal, fraudulent, improper, or abusive purpose.

1. Use PMMA Phones for business purposes only and preserve them in perfect condition.
2. The international call is available for an additional fee.
3. Except in the case of employees provided with private telephone lines, all outgoing telephone calls shall course through the Information Operator.
4. The telephone operator shall be obliged to maintain the telephone logbook and submit it to the respective authority at the end of the month

You also mentioned that the Academy's Data Privacy Office and ITSU are currently revisiting the policies on the usage of VoIP phones since the current policy does not include conversation recording. Neither have the employees been notified of this recent feature.

<sup>1</sup> Tags: lawful processing; legitimate interest; proportionality; security measures.

You thus ask whether the automatic conversation recording feature of the VoIP phone can lead to a possible violation of the DPA and other laws or regulations.

*Scope of the Data Privacy Act; lawful processing; recorded calls containing personal data; proportionality.*

RA 10173 or the Data Privacy Act of 2012 (DPA) applies to the processing of all types of personal information<sup>2</sup> and to any natural and juridical person involved in personal information processing.<sup>3</sup>

Processing as defined under the DPA 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.<sup>4</sup>

Recording telephone conversations may be considered as a form of data processing since personal information and sensitive personal information (collectively, personal data) may be given out or spoken in the course of these conversations. In NPC Advisory Opinion No. 201763<sup>5</sup>, the concept of biometrics as personal data was discussed, viz.:

“Under Republic Act (RA) No. 103676,<sup>6</sup> biometrics refer to ‘the quantitative analysis that provides a positive identification of an individual such as voice, photograph, fingerprint, signature, iris and/or such other identifiable features.’<sup>7</sup>

While under Article 29 Opinion 4/2007 (EU)<sup>8</sup>, a biometric data may be considered both as content of the information about a particular individual as well as an element to establish a link between one piece of information and the individual. As such, it can work as “identifier” for it produces a unique link to a specific individual.

On that note, it must be emphasized that 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.”<sup>9</sup> Corollary, hand written signatures, as may be used to identify an individual, is considered as personal information.

In the same manner, unique information relating<sup>10</sup> to an individual or when linked with other information will allow an individual to be distinguished from others, may be treated as personal information.” (underscoring supplied)

In your query, the recording of a telephone conversation is considered as processing

2 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.

3 Id. § 4.

4 Data Privacy Act of 2012, § 3 (f).

5 National Privacy Commission, NPC Advisory Opinion No.2017-063, (09 February 2017).

6 AN ACT PROVIDING FOR MANDATORY BIOMETRICS VOTER REGISTRATION, 15 February 2013, §2(b).

7 R.A. No. 10367, §2(a).

8 Opinion 4/2007 on the concept of personal data, Adopted on 20th June 2007.

9 Id., § 3(g).

10 EU Directive 95/46/EC Working Party Document No. WP 105 noted that “Data relates to an individual if it refers to the identity, characteristics or behavior of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated.”

of personal data when the parties to the conversation can be identified by their voice; or when linked to other information can identify an individual/s, such as an employee directory, or if the caller's identity is mentioned in the phone conversation.

The processing of a telephone conversation via recording is not prohibited by the DPA, but there must be a legitimate purpose for recording and such purpose is not contrary to law, morals or public policy. If a legitimate purpose has been established, the next step is to determine the applicable criteria for processing under Section 12 or 13 of the DPA, depending on the personal data involved, 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;
- (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.<sup>11</sup>

In your letter, the following are the stated purposes for the automatic recording of the Academy's outgoing calls through the VoIP system,;

1. to keep detailed call records;
2. to recover missed details; and
3. to protect the Academy and its employees and any possible potential legal dispute and for security reasons.

Based on the aforementioned purposes, it appears that the only applicable basis for processing would be to obtain the consent of the data subjects.

As presented, the purposes seem to be ambiguous and speculative; hence, they cannot qualify under the criterion of legitimate interest in Section 12 (f) of the DPA. The purposes failed to state what specific details would be recorded or are sought to be recorded to justify the automatic recording. This contravenes the data privacy principle of transparency which requires that the data subject (i.e., the parties to the telephone conversation) 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.<sup>12</sup>

The automatic recording of VoIP phone calls also appears to be disproportionate to the purposes it seeks to achieve. The data privacy 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. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.<sup>13</sup> The Academy has not shown that the purposes stated in the VoIP policy cannot be fulfilled through any other means aside from the recording of the phone calls.

#### *Reasonable expectation of privacy in the workplace*

Factual circumstances of every case determine the reasonableness of the expectation of privacy. Similarly, customs, community norms, and practices may, therefore, limit or

<sup>11</sup> Id. § 12,13.

<sup>12</sup> Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18(a) (2016).

<sup>13</sup> Id § 18(c) (2016).

extend an individual’s reasonable expectation of privacy. The reasonableness of a person’s expectation of privacy is determined on a case-to-case basis.<sup>14</sup>

NPC Advisory Opinion No. 2018-090<sup>15</sup> is highly instructive on the reasonable expectation of privacy in the workplace in light of the implementation of the DPA, viz.:

Likewise, courts have generally held that employees have a decreased expectation of privacy with respect to work device, email accounts, and internet surfing activities. The same may be said for the contents therein, since there is an assumption that its use will be limited to work-related purposes.

Yet, with the DPA now in place, the reasonable expectation test should be revisited and interpreted in the context of the law.

By virtue of a legislation on data protection and privacy, the assumption is that individuals now have an expectation of privacy. As to the second element, data privacy is now more than a reasonable expectation – it is now enshrined in the DPA. The reasonable expectation of privacy test then should take into consideration the standards provided under the DPA.

This means that employees must be aware of the nature, purpose, and extent of the processing of his or her personal data in the workplace. The processing of personal information of employees shall also be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. Lastly, the processing of such information shall be adequate, relevant, suitable, necessary and not excessive in relation to a declared and specified purpose.

Recent jurisprudence from foreign jurisdictions also provide guidance with regard to monitoring calls of employees at the workplace. In *Copland v. the United Kingdom*,<sup>16</sup> the European Court of Human Rights (ECtHR) held that monitoring calls without the employee’s knowledge, amounted to unnecessary interference with his privacy rights, viz:

42. The applicant in the present case had been given no warning that her calls would be liable to monitoring, therefore she had a reasonable expectation as to the privacy of calls made from her work telephone (see Halford, § 45). The same expectation should apply in relation to the applicant’s e-mail and Internet usage.

xxx

44. Accordingly, the Court considers that the collection and storage of personal information relating to the applicant’s telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence xxx.

xxx

47. The Court is not convinced by the Government’s submission that the College was authorized under its statutory powers to do “anything necessary or expedient” for the purposes of providing higher and further education, and

---

14 National Privacy Commission, NPC Advisory Opinion No. 2018-090 (28 November 2018).

15 Id.

16 ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007

finds the argument unpersuasive. Moreover, the Government do not seek to argue that any provisions existed at the relevant time, either in general domestic law or in the governing instruments of the College, regulating the circumstances in which employers could monitor the use of telephone, e-mail and the Internet by employees.

Hence, with the DPA in place, employers are expected to be more mindful of the privacy rights of their employees.

*Privacy notice; privacy policy; data security*

In your letter, you mentioned that no notice has been disseminated yet on the automatic recording feature of the VoIP phone. We recommend that the Academy gather the consent of the data subjects which may be done through an automatic voice prompt informing the data subjects that the conversation will be recorded for the purposes cited in your VoIP policy. This is also a good way to notify the data subjects of the nature, purpose and extent of the processing of their personal data.

Further, please note that the upgrade in the system necessarily signifies the need to revisit the Academy's security policies. We suggest the drafting a more comprehensive privacy policy which would also include other provisions on data privacy such as data retention, deletion, and access.

Moreover, a Privacy Impact Assessment (PIA) may be necessary prior to the introduction of this telephone system to identify existing and potential risks and enable the Academy to take the appropriate measures. A PIA will help you identify the type of security demanded on this kind of medium for personal data. A PIA will ensure the system's compliance with the DPA and protection of your data subject's rights:

A PIA should be conducted prior to the deployment of a project, product, or service that involves the collection of personal information. When there are new or revised industry standards, organization policy, law or regulation, or when there are changes to methods in which personal information is handled, a personal information controller should conduct a PIA again on the pertinent process.

To emphasize, it should not only identify the existing controls and risks a project, product, or service may have upon personal data privacy, but it should lead to the identification of remedial actions or mitigation measures necessary to avoid or reduce those risks. These remedial actions and mitigation measures may be incorporated in the organization's Privacy Management Program (PMP).<sup>17</sup>

As to your query on the other possible legal repercussions of the Academy's adoption of the system, (e.g. the Anti Wiretapping Law), it would be best to consult your legal department as they possess all the necessary information and facts to respond appropriately.

Please be advised that the foregoing was rendered based solely on the information provided. Any extraneous fact that may be subsequently furnished us may affect our

---

<sup>17</sup> 17 KRL vs. Trinity University of Asia, AA, MC, NCB, RG GV, GCT, RR, MR, PB, CID Case No. 17-K-003 (19 November 2019).

present position. Note that this communication is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-011<sup>1</sup>

17 March 2023

[REDACTED]

## RE: REQUEST FOR INFORMATION FROM LABOR UNIONS

Dear [REDACTED]

We respond to your request for an Advisory Opinion on whether the refusal of an employer to grant a labor union’s request for access to documents is proper.

You state that you represent the National Federation of Labor (NFL) which is a federation of labor unions with a nationwide membership. NFL actively helps its member-unions in negotiating collective bargaining agreements (CBAs) with employers among other advocacies for the rights and welfare of employees. For NFL to effectively negotiate CBAs, its member-unions need financial information from their respective employers. Presently, you mentioned that some of your member-unions sought financial information from their employers who are either hospitals or educational institutions. The information sought include financial statements, balance sheets, enrollment data, and patient/customer data.

For the private hospital unions, they also requested for documents relative to the distribution and amounts of Special Risk Allowance (SRA), Meals and Transportation Allowance (MAT), Health Emergency Allowance (HEA) and One COVID-19 Allowance (OCA) pursuant to Republic Act (R.A.) No. 11469 or the Bayanihan Heal As One Act and R.A. No. 11494, or the Bayanihan to Recover As One Act. The private hospitals, however, refuse to divulge such information citing the Data Privacy Act of 2012 (DPA). For the same reason, private educational institutions have also used refused to furnish data on employees, enrollment and “other income sources”, which are usually used as basis for collective bargaining negotiations, pursuant to R.A. No. 6728 or the Government Assistance to Students and Teachers in Private Education Act.

You thus ask whether the abovementioned employers may legally refuse to divulge the requested information citing the DPA.

*Scope of the DPA; Nature of financial documents*

---

<sup>1</sup> Tags: personal information; legitimate interest; legal claims; proportionality.

The DPA applies to the processing of all types of personal information and sensitive personal information (collectively, “personal data”) and to any natural or juridical persons involved in the processing of personal data.<sup>2</sup>

The processing of personal data referred to in the DPA is only limited to natural persons or individuals. Data pertaining to juridical persons (e.g., corporate name, address, financial information) are not considered personal data and, hence, do not fall within the scope of the DPA.

The financial statements, balance sheets, and profit and loss statements (collectively, “financial information”) referred to in the current matter pertain to the employers who are juridical entities. Juridical entities are not considered as data subjects entitled to the protection of the DPA and its Implementing Rules and Regulations (IRR). Thus, the disclosure or processing of a company’s financial information fall outside the scope of the DPA. Consequently, the employers’ refusal to divulge their financial information to the employees’ union due to data privacy concerns is misplaced.

*Lawful processing; legitimate interest*

On the other hand, a private educational institution’s data on its employees, student enrollment and “other income sources,” as well as a private hospital’s data on its patients and employees and the distribution and amounts of benefits mandated by law are all considered as personal information under the DPA. This is because such information can identify the individuals to which it pertains. Moreover, data on patients and students may involve sensitive personal information under Section 3(l)(2) of the DPA particularly information about an individual’s health and education.

As personal information controllers (PIC), private educational institutions and private hospitals are obliged to strictly process personal information in accordance with the DPA.

The NPC recognizes that employers are required to share information with labor unions for the latter to effectively negotiate CBAs and advocate for the general welfare of employees. Article 242 (c) of the Labor Code of the Philippines provides that legitimate labor organizations have the right to be furnished by their employers with its annual audited financial statements, including balance sheets and the profit and loss statement. However, the law did not mention the other documents that are being requested by your memberunions from their employers such as data on employees, enrollment of students and the distribution of benefits mandated by law. Be that as it may, Section 12 (f) of the DPA appears to be the most appropriate basis for processing such personal data, thus:

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

---

<sup>2</sup> 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).

(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.<sup>3</sup>

Legitimate interests are matters that are desired or important to a personal information controller which may include business, financial or other reasonable purpose and which are not contrary to law, morals or public policy.<sup>4</sup> Accordingly, the personal information controller or third party to whom personal information is disclosed must clearly identify and establish the existence of a legitimate interest, reasonable purpose and intended outcome.<sup>5</sup>

NPC discussed the criteria for the processing based on legitimate interest in *MAF v. Shopee, Inc.*,<sup>6</sup> viz.:

Processing based on legitimate interest requires the fulfillment of the following conditions: (1) the legitimate interest is established; (2) the processing is necessary to fulfill the legitimate interest that is established; and (3) the interest is legitimate or lawful and it does not override fundamental rights and freedoms of data subjects.

For the lawful criteria of legitimate interest to apply, the foregoing conditions must be satisfied. Thus, your union-members must establish their legitimate interest in the personal data they request by: first, establishing that the processing shall be for the sole purpose of pursuing the legitimate interest of the labor union to effectively negotiate for the benefits of its members; second, the disclosure or processing shall only be limited to the personal information specifically requested by the labor union and which are necessary and proportionate to achieve its legitimate interest; and, third, the processing of personal information must be done in the least intrusive way so as not to impede the rights of the data subjects. In the scenario you provided, the data subjects are the employees and students.

For the processing of sensitive personal information involved in the current matter, Section 13 (f) of the DPA appears to apply, *to wit*:

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

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

<sup>3</sup> Data Privacy Act of 2012, § 12 (c).

<sup>4</sup> National Privacy Commission, NPC Advisory Opinion No. 2022-005 (24 February 2022) citing United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/> [last accessed on 27 February 2023]

<sup>5</sup> Ibid.

<sup>6</sup> National Privacy Commission, *MAF v. Shopee Philippines, Inc.* [NPC 21-167] (Sept. 22, 2022).

defense of legal claims, or when provided to government or public authority.”<sup>7</sup>

The National Privacy Commission (NPC) clarified in *BGM v. IPP*,<sup>8</sup> that the term “processing as necessary for the establishment of legal claims” does not require an existing court proceeding:

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.

To reiterate, the labor unions’ request for student and patient data stems from their right to advocate for the welfare of all employees. Access to the requested data may provide the necessary means for them to have knowledge about the current financial status of their employers and effectively negotiate during policy and decision-making. The said acts may be considered as a labor union’s establishment of its legal claims from employers.

*General data privacy principles; proportionality; reasonable and appropriate security measures*

Granting that the disclosure of personal information is supported by a lawful basis, employers, as personal information controllers, are still obliged to comply with the other requirements of the DPA. The processing of personal information must be done lawfully and fairly and with strict adherence to the basic data privacy principles of transparency, proportionality and legitimate purpose.

The principle of proportionality is of particular significance to the current scenario. To reiterate, employers must only provide such personal information that are adequate and necessary for the labor union’s declared purpose. Stated differently, the disclosure

7 Data Privacy Act of 2012, § 13(f).

8 National Privacy Commission, *BGM v. IPP* [NPC 19-653] (Dec. 17, 2020).



shall only be limited to the personal information that is relevant to the labor union's purpose which is collective bargaining.

Further, employers should also guarantee the protection of the disclosed personal information and uphold the rights of the data subjects through the implementation of reasonable and appropriate physical, organizational and technical security measures. For instance, employers may establish policies, if there are none yet, in dealing with requests of this nature. Employers should also take into consideration the means by which the disclosure shall be made (e.g., electronically or through a hard copy personally handed to the labor union representative). It is worth noting that the implementation of the said reasonable and necessary security measures shall still be subject to the requirements of labor laws and other applicable laws.

Please note that NFL is also required to ensure the protection of the personal data that was disclosed to them. To reiterate, the disclosed personal data must only be used for the declared purpose and shall only be accessed by authorized persons or persons who are involved in the negotiations with employers. Further, NFL must also ensure that the disclosed data shall be deleted or destroyed once it has already served its purpose, subject to the relevant laws and policies on retention.

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

For your reference.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-012<sup>1</sup>

05 May 2023

[REDACTED]

## RE: COLLECTION OF INFORMATION OF CUSTOMERS, DELINQUENT BORROWERS, AND LOAN APPLICANTS OF CIBI MEMBERS

Dear [REDACTED]

We respond to your request for an Advisory Opinion on the proposed creation by CIBI, Information Inc. (CIBI) of its own private credit bureau through the collection of data from its members' customers, borrowers, and loan applicants.

You state that CIBI<sup>2</sup> is the Philippines' first credit reporting agency. It was previously operated as a business information division of the Department of Loans and Credit of the Bangko Sentral ng Pilipinas (BSP). In 2020, CIBI was acquired by Creador, a regional private equity firm.

Based on CIBI's website, CIBI aims to be the trusted partner of businesses and consumers for their hiring and lending needs by offering technology solutions to solve customer problems across hiring, lending, and partnering.<sup>3</sup>CIBI's goal is to assist individuals and organizations (hereafter referred to as "CIBI members") in optimizing their risk-based credit and hiring decisions through its "proprietary datasets" to be collected from the CIBI members' customers, borrowers or applicants.

CIBI's private credit bureau initiative is targeted to provide solutions for market needs with respect to the management of the end-to-end credit cycle process, such as: a) establishing the creditworthiness of juridical entities and individuals using their payment/nonpayment history; b) identifying/detecting fraud using the application details voluntarily shared by applicants to banks and financial solutions in the Philippines; and c) improving debt or payment collection from delinquent customers or borrowers.

---

1 Tags: lawful criteria for processing, data sharing, credit information, consent, legitimate interest  
2 Formerly known as the Credit Information Exchange System.  
3 CIBI website, About Us, available at <https://www.cibi.com.ph/about-us/> (last accessed 27 March 2023).

For such purpose, CIBI intends to collect the following specific datapoints:

- a. individual's name or juridical entity's name;
- b. address;
- c. contact information;
- d. loan type;
- e. transaction involved;
- f. principal amount;
- g. amount unpaid;
- h. due date;
- i. days outstanding; and
- j. other details in the signed application form, if applicable.

Desiring to pursue its initiative while committed to comply with Republic Act No. 10173, or the Data Privacy Act of 2012 (DPA),<sup>4</sup> CIBI seeks guidance on the following:

1. Whether information pertaining to juridical entities that are in default of their payment obligations either from sales transactions or loans be shared to CIBI to improve debt or payment collection;
2. Whether information pertaining to individuals who are in default of their payment obligations either from sales transactions or loans be shared to CIBI to improve debt or payment collection;
3. Whether information collected from financial institutions' application forms filled up by juridical entities be shared to CIBI to detect and prevent fraud; and
4. Whether information collected from financial institutions' application forms filled up by individuals be shared to CIBI to detect and prevent fraud.

#### *Scope of the DPA; juridical entities*

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing, subject to the exceptions laid down in the law.<sup>5</sup> 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.<sup>6</sup> Hence, the DPA is limited in its application to the processing of personal data of natural persons, not juridical entities.

We had the opportunity to discuss further the foregoing precept in Advisory Opinion No. 2020-002,<sup>7</sup> thus:

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

---

<sup>4</sup> 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).

<sup>5</sup> Data Privacy Act of 2012, § 4.

<sup>6</sup> Id. § 3 (g).

<sup>7</sup> National Privacy Commission, NPC Advisory Opinion No. 2020-002 (06 Feb 2020).

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.

Hence, the processing involved in your first and third questions above involve matters outside the scope of the DPA. Nevertheless, we explained in the same Advisory Opinion that while the DPA does not apply to the processing of information of juridical entities, there may exist other relevant laws and government issuances that govern their processing. In other words, if CIBI will process such data of juridical entities, it must find support in other laws and not the DPA.

*Lawful criteria for processing; consent; legitimate interest; data sharing agreement*

On the other hand, the second and fourth questions involve matters that are covered by the DPA since it involves the processing of personal information of individuals. Hence, for the processing of personal information to be valid, there must be a legitimate purpose and its processing is not otherwise prohibited by existing law. Section 12 of the DPA provides the criteria for lawful processing of personal information. In the given scenario, Sections 12 (a) and (c) appear to be the most applicable basis for CIBI's intended processing, *to wit*:

(a) The data subject has given his or her consent;

xxx

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

It must be noted that by virtue of the sale or loan transaction, it is the CIBI member that has the direct relationship with its individual customer, borrower, or applicant. As such, the DPA considers the CIBI member as the personal information controller (PIC) relative to the personal information of its individual clients who, in turn, are considered as data subjects. On the other hand, CIBI is considered as a third-party PIC to whom the personal information will be disclosed or shared.

Thus, one way of legally enabling the sharing of personal data between CIBI and its members is to obtain the consent of the clients of the CIBI member. The DPA defines consent of the data subject 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.<sup>8</sup> Thus, in clear and concise language, the CIBI member must first inform its individual clients of the intent to share their personal information to CIBI, its purpose, and other relevant details involved in the processing. Thereafter, the individual clients' consent must be evidenced by written, electronic or recorded means as prescribed by the DPA.

In keeping with best practices, CIBI may enter into a data sharing agreement (DSA)

---

<sup>8</sup> Id. § 3 (b).

with each of its members to properly document the obligations, responsibilities, and liabilities of the PICs involved in the transfer of personal data. Under NPC Memorandum Circular No. 202003,<sup>9</sup> the execution of a DSA demonstrates accountability on the part

of the PICs as Section 21 of the DPA requires the PIC to use contractual or other reasonable means to provide a comparable level of protection while the personal data is being processed by a third party.

Should the individual client refuse to consent to the processing, CIBI can also rely on Section 12 (f) which considers legitimate interests pursued by the PIC or by a third party or parties to whom the data is disclosed as lawful ground for processing.

The NPC previously adopted the three-part test of the United Kingdom's Information Commissioner's Office in the assessment of legitimate interest as a ground for processing of personal information, thus:

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.<sup>10</sup>

Subsequently, the NPC provided in *MAF v. Shopee*<sup>11</sup> the conditions for lawful processing based on legitimate interest under the DPA, *viz.*:

Processing based on legitimate interest requires the fulfillment of the following conditions: (1) the legitimate interest is established; (2) the processing is necessary to fulfill the legitimate interest that is established; and (3) the interest is legitimate or lawful and it does not override fundamental rights and freedoms of data subjects.

The CIBI member must therefore carefully assess and justify whether the above conditions provided in the *Shopee* case are met before it can process the personal data of its individual customers, borrowers, or applicants to CIBI based on legitimate interest.

### *Proportionality; Data subjects rights*

The DPA further mandates that a PIC should adhere to the data privacy principles of transparency, legitimate purpose, and proportionality. The principle of transparency dictates that the data subject must be informed of the processing of his or her personal information and the details thereof. Meanwhile, the principle of proportionality requires

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

<sup>10</sup> 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-generaldata-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/> [last accessed on Feb. 12, 2020].

<sup>11</sup> National Privacy Commission, *MAF v. Shopee*, NPC 21-167, [22 September 2022].

that the processing of personal information shall be adequate, suitable, necessary, and not excessive in relation to the purpose sought to be achieved by the PIC. Hence, even if CIBI and its members may justify the processing based on consent or legitimate interest, they must still comply with the foregoing principles of transparency and proportionality. As otherwise, the processing can still be invalidated.

It is worth mentioning further the recommendations stated in NPC Advisory Opinion 2020039,<sup>12</sup> that PICs are required to implement reasonable and appropriate organizational, physical, and technical security measures to protect the disclosed personal data. As PICs, CIBI and its members are required to regularly monitor for security breaches and take preventive, corrective and mitigating measures against incidents which may lead to security breaches.

In the same vein, the PICs shall uphold the rights of the data subject at all times. For more information on the rights of the data subjects, please see NPC Advisory No. 2021-01.

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

Please be guided accordingly.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

---

<sup>12</sup> National Privacy Commission, NPC Advisory Opinion No. 2020-039 (30 October 2020).

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-013<sup>1</sup>

21 June 2023

[REDACTED]

## RE: PROPOSED ORDINANCE ON THE ESTABLISHMENT OF A BARANGAY DATABASE OF ALL HOUSEHOLDS AND INDIVIDUALS IN THE PROVINCE OF PALAWAN.

Dear [REDACTED]

We respectfully provide you with our Advisory Opinion regarding your request for comments on the data privacy implications of the proposed Ordinance mentioned above (the “Ordinance”).

We gather from the Whereas clauses of the Ordinance that it was authored owing to the perceived need of the Province of Palawan to have a barangay-level counterpart to Republic Act No. 11315, or the Community-Based Monitoring System Act (CBMSA).<sup>2</sup> In essence, the CBMSA’s declared policy is to establish a database for conducting poverty analysis and needs prioritization with the end in view of designing appropriate policies and interventions for social services, but with due regard to the fundamental human right to privacy and the data protection principles under Republic Act No. 10173<sup>3</sup> or the Data Privacy Act of 2012 (DPA).

However, the CBMSA is implemented only at the Municipal/City Levels because of its complexity and costly requirements. Thus, the Ordinance was drafted for a similar purpose as the CBMSA but for the use of every barangay of component municipalities of the Province of Palawan. The Ordinance seeks to establish a database not only of inhabitants but also a demographic and socio-economic data that will provide profiles necessary for crafting of *barangay-level policies* and development plans for poverty related measures. Concomitantly, a local barangay ID System will be implemented for each *barangay*. Hence, your request for comments on the Ordinance.

<sup>1</sup> Tags: ordinance, barangay database, ID system, criteria for lawful processing; data privacy principles; rights of the data subject.

<sup>2</sup> Enacted on 17 April 2019.

<sup>3</sup> 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).

*Personal and Sensitive Personal Information;  
lawful criteria for processing of personal data.*

The DPA and its Implementing Rules and Regulations (IRR) apply to the processing<sup>4</sup> of all types of personal information by any natural or juridical person in the government or private sector.

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.”<sup>5</sup> On the other hand, Section 3 (I) of the DPA provides for what information are considered as sensitive personal information.<sup>6</sup>

To be lawful, the processing of personal information and sensitive personal information (collectively, personal data) must be supported by any of the lawful criteria provided in either Section 12 or Section 13 of the DPA.

Based on the provisions of the Ordinance, we understand that the establishment of the Registry of Barangay Inhabitants (RBI) for each barangay in the Province of Palawan is for the purpose of complying primarily with DILG Memorandum Circular (MC) 2020-117,<sup>7</sup> which directs all barangays to submit updated, aggregated, and disaggregated demographic data of each barangay to the Barangay Information System (BIS). Hence, assuming that the Ordinance will be enacted, the processing of personal data finds justification under either Section 12 or Section 13 of the DPA, depending on whether the personal data is considered as personal information or sensitive personal information.

Going over the list contained in Section 6 of the Ordinance, the following are considered as personal information: the individual’s full name, address, length of stay in the barangay, place of birth, highest educational attainment and occupation-related details, and the fact of the issuance of a birth certificate. For the processing thereof, Section 12 (e) of the DPA appears to be the most appropriate basis, viz.:

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

(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.**<sup>8</sup>

On the other hand, the following are considered as sensitive personal information: the date of birth, marital status, gender, and highest educational attainment, the individual’s solo parenthood, tribal affiliation, ethnicity, religion, impairment/disability, school

4 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.

5 Id. § 3(g).

6 Data Privacy Act of 2012, § 3 (I).

7 Guidelines in the Establishment of the Barangay Profile System (BPS) Module under Barangay Information System (BIS), September 4, 2020.

8 Emphasis supplied.



attendance, nutritional status, and pregnancy-related information (for females). For this sensitive personal information, their processing finds basis under Section 13 (b) of the DPA, viz:

(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;<sup>9</sup>(emphasis supplied)

Nevertheless, it must be pointed out that even though there may be lawful bases for collecting the personal data of barangay inhabitants in relation to the purposes stated in the Ordinance, the barangays concerned are still required to comply with its duties and responsibilities as a personal information controller (PIC) under the DPA. Hence, they still have the obligation to adhere to the general data privacy principles, uphold data subject rights, and implement reasonable and appropriate security measures for the protection of personal data.

*Data Privacy Principles: Transparency  
Legitimate purpose and Proportionality*

The data privacy principle of transparency requires that data subjects must be made 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, and the rights of the data subjects and how these can be exercised.<sup>10</sup>

We note that the Ordinance contains a provision directing enumerators to exhaustively explain to the respondents why a particular item of personal data is collected and why its processing is necessary to achieve the objectives of the Ordinance. Likewise, it provides an extensive list of personal information required to be collected. However, it does not include a provision on how the inhabitants will be informed of the extent of processing, the risks and safeguards involved, their rights as data subjects and how such rights may be exercised. For the proper observance of the principle of transparency, the data subjects must be made aware on how and to what extent the barangay intends to use their personal data, and if their personal data will be shared with any other government agencies or private entities. Thus, we recommend that a provision to such effect be included in the Ordinance.

On the other hand, the principle of legitimate purpose<sup>11</sup> states that the processing of personal information shall be compatible with a declared and specified purpose, which is not contrary to law, morals or public policy. Thus, we suggest that the legal basis of the Ordinance, which is to comply with DILG Memorandum Circular No. 2020-117, must also be indicated to ensure adherence to this privacy principle.

Lastly, the principle of proportionality requires that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared

9 Emphasis supplied.

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

11 Id., § 18 (b).

and specified purpose.<sup>12</sup> It must be emphasized that personal data must only be processed if the purpose of processing could not be reasonably fulfilled by other means.

The *Sangguniang Panlalawigan* of Palawan may consider the requirement of collecting statistical or aggregate data as sufficient in fulfilling the Ordinance's objectives. For example, the Ordinance can consider collecting the number of family members living in the household - adults and children, instead of collecting the names of all the occupants, to fulfill the purpose of determining the total number of inhabitants covered within the jurisdiction of a *barangay*.

As to additional sensitive personal information required by the Ordinance which include the blood type, place of origin, and religion, these data do not appear to be necessary in the fulfillment of the Ordinance's objectives. We suggest that the *barangay* refrain from collecting these personal data.

It is worth emphasizing also that there must be a guarantee that adequate safeguards are in place before processing of information, such as provisions on retention periods and records disposal.<sup>13</sup> The Ordinance lacks provisions on such safeguards. Hence, we also recommend that provisions relative thereto be included to ensure that personal data processed is kept secure. For reference as to what security measures should be put in place, you may refer to NPC Circular 16-01 – Security of Personal Data in Government Agencies >> National Privacy Commission.

#### *Barangay ID System; Sensitive Personal Information*

The Ordinance states that the Barangay ID to be issued to the inhabitants for the sole purpose of establishing barangay residency shall contain, among others, the name, place and date of birth, address, sex, blood type, photo, QR code, logo of province and barangay, and expiry date.

As stated in the above discussion, the processing of personal data should also adhere to the data privacy principles of transparency, legitimate purpose, and proportionality. We advise the *Sanggunian* to carefully evaluate if all the information to be included in the Barangay ID are required for its declared purpose/s.

We also advise that a privacy notice be posted in highly conspicuous areas of the *barangay* hall. The privacy notice should contain what personal data shall be reflected in the ID and the corresponding purpose/s for its issuance. The barangay inhabitants must also be made aware of the corresponding purpose/s at the earliest practicable opportunity, preferably before any personal data are collected from them.

We trust that the above discussion would guide the Sanggunian in evaluating the privacy implications of the Ordinance.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not

---

<sup>12</sup> Id., § 18 (c).

<sup>13</sup> Data Privacy Act of 2012, Republic Act No. 10173, §11 (f).

intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)

**VIDA ZORA G. BOCAR**

OIC Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-014<sup>1</sup>

21 June 2023

[REDACTED]

## RE: TRANSFER OF PERSONAL DATA AMONG PERSONAL INFORMATION CONTROLLERS

Dear [REDACTED]

We respectfully provide you with our Advisory Opinion on your query raising several privacy concerns regarding the transfer of personal data of your customers to a local electric cooperative.

You inform that your company is a third-party power generation and distribution company with clientele located in isolated areas in the Philippines. We understand that your company intends to transfer its power distribution rights to a local electric cooperative in one of your sites. However, there remain unpaid charges from some of your customers. Thus, you requested the local electric cooperative to collect the unpaid charges on your company's behalf, but this necessitates the disclosure of your list of customers including their addresses and contact details to the local electric cooperative.

Thus, you ask the following:

1. How can your company disclose customer information to its local partner for collection payables without violating the DPA or any NPC issuance?
2. Does the transfer of your company's rights as power distributor free it of its obligations towards its customers as data subjects?

*Personal information; lawful processing of personal data – contractual obligation; legitimate interest.*

Your company's intended action of transferring its client list to the new local distributor

---

<sup>1</sup> Lawful Processing; Contractual Obligation; Legitimate Interest; Accountability.

qualifies as “processing” under the Data Privacy Act (DPA).<sup>2</sup> On the other hand, the information in your client list (which consists of your clients’ names, addresses, and contact details) is classified as personal information under the law.<sup>3</sup> Hence, the processing of your company’s client list should therefore be supported by the appropriate basis under the DPA.

The collection of unpaid charges from delinquent customers can be considered as lawful processing of personal information for the purpose of the fulfillment of a contract with the data subject pursuant to Sec. 12 (b) of the DPA. Your intended processing also finds basis under Sec. 12 (f) of the DPA, since both your company and the local electric cooperative have a legitimate interest to ensure that all unpaid accounts and charges are fully settled. As such, your company can provide the local electric cooperative with the list of delinquent customers for proper collection and payment even without the execution of a Data Sharing Agreement (DSA). As provided in Section 8 of NPC Circular 2020-03, the execution of a DSA is no longer mandatory, and the parties may resort to other contractual schemes containing the terms and conditions of the sharing arrangement. Nevertheless, the execution of a DSA is considered as a best practice and a demonstration of accountability by the personal information controllers.

*Privacy Notice; Data Privacy Principle of Transparency.*

Since the execution of a DSA is not required in this particular case, a privacy notice to your customers may suffice if there will be no change as to the purpose of the personal data collected.

Nevertheless, your company should still observe the data privacy principle of transparency. The principle of transparency requires that data subjects 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.<sup>4</sup>

Applying the foregoing to your concern, the privacy notice must indicate what type of personal data will be processed, the purpose for processing (e.g., the transfer of distribution rights and collection of unpaid or pending charges), the Data Subject’s rights, and the channels by which to exercise it whenever applicable. We also recommend that these notices be sent individually to the customers concerned for proper dissemination and information.

*Accountability of PICs to data subjects.*

On your query as to whether your company is free from liability towards the data subjects by the transfer of rights to the local cooperative, we refer you to the principle of accountability under Sec.21 of the DPA’s IRR, to wit:

---

<sup>2</sup> 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).

<sup>3</sup> Id. §3 (g).

<sup>4</sup> Id. §18 (a).

SEC. 21. Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(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.<sup>5</sup>

Hence, your company remains to be a PIC if it retains the personal data of its customers and, consequently, remains accountable to the latter.

In connection with the foregoing, please note that the DPA allows retention of personal data only for as long as necessary for the fulfillment of purposes for which the data was obtained or for the establishment, exercise, or defense of legal claims, or for legitimate business purposes, or as provided by law.<sup>6</sup>

Some of the factors that may be considered by a PIC in determining retention periods of personal data include but are not limited to:

- (1) legal requirements which the company may be subject to;
- (2) applicable prescription periods in existing laws; and
- (3) industry standards, and other laws and regulations that apply to the sector.<sup>7</sup>

Thus, both your company and the local electric cooperative are considered as PICs with respect to the personal data of the customers. Both entities are therefore expected to be accountable for the personal data it processes to the end that the data subjects are protected from harm and other privacy risks.

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

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

---

5            5 Id. § 21

6            Id. §11 (e)

7            National Privacy Commission, NPC Advisory Opinion No. 2017-24 (21 June 2017).

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-015<sup>1</sup>

24 August 2023

[REDACTED]  
[REDACTED]  
[REDACTED]

## RE: DISCLOSURE TO THE NATIONAL BUREAU OF INVESTIGATION OF THE RECORD OF BARANGAY INHABITANTS

Dear [REDACTED]

We respond to your request for an Advisory Opinion on the above matter. We gather that your office received a letter from the National Bureau of Investigation (NBI) requesting for certified true copies of the list of all inhabitants in the building/s located at 14 General Malvar Street, Brgy. San Antonio, Pasig City. The NBI also asked for the certified true copies of the Record of Barangay Inhabitants by Household, the Individual Record of Barangay Inhabitant, and all other available records pertaining to the inhabitants (Records) that may aid it in its investigation.

We note from the NBI's letter that their request for information is pursuant to their ongoing investigation brought about by the request of ION Real Estate Development Corporation (IREDC). It appears that professional squatters and squatting syndicates are allegedly occupying a parcel of land situated in Escriva Drive, Brgy. San Antonio, Pasig (the Barangay).

Specifically, you ask the following:

1. Can your office be compelled to release or share the names and/or records of Barangay inhabitants to the NBI as part of the latter's investigation to determine if there are professional squatters or squatting syndicates in the address mentioned?
2. Whether Department of Interior and Local Government Memorandum Circular No. 2008-144 dated 19 September 2004, prohibits sharing and disclosure of RBI Form A and Form B sans consent of the owner.

*DILG Memorandum Circular No. 2008-144*

Department of Interior and Local Government Memorandum Circular No. 2008-144 dated 19 September 2008 (MC 2008-144) calls for the maintenance and updating of

---

<sup>1</sup> Tags: special cases; disclosure to public authority; general data privacy principles; list of barangay inhabitants

records of all barangay inhabitants to achieve the following purposes:

- For easy identification of inhabitants;
- As a tool in planning; and
- As an updated reference in the number of inhabitants in a specific Barangay.

Relevantly, MC 2008-144 instructed the City/Municipal Mayors and Punong Barangays to adopt necessary measures to ensure that the right to privacy of the inhabitants will be observed in the process of maintaining and updating said records, viz.:

d. Data collected and stored for this purpose shall be kept and treated as **strictly confidential and a personal written authorization of the Owner shall be required for access and disclosure of data.**

xxx

f. The **Chief of Police** and **Local Civil Registrar** may, from time to time, be allowed to verify the records kept by the Barangay Secretary, when circumstances warrant.

(Emphasis supplied).

It is clear from the above-quoted provisions that MC 2008-144 requires the owner's personal written authorization prior to the access and disclosure of his/her data. Hence, a mere letter request does not suffice. Moreover, the NBI is not among those expressly enumerated in MC 2008-144 to verify the Records kept by the Barangay Secretary.

*Section 4 (e); special cases; disclosure to public authority;*

To justify its request, the NBI cited Section 4(e) of the Data Privacy Act of 2012<sup>2</sup> (DPA) and proceeded to claim that the information it requests is exempt from the DPA, viz.:

This request is in pursuant (sic) to Sec. 4 (e) of RA 10173 otherwise known as the Data Privacy Act of 2012 stating that information requested by law enforcement agencies that is necessary to carry out its functions is **not covered by the act.**

(Emphasis supplied)

To avoid confusion, it is necessary to discuss the proper application of Section 4(e) of the Data Privacy Act of 2012 (DPA). NPC Advisory Opinion No. 2021-028 provides a relevant explanation as to the application of Section 4(e) of the DPA and Section 5(d) of the Implementing Rules and Regulations of the DPA, thus:

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.<sup>3</sup> 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, disclo-

<sup>2</sup> 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).

<sup>3</sup> Id. § 4 (e) (2012).



sure 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.<sup>4</sup> (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.”<sup>5</sup>

Applying the foregoing, Section 5 of R.A. No. 10867<sup>6</sup> provides for the general investigative jurisdiction of the NBI. Meanwhile, Executive Order No. 153, Series of 2002,<sup>7</sup> as amended by Executive Order No. 231, listed the NBI as one of the relevant agencies called to give their support, assistance, and cooperation in the identification of professional squatters and squatting syndicates, monitor and launch operations, through the proper agency or body, to curtail their activities.<sup>8</sup>

Hence, the officials of the Barangay may provide the personal information requested by

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

5 See: National Privacy Commission, NPC Advisory Opinion No. 2019-022 (07 May 2019) and NPC Advisory Opinion No. 2020-015 (24 Feb 2020).

6 NBI Reorganization and Modernization Act.

7 Instituting the National Drive to Suppress and Eradicate Professional Squatting and Squatting Syndicates, Amending Executive Order Nos. 178, s. 1999 and 129, s. 1993, and for Other Purposes, Executive Order No. 153, [December 10, 2002]

8 Id. § 3

the NBI provided that a formal subpoena has been issued to ensure that the request is authorized, proper, and lawful under existing rules and regulations.

*Processing provided for by existing laws and regulations;  
public authority;*

It is readily apparent from the sample form of the Records sent to us that they contain both personal information<sup>9</sup> and sensitive personal information,<sup>10</sup> the processing of which must be supported with the appropriate legal criteria provided under the DPA.

In processing personal information, the Barangay and the NBI may rely on Section 12 (e) of the DPA, which provides that the processing of personal information shall be permitted when it is necessary to fulfil the functions of a public authority which includes the processing of personal data for the fulfillment of its mandate.

Meanwhile, the processing of sensitive personal information must find basis under Section 13 of the DPA. Among the sensitive personal information included in the Records are date of birth, age, civil status, citizenship, and thumbmark.

Section 13 (f) recognizes processing for the establishment, exercise, or defense of legal claims, viz.:

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

x x x

(f)The processing concerns such personal information as is necessary for the protection of lawful rights and interest of natural or legal persons in court proceedings or the establishment, exercise, or defense of legal claims, or when provided to government or public authority.<sup>11</sup>

It must be noted that in determining whether a request based on the aforementioned provision should be granted, “the legitimacy of the purpose and the proportionality of the request (should) be taken into consideration.”<sup>12</sup>

We emphasize that, similar to the processing of personal information, the release of sensitive personal information to NBI personnel should also be upon a subpoena. Further, the Barangay should establish a system to avoid abuse and ensure that the requested information shall be limited only to the legitimate interest stated by the requesting party. As we stated in Advisory Opinion No. 2022-005<sup>13</sup> regarding a similar concern:

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

9 Data Privacy Act of 2012, § 3 (g).

10 Id. § 3 (l).

11 Id. § 13 (f).

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

13 National Privacy Commission, NPC Advisory Opinion No. 2022-005, 24 February 2022.

the purpose/s indicated. In Advisory Opinion No. 2021-044, it was recommended that in case a request for personal information is granted, the requesting party should be required to sign an undertaking that the information will only be used for the purpose that was declared: Should the CHMSC grant the request, it is suggested that the Requesting Party be required to sign an undertaking that the use of the documents will only be for the purpose of filing a complaint with the Ombudsman and that the proper disposal thereof is ensured if he does not push through with the filing of the complaint. Further, the undertaking must include a clause to the effect that the requestor acknowledges that he becomes a PIC by his receipt of the requested documents and therefore has the obligations of a PIC as prescribed under the DPA. Thus, LTO should similarly require a requesting party to sign an undertaking that the information that will be acquired will only be used for the purpose which was declared and authorized.

*General data privacy principles; legitimate purpose; proportionality*

We reiterate that the *Barangay*, as a Personal Information Controller (PIC), must adhere to the general data privacy principles under the DPA. In particular, 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.<sup>14</sup> Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.<sup>15</sup>

We thus advise that any disclosure of personal data should only contain relevant information necessary to achieve the purpose of determining if there are professional squatters or squatting syndicates in the subject property.

The *Barangay* may consider redacting personal information and sensitive personal information that may be considered as excessive and not relevant, suitable, or necessary to the purpose. It may also seek ask the NBI to detail its request instead of a general request for “*all other available records pertaining to the inhabitants that may aid [the NBI] in its investigation*”.

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

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

---

<sup>14</sup> Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (c) (2016).

<sup>15</sup> *Ibid.*

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-016<sup>1</sup>

08 September 2023

[REDACTED]

## RE: APPLICABILITY OF SOFT OPT-IN APPROACH IN THE PHILIPPINES

Dear [REDACTED]

We respond to your request for an Advisory Opinion on whether “soft opt-in” approach under the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications (ePrivacy Directive) is permissible in our jurisdiction.

You state in your letter that Recital 47 of the GDPR explicitly provides that “[T]he processing of personal data for direct marketing may be regarded as carried out for a legitimate interest.” On the other hand, while the general rule under the e-Privacy Directive is that opt-in consent is required before a company can engage in marketing communications, the exception is that marketing emails may be sent on an opt-out basis if the recipient’s details were collected “in the context of the sale of a product or a service.”<sup>2</sup> You further state that the GDPR and ePrivacy Directive, taken together, have generally enabled companies located in and targeting customers within the European Union and European Economic Area to send direct marketing communications to individuals whose details were obtained by a company in the context of a sale of a product or a service, or even during negotiations in pursuit of such a purchase.

Such a method, called the “soft opt-in” approach, may be adopted by companies if the following general conditions are fulfilled:

1. The company collects the individual’s personal information during discussions about the sale of a product or a service;
2. At the time that their personal information was collected, the individual had not explicitly opted out of receiving other related communications from the company;
3. The company intends to send marketing communications about its products

<sup>1</sup> Tags: (topics related to the subject of the advisory opinion, separated by commas).  
<sup>2</sup> Article 13(2), e-Privacy Directive.

and services, and items related to said products and services, to the individual;  
and

4. The company provides a simple and free mechanism through which the individual may opt-out of subsequent marketing communications from the company.

You thus submit that while there is no equivalent provision for “soft opt-in” under the Data Privacy Act of 2012 (DPA), such an approach may be allowed as long as the conditions enumerated above are also fulfilled, and the fundamental rights and freedoms of the data subject are upheld. Moreover, the foregoing conditions set clear limits on what type of direct marketing communication a company may engage in and provide ample protection to data subjects against misuse of their personal information.

### *Consent; Direct Marketing*

For context, the DPA defines consent 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.<sup>3</sup> Consent shall be evidenced by written, electronic or recorded means.<sup>4</sup>

Thus, consent under the DPA must be expressly given wherein the data subject voluntarily agrees to the processing of personal information. An implied, passive or negative consent does not meet the requirements of the law, including an opt-out approach wherein a data subject is merely notified of the period within which to object to the processing of his or her personal information.<sup>5</sup>

In the scenario you provided, the data subject’s personal information was collected by the company during discussions about a sale of a product or service, and such data subject has not explicitly opted-out from receiving other related communications from the company. Further, the company intends to send marketing communications to the data subject about its products or services and items related thereto. The company shall then provide a simple and free mechanism for the data subject to opt out of the subsequent marketing communications.

It, thus, appears that the consent relied upon by the company for its marketing communications will be based on the inaction of the data subject. It is worth noting that the data subject, at the time of the collection of his or her personal information, did not expressly agree to receive marketing communications from the company. Rather, there was only an absence of the data subject’s explicit opt-out from receiving marketing communications. Considering that the consent of the data subject is implied, there is no evidence of his or her assent through written, electronic or recorded means which is required under the DPA.

We reiterate that implied or inferred consent is not recognized in this jurisdiction. The data subject’s consent must never be assumed, regardless of the lack of explicit

objection. It is also worth noting that the DPA, unlike the e-Privacy Directive, does not provide for a similar exception to the express consent rule. Hence, the soft opt-in approach under the e-Privacy Directive cannot be applied in the Philippine setting.

---

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

4 Ibid.

5 See NPC Advisory Opinion Nos. 2017-31 and 2017-42.

*Legitimate interest as lawful criterion for marketing communications.*

Since the DPA does not consider the soft opt-in approach as valid consent for purposes of marketing communication purposes, you may rely on the other lawful criteria for processing stated under Section 12 of the DPA.

In particular, legitimate interest under Section 12(f) of the DPA may be utilized as a lawful criterion. NPC discussed the elements for processing based on legitimate interest in *MAF v. Shopee, Inc.*, <sup>6</sup>viz.:

Processing based on legitimate interest requires the fulfillment of the following conditions: (1) the legitimate interest is established; (2) the processing is necessary to fulfill the legitimate interest that is established; and (3) the interest is legitimate or lawful and it does not override fundamental rights and freedoms of data subjects.

For the lawful criteria of legitimate interest to apply, the foregoing conditions must be satisfied. In the current matter, the legitimate interest of the company is to be able to initiate marketing communications with potential customers to sell its products and services. As such, the company must establish: first, that the processing shall be for the sole purpose of pursuing the legitimate interest of the company, which is to be able to send marketing communications about its products and services to potential customers; second, the processing shall only be limited to the personal information necessary and proportionate to achieve its legitimate interest. Hence, only personal information which is necessary for the company to be able to contact the potential customers must be processed. Third, the processing of personal information must be done in the least intrusive way so as not to impede the rights of the data subjects.

As such, considering that all three elements are present in the current matter, Section 12(f) of the DPA is the more appropriate lawful criterion in the processing of potential customers' personal data for direct marketing communications.

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

Please be guided accordingly.

For your reference.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

---

<sup>6</sup> National Privacy Commission, *MAF v. Shopee Philippines, Inc.* [NPC 21-167] (Sept. 22, 2022)

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-017<sup>1</sup>

28 September 2023

[REDACTED]

## **RE: REQUEST OF GOVERNMENT AGENCIES TO ACCESS PNP'S CRIME INFORMATION, REPORTING AND ANALYSIS SYSTEM (CIRAS) AND OTHER DATABASES.**

Dear [REDACTED]

This refers to the request of the Directorate for Investigation and Detective Management for an Advisory Opinion on the data privacy implications of the request of some government agencies to access the Philippine National Police's (PNP) Crime Information, Reporting and Analysis System (CIRAS) and other databases.

We understand that CIRAS is a web-based database of the PNP that stores the data of all criminal complaints and reports, as well as the information of the victims and suspects. It includes the narrative reports contained in police blotters nationwide.

We gather that some government agencies have requested the PNP to have direct access to the CIRAS but without stating the purpose thereof. Thus, you seek guidance on whether it is permissible to grant the request considering that it stores both personal information and sensitive personal information.

### *Criminal records containing personal data.*

The Data Privacy Act of 2012 (DPA) protects individual personal information in information and communications systems in the government and the private sector.<sup>2</sup> 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. On the other hand, the DPA classifies the following as sensitive personal information, viz.:

X X X

<sup>1</sup> Lawful Processing; Contractual Obligation; Legitimate Interest; Accountability.

<sup>2</sup> 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) 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;**<sup>3</sup> (Emphasis Supplied)

x x x

Applying the foregoing to your present concern, since the CIRAS contains data of criminal complaints and reports including information pertaining to victims and suspects, its contents are considered as sensitive personal information under the DPA. As a general rule, the processing of sensitive personal information is prohibited. Nevertheless, Section 13 of the DPA provides for instances where processing of sensitive personal information may be allowed, such as when:

(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 by government or public authority.** (Emphasis supplied)

Thus, granting government agencies access to the CIRAS database is considered lawful processing of sensitive personal information as the information shall be provided to the government or public authority.

Furthermore, Section 4 of the DPA also recognizes special cases where the DPA's application may be limited or qualified, thus:

(e) **Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions.** Nothing in this Act shall be construed as to have 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);

(Emphasis supplied)

To assist you in evaluating a request for access by a government agency, it is worth revisiting the relevant discussions in NPC Advisory Opinion No. 2022-06<sup>4</sup> thus:

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

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

**a) The information is necessary in order to carry out the law enforcement**

<sup>3</sup> Ibid, § 3 (g), (l).

<sup>4</sup> National Privacy Commission, NPC Advisory Opinion No. 2022-06 (28 February 2022).



**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 should not be deemed to be a special case.**

Please also note that the interpretation of the aforementioned provision shall be strictly construed - only the specified information is outside the scope of the DPA, and the public authority remains subject to its obligations as a personal information controller (PIC) under the DPA, such as implementing security measures to protect personal data, upholding the rights of data subjects, and adhering to data privacy principles, among others.

(Emphasis Supplied)

As such, there is a basis under the DPA for the PNP to allow other government agencies to access the CIRAS as discussed above. However, each request must still be evaluated taking into account the attendant circumstances of the request for access, the type of personal data sought, and the mandate of the government agency involved.

General data protection principles; proportionality.

Please note that even if there is a legal basis for processing, the DPA does not permit unbridled processing of personal data. Personal Information Controllers (PICs), as the PNP in this case, are still required to adhere to the general data privacy principles set forth under the law.

One such principle is the principle of proportionality which states that the processing of personal data shall be adequate, relevant, suitable necessary and not excessive in relation to a declared specified purpose. It also states that personal data shall only be processed only if the purpose of the processing could not be reasonably fulfilled by any other means.<sup>5</sup> Thus, disclosure of personal data to requesting entities should be limited to its declared, specified, and legitimate purpose. In addition, only those personal data that are needed in relation to the declared and stated purpose should be disclosed to the requesting entities, which may be determined by the PNP on a case-to-case basis.

In NPC Advisory Opinion No. 2020-036,<sup>6</sup> we discussed the matter of inter-agency requests between PICs and its relation to the data privacy principle of proportionality, viz.:

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

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

6 National Privacy Commission, NPC Advisory Opinion No. 2020-36 (8 September 2020)

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 it 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.

(Emphasis Supplied)

Thus, in keeping with the data privacy principles, particularly on proportionality, any request for access to the CIRAS database containing personal data should undergo evaluation and judicious assessment to determine what specific personal data should be disclosed, and if the request is proportional to the purpose sought by the requesting agency.

*Data Subject Rights; safeguards; penalties under the DPA*

Under the DPA, PICs are required to implement organizational, physical, and technical security measures in their processing of personal data. It is imperative that guidelines must be crafted on the grant of access to other government agencies in your organization's Privacy Manual or Manual of Operations. This is to ensure that data subjects' personal data is kept secure and protected. Further, mechanisms should be put in place where data subjects may exercise their rights under the DPA, when appropriate and applicable.

Finally, we emphasize that the DPA is not intended to hamper or interfere with the performance of duties and functions of duly constituted public authorities. 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.

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

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-018<sup>1</sup>

29 September 2023



**RE: REQUEST FOR PERSONAL DATA OF CONDOMINIUM  
TENANTS BY PHILIPPINE DRUG ENFORCEMENT AGENCY  
(PDEA)**

Dear 

We respond to the Philippine Drug Enforcement Agency-National Capital Region's (PDEANCR) request for an Advisory Opinion regarding the data privacy concern of condominium building administrators/managers/owners (collectively, "CAMOs") relative to the PDEANCR's request for information pursuant to its investigations.

You mention that PDEA-NCR's anti-drug operations reveal that condominium units have been utilized as clandestine laboratories, drug dens, or as a venue for other illegal drug-related activities. As such, PDEA-NCR requested various CAMOs for information on the current tenants/owners of condominium units within the National Capital Region (NCR) and any information about suspected illegal drug activities.

However, reports from several PDEA-NCR district offices reveal that most of the CAMOs hesitate to provide the requested information due to the perceived violation of the data privacy rights of the condominium unit owners/tenants. You also inform that barangay officials share in PDEA-NCR's dilemma in connection with their barangay drug clearing programs.

Thus, you ask if the CAMOs within PDEA-NCR's jurisdiction can rightfully refuse the request for information citing the Data Privacy Act of 2012 (DPA).<sup>2</sup>

*Personal Data; special cases; lawful processing;  
Mandate of PDEA.*

The 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. Information about the identity of a person and

<sup>1</sup> Tags: special cases; law enforcement; lawful processing; investigations.  
<sup>2</sup> 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).

his or her corresponding address qualifies as personal data that is subject to protection under the DPA. The processing of personal data must be based on any of the grounds provided in Sections 12 or 13 of the DPA. Some of the provisions relevant to your concern are the following:

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

(a) The data subject has given his or her consent;

xxx

(e) The processing is necessary in order to respond to a 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;<sup>3</sup>

xxx

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

(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

(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 is not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;<sup>4</sup> (Emphasis Supplied)

xxx

On the other hand, Section 5 of the Implementing Rules and Regulations (IRR) of the DPA provides for a list of special cases where the application of the DPA may be limited or qualified, thus:

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

e. Information is 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

3 Id., §12 (a), (e).

4 Id., §13 (a), (b).

No. 9510, otherwise known as the Credit Information System Act (CISA);

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.

We note that under Section 84 (b) of the Republic Act (RA) 9165,<sup>5</sup> PDEA has the mandate to:

Section 84. Powers and Duties of the PDEA. – The PDEA shall: xxx

(b) Undertake the enforcement of the provisions of Article II of this Act relative to the unlawful acts and penalties involving any dangerous drug and/or controlled precursor and essential chemical and investigate all violators and other matters involved in the commission of any crime relative to the use, abuse or trafficking of any dangerous drug and/or controlled precursor and essential chemical as provided for in this Act and the provisions of Presidential Decree No. 1619; x x x

(Underscoring supplied)

RA 9165 also states that one of the powers of PDEA is the issuance of a subpoena relative to the conduct of an investigation, thus:

Section 84. Powers and Duties of the PDEA. – The PDEA shall: xxx

c) Administer an oath, issue a subpoena and subpoena duces tecum relative to the conduct of an investigation involving the violations of this act;<sup>6</sup>

(Underscoring supplied)

Further, PDEA's Code of Professional Conduct and Ethical Standards provides for a list of officials who may issue a subpoena, to wit:

I. Issuance of Subpoena from PDEA – The officers or officials authorized to issue the subpoena pursuant to Section 84(c) of R.A. 9165 include the Director General, and as a delegated authority, the Deputy Directors for Operations and Administration, the Service Directors of Legal and Prosecution Service, Investigation and Intelligence Service, Internal Affairs Service, and Compliance

Service of the National Head Office, and the respective Regional Directors within their areas of jurisdiction, as well as the Director (Head) of Special Enforcement Service.<sup>7</sup>

Considering that PDEA's own rules require the issuance of a subpoena duces tecum, then such procedure must be observed in requesting information involving personal

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 [Comprehensive Dangerous Drugs Act of 2002] (2002), §84(b).

6 Comprehensive Dangerous Drugs Act of 2002, §84(c).

7 PDEA Code of Professional Conduct and Ethical Standards, §1(l).

data from the CAMOs instead of a mere letter. The issuance of a subpoena duces tecum in lieu of a letter- request does not only ensure that due process is observed by PDEA, but it also demonstrates judicious assessment and evaluation of circumstances surrounding the request. It goes without saying that a subpoena also denotes the legitimacy of the operation and its purpose.

Thus, if PDEA-NCR were to course the request for personal information through a validly issued subpoena duces tecum, CAMOs can no longer refuse to furnish them with the information, as it falls under PDEA’s mandate and is in line with the DPA. Nevertheless, it is necessary to point out that having a basis for processing personal data under the law does not give PICs unbridled authority over the personal data collected. PICs, such as PDEA, must still adhere to the guidelines on how to properly process personal information under the DPA.

You also cited in your request our Advisory Opinion 2021-028,<sup>8</sup> and insisted on its application to your situation. To recall, Advisory Opinion 2021-028 involves somehow a similar situation in that a letter was sent by the Bureau of Internal Revenue (BIR) to a condominium corporation requesting the disclosure of personal data of tenants. In allowing the disclosure pursuant to Section 4 of the DPA, we discussed therein the following requirements, viz:

- 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.

At first glance, PDEA-NCR’s present concern appears to be similar to the situation presented in Advisory Opinion 2021-028. However, the difference lies in the fact that the BIR rules allow the issuance of an “access to records letter” pursuant to Sec. 5(b) of the National Internal Revenue Code, unlike the PDEA rules which requires a subpoena duces tecum. Consequently, for PDEA-NCR’s processing to be legal under the DPA, its rules on the issuance of a subpoena duces tecum must be complied with.

#### *Adherence to Data Privacy Principles.*

While the DPA recognizes the mandate of different government agencies, the law is categorical in stating that the processing of personal information must still adhere to the principles of transparency, legitimate purpose, and proportionality. Personal information must be collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purpose only.<sup>9</sup>

---

8 National Privacy Commission, NPC Advisory Opinion No. 2021-028 (16 July 2021).

9 RA No. 10173, §11(a).

For the principle of proportionality, it 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 be fulfilled by other means.<sup>10</sup> It also states that personal data shall only be processed only if the purpose of the processing could not be reasonably fulfilled by any other means.<sup>11</sup> In addition, only those personal data that are needed in relation to the declared and stated purpose should be disclosed to the requesting entities, such as PDEA-NCR.

Thus, in keeping with the data privacy principles, particularly on proportionality, any request for information containing personal data, including the method of request should undergo evaluation and judicious assessment to determine what specific personal data should be disclosed and if the request is proportional to the purpose sought by the requesting agency.

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

Please be guided accordingly.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

---

<sup>10</sup> Id. §13(c).

<sup>11</sup> Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §18 (c) (2016).



# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-019<sup>1</sup>

17 October 2023

[REDACTED]

## **RE: DISCLOSURE OF AN INDIVIDUAL CUSTOMER'S PERSONAL INFORMATION UPON THE REQUEST OF ANOTHER INDIVIDUAL CUSTOMER.**

Dear [REDACTED]

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

You inform that G-Xchange, Inc. (GCash) received a request from one of its individual customers for the home address of another individual customer (Recipient). The requesting customer (Sender) allegedly intended to transfer money from her Land Bank of the Philippines (LBP) account to her GCash account through PesoNet. But she mistyped her registered mobile number which resulted in the money being received by another individual (Recipient) who also happens to be a GCash user. The Sender then requested GCash for the Recipient's name and home address to resolve the situation. In its desire to balance the interest of both data subjects, GCash responded by providing the Sender only with the Recipient's name and registered email address.

However, the Sender deemed the email address as insufficient and insisted that GCash divulge the Recipient's home address. The Sender claims that the purpose for such request is to be able to send a copy of her complaint against the Recipient who allegedly failed to return the funds to her.

GCash hesitates to accede to the Sender's request considering that it already provided the name and email address of the Recipient. Further, it is GCash's position that the Sender's right to access does not include the disclosure to her of the Recipient's home address.

Thus, you ask if the refusal of GCash to provide the recipient's home address is justified under the Data Privacy Act of 2012 (DPA) and other relevant issuances.

---

<sup>1</sup> Tags: special cases; law enforcement; lawful processing; investigations.

### *Processing based on legitimate interest.*

For perspective, it is worth mentioning that an investigation concerning the failure to return funds erroneously sent to a recipient may be considered as an investigation for purposes of fraud prevention. In the current matter, the Recipient was not entitled to the money that was sent to him or her. Accordingly, the Recipient has the obligation to return the money to the Sender.<sup>2</sup> Since the Recipient failed to do so, the Sender would necessarily have to investigate and gather data to protect her rights through the filing of a complaint to recover the money. Hence, the Sender has a legitimate interest to conduct her investigation and process personal data necessary to rectify the alleged fraud committed upon her.

Section 12(f) of the DPA allows the processing of personal information when the same is necessary for purposes of the legitimate interests pursued by the personal information controller or by a third party to whom the personal information is disclosed.<sup>3</sup>

The United Kingdom's Information Commissioner's Office has crafted a three-part test in assessing a claim of legitimate interest as lawful basis for the processing of personal information, thus:

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 personal information controller 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 personal information controller or third party, considering the likely impact of the processing on the data subjects.<sup>4</sup>

In *MAF v. Shopee*,<sup>5</sup> the National Privacy Commission (NPC) adopted the three-part test above and provided the following conditions for processing based on legitimate interest:

Processing based on legitimate interest requires the fulfillment of the following conditions: (1) the legitimate interest is established; (2) the processing is necessary to fulfill the legitimate interest that is established; and (3) the interest is legitimate and lawful and it does not override the fundamental rights and freedoms of data subjects.

Applying the foregoing to the current matter, it appears that while the Sender was able to establish her legitimate interest, the scenario presented do not appear to satisfy the other two (2) requirements. To elaborate, the Sender's established legitimate interest is to recover the amount that was wrongfully sent to the Recipient. However, the disclosure of the Recipient's home address is not completely necessary for the Sender to

file a complaint since Section 16, Rule 14 of the Rules of Court allows for the service of

<sup>2</sup> Article 22, Civil Code of the Philippines.

<sup>3</sup> 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, § 12(f) (2012).

<sup>4</sup> 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/>.

<sup>5</sup> National Privacy Commission, *MAF v. Shopee Philippines, Inc.* [NPC 21-167] (Sept. 22, 2022).

summons when a defendant's whereabouts are unknown.

In addition, it cannot be said that the disclosure of the home address would be proportional to the legitimate interest sought to be protected since the Sender was already provided with the name and registered email address of the Recipient. Such information will permit the Sender to pursue her available remedies. To allow the disclosure of the home address in the given scenario would unnecessarily tilt the balance of rights in favor of the Sender which may possibly result in extreme detriment to the Recipient. It must be borne in mind that the Recipient is also a data subject who possesses privacy rights as well.

The Civil Code of the Philippines prohibits persons from prying into the private lives of other individuals,<sup>6</sup> thus:

Every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons and that the act of prying into the privacy of another's residence and meddling with or disturbing the private life or family relations of another, though it may not constitute a criminal offense, shall produce a cause of action for damages, prevention and other relief:

- (1) Prying into the privacy of another's residence;
- (2) Meddling with or disturbing the private life or family relations of another;
- (3) Intriguing to cause another to be alienated from his friends;
- (4) Vexing or humiliating another on account of his religious beliefs, lowly station in life, place of birth, physical defect, or other personal condition. (Underscoring supplied)

In *Spouses Hing v. Choachuy, Jr.*<sup>7</sup>, the Supreme Court had the chance to elaborate on the right to privacy under the context of Article 26 (1) of the Civil Code. Thus, it was held:

The right to privacy is the right to be let alone.

The right to privacy is enshrined in our Constitution and in our laws. It is defined as "the right to be free from unwarranted exploitation of one's person or from intrusion into one's private activities in such a way as to cause humiliation to a person's ordinary sensibilities." It is the right of an individual "to be free from unwarranted publicity, or to live without unwarranted interference by the public in matters in which the public is not necessarily concerned." Simply put, the right to privacy is "the right to be let alone."

The Bill of Rights guarantees the people's right to privacy and protects them against the State's abuse of power. In this regard, the State recognizes the right of the people to be secure in their houses. No one, not even the State, except "in case of overriding social need and then only under the stringent procedural safeguards," can disturb them in the privacy of their homes. (Internal citations omitted).

In sum, the Recipient's right to privacy in his or her home is afforded protection under the Constitution and the law. This includes the right to be secure in his or her own abode or physical space at any time.

In view of the foregoing, it appears that the Sender was not able to clearly establish her legitimate interest to the home address of the Recipient. Since there is no other lawful criterion to serve as basis for the processing of personal information, Gcash need not

6 Article 26. Civil Code of the Philippines.

7 *Spouses Bill and Victoria Hing v. Alexander Choachuy Sr. and Allan Choachuy*, G.R. No. 179736, June 26, 2013.

disclose the same to the Sender in this instance.

*Data subject request limited to  
own personal data*

It is also necessary to clarify that the Sender's request for the Recipient's home address cannot be considered as a data subject request. As contemplated by law, data subject requests are only limited to details on the processing of the personal information of the data subject himself/herself. These requests do not extend to personal information concerning another data subject.

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

For your reference.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-020<sup>1</sup>

05 October 2023

[REDACTED]

[REDACTED]

[REDACTED]

## **RE: USE OF BREATH ANALYZER ON EMPLOYEES AND SERVICE PROVIDERS.**

Dear [REDACTED]

We respond to your request for an Advisory Opinion regarding the proposed implementation by Entrego Express Corporation (Entrego) of the use of breath analyzers as part of its business operations process.

You state that Entrego is a duly-licensed fulfillment and solutions corporation organized under the laws of the Republic of the Philippines. As part of its efforts to comply with Republic Act No. 10586, otherwise known as the Anti-Drunk and Drugged Act of 2013 (ADDA),<sup>2</sup> Entrego intends to use breath analyzers in the course of the daily deployment of both employee and outsourced drivers (collectively, “data subjects”). The purpose is to prevent vehicular accidents by ensuring that the data subjects are in a good physical and mental state without the influence of alcohol.

Thus, you ask whether the use of breath analyzer falls within the scope of the Data Privacy Act of 2012 (DPA).<sup>3</sup>

<sup>1</sup> Tags: breath analyzers, sensitive personal information, lawful criteria for processing, consent, contract, compliance with legal obligation

<sup>2</sup> An Act Penalizing Persons Driving Under the Influence of Alcohol, Dangerous Drugs, and Similar Substances, and for Other Purposes [Anti-Drunk and Drugged Driving Act of 2013], Republic Act No. 10586 (2013).

<sup>3</sup> 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).

In particular, you seek guidance on the following:

1. Whether or not the collection and processing of personal data through the intended implementation of breath analyzers is allowed under the confines of the DPA, its Implementing Rules and Regulations (IRR), and other issuances of the NPC;
2. Whether or not collecting and processing of personal data through the intended use of breath analyzers involves sensitive personal information;
3. Whether or not the collection and processing through the intended use of breath analyzers fall within any of the criteria for lawful processing; and
4. Whether or not additional consent from the respective drivers would be necessary to implement the use of breath analyzers.

Scope of the DPA; sensitive personal information; health data.

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.<sup>4</sup>The DPA treats certain types of personal information as sensitive personal information, as the unlawful processing thereof may lead to the discrimination of the data subject involved. Health data is among those classified as sensitive personal information.<sup>5</sup>

While the DPA does not define health data, reference could be made to the NPC and Department of Health (DOH) Joint Memorandum Circular (JMC) No. 2020-0002.<sup>6</sup>Provision IV, paragraph 11 of JMC 2020-0002 provides that 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.<sup>7</sup>

As you explained in your letter, a breath analyzer is an equipment which can determine the blood alcohol concentration level of a person through testing of his breath; while blood alcohol concentration is the measure of the amount of alcohol in a person's blood, as defined in Section 3 (b) and (c) of the ADDA, respectively.

From the definition, a breath analyzer determines an individual's present physical condition, i.e., level of alcohol intoxication. Thus, we confirm that use of the breath analyzer entails the processing of the sensitive personal data information of the data subject. Strict compliance with the relevant provisions of the DPA, its IRR, and other issuances of the NPC should therefore be observed.

*Lawful criteria for processing; consent; legitimate interest; legal claims.*

Generally, the processing of sensitive personal information is prohibited unless allowed under the circumstances enumerated in Section 13 of the DPA.

---

4 Id. § 4.

5 Id. § 3 (I).

6 National Privacy Commission and Department of Health, Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response, Joint Memorandum Circular No. 2020-0002 [NPC-DOH Joint Memorandum Circular 2020-002] (April 24, 2020).

7 Id. § IV (11).

It is worth noting that given the nature of the relationship between Entrego and the data subjects, consent is not the most appropriate lawful basis for processing. In an employer-employee relationship, “consent is highly unlikely to be a legal basis for data processing at work, unless employees can refuse without adverse consequence” and that “employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship.”<sup>8</sup>

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. In an employment relationship, there would be concerns as to whether consent was indeed freely given by the employee. Hence, in the scenario presented, a request by Entrego upon the data subjects for additional consent for the use of breathalyzers would not be an appropriate criteria in lawfully processing their sensitive personal information.

Entrego cannot likewise rely on legitimate interest, considering that sensitive personal information is involved. Legitimate interest of Entrego as the Personal Information Controller (PIC) is not one of the allowable instances cited under Sec. 13 of the DPA where sensitive personal information of data subjects may be lawfully processed.

Nevertheless, Section 13 (f) of the DPA allows the processing of sensitive personal information when such 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.

In the current matter, Entrego intends to implement the use of breath analyzers to test the blood alcohol content of the data subjects to ensure that no driver is under the influence of alcohol. This intervention is in line with its obligation under Section 13 of the ADDA, viz:

**Section 13. Direct Liability of Operator and/or Owner of the Offending Vehicle. –**

The owner and/or operator of the vehicle driven by the offender shall be directly and principally held liable together with the offender for the fine and the award against the offender for civil damages unless he or she is able to convincingly prove that he or she has exercised extraordinary diligence in the selection and supervision of his or her drivers in general and the offending driver in particular.

This section shall principally apply to the owners and/or operators of public utility vehicles and commercial vehicles such as delivery vans, cargo trucks, container trucks, school and company buses, hotel transports, cars or vans for rent, taxi cabs, and the like. (Emphasis supplied).

Entrego’s legitimate purpose of having its drivers undergo a breath analyzer falls within the meaning of processing sensitive personal information to establish, exercise, or defend legal claims. We note that, although there is no actual or expected legal claim at the time the breath analyzers are administered, the purpose is to establish that Entrego is exercising extraordinary diligence in the supervision of its drivers as required by the ADDA, and to defend against any potential claims in the event any of its drivers become involved in a vehicular accident.

---

8 ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 2/2017 on data processing at work, available at [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=610169](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169)

*Privacy notice*

We highly suggest that Entrego provide a Privacy Notice to the drivers that enumerates the nature, purpose, and extent of the processing of their personal data including, among others, the risks and safeguards involved. It should also contain provisions relating to the retention period and secure disposal of the personal data collected.

In drafting the Privacy Notice, Entrego should also consider the use of plain and simple language to inform their drivers of how exactly their data will be used and the consequences of undergoing and refusing to undergo breath analysis.

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

For your reference.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office



# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-021<sup>1</sup>

19 October 2023

[REDACTED]

## RE: ACCESS TO DOCUMENTS RELATIVE TO A BUSINESS PERMIT APPLICATION.

Dear [REDACTED]

We respond to your request for an Advisory Opinion on whether a non-party may be allowed access to the documents attached to a business permit application pursuant to Section 4 of the Data Privacy Act of 2012 (DPA), and the public's right to information.

We gather that your law firm requested the Business Permit and License Office (BPLO) of San Juan City for the production of an individual's Business Permit Application, its attachments, and the corresponding Permit to Operate Business (PTOB). As justification, you reasoned that the information you seek are excluded from the scope of the Data Privacy Act of 2012 (DPA)<sup>2</sup> particularly Section 4 (c) of the DPA.

However, the BPLO denied your request on the grounds of confidentiality and data privacy. Nevertheless, the BPLO stated that they can issue the approved PTOB but not the submitted application documents and attachments which led to the issuance of the PTOB.

You acknowledge that Section 4 of the DPA provides for instances where the DPA does not apply; and the non-applicability of the DPA to the information mentioned therein is only to the minimum extent of processing necessary to achieve the specific purpose, function, or activity concerned.<sup>3</sup> However, you posit that any member of the public should be able to scrutinize government transactions that are of a discretionary and financial nature so that the public may, among others, be properly guided in their "social transactions" and as a recognition of the public's right to access information on matters of public concern.

<sup>1</sup> Tags: non-applicability of DPA; special case; business permit and supporting documents.

<sup>2</sup> 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).

<sup>3</sup> Section 5, IRR of the DPA.

Thus, you ask if your client should be granted access by the BPLO to the submitted Business Permit application and its attachments based on the public's constitutional right to access information on matters of public concern which, you state, is expressly recognized as a limitation to the DPA.

*Scope of the DPA; Section 4 – special cases; disclosure under special cases.*

Section 4 (c) of the DPA speaks of 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.

In the issuance of a PTOB, the applicant will submit documentary requirements requested by the BPLO.<sup>4</sup> Once all requirements are submitted, the BPLO will register and/or issue the concomitant license or permit as part of their regulatory mandate. The BPLO, however, does not have discretionary powers to determine who gets issued a PTOB or not. As such, Sec. 4 (c) of the DPA is not the applicable provision concerning your request for disclosure of documents.

*Lawful processing; Section 12 (f) and 13 (f); legal claims.*

The more appropriate basis for disclosure of the requested data would be Sections 12 (f) and 13 (f) of the DPA. The requested information appears to be 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.<sup>5</sup>

In *KRL v. Trinity University of Asia, etc.*,<sup>6</sup> the NPC clarified that a document containing sensitive personal information of an individual used for the purpose of establishing legal claims under Section 13 (f) of the DPA may be considered as a legitimate interest. The same case further held that in cases involving personal information, the protection of lawful rights and interests under Section 13 (f) of the DPA is considered as a legitimate interest contemplated by Section 12 (f) of the DPA.

*Data privacy principles; proportionality*

Despite the existence of a legal basis for processing, the DPA does not permit unbridled processing of personal data. Personal Information Controllers (PICs) are still required to adhere to the general data privacy principles set forth under the law.

One such principle is the principle of proportionality which states that the processing of personal data shall be adequate, relevant, suitable, necessary and not excessive in relation to a declared specified purpose. It also states that personal data shall only be processed if the purpose of the processing cannot be reasonably fulfilled by any other means. Thus, disclosure of personal data to requesting individuals should be limited to its declared, specified, and legitimate purpose. In addition, only those personal data needed in relation to the declared and stated purpose should be disclosed to the requesting entities.

<sup>4</sup> San Juan City, Business Permit and Licensing Office, available at [https://www.sanjuacity.gov.ph/SanJuanCity/Makabagong\\_SJ\\_DLForms](https://www.sanjuacity.gov.ph/SanJuanCity/Makabagong_SJ_DLForms)

<sup>5</sup> Id. § 13 (f)

<sup>6</sup> CID Case No. 17-K-003.

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

Please be guided accordingly.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-022<sup>1</sup>

28 November 2023

[REDACTED]

## RE: MEDIA ACCESS TO POLICE BLOTTERS

Dear [REDACTED]

We respond to your request for an Advisory Opinion on the apparent conflict between the media's right to access a police blotter for journalistic purposes vis-à-vis the confidential treatment by the Philippine National Police (PNP) of the same.

We were informed that you initiated a meeting with some officials of the PNP and of the National Privacy Commission (NPC) where you raised the concern that some media reporters are being prohibited from accessing the contents of police blotters. You argued that such prohibition violates the freedom of the press and of the right of the people to information.

For its part, the PNP cited PNP Memorandum Circular (MC) No. 2020-037<sup>2</sup> as their basis for the prohibition. PNP MC No. 2020-037 essentially states that the police blotter shall be treated with confidentiality since it contains personal information of complainants, victims, and suspects. Citing the Data Privacy Act of 2012 (DPA), the PNP limits access to the police blotter only to a real party-in-interest or upon order of a court. Media practitioners, however, may submit a data request to the Public Information Officer (PIO) of the police station, which will be treated similarly to a Freedom of Information (FOI) request.

Thus, you seek the NPC's opinion relative to the application of the DPA on the parties' seemingly opposing positions. of public concern.

*Personal data; lawful criteria for processing;  
Sec. 4(d), special cases*

Under the DPA, personal information refers to any information whether recorded in a material

<sup>1</sup> Tags: press freedom; journalistic purpose, special case; freedom of information; security measures.  
<sup>2</sup> Philippine National Police, Police Blotter and CIRAS Information Access, Memorandum Circular No. 2020-037 (May 20, 2020).

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.<sup>3</sup>

On the other hand, sensitive personal information refers to information:

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

As can be gleaned from the foregoing, a police blotter would, *a fortiori*, contain either personal information or sensitive personal information (collectively referred to as "personal data").

Generally, the processing of personal data requires the establishment of the applicable lawful basis provided in Sections 12 and/or 13 of the DPA. Nevertheless, Section 4(d) of the DPA expressly treats as a special case the processing of personal data for journalistic, artistic, literary or research purposes. This means that the media need not establish the lawful basis for processing of the personal data contained in a police blotter. But this exception afforded to the media does not equate to unbridled processing. The DPA limits the processing only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned.<sup>5</sup>

*Right to information vs. right to data privacy;  
balancing of interests.*

The people have a fundamental right to information particularly on matters of public concern. Every Filipino citizen is afforded this right, subject to certain limitations provided by law. 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.<sup>6</sup>

Equally recognized is the fundamental human right to privacy which is afforded protection by both the 1987 Constitution and the DPA. In essence, the privacy right protected by the DPA involves 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.<sup>7</sup> To strike a balance to these seemingly opposing rights, a brief discussion of the relevant laws involved is, thus, necessary.

Executive Order (EO) No. 02<sup>8</sup> relates to the operationalization of the people's right to information

3 Republic Act No. 10173, § 3(g).

4 Republic Act No. 10173, § 3(l).

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

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

7 NPC Advisory Opinion No. 2020-026 (June 26, 2020).

8 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

under the executive branch. EO No. 02 permits the disclosure of information in the possession or under the custody of the government unless they fall under any of the exceptions enshrined in the Constitution, existing law or jurisprudence. Pursuant to the Inventory of Exceptions to EO No. 02,<sup>9</sup> information deemed confidential for the protection of the privacy of persons is an exception to the general rule on the right of access to information.

It has been held that access to public documents may be duly regulated, despite their nature as such. Thus, the Supreme Court ruled in *Legaspi vs. Civil Service Commission*:<sup>10</sup>

A distinction has to be made between the discretion to refuse outright the disclosure of or access to particular information and the authority to regulate the manner in which the access is to be afforded. The first is a limitation upon the availability of access to the information sought, which only the Legislature may impose (Art. III, Sec. 6, 1987 Constitution). The second pertains to the government agency charged with the custody of public records. Its authority to regulate access is to be exercised solely to the end that damage to, or loss of, public records may be avoided, undue interference with the duties of said agencies may be prevented, and more importantly, that the exercise of the same constitutional right by other persons shall be assured.

In the present case, the people’s right to information, exercised through the media, should be considered alongside the PNP’s obligation as a personal information controller (PIC) to protect the personal data of individuals. Thus, a public record does not equate to public access in all cases, especially when there are other rights to be considered, such as the right to data privacy.

Consequently, the PNP may establish regulations or guidelines to properly safeguard personal data in police blotters, which includes classifying the information contained therein to determine the appropriate security measures to put in place. This is also in line with the provisions in E.O. No. 02, which allows for certain exceptions as to the disclosure of information marked as confidential by the appropriate government agency or authority.

It appears that PNP MC No. 2020-037 does not seek to prohibit the media from obtaining information contained in the police blotters. Rather, it only regulates the media’s access only to information that is necessary and proportionate to their purpose. As blotter entries are not considered official complaints or cases filed in court, the dissemination of its contents to the public without proper context may lead to a violation of the right of an accused to be presumed innocent until proven guilty. Moreover, unqualified processing or publication of news reports may prejudice the advancement of cases filed in court.<sup>11</sup>

If the media wishes to report on a specific incident listed in the police blotter, they can submit a data request to the PIO of the police station to access the specific police blotter entry, which the latter should not refuse without citing a legal ground. By doing so, media reporters can still acquire information on a matter they intend to cover; at the same time, the PNP can ensure that the personal data of individuals in the police blotter logbook are duly protected.

#### *Data privacy principles; proportionality*

Furthermore, the provisions of PNP MC No. 2020-037 on the submission of a data request to the station’s PIO is an example of the PNP’s adherence to the general data privacy principles set forth under the DPA.

Specifically, under the principle of proportionality which provides that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared specified purpose. This principle further states that personal data shall only be processed only

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

10 G.R. No. L-72119 (1987).

11 PNP MC No. 2020-037, § 3 (2020).

if the purpose of the processing could not be reasonably fulfilled by any other means.<sup>12</sup> Thus, disclosure of personal data to requesting entities, in this case the media, should be limited to its declared, specified, and legitimate purpose. In addition, only those personal data that are needed in relation to the declared and stated purpose should be disclosed to the requesting entities, which may be determined by the PNP on a case-to-case basis through its PIO.

PNP MC No. 2020-037 seeks to balance the interests concerning the media's right to information on access to police blotter entries, while adhering to the data privacy principle of proportionality by ensuring that only the necessary information are disclosed by the PNP stations or personnel to the media.

The freedom of the press is duly recognized, allowing the media to perform their functions whilst also allowing the PNP to perform its obligation as a PIC to protect the information of individuals whose personal data have been entrusted to them.

In sum, the PNP's classification of information in police blotter entries as confidential under PNP MC No. 2020-037 appear to be within its lawful mandate as a PIC and in accordance with the DPA. These guidelines do not run counter to the provisions of the DPA on special cases involving personal information processed for journalistic, artistic or literary purposes, considering that what is only regulated is the level of access to the information contained in the police blotter, and does not operate as a total prohibition in accessing the information itself.

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

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

---

<sup>12</sup> Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §18 (c) (2016).

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-023<sup>1</sup>

28 November 2023

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

**RE: REQUEST BY A THIRD-PARTY FOR ACCESS TO THE  
SUPPORTING DOCUMENTS RELATIVE TO HER FATHER'S  
APPLICATION FOR A MARRIAGE LICENSE.**

Dear [REDACTED]

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

You state in your letter that you received a request from a certain [REDACTED] (Requesting Party) for the certified true copies of the supporting documents that were used by her deceased father in his application for a marriage license. Attached to her request are the unregistered death certificate of her father, the Requesting Party's birth certificate, and a special power of attorney executed in her favor by her paternal grandmother. However, the Requesting Party failed to present any authority to obtain such documents from the other party to the marriage license.

You thus ask whether the Requesting Party is qualified to obtain the requested documents.

*PSA Memorandum Circular No. 2019-15;  
nature of supporting documents for marriage  
license application*

The Philippine Statistics Authority (PSA) issued Memorandum Circular (MC) No. 2019-15 to provide guidelines for requests for the issuance of Certificate of Live Birth, Certificate of Death, Certificate of Marriage, and Certificate of No Marriage/Advisory on Marriage.

A cursory reading of MC No. 2019-15 shows that it does not cover requests for supporting documents relative to the foregoing certificates. Be that as it may, the request for copies of the supporting documents may be considered as a data subject request under the Data Privacy Act of 2012 (DPA).

---

<sup>1</sup> Tags: press freedom; journalistic purpose, special case; freedom of information; security measures.



## *Sensitive personal information*

Parties applying for a marriage license are required to submit the following documents to the civil registrar:

1. Sworn application;
2. Original birth certificate or baptismal certificate;
3. Death certificate or decree of absolute divorce or judicial decree of annulment or declaration of nullity of marriage, in case either of the parties has been previously married;
4. Parental consent, in case either or both of the parties are between the ages of eighteen (18) and twenty-one (21);
5. Parental advice, in case either or both of the parties are between the ages of 21 and twenty-five (25);
6. Certificate stating that the parties have undergone marriage counseling, in cases where parental consent or advice is needed; and
7. Certificate of legal capacity to contract marriage, in case either or both of the parties are citizens of a foreign country<sup>2</sup>

It is readily apparent from the enumerated documents above that they contain sensitive personal information as the term is defined in the DPA.<sup>3</sup> As such, its processing is generally prohibited except when it falls under any of the circumstances provided in Section 13 the DPA.

It is worth noting that although the Requesting Party did not specify the reason for her request, it is reasonable to assume that it is intended for the establishment, exercise or defense of a legal claim. In which case, Section 13(f) of the DPA applies:

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

xxx

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

The National Privacy Commission (NPC) clarified in *BGM v. IPP*<sup>5</sup> that the term “processing as necessary for the establishment of legal claims” does not require an existing court proceeding, thus:

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

<sup>2</sup> Philippine Statistics Authority, Registration of Application for Marriage License available at <https://psa.gov.ph/content/registrationapplication-marriage-license> [last accessed 20 April 2023].

<sup>3</sup> 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, Republic Act No. 10173, [Data Privacy Act of 2012], § 3(l).

<sup>4</sup> Data Privacy Act of 2012, § 13(f).

<sup>5</sup> 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 20 April 2023).

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.

(Underscoring supplied)

In the current matter, you may ask the Requesting Party to state the purpose of her request. Once it becomes clear that her purpose falls within the provision above, you may then provide her with the requested documents subject to the data privacy principles as will be discussed further below.

*Data subject request; Right to access; transmissibility of rights*

Data subjects are entitled to various rights under the DPA and its Implementing Rules and Regulations (IRR). Among such rights is the right to reasonable access to, upon demand, the contents of one’s personal information and sensitive personal information (collectively, personal data) that have been processed, among other information relating to the processing of his or her personal data.<sup>6</sup>

We note that the right to access, along with the other rights of data subjects afforded under the DPA, must be read together with Section 17 of the DPA on transmissibility of rights. The provision states that the lawful heirs and assigns of the data subject may invoke the rights of the data subject for which he or she is an heir or assign at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights under the DPA.<sup>7</sup>

The determination as to who are “lawful heirs and assigns of the data subject” may be guided by the provisions of the Civil Code of the Philippines on the laws of succession and the rules on guardianship of incompetent persons under the Rules of Court.

In the instant matter, the Requesting Party was able to provide documents to prove her relationship with her father who is the data subject. Accordingly, under the principle of transmissibility of rights, the Requesting Party may invoke her father’s right to access with regard to the supporting documents used in his application for a marriage license.

*General data privacy principles;*

6 Data Privacy Act of 2012, § 16 (c).

7 Data Privacy Act of 2012, § 17.

*proportionality; reasonable and appropriate security measures*

While there may be lawful basis for the request for documents, the processing or disclosure of personal data must be done lawfully and fairly, with strict adherence to the data privacy principles of transparency, proportionality and legitimate purpose.

The principle of proportionality is of particular relevance to the present concern. This means that the disclosure must be limited only to personal data which may be relevant to the requestor's declared purpose. To reiterate, it is imperative for the Requesting Party to define the purpose for which the supporting documents will be used. As such, personal data which are not relevant may be redacted.

Further, the civil registrar must ensure the protection of the personal data. In particular, the personal information controller must be mindful of the manner by which the requested documents will be disclosed to the Requesting Party. Aside from asking her to define the purpose for which the documents will be used, the Requesting Party must also be asked to sign an undertaking that the documents shall be used solely for that stated purpose. This is to ensure accountability on her part.

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

For your reference.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-024<sup>1</sup>

19 November 2023



## RE: DISCLOSURE OF VESSEL RECORDS FROM REGULATORY AGENCY THRU REQUEST LETTER

Dear [REDACTED]

We respond to your query on whether the Maritime Industry Authority (MARINA) can release to a law firm the copies of the Certificate of Philippine Registration and other records of a vessel owned and operated by a shipping line.

You inform that a law firm wrote your office to request the following documents of a vessel owned by a particular shipping line: (1) Certificate of Ownership; (2) Certificate of Philippine Registry; and (3) Technical Drawing of the subject vessel. These documents are supposedly intended to support their client's claim against the shipping line for unpaid obligations related to the supply of materials and services.

Thus, you raise the following concerns:

1. Whether you may release the requested records relying merely on a request letter; and
2. What documents are required to be presented by the requesting party for the release of such records?

Scope of the DPA; juridical entities;  
Personal information.

The Data Privacy Act of 2012 (DPA)<sup>2</sup> applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing, subject to the exceptions laid down in the law.<sup>3</sup> 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

<sup>1</sup> Tags: Vessel records, scope of the DPA, personal information, juridical entities.

<sup>2</sup> 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).

<sup>3</sup> Data Privacy Act of 2012, § 4.

with other information would directly and certainly identify an individual.<sup>4</sup> Thus, the DPA applies only to the processing of personal information of natural persons, not juridical persons.<sup>5</sup>

Under Circular No. 2013-02<sup>6</sup> of the Maritime Industry Authority (MARINA), all ships of domestic ownership plying the Philippine waters, regardless of size and utilization must be properly registered and issued a Certificate of Philippine Registry. A Certificate of Vessel Registry contains the following information: (1) Name of Vessel; (2) Call Sign; (3) Type of Service; (4) Trading; (5) Homeport; **(6) Name of Company; (7) Business Address;** (8) General particulars, such as the Builder, Year Built, Place Built, amongst others; (9) Register Dimensions and Tonnages; and (10) Particulars and Propulsion System. (Emphasis supplied).

On the other hand, a Certificate of Ownership contains the following information: **(1) Owner/Company; (2) Business Address;** (3) Nationality; (4) Name of Vessel; (5) Body Number; (6) Call Sign; (7) Official No.; (8) Type of Recreational Boat; (9) Builder; (10) Place Built; (11) Year Built; (12) Hull Material; (13) Length; (14) Breadth; (15) Bread; (16) Depth; (17) No. of Engines; (18) Engine Make; (19) Serial Number/s; and (20) Kilowatt. (Emphasis supplied).

It is apparent from the foregoing that the information contained in the certificates that are being sought by the law firm are limited to the vessel. Since no personal information is involved in this scenario, the disclosure of the requested documents falls outside the ambit of the DPA. As such, the disclosure of such information must be determined according to MARINA's rules and other relevant laws and government issuances that govern this kind of processing.

As to your additional query on the disclosure of seafarers' records, this involves the processing of personal data and, hence, must find lawful basis under either Section 12 or Section 13 of the DPA. But the processing of personal information must also be done lawfully and fairly and with strict adherence to the basic data privacy principles. Particularly significant to your query is the data privacy principle of proportionality. This means that MARINA should only disclose such personal information that are adequate, necessary, and relevant to the declared purpose of the law firm. Considering that the personal information of seafarers is not necessary and relevant to the claim for unpaid supplies and services delivered by the law firm's client, we see no lawful basis for the release of said information.

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

For your reference.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

---

4 4Id. § 3 (g)

5 National Privacy Commission, NPC Advisory Opinion No. 2020-002 (06 Feb 2020).

6 Maritime Industry Authority, Revised Rules for the Registration, Documentation and Deletion of Ships Operating in Philippine Waters (January 18, 2023).

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-025<sup>1</sup>

29 December 2023



## RE: MULTI FACE ID INITIATIVE FOR FRAUD PREVENTION

Dear [REDACTED]:

We respond to your request for an Advisory Opinion regarding the Multi Face ID initiative by CIBI Information Inc. (CIBI).

We gather from your request that CIBI aims to be the trusted partner of businesses and consumers for their hiring and lending needs by offering technology solutions to solve customer problems across hiring, lending, and partnering. The goal of CIBI is to assist individuals and organizations (hereafter referred to as “CIBI members”) in optimizing their risk-based credit and hiring decisions through its “proprietary datasets” to be collected from the CIBI members’ customers, borrowers or applicants.

You state that CIBI intends to pursue a project to assist and improve the Philippine financial technology (FinTech) industry in identity mapping and fraud prevention at the onboarding level (the “Project”). The aim is to enable its members by delivering a tool which will provide face recognition on a consortium level supported by a third-party who can provide real-time identity checks. Further, the proposed arrangement is for the FinTech members to contribute the datapoints to CIBI with the latter acting as custodian of the information. CIBI shall then deliver the results to the members who wish to check the accuracy of the application and the consistency of the submitted information.

You further state that as the custodian of information, CIBI undertakes to limit access to only select individuals within the organization. In turn, such individuals shall only release the information to a requesting member following best practices that will protect the data. In addition, only members who contribute data shall be allowed access.

---

<sup>1</sup> Tags: facial recognition, personal information, sensitive personal information.

Your letter also provides that CIBI will establish the following safeguards and features in the implementation of the Project to comply with the Data Privacy Act of 2012 (DPA):<sup>2</sup>

- a. Every data point submitted by the members will be owned by them, not by CIBI;
- b. CIBI will only store information in the cloud with all the required security measures following the SOC 2 standards which covers implementation of encryption and data security;
- c. CIBI will not disclose the full database to any of the members, only on a per pull basis;
- d. Members will obtain the required data consent from their customers and comply with the DPA;
- e. Members will be responsible for adhering to strict security and privacy standards when using the product;
- f. Members will only use the product for its own legitimate business and operation purposes (account opening, credit/loan applications, financing applications, etc.);
- g. CIBI will implement Role-Based Access Control (RBAC) to limit access to data based on job responsibilities (i.e, certain user types cannot access certain product features and data);
- h. CIBI will regularly conduct information security training and will remain compliant with the DPA; and
- i. CIBI and each of the members will enter into a data sharing agreement (DSA) and a specific contract which will include the safeguards and features in place.

In line with the above, you specifically ask the following:

i) Can the participating Fintechs or banks share the following data points to CIBI for the purpose of establishing a database for fraud prevention in the initial stages of application: a) an individual's full name; b) date of birth; c) photo of individual's face; and

ii) Are the proposed safeguards and features compliant with the DPA?

*Personal information; sensitive personal information; biometrics; lawful basis.*

The DPA applies to the processing of all types of personal information and sensitive personal information (collectively, personal data). Personal information is defined as any information whether recorded in a material form or not, from which the identity of the 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.<sup>3</sup>

The full name of an individual is considered personal information. A photo of an individual's face, a form of biometric data, is also considered personal information since it directly and certainly identifies a particular individual. In Advisory Opinion No. 2017-063<sup>4</sup> we discussed the nature of biometrics as personal information, viz.:

<sup>2</sup> 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).

<sup>3</sup> Id. § 3(g).

<sup>4</sup> NPC Advisory Opinion No. 2017-063, (09 February 2017).

As can be gleaned from Republic Act (RA) No. 10367,3 biometrics refer to “the quantitative analysis that provides a positive identification of an individual such as voice, photograph, fingerprint, signature, iris and/or such other identifiable features.”

While under Article 29 Opinion 4/2007 (EU)<sup>5</sup>, a biometric data may be considered both as content of the information about a particular individual as well as an element to establish a link between one piece of information and the individual. As such, it can work as “identifier” for it produces a unique link to a specific individual.

On that note, it must be emphasized that 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.”<sup>6</sup> Corollarily, hand-written signatures, as may be used to identify an individual, is considered as personal information.

In the same manner, unique information relating to an individual or when linked with other information will allow an individual to be distinguished from others, may be treated as personal information.

Thus, the processing of an individual’s full name and photo must find lawful basis under Section 12 of the DPA.

On the other hand, date of birth is considered sensitive personal information as provided under Section 3(l)(1) of the DPA. Considering that the data set intended to be shared includes sensitive personal information, the processing of the entire data may find lawful basis under Section 13 of the DPA. It appears that Sections 13 (a) and 13 (f) of the DPA are the most appropriate lawful bases for the intended processing, viz.:

(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 his or her consent prior to processing;

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.<sup>5</sup>

Naturally, the easiest way to facilitate the lawful sharing of personal data among the participating members and CIBI is to obtain the consent of the individual clients. 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.<sup>6</sup> Thus, prior to the sharing of personal data, the participating CIBI member must inform its individual clients in clear and concise language of the intent to share their personal data to CIBI, its purpose of creating a database with facial recognition features and relevant details involved in the processing. The individual clients’ consent must be evidenced by written, electronic or recorded means pursuant to the requirement of the DPA.

---

<sup>5</sup> Data Privacy Act of 2012, § 13(f).

<sup>6</sup> Id. § 3 (b).



But if the individual clients refuse to give their consent, CIBI may then rely on Section 13 (f) which considers processing pursuant to the establishment of legal claims as lawful basis for processing.

In *BGM v. IPP*<sup>7</sup>, we had the occasion to clarify the nature of processing pursuant to Section 13(f), mainly:

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.

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)

Based on the above, fraud prevention may be considered a legal claim being established by the CIBI member. Consequently, the processing of sensitive personal information pursuant thereto may be allowed.

#### *General data privacy principles; security measures*

While the disclosure of personal data is supported by a lawful basis, CIBI members, as PICs of its clients' personal data, still have the obligation to comply with the other requirements of the DPA. Personal data must be processed lawfully and fairly with strict

---

7 National Privacy Commission, *BGM v. IPP* [NPC 19-653] (Dec. 17, 2020).

adherence to the general data privacy principles.

Personal data must be collected for specified and legitimate purposes which must be determined and declared beforehand and processed only in a way that is compatible with such declared and specific purpose.<sup>8</sup> Further, PICs must ensure that personal data is accurate and relevant at all times.<sup>9</sup> Personal data processed should be proportionate, adequate and not excessive in relation to the purposes for which they were collected.<sup>10</sup> To reiterate, data subjects must be aware of the nature, purpose and extent of the processing of his or her personal data, including the risks and safeguards involved and their rights as data subjects, among others.<sup>11</sup>

Thus, CIBI members must comply with the above requirements in the sharing of its clients' personal data to CIBI. CIBI should inform its clients that the sharing is limited only for purposes of establishing a database to prevent fraud, and that disclosed data shall only be limited to the datapoints necessary for the creation of the database (i.e., full name, date of birth and photo of the client's face).

Please note that once CIBI has received the personal data from its members, CIBI shall also be considered as a PIC. Hence, CIBI must also comply with the above requirements. In addition, CIBI must retain only such personal data for as long as necessary or once the fulfillment of the declared purpose has been achieved, unless such retention is required by other laws. This means that there must be a retention policy regarding the personal data stored in the database.

In addition, CIBI must retain only such personal data for as long as necessary or once the fulfillment of the declared purpose has been achieved, unless such retention is required by other laws. This means that there must be a retention policy regarding the personal data stored in the database. In addition, the data sharing agreement between CIBI and the participating IT-BPO companies should clearly provide for the party's obligations and liabilities not only to each other as contracting parties but to the data subjects as well. This will enable the principle of accountability on the part of CIBI and its members to its data subjects. The same also applies to outsourcing service agreements or similar agreements with service providers that will be engaged in the creation of the database.

PICs are also required to implement reasonable and appropriate physical, organizational and technical security measures to ensure the protection of the processed personal data. Furthermore, personal information controllers are also required to regularly monitor for security breaches and take preventive, corrective and mitigating measures against incidents which may lead to security breaches.<sup>12</sup>

Regarding your second query on whether CIBI's proposed safeguards and features comply with the DPA, we note that the proposed safeguards and features of the Project can be considered physical, organizational, and technical security measures. To determine if the proposed measures are appropriate with the processing of personal data, factors such as the nature of the personal data to be protected, the risks represented by the processing, the size of the organization and complexity of its operations,

---

8 Data Privacy Act of 2012, § 11 (a).

9 Id.

10 Id.

11 Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012" [Implementing Rules and Regulations of Data Privacy Act of 2012] (2016).

12 Data Privacy Act of 2012, § 20 (c) (4).

current data privacy best practices and the cost of security information must be considered.<sup>13</sup> These factors will determine if the personal data subject of processing will be kept safe and well protected.

On whether the proposed safeguards are compliant with the DPA, we wish to clarify that compliance does not end once security measures have been put in place. Compliance is a continuing process, involving regular evaluation on the safeguards' effectivity against encountered and projected risks and threats. We would like to note that a PIC's primary objective should not just be mere compliance with the DPA; instead, a PIC should always make sure that personal data are protected through appropriate and reasonable security measures.

We also recommend conducting a privacy impact assessment (PIA) prior to the launch of the Project to identify potential privacy risks to the data subjects. A PIA is a process used to assess and manage the impacts on privacy of a particular program, project, measure, system or technology product of a personal information controller or a personal information processor.

Lastly, the personal information controller must also establish a mechanism for data subjects to exercise their rights. This mechanism should inform data subjects about their rights under the DPA and the degree of control they have over their data, among others. This mechanism may be lodged with CIBI's Data Protection Officer or with the process owner in charge of implementing the proposed processing system.

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

For your reference.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

---

<sup>13</sup> Id. § 20 (c).

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-026<sup>1</sup>

29 December 2023



## RE: CREATION OF A SHARED EMPLOYEE FRAUD DATABASE

Dear [REDACTED] :

We respond to your request for an Advisory Opinion on CIBI Information, Inc.'s (CIBI) initiative to establish an Employee Fraud Database to prevent and detect fraud that may be perpetuated against employers.

In your letter, you mentioned that a common concern amongst various Information Technology Business Process Outsourcing (IT-BPO) Companies involve employees losing or not returning office-issued equipment. In certain instances, some employees simply disappear and omit the offboarding process. This prompted CIBI to propose the idea of an Employee Fraud Database (the "Project") to its client-members belonging to the IT-BPO sector.

Under the Project, the IT-BPO Companies will provide data points on concerned employees to CIBI. CIBI will then act as the custodian of the submitted information and deliver the results to its members who want to verify if a prospective applicant has committed fraud or any other detrimental act to any employer in the past.

As the custodian of information, CIBI undertakes to limit the access to the database to only a select group of individuals within the organization. These individuals will only release information to requesting members while following the best practices to protect data. Additionally, only CIBI members who contribute data will be granted access to the information.

Your also mentioned that CIBI will establish the following safeguards and features in the implementation of the Employee Fraud Database to comply with the Data Privacy Act of 2012 (DPA):

---

<sup>1</sup> Tags: sensitive personal information; fraud prevention; legal claims.

- a. Every data point submitted by the members will be owned by them, not by CIBI;
- b. CIBI will only store information in the cloud with all the required security measures following the SOC 2 standards which covers implementation of encryption and data security;
- c. CIBI will not disclose the full database to any of the members, only on a per pull basis;
- d. Members will obtain the required data consent from their customers and comply with the DPA;
- e. Members will be responsible for adhering to strict security and privacy standards when using the product;
- f. Members will only use the product for its own legitimate business and operation purposes (preventing fraud and instances of qualified theft);
- g. CIBI will implement Role-Based Access Control (RBAC) to limit access to data based on job responsibilities (i.e, certain user types cannot access certain product features and data);
- h. CIBI will regularly conduct information security training and will remain compliant with the DPA; and
- i. CIBI and each of the members will enter into a data sharing agreement (DSA) and a specific contract which will include the safeguards and features in place.

In line with the above, you now ask the following:

- i. Can the participating IT-BPO Companies share the following datapoints to CIBI for the purpose of establishing a database for fraud prevention and detection which may be perpetuated against employers: a) an individual's full name; b) date of birth; c) whether or not the individual has committed fraud or is under investigation for the possible commission thereof; and
- ii. Are the proposed safeguards and features compliant with the DPA?

*Personal information; sensitive personal information; lawful basis; shared database of employees.*

The DPA considers the name of an individual as personal information. Thus, the processing thereof must comply with the requirements of Section 12 of the DPA.

On the other hand, an individual's date of birth is considered sensitive personal information. The same applies to data relating to an individual's commission of fraud or the fact that an individual is involved in an investigation for the possible commission of fraud.<sup>2</sup>

It must be noted that the data set intended to be shared includes sensitive personal information. As such, the entire data set may be treated as sensitive personal information and, thus, draw the basis for its processing under Section 13 of the DPA. In particular, Section 13 (f) on processing for the establishment of legal claims appears to be applicable, viz.:

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

---

<sup>2</sup> 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).

(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.<sup>3</sup> (Underscoring supplied)

In *BGM v. IPP*, the National Privacy Commission (NPC) explained the nature of processing pursuant to Section 13(f):

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.

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.<sup>4</sup>

Relevant also to the Project is the concept of blacklisting as discussed in Advisory Opinion No. 2017-063, viz.:<sup>5</sup>

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,

<sup>3</sup> Data Privacy Act of 2012, § 13(f).

<sup>4</sup> National Privacy Commission, *BGM v. IPP* [NPC 19-653] (Dec. 17, 2020).

<sup>5</sup> National Privacy Commission, 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 [https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2002/wp65\\_en.pdf](https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2002/wp65_en.pdf)

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.

Applying the foregoing to CIBI's Project, the proposed sharing of data by an IT-BPO Company with CIBI can be considered processing for the purpose of establishing, exercising or defending a legal claim involving a fraudulent act. Consequently, the processing of such sensitive personal information pursuant to such purpose is allowed under the DPA. Nevertheless, while it cannot be gainsaid that a shared database for fraud prevention could potentially improve the operations and integrity of IT-BPO companies, it is also crucial to balance its potential legal implications to the rights and freedoms of the individuals included in the database.

*General data privacy principles; lawful processing; appropriate and reasonable security measures; privacy impact assessment*

Although the disclosure of personal data may be supported by a lawful basis, the IT-BPO Companies, who act as personal information controllers of their employees' personal data, are still required to comply with other requirements of the DPA. The personal data should be processed lawfully and fairly with strict adherence to the general data privacy principles.

Personal data must be collected for specified and legitimate purposes which must be determined and declared beforehand and processed only in a way that is compatible with such declared and specific purpose.<sup>6</sup> In this particular context, we emphasize that personal information controllers must ensure that personal data is accurate, relevant and up to date at all times.<sup>7</sup> Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.<sup>8</sup>

We emphasize that the processing of personal data must be proportionate, adequate and not excessive in relation to the intended purposes for which it was processed.<sup>9</sup> This means that the personal data that can be shared by the IT-BPO companies should be limited only to the data points mentioned or only such personal data that are necessary to create the proposed Employee Fraud Database.

Further, data subjects must be aware of the nature, purpose and extent of the processing of his or her personal data, including the risks and safeguards involved, their rights as data subjects, among others.<sup>10</sup> Mechanisms for rectifying or deleting inaccurate or irrelevant personal data must also be provided to data subjects.

In sum, the IT-BPO Companies must comply with the above requirements when sharing its employees' personal data to CIBI. The participating IT-BPO Companies should inform its employees that the sharing is limited only for purposes of establishing a database to prevent fraud and that the data that will be disclosed shall only be limited to the data points necessary for the creation of the database.

---

6 Data Privacy Act of 2012, § 11 (a).

7 Id. § 11 (c).

8 Ibid.

9 Id.

10 Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012" [Implementing Rules and Regulations of Data Privacy Act of 2012] (2016).

Please note that once CIBI has received the personal data from the participating IT-BPO Companies, it shall also be considered as a personal information controller. Hence, CIBI must also comply with the above requirements. In addition, CIBI must retain only such personal data for as long as necessary or once the fulfillment of the declared purpose has been achieved, unless such retention is required by other laws. This means that there must be a retention policy regarding the personal data stored in the database.

CIBI is also required to implement reasonable and appropriate physical, organizational and technical security measures to ensure the protection of the personal data that was shared by the IT-BPO companies. Furthermore, personal information controllers are also required to regularly monitor for security breaches and take preventive, corrective and mitigating measures against incidents that may lead to security breaches.<sup>11</sup>

As to your second query on whether CIBI's proposed safeguards and features for the Employee Fraud Database comply with the DPA, please note that these safeguards and features can be classified as physical, organizational, and technical security measures. To determine if the proposed measures are appropriate with the processing of personal data, factors such as the nature of the personal data to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security information must be considered.<sup>12</sup> These factors will determine if the personal data subject of processing shall be kept safe and well protected.

We also emphasize that compliance does not end once security measures have been put in place. Compliance is a continuing process, involving regular evaluation on the safeguards' effectiveness against encountered and projected risks and threats. Please also note that a PIC's primary objective should not just be mere compliance with the DPA; instead, a PIC should always make sure that personal data are protected through appropriate and reasonable security measures.

In addition, the data sharing agreement between CIBI and the participating IT-BPO companies should clearly provide for the party's obligations and liabilities not only to each other as contracting parties but to the data subjects as well. This will enable the principle of accountability on the part of CIBI and its members to its data subjects. The same also applies to outsourcing service agreements or similar agreements with service providers that will be engaged in the creation of the database.

We also recommend conducting a privacy impact assessment (PIA) prior to the launch of the Employee Fraud database to identify potential privacy risks to the data subjects. A PIA is a process used to assess and manage the impacts on privacy of a particular program, project, measure, system or technology product of a personal information controller or a personal information processor. It takes into consideration the nature of the personal data to be protected, the personal data flow, the risks to privacy and security caused 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.<sup>13</sup>The frequency of the conduct of a PIA shall depend on, among others, how often the proposed database is being updated (i.e., the introduction of new features).

---

11 Data Privacy Act of 2012, § 20 (c) (4).

12 Id. § 20 (c).

13 NPC Advisory No. 2017-03, Guidelines on Privacy Impact Assessment, 31 July 2017.



IT-BPO Companies and CIBI must also establish a mechanism for the exercise of data subject rights. This mechanism should inform data subjects about their rights under the DPA and the level of control they have over their data.

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

For your reference.

Very truly yours,

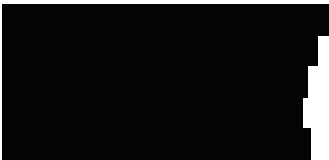
(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2023-027<sup>1</sup>

29 December 2023



## RE: EMPLOYER'S DATA PRIVACY OBLIGATIONS CONCERNING ITS FINANCIAL SERVICES BENEFIT TO ITS EMPLOYEES.

Dear [REDACTED] :

We respond to your request for an Advisory Opinion on the obligations of Infosys BPM Philippines' (IBPM) under the Data Privacy Act of 2012 (DPA)<sup>2</sup> concerning the financial services benefit it desires to extend to its employees.

You state that IBPM is a business process management company. IBPM intends to partner with Templetech Finance Corp (TendoPay) for the provision of financial services to IBPM employees, including the option to obtain loans. Under the proposed partnership, your employees will directly engage with TendoPay to secure their loans. The repayment of these loans may be facilitated through payroll deductions in accordance with relevant legal requirements.

Thus, you ask if you will be classified as a Personal Information Controller and/or Processor under the proposed partnership with TendoPay and your concomitant obligations as such.

### *Personal Information Controller and Personal Information Processor*

The DPA defines a Personal information Controller (PIC) as a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf.<sup>3</sup> Whereas a Personal Information Processor (PIP) refers to any natural or juridical person to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.<sup>4</sup>The decisive element in determining whether an individual or an entity is a PIC or PIP is the existence and level of control over the processing of personal information

Control over personal data exists when an individual or entity has the authority to determine the kind of information gathered, its intended use, or the scope of data processing. It bears stressing that a PIP does not have a right to control the collection, holding, processing, or use of personal information of data subjects. PIPs must process personal data only in accordance with instructions from or under an agreement with a PIC.

Under the proposed scheme, both IBPM and TendoPay will be considered as a PIC. As the employer,

1 Tags: Vessel records, scope of the DPA, personal information, juridical entities.

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 Data Privacy Act of 2012, § 3 (h) (2012).

4 Id. § 3(i).

IBPM is considered as a PIC responsible for managing the personal data of its employees. On the other hand, Tendopay will necessarily have to process the IBPM employees' personal data in order for it to determine if the employees are eligible for the financial services it offers. Hence, Tendopay is likewise considered as a PIC with the concomitant responsibilities of such. Moreover, the proposed partnership will also inevitably involve the sharing of the personal data of IBPM employees with TendoPay. NPC Circular No. 2020-03 defines data sharing 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 personal information controller/s. In this regard, it is important for both entities to manage the shared personal data in a collaborative and responsible manner. We recommend that the parties execute a Data Sharing Agreement (DSA) containing the terms and conditions of the sharing arrangement. Though the execution of a DSA is no longer mandatory under NPC Circular No. 2020-03, it is still considered as a best practice and a demonstration of accountability by the PICs.

Furthermore, as PICs processing employees' personal data, both IBPM and TendoPay must adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. In line with these data privacy principles stated under the DPA, both parties should have a privacy notice informing data subjects of the nature, scope, and purpose of data sharing between the two PICs involved. Furthermore, the PICs should choose the appropriate lawful basis under Sections 12 and 13 of the DPA that is most applicable for the purpose of the intended processing. In this instance, it appears that IBPM and TendoPay have distinct legal bases in processing the employees' personal data. IBPM's processing is anchored on its employment contract with covered data subjects, while TendoPay's lawful basis for processing is for the fulfillment of a loan contract or other financial service to be availed of by the employee. Finally, in adherence to the principle of proportionality, IBPM should only disclose to TendoPay the necessary personal data required to facilitate the utilization of financial services offered by TendoPay.

#### *Obligations of a PIC and PIP*

Apart from adherence to the data privacy principles, PICs also have the duty to uphold data subjects' rights under Sections 16 and 18 of the DPA. The exercise of data subjects' rights will be different for IBPM and TendoPay, since their processing have different purposes.

In addition, Section 20 of the DPA requires PICs to implement reasonable and appropriate physical, organizational and technical security measures for the protection of the personal data of employees. To determine if the security measures are appropriate with the processing of personal data, factors such as the nature of the personal data to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security information must be considered.<sup>5</sup>

Finally, we underscore that both the PICs have the obligation and duty to adhere to the DPA, its IRR, issuances by the NPC, and all other applicable laws. Notably, PICs remain accountable for personal information that is in its control including data outsourced to third parties.<sup>6</sup>

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

For your reference.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

---

<sup>5</sup> Data Privacy Act of 2012, § 20 and § 25.

<sup>6</sup> *Ibid.* § 21.

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2024-001<sup>1</sup>

18 January 2024



## RE: REQUEST FOR ACCESS TO PERSONAL DATA FOR AUDIT PURPOSES

Dear [REDACTED]:

We respond to your request for an Advisory Opinion regarding the Commission on Audit's (COA) request to access personal and sensitive personal information in relation to its performance audit.

You mention that the COA is conducting a performance audit on the COVID-19 National Vaccination Program, which is helmed by the Department of Health (DOH). As part of the audit process, the COA's audit team needs access to the COVID-19 Vaccination Information Management System (VIMS) to review the accuracy and reliability of data generated therefrom. The Epidemiology Bureau (EB) of the DOH maintains processing over the VIMS and serves as the primary source of information for the nationwide vaccination status posted on the DOH website.

However, the DOH expressed concerns about data privacy regarding the COA's request for access to the VIMS. The DOH reasoned that the local government units (LGUs) were solely responsible for collecting the data stored in the VIMS, while EB's role is limited to storing and managing the data in accordance with its mandate. Although the audit team had already conducted tests of the data against the source documents held by the LGUs, the conduct of a national-level review of the data from the VIMS will achieve a different audit objective.

You thus seek guidance on how to conduct the audit process in compliance with the Data Privacy Act of 2012 (DPA).

*NPC Advisory Opinion No. 2020-016;  
constitutional or statutory mandate.*

We reiterate our stance in NPC Advisory Opinion No. 2020-016 in which we acknowledged the authority of the COA as an independent constitutional body and recognized its power, authority, and duty to examine, audit and settle all accounts and expenditures of the funds and properties of the Philippine government.<sup>2</sup> We also stated therein that:

The DPA shall not be used to hamper, or interfere with, the performance of the duties and func-

<sup>1</sup> Tags: processing; audit function; constitutional mandate.

<sup>2</sup> § 2(1), Article IX-D, The 1987 Philippine Constitution.

tions 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.

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.

As such, the COA's intended access to the VIMS database to review its completeness, reliability, and overall performance falls within COA's constitutional mandate and, hence, the processing thereof is generally allowed.<sup>3</sup>

*General data privacy principles;  
Security measures*

Please note that although the COA has the authority to process personal data pursuant to its mandate, it still bears the responsibility of following other rules and regulations laid out in the DPA, its IRR, and any other guidelines set by the National Privacy Commission (NPC). This means that COA must process personal data lawfully and fairly, with strict adherence to the general data privacy principles. It is important to note that personal data collected must be proportionate, adequate and not excessive in relation to the original purposes for which they were collected,<sup>4</sup> which is particularly relevant in the given scenario.

The COA is also required to implement reasonable and appropriate physical, organizational and technical security measures to ensure the protection of the processed personal data. Furthermore, it is also required to regularly monitor for security breaches and take preventive, corrective and mitigating measures against incidents which may lead to security breaches.<sup>5</sup> This is particularly significant as the data being processed are classified as sensitive personal information. Additionally, COA must ensure that the audit is confined only to data related to the COVID-19 National Vaccination Program, as specified in the engagement letter addressed to the DOH.

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

For your reference.

Very truly yours,

(Sgd.)

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

---

3 § 4(e), Data Privacy Act of 2012.  
4 § 11(d), Data Privacy Act of 2012.  
5 § 20 (c) (4), Data Privacy Act of 2012.

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2024-002<sup>1</sup>

19 January 2024



## RE: REQUEST FOR COMMENTS/INSIGHTS REGARDING THE USE OF ARTIFICIAL INTELLIGENCE (AI) IN THE CIVIL SER- VICE COMMISSION'S (CSC) CORRESPONDENCE

Dear [REDACTED]:

We provide this Advisory Opinion upon the referral of the Department of Information and Communications Technology (DICT) as regards your request for comments and insights on the data privacy implications in the use of artificial intelligence (AI) for the Civil Service Commission's (CSC) correspondence.

*On the use of AI in the processing of personal information;  
general principles; data subject rights;  
privacy impact assessment*

According to the Organization for Economic Co-operation and Development (OECD), “[a]n AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.”<sup>2</sup>

We reiterate the discussion in our 18 August 2023 letter that, at present, we see no manifest conflict with the use of AI in relation to the provisions of the Data Privacy Act of 2012 (DPA).<sup>3</sup> The DPA recognizes the policy of the State to ensure the free flow of information and to promote innovation and growth, alongside its duty to protect the fundamental human rights of privacy and of communication.

Section 4 of the DPA states that the law applies to the processing of all types of personal information, save for some exceptions. The DPA does not distinguish as to the type of technology used in the processing of personal information. Hence, whether the processing uses AI technology or not, the processing must abide by the provisions of the DPA as with other means and methods of processing information.

<sup>1</sup> Tags: Artificial Intelligence, General Principles of Privacy, Data Subject Rights, Privacy Impact Assessment.

<sup>2</sup> Organization for Economic Co-operation and Development (OECD), AI terms & concepts, available at: <https://oecd.ai/en/aiprinciples> [last accessed date: 15 January 2024].

<sup>3</sup> An Act Protecting Individual Personal Information in Information and Communication 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)

In other words, personal information controllers (PICs) who are processing personal information using AI technology must adhere to the general principles of privacy, have a lawful basis for processing, implement reasonable appropriate security measures, and uphold data subject rights, among other obligations under the DPA. Consequently, PICs are accountable for the means and methods they use in processing personal information.

Specifically for the principle of transparency in relation to the right of data subjects to be informed and right to rectify, the CSC must provide adequate information to data subjects and have mechanisms in place to enable them to exercise their rights. Please refer to NPC Advisory No. 2021-01: Data Subject Rights for further information.

In addition, the CSC should assess whether the use of any AI technology is fair and proportional to the purpose of processing, considering the risks to the rights and freedoms of data subjects. This may be done by conducting a privacy impact assessment (PIA). For further guidance on PIAs, please see NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments.

*On the use of AI to improve correspondences and communication*

We acknowledge that using AI has its advantages such as improving human productivity. The OECD has also acknowledged its potential:

“Artificial Intelligence (AI) is a general-purpose technology that has the potential to: improve the welfare and well-being of people, contribute to positive sustainable global economic activity, increase innovation and productivity, and help respond to key global challenges. It is deployed in many sectors ranging from production, finance and transport to healthcare and security.”<sup>4</sup>

On this note, we do not see any apparent issues in using AI, such as Chat Generative PreTrained Transformer (ChatGPT), to improve CSC’s correspondence. However, we emphasize that if personal information is processed using such AI, PICs must implement proper safeguards to ensure the protection of the rights of data subjects.

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

For your reference.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

cc :

A large black rectangular redaction box covering several lines of text in the distribution list.

<sup>4</sup> Organization for Economic Co-operation and Development (OECD), Recommendation of the Council on Artificial Intelligence [OECD/Legal/0449], available at: <https://legalinstruments.oecd.org/en/instruments/oecd-legal0449#:~:text=The%20OECD's%20work%20on%20Artificial,respond%20to%20key%20global%20challenges.> [last accessed date: 15 January 2024]

# PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2024-003<sup>1</sup>

02 April 2024



## **RE: RANDOM SURVEILLANCE OF TELECOMMUTING EMPLOYEES AND CONSENT TO THE RECORDING OF VIRTUAL MEETINGS.**

Dear [REDACTED]:

We respond to your request for an Advisory Opinion on the data privacy implications of the employee monitoring policies that your company intends to implement.

You state that your company is a business process outsourcing solutions and information technology-enabled services provider. As such, your employees regularly process personal information of customers, such as their full name, credit card number, card verification number, address, and phone number.

Your company allows its employees to telecommute, or work remotely, using either company-issued equipment or their own device. To provide an additional level of security to prevent mishandling or unnecessary disclosure of confidential data to unauthorized third parties, your company is considering the adoption of certain policies that involve the requisition of web cameras with built-in microphones that will be turned on at random intervals to record short videos (including image and audio) of the subject employee and his/her immediate surroundings. Also, your company intends to record all work-related virtual meetings, conferences, trainings, and coaching sessions.

Thus, you ask whether the Data Privacy Act of 2012<sup>2</sup> (DPA): 1) permits the installation of a monitoring software to randomly record telecommuting employees and their immediate surroundings for purposes of data security; and 2) requires your company to secure the written consent of the employees every time a work-related virtual meetings, conferences, trainings, and coaching sessions (collectively, “virtual meetings”) is held.

---

<sup>1</sup> Tags: Telecommuting, monitoring software, employee surveillance, contract, legitimate interest.

<sup>2</sup> 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).



*Reasonable expectation of privacy.*

Generally, the factual circumstances of each case determine the reasonableness of the expectation of privacy. Similarly, customs, community norms, and practices may limit or extend an individual's reasonable expectation of privacy. The reasonableness of a person's expectation of privacy is, thus, determined on a case-to-case basis.<sup>3</sup>

Nevertheless, it is worth revisiting our discussion in NPC Advisory Opinion No. 2018-090<sup>4</sup> on the application of this concept in the workplace, viz.:

(C)ourts have generally held that employees have a decreased expectation of privacy with respect to work devices, email accounts, and internet surfing activities. The same may be said for the contents therein, since there is an assumption that its use will be limited to work-related purposes.

Yet, with the DPA now in place, the reasonable expectation test should be revisited and interpreted in the context of the law.

By virtue of a legislation on data protection and privacy, the assumption is that individuals now have an expectation of privacy. As to the second element, data privacy is now more than a reasonable expectation – it is now enshrined in the DPA. The reasonable expectation of privacy test then should take into consideration the standards provided under the DPA.

This means that employees must be aware of the nature, purpose, and extent of the processing of his or her personal data in the workplace. The processing of personal information of employees shall also be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. Lastly, the processing of such information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

*Scope of the DPA; personal information; processing; lawful basis; general data privacy principles.*

The DPA applies to the processing of personal and sensitive personal information (collectively, personal data) and to any juridical person involved in the processing of personal information.<sup>5</sup> 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.<sup>6</sup>

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.<sup>7</sup>

---

3 National Privacy Commission, NPC Advisory Opinion No. 2018-090 (28 November 2018).

4 *Id.*

5 Data Privacy Act of 2012, § 4.

6 *Id.* § 3 (g).

7 *Id.* § 3 (j).

The installation of a monitoring software is considered as processing under the DPA since it involves the collection and/or recording of the employees' personal data. As such, a lawful basis must be established for processing of personal data under either Sections 12 or 13 of the DPA.

In the scenario you provided, your company may rely on either Section 12 (b) or 12 (f) of the DPA. Section 12 (b) of the DPA allows processing for the fulfillment of a contract with the data subject. You may utilize this basis as long as the employment contract provides specific provisions allowing the installation of equipment/software for furtherance of employment, including enhancement of productivity of telecommuting employees to ensure that they adapt with flexible working arrangements, for the protection of the interest of the clients or customers, or the enforcement of company policies. In which case, the installation of monitoring software is justified as a necessary consequence of the employer-employee relationship.

On the other hand, Section 12 (f) of the DPA allows processing if it is necessary for the purposes of the legitimate interests pursued by the PIC. We acknowledge that employers have legitimate business interests, such as management of workplace productivity, service quality control or enforcement of company policies, employee safety, protection of business assets, intellectual property or other propriety rights, prevention of vicarious liability where the company assumes legal responsibility for the actions and behavior of employees, compliance with statutory or regulatory obligations that provide, or give reasonable cause, for the preventive monitoring of employees,<sup>8</sup> amongst others. However, they must ensure that the processing activity should be directly related to the legitimate interest being pursued.

Thus, while the processing of personal information based on the legitimate interests of the PIC is allowed under the DPA, an employer must still assess if the installation of a monitoring software will pass the three-part test of legitimate interest, namely:

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

The processing must also comply with the general data privacy principles of transparency, legitimate purpose, and proportionality. In NPC Advisory Opinion No. 2018-084, we stated that it is incumbent upon the employer to determine the purpose/s of computer monitoring which must not be contrary to law, morals, or public policy. Additionally, the principle of proportionality directs the employer to assess the proportionality of the information collected, and the ways and means of processing. This means that the employer shall process information that is adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified purpose. Since the monitoring of the employees' surroundings may result in the capturing of personal data of other

<sup>8</sup> Privacy Guidelines: Monitoring and Personal Data Privacy at Work (April 2016), available at [https://www.pcpd.org.hk/english/data\\_privacy\\_law/code\\_of\\_practices/files/Monitoring\\_and\\_Personal\\_Data\\_Privacy\\_At\\_Work\\_revis\\_Eng.pdf](https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf) (last accessed Feb. 23, 2024).

individuals, the company should determine whether the data collected is proportional to the achievement and fulfillment of the purpose of monitoring and that it clearly aligns with the need and objectives of the organization.<sup>9</sup> Lastly, to ensure adherence to the principle of transparency, the employer should effectively communicate to the employees, through the issuance and dissemination of a policy, the conduct of employee monitoring, the specific purpose, scope and actual method of monitoring, 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.

As to your query on written consent of the employees for virtual meetings, please note that consent may not be the most appropriate basis for such processing since employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the company-employee relationship.<sup>10</sup> Instead, your company may still rely on either Sections 12(b) or 12(f) of the DPA as long as the recording of virtual meetings is work-related. Consequently, you may dispense with the requirement of obtaining the consent of employees every time virtual meetings are recorded.

*Privacy Impact Assessment.*

Finally, we recommend the conduct of a Privacy Impact Assessment (PIA) prior to the establishment and use of the proposed monitoring software or whenever there is a significant change in the software or software to assess and mitigate risks on the rights and freedoms of data subjects.

A PIA is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a PIC or a personal information processor (PIP). It considers the nature of the personal data to be protected, the personal data flow, the risks to privacy and security posed by the processing, current data privacy best practices, the cost of security implementation, and, where applicable, the size of the organization, its resources, and the complexity of its operations.<sup>11</sup>

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

For your reference.

Very truly yours,

(Sgd.)

**FRANKLIN ANTHONY M. TABAQUIN IV**

Director IV, Privacy Policy Office

---

9 *Id.*

10 ARTICLE 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, available at <https://ec.europa.eu/newsroom/article29/items/610169> (last accessed Feb.22, 2024).

11 NPC Advisory No. 2017-03, Guidelines on Privacy Impact Assessment, 31 July 2017.



# DECISIONS



INITIATED AS A *SUA SPONTE* NPC  
INVESTIGATION ON POSSIBLE  
DATA PRIVACY VIOLATIONS COMMITTED IN  
RELATION TO THE ALLEGED HACK AND BREACH  
OF THE COMMISSION ON  
ELECTIONS SYSTEM OR SERVERS

X-----X

## **DECISION**

### **AGUIRRE, D.P.C.;**

Before this Commission is a sua sponte initiated case by the Complaints and Investigation Division (CID) of the National Privacy Commission (NPC) against the Commission on Elections (COMELEC), Smartmatic Group of Companies (Smartmatic), RVA, WS (WS), and other John Does and Jane Does for an alleged violation of Section 29 and Section 30 of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

### **Facts**

The case arose from a news article of Manila Bulletin published on 10 January 2022 entitled “Comelec servers hacked; Downloaded data may include information that could affect 2022 elections.”<sup>1</sup> The news article reported that the Manila Bulletin Technews team allegedly discovered that hackers breached the server of COMELEC and “downloaded files that included, among others, usernames, and PINS of vote-counting machines (VCM) [...] network diagrams, IP addresses, list of all privileged users, domain admin credentials, list of all passwords and domain policies, access to the ballot handling dashboard, and QR code captures the bureau of canvassers with login and password.”<sup>2</sup> The news article further stated that the downloaded data “included list of overseas absentee voters, location of all voting precincts with details of board of canvassers, all configuration list of database, and list of all user accounts of [COMELEC] personnel.”<sup>3</sup>

On the same day, COMELEC made an announcement on its official website entitled “COMELEC Statement on Alleged Hacking Incident” stating:

The COMELEC is presently validating the allegations of the article published by the Manila Bulletin, specifically whether COMELEC systems have, in fact been compromised. With no independent verification that a hack has indeed taken place, one thing

<sup>1</sup> Manila Bulletin Technews, *Comelec servers hacked; Downloaded data may include information that could affect 2022 elections*, MANILA BULLETIN, 10 January 2022, available at <https://mb.com.ph/2022/01/10/comelec-servers-hacked-downloadeddata-may-include-information-that-could-affect-2022-elections/> (last accessed 28 September 2022).

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

immediately stands out: the article alleges that the hackers were able to “download files that included, among others, usernames and PINS of vote-counting machines (VCM).” The fact, however, is that such information still does not exist in COMELEC systems simply because the configuration files – which includes usernames and PINS – have not yet been completed. This calls into question the veracity of the hacking claim.

As for the rest of the allegations made, please note that the article offers scant substantiation for its assertions despite claiming that the authors had “verified that there was an ongoing hack.” Indeed, the article does not even offer proof of such verification.

Moving forward, the COMELEC assures the public of its full and scrupulous compliance with the Data Privacy Act, as well as its continuing cooperation with the National Privacy Commission. The COMELEC will likewise continue its efforts to validate the assertions made by the article. In this regard, we invite the authors to shed light on their allegations, particularly with regard to the “verification” they claim to have carried out. Considering that “news” like this could potentially damage the credibility of the elections, the COMELEC stands ready to pursue all available remedies against those who, either deliberately or otherwise, undermine the integrity of the electoral process.<sup>4</sup>

On 11 January 2022, the CID conducted an initial investigation and drafted its Initial Report.<sup>5</sup> The CID reported that it checked the website of COMELEC for any vulnerabilities and did not find any major vulnerability while using online tools.<sup>6</sup> It also discovered that the website of COMELEC uses Cloudflare to protect the website against Distributed Denial of Service (DDoS) attacks.<sup>7</sup> The CID sent Notices to Explain to COMELEC, Manila Bulletin, and ASJ, an editor of Manila Bulletin, and invited them to appear for a clarificatory hearing on 25 January 2022.<sup>8</sup>

On 15 January 2022, ASJ complied with the Notice to Explain and submitted artifacts that he allegedly received from his source.<sup>9</sup> On 20 January 2022, COMELEC requested the postponement of the Clarificatory Hearing scheduled on 25 January 2022.<sup>10</sup>

On 21 January 2022, the CID denied COMELEC’s request and directed COMELEC to appear during the 25 January 2022 Clarificatory Hearing and to submit additional documents and information.<sup>11</sup>

On 24 January 2022, the CID, in a Supplemental Technical Report, narrated that on 20

4 Commission on Elections, *COMELEC Statement on Alleged Hacking Incident*, COMMISSION ON ELECTIONS, 10 January 2022, available at <https://comelec.gov.ph/?r=References/Announcements/10Jan2022pr> (last accessed 30 September 2022).

5 Initial Report, Complaints and Investigation Division, 11 January 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

6 Id. at 2.

7 Id. at 3.

8 Notices to Explain, Complaints and Investigation Division, 11 January 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

9 Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 2, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

10 Id. at 2.

11 Order (To submit additional documents and provide further information), Complaints and Investigation Division, 21 January 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

January 2022, it contacted “XSOX Group” (XSOX Group), the group claiming responsibility for the alleged hacking of the COMELEC and Smartmatic servers, via their TOX messenger address supplied by ASJ.<sup>12</sup> It requested for more samples of election canvassers and a sample of the overseas absentee voters list to gather evidence and information regarding the alleged hacking and data leak in the COMELEC and Smartmatic servers.<sup>13</sup> As a response to the request, the XSOX Group gave the CID an additional ten (10) files that contained details of election canvassers dated 2016.<sup>14</sup>

On 25 January 2022, during the Clarificatory Hearing, COMELEC Director James Jimenez narrated the circumstances surrounding the alleged hacking incident.<sup>15</sup> His narration later formed part of a Memorandum that was eventually submitted to the CID on 28 January 2022.<sup>16</sup> COMELEC contradicted the assertions of the published news article by contending that “COMELEC’s system for generating the usernames and P[ersonal] I[nformation] N[umber]s for the VCMs is not online. Therefore, it has not been breached and cannot be breached as claimed in the article.”<sup>17</sup> COMELEC alleged that it has not started generating the PINs yet for the VCMs for the 2022 elections as the list of candidates has not been finalized as of the date of the published news article.<sup>18</sup> COMELEC also asserted that it does not have a system with a “ballot handling dashboard” and “QR code captures” and it also stated that it does not constitute a “bureau of canvassers” as what the news article published.<sup>19</sup>

COMELEC also addressed the issue regarding the list of overseas absentee voters.<sup>20</sup> COMELEC alleged that the list is not included in any component of the automated election system and the list is available in the official COMELEC website “www.comelec.gov.ph” as a required publication in compliance with the law.<sup>21</sup> As such, COMELEC stated that the list of overseas absentee voters does not need to be “hacked” in order for it to be accessed.<sup>22</sup>

COMELEC further alleged that its server for the preparation of election data for the 2022 elections is installed offline and is only accessible via a Local Area Network (LAN) at the COMELEC Warehouse.<sup>23</sup> COMELEC asserted that access to its server is governed by strict security protocols and an individual who gains access to its server must be authorized and must be physically present at the COMELEC Warehouse to do so.<sup>24</sup>

On the same date, the CID also conducted a clarificatory hearing with ASJ and SCO of the Manila Bulletin where ASJ narrated his version of the circumstances surrounding the incident.<sup>25</sup>

---

12 Supplemental Technical Report, Complaints and Investigation Division, 24 January 2022, at 1, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS

13 Id.

14 Id.

15 Clarificatory Hearing with the Commission on Elections, 25 January 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

16 Id.

17 Id.

18 Id.

19 Id.

20 Id.

21 Clarificatory Hearing with the Commission on Elections, 25 January 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

22 Id.

23 Id.

24 Id.

25 Id.

On 27 January 2022, the CID sent an Order to Submit Compliance directing COMELEC to submit documents and information that were discussed during the Clarificatory Hearing.<sup>26</sup>

On 28 January 2022, COMELEC submitted a Memorandum and an internal Position Paper dated 19 January 2022 on the alleged hacking incident.<sup>27</sup> The Memorandum containing the Position Paper reiterated COMELEC's position during the 25 January 2022 Clarificatory Hearing.<sup>28</sup>

On 27 January 2022, the CID issued an Order to Appear for Clarificatory Hearing on 04 February 2022 and Submit Compliance to Smartmatic.<sup>29</sup> On 04 February 2022, during the Clarificatory Hearing with Smartmatic, Smartmatic narrated that COMELEC ordered Smartmatic to explain the alleged hacking incident when the Manila Bulletin news article was released.<sup>30</sup> Smartmatic submitted documents and information in compliance with the Order dated 28 January 2022.<sup>31</sup>

On 08 February 2022, the CID issued an Order to Ventureslink Management Solutions, Inc. (VMSI), a manpower agency contracted to perform site surveys during the 2016 elections, to attend a clarificatory hearing on 11 February 2022.<sup>32</sup> During the 11 February 2022 Clarificatory Hearing, VMSI confirmed that it was engaged to conduct site survey of precincts in Regions IV-A, IV-B, VI, VII, and VIII for the 2016 elections.<sup>33</sup> Its representative informed the CID that he could not confirm that the artifact presented to him was the same form used during the conduct of the site survey.<sup>34</sup> He also stated that VMSI surrendered all documents and information to Smartmatic.<sup>35</sup>

On 11 February 2022, Smartmatic's counsels manifested that it cannot participate in the ongoing investigation due to an alleged Letter dated 10 February 2022 sent by COMELEC Commissioner Marlon Casquejo (Commissioner Casquejo).<sup>36</sup> The Letter allegedly contained a directive to Smartmatic that prohibited it from disclosing further information since the matter was covered by a non-disclosure agreement and involved the preparations and conduct of elections that COMELEC asserted to be within its exclusive jurisdiction.<sup>37</sup>

On 14 February 2022, the CID issued Orders directing COMELEC and Smartmatic to

---

26 Order (To Submit Compliance), 27 January 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

27 Memorandum No. 220177, 26 January 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

28 Id.

29 Order (To Appear), 28 January 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

30 Clarificatory Hearing with Smartmatic Group of Companies, 04 February 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

31 Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 5, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

32 Order (To Appear), 08 February 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

33 Id.

34 Id.

35 Id.

36 Clarificatory Hearing with Smartmatic Group of Companies, 11 February 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

37 Id.



appear for a clarificatory hearing on 22 February 2022 and to submit compliance.<sup>38</sup> It also directed Smartmatic to appear for a clarificatory hearing on 24 February 2022.<sup>39</sup>

On 18 February 2022, COMELEC submitted a Memorandum on the voting system and data policy of overseas voters, and sample forms used in the registration of overseas voters.<sup>40</sup>

On 22 February 2022, during the Clarificatory Hearing with COMELEC and Smartmatic, the CID requested a copy of the purported Letter dated 10 February 2022 but Commissioner Casquejo declined to furnish a copy of the Letter to the CID.<sup>41</sup>

In the same hearing, the CID presented an artifact that purports to be the list of overseas absentee voters for COMELEC to verify.<sup>42</sup> COMELEC refuted the artifact presented because there are data fields, specifically “height” and “weight”, that are not collected in the forms.<sup>43</sup> COMELEC submitted its overseas voter registration form to make a comparison to the artifact presented to show that there is no collection of data pertaining to “height” and “weight”.<sup>44</sup>

On 24 February 2022, Smartmatic did not appear in the scheduled Clarificatory Hearing. Instead, it filed a Manifestation and Motion dated 24 February 2022 and reiterated its position in the 22 February 2022 Clarificatory Hearing.<sup>45</sup>

On the 04 March 2022 Clarificatory Hearing, Smartmatic reiterated its Manifestation with Motion dated 24 February 2022.<sup>46</sup> It also filed an Omnibus Manifestation stating that it dispenses its right to participate as a witness and will comment when evidence is presented in the appropriate forum.<sup>47</sup>

On 09 March 2022, the CID issued a Notice for On-site Inspection scheduled on 18 March 2022,<sup>48</sup> and an Order directing COMELEC to submit a copy of the Letter dated 10 February 2022.<sup>49</sup> The CID did not receive any response from COMELEC.<sup>50</sup> As a result, it

---

38 Order (To Appear), 14 February 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

39 Id.

40 Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 7, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

41 Clarificatory Hearing with the Commission on Elections and Smartmatic Group of Companies, Inc., 22 February 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

42 Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 7, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

43 Id.

44 Id.

45 Manifestation with Motion, 24 February 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

46 Clarificatory Hearing with Smartmatic Group of Companies, 04 March 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

47 Omnibus Manifestation, 04 March 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

48 Notice, 09 March 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

49 Order (To Submit Compliance), 09 March 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

50 Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 7, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

served a copy of the Notice for On-Site Inspection and Order on 16 March 2022.<sup>51</sup>

On 17 March 2022, the CID’s representatives appeared before the Senate Committee on Electoral Reform and People’s Participation to provide information on the alleged breach of COMELEC servers.<sup>52</sup> On 18 March 2022, the CID attempted to conduct an on-site inspection of COMELEC’s Warehouse.<sup>53</sup> COMELEC, however, refused the CID’s admission to its premises. It also informed the CID of a letter dated 17 March 2022, which provides that the COMELEC was not amendable to an on-site inspection for various reasons.<sup>54</sup>

The CID sent a Letter dated 18 March 2022 to the National Bureau of Investigation (NBI) requesting for information that its Cybercrime Division had gathered regarding the breach in COMELEC and Smartmatic servers.<sup>55</sup> Subsequently, the NBI supplied the CID with the *Sinumpaang Salaysay* of RVA dated 02 February 2022.<sup>56</sup> The lawyer who assisted RVA in his *Sinumpaang Salaysay* informed him that he was being investigated for the crime of Illegal Access under the Cybercrime Prevention Act of 2012.<sup>57</sup>

In his *Sinumpaang Salaysay*, RVA stated that he worked at Smartmatic from August 2021 to January 2022 as a Quality Assurance Tester and, due to his role, he had access to the virtual private network (VPN) of Smartmatic.<sup>58</sup> When asked about the details leading up to the alleged Illegal Access he had committed, RVA narrated that he received a private message from a certain WS on Facebook Messenger promising to pay him Fifty Thousand Pesos (Php 50,000.00) to Three Hundred Thousand Pesos (Php 300,000.00) in exchange for giving access to his computer while connected to Smartmatic’s servers.<sup>59</sup>

RVA narrated that when he went to the COMELEC Office for work, he gave access to his computer using AnyDesk App through the internet while connected to Smartmatic servers on the last week of December 2021.<sup>60</sup> RVA further explained that the AnyDesk App is a closed source remote desktop application that gains remote access or control of file transfers and VPN functionality in another computer device without even having physical control over the computer and that may be accessed at a different location.<sup>61</sup>

RVA also stated that while he accomplished his end of the deal, WS did not carry out his promise of paying him the sum of money.<sup>62</sup> Instead, he was given online computer lectures such as Cobalt Strike and Lateral Movement.<sup>63</sup>

---

51 Id.  
52 Id.  
53 Id.  
54 Letter, 17 March 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).  
55 Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 8, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).  
56 Id. Annex S.  
57 Id. Annex S at 1.  
58 Id. Annex S at 2.  
59 Id. Annex S at 2-3.  
60 Id. Annex S at 3.  
61 Consolidated Fact-Finding Report, Complaints and Investigation Division, Annex S at 3, 05 April 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22001 and NPC SS 22-008 (NPC 2022).  
62 Id.  
63 Id.

On 05 April 2022, the CID submitted its Consolidated Fact-Finding Report<sup>64</sup> that serves as the Complaint for sua sponte initiated cases with the CID as the Nominal Complainant.<sup>65</sup> It asserted that RVA, WS, and several John Does and Jane Does (RVA, et al.) are liable for Section 29 (Unauthorized Access or Intentional Breach) of the DPA. The CID stated that it was through RVA's actions that WS and other unknown individuals "were able to breach and consequently access the overseas [absentee] voters list and site survey forms."<sup>66</sup> Thus, the CID contended that without RVA's indispensable participation, the breach would not have happened, and the access of WS and other unknown individuals to the personal data stored in Smartmatic's servers could have been averted.<sup>67</sup>

The CID also opined that COMELEC and Smartmatic be recommended for prosecution to the Department of Justice (DOJ) for a violation of Section 30 (Concealment of Security Breaches Involving Sensitive Personal Information) of the DPA.<sup>68</sup> The CID alleged that the data fields in the site survey form and overseas absentee voter list involve personal data that can be used for identity fraud.<sup>69</sup> The CID claimed that COMELEC and Smartmatic concealed the personal data breach as both entities, after several hearings, have adamantly denied and insisted that no breach has ever occurred on their servers.<sup>70</sup>

On 11 April 2022, the Commission issued an Order directing COMELEC, Smartmatic, RVA, and WS to submit their Comment within fifteen (15) days from receipt of the Order. It provides:

WHEREFORE, premises considered, Respondents Commission on Elections, Smartmatic Group of Companies, RVA, and WS are ORDERED, within fifteen (15) days from receipt of this Order, to file their respective COMMENTS on the allegations in the attached Consolidated Fact-Finding Report, pursuant to Section 6 of Rule X of NPC Circular No. 2021-01.

Further, the Complaints and Investigation Division (CID) of the National Privacy Commission, may, in its discretion, submit its REPLY within ten (10) days from receipt of Respondents' respective comments.

Respondents may, in their discretion, submit their respective REJOINDERS to the CID's Reply within ten (10) days from receipt of the Reply.

SO ORDERED.<sup>71</sup>

On 20 May 2022, the NPC received Smartmatic's Manifestation.<sup>72</sup> Smartmatic stated that the CID's Consolidated Fact-Finding Report was not attached to the Order dated 11 April 2022.<sup>73</sup>

64 Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

65 See National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC 2021 Rules of Procedure], rule X, §§ 5-6 (28 January 2021).

66 Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 21, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

67 Id.

68 Id.

69 Id. at 16.

70 Id. at 17.

71 Order to Comment, 11 April 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008, (NPC 2022).

72 Smartmatic Group of Companies Manifestation, 20 May 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

73 Id.

On 23 May 2022, COMELEC and Smartmatic was served a copy of the Order, the CID’s Consolidated Fact-Finding Report, and its corresponding annexes.<sup>74</sup>

On 03 June 2022, Smartmatic filed a Manifestation with Motion for Additional Time to File a Comment.<sup>75</sup> Smartmatic stated that it needed an extension to “properly verify the allegations in the Consolidated Fact-Finding Report and the voluminous attachments and/or annexes referred therein[.]”<sup>76</sup> Smartmatic also alleged that it “is still engaged with the post-election matters in the conduct of the 2022 National and Local Elections.”<sup>77</sup> Thus, Smartmatic prayed that an additional period of fifteen (15) calendar days from 07 June 2022, or until 22 June 2022 to submit its Comment on the Consolidated Fact-Finding Report.<sup>78</sup>

On 07 June 2022, COMELEC filed a Motion for Extension of Time to Submit a Comment.<sup>79</sup> COMELEC alleged that although the National and Local Elections had come to an end, it is still “engaged in the assessment and winding up of various election-related activities, [as well as] being called to immediately exercise its administrative and quasi-judicial functions over election matters and cases filed before it[.]”<sup>80</sup> COMELEC further alleged that “[it] is already on another cycle of its election preparations [... for the ...] Synchronized Barangay and Sangguniang Kabataan Elections.”<sup>81</sup> Aside from internal reasons given by the COMELEC, it claimed that it “is still awaiting the reply from the Office of the Solicitor General (OSG), whose legal assistance was sought by it.”<sup>82</sup>

Thus, COMELEC prayed that it be given an additional period of fifteen (15) days from 07 June 2022, or until 22 June 2022 to file its Comment on the Consolidated Fact-Finding Report.<sup>83</sup>

On 10 June 2022, the Commission issued an Order granting Smartmatic’s request for additional time to file its Comment.<sup>84</sup> The Commission also firmly reminded Smartmatic to strictly comply with the additional period it requested for and that no further extension shall be allowed.<sup>85</sup>

On 20 June 2022, the Commission issued an Order granting COMELEC’s request for additional time to file its Comment.<sup>86</sup>

On 22 June 2022, Smartmatic submitted its Comment on the Consolidated Fact-Finding Report.<sup>87</sup> Smartmatic argued that the CID’s investigation and report did not state

---

74 Order, 10 June 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

75 Smartmatic Group of Companies Manifestation, 03 June 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

76 Id. at 2.

77 Id.

78 Id. at 2-3.

79 Commission on Election Motion for Extension, 07 June 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

80 Id. at 2.

81 Id.

82 Id.

83 Id.

84 Order, 10 June 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

85 Id.

86 Id.

87 Smartmatic Group of Companies Comment, 22 June 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

sufficient basis for its conclusion that there was a personal data breach in COMELEC’s or Smartmatic’s servers.<sup>88</sup> Smartmatic alleged that the CID’s investigation and report were based on sources provided by a certain XSOX Group that should be considered as an anonymous tip or complaint.<sup>89</sup> Smartmatic claimed that “there was no verification or substantiation as the CID essentially accepted the validity of the documents from an anonymous criminal group wholesale.”<sup>90</sup> As such, Smartmatic contended that the proceedings before the CID in validating the alleged artifacts were improper and not credible as the CID could not verify the artifacts by independent means and the CID merely resorted to inviting resource persons to “shed light” on the matter.<sup>91</sup>

On 24 June 2022, the Commission received another Motion for Extension of Time to Submit its Comment dated 17 June 2022 from the OSG requesting for additional period of fifteen (15) days from 22 June 2022, or until 07 July 2022. The OSG explained that “considering the intricacies of the issues involved in this case and the need to coordinate with the COMELEC Law Department regarding the preparation of the Comment, additional time is needed by the OSG.”<sup>92</sup> The OSG also stated that the case was assigned to the undersigned Solicitor only on 15 June 2022, a week before the deadline given to COMELEC to file its Comment.<sup>93</sup>

On 08 July 2022, a day after the lapse of the initial extension of time it requested, the Commission received another Motion for Additional Extension of Time to File Comment from the OSG dated 04 July 2022.<sup>94</sup> The OSG claimed that “while [it] has already coordinated with the COMELEC Law Department regarding the filing of the required Comment, the OSG is still awaiting their reply to its Letter dated 17 June 2022 requesting for pertinent documents and additional significant information on the matter.”<sup>95</sup> Thus, the OSG prayed that the COMELEC be given an additional period of fifteen (15) days from 07 July 2022, or until 22 July 2022 to file its Comment.<sup>96</sup>

On 14 July 2022, the Commission issued an Order granting the OSG’s Motion for Additional Extension of Time to File Comment dated 04 July 2022.<sup>97</sup> The Commission ordered the OSG to submit COMELEC’s Comment on the Consolidated Fact-Finding Report within a nonextendible period of fifteen (15) days from 07 July 2022, or until 22 July 2022.<sup>98</sup>

On 22 July 2022, the COMELEC, through the OSG, submitted its Comment.<sup>99</sup> COMELEC contended that “the CID significantly failed to determine with reasonable certainty that the breach involving [Smartmatic’s] servers/system has a positive connection with per-

---

88 Id. at 6.

89 Id. at 6-8.

90 Id. at 8.

91 Id. at 9-10

92 Motion for Extension of Time to Submit Comment, Office of the Solicitor General, 17 June 2022, at 2, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22001 and NPC SS 22-008 (NPC 2022).

93 Id.

94 Motion for Additional Extension of Time, Office of the Solicitor General, 04 July 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

95 Id. at 2-3.

96 Id. at 3.

97 Order, 14 July 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

98 Id. at 3.

99 Commission on Elections Comment, Office of the Solicitor General, 22 July 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

sonal data contained in [ ] COMELEC’s certified list of overseas voters and/or the post-ed computerized voters list.”<sup>100</sup> As such, COMELEC claimed that the CID committed “serious error”<sup>101</sup> in recommending COMELEC to be liable for violating Section 30 of the DPA for allegedly concealing the personal data breach in Smartmatic’s servers.<sup>102</sup> Thus, COMELEC prayed that CID’s recommendation be set aside for lack of factual and legal basis.

### Issues

- I. Whether RVA, WS, and other John Does and Jane Does (RVA, WS, and other unknown individuals) are liable under Section 29 (Unauthorized Access or Intentional Breach) of the DPA.
- II. Whether COMELEC and Smartmatic are liable for Section 30 (Concealment of Security Breaches Involving Sensitive Personal Information) of the DPA.

### Discussion

#### **I. RVA, WS, and other unknown individuals are liable under Section 29 (Unauthorized Access or Intentional Breach) of the DPA.**

In the CID’s Consolidated Fact-Finding Report, which serves as the Complaint in this *sua sponte* initiated case,<sup>103</sup> the CID pointed to RVA’s statements contained in his *Sinump-aang Salaysay* and alleged that RVA “knowingly and

willingly allowed a certain WS access to [Smartmatic’s] network[.]”<sup>104</sup> Thus, the CID recommended finding RVA, WS, and other unknown individuals liable in violation of Section 29 of the DPA. The pertinent provision provides:

Section 29. Unauthorized Access or Intentional Breach. The penalty of 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.<sup>105</sup>

Unauthorized Access or Intentional Breach is committed when the following requisites concur:

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.<sup>106</sup>

<sup>100</sup> Id. at 4.

<sup>101</sup> Id.

<sup>102</sup> Id.

<sup>103</sup> See NPC 2021 Rules of Procedure, rule X, § 5-6.

<sup>104</sup> Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 21, in *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

<sup>105</sup> 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 § 29 (2012)

<sup>106</sup> *ACN v. DT*, NPC 18-109, 01 June 2021, available at <https://www.privacy.gov.ph/wpcontent/uploads/2022/01/Decision-NPC-18-109-ACN-v.-DT.pdf> (20 October 2022).

In this case, all requisites are present. As such, the Commission finds RVA, WS, and other unknown individuals liable for Unauthorized Access or Intentional Breach.

The first requisite is present in this case. It is not disputed that Smartmatic’s data system stores personal or sensitive personal information. The data system of Smartmatic stores personal data of voters by reason of the election results transmissions solutions, management, and services (ERTSMS Contract) in connection with the 2016, 2019, and 2022 elections that it entered into with COMELEC.<sup>107</sup> As such, Smartmatic possessed the personal data of voters and rendered its services in relation to the conduct of elections as COMELEC’s Personal Information Processor (PIP).<sup>108</sup> Thus, the first requisite of a data system storing personal or sensitive personal information is present.

As for the second requisite or “the accused breaks into the system”, RVA admitted in his Sinumpaang Salaysay that he gave unauthorized access to WS and other unknown individuals through the use of the AnyDesk App.<sup>109</sup> RVA narrated that on December 2021, he gave access to his computer using the AnyDesk App through the internet while connected to Smartmatic servers.<sup>110</sup> RVA while connected to Smartmatic’s servers was at the COMELEC Office when he gave unauthorized access through the AnyDesk App to WS and other unknown individuals.<sup>111</sup> As the CID pointed out, “[i]t was through...

RVA’s actions this WS and other unknown individuals were able to breach and consequently access the voters list and site survey forms.”<sup>112</sup> It was through RVA’s indispensable participation that led to WS and unknown individuals’ breaking into the system, thus, the second requisite is present in this case.

The third requisite is satisfied in this case. RVA, WS, and other unknown individuals knowingly and unlawfully broke into or breached Smartmatic’s servers that violated data confidentiality and security data systems. There is no question that these individuals knowingly and unlawfully consummated the act of breaking into Smartmatic’s system. Further, the bribe offered to RVA by WS and other unknown individuals shows the intention to do the illegal act of Unauthorized Access and Intentional Breach penalized under Section 29 of the DPA. For RVA, money was the motivation to commit the crime as he supposedly needed it to feed his two-monthold child.<sup>113</sup> Regardless of his motivations, RVA must face the consequences of his illegal action of knowingly and unlawfully breaking into Smartmatic’s servers that resulted in violating data confidentiality and the security of data systems. Thus, the third element is satisfied.

Given the foregoing, the Commission finds RVA, WS, and other unknown individuals liable for violating Section 29 of the DPA. These individuals committed Unauthorized Access or Intentional Breach when they broke into Smartmatic’s servers that store personal or sensitive personal information. These individuals are recommended for prosecution to the DOJ.

---

107 Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 21, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

108 Id. at 21.

109 Id. Annex S at 3.

110 Id.

111 Id.

112 Id. at 21.

113 Consolidated Fact-Finding Report, Complaints and Investigation Division, Annex S at 5, 05 April 2022, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22001 and NPC SS 22-008 (NPC 2022).

## II. COMELEC and Smartmatic are not liable under Section 30 (Concealment of Security Breaches Involving Sensitive Personal Information) of the DPA.

As previously discussed, the Consolidated Fact-Finding Report serves as the Complaint in sua sponte investigations, with the CID as the Nominal Complainant.<sup>114</sup> In this case, the CID alleged that there are two sets of personal data breaches that occurred in Smartmatic and COMELEC's servers.<sup>115</sup> The first relates to site survey forms, and the second relates to the overseas absentee voters list.

A. COMELEC and Smartmatic did not violate Section 30 of the DPA in relation to the site survey forms.

In the CID's FFR, the CID alleged that COMELEC and Smartmatic are liable for Concealment of Security Breaches Involving Sensitive Personal Information under Section 30 of the DPA. It provides:

*Section 30. Concealment of Security Breaches Involving Sensitive Personal Information.* The penalty of imprisonment of 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 who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach.<sup>116</sup>

The requisites of Concealment of Security Breaches Involving Sensitive Personal Information are:

1. A personal data breach occurred;
2. The breach is one that requires notification to the Commission; and
3. The person knowingly conceals the fact of such breach from the Commission.<sup>117</sup>

Although Section 30 of the DPA penalizes the concealment or failure to notify the Commission of a security breach, the concealed security breach must be one that requires mandatory breach notification under Section 20 (f) of the DPA. This is because Section 30 refers to "the obligation to notify the Commission pursuant to Section 20(f)." Section 20 (f) of the DPA states:

Section. 20. Security of Personal Information.

...

(f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Noti-

<sup>114</sup> See NPC 2021 Rules of Procedure, rule X, § 5-6.

<sup>115</sup> Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 10-11, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22001 and NPC SS 22-008 (NPC 2022).

<sup>116</sup> Data Privacy Act of 2012, § 30.

<sup>117</sup> See Data Privacy Act of 2012, § 30.



fication may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.<sup>118</sup>

In relation to Section 20 (f) of the DPA, Section 11 of NPC Circular 1603 (Personal Data Breach Management) discusses the parameters of mandatory breach notification:

Section 11. *When notification is required.* Notification shall be required upon knowledge of, or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.

...

B. There is reason to believe that the information may have been acquired by an unauthorized person; and

C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.<sup>119</sup>

As such, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.<sup>120</sup>

The Commission acknowledges that there had been a breach in Smartmatic's servers through the acts of RVA, WS, and other unknown individuals. The Commission, however, finds that there is no obligation on the part of COMELEC, the Personal Information Controller (PIC), and Smartmatic, the Personal Information Processor (PIP) to report the breach to the Commission because the first and third requisite for mandatory breach notification are not present.

As to the first requisite, the breach does not involve sensitive personal information or information that may be used to enable identify fraud. In this case, the CID presented artifacts relating to site survey forms allegedly taken from Smartmatic or COMELEC's servers.<sup>121</sup>The CID stated that it "discovered that the name and signature of both the person who performed the site survey and the contact person or a representative of the latter appeared [in these forms].<sup>122</sup> The CID claims that it was able to verify and authenticate these forms when it "matched the name of RVA to the personnel list pro-

<sup>118</sup> Data Privacy Act of 2012, § 20 (f). Emphasis supplied.

<sup>119</sup> National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).

<sup>120</sup> NPC Circ. No. 16-03, §11.

<sup>121</sup> Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 11, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

<sup>122</sup> Id.

vided for by VMSI,<sup>123</sup> the manpower agency that employed RVA to perform site surveys.<sup>124</sup> Aside from the name and signature alleged by CID, the site survey forms also shows the positions or designations of the data subjects.

The name, signature, and designation of the data subject cannot be considered as sensitive personal information, which refers to:

### Section 3. Definition of Terms.

...

(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.<sup>125</sup>

A data subject's name, signature, and designation clearly do not fall within the definition of sensitive personal information.

The name, signature, and designation when taken by themselves, cannot also be considered as information that may be used to enable identity fraud. A determination of whether the compromised information may enable identity fraud requires a consideration of circumstances other than the nature of the personal information involved, including the manner in which the personal information was obtained, whether that information was specifically targeted, and the specific nature of the breach. In this case, a data subject's name and signature without other pieces of information that substantiate a data subject's identity cannot be considered as sufficient to perpetuate identity fraud. To add to this, the data subjects whose personal information were exposed in the site survey forms were either government employees or were performing services pursuant to a contract with the government. Following Section 4 (a) and (b) of the DPA, the names and designations of these data subjects are excluded from the scope of the DPA, thus:

### Section. 4. Scope.

...

This Act does not apply to the following:

- (a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual

---

123      Id.  
124      Id. at 5.  
125      Data Privacy Act of 2012, § 3 (l).

...

(b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services[.]<sup>126</sup>; .

Given all this, the first requisite for mandatory breach notification is lacking.

The third requisite that the unauthorized acquisition is likely to give rise to a real risk of serious harm is also not present. The CID presented artifacts of the site survey forms that contain data fields regarding the 2016 elections.<sup>127</sup> Given that the alleged breach happened in 2022, the personal information taken from the breach may be inaccurate and outdated. Taken together with the fact that the personal information involved is neither sensitive personal information nor information that enables identity fraud, the unauthorized acquisition of personal information in the site survey forms is unlikely to give rise to a real risk of serious harm to the affected data subjects.

Considering that the first and third requisites for mandatory breach notification are

absent in this case, the Commission finds that the breach pertaining to personal information leaked through the site survey forms does not require mandatory breach notification to the Commission. Since the PIC and the PIP do not have an obligation to notify the Commission of the breach under Section 20 (f) of the DPA, the Commission finds Smartmatic and COMELEC not liable for Concealment of Security Breaches Involving Sensitive Personal Information.

B. COMELEC and Smartmatic did not violate Section 30 of the DPA in relation to the overseas absentee voters list.

On the issue of the overseas absentee voters list, the CID presented several artifacts supplied by the XSOX Group relating to the overseas absentee list that allegedly contained personal data of approximately one hundred thirty-eight thousand nine hundred (138,900) individuals.<sup>128</sup> As these artifacts received by the CID are uncorroborated, the CID contended that it took steps to verify the artifacts stating:

To verify and determine whether the artifact may be an actual voters list, the CID randomly selected individuals and attempted to cross-reference them to the overseas voters' list on the COMELEC website, however, no such list was available therein. As an alternative, the CID cross-referenced the names on the artifact to certified voters' list provided for in the Department of Foreign Affairs (DFA) website for various Philippine Embassies in different countries, however, no matches were made. Also, the sheer size and volume of records and the limited overseas list available for cross-referencing made it an impractical pursuit.

Notwithstanding, the CID also randomly selected from the artifact, ten (10) individuals and searched over the Internet for any digital footprint or identifier. This resulted in a

<sup>126</sup> Data Privacy Act of 2012, § 4.

<sup>127</sup> Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 18, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

<sup>128</sup> Id. at 10.

match with ten (10) Facebook profiles. From the ten (10) selected, nine (9) individuals matched details with respect to their name and city or province of their residence as stated in their respective profiles. Moreover, these individuals maintain relatively active profiles.

As such, the CID can reasonably conclude that the artifact contains actual data pertaining to existing individuals.

We recall that during the clarificatory hearing conducted on 25 January 2022 and again on 22 February 2022, the CID confronted representatives of COMELEC with the voter's list reduced into an excel file and readily denied its ownership. COMELEC observed that it contained data fields with respect to height and weight and noted that COMELEC did not collect such information for registration purpose. To support COMELEC's assertions, it submitted sample registration forms used during the 2016 elections up to the present.<sup>129</sup>

An examination of the records shows that the CID failed to sufficiently prove that the artifacts it received from the XSOX Group were gathered from an alleged breach of Smartmatic or COMELEC's servers. In this case, the CID, as the Nominal Complainant, has the burden of proof and must prove its allegations with substantial evidence.

In administrative proceedings, 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."<sup>130</sup> Section 1, Rule 131 of the 2019 Amendments to the Revised Rules on Evidence provides:

Section 1. Burden of proof and burden of evidence. Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim or defense by the amount of evidence required by law. Burden of proof never shifts.

Burden of evidence is the duty of a party to present evidence sufficient to establish or rebut a fact in issue to establish a prima facie case. Burden of evidence may shift from one party to the other in the course of the proceedings, depending on the exigencies of the case.<sup>131</sup>

It is the party who alleges a fact that has the burden of proving it. The Supreme Court held that "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."<sup>132</sup> Thus, the CID will not be able to discharge its burden of proof with substantial evidence by mere allegations.

The CID cannot simply conclude that the unverified artifacts came from a breach because it tested ten (10) out of the one hundred thirtyeight thousand nine hundred (138,900) individuals. From the ten (10) individuals selected, nine (9) of them had Facebook profiles that matched the purported overseas absentee voters list that was taken from the alleged breach of Smartmatic's server. Testing ten (10) out of one hundred

129 Id. at 10-11.

130 Ombudsman v. Fetalvero, G.R. No. 211450, 23 July 2018.

131 2019 AMENDMENT TO THE 1989 REVISED RULES ON EVIDENCE, A.M. No. 19-08-15-SC, Rule 131, §1 (1 May 2020). Emphasis supplied.

132 Government Service Insurance System v. Prudential Guarantee and Assurance, Inc., Development Bank of the Philippines and Land Bank of the Philippines, G.R. No. 165585, 20 November 2013.

thirty-eight thousand nine hundred (138,900) individuals is insufficient because verifying ten (10) individuals is too small of a sample size and will not produce a meaningful result. Further, the only thing that the CID's test confirmed is that some of the people on the artifacts are real people. The test results, however, do not show that the list came from a breach of COMELEC's or Smartmatic's systems or servers.

Further, the artifact of overseas absentee voters list presented by the CID contained data fields that COMELEC does not collect, specifically height and weight. To support COMELEC's assertions, COMELEC submitted sample registration forms that were used during the 2016 elections up to the present.<sup>133</sup> After reviewing the submitted sample registration forms of COMELEC, the data fields of "height" and "weight" were not collected by COMELEC. Thus, in comparing CID's artifacts to COMELEC's sample registration forms that have been used in the past several elections, the irregularities between the two opposing evidence cast doubt on the veracity and authenticity of CID's evidence.

Smartmatic argued that the CID's evidence were not properly authenticated and verified:

17. The subsequent parallel investigation covered by Reference No. SS 22-008 ("SS 22-008") (which is essentially identical to SS 22-[0]01 except in its title) was also prompted by the posts of the same XSOX.Group in social media:

'On 11 February 2022, while conducting active monitoring of the internet for privacy violations, data breaches, and data dumps affecting personal information, the Commission monitored posts made by XSOX Group.

An extensive examination of the numerous posts made by XSOX [Group] revealed artifacts that point to a probable breach of Smartmatic servers/system, which appear to involve personal information.'

18. Curiously, however, even after the Investigation was already concluded, the CID still acknowledges that its sources have not been properly verified, thus:

'xxx at the very beginning of this controversy, a group identified only as XSOX Group has expressly taken responsibility and authorship over the attack on [Smartmatic's] servers/system. The members of this group are still unknown, and there is insufficient evidence or lead/information, at this point, to readily identify the members of this organization. Similarly, the identity of ASJ's Source cannot be determined with certainty.'

19. In *Anonymous Complaint v. Presiding Judge Dagala*, the Supreme Court ruled that anonymous complaints should always be treated with great caution. Consequently, the Supreme Court will act on an anonymous complaint provided its allegations can be reliably verified and properly substantiated by competent evidence, like public records of indubitable integrity. In this case, however, there was no verification or substantiation as the CID essentially accepted the validity of the documents from an anonymous criminal group wholesale.<sup>134</sup>

---

<sup>133</sup> Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 11 and Annex F, in *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22001 and NPC SS 22-008 (NPC 2022);

<sup>134</sup> Smartmatic Group of Companies Comment, 22 June 2022, at 7-8, in *In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does*, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

Smartmatic asserted that CID’s artifacts can be likened to an “anonymous complaint” that needs to properly authenticated and corroborated by competent evidence.<sup>135</sup> The CID, however, erroneously concluded that the artifacts have sufficiently been verified and authenticated by cross-checking merely ten (10) selected individuals as its sample size. The CID’s procedure of verifying and substantiating the anonymous tips provided by the XSOX Group did not overcome its dubious origin.

The COMELEC asserted that the CID found that there was no breach in COMELEC’s servers or system.<sup>136</sup> The COMELEC pointed to the CID’s Consolidated Fact-Finding Report as basis:

## 2. Whether there was a hack or breach of COMELEC servers/system

While the news article published by Manila Bulletin alluded to a hack or breach of COMELEC servers, the CID is not convinced that COMELEC servers or its system were breach nor is it convinced that the artifacts that it has gathered from multiple sources are any indication that said COMELEC servers or system was compromised.

The pieces of evidence gathered in the course of CID’s investigation in this case also suggest that COMELEC servers or its system were not breached.<sup>137</sup>

COMELEC further argued that Smartmatic’s system and COMELEC’S system are separate and are completely different from one another.<sup>138</sup> It averred that an alleged breach in Smartmatic’s servers or system does not necessarily relate to the personal information stored in COMELEC’s database pertaining to the overseas absentee voters list:

3. [...] In this case, the CID significantly failed to determine with reasonable certainty that the breach involving the [Smartmatic] servers/system has a positive connection with personal data contained in respondent’s COMELEC’s certified list of overseas voters and/or posted computerized voter’s list. Such being the case, the CID committed serious error in holding respondent COMELEC liable for violation of Section 30 of R.A. No. 10173 for allegedly concealing the security breach of [Smartmatic] servers/system involving personal data contained in an overseas absentee voter’s list that is speculated to have originated from respondent COMELEC but which speculation was not duly substantiated.<sup>139</sup>

The burden of proof is on the CID to provide a direct link that connects the alleged breach in Smartmatic’s servers or system to COMELEC’s servers or system. The CID,

however, failed to make a positive connection and simply concluded that the system was not breached by the alleged hacking by the XSOX Group.<sup>140</sup>

---

135 Id. at 7-8.

136 Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 12, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

137 Id. Emphasis supplied.

138 Id. at 4.

139 Commission on Elections Comment, Office of the Solicitor General, 22 July 2022, at 4, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022). Emphasis supplied.

140 Consolidated Fact-Finding Report, Complaints and Investigation Division, 05 April 2022, at 20-21, in In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008 (NPC 2022).

Assuming that the overseas absentee voters list did come from Smartmatic's servers or system, COMELEC may be held liable for a breach of Smartmatic's servers or system following the principle of accountability. The DPA provides for the Principle of Accountability and concomitant obligations of a PIC:

Section. 21. Principle of Accountability. Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(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.<sup>141</sup>

In this case, COMELEC is considered as the PIC as it is the Constitutional Commission with exclusive jurisdiction relative to the conduct of elections. It is in a position to exercise control and discretion in matters relating to the conduct of elections. COMELEC entered into the ERTSMS Contract with Smartmatic, its PIP, in order for Smartmatic to render its services. Thus, COMELEC, as the PIC, is accountable for any personal data breach that may have occurred in Smartmatic's servers or system.

Although COMELEC may be held accountable for a breach that occurred in Smartmatic's servers or system, the Commission finds that there is no breach in relation to the overseas absentee voters list. The CID failed to prove with substantial evidence its allegations that the overseas absentee voters list resulted from a breach of Smartmatic's servers or system. Thus, its assertions that Smartmatic and COMELEC should be held liable for Concealment of a Breach of Sensitive Personal Information in relation to the overseas absentee voters list must fail.

To summarize, the Commission does not find COMELEC and Smartmatic liable for Concealment of Security Breaches Involving Sensitive Personal Information under Section 30 of the DPA. On matters relating to the site survey forms, there is no obligation to notify the Commission of the breach because the first and third requisites for mandatory breach notification are lacking.

On the issue regarding the overseas absentee voters list, the CID failed to discharge its burden of proof and was unable to prove its allegations with substantial evidence. The Commission cannot find COMELEC and Smartmatic liable on the basis of mere allegations of the CID in its FFR.

The Commission notes that there is no evidence on record that shows that there was a lack of reasonable and appropriate security measures that could have resulted in the breach. Smartmatic's servers or system being breached was caused by employee malfeasance. While there is no security measure that is 100% effective, this becomes all the more true when there is employee malfeasance involved. Nevertheless, it remains the obligation of PICs to take proactive steps to ensure that its security measures minimize, if not altogether eliminate, these risks. The inevitability of breaches should not give rise to indolence but instead spur action. After all, the protection of our fundamental human right to privacy is at stake.

---

<sup>141</sup> Data Privacy Act of 2012, § 21.

WHEREFORE, premises considered, this Commission hereby:

1. FINDS RVA, WS, and other John Does or Jane Does violated Section 29 of the Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

2. FORWARDS this Decision and a copy of the pertinent case records to the Secretary of Justice and RECOMMENDS the prosecution of RVA, WS, and other John Does or Jane Does for Unauthorized Access or Intentional Breach under Section 29 of the DPA;

3. DISMISSES the case against Commission on Elections and the Smartmatic Group of Companies for lack of merit. This is without prejudice to the filing of appropriate civil, criminal or administrative cases against Respondents Commission on Elections, Smartmatic Group of Companies, RVA, WS, and other John Does or Jane Does before any other forum or tribunal, if any.

**SO ORDERED.**

City of Pasay, Philippines.  
22 September 2022.

**Sgd.**

**LEANDRO ANGELO Y. AGUIRRE**

Deputy Privacy Commissioner

I CONCUR:

**Sgd.**

**JOHN HENRY D. NAGA**

Privacy Commissioner



Copy furnished:

**BSJ**

*Data Protection Officer*

**COMMISSION ON ELECTIONS**

**COMMISSION ON ELECTIONS**

**LAW DEPARTMENT**

8/F Palacio del Gobernador,

General Luna Street,

Intramuros, Manila

law@comelec.gov.ph

comelec.law@gmail.com

**RVA**

**OFFICE OF THE SOLICITOR GENERAL**

*Counsel for Commission on Elections*

134 Amorsolo St., Legaspi Village,

Makati City

docket@osg.gov.ph

**ANGARA ABELLO CONCEPCION REGALA & CRUZ**

*Counsel for Smartmatic Philippines, Inc., Smartmatic TIM Corporation,  
SMMT, INC., and SMMT-TIM 2016, INC.*

**COMPLAINTS AND INVESTIGATION DIVISION**

**ENFORCEMENT DIVISION**

**GENERAL RECORDS UNIT**

National Privacy Commission

**MAF,**

*Complainant,*

-versus-

**NPC 21-167**  
For: Violation of the  
Data Privacy Act of  
2012

**SHOPEE PHILIPPINES, INC.,**  
*Respondent.*

X-----X

**DECISION**

**AGUIRRE, D.P.C.;**

Before this Commission is a complaint filed by MAF against Shopee Philippines, Inc. (Shopee) for an alleged violation of Section 28 (Processing for an Unauthorized Purpose) and Section 32 (Unauthorized Disclosure) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA)

**Facts**

On 12 August 2021, the National Privacy Commission (NPC), through its Complaints and Investigation Division (CID), received MAF’s Complaints-Assisted Form (CAF).<sup>1</sup> MAF alleged that on 06 August 2021, “[her] minor child’s picture was used as proof of delivery. The courier service took his picture without his consent and was not told of the purpose.”<sup>2</sup> She contended that instead of the rider taking a picture of her son as proof of delivery, “the rider should have at least taken a [picture] of his arm and package or have done the geotagging as said in their guidelines.”<sup>3</sup>

She claimed that “[w]hen the seller asked for proof of delivery, Shopee forwarded [her] son’s photo to the seller and was sent to [her] as proof of delivery.”<sup>4</sup> She also claimed that she requested Shopee “to remove [her] son’s photo out of their system”<sup>5</sup>but Shop-ee refused her request.<sup>6</sup>

MAF asserted that Shopee violated Section 28 (Processing for an Unauthorized Purpose) and Section 32 (Unauthorized Disclosure) of the DPA.<sup>7</sup> MAF also prayed for a fine to be imposed on Shopee and for Shopee to remove her son’s photo and to “include in their guidelines that [under] no circumstance [should] a minor’s picture be taken as proof of delivery.”<sup>8</sup>

On 02 November 2021, an Order was issued directing Shopee to file a verified comment within fifteen (15) calendar days from receipt of the Order.<sup>9</sup> The parties were also or-

1 Complaints Assisted Form, 12 August 2021, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2021).  
2 *Id.* at 3.  
3 *Id.*  
4 *Id.*  
5 *Id.* at 4.  
6 *Id.*  
7 Complaints Assisted Form, 12 August 2021, at 3, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2021).  
8 *Id.* at 5.  
9 Order, 02 November 2021, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2021).

dered to appear virtually for a preliminary conference on 26 January 2022.<sup>10</sup>

On 17 November 2021, Shopee filed its Verified Comment.<sup>11</sup> Shopee contended that when “MAF signed up for an account, she agreed to the Terms of Service and expressly consented to the Privacy Policy.”<sup>12</sup> Shopee’s Privacy Policy provides:

## 9. INFORMATION ON CHILDREN

9.1 The Services are not intended for children under the age of 13. We do not knowingly collect or maintain any personal data or non-personally-identifiable information from anyone under the age of 13 nor is any part of our Platform or other Services directed to children under the age of 13. **As a parent of legal guardian, please do not allow such children under your care to submit personal data to Shopee. In the event that personal data of a child under the age of 13 in your care is disclosed to Shopee, you hereby consent to the processing of the child’s personal data and accept and agree to be bound by this Policy on behalf of such child.** We will close any accounts used exclusively by such children and will remove and/or delete any personal data we believe was submitted without parental consent by any child under the age of 13.<sup>13</sup>

Shopee alleged that on 04 August 2021, the Third-Party Logistics Rider (rider) attempted to deliver the package directly to MAF.<sup>14</sup> Shopee claimed that MAF, however, was unavailable to receive the delivery and it was her son who answered the door to receive the package.<sup>15</sup>

Shopee further alleged that MAF had initially filed a request for refund prior to the delivery of the package on 04 August 2021.<sup>16</sup> Shopee claimed that because the seller tagged the Order as “Completed”, MAF reached out to the seller to question the tagging of the Order.<sup>17</sup>

Shopee stated that the photo was “taken as proof that the package was safely delivered or the status of delivery, for the protection buyers, sellers, and partners, and for audit purposes.”<sup>18</sup> Contrary to MAF’s assertions that Shopee provided a copy of the proof of delivery to the seller, Shopee stated that “unlike the buyer, the seller cannot readily access the [proof of delivery].”<sup>19</sup>

On 16 December 2021, Shopee filed a Manifestation.<sup>20</sup> Shopee stated that as of 06 December 2021, it updated its Guidelines to prohibit the taking of a minor’s picture as proof of delivery.<sup>21</sup> It added the following statement to the Guidelines: “Packages shall

---

10 *Id.*  
11 Respondent’s Verified Comment, 17 November 2021, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2021).  
12 *Id.* at 3.  
13 *Id.* at 4.  
14 *Id.* at 5.  
15 *Id.*  
16 *Id.* at 6.  
17 Respondent’s Verified Comment, 17 November 2021, at 6, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2021).  
18 *Id.* at 5.  
19 *Id.* at 6.  
20 Respondent’s Manifestation, 16 December 2021, at 1, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2021).  
21 *Id.*

not be delivered to or left with minors except upon the written instructions of the buyer who is the minor's parent or guardian. Photos of minors shall not be taken under any circumstances."<sup>22</sup>

On 26 January 2022, both parties were present at the Preliminary Conference.<sup>23</sup> During Discovery Proceedings, MAF requested Shopee to produce its data retention policy. Shopee, on the other hand, requested MAF "to show any document or proof showing that the seller was the one who sent her the picture of her supposed son as proof of delivery" based on the statement MAF made in her CAF.<sup>24</sup> MAF clarified that the proof of delivery can be accessed through a link in the Shopee application that directs the Shopee account holder to the picture as proof of delivery.<sup>25</sup>

MAF manifested during the Preliminary Conference that she will submit additional evidence to counter Shopee's allegations that she allegedly gave consent to the rider that her son will receive the package.<sup>26</sup> Shopee's counsel moved that Shopee be allowed to comment on the additional evidence of MAF.<sup>27</sup> This motion was granted.<sup>28</sup>

The parties manifested that they are both willing to undergo mediation proceedings. They, however, requested to be allowed to submit the documents and pleadings required before mediation.<sup>29</sup>

On 26 January 2022, MAF submitted her additional evidence composed of screenshots of the text messages allegedly between her and the rider on 08 November 2021 to prove that she did not give consent to let her son receive the package nor take his photo.<sup>30</sup> In the series of text messages, the rider apologized for taking her son's photo and explained that the reason he took the son's photo was because it was her son who answered the door when he attempted to deliver the package.<sup>31</sup>

On 14 February 2022, Shopee filed its Comment/Opposition to the additional evidence submitted by MAF.<sup>32</sup>Shopee averred that the 08 November 2021 text exchange should not be admitted for being hearsay under the 2019 Amendments to the 1989 Revised Rules on Evidence (Revised Rules of Evidence).<sup>33</sup>

On 06 April 2022, the parties failed to reach a settlement.<sup>34</sup> As such, a Notice of Non-Settlement of Dispute was issued.<sup>35</sup>

On 07 April 2022, an Order was issued to resume the proceedings and to direct both parties to submit their respective memoranda.<sup>36</sup>

---

22 *Id.* at 1-2.  
23 Order After 1st Preliminary Conference, 26 January 2022, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2022).  
24 *Id.*  
25 *Id.*  
26 *Id.*  
27 *Id.*  
28 *Id.*  
29 Order After 1st Preliminary Conference, 26 January 2022, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2022).  
30 Complainant's Additional Evidence, 26 January 2022, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2022).  
31 *Id.*  
32 Respondent's Comment/Opposition, 14 February 2022, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2022).  
33 *Id.*  
34 Notice of Non-settlement of Dispute, 06 April 2022, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2022).  
35 *Id.*  
36 Order, 07 April 2022, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2022).

On 06 May 2022, MAF submitted her Memorandum.<sup>37</sup>MAF stated that she specifically instructed the rider to wait for her so that she can personally receive the delivery.<sup>38</sup> She alleged that despite her instructions, the rider delivered the package to the person who answered the door, which was MAF’s son, because he was pressed for time.<sup>39</sup> She

claimed that her son answered the door because he thought that it was his grandfather who had arrived.<sup>40</sup> Thereafter, MAF alleged that the rider gave the package to her son and took his picture without his consent and the photo was then uploaded in the Shopee App as proof of delivery.<sup>41</sup>

MAF also stated that when she reported the incident to Shopee, she discovered that the rider made “an untruthful narration in his incident report, stating that [the rider] notified [MAF] that a minor is not allowed to receive packages. This did not happen.”<sup>42</sup>She alleged that the apology in the text exchange between her and the rider is proof that the rider made untruthful statements in his incident report.<sup>43</sup>

On 10 May 2022, Shopee submitted its Memorandum.<sup>44</sup> Shopee reiterated the facts it narrated in its Verified Comment. Shopee argued that it already complied with MAF’s prayers by deleting the son’s photo in their system and updated its Guidelines that prohibits the taking of a minor’s picture as proof of delivery, thus, making the case moot.<sup>45</sup>Hence, Shopee prays for the dismissal of the case.<sup>46</sup>

### **Issues**

- I. Whether Shopee is liable under Section 28 (Processing for an Unauthorized Purpose) of the DPA.
- II. Whether Shopee is liable under Section 32 (Unauthorized Disclosure) of the DPA.
- III. Whether Shopee violated the general privacy principle of proportionality.

### **Discussion**

Shopee, as the Personal Information Controller (PIC), is responsible for the actions of the Personal Information Processor (PIP), the ThirdParty Logistics Provider and consequently, its rider. Section 21 of the DPA discusses the principle of accountability:

Section 21. *Principle of Accountability.* **Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing**, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(a) The personal information controller is accountable for complying with the require-

---

37 Complainant’s Memorandum, 06 May 2022, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2022).  
38 *Id.* at 1.  
39 *Id.*  
40 *Id.*  
41 *Id.* at 2.  
42 *Id.*  
43 Complainant’s Memorandum, 06 May 2022, at 2, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2022).  
44 Respondent’s Memorandum, 10 May 2022, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2022).  
45 *Id.* at 29-31.  
46 *Id.* at 39-40.

ments 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.<sup>47</sup>

While Shopee, as the PIC, subcontracted the processing of personal information to the Third-Party Logistics Provider, its PIP, Shopee remains responsible for the Third-Party Logistics Provider's actions following the principle of accountability. This includes the processing of the photo as proof of delivery.

Nevertheless, Shopee is not liable under Section 28 (Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes) of the DPA and Section 32 (Unauthorized Disclosure) of the DPA. Shopee, however, violated the general privacy principle of proportionality.

### **I. Shopee is not liable under Section 28 (Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes) of the DPA.**

MAF alleged that Shopee is liable for violation of Section 28 of the DPA when Shopee processed a photo of her son as proof of delivery when the rider delivered the package to MAF's residence. Section 28 (a) of the DPA provides:

*Section. 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.* (a) 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.**<sup>48</sup>

To be held liable under Section 28 or the Processing of Personal or Sensitive Personal Information for Unauthorized Purposes, the following requisites must concur:

1. A person processed information of the data subject;
2. The information processed is classified as personal or sensitive personal information;
3. The person processing the information obtained consent of the data subject or is granted authority under the DPA or existing laws; and
4. The processing of personal or sensitive personal information is for a purpose that is neither covered by the authority given by the data subject and could not have been reasonably foreseen by the data subject nor otherwise authorized by the DPA or existing laws.<sup>49</sup>

The first three (3) requisites are present in this case.

On the first and second requisites, there is no question that Shopee, as the PIC,

<sup>47</sup> 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 § 21 (2012). Emphasis supplied.

<sup>48</sup> Data Privacy Act of 2012, § 28 (a). Emphasis supplied.

<sup>49</sup> NPC 19-142, 31 March 2022, at 12-13 (NPC 2022) (unreported).

processed the son’s personal information. Section 3 of the DPA defines personal information and processing as follows:

Section 3. *Definition of Terms.* Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

...

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

...

(j) Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.<sup>50</sup>

Without doubt, a photo is personal information because the identify of an individual, MAF’s son, is apparent. Processing of personal information occurred when the rider took the photo of MAF’s son and uploaded the photo as proof of delivery in the Shopee platform. Thus, the first and second requisites are present.

Without doubt, a photo is personal information because the identify of an individual, MAF’s son, is apparent. Processing of personal information occurred when the rider took the photo of MAF’s son and uploaded the photo as proof of delivery in the Shopee platform. Thus, the first and second requisites are present.

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

...

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.<sup>51</sup>

Processing based on legitimate interest requires the fulfillment of the following conditions: (1) the legitimate interest is established; (2) the processing is necessary to fulfill the legitimate interest that is established; and (3) the interest is legitimate or lawful and it does not override fundamental rights and freedoms of data subjects.<sup>52</sup>

Shopee had legitimate interest to process the photo as proof of delivery. Shopee’s Terms of Service provides that it “acts as an intermediary that brings together the Seller and the Buyer.”<sup>53</sup> As such, “[it] is responsible for facilitating reports/ complaints from

50 Data Privacy Act of 2012, § 3 (g) & (j).

51 Data Privacy Act of 2012, § 12 (f). Emphasis supplied.

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

53 Respondent’s Memorandum, 10 May 2022, at 24, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2022).

[b]uyers if the [b]uyer has not received the product within the estimated timeframe.”<sup>54</sup> To effectively do so, it is necessary for Shopee to secure proof by taking a photo that proves that the package has been delivered to the buyer, as explained in its Verified Comment:

47. The POD plays a crucial role in the confirmation of delivery for the consummation of the sale transactions through the Shopee App.

47.1. It is only upon receiving confirmation from the buyer and clicking “Order Received” in the Shopee App that Shopee releases the amount to be paid to the sellers. Otherwise, the seller will have to wait for a certain period from actual delivery, without getting any complaint, before receiving payments. Prior to confirmation or the lapse of the foregoing period, the seller will not receive the buyer’s payment, thereby preventing the consummation of the sale transaction between the buyers and sellers using the Shopee App.

47.2. If there are any issues relating to delivery of the orders made through the Shopee App, the buyer should not click “Order Received”, which suspends the release of payment to the seller. The POD is one of the means in resolving issues relating to deliveries of such orders, and taken for the protection of both the buyer and the seller (i.e. processing refunds for incomplete or wrong orders), as well as the Company, 3PL service providers and their respective service providers (i.e. mis-delivery or non-delivery). Said photos are used as evidence in case of issues relating to the delivery and receipt of the items ordered via the Shopee App.<sup>55</sup>

There is legitimate interest in taking a photo as proof of delivery as is necessary in this case. Thus, the third requisite is present.

The fourth requisite, however, is lacking in this case. MAF could have reasonably foreseen that the processing is for a purpose that is necessary and related to Shopee’s legitimate interest. In fact, it was MAF herself who filed for a refund because of a missing item on her order. A complaint for incomplete or wrong orders necessarily gives rise to a review of the proof of delivery of the package for the buyer, seller, and Shopee to resolve the issue. Thus, MAF cannot claim that the proof of delivery was processed for an unauthorized purpose.

Given the absence of the fourth requisite, Shopee is not liable under Section 28 (Processing of Personal or Sensitive Personal Information for Unauthorized Purposes) of the DPA.

## **II. Shopee is not liable under Section 32 (Unauthorized Disclosure) of the DPA.**

MAF alleged that Shopee committed Unauthorized Disclosure under Section 32 of the DPA when Shopee disclosed her son’s photo as proof of delivery to the seller. Section 32 (a) of the DPA provides:

Section. 32. Unauthorized Disclosure. (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding sec-

<sup>54</sup> *Id.*  
<sup>55</sup> Respondent’s Verified Comment, 17 November 2021, at 18-19, in MAF v. Shopee Philippines, Inc. NPC 21-167 (NPC 2021).



tion 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).<sup>56</sup>

The Commission has previously explained that a strict and literal reading of Section 32 of the DPA will result in absurdity:

A strict and literal reading of Section 32 of the DPA on Unauthorized Disclosure shows that a personal information controller (PIC) or personal information processor (PIP) is liable if it discloses to a third party personal information without the consent of the data subject. Such reading, however, will result in absurdity since it penalizes a PIC or a PIP if the disclosure is without the consent of the data subject even if such disclosure is justified under some other criteria for lawful processing in Sections 12 and 13 of the DPA.<sup>57</sup>

The rules of statutory construction provide that:

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.<sup>58</sup>

Given this, Section 32 of the DPA must be read together with other provisions of the DPA:

A law must not be read in truncated parts; its provisions must be read in relation to the whole law. It is the cardinal rule in statutory construction that a statute's clauses and phrases must not be taken as detached and isolated expressions, but the whole and every part thereof must be considered in fixing the meaning of any of its parts in order to produce a harmonious whole. Every part of the statute must be interpreted with reference to the context, i.e., that every part of the statute must be considered together with other parts of the statute and kept subservient to the general intent of the whole enactment.<sup>59</sup>

Thus, Unauthorized Disclosure is committed when:

[T]he perpetrator processes personal information without any of the lawful basis for processing under Sections 12 and 13 of the DPA. The interpretation is in line with the principle that "when two or more interpretations are possible, that interpretation which is favorable or beneficial to the accused must be adopted." It benefits the accused since it narrows the extent to which the disclosure of personal information may be considered as Unauthorized Disclosure.<sup>60</sup>

Unauthorized Disclosure under Section 32 requires that personal information or sensitive personal information is disclosed to a third party without any of the lawful criteria under Sections 12 and 13, as applicable.<sup>61</sup>

Here, MAF claimed that Shopee, as the PIC that acted through its PIP, allegedly disclosed personal information to the seller, a third party, without her consent.

<sup>56</sup> Data Privacy Act of 2012, § 32 (a).

<sup>57</sup> NPC 19-134, 10 December 2021 (NPC 2021) (unreported).

<sup>58</sup> Metropolitan Bank and Trust Co. v. Liberty Corrugated Boxes Manufacturing Corp., G.R. No.184317 (2017).

<sup>59</sup> Fort Bonifacio Development Corp. v. Commissioner of Internal Revenue, G.R. Nos. 158885 & 170680 (Resolution) (2009).

<sup>60</sup> NPC 21-032, 16 May 2022 (NPC 2022) (unreported).

<sup>61</sup> NPC 21-010, 03 February 2022 (NPC 2022) (unreported).

As previously discussed, Shopee, through its PIP, processed the photo because it was necessary for its legitimate interest. Consent is not the only the lawful basis for processing personal information. Aside from consent, processing of personal information is allowed when the disclosure is done under one of the lawful criteria for processing in Section 12 of the DPA.<sup>62</sup>

Further, the seller is not considered a third party to the online shopping transaction. As previously stated, Shopee “acts as an intermediary that brings together the Seller and the Buyer.”<sup>63</sup> The parties to the sale remain the buyer and the seller. Thus, the supposed disclosure of Shopee to the seller of the photo as proof of delivery cannot be considered as Unauthorized Disclosure under Section 32 of the DPA.

### III. Shopee violated the general privacy principle of proportionality.

Shopee violated the proportionality principle when the PIP’s rider took the photo as proof of delivery. The general privacy principle of proportionality requires that the processing is adequate, relevant, suitable, and necessary processing that is not excessive in relation to the declared and specified purpose.

Section 11 of the DPA provides principles that rest on proportionality:

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 proportionality, transparency,

Personal information must, be:

...

(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;

(d) **Adequate and not excessive in relation to the purposes for which they are collected and processed[.]**<sup>64</sup>

Section 18 of the Implementing Rules and Regulations of the DPA (IRR) elaborates on proportionality:

Section 18. *Principles of Transparency, Legitimate Purpose and Proportionality.* The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.

...

c. Proportionality. The processing of information shall be **adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.** Personal data shall be processed only if the purpose of the processing could

62 Data Privacy Act of 2012, § 12.  
63 Respondent’s Memorandum, 10 May 2022, at 24, in *MAF v. Shopee Philippines, Inc.* NPC 21-167 (NPC 2022).  
64 Data Privacy Act of 2012, § 11. Emphasis supplied.

not reasonably be fulfilled by other means.<sup>65</sup>

Given this, processing is deemed proportional when (1) processing is adequate, relevant, and necessary to the declared and specified purpose; and (2) the means by which processing is performed is the least intrusive means available.<sup>66</sup>

In this case, Shopee's act of taking the son's photo as proof of delivery is disproportional to the declared and specified purpose. The act of taking the son's photo is not necessary to the declared and specified purpose and the means is not the least intrusive means available. Shopee could have fulfilled the declared and specified purpose of securing proof of delivery with less intrusive means such as by taking a picture of an arm with the package.

In fact, Shopee's Privacy Guidelines for Shipments and Delivery provides that an arm of recipient and package, or house and package is sufficient in cases where the recipient of the package does not consent to his photo being taken. It states:

#### **Manner of Collection**

Consent is an essential element for taking the delivery photo. Before taking a delivery photo of the Customer/Recipient/Data Subject with the parcel, a consent from the Customer/Recipient/Data Subject should always be secured by the 3PL Rider.

In the event the Customer/Recipient/Data Subject refuses the above, the 3PL rider will request for the consent of the Customer/Recipient/Data Subject to capture proof of the following:

- a. An arm of Recipient and package or;
- b. House and parcel

In every instance, the delivery photo will focus on the placement of the package.<sup>67</sup>

Here, Shopee violated its own Guidelines when it took the photo of the son as proof of delivery. Shopee could have instead taken a photo of the son's arm and package, or house and package as its proof of delivery.

Further, Shopee mishandled the situation when MAF exercised her son's data subject rights. MAF exercised her son's right to have the photo removed when she initiated the "Live Chat" with a Customer Service (CS) Agent in the Shopee App and demanded that her son's photo be removed. Although the CS Agent tried to file a request, it was not immediately acted upon because the son's photo was used as the proof of delivery.<sup>68</sup> The CS Agent merely informed MAF that "[u]sers were advised that this was a standard procedure to take photos for proof of delivery" and provided MAF with a link to Shopee's Privacy Guidelines for Shipments and Delivery.<sup>69</sup>

Shopee was remiss in its obligation as a PIC. As a PIC, it should have complied with the

<sup>65</sup> National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule IV, § 18 (c) (2016).

<sup>66</sup> See Rules and Regulations Implementing the Data Privacy Act of 2012, rule IV, § 18 (c).

<sup>67</sup> Complainant's Memorandum, 06 May 2022, at 25, in *MAF v. Shopee Philippines, Inc.* NPC 21-167 (NPC 2022).

<sup>68</sup> *Id.* at 20-21.

<sup>69</sup> *Id.* at 20.

principle of proportionality under Section 11 (c) and (d) of the DPA. Although Shopee outsourced the delivery and consequently, securing proof of delivery to its PIP, it remains responsible for the PIP's actions following the principle of accountability. Nonetheless, Shopee's actions are insufficient to warrant a recommendation for its prosecution since the processing of personal information is still based on a lawful basis to process under Section 12 (f) of the DPA.

Shopee's actions, however, is sufficient to warrant an award of nominal damages.

Nominal damages are awarded in order to vindicate or recognize the complainant's right that was violated by the respondent even if no actual loss was shown.<sup>70</sup>The relevant provision in the New Civil Code, which governs the restitution of any party aggrieved in relation to the DPA, states:

Art. 2221. Nominal damages are adjudicated in order that a right of the plaintiff, which has been violated or invaded by the defendant, may be vindicated or recognized, and not for the purpose of indemnifying the plaintiff for any loss suffered by him.

The Supreme Court explained that no actual present loss is required to warrant the award of nominal damages:

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.<sup>71</sup>

The DPA does not require actual or monetary damages for data subjects to exercise the right to damages.<sup>72</sup> Shopee's violation of the proportionality principle and the mis-handling of the situation when MAF exercised the son's right to be removed from Shop-ee's system, are sufficient to award nominal damages.

**WHEREFORE**, premises considered, the Commission resolves to **DISMISS** the Complaint of MAF against Shopee Philippines, Inc. The Commission **AWARDS** nominal damages, in the amount of Fifteen Thousand Pesos (Php 15,000.00), to MAF for Shopee Philippines, Inc.'s violation the general privacy principle of proportionality.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against Shopee Philippines, Inc. before any other forum or tribunal, if any.

**SO ORDERED.**

City of Pasay, Philippines.  
22 September 2022.

**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

70 An Act to Ordain and Institute the Civil Code of the Philippines [CIVIL CODE], Republic Act No. 386, art. 2221 (1949).

71 Seven Brothers Shipping Corporation v. DMC-Construction Resources, Inc. G.R. No. 193914. November 26 2014.

72 NPC 18-038, 21 May 2020 (NPC 2020) (unreported).

I CONCUR:

**JOHN HENRY D. NAGA**  
Privacy Commissioner

Copy furnished:

**MAF**

*Complainant*

**SHOPEE PHILIPPINES, INC.**

*Respondent*

37/F Net Park Building  
5th Avenue Bonifacio  
Global City Fort Bonifacio  
Taguig City

**MARTINEZ VERGARA GONZALEZ & SERRANO (MVGS) LAW FIRM**

*Counsel for Respondent*

33rd Floor, The Orient Square  
F. Ortigas, Jr. Road, Ortigas Center 1600  
Pasig City, Metro Manila

**COMPLAINTS AND INVESTIGATION DIVISION**

**ENFORCEMENT DIVISION**

**GENERAL RECORDS UNIT**

National Privacy Commission

**MVC,**

*Complainant,*

-versus-

**NPC 21-010**  
For: Violation of the  
Data Privacy Act of  
2012

**DSL,**

*Respondent.*

X-----X

**RRB,**

*Complainant,*

-versus-

**NPC 21-011**  
For: Violation of the  
Data Privacy Act of  
2012

**DSL,**

*Respondent.*

X-----X

**NMB,**

*Complainant,*

-versus-

**NPC 21-012**  
For: Violation of the  
Data Privacy Act of  
2012

**DSL,**

*Respondent.*

X-----X

**RMP,**

*Complainant,*

-versus-

**NPC 21-013**  
For: Violation of the  
Data Privacy Act of  
2012

**DSL,**

*Respondent.*

X-----X

**NDL,**

*Complainant,*

-versus-

**NPC 21-014**  
For: Violation of the  
Data Privacy Act of  
2012

**DSL,**

*Respondent.*

X-----X

**MBN,**

*Complainant,*

-versus-

**NPC 21-015**  
For: Violation of the  
Data Privacy Act of  
2012

**DSL,**

*Respondent.*

X-----X

## DECISION

### AGUIRRE, D.P.C.;

Before this Commission are six separate Complaints filed against DSL for an alleged violation of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (DPA).

#### Facts

MVC, RRB, NMB, RMP, NDL, and MBN (Complainants) filed separate complaints against DSL.<sup>1</sup>

Complainants are condominium unit owners of GA Tower I, a condominium managed by GA Tower 1 Condominium Corporation (GAT1CC).<sup>2</sup> DSL, allegedly as the President of GAT1CC, published a letter containing Complainants' personal information.<sup>3</sup>

Complainants alleged that DSL caused the posting of a letter dated 23 November 2020 which contains a list of delinquent unit owners, their respective addresses, and their corresponding unpaid dues.<sup>4</sup> The letter was posted in the public spaces of the condominium and published in a magazine distributed to other unit owners.<sup>5</sup> Complainants assert that DSL's act resulted in the disclosure of their personal information.<sup>6</sup> Complainants pray for damages and a fine imposed against DSL for maligning their integrity.<sup>7</sup> Complainants also pray that the Commission find DSL liable for unlawfully disclosing their personal information which results in a violation of the DPA.<sup>8</sup>

On 21 July 2021, the Commission issued an Order directing DSL to file a verified comment within fifteen (15) calendar days from receipt of this Order.<sup>9</sup>

On 02 September 2021, DSL filed his Comment (Consolidated).<sup>10</sup> He alleged that GAT1CC is within its right to assess and collect unpaid condominium dues from delinquent unit owners, which includes Complainants.<sup>11</sup> He maintains that there was no violation of the DPA since GAT1CC necessarily processed Complainants' personal information for compliance with a legal obligation to which it, as a personal information controller (PIC), is subject.<sup>12</sup> It explains that its legal obligation to collect reasonable assessments and dues stems from Republic Act No. 4726 or the Condominium Act, which recognizes that assessments may be made against unit owners:

Section 20. An assessment upon any condominium made in accordance with a duly registered declaration of restrictions shall be an obligation of the owner thereof at

---

1 Complaint-Assisted Form, 08 June 2018, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending).

2 *Id.*

3 *Id.*

4 *Id.*

5 *Id.*

6 *Id.*

7 Complaint-Assisted Form, 08 June 2018, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending).

8 *Id.*

9 Order to Comment, 21 July 2021, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending).

10 Comment (Consolidated), 31 August 2021, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending).

11 *Id.* at 2.

12 *Id.* at 10.

the time the assessment is made.<sup>1</sup>

It also maintains that its Master Deed states that assessments for common expenses may be made against unit owners:

Section 24. ASSESSMENTS: (a) Assessments against units owners, purchaser or tenants for common expenses, particularly but not by way of limitation, common expenses shall include: expenses for administration of the project, and expenses of maintenance, operation, repair or replacement of common areas.<sup>2</sup>

Its By-Laws further provide:

Article V. Section 2. Regular Assessments for Operating Expenses. The Board of Directors shall from time to time, and at least annually prepare an estimate of the operating expenses of the corporation and against the member, proportion to such members' appurtenant propriety interest or participation in the corporation, such as shall be necessary to meet the operating expenses.<sup>3</sup>

Its House Rules and Regulations state:

#### 24. PAYMENT OF CONDOMINIUM ASSESSTMENTS (sic)

All unit owners will be ultimately liable (regardless whether or not the unit is occupied by the owner/ lessee) for the duly authorized Association expenses and projects which will be assessed against each one of them and paid to the Association subject to requirements of Master of Deeds. The condominium corporation shall time to time determine the amount of fees, dues, assessments (Realty Estate Tax, Insurance Premium, etc.) that shall be levied against unit owners, which are necessary for the maintenance, operation, preservation, protection, improvements and enhancement of the condominium building and its facilities. All interests are compounded monthly.<sup>4</sup>

DSL prays for dismissal of the case.<sup>5</sup>

On 28 September 2021, the Commission ordered the parties to submit their respective Memoranda within fifteen (15) calendar days from receipt of the Order.<sup>6</sup>

On 08 October 2021, DSL filed his Memoranda (Consolidated).<sup>7</sup> He reiterated that GAT1CC's lawful basis to process Complainants' personal information for the compliance of a legal obligation to assess and collect unpaid dues.<sup>8</sup> He further states that Complainants, as members of GAT1CC, are bound by the Condominium Act, Master Deed, By-Laws, and its House Rules and Regulations.<sup>9</sup>

DSL asserts that GAT1CC, through DSL, its President, was well within its right to post the

---

1 *Id.* at 11.

2 *Id.*

3 *Id.* at 12-13

4 Comment (Consolidated), 31 August 2021, at 13-14, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending).

5 *Id.* at 20.

6 Order, 28 September 2021, in MVCVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending).

7 Memoranda(Consolidated), 08 October 2021, at 13-14, in MVCVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending).

8 *Id.* at 12-19.

9 *Id.*



names of delinquent unit owners in order to collect reasonable dues and assessments.<sup>10</sup>

On 11 October 2021, Complainants RRB, NMB, RMP, NDL, and MBN filed their respective Memoranda.<sup>11</sup> They allege that DSL acted in bad faith and malice and had no authority to post the letter dated 23 November 2020, and process their personal information, since he was no longer the President of GAT1CC when the letter was published in the magazine distributed to other unit owners. They further claim that the House Rules and Regulations cited by DSL is different from that they received as unit owners. The relevant provision states:

#### M. CONDOMINIUM DUES, CHARGES, AND ASSESSMENTS

1. In order to operate and maintain the condominium building as well as to sustain the delivery of common utilities and services, all unit owners and/or tenants are under obligation to pay the condominium dues, charges and assessments, whether the unit concerned is occupied or not by the owner/ lessee, constructive delivery of the unit being sufficient.

...

3. All unit owners and/ or tenants will be proportionately liable for common area expenses or other duly authorized expenses and project costs, which shall be assessed against each unit owner and/ or tenant and these shall be paid to (each DECLARANT and shall be forwarded) to the Condominium Corporation.<sup>12</sup>

### Issues

I. Whether DSL's publication of the 23 November 2021 letter containing Complainants' personal information is necessary for compliance under a legal obligation that GAT1CC is subject to, pursuant to Section 12 (c) of the DPA.

II. Whether DSL's publication of the 23 November 2021 letter containing Complainants' personal information violates Section 32 (Unauthorized Disclosure) of the DPA.

### Discussion

At the onset, it bears stressing that the 23 November 2021 letter contains personal information, particularly the names of some delinquent unit owners. Matters concerning the processing of personal information is within the scope of the DPA and under the jurisdiction of the Commission.<sup>13</sup>

---

<sup>10</sup> *Id.*

<sup>11</sup> Memorandum by RRB, 11 October 2021, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending), Memorandum by NMB, 11 October 2021, in MVC, et al. v. Delfin S. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending), Memorandum by Regidor M. RMP, 11 October 2021, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending), Memorandum by NDL, 11 October 2021, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending), Memorandum by MBN, 11 October 2021, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending).

<sup>12</sup> Memorandum by MBN, 11 October 2021, Annex I, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending).

<sup>13</sup> See Data Privacy Act of 2012, § 4 on the scope of the DPA which provides "This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing"

The publication of the 23 November 2021 letter in a magazine distributed to other unit owners was without lawful basis of processing under Section 12 (c) of the DPA. Thus, it is a violation of Section 32 of the DPA on Unauthorized Disclosure.

The Commission did not consider in this Decision the notices posted in GA Tower I's premises since the contents of the notices cannot be deciphered from the photos attached in the complaints. Aside from this, the Complainants hardly discussed the notices such that the Commission cannot determine who posted the notices and the purpose behind the posting of such notices.

### **I. DSL's act of publishing the 23 November 2021 letter is not necessary for compliance under a legal obligation that GAT1CC is subject to.**

DSL claims that the disclosure of Complainants' personal information is based on the lawful criterion of fulfilment of a necessary obligation to which the personal information controller (PIC) is subject under Section 12 (c) of the DPA. Contrary to his assertions, DSL's act of publishing the letter dated 23 November in a magazine distributed to the unit owners of GA Tower I is not necessary for compliance under a legal obligation that GAT1CC is subject to. As such, it cannot be construed as processing based on lawful criteria under Section 12 (c) of the DPA. Section 12 (c) 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:

...

(c) The processing is **necessary for compliance with a legal obligation** to which the personal information controller is subject;<sup>14</sup>

When a PIC claims lawful processing on the basis of a legal obligation, the burden is on the PIC to show that all that is required by that particular lawful criterion is present. A PIC must be able to prove that the legal obligation it cites as basis exists and applies to the processing it performed, and that the processing is necessary to comply with the legal obligation.

In this case, DSL maintains that the disclosure of Complainants' personal information is for the purpose of complying with GAT1CC's legal obligation to assess and collect unpaid dues. While GAT1CC is entitled to undertake the processing of Complainants' personal information based on the Condominium Act, its By-Laws, Master Deed, and the different versions of the House Rules presented by the parties, DSL's actions were not pursuant to the declared and specified purpose.

The PIC should only process as much information as is proportional or necessary to achieve its clearly defined and stated purposes.<sup>15</sup>In this case, it is the collection of unpaid dues provided under a valid contract with its unit owners.

While it is necessary to process the delinquent unit owners' personal information in

<sup>14</sup> 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 (c) (2012).

<sup>15</sup> *Id.* § 11.

order to assess and collect payments pursuant to a contract, the processing in the form of issuing the letter was neither necessary nor proportional. The purpose of the letter was not for the collection of delinquent dues. Rather, the evidence on record shows that DSL disclosed Complainants' personal information as delinquent unit owners to cast doubt on their capability to manage the affairs of the condominium corporation in light of the recently held election of the Board of Directors. As DSL stated in his letter dated 23 November 2020:

I have been informed that a few unit owners are attempting to surreptitiously and illegally take charge of the management of the Condominium Corporation. Please be guided that these individuals are continuously tagged by the present management as delinquent unit owners. Hence they lack the minimum qualification and moral ascendancy to direct the affairs of the Condominium Corporation.

...

Now, in case the management of the Condominium Corporation be in the hands of those delinquent unit owners aspiring to become members of the Board, what will happen to our building?

...

Now, do you want to risk the management of the Condominium Corporation to some delinquent unit owners?<sup>16</sup>

DSL claims that he wrote the letter on behalf of the condominium corporation as its President.<sup>17</sup> A mere claim that it was done on behalf of the condominium corporation is not sufficient. Had it truly been on behalf of the Board of Directors, then DSL would have been able to present something other than a mere statement in the letter.

Thus, DSL's processing of Complainants' personal information is not based on a lawful criterion under Section 12 (c) of the DPA.

## **II. DSL is liable for Section 32 (Unauthorized Disclosure) of the DPA when he published the 23 November 2021 letter containing Complainants' personal information.**

DSL violated Section 32 of the DPA on Unauthorized Disclosure. Section 32 of the DPA 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).<sup>18</sup>

Section 32 of the DPA refers to the "immediately preceding section" or Section 31 of the DPA on Malicious Disclosure, which provides:

<sup>16</sup> Complaint-Assisted Form, 08 June 2018, Annex, in Manuel D.V. MVCMVC, et al. v. Delfin S. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, and NPC 21-015 (NPC 2021) (pending).

<sup>17</sup> *Id.*

<sup>18</sup> *Id.* § 32.

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).<sup>19</sup>

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.<sup>20</sup> 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.

Malicious Disclosure requires the disclosure of personal information is malicious or in bad faith. The existence of malice or bad faith cannot be presumed.<sup>21</sup> In this case, the evidence on record does not show that DSL’s disclosure of their personal information was malicious or done in bad faith. Section 131 of the 2019 Amendments to the Revised Rules of Evidence provides:

Section 1. *Burden of proof and burden of evidence.* - Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim or defense by the amount of evidence required by law. Burden of proof never shifts.<sup>22</sup>

Thus, it was incumbent upon Complainants to prove their claim that DSL’s acts were malicious or in bad faith. The quantum of proof necessary for a finding of guilt in administrative proceedings is substantial evidence:

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.<sup>23</sup>

Complainants failed to present substantial evidence to show that DSL’s actions were malicious or amounting to bad faith. Absent the third requisite of Malicious Disclosure, the offense falls under Section 32 or Unauthorized Disclosure.

Based on a literal reading of Section 32 of the DPA, a PIC or a PIP is liable if it discloses to a third party personal or sensitive personal information without the consent of the

---

19 *Id.* § 31.  
20 *Id.*  
21 Cruz v. Intermediate Appellate Court, G.R. No. 66327 (1984).  
22 Supreme Court of the Philippines, A.M. No. 19-08-15-SC “2019 Amendments to the 1989 Revised Rules on Evidence” [Rules of Court], Rule 131, §1 (1 May 2020).  
23 BSA Tower Condominium Corp. v. Reyes II, A.C. No. 11944 (2018).

data subject.<sup>24</sup> Following a literal reading, a PIC or a PIP will have committed Unauthorized Disclosure if the disclosure is without the consent of the data subject even if the disclosure is justified by another lawful criterion for processing. It does not recognize that such disclosure may be based on other criteria for lawful processing enumerated in Sections 12 and 13 of the DPA. As such, a literal reading of Section 32 of the DPA will result in absurdity. 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.<sup>25</sup>

Since a literal reading of Section 32 of the DPA will result in absurdity, the provision should be further examined. It should be read together with other provisions of the DPA:

A law must not be read in truncated parts; its provisions must be read in relation to the whole law. It is the cardinal rule in statutory construction that a statute's clauses and phrases must not be taken as detached and isolated expressions, but the whole and every part thereof must be considered in fixing the meaning of any of its parts in order to produce a harmonious whole. Every part of the statute must be interpreted with reference to the context, i.e., that every part of the statute must be considered together with other parts of the statute and kept subservient to the general intent of the whole enactment.<sup>26</sup>

Thus, Section 32 of the DPA on Unauthorized Disclosure should be read together with Sections 12 and 13 on the criteria for lawful processing of personal and sensitive personal information. The presence of any of the criteria listed in Sections 12 and 13 is sufficient to justify the processing of personal or sensitive personal information, as the case may be, including its disclosure.<sup>27</sup> Reading Section 32 of the DPA in isolation will render Sections 12 and 13 of the DPA inoperative violating a basic rule of statutory construction:

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.**<sup>28</sup>

Given the foregoing, 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.<sup>29</sup> 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."<sup>30</sup>

This interpretation benefits the accused since it narrows the extent to which the disclosure of personal information may be considered as Unauthorized Disclosure.<sup>31</sup>

24 Data Privacy Act of 2012, § 32.

25 Metropolitan Bank and Trust Co. v. Liberty Corrugated Boxes Manufacturing Corp., G.R. No.184317 (2017).

26 Fort Bonifacio Development Corp. v. Commissioner of Internal Revenue, G.R. Nos. 158885 & 170680 (Resolution) (2009).

27 See Data Privacy Act of 2012, § 3(j) on the definition of processing which "refers to any operation or any set of operations performed upon personal information" which necessarily includes the sharing and disclosure of personal information.

28 JMM Promotions & Management, Inc. v. National Labor Relations Commission, G.R. No. 109835 (1993). Emphasis supplied.

29 NPC 19-134, 10 December 2021 (NPC 2021) (unreported).

30 People v. Liban, G.R. Nos. 136247 & 138330 (2000).

31 NPC 19-134, 10 December 2021 (NPC 2021) (unreported).

A finding of Unauthorized Disclosure requires that the following requisites are satisfied:

1. The perpetrator is a personal information controller or personal information processor;
2. The perpetrator disclosed information;
3. The information relates to personal or sensitive personal information;
4. The perpetrator disclosed the personal or sensitive personal information to a third party;
5. The disclosure was without any of the lawful basis for processing, consent or otherwise, under Sections 12 and 13 of the DPA; and
6. The disclosure is neither malicious nor done in bad faith and the information disclosed is not unwarranted or false information.

Here, DSL disclosed Complainant’s personal information to third parties when he caused the publication of their names in the magazine distributed to other unit owners of GA Tower I. Contrary to DSL’s assertions, the disclosure of Complainants’ personal information was not according to a valid criterion of lawful processing, particularly Section 12 (c) of the DPA. As previously discussed, DSL cannot rely on compliance of a legal obligation because he disclosed Complainants’ personal information for a completely different purpose. In fact, he did not issue the letter in the interest of the condominium corporation. Thus, DSL is liable under Section 32 of the DPA on Unauthorized Disclosure.

**WHEREFORE**, premises considered, the Commission hereby:

1. **FINDS** Delfin S. DSL liable for Section 32 (Unauthorized Disclosure) of the Data Privacy Act of 2012; and
2. **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice and recommends the prosecution of DSL for the offense of Unauthorized Disclosure under Section 32 of the DPA.

**SO ORDERED.**

Pasay City, Philippines.  
03 February 2022.

**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

I CONCUR:

**JOHN HENRY D. NAGA**  
Privacy Commissioner

Copy furnished:

**MVC**  
Complainant

**RRB**

Complainant

**NMB**

Complainant

**RMP**

Complainant

**NDL**

Complainant

**MBN**

Complainant

**ERP**

Counsel for Respondent

**CTB**

Counsel for Respondent

**COMPLAINTS AND INVESTIGATION DIVISION**

**ENFORCEMENT DIVISION**

**GENERAL RECORDS UNIT**

National Privacy Commission

**GBA,**

*Complainant,*

**NPC 20-317**  
For: Violation of the  
Data Privacy Act of  
2012

-versus-

**SBG**

*Respondent.*

X-----X

**LPL,**

*Complainant,*

**NPC 20-318**  
For: Violation of the  
Data Privacy Act of  
2012

-versus-

**SBG**

*Respondent.*

X-----X

## DECISION

### AGUIRRE, D.P.C.;

Before this Commission are the consolidated cases filed by GBA and by LPL (Complainants) against SBG for an alleged violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

### Facts

The Complainants are members of the Benguet State University and Community Multipurpose Cooperative (Cooperative).<sup>1</sup> They alleged that on two separate occasions, SBG accessed the IT Accounting System of the Cooperative, printed the accounts of some of the members, including those of the Complainants, and showed the printed documents to some officers of the Cooperative.<sup>2</sup> The Complainants claimed that SBG accessed their personal data, particularly their names, addresses, marital status, and details of their savings and loans accounts.<sup>3</sup>

According to the Complainants, SBG had no authority to access the accounts because she was no longer an employee of the Cooperative when she accessed their accounts.<sup>4</sup> Further, the Complainants asserted that they did not give their consent to the processing of their accounts.<sup>5</sup> The Complainants claimed that they are entitled to damages for the alleged unauthorized access of their accounts.<sup>6</sup>

On 18 August 2021, the Commission, through its Complaints and Investigation Division

1 Complaints-Assisted Form, 01 December 2020, in GBA v. SBG, NPC 20-317 (NPC 2022); Complaints-Assisted Form, 03 December 2020, in LPL v. SBG, NPC 20-318 (NPC 2022).

2 *Id.*

3 *Id.*

4 *Id.*

5 *Id.*

6 *Id.*



(CID), issued an Order directing the Complainants to submit their evidence to support the allegations in their complaints.<sup>7</sup>

On 23 August and 24 August 2021, LPL and GBA, respectively, submitted the same set of documentary evidence, which includes:

1. Joint Affidavit of JTA and Rhodora LPL, who personally witnessed SBG’s alleged processing of the Complainants’ accounts;<sup>8</sup> and
2. Copies of the accounts and ledgers, which SBG allegedly processed.<sup>9</sup>

On 14 October 2021, the CID issued an Order directing SBG to file her comment and scheduling the preliminary conference on 18 January 2022.<sup>10</sup>

On 10 December 2021, SBG filed her Comment.<sup>11</sup> She denied all the allegations of the Complainants and argued that her acts “were in accordance with her function as Audit and Compliance Officer (ACO).”<sup>12</sup>

She claimed that:

On or about June 2019, as part of her duty to render report to the CEO/BOD that reflect audit result on all discrepancies, deficiencies or any unusual noted in the course of audit, [SBG] was tasked by the CEO of [the Cooperative] and wife of Complainant GBA, JTA, to review the 2017 Risk-Based Evaluation Report of [the Cooperative], comparing the same to the performance of the Cooperative for the years 2018 and 2019, and providing a report indicating any developments during the said reporting periods.<sup>13</sup>

She further narrated that while she was reviewing the Cooperative’s accounts, she discovered questionable transactions that involved JTA, who is the Cooperative’s Chief Executive Officer (CEO), and LPL, who is the Cooperative’s accountant and bookkeeper.<sup>14</sup> SBG further alleged that the transactions also involved the Complainants, who are family members of JTA and LPL.<sup>15</sup>

According to SBG, after she resigned from the Cooperative, she received a letter from the Cooperative’s Audit Committee requesting for her assistance in the conduct of an audit in relation to the questionable transactions she previously discovered.<sup>16</sup>

SBG alleged that during the audit, the Board of Directors and the Audit Committee requested LPL “to print a copy of the journal vouchers, ledgers, and financial statements.”<sup>17</sup> She denied the allegation of the Complainants that she accessed the accounts and claimed that it was actually LPL who “searched, accessed, and printed the copies

7 Order, 18 August 2021, in GBA v. SBG and LPL v. SBG, NPC 20-317 and 20-318 (NPC 2022).

8 Submission and Offer of Documentary Evidence, 23 August 2021, Exhibit A, in GBA v. SBG and LPL v. SBG, NPC 20-317 and 20-318 (NPC 2022); Submission and Offer of Documentary Evidence, 24 August 2021, Exhibit A, in GBA v. SBG and LPL v. SBG, NPC 20-317 and 20-318 (NPC 2022).

9 *Id.*, 23 August 2021, Exhibits B-I; *Id.*, 24 August 2021, Exhibits B-I.

10 Order, 14 October 2021, at 1, in GBA v. SBG and LPL v. SBG, NPC 20-317 and 20-318 (NPC 2022).

11 Comment, 10 December 2021, in GBA v. SBG and LPL v. SBG, NPC 20-317 and 20-318 (NPC 2022).

12 *Id.* at 2.

13 *Id.* at 3.

14 *Id.* at 3-4.

15 *Id.*

16 *Id.* at 5.

17 Comment, 10 December 2021, at 5, in GBA v. SBG and LPL v. SBG, NPC 20-317 and 20-318 (NPC 2022).

of the Journal Vouchers.”<sup>18</sup>

SBG argued that the processing of the Complainants’ personal data was “necessary for the legitimate interest of [the Cooperative] and its General Assembly”<sup>19</sup> and “necessary for the protection of the lawful rights and interests of the [Cooperative] and its members as well as for the establishment and exercise of a legal claim”.<sup>20</sup> She further asserted that “[a]sking the consent of the persons involved prior to the audit is not only impractical but will also run counter to the goal of the [C]ommittee to investigate possible fraudulent transactions.”<sup>21</sup>

In addition, SBG asserted that she did not violate the general privacy principles of transparency, legitimate purpose, and proportionality.<sup>22</sup> SBG argued that during the pre-membership seminar, the members of the Cooperative are “apprised of the data/information that he or she needs to provide to the [C]ooperative, as well as the purpose of collecting the said data” and the duties and responsibilities of the Cooperative’s Board of Directors, officers, and committees.<sup>23</sup> Thus, SBG claimed that the Complainants “cannot feign ignorance as to the necessity of processing [their] information for audit purposes.”<sup>24</sup> She also alleged that as the ACO, she “was well within the scope of her duty to look into irregular and unusual transactions involving the money of the cooperative members.”<sup>25</sup>

During the Preliminary Conference on 18 January 2022, the Complainants’ counsel moved for the consolidation of the cases on the ground that both have the same facts and issues.<sup>26</sup> The CID granted the motion to consolidate the cases and directed the parties to submit their respective pre-trial briefs and their respective comments to the pretrial briefs.<sup>27</sup>

The Complainants submitted their Joint Pre-Trial Brief dated 28 January 2022, which included their proposed facts for stipulation and admission and their manifestation to present additional documentary evidence.<sup>28</sup> SBG filed her Compliance with Pre-Trial Brief dated 02 February 2022, which also included her proposed stipulation of facts and the list of documents she manifested to offer as evidence.<sup>29</sup>

Thereafter, the Complainants filed their Comment to the Stipulations of Fact Proposed by the Respondent dated 15 February 2022.<sup>30</sup> SBG filed her Comment/Objection to the Pre-Trial Brief of the Complainants dated 16 February 2022.<sup>31</sup>

---

18 *Id.*

19 *Id.* at 8.

20 *Id.* at 10.

21 *Id.* at 5.

22 *Id.* at 5-8.

23 Comment, 10 December 2021, at 6, in *GBA v. SBG and LPL v. SBG*, NPC 20-317 and 20-318 (NPC 2022).

24 *Id.* at 7.

25 *Id.* at 8.

26 6 Order, 18 January 2022, at 1, in *LPL v. SBG*, NPC 20-318 (NPC 2022).

27 *Id.*

28 Joint Pre-Trial Brief for the Complainants, 28 January 2022, in *GBA v. SBG and LPL v. SBG*, NPC 20-317 and 20-318 (NPC 2022).

29 Compliance with Pre-Trial Brief, 02 February 2022, in *GBA v. SBG and LPL v. SBG*, NPC 20-317 and 20-318 (NPC 2022).

30 Comment to the Stipulations of Fact Proposed by Respondent, 15 February 2022, in *GBA v. SBG and LPL v. SBG*, NPC 20-317 and 20-318 (NPC 2022).

31 Comment/Objection to the Pre-Trial Brief of the Complainants, 16 February 2022, in *GBA v. SBG and LPL v. SBG*, NPC 20-317 and 20-318 (NPC 2022).

On 27 May 2022, the Complainants filed their Memorandum.<sup>32</sup> They alleged that SBG violated the provisions of the DPA when she accessed and processed the Complainants' personal information without their consent.<sup>33</sup>

The Complainants argued that the fulfillment of the Cooperative's legitimate interest does not excuse SBG from securing the consent of the data subjects.<sup>34</sup> They questioned SBG's authority since she was neither an employee nor an officer of the Cooperative at the time of her processing of their personal information.<sup>35</sup>

They asserted that they are entitled to damages considering that SBG "accessed and processed their personal information without their knowledge and consent."<sup>36</sup>

In her Memorandum, SBG claimed that she was authorized to assist with the audit "by virtue of a decision from the Board of Directors ordering the Audit Committee to request for [her] assistance."<sup>37</sup> She further argued that the audit was for the protection of the legitimate interest of the Cooperative and its General Assembly and for the establishment of a legal claim.<sup>38</sup> She alleged that as a result of the audit, a criminal case was filed against the Complainants, GBA, LPL, and other persons involved.<sup>39</sup>

SBG asserted that the processing of Complainants' personal information was proportionate and necessary to pursue the Cooperative's legitimate interest:

The processes employed by the Audit Committee, as well as [SBG] in the conduct of the audit are in accordance with the cooperative [sic] policies, and are proportionate and necessary to pursue the cooperative's legitimate interest. In the conduct of the audit, [SBG] did not disclose to third persons the contents of the information that were subjected to audit. [...] In fact, throughout the audit proceedings, [SBG] made sure that the information handed to her would not be leaked prior to the validation and verification of the irregular transactions.<sup>40</sup>

Lastly, SBG claimed that she is entitled to damages "for the baseless and unwarranted filing of these cases."<sup>41</sup>

### **Issue**

Whether SBG is liable for Unauthorized Processing of Personal Information or Sensitive Personal Information under Section 25 of the DPA.

### **Discussion**

The Commission finds that SBG is not liable for Unauthorized Processing of Personal Information or Sensitive Personal Information under Section 25 of the DPA. Her processing of the Complainants' personal information was lawful in accordance with Section 12 (f) of the DPA.

32 Memorandum for the Complainants, 27 May 2022, in GBA v. SBG and LPL v. SBG, NPC 20-317 and 20-318 (NPC 2022).

33 *Id.* at 5-9.

34 *Id.* at 10.

35 *Id.* at 14.

36 *Id.* at 15.

37 Memorandum for the Respondent, 27 May 2022, at 8, in GBA v. SBG and LPL v. SBG, NPC 20317 and 20-318 (NPC 2022).

38 *Id.* at 10-11.

39 *Id.* at 11.

40 *Id.*

41 *Id.* at 12.

To determine whether there is an Unauthorized Processing of Personal Information or Sensitive Personal Information, the following requisites must concur:

1. The perpetrator processed the information of the data subject;
2. The information processed was personal information or sensitive personal information; and
3. The processing was done without the consent of the data subject, or without being authorized under the DPA or any existing law.<sup>42</sup>

As to the first requisite, SBG did not refute the allegation that she processed the personal information of the Complainants. While it is not clear who really accessed the accounts of the members of the Cooperative, it is undisputed that SBG obtained a printed copy of the ledgers and account transactions of some of the members of the Cooperative and used the documents for the audit investigation.<sup>43</sup> The acquisition and use of the printed copy of the ledgers and account transactions are within the definition of “processing” under Section 3 (j) of the DPA:

Section 3. *Definition of Terms.* Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

...

(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.<sup>44</sup>

Thus, SBG processed personal data when she obtained and used the printed copy of the ledgers and account transactions.

As to the second requisite, the information processed was personal information. Section 3 (g) of the DPA defines personal information:

Section 3. *Definition of Terms.* Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

...

(g) *Personal information* refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.<sup>45</sup>

The printed ledgers and account transactions include the names and the account numbers of the Cooperative members.<sup>46</sup> These names and account numbers, when put

<sup>42</sup> NPC SS 21-006, 16 May 2022, at 31 (NPC 2022) (unreported).

<sup>43</sup> Memorandum for the Respondent, 27 May 2022, at 11, in GBA v. SBG and LPL v. SBG, NPC 20317 and 20-318 (NPC 2022).

<sup>44</sup> 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 (j) (2012).

<sup>45</sup> *Id.* § 3 (g).

<sup>46</sup> See Comment, 10 December 2021, Annex F, in GBA v. SBG and LPL v. SBG, NPC 20-317 and 20318 (NPC 2022).

together with other information, can directly and certainly identify the members of the Cooperative. Thus, they are considered personal information under the DPA.

The third requisite is not present. The members of the Cooperative claimed that SBG did not obtain their consent before processing their personal information.<sup>47</sup> SBG's processing, however, is still pursuant to a lawful criterion for processing personal information. Section 12 (f) of the DPA provides:

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

...

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.<sup>48</sup>

The Commission previously identified the following requisites for processing based on a legitimate interest:

Processing based on legitimate interest requires the fulfillment of the following conditions: (1) the legitimate interest is established; (2) the processing is necessary to fulfill the legitimate interest that is established; and (3) the interest is legitimate or lawful and it does not override fundamental rights and freedoms of data subjects.<sup>49</sup>

In this case, SBG clearly established that the processing of Complainants' personal information was not for her own interest, but for the interests of the Cooperative and upon the request and under the authority of the Board of Directors. As proof, she submitted the letter she received from the Audit Committee requesting her presence and assistance in the audit.<sup>50</sup> She also submitted a copy of the minutes of the meeting of the Board of Directors where they agreed to conduct an audit and to ask SBG's assistance in the audit.<sup>51</sup>

Further, SBG established that the Cooperative has the legitimate interest to protect its assets and its members.<sup>52</sup> She claimed that when the Cooperative confirmed, through the audit, that there were fraudulent transactions, it filed a criminal complaint against the persons involved in those transactions.<sup>53</sup> In order to substantiate these allegations, she submitted a copy of the Investigation Data Form and the Affidavit-Complaint of the Board of Directors in relation to the criminal complaint.<sup>54</sup>

As to the second and third requisites of legitimate interest, not only must the interest

47 Complaints-Assisted Form, 01 December 2020, in *GBA v. SBG*, NPC 20-317 (NPC 2022); Complaints-Assisted Form, 03 December 2020, in *LPL v. SBG*, NPC 20-318 (NPC 2022).

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

49 NPC 21-167, 22 September 2022, at 9 (NPC 2022) (unreported).

50 See Comment, 10 December 2021, Annex G, in *GBA v. SBG and LPL v. SBG*, NPC 20-317 and 20318 (NPC 2022).

51 See *Id.* Annex H.

52 Memorandum for the Respondent, 27 May 2022, at 11, in *GBA v. SBG and LPL v. SBG*, NPC 20317 and 20-318 (NPC 2022).

53 *Id.*

54 See Comment, 10 December 2021, Annex K & L, in *GBA v. SBG and LPL v. SBG*, NPC 20-317 and 20-318 (NPC 2022).

established be legitimate but the manner in which that legitimate interest is sought to be achieved is equally important. It must be done in a way that does not override the fundamental rights and freedoms of the data subjects taking into consideration the principles of proportionality and fairness.

In this case, the Commission finds that this interest is legitimate and does not override the fundamental rights and freedoms of the data subjects, including the Complainants. The Cooperative has the right to protect its interests, especially the savings and investments of its members. This legitimate interest does not, in any way, disregard the fundamental rights and freedoms of the Complainants.

SBG's processing of the Cooperative members' personal information was necessary for the conduct of the audit investigation to verify questionable transactions.<sup>55</sup> The Cooperative's interest to conduct the audit investigation is necessary to ensure that the financial information relating to the Cooperative is accurately recorded and to detect any irregular transactions.

It is within the legitimate interest of the Cooperative, through its Board of Directors, to authorize the conduct of the audit and the person who will conduct the same. The documents submitted<sup>56</sup> demonstrate that the Board of Directors authorized SBG to process the Complainants' personal information for the audit investigation. In this case, the totality of the evidence on record shows that when SBG processed the members' personal information, she was doing so under the authority granted to her and for the protection of the interests of the Cooperative and ultimately, its members. Further, from the evidence on record, the manner in which the audit was conducted was both proportional and fair to the Complainants. It involved only the information necessary to achieve its purpose and took steps to ensure the confidentiality of the audit.

All these circumstances taken together leads the Commission to reasonably conclude that SBG had authority to process the personal information of the Complainants for the purpose of the audit investigation. Further, there is nothing on record showing that SBG processed the Complainants' personal information for a purpose that is unrelated to the audit investigation. Given these, SBG lawfully processed the Complainants' personal information.

Considering that the third requisite is not present, SBG cannot be held liable for Unauthorized Processing of Personal Information or Sensitive Personal Information under Section 25 of the DPA.

**WHEREFORE**, premises considered, the Commission resolves that the Complaints filed by GBA and LPL against SBG is hereby **DISMISSED** for lack of merit.

This is without prejudice to the filing of appropriate civil, criminal, or administrative cases against the Respondent SBG before any other forum or tribunal, if any.

**SO ORDERED.**

City of Pasay, Philippines.  
13 October 2022.

<sup>55</sup> See *Id.* at 3-4.

<sup>56</sup> See *Id.* Annex G & H.

**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

I CONCUR:

**JOHN HENRY D. NAGA**  
Privacy Commissioner

Copy furnished:

**GBA**  
*Complainant*

**LPL**  
*Complainant*

**PABLITO, KIAT-ONG, CAPUYAN  
AND ASSOCIATES LAW OFFICE**  
*Counsel for the Respondent*  
Suite 206 2/F Golden Court Bldg.,  
Magsaysay Ave.,  
Baguio City

**COMPLAINTS AND INVESTIGATION DIVISION  
ENFORCEMENT DIVISION  
GENERAL RECORDS UNIT**  
National Privacy Commission

RJC,

*Complainant,*

**NPC 22-012**  
For: Violation of the  
Data Privacy Act of  
2012

-versus-

DL,

*Respondent.*

X-----X

## DECISION

### AGUIRRE, D.P.C.;

Before this Commission is a Complaint filed by RJC against DL for an alleged violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

#### Facts

On 31 January 2022, RJC, a student at the University of the Philippines Cebu (UP Cebu), filed a Complaint against DL, the College Secretary of the university’s College of Science.<sup>1</sup>

RJC alleged that he filed a complaint before the Office of the Ombudsman Region VII (Ombudsman case) against some personnel from UP Cebu, including DL.<sup>2</sup> He claimed that DL attached a copy of his transcript of records in DL’s counter-affidavit for the Ombudsman case.<sup>3</sup> According to RJC, DL used his transcript of records without his consent to prove that he is incapable of completing his Master of Science (MS) degree on time.<sup>4</sup> Thus, RJC argued that DL’s use of his transcript of records without his consent is in violation of the DPA.<sup>5</sup>

Further, RJC claimed that “it is against the law to process and disclose personal data [...] that is subject to vilification and harassment without the consent of the subject.”<sup>6</sup>

On 11 February 2022, the Commission, through its Complaints and Investigation Division (CID), issued an Order directing DL to file his comment within fifteen (15) calendar days from receipt of the Order.<sup>7</sup> It also directed the parties to appear for preliminary conferences on 06 April 2022 and on 17 May 2022.<sup>8</sup>

In his Comment, DL denied RJC’s allegations and claimed that he did not violate the DPA.<sup>9</sup> Thus, he prayed that the Complaint against him should be dismissed.<sup>10</sup> He stated that RJC filed the Ombudsman case claiming that the respondents in that case, including DL, “were deliberately and/or negligently delaying his graduation for no val-

1 Complaints-Assisted Form, 31 January 2022, Annex, in RJC v. DL, NPC 22-012 (NPC 2022).

2 *Id.*

3 *Id.*

4 *Id.*

5 *Id.*

6 *Id.*

7 Order, 11 February 2022, at 1, in RJC v. DL, NPC 22-012 (NPC 2022).

8 *Id.*

9 Comment, 07 March 2022, ¶¶ 6-7, in RJC v. DL, NPC 22-012 (NPC 2022).

10 *Id.*



id reason.”<sup>11</sup>He claimed that RJC made material allegations in the case, “which if not controverted by documentary evidence, may lead to the erroneous conclusion that [the] respondents in said Ombudsman cases [sic] abused their authority and committed grave misconduct in allegedly delaying the graduation of [RJC].”<sup>12</sup> He further argued that:

10. While students, in general, have a reasonable expectation of privacy as regards their school records, and granting arguendo that school records are protected by some measure of confidentiality, the confidentiality of such records is deemed waived by the student when he himself expressly makes a factual claim under oath, the falsity of which can only be substantiated by the presentation of his school records.<sup>13</sup>

DL argued that his act of attaching RJC’s transcript of records as evidence in the Ombudsman case is necessary for the exercise or defense of legal claims.<sup>14</sup>He claimed that the transcript of records contained specific information “which would debunk the claims made by [RJC] that [DL] along with other professors of UP Cebu deliberately and/or negligently caused his failure from earning his master’s degree.”<sup>15</sup>Further, he emphasized that:

22. In the University of the Philippines (UP) Privacy Notice for Students (Revised as of the 1st Semester/Trimester 2019- 2020), it is stated that sensitive personal information (e.g. educational records) may be processed when needed for the protection of lawful rights and interests of natural or legal persons in court proceedings; and for the establishment, exercise or defense of legal claims; or where provided to government or public authority.<sup>16</sup>

On 06 April 2022, RJC and DL attended the first preliminary conference.<sup>17</sup>The CID, however, rescheduled it to 12 July 2022.<sup>18</sup>

On 12 July 2022, the CID ordered both parties to submit their respective memoranda within fifteen (15) days from receipt of the Order.<sup>19</sup>

In his Memorandum dated 04 August 2022, RJC claimed that in accordance with Batas Pambansa Blg. 232 (Education Act of 1982), “schools shall maintain and preserve the confidentiality of school records.”<sup>20</sup>He also argued that school records are sensitive personal information, the processing of which is prohibited, unless authorized by law.<sup>21</sup>

RJC alleged that the disclosure of his grades before the Office of the Ombudsman was “unauthorized, malicious, and in direct violation of the principles of transparency, proportionality, and legitimate purpose.”<sup>22</sup> He claimed that DL’s processing was done without his consent and was not authorized under the DPA.<sup>23</sup>

RJC further alleged that DL’s disclosure of his transcript of records “despite the marking ‘for advising purposes only’ on such copy is a clear, patent[,] and direct violation

---

11 *Id.* ¶ 11.

12 *Id.* ¶ 12.

13 *Id.* ¶ 10.

14 *Id.* ¶ 20.

15 Comment, 07 March 2022, ¶ 24, in RJC v. DL, NPC 22-012 (NPC 2022).

16 *Id.* ¶ 22.

17 Order, 06 April 2022, at 1, in RJC v. DL, NPC 22-012 (NPC 2022).

18 *Id.* at 2.

19 Order, 12 July 2022, at 1-2, in RJC v. DL, NPC 22-012 (NPC 2022).

20 Memorandum, 04 August 2022, at 5, in RJC v. DL, NPC 22-012 (NPC 2022).

21 *Id.* at 5-7.

22 *Id.* at 1.

23 *Id.* at 9-10.

of the authorized purpose of the processing, issuance and disclosure of [his] sensitive personal information.”<sup>24</sup>

RJC asserted that DL’s disclosure of his transcript of records was malicious and unwarranted since it is irrelevant to the allegations in the Ombudsman case:

64. [DL] tried to argue that the school records contained relevant information that refutes [RJC’s] accusations and allegations. However, [DL] failed to specify with clarity why the entire scholastic grades of [RJC] in UP Cebu be [sic] relevant and necessary in his Counter-Affidavit[.]<sup>25</sup>

Aside from this, he claimed that it was “clearly an attempt to demean, discredit and embarrass [RJC] in the attempt to refute the latter’s assertion that he has a ‘pretty solid background in Computer Science’.”<sup>26</sup>

Lastly, RJC argued that he is entitled to moral, exemplary, and nominal damages considering DL’s violation of the DPA.<sup>27</sup>

In his Memorandum, DL, argued that he did not violate the DPA and claimed that the submission of RJC’s transcript of records to the Office of the Ombudsman was in accordance with Section 13 (f) of the DPA.<sup>28</sup> DL alleged that:

11. [RJC] in the above-said complaint before the Office of the Ombudsman built his legal claims on the basis of his own supposed solid academic background, contrasting this with the therein respondents’ alleged incompetence and negligence, and blaming the latter for his supposed ignorance of the school’s Maximum Residency Rule (MRR).

12. Thus, the natural and legal recourse for the respondents in the said complaint before the Ombudsman, including [DL], was to controvert [RJC’s] unfounded claims by documentary evidence on record. Otherwise, [RJC’s] sole, uncontroverted averments could lead to the erroneous conclusion that respondents in said Ombudsman case abused their authority and committed grave misconduct in allegedly delaying the graduation of [RJC].<sup>29</sup>

DL claimed that his purpose in attaching RJC’s transcript of records to his counter-affidavit was to controvert RJC’s “false material claims.”<sup>30</sup>DL further argued that:

25. Attaching as evidence during the Ombudsman administrative and criminal proceedings a copy of the student’s scholastic record comprises a different context as compared to releasing such record to any third party or publicizing it in a social media platform or website. The former is necessary and proportional to the exercise or defense of legal claims, while the latter is unnecessary and disproportional for any purpose.<sup>31</sup>

Considering that he had a lawful basis for processing RJC’s transcript of records, DL asserted that the complaint should be dismissed for lack of merit.<sup>32</sup>

24 *Id.* at 12.

25 *Id.* at 14.

26 Memorandum, 04 August 2022, at 17, in RJC v. DL, NPC 22-012 (NPC 2022).

27 *Id.* at 18-20.

28 *Id.* at 3.

29 *Id.* at 5-6.

30 *Id.* at 7-8.

31 *Id.* at 8.

32 Memorandum for Respondent, 04 August 2022, at 10, in RJC v. DL, NPC 22-012 (NPC 2022).

## Issue

Whether DL's processing of RJC's personal data violated the DPA.

## Discussion

DL did not violate the DPA when he processed RJC's personal data. The use of RJC's transcript of records in DL's counteraffidavit was lawful in accordance with Section 13 (f) of the DPA.

RJC correctly argued that school records are sensitive personal information. Section 3 (l) of the DPA provides an enumeration of what constitutes sensitive personal information:

Section 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

...

- (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.<sup>33</sup>

The DPA considers information about an individual's education as sensitive personal information. In a previous case, the Commission stated that educational records are considered sensitive personal information.<sup>34</sup> The Commission, however, emphasizes that not all information related to education should automatically be considered as sensitive personal information.

The enumeration provided in Section 3 (l) of the DPA includes information from which an individual can be personally identified. Such interpretation of Section 3 (l) should be observed in determining what particular information about an individual's education is deemed as sensitive personal information. Following the rules of statutory construction:

[U]nder 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

<sup>33</sup> 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 § 13 (l) (2012). Emphasis supplied.

<sup>34</sup> *MHH v. VCF and SFPS*, NPC 18-141, 09 June 2020, at 7 available at <https://www.privacy.gov.ph/wp-content/uploads/2022/01/Decision-NPC-Case-No.-18-141MHH-v.-VCF-SFPS-1.pdf> (last accessed 23 December 2022).

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.<sup>35</sup>

In construing Section (3) (l) of the DPA as a whole and considering the company of words in this Section, the information enumerated, which includes “education”, may be used to profile an individual. Thus, to harmonize and give effect to the provision as a whole, only information about education which can profile a particular individual falls within the definition of sensitive personal information.

Granular or detailed information relating to the education of an individual can be used to profile that particular individual. For instance, transcript of records containing a comprehensive breakdown of a student’s grades and other definitive administrative information, such as a student identification number, can be used to personally identify the student.

In the case at bar, RJC’s transcript of records contained the breakdown of the grades he obtained for each course he took. These particular grades are considered sensitive personal information considering that these information can profile RJC. Given that these are sensitive personal information, the processing in relation to them should be in accordance with Section 13 of the DPA.

DL alleged that his purpose in using RJC’s transcript of records in his counter-affidavit was to disprove RJC’s “false material claims.”<sup>36</sup>Such purpose may be deemed for the “establishment, exercise or defense of legal claims” under Section 13 (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:

(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.<sup>37</sup>

When determining whether there is lawful processing under Section 13 (f) of the DPA, the Commission clarifies that it cannot rule on the admissibility of evidence or its probative value to a particular case outside its jurisdiction. As previously discussed by the Commission:

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

<sup>35</sup> Francisco Chavez v. Judicial and Bar Council, Sen. Francis Escudero, and Rep. Niel Tupas, Jr., G.R. No. 202242 (2012).

<sup>36</sup> Memorandum for Respondent, 04 August 2022, at 7-8, in RJC v. DL, NPC 22-012 (NPC 2022).

<sup>37</sup> Data Privacy Act of 2012, § 13 (f). Emphasis supplied.

legal claims' consistent with the general principles of legitimate purpose and proportionality.<sup>38</sup>

In this case, however, it is the Complainant, RJC, who raised his academic records as an issue in the Ombudsman case. The Commission stresses that DL would not have to present RJC's transcript of records if it were not for RJC's presentation of the issue on his academic records. Thus, it was RJC who opened the door for the submission of these types of evidence.

Given that the processing of RJC's personal data had lawful basis under Section 13 (f) of the DPA, DL cannot be held liable for violating the DPA.

**WHEREFORE**, premises considered, the Commission resolves that the Complaint filed by RJC against DL is hereby **DISMISSED** for lack of merit.

This is without prejudice to the filing of appropriate civil, criminal, or administrative cases before any other forum or tribunal, if any.

**SO ORDERED.**

City of Pasay, Philippines.  
10 November 2022.

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRE**  
Deputy Privacy Commissioner

I CONCUR:

**Sgd.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

Copy furnished:

**RJC**  
Complainant

**DL**  
Respondent

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

<sup>38</sup> EA and TA v. EJ, EE, and HC, NPC 17-018, 15 July 2019, at 8, available at <https://www.privacy.gov.ph/wp-content/uploads/2022/04/NPC-17-018-EA-and-TA-v-EJDecision-2019.07.15-.pdf> (last accessed 01 December 2022).

JBA

Complainant,

NPC 20-026

For: Violation of the  
Data Privacy Act of  
2012

-versus-

FNT and NNT,

Respondent.

X-----X

### DECISION

#### AGUIRRE, D.P.C.;

Before this Commission is a complaint filed by JBA against FNT and NNT for an alleged violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

#### Facts

In her Complaints-Assisted Form (CAF) dated 20 January 2020, JBA claimed that FNT and NNT committed identity theft “by using [her] name in different website[s] with their pictures and contact number[s].”<sup>1</sup> Further, JBA stressed that FNT and NNT’s act affected her profession as a Real Estate Broker and that as of the date she filed the complaint, the websites using her name were still active.<sup>2</sup> As evidence, JBA attached to her CAF various screenshots of website advertisements (ads) containing her name.<sup>3</sup>

According to JBA, she was a real estate sales person for FNT and NNT from 2014 to 2017.<sup>4</sup> She only submitted her official resignation, on 30 October 2018.<sup>5</sup> On the same date, FNT received and signed the resignation letter.<sup>6</sup> The resignation letter stated:

I hereby tender my irrevocable resignation as a Sales Persons of Homeplus Realty effective today, October 30, 2018.

And hoping that my remaining commissions from my previous sales will be release [sic] as soon as it is available **and all the dummy account [sic] you created in my name will be remove [sic] in [sic] Facebook, [LinkedIn] [and] any website and other online services.**<sup>7</sup>

On 07 December 2020, an Order to Confer for Discovery was issued to the parties.<sup>8</sup> On 02 September 2021, an Order was issued instructing FNT and NNT to file their respective verified comments within fifteen (15) days from receipt of the Order.<sup>9</sup> Further, the parties were invited to virtually attend the preliminary conference scheduled on 11 No-

1 Complaints-Assisted Form, 20 January 2020, at 3, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).  
2 *Id.* at 5.  
3 *Id.* at 13-120.  
4 *Id.* at 5.  
5 *Id.*  
6 *Id.* at 11.  
7 Complaints-Assisted Form, 20 January 2020, at 11, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022). Emphasis supplied.  
8 Order to Confer for Discovery, 07 December 2020, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).  
9 Order (To File Verified Comment and Appear Virtually for Preliminary Conference), 02 September 2021, at 1, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

vember 2021 and 09 December 2021.<sup>10</sup>

Both parties failed to appear for the 11 November 2021 Preliminary Conference.<sup>11</sup> As such, an Order was issued resetting the preliminary conference to the second schedule on 09 December 2021.<sup>12</sup>

On 09 December 2021, JBA and FNT were present, but NNT failed to appear for the second time.<sup>13</sup> During the preliminary conference, FNT manifested that her sister, NNT, should be excluded from the complaint since she is not the head broker.<sup>14</sup> Thereafter, the parties were instructed to virtually appear for the third setting of the preliminary conference on 28 January 2022.<sup>15</sup> FNT and NNT were ordered to submit their verified comments within fifteen (15) days from receipt of the Order.<sup>16</sup>

In her email dated 13 December 2021, NNT explained that she has only received the forwarded email from her sister, FNT, on 13 December 2021.<sup>17</sup> Further, she claimed the following:

I am not aware of this complaint until now from Ms[.] JBA, since as mentioned by my sister, I have no direct authority over Ms[.] JBA when she was an accredited agent with my sister. Yes, I am a [sic] also an Agent/Seller & Real Estate Broker at the same time by my sister but I have no authority over her direct recruits or agents. Ms[.] JBA is a direct recruit of Ms. FNT. My involvement with Ms[.] FNT's direct agents/recruits before was merely to conduct classroom and onsite trainings/orientation and provide the best practices within the real estate industry. Any issues or problems encountered by my sister's direct agents/recruits is under her full authority. I also have no personal involvement as to her complaint on identity theft or hacking into her social media or any online account. As far as I know she was an accredited agent and with mutual consent to be under the online marketing programs that was employed to agents/sellers to HELP THEM GENERATE SALES LEAD AND CONVERT THIS TO COMMISSIONABLE INCOME. As for the hacking complaint, I will not further comment on this since she has NO VALID EVIDENCE presented to point to us as the perpetrator. [...] Lastly, to get me involved since I was on a posted picture is preposterous since I am not even aware of such online site or account being created.<sup>18</sup>

On 15 December 2021, an Order was issued noting the email manifestation of NNT and ordering that it be treated as her Comment to the complaint.<sup>19</sup>

On 23 December 2021, FNT submitted her Verified Comment.<sup>20</sup> She reiterated that her sister NNT is not involved in the dispute:

My sister Miss NNT now may [sic] Co-Broker, has no direct participation of creating

---

10 *Id.*  
11 Order (After the 1st Preliminary Conference held on 11 November 2021), 11 November 2021, at 1, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).  
12 *Id.*  
13 Order (After the 2nd Preliminary Conference held on 09 December 2021, to Submit Email Address and Verified Comment, and to Appear for the 3rd Setting of the Preliminary Conference), 09 December 2021, at 1, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).  
14 *Id.*  
15 *Id.* at 2.  
16 *Id.*  
17 Email from NNT, to NPC CID Hearings (13 December 2021).  
18 *Id.*  
19 Order (Noting the Manifestation of the Respondent NNT and Treating such Manifestation as Respondent NNT's Comment), 15 December 2021, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).  
20 Verified Comment of FNT, 23 December 2021, at 1, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).

any Secondary Facebook Accounts; Multiple Posting of Ads and running Pay-Ads in any of our Facebook Page and other Websites. Ginagamit ang SECONDARY FACEBOOK ACCOUNT ng kapatid for AUTOPOSTING, PAY-ADS at ipapaliwanag ko ito. I will take the responsibility on this, on her behalf.<sup>21</sup>

FNT explained that the term “online marketing” is intentionally indicated in her recruitment ads for “online marketing real estate agent[s]” and similar positions so that the applicant would know that the selling of real estate and the finding of potential buyers will be through the internet and various social media platforms (e.g., Facebook, Lamudi, and Property24).<sup>22</sup> Thus, online marketing ads are the medium used for her real estate ads placement.<sup>23</sup> FNT claimed that her agents knew that real estate websites are used to post the ads.<sup>24</sup>

FNT gave an overview of her recruitment process:

Ang proseso ng Recruitment ko para sa gustong mag-Ahente, kapag nakapirma na ng Seller Accreditation at naka-ATTEND ng Basic Orientation on Real Estate Selling, ang kasunod ay ang pagtuturo ng ONLINE MARKETING gamit ang Facebook, at pagpost sa My Property, Property 24 at OLX na dating Sulit.com at iba pang kilalang Real Estate E-Commerce website. Ako ang nagka-conduct ng Orientation for newly recruits. At Staff ko naman po ang nagtuturo o Hands-On Tutorial sa pag create ng Facebook Page o tinawatawag na Business Page, Multiple Posting Ads sa mga iba’t ibang Group Page ng Facebook and creating Account and Posting Ads sa mga Real Estate Websites or E- Commerce.<sup>25</sup>

...

After ng Basic Real Estate Orientation, gagawa ng Secondary Facebook Account ang mga Agent sa tulong ng Staff ko. Gumagawa din ng Real Estate Facebook Page, depende sa Ahente kung nais nito may sariling Real Estate Facebook Page. Ang pag-create ng Secondary Facebook Account at Facebook Page ay trabaho ng staff ko, kasama ang pagtuturo paano magLay-out or Edit na mga picture ng bahay at magposts sa mga Group Page o tinatawag na Multiple Posting.

Kailan meron Customized EMAIL Address for Real Estate ang Ahente, dahil gagamitin ito para sa pagsend ng UPDATED INVENTORIES, Pricelists, Project Details, PowerPoint Presentation ng House and Lot, Maps, Photos, Videos etc. Inaannounce ko sa group chat kapag hinihingi ng Lead Broker o Marketing Arm o Broker Coordinator ang mga email address ng mga ACCREDITED AGENT. Kung sino lang nagpasa ng email address sila lang ang makakatanggap ng updates. Karamihan sa mga Lead Broker at Developer nakaMASSIVE SENT ng email.<sup>26</sup>

On an agent’s first day of accreditation, it is already explained to the agent that an effective way to find buyers is through Facebook and real estate websites since these are free and easy to use—all that is necessary is it to create an account and register.<sup>27</sup>

Particularly for Facebook, FNT explained the process for creating the agent’s Facebook account:

---

21 Verified Comment of FNT, 23 December 2021, at 1, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).

22 *Id.*

23 *Id.* at 2.

24 *Id.* at 5.

25 *Id.* at 2.

26 *Id.* at 5. Emphasis supplied.

27 Verified Comment of FNT, 23 December 2021, at 12, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).



1) Una, gagawa ng Secondary Facebook Account ang mga Ahente, gagamitin lamang ito sa Real Estate Selling. Nererequire ko na ang Secondary Facebook Account para hindi gamitin ang Primary Account dahil may posibilidad na maBLOCK or iSuspend ang Facebook ang Personal or Primary Account kapag gagamitin sa Multiple Posting ng Ads.

2) Pangalawa, tutulongan ng staff ko ang Ahente sa pag-create ng Facebook Page or tinawag ngayon Business Page para din sa Real Estate. Ito ang Shop or Website ng Ahente sa Facebook. Maaaring gamiting ang Facebook Page sa pagpost ang mga Ads at ishare sa iba't ibang Group Pages. Dito sa Facebook Page ina-upload ang mga pictures ng bahay na gustong ibenta ng Ahente. Gagawa ng ALBUM bawat House Model. Kapag Staff ko ang nagcreate ng Facebook Page may abiso sa Ahente na ipopost ang Contact Number nya dahil direct syang tatawagan if may prospect buyers. After po magawa ng Facebook Page, ay i-Turn-Over na ito sa Ahente, i-aadd ang Ahente as Admin sa Page para sya ay may access at full control. Ahente na ang nag-uupload ng mga photos at nag-eencode ng details.

3) Pangatlo, tuturuan ang Ahente kung paano ang pag-join sa mga Group Pages, at paano magpost ng ADS gamit ang Multi-Posting. Tuturuan ng Multiple Posting upang mabilis ang pagposts ng Ads sa iba't ibang grupo.

4) Pang-apat, Editing o Layout ng mga Main Photos na may pangalan at phone number ng Ahente. May pahintulot sa Ahente, ini-inform namin na ilalagay ang contact number nya at direct syang tatawagan ng prospect buyers.

5) Kapag may oras pa, tutulongan ng staff ko ang ahente gumawa ng account sa Sulit.com; Ayos Dito; My Property gamit ang kanyang pangalan at phone number. Siya lang ang nakakaalam ng password at username, wala kaming access dito. Kapag sa Lamudi Ads ay account ko ang ginagamit, at ang mga Selected Agents or Assigned Agents ang nagpopost ng Ads. Kapag ito ay Premium or may bayad, binibigay ko ang password sa Ahente para pwede sya magpost ng sarili nyang Ads na may Contact Number niya. Siya rin ang sasagot ng Inquiries base sa naipost nyang ADS. Kapag nagrequest ang Ahente na gawan sya ng Account halimbawa sa Ayos Dito, ginagawa ito ng Staff ko at iturn—over sa Ahente ang AyosDito account ibibigay ang username at password.<sup>28</sup>

Further, FNT stressed that:

Kapag created ng staff ko, gagawa sya ng 'Customized Email Address['] or BUSINESS email example [ ]. [...] Ibinibigay ng staff ko ang USERNAME at Password sa Ahente. Pero kapag gawa ng Ahente ang Secondary Facebook Account, wala kaming access dito. Hindi hinihingi ng Staff ko or ako ang Password ng Ahente. Maliban nalang kung ibibigay ng Ahente sa staff ko ang username at password at magpapatulong sa posting ng Ads<sup>29</sup>

She also mentioned in her Verified Comment that, for the Sheryna.ph listing, there was a "[m]onthly [a]uto [r]enew of post, up to December 2018."<sup>30</sup>

As for the cellphone numbers used in some of the posted ads, FNT admitted that the [ ] and [ ] numbers were previous office contact numbers and were assigned to accounts of agents.<sup>31</sup>If there were inquiries made through these contact numbers, then the inqui

28 *Id.* at 12-16.

29 *Id.* at 18.

30 *Id.* at 82.

31 *Id.* at 65.

ries were passed on to the agent.<sup>32</sup>

As to the usage of FNT's photograph, she argued that this is due to human error:

Ang pag-create ng account sa iba't ibang website ay nakaassign ang task na ito sa Staff ko, ganun din ang manual Posting of Ads assigned sa kanya. Masasabi kong HUMAN ERROR o hindi sinasadyang pagkakamali ng staff ko na nag-create ng mga account at ADS, at ginagamit ang picture ko. Apat ang nakita ko sa Google, not a LARGE NUMBER. More than 100 Real Estate Website na pwedeng maAds ang mga Ahente dito sa Pilipinas.<sup>33</sup>

Human Error from my Staff o pagkakamali na walang intention, bakit picture ko ang inilagay. Ang instruction ko sa Staff, create ng account sa iba't ibang website na gamit pangalan ko profile picture at email address ko at contact number dito office kapag nagregister. Sa post ilalagay ang contact number agent at pangalan para sila na direct na kakausapin ng prospect buyer.<sup>34</sup>

...

Last December 2021 nalaman na may mga account ginawa para sa agent na picture ko ang nakalagay. Wala akong full knowledge, created ito ng Staff ko at wala po akong alam na nilagay picture ko sa Profile at pangalan sa Ahente.<sup>35</sup>

Regarding the deletion or deactivation of accounts, FNT reasoned that she is not aware of all the website accounts created by her staff, stating that, “[a]ng dami ng deleted posts, at deactivated account at website na deactivated na rin. Exhausted na kame dahil dati pa dini-delete ang mga posts. Hindi ko kabisado ang mga website kung saan nagregister at nagcreate ang staff ko.”<sup>36</sup>She further stressed that she cannot verify these information since her staff has passed away.<sup>37</sup>She also reasoned that she has no back-up files of the broken computer hard-drive her staff previously used.<sup>38</sup> She claimed: “[w]ala akong alam sa mga Username at Password na ginagamit ng Staff ko para makalog-in[.]”<sup>39</sup>

In her Verified Comment, FNT mentioned that the Facebook account created for JBA has been deactivated<sup>40</sup> and that some websites were already inactive.<sup>41</sup> She demonstrated that some websites, however, do not have a deactivation or delete account option.<sup>42</sup>

FNT emphasized that the accounts were created with JBA's consent, stating that “[g] inawa po ang mga account during the time accredited po kayo sa amin. At aware po kayo sa PAY-ADS PROGRAM or POSTING ADS sa iba't ibang website. Nakita nyo noon ang mga OJT kung paano sila magposts ng Ads sa Sulit.com at Aayos Dito.”<sup>43</sup>

In any case, FNT attempted to delete and deactivate the posts and ads.<sup>44</sup>She explained that there are some websites, like Sheryna.ph, however, that cannot be accessed and

---

32 *Id.*  
33 Verified Comment of FNT, 23 December 2021, at 83, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).  
34 *Id.* at 142.  
35 *Id.*  
36 *Id.* at 85.  
37 *Id.*  
38 *Id.* at 97.  
39 Verified Comment of FNT, 23 December 2021, at 97, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).  
40 *Id.* at 86.  
41 *Id.* at 88-90.  
42 *Id.* at 87, 91,93.  
43 *Id.* at 112.  
44 *Id.* at 137-139.

deleted because it was created by her staff and she claimed that she does not know the corresponding username.<sup>45</sup> Further, these details cannot be verified with her staff who has passed away: “[h]indi ko na rin makausap ang staff ko na nakikipag-Coordinate sa mga Ahente dahil namayapa na ito after 2 years na nakalipas nag-Resign sya sa akin bilang staff. She resigned End Quarter of 2016 and passed-away 2018.”<sup>46</sup>

Ultimately, FNT argued that she obtained JBA’s consent for the ads support scheme: Ang Tatlong (3) na taon na pag-Ahente accredited to me, is a way saying ‘approved’ o ‘with consent’ na nagjoin ka ng Online Marketing o Pay-Ads Program. Wala po kayong pagtututol sa Three (3) years na Online Marketing o Pay-Ads Program na aavail nyo.<sup>47</sup>

On 24 December 2021, an Order was issued noting the Verified Comment of FNT and instructing that it be furnished to JBA.<sup>48</sup>

On 28 January 2022, both JBA and FNT attended the Preliminary Conference.<sup>49</sup> For the discovery proceedings, JBA required a death certificate of FNT’s staff who posted the ads.<sup>50</sup> It was pointed out, however, that only certain individuals can request for death certificates pursuant to the Philippine Statistics Authority rules.<sup>51</sup>

Instead, FNT and NNT were ordered to submit an affidavit from their agent that their staff in fact, died two (2) years ago.<sup>52</sup>

FNT and JBA submitted their Application for Mediation dated 31 January 2022 and 01 February 2022, respectively.<sup>53</sup>

On 09 February 2022, JBA filed her Response to FNT’s Verified Comment.<sup>54</sup> She attached more screenshots demonstrating that, on January to February 2022, posted ads still existed containing her name.<sup>55</sup> Further, she stressed that she was never informed that the cellphone numbers posted on the ads were assigned to her as an agent.<sup>56</sup> Rather, she alleged that FNT and NNT have full control of the numbers.<sup>57</sup> Regarding FNT’s argument that she cannot delete or deactivate some accounts due to her staff’s passing, JBA pointed out that there must have been some sort of turn-over policy before the staff left.<sup>58</sup> Lastly, she stressed that she was not informed of the posted ads for some of the websites:

---

45 Verified Comment of FNT, 23 December 2021, at 139, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).

46 *Id.* at 142.

47 *Id.* at 144.

48 Order (Noting the Submission of Comment of Respondent FNT), 24 December 2021, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

49 Order (After the 3rd Preliminary Conference held on 28 January 2022, Submission of Documents from the Parties, and to Submit a Filled-Out Application for Mediation Form), 28 January 2022, at 1, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

50 *Id.*

51 Order (After the 3rd Preliminary Conference held on 28 January 2022, Submission of Documents from the Parties, and to Submit a Filled-Out Application for Mediation Form), 28 January 2022, at 1, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

52 *Id.*

53 Application for Mediation, 31 January 2022, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022); Application for Mediation, 01 February 2022, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

54 Response to FNT’s Verified Comment, 09 February 2022, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

55 *Id.* at 1-19.

56 *Id.* at 22.

57 *Id.*

58 *Id.*

Hindi nyo rin po ako ininform na meron kayong ginawang websites ng Property findersph.com, Chitku, Sheryna.ph, Cebu classified.com, Terraconnector.com, Pinoy Professionals, VigattinTrade.com, Piliko.com, BigBenta, Piyesta.com, Hanapbahay.com at adpost.com para sa pangalan ko gamit ang inyong larawan, Contact Nos. at gmail na [ ] na kayo ang may gawa. Wala din po kayong binigay na password sa mga Websites na nabanggit ko.<sup>59</sup>

JBA similarly filed a Response to NNT's Comment. She attached various check vouchers containing NNT's signature and checks issued from joint accounts of which NNT was a joint holder to demonstrate that her commissions were received from NNT.<sup>60</sup> She emphasized that FNT instructed that sales be entered in NNT's name, and that at around November 2016, FNT told them to report to NNT.<sup>61</sup> In addition, she alleged that NNT also assisted in answering queries in the group chat.<sup>62</sup>

On 24 February 2022, FNT submitted the Affidavit of Ms. LGM dated 23 February 2022 attesting that she informed FNT of the demise of her staff, Ms. MSA, in 2021:

That in year 2021, I informed MISS FNT, that her former staff MISS MSA passed away due to Cardiac Arrest.

That, I personally know MISS MSA, and also known to me that she worked as Accredited Agent and Staff of MISS FNT.<sup>63</sup>

FNT also submitted a letter dated 24 February 2022 explaining the status of some of the posted ads:

Ang iba posts hindi na naming ma-retrieve. Hundreds ang mga posts sa facebook at iba't ibang WEBSITE sa lahat ng Agents. MASSIVE POSTING NG ADS lahat na sumang-ayon sa ONLINE MARKETING PROGRAM. Dahil sa dami, hindi ko binubuksan yan iniisa isa iopen para icheck kung may inquiries. Madalas wala sa opisina, ang dami ng Screenshot na sinasabi ng staff wala dito si Mam FNT. Any important transaction, details o request, minimessage sa akin staff o sinusulat sa papel para balikan ko ang Ahente o Buyer kung may katanungan kung hindi nila masugatan. Ganun din kapag may ginagawa tasks, nagmemessage ang Staff, sinasabi mam tapos na po, mam ito hindi pa po nagawa tatapos bukas. After ng training, kahit mga dinadala dito na mga Recruit ng complainant, ang naka-assign training ng mga postings ay staff ko at yun din ng nagtuturo paano ang Multiple posting ng Ads.<sup>64</sup>

Sa mga posts ng Ads, ganun din Staff, hindi binubuksan araw araw, dahil hindi araw araw yan lang ang gagawin na Staff magpost ng mga Ads. Isang beses lang magposts, at hindi na binabalikan dahil ang ibang posting naka AUTO RENEW, ibig sabihin, after 30days kapag na-expire may auto renewal posts either 3 months, 6 months or 1 year. Ang maidelete na mga Ads, kapag meron access at tama ang mga password. Kapag hindi approved change ng Title ng Page, Username hindi napalitan, inactivate na ito. Kaya walang bagong postings.<sup>65</sup>

...

And also, in my COMMENTS I already presented, regarding Posting Ads, Website with my Photos still exists with the Ads, these websites are no longer Accessible

59 *Id.* at 27.

60 Response to NNT's Comments, 09 February 2022, at 1, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

61 *Id.*

62 *Id.*

63 Affidavit, 23 February 2022, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

64 FNT's Letter to NPC, 24 February 2022, at 3-4 in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

65 *Id.* at 4. Emphasis supplied.

and other ADS was deleted but posting still exists.

Kung naiintihan ang kabuan ng internet at website, sinabi ‘Google Search shows information gathered from websites across the web. Even if we remove content from Google Search, it may still exist on the web. This means someone might still find the content on the page that hosts it, through social media, on other search engines’.

As explained, there are **other posts are paid or with subscription for AUTO RE-NEWAL for a year.**<sup>66</sup>

On 20 April 2022, the Mediation Officer issued a Notice of Nonsettlement of Dispute stating that the parties were unable to reach a settlement.<sup>67</sup> On 25 April 2022, an Order was issued instructing the parties to submit their respective memoranda within fifteen (15) days from receipt of the Order, including a list of all the evidence presented by the parties and its respective purpose.<sup>68</sup>

On 08 May 2022, FNT submitted her (1) Memorandum containing a summary of her causes of action and defense and website recovery, deactivation, and deletion; (2) tabulation of the pieces of evidence; and (3) evidence demonstrating that the ads posted are for marketing only.<sup>69</sup> On 31 May, she submitted a revised Tabulation of Additional Evidence.<sup>70</sup>

JBA, on the other hand, requested an extension of time to submit her Memorandum.<sup>71</sup> In an Order dated 24 May 2022, the CID granted JBA’s request and gave her fifteen (15) calendar days from receipt of the Order to submit her Memorandum.<sup>72</sup> JBA submitted her Memorandum dated 07 June 2022 where she reiterated that her personal information was used even after her contract with FNT expired.<sup>73</sup> As a result, she prayed that damages be awarded in her favor.<sup>74</sup>

After received JBA’s Memorandum, FNT, through an email dated 14 June 2022, requested an additional fifteen (15) days “to verify other links” found in the Memorandum and “to submit another tabulation”.<sup>75</sup> On 15 June 2022, the CID issued an Order granting FNT’s request and giving her fifteen (15) calendar days from receipt of the Order to file her pleading.<sup>76</sup>

## Issues

- I. Whether NNT is liable for violating the DPA; and
- II. Whether FNT is liable for Section 25 (Unauthorized Processing of Personal or Sensitive Personal Information) of the DPA.

<sup>66</sup> *Id.* at 4. Emphasis removed. Emphasis supplied.

<sup>67</sup> Notice of Non-Settlement of Dispute, 20 April 2022, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).

<sup>68</sup> Order (for Resumption of Complaints Proceedings, Noting the Submissions of the Respondents, and Requiring the Parties to Submit their Simultaneous Memoranda), 25 April 2022, at 2-3, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

<sup>69</sup> Email from FNT, to NPC CID Hearings (08 May 2022).

<sup>70</sup> Tabulation of Additional Evidence, 31 May 2022, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

<sup>71</sup> Email from JBA, to NPC CID Hearings (23 May 2022).

<sup>72</sup> Order (Granting the Complainant’s Request for Extension of Time to File Memorandum), 24 May 2022, at 1, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

<sup>73</sup> Memorandum, 07 June 2022, at 2, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

<sup>74</sup> *Id.* at 6-7.

<sup>75</sup> Email from FNT, to NPC CID Hearings (14 June 2022).

<sup>76</sup> Order (Granting the Respondent’s Email Manifestation), 15 June 2022, at 3, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

## Discussion

### **I. NNT is not liable for violating the DPA.**

The case against NNT should be dismissed for lack of merit. The CAF filed by JBA was dated 20 January 2020.<sup>77</sup> Seeing as it was filed before 12 February 2021, which is the effectivity of NPC Circular 2021-01 or the 2021 NPC Rules of Procedure, NPC Circular 16-04 or the 2016 NPC Rules of Procedure is the applicable rule in this case.

Rule II, Section 10 of the 2016 NPC Rules of Procedure states the following:

Section 10. **Form and Contents of the Complaint.**

...

The **complaint shall include a brief narration of the material facts and supporting documentary and testimonial evidence, all of which show:** (a) the violation of the Data Privacy Act or related issuances; or (b) **the acts or omissions allegedly committed by the respondent amounting to a privacy violation or personal data breach.**<sup>78</sup>

In administrative cases, it is the complainant that must prove her allegations with substantial evidence:

In administrative proceedings, such as this case, it is the complainant who carries the burden of proving her allegations in the complaint with substantial evidence or such ‘relevant evidence that a reasonable mind might accept as adequate to support a conclusion.’

...

Thus, it is the party who alleges a fact that has the burden of proving it. Allegations alone do not constitute evidence since ‘self-serving assertion[s] cannot be given credence.’

...

Ultimately, it is [the complainant] that bears the burden of proving the allegations in her Complaint with substantial evidence. Jurisprudence is settled that if she ‘fail[s] to show in a satisfactory manner the facts upon which [her] claims are based, the [respondent is] **not obliged** to prove [its] exception or defense.’<sup>79</sup>

In this case, JBA was not able to sufficiently demonstrate with any substantial evidence that NNT committed acts or omissions that amounted to a violation of the DPA.

In her CAF, JBA impleaded NNT as a respondent, along with FNT, and claimed that they committed identity theft “by using [her] name in different website[s] with their pictures and contact number[s].”<sup>80</sup> To demonstrate NNT’s involvement in the alleged identity theft, JBA also submitted to the Commission various check vouchers containing NNT’s

<sup>77</sup> Complaints-Assisted Form, 20 January 2020, at 5, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

<sup>78</sup> National Privacy Commission, 2016 Rules of Procedure of the National Privacy Commission [NPC 2016 Rules of Procedure], rule II, § 10 (15 December 2016). Emphasis supplied.

<sup>79</sup> NPC 19-465, 03 March 2022, at 7, 10 (NPC 2022) (unreported).

<sup>80</sup> Complaints-Assisted Form, 20 January 2020, at 3, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

signature and checks issued from joint accounts of which NNT was a joint holder.<sup>81</sup> She argued that these showed that her commissions were received from NNT.<sup>82</sup> Further, she alleged that FNT instructed that the sales be entered in NNT's name.<sup>83</sup> Upon further scrutiny of the various checks and check vouchers submitted, the Commission finds that these are not enough to substantially demonstrate NNT's involvement in any privacy violation, particularly, the posting of ads containing JBA's personal information even after her withdrawal of consent.

The check vouchers contained NNT's signature under the portion indicating "Approved By:."<sup>84</sup> As for the checks addressed to JBA, they were issued from the following joint accounts: (1) NNT or CMN; or (2) NNT and/or FNT.<sup>85</sup> Contrary to JBA's claims, these various checks and check vouchers merely demonstrate that NNT is an account holder of the checks issued and that she is involved in the organization's finances. These checks and check vouchers, however, do not show that NNT committed any act or omission in violation of the DPA. Thus, NNT cannot be said to have violated the DPA solely on the basis that she is a signatory and account holder of "commission" checks received by JBA.

Further, NNT maintained that she had no direct authority over JBA since JBA is a direct recruit or agent of her sister FNT.<sup>86</sup> With this, FNT herself manifested in her Verified Comment that NNT "has no direct participation of creating any Secondary Facebook Accounts; Multiple Posting of Ads and running Pay-Ads in any of our Facebook Page and other Websites."<sup>87</sup>

Given that JBA was not able to discharge the necessary burden of proof, the case against NNT should be dismissed for lack of merit.

## **II. FNT is liable for Section 25 (Unauthorized Processing of Personal or Sensitive Personal Information) of the DPA.**

FNT violated Section 25 of the DPA, or Unauthorized Processing of Personal or Sensitive Personal Information, when she continued to post ads containing JBA's personal information even after JBA's withdrawal of consent.

Unauthorized Processing of Personal or Sensitive Personal Information is committed when:

1. The perpetrator processed the information of the data subject;
2. The information processed was personal information or sensitive personal information; and
3. The processing was done without the consent of the data subject, or without being authorized under the DPA or any existing law.<sup>88</sup>

All three (3) requisites are present.

---

81 Response to NNT's Comments, 09 February 2022, at 1-3, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

82 *Id.* at 1.

83 *Id.*

84 *Id.*

85 *Id.* at 1, 3.

86 Email from NNT, to NPC CID Hearings (13 December 2021).

87 Verified Comment of FNT, 23 December 2021, at 1, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).

88 NPC 19-134, 10 December 2021, at 12 (NPC 2021) (unreported).

On the first requisite, FNT processed the information of her data subject, JBA. Section 3 of the DPA defines processing as follows:

Section 3. Definition of Terms.

...

(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.<sup>89</sup>

As mentioned by FNT in her Verified Comment, her staff assisted her agents in posting ads on multiple platforms such as “My Property, Property 24 at OLX na dating Sulit.com at iba pang kilalang Real Estate E-Commerce website.”<sup>90</sup> Thus, FNT processed JBA’s personal information through her staff, who used JBA’s name in the posted online marketing ads.<sup>91</sup>

As for the second requisite, the information that FNT processed is personal information. Section 3 of the DPA defines personal information:

Section 3. Definition of Terms.

...

(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.<sup>92</sup>

As previously held by the Commission, a name is personal information:

The names stated in the affidavit can reasonably and directly ascertain the identities of the individuals involved in the incidents. The names, therefore, are considered personal information, the processing of which must be in accordance with the DPA.<sup>93</sup>

The various screenshots JBA submitted to the Commission show that her name, “JBA” is displayed on the posted ad listings.<sup>94</sup> Thus, FNT processed JBA’s personal information.

The third requisite is similarly present. FNT’s posting of ads were done without JBA’s consent nor were they authorized under the DPA or any existing laws.

---

89 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 (j) (2012). Emphasis supplied.

90 Verified Comment of FNT, 23 December 2021, at 2, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).

91 See Complaints-Assisted Form, 20 January 2020, at 25-120, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

92 Data Privacy Act of 2012, § 3 (g)

93 NPC 21-031, 03 March 2022, at 9 (NPC 2022) (unreported).

94 Complaints-Assisted Form, 20 January 2020, at 25-120, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).



To recall, JBA submitted her official resignation letter on 30 October 2018.<sup>95</sup> She withdrew her consent and explicitly exercised her right to erasure when she stated that she hoped “all the dummy account [sic] you created in my name will be remove [sic] in [sic] Facebook, [LinkedIn] [and] any website and other online services.”<sup>96</sup>

JBA submitted multiple screenshots of ads posted prior to her official resignation.<sup>97</sup> These were posted with JBA’s consent, seeing as she was still a sales agent at the time.

JBA, however, also presented screenshots of websites demonstrating that ads were posted on Sheryna.ph containing her personal information even after her resignation on 30 October 2018:

1. Imus Gen Trias Cavite 3BR 2T&B Catherine (Ad ID: 408339) – posted on 23 November 2018;<sup>98</sup>
2. Gabrielle Imus Gen Trias Cavite 3BR 2T&B (Ad ID: 408330)– posted on 27 December 2018;<sup>99</sup>
3. Imus Gen Trias Cavite 3BR 2T&B Catherine (Ad ID: 408339) – posted on 29 November 2021;<sup>100</sup> and
4. Imus Gen Trias Cavite 4BR 3T&B Alexandra (Ad ID: 408326) – posted on 08 February 2021.<sup>101</sup>

The dates of these particular ad listings show that they were posted after JBA’s resignation dated 30 October 2018. To recall, JBA’s resignation letter explicitly contained her withdrawal of consent and request for the exercise of her right to erasure.<sup>102</sup> Thus, since these ads were posted after JBA’s resignation, FNT’s processing of JBA’s personal information on these particular ads was done without her consent or authority under the DPA or any existing law.

Section 16 of the DPA specifically provides for a data subject’s right to erasure:

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

...

(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller’s filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information[.]<sup>103</sup>

Section 34 of the Implementing Rules and Regulations (IRR) further explains when this right may be exercised:

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

95 *Id.* at 11.

96 *Id.*

97 See Complaints-Assisted Form, 20 January 2020, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

98 Complaints-Assisted Form, 20 January 2020, at 109, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).

99 *Id.* at 111.

100 Response to FNT’s Verified Comment, 09 February 2022, at 15-16, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

101 *Id.* at 17.

102 Complaints-Assisted Form, 20 January 2020, at 11, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).

103 Data Privacy Act of 2012, § 16 (e).

rights:

...

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.<sup>104</sup>

Certain obligations are imposed upon the Personal Information Controller (PIC) in relation to the right to erasure or blocking:

Section 10. Right to Erasure or Blocking.

...

C. PICs shall **inform the recipients or third parties who have previously received such personal data of the fact of erasure.** PICs shall likewise **inform the data subject about such recipients of his or her personal data.**

D. Where personal data that is the subject of a request for erasure is publicly available, i.e. online, reasonable and appropriate measures shall be taken by the PIC to **communicate with other PICs, including third party indexes, and request them to erase copies or remove or de-list search results or links to the pertinent personal data.** In determining what is reasonable and appropriate, the available technology and the cost of implementation shall be considered.

E. Data subjects must be adequately informed of the consequences of the erasure of their personal data.<sup>105</sup>

<sup>104</sup> National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 34 (e) (2016). Emphasis supplied.

<sup>105</sup> National Privacy Commission, Data Subject Rights, Advisory No. 01, Series of 2021 [NPC Advisory No. 21-01], § 10 (C) – (E) (29 January 2021). Emphasis supplied.

The PIC, however, may deny the request for erasure or blocking, wholly or partly, when the personal data is still necessary for any of the following:

Section 10. Right to Erasure or Blocking.

...

B. PICs should judiciously evaluate requests for the exercise of the right to erasure or blocking.

...

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

a) Fulfillment of the purpose/s for which the data was obtained; b) Compliance with a legal obligation which requires personal data processing; c) Establishment, exercise, or defense of any legal claim;

d) Legitimate business purposes of the PIC, consistent with the applicable industry standard for personal data retention;

e) To apprise the public on matters that have an overriding public interest or concern, taking into consideration the following factors: i. constitutionally guaranteed rights and freedoms of speech, of expression, or of the press; ii. whether or not the personal data pertains to a data subject who is a public figure; and iii. other analogous considerations where personal data are processed in circumstances where data subjects can reasonably expect further processing.

f) As may be provided by any existing law, rules, and regulations.<sup>106</sup>

In this case, none of the circumstances that would warrant a denial of a request for erasure under Section 10 (B) (2) of NPC Advisory 21-01 (Data Subject Rights) are present. Thus, there is no reason for FNT to deny the request for erasure. As the PIC, she should have complied with the request.

FNT received and acknowledged the resignation of JBA on 30 October 2018.<sup>107</sup> After acknowledging JBA's withdrawal of consent to process her personal information and exercise of her right to erasure in her resignation letter, FNT, as the PIC, should not have processed JBA's personal information from that point onwards. Rather, she should have initiated the removal of JBA's personal information in the currently posted ads.

Further, there is no longer any reason to post ads with JBA's name after the resignation since, at that point, JBA was no longer affiliated with FNT.

The Commission also refutes FNT's argument regarding the automatic renewal of ads for the Sheryna.ph listing.<sup>108</sup> To recall, FNT explained as follows:

Isang beses lang magposts, at hindi na binabalikan dahil ang ibang posting naka AUTO RENEW, ibig sabihin, after 30days kapag na-expire may auto renewal posts either 3 months, 6 months or 1 year.<sup>109</sup>

106 *Id.* § 10 (B) (2).

107 Complaints-Assisted Form, 20 January 2020, at 11, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).

108 See Verified Comment of FNT, 23 December 2021, at 82, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022); FNT's Letter to NPC, 24 February 2022, at 4, 6, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

109 FNT's Letter to NPC, 24 February 2022, at 4, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

...

As explained, there are other posts are paid or with subscription for AUTO RENEW-AL for a year.<sup>110</sup>

Availing of automatic renewal methods, however, does not remove a PIC's obligation to ensure that personal information is properly processed and that a data subject's rights are observed. FNT, as the PIC, cannot deny accountability by stating that the posts were subject to automatic renewal. As a PIC, she should have had measures in place or taken the necessary steps after receiving JBA's resignation to ensure that she can control when the posted ads would be posted or removed. The mere act of uploading and posting ads on internet websites does not remove a PIC's liability since the PIC is expected to have control over the posted ads.

FNT similarly cannot deflect responsibility by pointing to her deceased staff member, stating that “[h]indi ko kabisado ang mga website kung saan nag-register at nagcreate ang staff ko,”<sup>111</sup> and “[w]ala na akong mapagtanungan dahil namayapa na siya.”<sup>112</sup> Therefore, “[w]ala akong alam sa mga Username at Password na ginagamit ng Staff ko para makalog-in[.]”<sup>113</sup>

According to the Affidavit of Ms. LGM, FNT was informed of the demise of her staff in 2021.<sup>114</sup> JBA, however, resigned in October 2018.<sup>115</sup> Thus, FNT could have and should have removed the posted ads starting from the date of resignation. Further, even assuming that she could no longer delete the accounts created under the name of JBA, she should have taken steps to ensure that there will be no further processing of personal information in relation to these accounts.

Instead, the records show that listings were still being posted under the name of JBA as late as February and November 2021.<sup>116</sup>

Given these, any processing made by FNT after she acknowledged JBA's resignation and exercise of her right to erasure is without consent or authority under the DPA or any existing law. Therefore, the processing of those particular ads were unauthorized and done in violation of Section 25 of the DPA.

**WHEREFORE**, premises considered, this Commission hereby:

1. **DISMISSES** the case against NNT for lack of merit; and
2. **FINDS** that FNT violated Section 25 of the Data Privacy Act of 2012 (DPA) and **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice. This Commission **RECOMMENDS** the prosecution of FNT for Unauthorized Processing of Personal or Sensitive Personal Information under Section 25 of the DPA.

---

110 *Id.* at 16.

111 Verified Comment of FNT, 23 December 2021, at 85, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).

112 *Id.*

113 *Id.* at 97.

114 Affidavit, 23 February 2022, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

115 Complaints-Assisted Form, 20 January 2020, at 11, in JBA v. FNT and NNT, NPC Case No. 20026 (NPC 2022).

116 Response to FNT's Verified Comment, 09 February 2022, at 15-17, in JBA v. FNT and NNT, NPC Case No. 20-026 (NPC 2022).

**SO ORDERED.**

City of Pasay, Philippines.  
22 September 2022.

**Sgd.**

**LEANDRO ANGELO Y. AGUIRRE**

Deputy Privacy Commissioner

I CONCUR:

**Sgd.**

**JOHN HENRY D. NAGA**

Privacy Commissioner

Copy furnished:

**JBA**

*Complainant*

**FNT and NNT**

*Respondents*

**COMPLAINTS AND INVESTIGATION DIVISION**

**ENFORCEMENT DIVISION**

**GENERAL RECORDS UNIT**

National Privacy Commission

NFM,

*Complainant,*

**NPC 19-1273**  
For: Violation of the  
Data Privacy Act of  
2012

-versus-

**BANK OF THE PHILIPPINE ISLANDS FAMILY –  
CREDIT CARD DIVISION**

*Respondent.*

X-----X

### DECISION

**AGUIRRE, D.P.C.;**

Before the Commission is a complaint filed by NFM against the Bank of the Philippine Islands Family – Credit Card Division (BPI) for an alleged violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

#### Facts

On 29 October 2018, NFM, a BPI Family MasterCard credit card holder, alleged that her credit card was used for an unauthorized transaction amounting to Eleven Thousand Seven Hundred Ninety Pesos (Php 11,790.00) on Lazada Philippines (Lazada).<sup>1</sup> She claimed that her username and password in BPI Express Online, BPI’s internet banking facility, was accessed by changing her registered mobile number without her knowledge.<sup>2</sup>The mobile number was then used in authenticating the online transaction via a One-Time Password (OTP).<sup>3</sup>

On 07 November 2018, NFM discovered the purported transaction when she checked her BPI account through its mobile application.<sup>4</sup> As a result, NFM filed a complaint with BPI through its hotline number.<sup>5</sup>

On 08 November 2018, NFM also called Lazada’s hotline and reported the incident.<sup>6</sup>She later received a reference number and the matter was referred to Lazada’s Payment Team.<sup>7</sup>

On 09 January 2019, BPI’s Fraud Control Team sent a Liability Letter, stating that NFM should still pay for the credit card transaction with Lazada amounting to Eleven Thousand Seven Hundred Ninety Pesos (Php 11, 790.00).<sup>8</sup>BPI explained that:

1 Letter from NFM to BPI, 02 January 2019, at 1, in NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2019).

2 Complaints-Assisted Form, 17 September 2019, at 3, in NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2019).

3 *Id.*

4 Complaints-Assisted Form, 17 September 2019, at 5, in NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2019).

5 *Id.*

6 Letter from NFM to BPI, 01 March 2019, at 1, in NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2019).

7 *Id.*

8 Letter from BPI to NFM, 09 January 2019, at 1, in NFM v. Bank of the Philippine Islands Family – Credit Card

[E]ach of the credit card transactions was made online and would not have gone through without the concurrence of the following:

1. Your 16-digit credit card number;
2. Your 3-digit CVC printed at the back of your credit card;
3. The expiry date of your credit card; and
4. Authentication of each transaction via a One-Time Password (OTP) that you opted sent to your registered **mobile number at the time of the transaction.**<sup>9</sup>

BPI reiterated that an OTP can be received only by one who has access to the registered mobile number.<sup>10</sup> BPI concluded that the circumstances show that the transaction was only made by NFM or by anyone to whom NFM had given her credit card details and access to her registered mobile number.<sup>11</sup>

BPI also emphasized that based on the records, the registered mobile number was amended from [ ] to [ ] through the BPI Express Online Account Maintenance Services for Credit Card.<sup>12</sup> BPI explained that a request for a change of mobile number requires the correct BPI Express Online username and password.<sup>13</sup>

On 10 January 2019, NFM wrote another letter to BPI disputing the BPI Fraud Control Team's decision.<sup>14</sup> In the letter, NFM reiterated that she had nothing to do with the transaction.<sup>15</sup> She also claimed that she neither changed her mobile number nor shared any personal information, such as her credit card details, username, and password, with anyone.<sup>16</sup>

On 01 March 2019, NFM requested BPI to provide a copy of the record of the charge slip evidencing the transaction allegedly done through Lazada using her credit card.<sup>17</sup> She also requested the following information: (1) items purchased and the amounts of each, (2) name of Merchant, (3) person who did the transaction and their respective contact numbers, (4) IP Address used, (5) date and time of the delivery of the item, and (6) the recipient of the items purchased.<sup>18</sup> NFM also requested BPI to provide a written explanation on "how BPI fulfill [its] duty to protect its customers' personal information and ensure a safer online transaction, if it allows personal information to be easily changed online through the online account and why no message in any form about the mobile update is given to the owner of the account."<sup>19</sup>

On the same day, NFM also wrote a letter addressed to Lazada asking for the same information.<sup>20</sup> In the letter, NFM provided a summary of the communications made between her and various Lazada representatives.<sup>21</sup>

---

Division, NPC 19-1273 (NPC 2019).

9 *Id.*

10 *Id.*

11 *Id.*

12 *Id.*

13 *Id.*

14 Letter from NFM to BPI, 10 January 2019, at 1, in NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2019).

15 *Id.*

16 *Id.*

17 *Id.*

18 *Id.*

19 *Id.*

20 Letter from NFM to Lazada, 02 March 2019, at 1, in NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2019)

21 *Id.*

On 17 September 2019, NFM filed a complaint against BPI.<sup>22</sup>She alleged that because of the unauthorized transaction, BPI processed her online banking username, password, mobile number, and credit card in violation of Section 25 of the DPA (Unauthorized Processing of Personal Information and Sensitive Personal Information).<sup>23</sup>

NFM prayed for the reversal of payment with interest of the unauthorized transaction and for damages, and sought an Order to stop the temporary or permanent processing of her data.<sup>24</sup>

On 24 October 2019, the National Privacy Commission (NPC), through the Complaints and Investigation Division (CID), issued an Order for the parties to confer for discovery.<sup>25</sup>

On 27 November 2019, both parties appeared for the discovery conference but failed to reach an agreement. NFM required the following documents from BPI:

1. Details of the subject transaction in the complaint;
2. Documents showing that the transaction complained of was referred to Lazada for appropriate action; and
3. Personal information of complainant recorded with respondent.<sup>26</sup>

On the same day, the CID then issued an Order directing BPI to submit the documents within ten (10) days from 27 November 2019.<sup>27</sup>It also ordered BPI within ten (10) days from the expiration of the period to submit the required documents to file its responsive comment to the complaint, together with any supporting documents the respondent may have, including affidavits of the respondent's witnesses, if any.<sup>28</sup>

The CID also gave NFM ten (10) days from receipt of the responsive comment to file her reply and BPI ten (10) days from receipt of the reply to file its rejoinder.<sup>29</sup>

On 17 December 2019, BPI filed an Urgent Motion for Extension of Time to File a Responsive Comment asking for an additional twenty (20) days from 17 December 2019 or until 06 January 2020 within which to file a responsive comment.<sup>30</sup> BPI explained that it needed to review the facts and circumstances of the case because of its heavy workload.<sup>31</sup>

On 06 January 2020, BPI filed an Urgent Second Motion for Extension of Time to File a Responsive Comment and asked for an additional ten (10) days from 06 January 2020 or until 16 January 2020 to file a responsive comment.<sup>32</sup>BPI reasoned that the holiday season and consequent non-working days prevented it from collating all the documents

---

22 Complaints-Assisted Form, 17 September 2019, at 5, in *NFM v. Bank of the Philippine Islands Family – Credit Card Division*, NPC 19-273 (NPC 2019).

23 *Id.* at 1.

24 Complaints-Assisted Form, 17 September 2019, at 6-7, in *NFM v. Bank of the Philippine Islands Family – Credit Card Division*, NPC 19-273 (NPC 2019).

25 Order to Confer for Discovery, 24 December 2019, at 1, in *NFM v. Bank of the Philippine Islands Family – Credit Card Division*, NPC 19-273 (NPC 2019).

26 Order, 27 November 2019, at 1, in *NFM v. Bank of the Philippine Islands Family – Credit Card Division*, NPC 19-1273 (NPC 2019).

27 *Id.*

28 *Id.*

29 *Id.*

30 *Urgent Motion for Extension of Time to File Responsive Comment*, 16 December 2019, at 1, in *NFM v. Bank of the Philippine Islands Family – Credit Card Division*, NPC 19-1273 (NPC 2019).

31 *Id.*

32 *Id.*



pertaining to the case.<sup>33</sup>

On 15 January 2020, BPI filed its Comment.<sup>34</sup> BPI refuted NFM's claim and explained that NFM has no cause of action against BPI under Section 25 (Unauthorized Processing of Personal Information and Sensitive Personal Information) and Section 30 (Concealment of Security Breaches Involving Sensitive Personal Information) of the DPA.<sup>35</sup> BPI explained that:

It must be noted that Complainant voluntarily and expressly authorized Respondent [BFSB] BPI to process her personal data as a credit card holder. This is specifically provided in the terms and conditions she acceded to during card application. Hence, it is peculiar that she is accusing Respondent [BFSB] BPI of processing her personal data without her consent.

...

It cannot be emphasized enough that the foregoing details, particularly the card number, CVC, and expiry date, are supposed to be known only to the cardholder. There is no way that anyone would know the same unless disclosed by the cardholder, or someone had possession of the credit card at the time of the transaction.

...

Based on the foregoing, the Complainant has the burden of proving that the transactions were unauthorized. Unfortunately, she failed to present even an iota of evidence to prove the same. The present complaint only contains self-serving allegations and mere speculations.

...

However, assuming for the sake of argument that the disputed transaction was not made by the Complainant, it is humbly submitted that she also failed to present substantial evidence to prove that the same was made possible by means of personal data breach.<sup>36</sup>

Relying on the legal doctrine of *res ipsa loquitur*, BPI asserted that:

The fact that someone was able to make the disputed transaction using personal data and log-in details known only to the Complainant is *prima facie* evidence of negligence on the [latter's] Complainant's part in securing or safeguarding her data.<sup>37</sup>

BPI also explained that the transaction was deemed properly authenticated through the OTP.<sup>38</sup> It stated that is the reason why it remitted payment to Lazada and that it could no longer reverse the disputed transaction.<sup>39</sup>

Thus, BPI prayed that the Commission dismiss the complaint outright for lack of merit.<sup>40</sup>

---

33

*Id.*

34 Comment, 15 January 2020, at 4, in *NFM v. Bank of the Philippine Islands Family – Credit Card Division*, NPC 19-1273 (NPC 2020).

35

*Id.*

36 Comment, 15 January 2020, at 5, in *NFM v. Bank of the Philippine Islands Family – Credit Card Division*, NPC 19-1273 (NPC 2020).

37

*Id.* at 7.

38

*Id.*

39

*Id.*

40

*Id.*

On 10 February 2020, NFM filed a Reply with Motion to Admit.<sup>41</sup>In her Reply, she emphasized that BPI failed to comply with the production of documents as stated in the Order dated 27 November 2019.<sup>42</sup>

NFM denied any involvement in the disputed transaction.<sup>43</sup>She stated that based on her record history, she never made a purchase in an amount higher than Ten Thousand Pesos (Php 10,000.00).<sup>44</sup>She reiterated that her mobile number was changed without her consent:

Complainant’s mobile number was changed online without her consent and there were no means of communication forwarded to the Complainant by respondent suggesting/informing her of this change. Thus, the One-Time Password (OTP), which is supposed to be a security feature, proves to be a means to make unauthorized transactions, to the prejudice of the Complainant.<sup>45</sup>

NFM maintained that she is not only disputing the unauthorized transaction in her credit card, but also the failure of BPI to secure her personal information which led to the fraudulent transaction.<sup>46</sup>

NFM also contended that BPI’s supposed failure to implement security measures and to safeguard her personal information resulted in a breach of her confidential personal information.<sup>47</sup>Further, she alleged that BPI concealed the data breach which facilitated the change of her mobile number and resulted in the successful authentication of the disputed transaction.<sup>48</sup>

BPI did not file any Rejoinder.

On 04 June 2021, the CID issued an Order reiterating the Order dated 27 November 2019.<sup>49</sup>The CID directed BPI to submit details of the transaction, documents showing that the transaction complained of was referred to Lazada for appropriate action, and NFM’s personal information recorded with BPI.<sup>50</sup>It also ordered BPI to submit additional information on the circumstances surrounding the change of NFM’s mobile number during the alleged unauthorized transaction and documentation on BPI’s security measures at the time of the incident.<sup>51</sup>

On 04 August 2022, the CID issued an Order to BPI directing it to show cause why it should not be held in contempt, and to comply with the Orders dated 27 November 2019 and 04 June 2021.<sup>52</sup>

On 17 October 2022, BPI submitted its Compliance to the Order dated 04 August

---

41 Reply with Motion to Admit, 10 February 2020, at 5, NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2020).

42 *Id.*

43 *Id.* at 3.

44 *Id.*

45 Reply with Motion to Admit, 10 February 2020, at 5, in NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2020).

46 *Id.*

47 *Id.*

48 *Id.*

49 Order, 04 June 2021, at 1, in NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2021).

50 *Id.*

51 *Id.*

52 *Id.*

2022.<sup>53</sup>BPI stated that it sufficiently complied with the information required from the 27 November 2019 Order when it submitted its Comment dated 15 January 2020.<sup>54</sup>

NFM emphasized that extraordinary diligence is required of banks since their business is imbued with public interest.<sup>55</sup>She claimed that BPI has been remiss in ensuring that its own system is fully capable of protecting the security and privacy of data of its clients.<sup>56</sup>

### Issues

Whether BPI's supposed failure to safeguard NFM's personal information constitutes a violation of the DPA.

### Discussion

The Commission dismisses the case for lack of substantial evidence. NFM did not overcome the burden of proof necessary to shift the burden of evidence to BPI.

In administrative proceedings, the quantum of proof necessary for a finding of guilt is substantial evidence.<sup>57</sup> Thus, complainants must carry the burden of proving their allegations with such relevant evidence that a reasonable mind might accept as adequate to support a conclusion.<sup>58</sup>

Section 1 of Rule 131 of the 2019 Amendments to the Revised Rules on Evidence distinguishes between burden of proof and evidence:

Section 1. Burden of proof and burden of evidence Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim or defense by the amount of evidence required by law.

Burden of proof never shifts. Burden of evidence is the duty of a party to present evidence sufficient to establish or rebut a fact in issue to establish or rebut a fact in issue to establish a prima facie case. **Burden of evidence may shift from one party to the other** in the course of the proceedings, depending on the exigencies of the case.<sup>59</sup>

Thus, it is the party who alleges a fact that has the burden of proving it.<sup>60</sup>

To prove her claim that she did not make the alleged Lazada transaction, NFM provided a record of her previous credit card transactions to show that she has never purchased an item with an amount higher than Ten Thousand Pesos (Php 10,000.00).<sup>61</sup>The disputed transaction amounts to Eleven Thousand Seven Hundred Ninety Pesos (Php 11,790.00).<sup>62</sup>

53 Compliance (re: Order dated 04 August 2022), 17 October 2022, at 1, in NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2022).

54 *Id.*

55 Reply with Motion to Admit, 10 February 2020, at 7, NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2020).

56 *Id.*

57 DOH v. Aquintey, et al., 806 Phil. 763, 772 (2017).

58 De Jesus v. Guerrero III, 614 Phil. 520, 528-529 (2009).

59 2019 AMENDMENT TO THE 1989 REVISED RULES ON EVIDENCE, A.M. NO. 19-08-15-SC, Rule 131, § 1 (1 May 2020). Emphasis supplied,

60 De Jesus v. Guerrero III, 614 Phil. 520, 528-529 (2009).

61 Reply with Motion to Admit, 10 February 2020, at 2, in NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2019).

62 *Id.*

NFM also provided a Lazada screenshot to show that she placed her latest transaction only on 03 August 2018 and that she did not make any transaction on November 2018.<sup>63</sup> Additionally, NFM sought to prove through the same screenshot that her history of purchases in Lazada nowhere exceeded Three Thousand Pesos (Php 3,000.00).<sup>64</sup>

Further, NFM concluded that the transaction was indeed fraudulent because BPI stated in its Comment that “it conducted a thorough investigation of the incident.”<sup>65</sup>NFM contended, however, that BPI actually “failed to coordinate with Lazada” in terms of the reversal of the charges incurred from the alleged transaction.<sup>66</sup>

Finally, NFM included accusations that she heard similar experiences from different people that their mobile numbers were also allegedly being changed by BPI and that their credit cards were also used for other online transactions.<sup>67</sup>NFM narrated that she, along with other credit card holders who are also alleged victims of unauthorized online transactions, went to the Bangko Sentral ng Pilipinas (BSP) and the NPC to file separate complaints.<sup>68</sup>

These assertions presented by NFM are merely speculative and cannot serve as basis to establish a fact. Other than her bare allegations that someone was able to access her online account and change her registered mobile number without her knowledge, NFM failed to provide evidence to categorically substantiate her claims that a breach occurred and BPI was responsible for such incident. She was not able to provide evidence to support her claim that BPI was at fault for the unauthorized access to her account or that BPI was negligent in allowing changes to her mobile number.

It is not sufficient for a Complainant, such as NFM, to make allegations without substantial evidence to support her claims, considering that:

The basic rule is that mere allegation is not evidence and is not equivalent to proof. Likewise, charges based on mere suspicion and speculation cannot be given credence.<sup>69</sup>

In this case, NFM did not present substantial evidence to prove that BPI’s supposed failure to implement proper security measures was the cause of the unauthorized transaction and not her own negligence. Thus, the Commission cannot find BPI liable for violating Section 25 (Unauthorized Processing of Personal Information and Sensitive Personal Information) and Section 30 (Concealment of Security Breaches Involving Sensitive Personal Information) of the DPA.

NFM’s contentions cannot give rise to the conclusion that BPI violated the DPA for its lack of security measures.

BPI averred in its Comment that there is reasonable, if not, conclusive presumption

---

63 *Id.*  
64 *Id.* at 3.  
65 *Id.*  
66 *Id.*  
67 Letter from NFM to BPI, 10 January 2019, at 2 in NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2019).  
68 Reply with Motion to Admit, 10 February 2020, at 4, in NFM v. Bank of the Philippine Islands Family – Credit Card Division, NPC 19-1273 (NPC 2020).  
69 BSA Tower Condominium Corp. v. Reyes II, A.C. No. 11944 (2018).

that NFM effected the change in her registered mobile number.<sup>70</sup>BPI explained that the request requires the correct BPI Express Online username and password which are supposed to be confidential and known only to her.<sup>71</sup>

Further, as part of its security measures at the time the incident took place, BPI implemented a multi-factor authentication method to verify online credit card transactions.<sup>72</sup>This method requires the concurrence of the following personal data conclusively presumed to be known only to the cardholder:

- a. 16-digit credit card number printed on the face of the credit card;
- b. expiry date printed on the face of the card;
- c. 3-digit CVC printed on the back of the card; and
- d. one-time password (“OTP” for brevity) sent to the cardholder’s registered mobile number.<sup>73</sup>

BPI’s verification process, using the OTP sent to NFM’s supposed registered mobile number, shows that BPI had some level of security in place during the time of the alleged online transaction.

The Commission sternly reminds Personal Information Controllers (PICs) of their continuing obligation to ensure that the personal data they process, whether offline or online, are properly protected. As such, PICs must monitor, evaluate, and update their security measures considering the developments in technology and the risks that data subjects are exposed to.

Section 20 (a) and (c) of the DPA provide the PIC’s obligation to implement measures for the protection of personal information:

*Section 20. Security of Personal Information.*

(a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

...

(c) The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:

- (1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;
- (2) A security policy with respect to the processing of personal information;
- (3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and

<sup>70</sup> Compliance (re: Order dated 04 August 2022), 17 October 2022, at 1, in *NFM v. Bank of the Philippine Islands Family – Credit Card Division*, NPC 19-1273 (NPC 2022).

<sup>71</sup> *Id.*

<sup>72</sup> *Id.* at 3.

<sup>73</sup> *Id.*

(4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.<sup>74</sup>

In this case, the security measures implemented by BPI involved sending the OTP to the account holder's registered mobile number. Considering that the two-factor authentication method it implemented was entirely dependent on the registered mobile number, it should have ensured that any changes to this number was also properly verified and authenticated to secure the integrity of the two-factor authentication. Since the process for changing the registered mobile number is not secure, data subjects are unnecessarily exposed to higher levels of risk.

Thus, this Commission finds that the award of nominal damages to NFM is warranted.

The DPA provides that restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.<sup>75</sup> Article 2221 of the New Civil Code provides:

Article 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.<sup>76</sup>

As stated, there is an obligation for a PIC to observe regular monitoring and processes intended for the protection of personal information.<sup>77</sup> An obligation implies not just a duty on the part of one party, but also denotes a correlative right on the other.<sup>78</sup> Since there is an obligation on the part of a PIC to implement measures to protect the personal information that it processes, there is also a correlative right on the part of data subjects to expect that their personal information is being protected.

Thus, as a recognition and vindication of this right, this Commission awards nominal damages to NFM in the total amount of Five Thousand Pesos (Php 5,000.00). NFM, as a data subject, has a correlative right to anticipate that BPI is safeguarding her personal information.

Although this case occurred before the effectivity of the NPC Circular 22-01 or the Guidelines on Administrative Fines, the Commission stresses that it will not hesitate to impose fines in order for PICs, such as banks, to adopt optimal levels of data protection and security in handling personal and sensitive personal information of their customers.

On NFM's prayer on the reversal of unauthorized transactions, such is beyond the jurisdiction of the Commission.

**WHEREFORE**, premises considered, the Commission **DISMISSES** the complaint filed by NFM against Bank of the Philippine Islands Family – Credit Card Division (BPI).

<sup>74</sup> An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (a), (c) (4) (2012).

<sup>75</sup> *Id.*

<sup>76</sup> An Act to Ordain and Institute the Civil Code of the Philippines [NEW CIVIL CODE], Republic Act No. 386, art. 2221 (1950).

<sup>77</sup> Data Privacy Act, § 20 (c) 4.

<sup>78</sup> *Serrano v. Court of Appeals*, 363 SCRA 223, 231 (2001)

The Commission **AWARDS** nominal damages in the amount of Five Thousand Pesos (Php 5,000.00) to NFM to vindicate her right arising from BPI's noncompliance with Section 20 (a) and (c) of Republic Act No. 10173 or the Data Privacy Act of 2012. This is without prejudice to the filing of appropriate civil, criminal, or administrative cases before any other forum or tribunal, if any.

**SO ORDERED.**

City of Pasay, Philippines.  
19 January 2023.

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

**Sgd.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**Sgd.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

Copy furnished:

**NFM**  
*Complainant*

**BANK OF THE PHILIPPINE ISLANDS  
FAMILY – CREDIT CARD DIVISION**  
*Respondent*

**BANK OF THE PHILIPPINE ISLANDS BPI LEGAL  
AFFAIRS AND DISPUTE RESOLUTION DIVISION**  
*Respondent*

**COMPLAINTS AND INVESTIGATION DIVISION  
ENFORCEMENT DIVISION  
GENERAL RECORDS UNIT**  
National Privacy Commission

EG,

Complainant,

NPC 21-111

For: Violation of the  
Data Privacy Act of  
2012

-versus-

JI, RO, and RR

Respondent.

X-----X

## DECISION

### NAGA, P.C.;

Before this Commission is a Complaint filed by EG against JI, RO, and RR (collectively, Respondents) for an alleged violation of Section 32 of Republic Act No. 10173, or the Data Privacy Act of 2012 (DPA).

### Facts

On 01 June 2021, EG filed a Complaint-Affidavit with the NPC’s Complaints and Investigation Division (CID), alleging that he was a resident of CEC, a condominium in XXXX, while Respondents JI works as an (AA), RO works as the (AM), and RR as the (CS) of CEC<sup>1</sup>

In his Complaint-Affidavit, EG alleged that he “had a verbal argument with another tenant in his building, a British-Filipino citizen, which alerted the security agency, including the respondent RR.”<sup>2</sup>EG averred that “when things escalated, matters were reported to the building administrators and the British Filipino nurse, conducted their (sic) own private investigation about [the Complainant].”<sup>3</sup>

EG claimed that “[t]hey talked to the security and was able to secure a video footage of the Complainant, his identity, whereabouts, and other footage containing his personal information without his consent.”<sup>4</sup>

EG alleged that “[i]n the meeting with the Barangay, Respondents JI and RO (sic), employees of , admitted that they [had] released the video footage to the British-Filipino Nurse and admitted that they did so without the consent of EG.”<sup>5</sup>

EG further alleged that there was no privacy notice from the Condominium Corporation informing the tenants that the building administration was processing personal data.<sup>6</sup>

Subsequently, EG filed a complaint with the barangay due to alleged privacy violations.<sup>7</sup> EG attached in his Complaint-Affidavit a letter addressed to the Respondents dated 01

1 Complaint-Affidavit dated 26 May 2021 of EG, at p. 1.

2 *Id.*, at ¶ 4.

3 *Id.*, at ¶ 5.

4 *Id.*, at ¶ 5.

5 Complaint-Affidavit dated 26 May 2021 of EG, at ¶ 8.

6 *Id.*, at ¶ 7.

7 *Id.*, at ¶ 9.



December 2020.<sup>8</sup> In the letter, EG informed the Respondent of the alleged privacy violation and demanded “for damages as reparation and indemnity for [the] unauthorized disclosure of personal information.”<sup>9</sup>

An Order to Comment dated 30 June 2021 was issued ordering Respondents to file a verified comment within fifteen (15) calendar days from receipt of the Order.<sup>10</sup>

On 27 August 2021, an Order to Appear for Preliminary Conference was issued ordering the parties to appear virtually for Preliminary Conference on 13 October 2021 and 27 October 2021.<sup>11</sup>

Respondents filed their Comment dated 25 September 2021 praying that the complaint be dismissed for lack of merit.<sup>12</sup> Respondents averred that they were deployed in the CEC, with RO working as the “AM of MGSJ.”; JI as an “AA” of the same agency; and RR as a “SO of CSSI [.]”.<sup>13</sup>

Respondents stated that “EG [had] a misunderstanding or quarrel [with] one of the tenant[s] namely [JM and PM] at the lobby of Cluster 5.”<sup>14</sup> Respondents alleged that EG filed a complaint before the Barangay due to the incident, and that Spouses JM and PM went to the Property Management Office and requested for the closed-circuit television (CCTV) footage to prove “that there [was] no physical interaction between the two parties and to enlightened (sic) the Barangay Lupon [on] what really happened [during] that time.”<sup>15</sup>

Though not explicitly stated, the “British Filipino nurse” mentioned in EG’s Complaint-Affidavit<sup>16</sup> can reasonably be inferred to be PM as mentioned in the subsequent submissions of the parties. This is bolstered by the fact that EG, in his Memorandum, alleged that he had a verbal argument with PM sometime in January 2020.<sup>17</sup>

Respondents also alleged that EG went to the administrative office to complain about RR for releasing the CCTV footage to the Spouses JM and PM.<sup>18</sup>

Respondents averred that as part of the protocol for this kind of request for investigation, JI, as the (AA), will only receive the complaint or request and collate relevant details which will then be endorsed to the Head of Security or Shift-in-Charge for investigation.<sup>19</sup> Here, JI, forwarded the request to obtain the CCTV to RR, who was the Security-in-Charge at that time.<sup>20</sup> Respondents alleged that JI had no authority nor jurisdiction to approve the release of any documents, personal information, or CCTV footage to any person without the approval of the proper authority.<sup>21</sup>

---

8 Complaint-Affidavit dated 26 May 2021 of EG, at p. 6, See Letter dated 1 December 2020 of LB.

9 *Id.*

10 EG vs JI, RO and RR., NPC 21-111, Order to Comment dated 30 June 2021.

11 EG vs JI, RO, and RR, NPC 21-111, Order to Appear for Preliminary Conference dated 27 August 2021.

12 Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 6.

13 *Id.*, at p. 1.

14 *Id.*, at pp. 1-2.

15 *Id.*, at p. 2.

16 Complaint-Affidavit dated 26 May 2021 of EG, at ¶ 5.

17 Memorandum of Complainant EG dated 23 February 2022, at ¶ 4.

18 Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 3.

19 *Id.*, at p. 2.

20 *Id.*, at p. 2.

21 *Id.*, at p. 2.

Respondents alleged that RR interviewed and investigated the Spouses JM and PM request and retrieved the CCTV footage as evidence to show the lack of physical altercation between Spouses JM and PM and EG.<sup>22</sup> Respondents averred that “[the Spouses JM and PM] presented a letter to RR from Barangay, a Subpoena, and a request letter requesting the evidence on the said incident.”<sup>23</sup> Thus, RR was convinced to release the CCTV footage to assist the Spouses JM and PM “without the approval of the Management or the Security Agency.”<sup>24</sup>

At the hearing before the Barangay, the Spouses JM and PM presented the CCTV footage received from RR which “is one of the pieces of evidence in helping the Barangay to resolve the issues of both parties and to amicably settle the issue between the conflicting parties.”<sup>25</sup>

As their defense, Respondents alleged the following:

1. At the onset, [Respondents] were not furnished [with] a copy of the complaint and thus, had no opportunity to contest the allegations of the complainant.
2. The Complainant failed to comply [with] the substantial requirements for PRE-INVESTIGATION PHASE for failure to give the Respondent the opportunity to address the issue when it sent a defective demand letter as stated in Rule IV Section 1.<sup>26</sup>

Respondents further argued that EG “improperly informed the Respondents of the sufficient factual circumstances surrounding the alleged violation by failing to specify on the demand letter sufficient information on what is [sic] necessary action to be done and the nature of the alleged violation.”<sup>27</sup>

Respondents argued that RO and JI should not be liable for the release of the CCTV footage.<sup>28</sup> RO was out of the office when the Spouses JM and PM requested the said footage and was unaware of the request.<sup>29</sup> Further, Respondents alleged that “JI was only performing her duty as an (AA) in recording, receiving the complaint, and endorsing the concerns or issues to the investigating department.”<sup>30</sup>

Moreover, Respondents alleged that the actions RR took by providing the CCTV footage to the Spouses JM and PM, upon their request, was a “lawful exercise of rights and duties and not violative of any existing privacy laws, guidelines, or policies and done in good faith.”<sup>31</sup>

After the preliminary conference on 13 October 2021, both parties manifested that they were willing to undergo mediation proceedings.<sup>32</sup>

In an Order dated 13 October 2021, the CID stated that:

---

22 Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 2.  
23 *Id.*, at p. 3.  
24 *Id.*, at p. 3.  
25 *Id.*, at p. 3.  
26 Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 4.  
27 *Id.*, at p. 4.  
28 *Id.*, at p. 4.  
29 *Id.*, at p. 5.  
30 Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 5.  
31 *Id.*, at p. 6.  
32 EG vs JI, RO, and RR., NPC 21-111, Order (After the 1st Preliminary Conference on 13 October 2021) dated 13 October 2021.

DL manifested that while respondents received the Order to Virtually Appear for Preliminary Conference dated 17 August 2021, no copy of the complaint and its annexes was attached as raised in the verified comment they have filed. Hence, he requested that respondents be given additional period of time to file amended or supplemental verified comment after receiving a copy of the complaint. Complainant, through counsel, opposed no objection thereto.<sup>33</sup>

The CID ordered that “a copy of the complaint and its attachments, Order to Comment dated 30 June 2021 and all verified comments be furnished” to the parties’ specified addresses.<sup>34</sup>

Subsequently, EG filed a Manifestation with Motion dated 31 October 2021 with a prayer to terminate the mediation proceedings.<sup>35</sup> In the Manifestation, it was alleged that EG emailed his counsel and expressed his unwillingness to enter into mediation with the Respondents.<sup>36</sup>

An Order dated 07 December 2021 was issued granting the motion to terminate the mediation process.<sup>37</sup> Moreover, the Respondents were ordered to submit their amended/supplemental verified comment within fifteen (15) days from receipt of the Order.<sup>38</sup> Further, the parties were ordered to appear for a preliminary conference on 26 January 2022.<sup>39</sup>

The Respondents filed their Joint Counter-Affidavit dated 28 December 2021 wherein they reiterated the discussions made in their initial Comment.<sup>40</sup>

In the Joint Counter-Affidavit, Respondents further alleged that:

6. The releasing of video footage (sic) in favor of JM and PM, the British-Filipino nurse, was decided solely by RR;

a. RR is the SO/CCTV System Operator, who assisted JM and PM do during the investigation of the facts and circumstances that transpired between subjects of the video footage. He released the same to JM and PM upon their request and consent as part of the evidence to prove that there was no physical interaction that transpired between them and the complainant during their confrontation last 9 January 2020.

b. That JM and PM are one of the registered tenants of CEC who provided all documents necessary for the release of the video footage involving them for proper investigation such as investigation request form and waiver declaring that the CCTV footage requested will be used only to resolve their issues with the complainant in the Barangay and not to post in social media or other media platforms. They [JM and PM] also declared taking full responsibility of any legal consequences that may arise from request especially the Data Privacy Act of 2012.<sup>41</sup>

The CID issued an Order dated 04 January 2022 noting the submission of the Joint

33 *Id.*

34 *Id.*

35 Manifestation with Motion of EG dated 31 October 2021, at p. 2.

36 *Id.*, at p. 1.

37 EG vs JI, RO, and RR, NPC 21-111, Order (on the Manifestation and Motion filed by the Complainant) dated 07 December 2021, at p. 1.

38 *Id.*, at p. 1.

39 *Id.*, at p. 2.

40 Joint Counter-Affidavit dated 28 December 2021 of Respondents JI, RO and RR.

41 *Id.*, at ¶ 6.

Counter Affidavit.<sup>42</sup>

In the second preliminary conference on 26 January 2022, the parties stipulated the following issues to be resolved:

- 1) whether or not the release of the CCTV footage constitutes a violation of the Data Privacy Act; and
- 2) whether or not Respondents RO and JI, who have not participated in the release of the video coverage would be held liable.<sup>43</sup>

The parties were ordered to simultaneously submit their respective memoranda.<sup>44</sup>

Respondents filed their Memorandum dated 22 February 2022, wherein they reiterated their claims and defenses in their past submissions and further made additional allegations.<sup>45</sup>

In their Memorandum, Respondents claimed that they “informed JM and PM regarding the legal action taken by [EG] for releasing the requested CCTV Footage.”<sup>46</sup> Moreover, the Spouses JM and PM “provided a signed a letter to the Property Management Office of CEC declaring the CCTV Footage they [got] from CEC will be used as evidence to enlighten the Barangay on what truly happened during their confrontation with EG.”<sup>47</sup>

Respondents alleged that “the CCTV System installed at the CEC was provided by the CSSI. to the Condominium Corporation as part of the Contract Service Agreement and was publicly conveyed to all the members and unit owners based on this contract.”<sup>48</sup> Respondents alleged that RR was “assigned to [the] position [of] SO who will conduct [the] review, [restoration], and make (sic) an investigation report pertaining to the CCTV System operation as part of his duties and responsibilities.”<sup>49</sup>

Respondents, as part of their defense, argued that the release of the CCTV footage was justified since it was in accordance with Section 7 of NPC Advisory No. 2020-04 in relation to Section 13 of the DPA.<sup>50</sup>

Moreover, the Respondents argue that the “consent of the other party (like [EG]) is not necessary particularly when its release is contrary to the interest of the non-consenting [party] and necessary for the defense of the data subject, which is considered a legitimate interest.”<sup>51</sup>

Respondents also argued that the data subjects whose personal information were processed are those of Spouses JM and PM personal information, which was necessary for their defenses against EG’s accusation in the barangay proceedings.<sup>52</sup>

---

42 EG vs JI, RO, and RR, NPC 21-111, Order (Noting the Submission of Joint Counter Affidavit) dated 04 January 2022.

43 EG vs JI, RO, and RR, NPC 21-111, Order (After the 2nd Preliminary Conference) dated 26 January 2022.

44 EG vs JI, RO and RR, NPC 21-111, Order (Noting the Submission of Joint Counter Affidavit) dated 26 January 2022.

45 Memorandum dated 22 February 2022 of Respondents JI, RO, and RR.

46 *Id.*, at ¶ 7.

47 *Id.*, at ¶ 7.

48 *Id.*, at ¶ 17.

49 Memorandum dated 22 February 2022 of Respondents JI, RO, and RR, at ¶ 19.

50 *Id.*, at ¶ 20.

51 *Id.*, at ¶ 22.

52 *Id.*, at ¶ 26.

EG submitted his Memorandum dated 23 February 2022, alleging that he is a “data subject and that his personal information is being processed by the building administrator and security personnel.”<sup>53</sup> Moreover, EG alleged that “the release of PM’s personal information for whatever purpose may be achieved without disclosure of the personal information of non-consenting subjects by masking portions of the video.”<sup>54</sup>

Further, EG argued that as the personal information controller (PIC), Respondents were bound “to safeguard [the] personal information and not disclose said information without the data subject’s consent.”<sup>55</sup> EG further alleged that Respondents admitted that the CCTV was released without his consent and was therefore unauthorized.<sup>56</sup> EG also argued that the access to the CCTV Footage did not comply with the provisions of NPC Advisory No. 2020-04.<sup>57</sup> He also averred that “the lack of CCTV Notice on the premises shows their unawareness of their responsibilities under the law and of the sanctions it can bring.”<sup>58</sup>

### **Issues**

Whether Respondents committed a violation of the DPA.

### **Discussion**

The Commission dismisses the complaint for lack of merit.

EG, as the complainant, has the obligation to prove by substantial evidence that either JI, RO, or RR committed a privacy violation under Section 32 of the DPA.

As already established in past rulings, in administrative proceedings such as in this Commission, the burden is on the Complainant to prove by substantial evidence that the allegations in the complaint are true.<sup>59</sup> In the case of *Billanes vs. Latido*, the Supreme Court defined substantial evidence as “that amount of evidence which a reasonable mind might accept as adequate to justify a conclusion.”<sup>60</sup>

In EG’s Memorandum, it was averred that Respondents “committed a violation upon the release of the video containing the personal information of a non-consenting subject.”<sup>61</sup> Further, EG alleged that “the purpose could be achieved without disclosing personal information of a non-consenting subject by the testimony of witnesses or, should the video be indispensable, by masking of personal information of the non-consenting subject.”<sup>62</sup> Lastly, EG averred that as a “[PIC], [Respondents] have the duty to safeguard personal information of the data subject and may only release personal information with the consent of the subject concerned.”<sup>63</sup> EG alleged that such unauthorized disclo

---

53 Memorandum of Complainant EG dated 23 February 2022, at ¶ 11.

54 *Id.*, at ¶ 19.

55 *Id.*, at ¶ 12.

56 *Id.*, at ¶ 14.

57 Memorandum of Complainant EG dated 23 February 2022, at ¶ 16.

58 *Id.*, at ¶ 25.

59 M vs B, G.R. No. 149335, 01 July 2003.

60 B vs L, A.C. No. 12066, 28 August 2018.

61 Memorandum of Complainant EG dated 23 February 2022, at ¶ 21.

62 *Id.*, at ¶ 24..

63 *Id.*, at ¶ 26..

sure is penalized under Section 32 of DPA.<sup>64</sup>

Respondents, in their defense, argued that the “consent of the other party (like [EG]) is not necessary particularly when its release is contrary to the interest of the non-consenting [party] and necessary for the defense of the data subject, which is considered a legitimate interest.”<sup>65</sup> Further, Respondents alleged that “the action made by [RR] by providing [the] CCTV Footage [to] JM and PM upon their request is a lawful exercise of [their] rights and duties and [is] not violative of any existing privacy laws, guidelines or policies and done in good faith to resolve the issues arising from the contending parties and to facilitate an amicable settlement between them.”<sup>66</sup>

The Commission, after extensively reviewing the evidence and claims of both parties, finds that there is no substantial evidence to conclude that Respondents are liable since EG failed to establish that the processing of the CCTV footage was violative of Section 32 of the DPA or his data privacy rights.

Section 32 of the DPA provides:

Section 32. Unauthorized Disclosure. – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).<sup>67</sup>

As discussed by the Commission in NPC 21-010 to 21-015,

Based on a literal reading of Section 32 of the DPA, a PIC or a PIP is liable if it discloses to a third party personal or sensitive personal information without the consent of the data subject. Following a literal reading, a PIC or PIP will have committed Unauthorized Disclosure if the disclosure is without the consent of the data subject even in the disclosure is justified by another lawful criterion for processing. It does not recognize that such disclosure may be based on other criteria for lawful processing enumerated in Sections 12 and 13 of the DPA. As such a literal reading of Section 32 of the DPA will result in absurdity.<sup>68</sup>

To be liable for Section 32 of the DPA, the following elements must concur:

1. The perpetrator is a personal information controller or personal information processor or any of its officials, employees or agents;
2. The information relates to personal or sensitive personal information;
3. The perpetrator disclosed personal or sensitive personal information;
4. The disclosure was made to a third party;
5. The personal or sensitive personal information disclosed is neither unwarranted nor false information;
6. The disclosure was not malicious nor done in bad faith; and

64 *Id.*, at ¶ 27..

65 Memorandum dated 22 February 2022 of Respondents JI, RO, and RR, at ¶ 22.

66 *Id.*, at ¶ 22.

67 An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter VIII, § 32 (2012).

68 NPC 21-010 to 21-015, Decision dated 03 February 2022, at p. 11.

7. The disclosure was without any of the lawful bases for processing under Section 12 and 13 of the DPA.

As will be discussed below, not all of the elements for a Section 32 violation of the DPA are present in this case.

*I. Respondent RR is an employee of a personal information processor.*

The first element is present in this case as to RR. For clarity, a 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.”<sup>69</sup>

Meanwhile, a personal information processor (PIP) “refers to any natural or juridical person qualified to act as such under this Act to whom a [PIC] may outsource the processing of personal data pertaining to a data subject.”<sup>70</sup>

Respondents averred that they were deployed in the condominium, with RO working as the “Admin Manager of Maininvest General Services Inc.”; JI as an “AA” of the same agency; and RR as a “SO of CSSI [.]”<sup>71</sup>

Further, in Respondents’ Memorandum, it was stated that the CCTV System installed at CEC was provided by CSSI. to the Condominium Corporation as part of the Contract Service Agreement.<sup>72</sup> From the circumstances, CSSI. acts as a PIP by virtue of its contract with the Condominium Corporation to install and operate a CCTV system within their premises. It can be inferred that the processing of information through the CCTV medium is being processed on behalf of the CEC. It is CEC that controls the processing of personal information through CCTV. Thus, based on the foregoing, the PIC in relation to the CCTV system is the Condominium Corporation.

In this respect, RR, as an employee of CSSI., is an agent acting on behalf of the PIP.

However, it is unclear from the records whether JI and RO may be considered PIPs in relation to EG complaint. It should be noted that JI and RO belong to a different agency from RR. They are employed by Maininvest General Services Inc. This agency’s role as a PIP was not fully elaborated in this case. It fell to EG, as the complainant, to prove with substantial evidence how JI and RO actions are within the scope of the DPA either as agents acting on behalf of the PICs or PIPs.

In EG Memorandum, he lumps all the respondents together as violators of the DPA since they are allegedly PICs.<sup>73</sup> However, as the complainant, he had the burden of explaining how each respondent acted in violation of the DPA. After scrutinizing the records, the Commission cannot adequately conclude that JI and RO may fall under the same

69 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).

70 Data Privacy Act of 2012, § 3 (i).

71 Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 1.

72 Memorandum dated 22 February 2022 of Respondents JI, RO, and RR, at ¶ 17.

73 Memorandum of Complainant EG dated 23 February 2022, at ¶ 12.

category as agents acting on behalf of the PIPs. There was no adequate discussion on the role of MGSI., what personal data was processed by the agency or by JI and RO, and how their actions may characterize them as agents of the PICs or PIPs.

Thus, the first element is present for RR since he is an agent acting on behalf of the PIP. However, the first element is absent for JI and RO.

*II. The CCTV footage contains personal information.*

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.”<sup>74</sup>

A CCTV “refers to closed-circuit television or camera surveillance system in a fixed or stationary location that can capture images of individuals or other information relating to individuals.”<sup>75</sup>In NPC Advisory Opinion No. 2019-023, “if a camera surveillance footage is of sufficient quality, a person with the necessary knowledge will be able to reasonably ascertain the identity of an individual from the footage.”<sup>76</sup>

Here, the CCTV footage contains personal information since it could identify parties such as EG through its system of recording videos or capturing images of the data subjects. Thus, the second element is present.

*III. Respondent RR disclosed the personal information of EG.*

In EG Complaint-Affidavit, it was alleged that the Spouses JM and PM were able to secure the CCTV footage of the incident without his consent.<sup>77</sup> In Respondents’ Comment, it was admitted that the CCTV footage was released after RR investigated the request and was convinced that the footage will be used in the barangay proceedings involving the dispute between EG and the Spouses JM and PM.<sup>78</sup>

Disclosure has been defined as “the release, transfer, provisions of, access to, or divulgence in any manner of information outside the entity holding the information.”<sup>79</sup>

In this case, the act of RR releasing the CCTV footage to the Spouses JM and PM constituted an act of disclosure. Thus, the third element is present as to RR.

However, the third element is absent when it comes to JI and RO.

Based on Respondents’ Comment, JI actions were limited to receiving the complaint and endorsing the concerns to the investigating department.<sup>80</sup> Particularly, JI endorsed the request of the spouses to RR, who was the security-in-charge at that time, who then

<sup>74</sup> Memorandum of Complainant EG dated 23 February 2022, at ¶ 12.  
<sup>75</sup> National Privacy Commission, Guidelines on the use of Closed-Circuit Television (CCTV) Systems, NPC Advisory 2020-04, § 3 (c) (16 November 2020) (NPC Advisory 2020-04).  
<sup>76</sup> National Privacy Commission Advisory Opinion No. 2019-023 dated 13 June 2019, Re: Processing of CCTV Footage Under the Data Privacy Act of 2012, at p. 2.  
<sup>77</sup> Complaint-Affidavit dated 26 May 2021 of EG, at ¶ 5.  
<sup>78</sup> Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 3.  
<sup>79</sup> Disclosure (Definition), 2017 Glossary of HIPAA Related Terms, Indiana University.  
<sup>80</sup> Disclosure (Definition), 2017 Glossary of HIPAA Related Terms, Indiana University.



investigated and eventually released the footage to the Spouses JM and PM.<sup>81</sup>

Further, while RO worked as the “AM” of the condominium,<sup>82</sup> Respondents argued that he was on official business at the time and was not in the office during the incident.<sup>83</sup> The records do not show any sufficient proof to refute this claim.

Thus, EG has not established with substantial evidence that either JI or RO actively participated in the release of the CCTV footage.

*IV. The Spouses JM and PM  
are not third parties.*

In EG Complaint, he alleged that “he did not give his consent in the disclosure of his personal information to strangers conducting their own private investigation about him.”<sup>84</sup>

Respondents further alleged that the Spouses JM and PM requested a copy of the CCTV Footage “as evidence to show lack of physical interaction (sic) between the two parties and to enlighten the Barangay that only [a] simple misunderstanding of both parties had transpired.”<sup>85</sup> Respondents also argued that the data subjects whose personal information was processed are those of Spouses JM and PM personal information, which was necessary for their defenses against EG accusation in the barangay proceedings.<sup>86</sup>

Meanwhile, under Section 7 of NPC Advisory No. 2020-04:

SECTION 7. Data subject request for access. — **Any person whose image is recorded on a CCTV system has a right to reasonable access and/or be supplied with a copy of their own personal data from the footage**, subject to the provisions of Section 13 of this Advisory.

xxx

Where images of parties other than the requesting data subject and/or the person/s sought to be identified as part of the request (e.g. identification of malefactors for investigation or law enforcement purposes) appear on the CCTV footage, legitimate interest under Section 12(f) of the DPA may apply as basis for disclosing, subject to Section 9 of this Advisory.<sup>87</sup> (Emphasis supplied)

Here, the Spouses JM and PM cannot be reasonably considered third parties, given that they are also data subjects captured in the CCTV footage. As data subjects, Spouses JM and PM has a reasonable claim to access and obtain the CCTV footage used in the barangay dispute between EG and the Spouses JM and PM.

*V. The personal information is neither  
unwarranted nor false information.*

For a violation of Section 32 of the DPA to be committed, the personal or sensitive in-

81 *Id.*, at p. 3.

82 *Id.*, at p. 2.

83 *Id.*, at p. 5.

84 Complaint-Affidavit dated 26 May 2021 of EG, at ¶ 11.

85 Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 2.

86 Memorandum dated 22 February 2022 of Respondents JI, RO, and RR, at ¶ 26.

87 Section 7, of NPC Advisory 2020-04, otherwise known as Guidelines on the use of ClosedCircuit Television (CCTV) Systems.

formation should neither be unwarranted nor false.

In this case, there is no indication that the CCTV footage was falsified, altered, or considered unwarranted. Though EG alleged that the footage was disclosed without his consent, the disclosure was in relation to the barangay dispute. The presentation of the CCTV footage is warranted and necessary in the barangay dispute to prove the defense of Spouses JM and PM. Moreover, EG did not dispute the veracity of the CCTV footage that it was false or altered. Thus, the fifth element is present.

*VI. There was no bad faith or malice on the part of Respondents*

The Supreme Court has defined “malice” as that 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.”<sup>88</sup> As to bad faith, it “implies a conscious and intentional design to do a wrongful act for a dishonest purpose or some moral obliquity.”<sup>89</sup>

Further, the Supreme Court ruled in *Wong vs. Wong*:<sup>90</sup>

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 once more, his self-serving assertion cannot be given credence. This is especially so in light of the presumption of regularity, which herein ought to prevail due to the absence of any clear and convincing evidence to the contrary.<sup>91</sup>

In this case, EG did not prove that Respondents acted with malice or bad faith in disclosing his personal information. Indeed, EG accused the Respondents of violating Section 32 of the DPA, which is a privacy violation falling outside Malicious Disclosure under Section 31 of the DPA. Thus, the sixth element is also present.

*VII. There is a lawful basis on the part of Respondent RR in releasing the CCTV footage to Spouses JM and PM.*

The seventh element is absent. EG alleged that the release of the CCTV footage was made without his consent.<sup>92</sup> However, consent is not the only criterion for lawful processing under the DPA.

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

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

xxx

(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

88 Delgado v. HRET, G.R. No. 219603, 26 January 2016

89 Montinola vs. Philippine Airlines, G.R. No. 198656, 8 September 2014.

90 Tzu Sun Wong vs. Kenny Wong, G.R. No. 180364, 03 December 2014.

91 Tzu Sun Wong vs. Kenny Wong, G.R. No. 180364, 03 December 2014, citing Alcazar vs. Arante, G.R. No. 177042, 10 December 2012.

92 Complaint-Affidavit dated 26 May 2021 of EG, at ¶ 11.

the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

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

xxx

(f) The processing concerns such personal information as is **necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims**, or when provided to government or public authority.<sup>93</sup> (Emphasis supplied)

Further, Section 9 of NPC Advisory No. 2020-04, provides:

SECTION 9. Legitimate interest three-part test. **In determining whether the data subject access request, in instances when the CCTV footage includes other data subjects, under Section 7, or the third-party access request under Section 8(E) may be allowed pursuant to legitimate interest as provided for under Section 12(f) of the DPA**, the following shall be considered:

A. Purpose test - The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve.

B. 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

C. 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.

In this regard, CCTV footages requested for purposes of the protection of lawful rights and interests or the establishment, exercise or defense of legal claims under Section 13(f) of the DPA may be considered as legitimate interest.<sup>94</sup>

It is apparent in the submissions of the parties that the CCTV footage obtained by the Spouses JM and PM was used as part of their defense in a complaint against them before the barangay. The CCTV footage was used to prove that there was no physical altercation between the Complainant and the Spouses JM and PM.<sup>95</sup> Thus, the release of the footage was necessary for the exercise of the spouses' defenses in the barangay proceeding. The purpose for the release of the footage was adequately shown through the Investigation Request Form,<sup>96</sup> and the Spouses JM and PM's letter dated 31 January 2020.<sup>97</sup>

In the case of KRL vs. Trinity University of Asia, et. al., the Commission ruled:

93 Section 12 (f) and Section 13 (f) of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012  
94 Guidelines on the use of Closed-Circuit Television (CCTV) Systems, NPC Advisory 2020-04, § 9  
95 Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 2.  
96 Memorandum dated 22 February 2022 of Respondents JI, RO, and RR, See: Annex "B".  
97 Memorandum dated 22 February 2022 of Respondents JI, RO, and RR, See: Annex "B".

Although Section 13(f) applies to sensitive personal information while the information involved in this case is just personal information, the protection of lawful rights and interests under Section 13(f) by the respondent faculty members in this case is considered as legitimate interest pursuant to Section 12(f) of the DPA.<sup>98</sup>

In this case, although the CCTV footage is considered as personal information, Section 13 (f) is applicable since the processing of the CCTV is pursued under a legitimate interest 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 of Spouses JM and PM.

Moreover, in NPC 21-031, the Commission ruled:

The phrase ‘for the protection of lawful rights and interests of natural or legal persons in court proceedings’ cannot be interpreted to relate only to the person asserting the lawful basis of the processing of personal information. It also contemplates situations where those persons whose lawful rights and interests are protected in court proceedings may not be the same individuals who processed the personal information, such as in the case of witnesses. Similarly, the next clause ‘establishment, exercise or defense of legal claims’ may be interpreted to refer to the legal claims of persons other than those who processed the personal information.<sup>99</sup>

Here, it was admitted that the CCTV footage was released after RR investigated the request and was convinced that the footage will be used in the barangay proceedings involving the dispute between EG and the Spouses JM and PM.<sup>100</sup> Considering that Section 13 (f) of the DPA may be invoked by persons other than those who processed the personal information, the act of RR in releasing the CCTV footage for the establishment of the defense of Spouses JM and PM in the Barangay proceeding is considered lawful processing.

Second, the release of the CCTV footage can be considered necessary since it is a crucial piece of evidence to prove the defense of the spouses in the barangay proceeding. It is not shown that there were other means to support their defenses other than the CCTV footage.

Lastly, there is no substantial evidence to show that the fundamental rights and freedom of EG have been overridden by the release of the CCTV footage. Thus, Respondent’s lawful processing of EG’s personal information was for the legitimate interest of Spouses JM and PM for their defense in the barangay proceedings.

In totality, not all of the elements are present to warrant a finding that the Respondents violated Section 32 of the DPA. There is a lack of substantial evidence to prove a privacy violation.

**WHEREFORE**, premises considered, this Commission resolves that the instant Complaint filed by EG against JI, RO, and RR is hereby **DISMISSED** for lack of merit.

**SO ORDERED.**

City of Pasay, Philippines.

22 September 2022.

98 KRL vs. Trinity University of Asia, AA, MC, NCB, RG, GV, GCT, RR, MR, PB, CID Case no. 17K-003, dated 19 November 2019.

99 JCB vs. FRL, NPC 21-031, dated 03 March 2022

100 Comment dated 25 September 2021 of Respondents JI, RO, and RR, at p. 3.

**Sgd.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

I CONCUR:

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

Copy furnished:

**EG**  
*Complainant*

**LB**  
*Counsel for Complainant*

**JI, RO, and RR**  
*Respondents*

**DL**  
*Counsel for Respondents*

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

RGC

*Complainant,*

**NPC 21-054**  
For: Violation of the  
Data Privacy Act of  
2012

-versus-

**JK INCORPORATED & RECOVERY, INC.**

*Respondent.*

X-----X

## DECISION

**NAGA, P.C.;**

Before this Commission is a Complaint filed by RGC against JK Incorporated & Recovery, Inc. (JK Incorporated) for alleged privacy violations of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

### Facts

On 19 March 2021, the Commission, through its Complaints and Investigation Division (CID), received RGC Complaints-Assisted Form dated 25 February 2021 (CAF).<sup>1</sup> RGC alleged:

MS of [JK Incorporated] – accredited agency of PSBank contacted me via phone call and sent some messages to my relatives and friends at around 11 AM on Facebook disclosing [that I have] an obligation [with] them.<sup>2</sup>

To support his claim, RGC attached a screenshot of a message purportedly from MS:

Good Day! may we ask for your assistance regarding one of your friend/colleague/relative of RGC to relay to the person to coordinate with us the soonest time possible likewise, the person may refer to all our contact details indicated herewith. Thanks and hoping for your urgent feedback. Please look for any officer of under legal counsel of JTF Tel. no. XXX/XXX.<sup>3</sup>

RGC also claimed that the message was sent to his sister, RMC to disclose his obligation to JK Incorporated.<sup>4</sup>

Thus, RGC argued that based on the foregoing incident, JK Incorporated violated the DPA.<sup>5</sup> He also prayed that damages and a fine be imposed against JK Incorporated.<sup>6</sup>

On 23 June 2021, JK Incorporated was ordered by the CID to file a verified comment within fifteen (15) calendar days from the receipt of the Order.<sup>7</sup>The same Order also stated that after the lapse of the reglementary period, the parties shall be ordered to

1 Complaints-Assisted Form dated 25 February 2021 of RGC.  
2 *Id.*, at p. 3.  
3 Complaints-Assisted Form dated 25 February 2021 of RGC, See Annex "A", Screenshot of the Message from MS.  
4 Complaints-Assisted Form dated 25 February 2021 of RGC, at p. 4.  
5 *Id.*, at p. 3.  
6 *Id.*, at p. 5.  
7 RGC v. JK Incorporated & Recovery Inc., NPC 21-054, Order to Comment dated 23 June 2021, at p. 1.

appear for a preliminary conference.<sup>8</sup>

On 15 July 2021, JK Incorporated filed its Comment with Affirmative Defense/s dated 08 July 2021 praying that the complaint be dismissed for lack of cause of action and lack of merit.<sup>9</sup> JK Incorporated averred that RGC CAF “states no cause of action and is frivolous, vexatious and made in bad faith.”<sup>10</sup>

JK Incorporated argued that no personal data or information of RGC was divulged to any person.<sup>11</sup> It further stated that the screenshot attached to the CAF “does not mention of any obligation which the Complainant alleged.”<sup>12</sup> JK Incorporated also stated that RGC claims about his relatives being contacted regarding his obligation is but a “product of his lies and/or imagination.”<sup>13</sup>

JK Incorporated further argued that the filing by RGC of the case is “a desperate attempt on his part to evade payment of his obligation.”<sup>14</sup>

On 12 July 2021, the parties were ordered by the CID to appear for preliminary conferences on 05 August 2021 and 18 August 2021.<sup>15</sup>

On 05 August 2021, an Order (After 1st Preliminary Conference held on 05 August 2021) was issued wherein both parties manifested that they were willing to undergo mediation proceedings to explore the possibility of amicable settlement.<sup>16</sup>

After both parties filed their Applications for Mediation,<sup>17</sup> the CID issued an Order to Mediate dated 09 September 2022, wherein the complaint proceedings were to be suspended for sixty (60) days for the conduct of the mediation proceedings.<sup>18</sup>

On 13 October 2021, a Notice of Non-Settlement of Dispute was issued for failure of the parties to reach a settlement.<sup>19</sup> Thereafter, on the same date, the CID issued an Order (for Resumption of Complaints Proceedings and Submission of Documents and Memoranda) ordering the parties to submit their respective Memoranda together with a list of evidence presented to prove their respective claims or defenses.<sup>20</sup>

RGC filed his Memorandum dated 25 October 2021, alleging that in 2017, he applied for a “revolving loan/Flexi loan” from PS Bank, with the loan being approved for three (3) years in a row.<sup>21</sup> RGC alleged that during his application and the credit investigation, “the bank never asked for a list of contact reference[s] to which the bank may contact in case Complainant failed to make good his obligation.”<sup>22</sup>

---

8 *Id.*  
9 Comment with Affirmative Defense/s dated 08 July 2021 of JK Incorporated & Recovery Inc.  
10 *Id.*, ¶ 2.  
11 *Id.*, ¶ 3.  
12 *Id.*, ¶ 4.  
13 Comment with Affirmative Defense/s dated 15 July 2021 of JK Incorporated & Recovery Inc., ¶ 4.  
14 *Id.*, ¶ 5.  
15 RGC v. JK Incorporated & Recovery Inc., NPC 21-054, Order to Comment dated 12 July 2021, at p. 1.  
16 *Id.*  
17 Application for Mediation dated 09 September 2022 of RGC and Application for Mediation of JK Incorporated & Recovery Inc. dated 09 September 2022.  
18 RGC v. JK Incorporated & Recovery Inc., NPC 21-054, Order to Mediated dated 09 September 2022, at p. 1.  
19 *Id.*  
20 *Id.*  
21 Memorandum (Complainant) dated 25 October 2021, ¶ 5.  
22 *Id.*, ¶ 5.

In addition, RGC alleged that in April 2020, he could no longer avail of the loan scheme.<sup>23</sup> The bank demanded from him the payment of his full obligation and in November 2020, he received the Statement of Account.<sup>24</sup>

RGC claimed that on 07 December 2020, JK Incorporated contacted him about his outstanding loan via e-mail.<sup>25</sup> RGC tried to reason with JK Incorporated that he could not pay the obligation and asked for more time to pay it.<sup>26</sup> RGC averred that throughout January and February 2021, JK Incorporated flooded him with calls to pay his obligation.<sup>27</sup>

On 25 February 2021, RGC alleged that his Facebook friends received a message that read:

Good Day! may we ask for your assistance regarding one of your friend/colleague/relative of RGC to relay to the person to coordinate with us the soonest time possible likewise, the person may refer to all our contact details indicated herewith. Thanks and hoping for your urgent feedback. Please look for any officer of under legal counsel of JTF Tel. no. XXX/XXX.<sup>28</sup>

As a result, RGC alleged that his Facebook friends contacted him to inform him that the message is circulating among his Messenger contacts.<sup>29</sup> Thus, this prompted RGC to inform JK Incorporated that it was illegal to access his personal information and that the latter maliciously disclosed his information to parties who were not privy to the transaction.<sup>30</sup> RGC claimed that after informing JK Incorporated, “the message was suddenly ‘unsent’.”<sup>31</sup>

RGC Memorandum provided the following pieces of evidence: 1) a screenshot of the purported Facebook message subject of the complaint,<sup>32</sup> the affidavit of RMC,<sup>33</sup> and the affidavit of RC.<sup>34</sup> JK Incorporated’s act, according to RGC, was a violation of Section 29 (Unauthorized Access or Intentional Breach)<sup>35</sup> and Section 31 (Malicious Disclosure)<sup>36</sup> of the DPA. RGC further argued that none of the circumstances in Section 12 of the DPA were present to justify the use of RGC personal information.<sup>37</sup>

JK Incorporated filed its Memorandum dated 29 October 2021, alleging that it was the collecting agent of PS Bank.<sup>38</sup> On 03 December 2020, it received an endorsement from PS Bank regarding RGC loan.<sup>39</sup>

According to JK Incorporated, since RGC refused to answer its calls and emails, it

---

23 *Id.*, ¶ 6.  
24 *Id.*, ¶ 7.  
25 Memorandum (Complainant) dated 25 October 2021, ¶ 8.  
26 *Id.*, ¶ 9.  
27 *Id.*, ¶ 10.  
28 *Id.*, ¶ 11.  
29 Memorandum (Complainant) dated 25 October 2021, ¶ 13.  
30 *Id.*  
31 *Id.*  
32 Memorandum (Complainant) dated 25 October 2021, Annex “A”.  
33 *Id.*, ¶ Annex “B”.  
34 *Id.*, ¶ Annex “C”.  
35 *Id.*, ¶ 20.  
36 Memorandum (Complainant) dated 25 October 2021, ¶ 22.  
37 *Id.*, ¶ 28.  
38 *Id.*, at p. 2.  
39 *Id.*



resorted to the practice of “skip tracing”.<sup>40</sup> Particularly, JK Incorporated alleged that since RGC could no longer be contacted despite several messages and calls, it visited his Facebook account.<sup>41</sup> JK Incorporated claimed that RGC Facebook Account contained a public post with several comments.<sup>42</sup> One of the comments came from RMC calling RGC “Kuya” (brother), and to whom RGC responded to as “Sis”.<sup>43</sup> JK Incorporated inferred that they were related, thus, it messaged RMC.<sup>44</sup>

JK Incorporated posited that instead of settling the obligation, RGC filed the subject Complaint against it.<sup>45</sup>

It argued that RGC failed to state a cause of action since the complaint failed to allege the “manner and circumstances” of the commission of the offense charged.<sup>46</sup>

Further, JK Incorporated argued that it could not be liable for Section 29 of the DPA (Unauthorized Access or Intentional Breach) since it should be proven that “the offender [broke] in any way into the system where personal and sensitive personal information is stored.”<sup>47</sup> Here, JK Incorporated contended that it could not have committed unauthorized access when the information was readily and publicly available on the internet, particularly on Facebook.<sup>48</sup>

JK Incorporated further argued that it could not be liable for Section 32 of the DPA (Malicious Disclosure) since the message only requested to relay the message to RGC and it never mentioned his loan obligation.<sup>49</sup> JK Incorporated also disputed RGC allegation that it sent messages to both RMC and to RC, since RMC was the only one identified by JK Incorporated through skip tracing.<sup>50</sup>

Thus, JK Incorporated prayed that the RGC complaint be dismissed.<sup>51</sup>

### **Issues**

Whether JK Incorporated committed a violation of the DPA.

### **Discussion**

The Commission dismisses the Complaint.

The Commission shall first discuss the act that was allegedly a violation of the DPA. RGC does not dispute the authority of JK Incorporated to collect outstanding obligations. Indeed, in his CAF, RGC mentions that JK Incorporated was an accredited agency of PS Bank.<sup>52</sup> Rather, he specifically claims that JK Incorporated’s act of contacting persons in his social media list was violative of the DPA.<sup>53</sup>

40 Memorandum of the Respondent dated 29 October 2021, at p. 3.

41 *Id.*

42 *Id.*

43 *Id.*

44 Memorandum of the Respondent dated 29 October 2021, at p. 3.

45 Complaints-Assisted Form dated 25 February 2021 of RGC.

46 Memorandum of the Respondent dated 29 October 2021, at p. 4.

47 *Id.*, at p. 7.

48 *Id.*

49 *Id.*

50 Memorandum of the Respondent dated 29 October 2021, at p. 9.

51 *Id.*, at p. 10.

52 Complaints-Assisted Form dated 25 February 2021 of RGC, at p. 3

53 Memorandum (Complainant) dated 25 October 2021, ¶¶ 21-24.

JK Incorporated can be considered to have engaged in the practice of skip tracing after messaging at least one person, RMC, on Facebook in order to reach RGC. To recall, the message that was sent to RMC states:

Good Day! may we ask for your assistance regarding one of your friend/colleague/relative of RGC to relay to the person to coordinate with us the soonest time possible likewise, the person may refer to all our contact details indicated herewith. Thanks and hoping for your urgent feedback. Please look for any officer of under legal counsel of JTF Tel. no. XXX/XXX.<sup>54</sup>

The Commission explained the concept of skip tracing in relation to the DPA in its Advisory Opinion No. 2018-059:

The DPA does not prohibit the collection of personal information through skip tracing or probing, provided that the collection or any further processing is done in accordance with the law. In general, processing of personal data should adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. There should be procedures in place for data subjects to exercise their rights and appropriate security measures for data protection.

xxx

Collection agencies are considered personal information processors (PIPs) to whom a personal information controller (PIC) has outsourced the processing of personal data of borrowers. This is due to the nature of their business, which, in general, performs the processing of personal data for the benefit of other companies. As PIPs, collection agencies are expected to process personal data only in accordance with their agreement with a PIC.<sup>55</sup>

Thus, though skip tracing is not prohibited, the practice still has to comply with the DPA.

Second, for complaints before the Commission to prosper, the burden of proof required is substantial evidence, or “that amount of relevant evidence that a reasonable mind might accept as adequate to support a conclusion.”<sup>56</sup> The Supreme Court has explained that:

[T]he complainant has the burden of proving by substantial evidence the allegations in his complaint. The basic rule is that mere allegation is not evidence and is not equivalent to proof. Charges based on mere suspicion and speculation likewise cannot be given credence.<sup>57</sup> (Emphasis supplied)

Thus, RGC has the burden to prove by substantial evidence that a privacy violation was committed. However, in this case, RGC provided a screenshot of an alleged Facebook message to RMC from a certain MS and an affidavit supporting the said screenshot.<sup>58</sup> Such cannot be considered sufficient evidence to prove that unauthorized access and malicious disclosure was committed by JK Incorporated.

The mere screenshot of a message from MS does not show that JK Incorporated actually

---

54 *Id.*, ¶ 11.

55 National Privacy Commission Advisory Opinion 2018-059, Skip tracing and probing of contact details through the internet and third parties, (4 October 2018).

56 *De Jesus v. Guerrero III*, G.R. No. 171491, 04 September 2009.

57 *Id.*

58 Memorandum (Complainant) dated 25 October 2021, Annex “A”.

broke into a data system where his personal or sensitive personal information is stored. Further, such screenshot does not substantiate that the disclosure was malicious or was done in bad faith or involved unwarranted or false information relative to his personal data, since the screenshot only shows a message from MS asking for assistance to relay their message to RGC.

Consequently, absent the supporting evidence that JK Incorporated indeed broke into the system and that there is malice or bad faith in the disclosure of his personal information, such allegations cannot be given credence by the Commission.

In addition, the Commission stresses, “[t]he burden to establish the charges rests upon the complainant. The case should be dismissed for lack of merit if the complainant fails to show in a satisfactory manner the facts upon which his accusations are based. The respondent is not even obliged to prove his exception or defense.”<sup>59</sup>

Taken all together, RGC pieces of evidence were not sufficient to prove that a privacy violation was committed since RGC failed to establish that the message sent by JK Incorporated was violative of his data privacy rights or that its actions rose to the level of a DPA violation, as will be further discussed below.

*I. JK Incorporated adhered to the general data privacy principles of transparency, legitimate purpose, and proportionality.*

There is no substantial evidence to prove that JK Incorporated violated the general data privacy principles of transparency, legitimate purpose, and proportionality.<sup>60</sup>

The Commission notes that based on the record, RGC did not adequately discuss how JK Incorporated’s actions violated the general data privacy principles. There is insufficient evidence on record to show that JK Incorporated did not adhere to the principles.

As discussed, the act of skip tracing is not per se prohibited. Thus, JK Incorporated’s actions do not automatically mean that it was contrary to law, morals, or public policy. There is no substantial evidence to show that JK Incorporated did not provide a specific or declared purpose for its processing of personal data or that the processing was incompatible with a declared or specified purpose. The record shows that the message was sent in relation to the collection of RGC’s debt. This was resorted to because RGC was not responsive in settling his obligation.<sup>61</sup> Debt collection is not a prohibited purpose to process personal data. As long as it complies with the relevant laws, like the DPA and related NPC issuances, the processing of personal data for debt collection is a legitimate purpose.

Here, JK Incorporated’s message to RMC was straightforward in its purpose, which was to ask for assistance in contacting RGC in order for him to coordinate with JK Incorporated. In fact, the message did not even disclose that RGC had a loan obligation. It was just a message asking for assistance to reach RGC.

<sup>59</sup> National Bureau of Investigation v. Najera, G.R. No. 237522 (Resolution), 30 June 2020.

<sup>60</sup> Data Privacy Act of 2012, chapter III, § 11. See also National Privacy Commission, Implementing Rules and Regulations of the Data Privacy Act of 2012, rule IV, § 18 (2016) (IRR of the DPA).

<sup>61</sup> See Memorandum of the Respondent dated 29 October 2021, at p. 3; Memorandum (Complainant) dated 25 October 2021, ¶ 10.

As to transparency, JK Incorporated has been in contact<sup>62</sup> with RGC prior to the skip tracing and that RGC is aware of the purpose to which his personal information is being processed by the former. Also, in terms of proportionality, the screenshot shows that JK Incorporated did not disclose any information other than his name, which is relevant and necessary for JK Incorporated to identify RGC in its request for assistance from RMC. Moreover, the message to RMC is proportional and not excessive since it did not disclose excessive information such as RGC’s loan obligation.

Taken all together, the prevailing circumstances do not show any violation of the general data privacy principles. Thus, given the context of debt collection and JK Incorporated’s position as a collecting agent, the message to RMC was transparent, legitimate, and proportional to the purpose in collecting RGC debt.

*II. JK Incorporated is not liable for Section 29 (Unauthorized Access or Intentional Breach) of the DPA.*

RGC alleged that JK Incorporated violated Section 29 of the DPA since “he never gave any contact information of any person to...[JK Incorporated]. However, without his authority, [JK Incorporated] accessed his Friends List [on] Facebook and started messaging the said contacts [through] Facebook Messenger.”<sup>63</sup>

Section 29 of 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.<sup>64</sup>

The case of ACN v. DT enumerated the elements of a violation of Section 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.<sup>65</sup>

The first element is present. Though there was no substantial discussion on whether the data system stored personal data, the Commission notes that Facebook’s Privacy Policy, at the time the message was sent, states: “[w]e collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others.”<sup>66</sup> As to managing the information, it is stated that “[w]e store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no l

62 Memorandum (Complainant) dated 25 October 2021, ¶ 8.

63 *Id.*, ¶ 21.

64 An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter VIII, § 29 (2012).

65 NPC 18-109, 01 June 2021.

66 Facebook Privacy Policy, 9 September 2016, See “What kinds of information do we collect”.

longer need the data to provide products and services.”<sup>67</sup> Thus, Facebook, particularly its Messenger platform, may be considered a data system that stores personal data.

However, there is a lack of substantial evidence to prove that the second and third elements exist. RGC has not proven that JK Incorporated broke into his Facebook account or into his Messenger platform to access his contacts, much more that it did so knowingly and unlawfully.

On the contrary, JK Incorporated stated that it was able to message Rica by visiting RGC’s Facebook Account.<sup>68</sup> Further, it alleged that it was able to get RMC details through the comments of RGC’s public Facebook post.<sup>69</sup> On this note, JK Incorporated argued that there could not be unauthorized access to information when it is available “readily and publicly” on Facebook.<sup>70</sup>

The Commission emphasizes that the availability of personal data in the public sphere does not mean that the DPA no longer applies, given that the DPA looks into the processing of personal data, regardless of whether it is publicly available or not. As provided in NPC Advisory Opinion No. 2018-059:

It should be clarified that the public availability of personal information does not exclude it from the scope of the DPA. This law applies to the processing of all types of personal information, publicly available or not, and to any natural and juridical person involved in personal information processing. ‘Processing’ in this context refers to the collection, use, storage, disposal and any other operation performed upon personal information.<sup>71</sup>

There was also no evidence provided that RGC fully utilized the Facebook privacy tools, or that his intention was to keep his posts private. Nevertheless, in this case, the Commission finds that between the two allegations of the parties, it is more reasonable to conclude that JK Incorporated was able to get RGC and RMC’s details by searching for their respective Facebook profiles.

Thus, there is no substantial evidence to find that JK Incorporated violated Section 29 of the DPA.

*III. JK Incorporated is not liable  
for Section 31 (Malicious  
Disclosure) of the DPA.*

RGC alleged that JK Incorporated violated Section 31 of the DPA since “people who were not listed by [RGC] as reference list received messages from [JK Incorporated] about the fulfillment of [RGC’s obligations.]”<sup>72</sup>

Section 31 of the DPA provides:

SEC. 31. Malicious Disclosure. – Any personal information controller or personal in

67 Id, See “How can I manage or delete information about me”.

68 Memorandum of the Respondent dated 29 October 2021, at p. 3.

69 Id.

70 Id, at p. 7.

71 NPC Advisory Opinion 2018-059, Skip tracing and probing of contact details through the internet and third parties, (4 October 2018). See, DPA definition of processing in footnote.

72 Memorandum (Complainant) dated 25 October 2021, ¶ 24.

formation 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).<sup>73</sup>

The elements of Section 31 are:

1. The perpetrator is a personal information controller or a personal information processor or any of its officials, employees or agents;
2. The perpetrator disclosed personal or sensitive personal information;
3. The disclosure was made with malice or in bad faith; and 4. The information disclosed was unwarranted or false information.<sup>74</sup>

Here, JK Incorporated claimed that it is the collecting agent of PS Bank and received the endorsement of RGC's loan obligation.<sup>75</sup>

Section 2 (i) of the DPA provides:

(i) *Personal information processor* refers to 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.

As PS Bank's collecting agent, JK Incorporated may be considered a personal information processor (PIP). PS Bank is the one who has control over RGC's information, which it outsourced to JK Incorporated in order for it to collect RGC's outstanding loan balance. Thus, the first element is present.

As to the second element, RGC alleged that:

MS of [JK Incorporated] – accredited agency of PSBank contacted me via phone call and sent some messages to my relatives and friends at around 11 AM on Facebook disclosing [that I have] an obligation [with] them.<sup>76</sup>

JK Incorporated's act of contacting the "relatives" of RGC, is considered an act of disclosure since it divulged the full name of RGC in the Facebook message. Thus, the second element is present.

However, the third and fourth elements are absent. A reading of the message does not show that JK Incorporated acted in malice or bad faith in disclosing the personal information nor that the message contained any unwarranted or false information. To quote:

Good Day! may we ask for your assistance regarding one of your friend/colleague/relative of RGC. to relay to the person to coordinate with us the soonest time possible likewise, the person may refer to all our contact details indicated herewith. Thanks and hoping for your urgent feedback. Please look for any officer of under

---

73 An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter VIII, § 31 (2012).

74 NPC 21-015, 03 February 2022

75 Memorandum of the Respondent dated 29 October 2021, at p. 2.

76 Complaints-Assisted Form dated 25 February 2021 of RGC, at p. 3.

legal counsel of JTF Tel. no. XXX/XXX.<sup>77</sup>

As to the third element, the Supreme Court defined 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.”<sup>78</sup> Meanwhile, as to bad faith, it “implies a conscious and intentional design to do a wrongful act for a dishonest purpose or some moral obliquity.”<sup>79</sup>

Here, RGC failed to adduce sufficient proof that JK Incorporated acted with malice or bad faith in the disclosure of his personal information. In the screenshot that RGC himself provided, the message only shows that JK Incorporated is requesting for assistance from RMC. Nowhere in the message indicates spite, ill will, or any statement to injure RGC’s reputation, and does not imply any intention to do a wrongful act against him since no other information was disclosed aside from his name.

To stress, the message to RMC only disclosed RGC’s full name and did not mention RGC’s loan or financial obligation at all. JK Incorporated only stated that it was seeking assistance to relay to RGC the need to coordinate with the name and contact number of its representative.

JK Incorporated’s message was straightforward and was a request for RGC to contact its legal counsel. Aside from RGC’s full name, no other information was disclosed by JK Incorporated besides the name and contact number of its legal counsel. These circumstances are not indicative of bad faith on the part of JK Incorporated, especially given the context that RGC allegedly was no longer responsive to its messages.<sup>80</sup> Thus, by itself, the message cannot be considered malicious or made in bad faith.

In terms of the fourth element, there is no indication that the name involved is unwarranted or a false information since RGC did not dispute that the name involved is false and it is, in fact, his full name. Nevertheless, the Commission notes that JK Incorporated only mentioned RGC’s name, and not his loan obligation. The surrounding context shows that the information disclosed was warranted since it was necessary for JK Incorporated to identify RGC in its request for assistance from RMC.

Considering the foregoing, the Commission finds that JK Incorporated did not violate Section 31 of the DPA since not all the elements for Malicious Disclosure are present.

After scrutinizing the evidence and arguments of both parties, the Commission cannot find that JK Incorporated committed a privacy violation under the DPA.

**WHEREFORE**, premises considered, this Commission resolves that the Complaint filed by RGC against JK Incorporated & Recovery, Inc. is hereby **DISMISSED**.

**SO ORDERED.**

<sup>77</sup> Id. Annex A

<sup>78</sup> Delgado v. HRET, G.R. No. 219603, 26 January 2016.

<sup>79</sup> Montinola vs. Philippine Airlines, G.R. No. 198656, 8 September 2014.

<sup>80</sup> Montinola vs. Philippine Airlines, G.R. No. 198656, 8 September 2014.

City of Pasay, Philippines.  
22 September 2022.

**Sgd.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

I CONCUR:

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

Copy furnished:

**RGC**  
*Complainant*

**JK INCORPORATED & RECOVERY, INC.**  
*Respondent*

**JTF**  
*Counsel for Respondent*

**COMPLAINTS AND INVESTIGATION  
DIVISION ENFORCEMENT DIVISION  
GENERAL RECORDS UNIT**  
National Privacy Commission



**JBZ,**

*Complainant,*

**NPC 21-122**

For: Violation of the  
Data Privacy Act of  
2012

-versus-

**METROPOLITAN BANK & TRUST,  
COMPANY AND CDR  
AS VP CARDS AND PERSONAL  
CREDIT SECTOR**

*Respondent.*

X-----X

## **DECISION**

**AGUIRRE, D.P.C.;**

Before this Commission is a Complaint filed by JBZ against Metropolitan Bank & Trust Company (Metrobank) and CDR as Vice President, Cards and Personal Credit Sector for alleged violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

### **Facts**

On 08 February 2021, JBZ filed a complaint against Metrobank and CDR for violations of the DPA.<sup>1</sup>

JBZ alleged that he has been a Metrobank cardholder with credit card ending in [ ] since July 2013.<sup>2</sup> He regularly received his billing from Metrobank through his mobile number, and his Statement of Account through his email address.<sup>3</sup>

He claimed that he received an email dated 18 March 2020 from CDR, on behalf of Metrobank, informing him that Metrobank already endorsed his account to its collection agents.<sup>4</sup> He alleged that the endorsement was done “without [his] approval.”<sup>5</sup>

To support his allegation, he attached a letter signed by CDR on behalf of Metrobank.<sup>6</sup> CDR explained in the letter that JBZ sent an email to the Consumer Empowerment Group of the Bangko Sentral ng Pilipinas (BSP) on 24 February 2020 to complain that Metrobank failed to respond to his request for a balance restructuring program.<sup>7</sup>

CDR also stated that the BSP forwarded the matter to Metrobank “for appropriate action” on 10 March 2020.<sup>8</sup> CDR explained that Metrobank did not receive any request for

1 Complaints-Assisted Form, 08 February 2021, at 5-6, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

2 *Id.* at 3.

3 *Id.* Annex 3.

4 *Id.* at 3.

5 *Id.*

6 *Id.* Annex 3.

7 Complaints-Assisted Form, 08 February 2021, Annex 3, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

8 *Id.*

restructuring from JBZ.<sup>9</sup> Metrobank’s collection agents tried contacting JBZ through his declared phone numbers from 12 to 16 March 2020 to no avail.<sup>10</sup> As a result, Metrobank requested JBZ to provide other contact numbers and a schedule to discuss available payment options through a phone call.<sup>11</sup>

JBZ alleged that he began receiving anonymous calls and emails as a result of the endorsement of his account to Metrobank’s collection agents.<sup>12</sup> He claimed that as a result of the alleged disclosure, he began receiving demands for the collection of his unsettled obligation through emails and phone calls from several senders he did not recognize.<sup>13</sup> JBZ submitted screenshots of his mobile phone call logs that showed incoming phone calls from several untagged numbers from May 2020 to August 2020.<sup>14</sup> According to the evidence JBZ attached to his complaint, the senders represented themselves as collection agents of Metrobank through email and Short Message Service (SMS):

1. By email dated 03 September 2020, from a certain RS, MIS, representing Cendana Neri Credit and Collection Services;<sup>15</sup>
2. By Short Message Service (SMS) dated 08 September 2020, from LE , representing Bernales & Associates;<sup>16</sup>
3. By email dated 08 December 2020, from GM representing Anonuevo Credit and Collection Services, Inc. (ACCSI Cebu);<sup>17</sup> and
4. By email dated 15 November 2020, from ET representing Admerex Solutions.<sup>18</sup>

JBZ claimed that he also received scam offers from the Pacquiao Foundation through SMS<sup>19</sup> and one AP through a Facebook message.<sup>20</sup>

JBZ also alleged that on 15 December 2020, he received an email from Metrobank informing him that his card ending in [ ] was being cancelled and that he should no longer use it to avoid inconvenience.<sup>21</sup> JBZ presented an email dated 14 December 2020 from “Collections – MCC [ ]”:

Dear Cardholder,

Please be informed we have cancelled your credit card privileges and we advise you to refrain from using the card ending in [ ] to avoid any inconvenience.

For inquiries, you may contact our representatives at [ ] or [ ] (toll free) during regular office hours or through [ ]

---

9 *Id.*  
10 *Id.*  
11 *Id.*  
12 *Id.*  
13 Complaints-Assisted Form, 08 February 2021, at 5, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).  
14 *Id.* Annex 4.  
15 *Id.* at 5.  
16 *Id.* Annex 7.  
17 *Id.* Annex 8.  
18 *Id.* Annex 9.  
19 Complaints-Assisted Form, 08 February 2018, Annex 12, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).  
20 *Id.* Annex 13.  
21 *Id.* Annex 10.

Sincerely,  
Collections Department  
**Consumer Business Sector**  
Metropolitan Bank & Trust Company<sup>22</sup>

JBZ categorically stated that he does not have a Metrobank card ending in [ ] “as [his Metrobank] Card ends in xxxx [ ].”<sup>23</sup> He likewise submitted a photocopy of his Metrobank Titanium Credit Card, which shows that its last four digits are [ ].<sup>24</sup>

JBZ alleged that the numerous anonymous emails and calls resulted in him being “practically in chaos and mentally tortured asking who really was/were trying to fool [him] or were trying to snare [him] in a scam.”<sup>25</sup>

JBZ prayed for “damages pursuant to the DPA,” and “for the appropriate complaint/case be filed against Metrobank Card Corporation for culpable violation” of Sections 19 and 20 of the DPA.<sup>26</sup>

On 10 September 2021, the Commission, through the Complaints and Investigation Division (CID), issued an Order directing Metrobank to file its Verified Comment within fifteen (15) days from receipt of the Order and to appear for preliminary conferences on 09 November 2021 and 07 December 2021.<sup>27</sup>

Metrobank filed its Verified Comment dated 23 September 2021.<sup>28</sup>

Metrobank claimed that it emailed JBZ, through CDR, to inform him that Metrobank “may possibly accept the offer as to Balance Restructuring Program.”<sup>29</sup> Metrobank explained that it did not grant JBZ’s request because could not be contacted through any of his numbers on record, and he failed to respond to the email.<sup>30</sup>

As of 07 April 2020, JBZ’s unpaid obligation on the Credit Card amounted to Eighty-eight Thousand Four Hundred Two Pesos (Php 88,402.00), with the minimum amount of Four Thousand Four Hundred Twenty Pesos and Ten Centavos (Php 4,420.10) due for payment on or before 28 April 2020.<sup>31</sup> Of the outstanding amount, Metrobank claimed JBZ only paid Two Thousand Pesos (Php 2,000.00).<sup>32</sup>

Metrobank explained that on 11 July 2020, it sent another letter to JBZ reminding him of his unpaid obligation.<sup>33</sup> It reminded JBZ of Section 30 of the Metrobank Terms and Conditions Governing the Issuance and Use of the Credit Card (Terms and Conditions), which provides:

---

22 *Id.* at 10.

23 *Id.* at 4.

24 *Id.* Annex 1.

25 Complaints-Assisted Form, 08 February 2021, at 5, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

26 *Id.* at 6-7.

27 Order, 10 September 2021, at 1, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

28 Comment, 23 September 2021, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

29 *Id.* at 2.

30 *Id.* at 2-3.

31 Complaints-Assisted Form, 08 February 2021, Annex 2, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

32 Comment, 23 September 2021, at 3, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

33 *Id.*

### 30. COLLECTION

a. ENDORSEMENT TO COLLECTION AGENCIES. The Card Member consents and authorizes Metrobank to process, share or transfer his/ her personal data to Metrobank's agency/ agent for collections should the account be referred to an agency/ agent for collection activity.<sup>34</sup>

Metrobank stated that a cardholder “must agree to Section 30 prior to the usage of its credit card.”<sup>35</sup> Metrobank explained that JBZ already consented to such endorsement and authorized Metrobank to share his personal data should his account be referred to its collection agents, when he signed the Application Form.<sup>36</sup>

Metrobank claimed that the outsourcing of JBZ's account is valid under Republic Act No. 10870, or the Philippine Credit Card Industry Regulation Law (R.A. No. 10870).<sup>37</sup> R.A. No. 10870 provides:

*Section 21. Endorsement of Credit Card Debt Collection by the Credit Card Issuer to a Collection Agency.* A credit card issuer shall inform its cardholder in writing of the endorsement of the collection of the account to a collection agency, or the endorsement of the account from one collection agency to another, prior to the actual endorsement. The notification shall include the full name of the collection agency and its contact details. The requirement to notify a cardholder in writing about the endorsement of the account to the collection agency shall be included in the terms and conditions of the credit card agreement: Provided, That the credit card issuer shall refer the collection of an account to only one collection agency at any one time.<sup>38</sup>

Metrobank argued that even in the absence of Section 21 of R.A. No. 10870, Section 14 of the DPA recognizes outsourcing of personal data:

*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.<sup>39</sup>

Metrobank also cited NPC Advisory Opinion 2018-15<sup>40</sup> to support its argument:

Whether processing is based on consent, law, or some other criteria for lawful processing, the PIC is not required to obtain a separate consent from the data subject before entering into an outsourcing agreement as the purpose of the processing remains to be the same and the PIC remains to be the same.

...

---

34 *Id.*  
35 *Id.*  
36 *Id.*  
37 *Id.* at 3-4.  
38 Comment, 23 September 2021, at 3-4, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).  
39 *Id.* at 10.  
40 See National Privacy Commission, Re: Consent Requirement on Outsourcing Agreement with an External Service Provider, Advisory Opinion No. 15, Series of 2018, at 2 (12 April 2018).

Nevertheless, considering the right of data subjects to be informed and notified of the processing of their personal data, the PIC must indicate in its privacy notice or privacy policy the particular data processing activities that are outsourced.<sup>41</sup>

Metrobank claimed that its collection agents are “governed by the same strict level of privacy policy with the Bank”, which includes the secure storage of information and deletion of information once the service has been performed.<sup>42</sup> Metrobank also stated it referred JBZ’s account to only one collection agency at any one time.<sup>43</sup>

Metrobank further argued that JBZ failed to discharge the burden of proving the messages resulted from a data breach on Metrobank’s part:

25. Here, the Complainant merely assumed that he began receiving anonymous calls and emails after Metrobank endorsed his account to the collection agencies, without establishing:

- a. How a breach occurred from the side of Metrobank;
- b. The connection between the anonymous messages from Pacquiao Organization, AP, and DOH, which are obviously sent in random; and
- c. The details as to how each of the privacy offenses were committed by Respondents Metrobank/Ms. CDR.

26. It appears that Complainant himself is not even certain about his charges to Metrobank, as he cannot specify when and how the alleged “data breach” occurred. All he knows is that there are anonymous emails and calls, and he concluded (without aptly describing how) that it is Metrobank’s fault.<sup>44</sup>

Metrobank noted that JBZ, without settling his dues, sent an email on 26 August 2020.<sup>45</sup> Metrobank stated that JBZ claimed that he received “hundred [sic] calls from unknown callers”<sup>46</sup>alleging to be from Metrobank, and that he will only pay once the issue is cleared and he is assured his data privacy rights are not violated.<sup>47</sup> Metrobank argued, however, that these calls were from generic and unidentified numbers, with only one tagged as “MB”.<sup>48</sup> Metrobank also argued that even if the calls were from Metrobank, one to two calls a day with gaps in between is not, by its own, intrusive in nature.<sup>49</sup> Further, it stated that the scam messages from the Pacquiao Foundation and AP were widely known to be sent in random.<sup>50</sup>

Metrobank noted that the breach occurred in September 2020, but JBZ only filed the case in February 2021, or “after he was sternly reminded about his obligation to pay and cancellation of his credit card perks.”<sup>51</sup>

Metrobank concluded that JBZ failed to show a data breach on its part, and that “his intention to file the instant case is certainly not to admonish Metrobank for the data

---

41 Comment, 23 September 2021, at 10-11, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

42 *Id.* at 4.

43 *Id.*

44 *Id.* at 8.

45 *Id.* at 4.

46 *Id.* at 4-5.

47 Comment, 23 September 2021, at 4-5, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

48 *Id.* at 5.

49 *Id.*

50 *Id.*

51 *Id.* at 5-6.

breach (because there is none), but for a purpose that would only serve the convenience of [JBZ].”<sup>52</sup>

Further, Metrobank argued that JBZ failed to state a cause of action against CDR.<sup>53</sup> Metrobank explained that CDR’s name was only mentioned in the complaint as the one who sent the letter dated 18 March 2020 on behalf of Metrobank and that there were no other claims on CDR’s involvement in the alleged data breach.<sup>54</sup>

Metrobank argued that none of the circumstances in Section 34 of the DPA on the liability of responsible officers applies to CDR.<sup>55</sup> Metrobank claimed that she only signed the letter for and on behalf of Metrobank.<sup>56</sup> Metrobank concluded that it would be unjust to drag the name of a bank officer without clear basis on her involvement in the alleged violations of the DPA.<sup>57</sup>

Metrobank also argued that it is not liable for violating Section 26 (Access Due to Negligence), Section 27 (Improper Disposal), Section 31 (Malicious Disclosure), and Section 32 (Unauthorized Disclosure) of the DPA.<sup>58</sup> Metrobank maintained that it disclosed JBZ’s information to its collection agents with his consent, and that JBZ neither raised clear allegations nor presented evidence to substantiate his allegations.<sup>59</sup>

Metrobank argued it is not liable for Section 26 (Access due to Negligence):

45. In the absence of clear allegations and evidence as to how Metrobank disregarded its duty to protect Complainant’s personal data resulting in carelessness or indifference, or how Metrobank failed to give proper attention to the Personal Data that it is handling, Complainant’s claim is certainly bereft of merit.<sup>60</sup>

Metrobank also argued it is not liable for Section 27 (Improper Disposal):

47. Metrobank has defined policies on how to dispose its personal data, being an institution highly-regulated by the Bangko Sentral ng Pilipinas. Both hard copies and soft copies are being disposed in accordance with standards acceptable to the BSP, and for a period of five years from the closure of the account.<sup>61</sup>

Metrobank argued that it is not liable for Section 31 (Malicious Disclosure):

50. In “**Manila Bulletin Publishing Corporation vs. VD**”, the Supreme Court defined malice as:

“Malice 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. **Malice is bad faith or bad motive.** It is the essence of the crime of libel.” (Emphasis supplied)

---

52 *Id.*  
53 Comment, 23 September 2021, at 11-12, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).  
54 *Id.* at 12.  
55 *Id.*  
56 *Id.*  
57 *Id.*  
58 *Id.*  
59 Comment, 23 September 2021, at 12-15, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).  
60 *Id.* at 12-13.  
61 *Id.* at 13.

51. As culled from the above case, for a disclosure to be malicious under Sec. 31 of the DPA, the same must be attended with bad motive or bad faith.

52. Conversely, disclosure of Complainant's information to the collection agents is simply for the purpose of **collecting his unpaid balance**, pursuant to Sec. 30 of the Terms and Conditions, Sec. 21 of R.A. 10870, and Sec. 14 of the DPA.

53. Since there are clear grounds on why the said disclosure was made, the same could not fall as "malicious". Again, the claim of the Complainant falls short of any legal basis.<sup>62</sup>

Finally, Metrobank argued that it is also not liable for Section 32 (Unauthorized Disclosure):

54. For this offense to be considered as Unauthorized Disclosure, the disclosure must not be supported by any legal basis.

55. In contrast, Complainant agreed to the Terms and Conditions of the Credit Card, which allows disclosure of his personal data to Metrobank's collection agents, as shown by the frequency of his usage.

56. Again, the said disclosure is likewise supported by Sec. 21 of R.A. 10870 and Sec. 14 of the DPA.

57. As such, it is clear that there are both CONSENT and LEGAL BASIS under the law on the disclosure made by Metrobank. The contentions of the Complainant are hence, bereft of merit.<sup>63</sup>

Metrobank's arguments against JBZ's allegation of its violation of the DPA hinged on the insufficiency of JBZ's evidence to support his allegation. It prayed that the complaint be dismissed and that other reliefs as may be just and equitable be granted.<sup>64</sup>

On 09 November 2021, Metrobank, through counsel, appeared for the first preliminary conference and expressed its willingness to undergo mediation proceedings.<sup>65</sup> JBZ, however, did not appear and instead informed the Commission that he was experiencing technical difficulties due to heavy rains.<sup>66</sup>

On 07 December 2021, both parties appeared and manifested that they will not require any documents and evidence from each other.<sup>67</sup> JBZ manifested that he was not willing to undergo mediation proceedings and that he will be adopting his notarized complaint and the attached evidence as his Memorandum.<sup>68</sup>

On 07 December 2021, the CID directed Metrobank to file its Memorandum within fifteen (15) calendar days from receipt of the Order.<sup>69</sup>

On 17 December 2021 Metrobank filed its Memorandum where it restated the state-

62 *Id.* at 13-14.

63 *Id.* at 14.

64 *Id.* at 15.

65 Order after the 1st Preliminary Conference, 09 November 2021, at 1, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

66 Fact-Finding Report, 13 January 2022, at 3, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

67 *Id.*

68 *Id.*

69 *Id.*

ments and arguments it previously presented in its Comment.<sup>70</sup>

On 03 June 2022, Metrobank submitted its Manifestation and Compliance dated 03 June 2022, and attached the version of the Terms and Conditions and the Certified True Copy of the Application Form that were signed by JBZ in response to the CID's Order dated 27 May 2022.<sup>71</sup> Metrobank manifested that as a practice, its clients only sign the Application Form containing the undertaking and declaration.<sup>72</sup> Since JBZ signed his Application Form, he consented to be bound by the Terms and Conditions.<sup>73</sup>

### Issues

I. Whether Metrobank's outsourcing of the collection of unpaid accounts is a violation of the DPA;

II. Whether there is substantial evidence to find Metrobank and CDR liable for a violation of the DPA.

### Discussion

#### **I. Metrobank's outsourcing of the collection of unpaid accounts is not a violation of the DPA.**

Metrobank is not liable for outsourcing JBZ's unsettled account to its collection agents.

Outsourcing by an issuing bank of a credit card holder's unpaid account to its collection agents is allowed under Section 14 of the DPA. Section 14 of the DPA provides:

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.<sup>74</sup>

Section 43, Rule X of the Implementing Rules and Regulations of the DPA (IRR) provides that a Personal Information Controller (PIC) shall use contractual or other reasonable means to ensure proper safeguards are in place:

Section 43. *Subcontract of Personal Data.* **A personal information controller may subcontract or outsource the processing of personal data:** Provided, that the personal information controller shall use **contractual or other reasonable means** to ensure that proper safeguards are in place, to ensure the confidentiality, integrity

---

<sup>70</sup> *Id.*

<sup>71</sup> Manifestation and Compliance, 03 June 2022, Annex A, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

<sup>72</sup> Memorandum, 09 June 2022, at 2, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

<sup>73</sup> Manifestation and Compliance, 03 June 2022, at 2, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

<sup>74</sup> 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 § 14 (2012). Emphasis supplied.



and availability of the personal data processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the Act, these Rules, other applicable laws for processing of personal data, and other issuances of the Commission.<sup>75</sup>

The outsourcing or subcontracting of the processing of personal data to third parties is permitted under the DPA and its IRR. In such cases, a PIC, such as Metrobank, is accountable for the actions of collection agents, or its Personal Information Processors (PIP). The PIC also remains responsible for ensuring the confidentiality of the personal data processed, prevention of any unauthorized processing, and compliance with relevant laws.<sup>76</sup>

Section 21 of the DPA provides for the Principle of Accountability and concomitant obligations of PICs:

Section 21. *Principle of Accountability.* **Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing**, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(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.<sup>77</sup>

A PIC does not need to secure separate consent from the data subject before subcontracting or outsourcing the processing of personal information to a PIP, provided the purpose for processing remains the same. Under an outsourcing agreement, a PIP merely carries out the processing under the instruction of the PIC and with the safeguards set by the same pursuant to Section 14 of the DPA<sup>78</sup> and Section 43, Rule X of the IRR, and taking into consideration the Principle of Accountability provided in Section 21 of the DPA.<sup>79</sup> As such, the initial consent to process personal information secured by the PIC from the data subject is sufficient for purposes of entering a subcontracting or outsourcing agreement

Here, Metrobank's purpose in outsourcing was to enforce its right against JBZ to recover his unpaid obligation. The purpose for processing JBZ's personal data remained the same when Metrobank outsourced the collection to its PIPs.

In any case, JBZ also failed to show that he had no knowledge of the outsourcing. In several instances, Metrobank informed JBZ that his account was overdue and that it had been endorsed for collection:

---

<sup>75</sup> Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012" [Implementing Rules and Regulations of the Data Privacy Act of 2012], IRR of Republic Act No. 10173 rule X, § 43 (2016). Emphasis supplied.

<sup>76</sup> *Id.*

<sup>77</sup> Data Privacy Act of 2012, § 21. Emphasis supplied.

<sup>78</sup> *Id.* § 1.

<sup>79</sup> *Id.* § 2.

1. the email dated 18 March 2020 to JBZ from Metrobank dated reminding him of his unpaid account and informing him of their attempts to contact him by phone call<sup>80</sup>;
2. the Statement of Account dated 7 April 2020 reminding JBZ of his unpaid account<sup>81</sup>;
3. the System-Generated Letter dated 11 July 2020 similarly reminding JBZ of his unpaid account<sup>82</sup> that Metrobank attached it to its Memorandum filed on 17 December 2021.

Given the foregoing, Metrobank's referral of JBZ's account to its PIPs pursuant to an outsourcing agreement is permitted under the DPA.

## **II. There is no substantial evidence to find Metrobank and CDR liable for a violation of the DPA.**

Metrobank and CDR cannot be held liable for violation of the DPA based on the allegations and evidence submitted by JBZ.

JBZ claims that as a result of a breach on the part of Metrobank, his personal data was disclosed without authorization and he was subjected to numerous anonymous emails, calls, and scam offers that caused him distress.<sup>83</sup> He alleged Metrobank was liable for violation of Section 26 (Access due to Negligence), Section 27 (Improper Disposal), Section 31 (Malicious Disclosure), and Section 32 (Unauthorized Disclosure).<sup>84</sup> To substantiate his complaint, JBZ submitted his e-mail correspondences with Metrobank,<sup>85</sup> a copy of the System-Generated Letter reminding him of his unpaid obligation,<sup>86</sup> screenshots of text messages and emails from collection agents,<sup>87</sup> of call logs from untagged numbers,<sup>88</sup> and scam messages from the Pacquiao Foundation<sup>89</sup> and AP.<sup>90</sup>

Section 1 of Rule 131 of the 2019 Amendments to the Revised Rules on Evidence provides:

Section 1. *Burden of proof and burden of evidence.* Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim or defense by the amount of evidence required by law.

Burden of proof never shifts. Burden of evidence is the duty of a party to present evidence sufficient to establish or rebut a fact in issue to establish a prima facie case. Burden of evidence may shift from one party to the other in the course of the proceedings, depending on the exigencies of the case.<sup>91</sup>

80 Complaints-Assisted Form, 08 February 2021, Annex 3, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

81 *Id.* Annex 2.

82 Memorandum by the Respondent, 17 December 2022, Annex A, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-222 (NPC 2021).

83 Complaints-Assisted Form, 08 February 2021, at 5, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

84 *Id.* at 3.

85 *Id.* Annex 1, Annex 3, and Annex 5.

86 *Id.* Annex 2.

87 *Id.* Annex 7-9.

88 *Id.* Annex 4.

89 Complaints-Assisted Form, 08 February 2021, Annex 12, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

90 *Id.* Annex 13.

91 2019 AMENDMENT TO THE 1989 REVISED RULES ON EVIDENCE, A.M. No. 19-08-15-SC, Rule 131, § 1 (1 May 2020).

Section 6 of Rule 133 of the 2019 Amendments to the Revised Rules on Evidence provides:

Section 6. *Substantial Evidence.* In cases filed before administrative or quasi-judicial bodies, a fact may be deemed established if it is supported by substantial evidence, or that amount of relevant evidence which a reasonable mind might accept as adequate to justify a conclusion.<sup>92</sup>

In this case, JBZ, as the complainant, has the burden of proof in alleging violation of the DPA. He did not discharge this, however, as he failed to support his allegations with substantial evidence.

JBZ could have utilized the discovery proceedings during preliminary conference to obtain other pieces of evidence to substantiate his allegations. Rule V, Section 1 of the 2021 NPC Rules of Procedure provides:

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.<sup>93</sup>

Discovery proceedings are essential, such as in this case, where the complainant cannot simply rely on the evidence it has to properly substantiate its allegations. The Supreme Court held:

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.<sup>94</sup>

The Supreme Court explained the purpose of discovery proceedings:

What is chiefly contemplated is the discovery of every bit of information which may be useful in the preparation for trial, such as the identity and location of persons having knowledge of relevant facts; those relevant facts themselves; and the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things.<sup>95</sup>

The evidence that JBZ could have presented to prove the existence of a privacy violation and Metrobank's supposed liability are most likely in the hands of Metrobank, such as evidence of the outsourcing agreement with collection agencies and details surrounding the outsourcing of the collection of JBZ's unpaid obligations.

---

92 *Id.* § 6.

93 National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC 2021 Rules of Procedure], rule IV, § 1 (28 January 2021). Emphasis supplied.

94 *BSA Tower Condominium Corp. v. Reyes II*, A.C. No. 11944 (2018).

95 *Producers Bank of the Philippines v. Court of Appeals*, G.R. No. 11049 (1998).

The documents attached to his complaint can only serve to prove that Metrobank and its collection agents were attempting to collect on his unpaid obligation incurred using the credit card. The CAF and attached documents do not show, nor does JBZ even allege, any connection between Metrobank’s outsourcing of his account and the supposed data breach that resulted in a violation of Section 26 (Access due to Negligence), Section 27 (Improper Disposal), Section 31 (Malicious Disclosure), and Section 32 (Unauthorized Disclosure). In the absence of any substantial evidence, the connection between any supposed action or inaction on the part of Metrobank and the numerous anonymous emails, calls, and scam offers that JBZ alleged to have caused him distress with is only speculative.

Instead of availing himself of discovery proceedings during the preliminary conference to seek additional information and documents from Metrobank to substantiate his claims, JBZ merely relied on the insufficient evidence he submitted with his complaint.<sup>96</sup> Thus, Metrobank cannot be held liable for the violating the DPA.

Aside from Metrobank, JBZ also impleaded CDR as a respondent in his complaint.<sup>97</sup> JBZ, however, failed to substantiate CDR’s participation in Metrobank’s alleged violation of the DPA.

Under Section 34 of the DPA, an officer of a corporation, partnership, or any juridical person may be held liable if they participated in or allowed the commission of the crime by their gross negligence:

Section 34. *Extent of Liability.* If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and he or she is found guilty of acts penalized Under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.<sup>98</sup>

In this case, JBZ failed not only to allege, but also to submit evidence, that CDR was involved in Metrobank’s supposed violation of the DPA, either by her direct participation or by allowing the supposed violation to happen through her gross negligence.

CDR was mentioned only one time in the complaint:

3. On March 18, 2020 A certain CDR, VP Cards and Personal Credit Sector Metro Bank and Trust Company sent me an email informing me that my account had been endorsed to a collection agent but no specific names given; and without my approval (Annex 3)<sup>99</sup>

<sup>96</sup> Order (After the 2nd Preliminary Conference held on 07 December 2021, Granting the Adoption of the Complaint as Complainant’s Memorandum, and for the Respondent to Submit its Memorandum), at 1, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

<sup>97</sup> Complaints-Assisted Form, 08 February 2021, at 2, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

<sup>98</sup> Data Privacy Act of 2012, § 34.

<sup>99</sup> Complaints-Assisted Form, 08 February 2021, at 3, in JBZ v. Metropolitan Bank & Trust Company, CDR as VP Cards and Personal Credit Sector, NPC 21-122 (NPC 2021).

Other than this statement, JBZ neither specified nor discussed the provisions of the DPA that CDR supposedly violated. He failed to specify whether she is liable for violating the same provisions of the DPA as Metrobank, or liable for an entirely different violation.

Further, Section 34 of the DPA assumes that the PIC committed a violation of the provisions of the DPA when its responsible officers are held liable.<sup>100</sup> Thus, CDR cannot be held liable as a responsible officer of Metrobank under Section 34 of the DPA.

Given the lack of substantial evidence presented by JBZ, the Commission cannot find Metrobank and CDR liable for violating the DPA. JBZ failed to prove that Metrobank committed a violation of the DPA through the allegations in his complaint or by the evidence he submitted. He likewise failed to prove that CDR was responsible for any violation of the DPA, whether in her official or personal capacity.

The Commission also cannot award damages to JBZ for the erroneous email from Metrobank regarding the cancellation of another client's credit card. While Metrobank sent the wrong email to JBZ, it neither contained personal information of another card holder nor involved JBZ's personal information. As such, the Commission has no reason to award damages to JBZ.

Nevertheless, the Commission sternly warns Metrobank to ensure that proper safeguards are in place when referring unpaid accounts such as JBZ's to its collection agents, and that the processing of personal information is accurate and up to date following Section 11 of the DPA:

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 proportionality.

Personal information must, be:

...

**(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[.]**<sup>101</sup>

The Commission also sternly reminds Metrobank that it remains responsible for the processing of its clients' personal information. While Metrobank claims to be compliant with the proper requirements under the law, it is nevertheless duty-bound as a PIC to remind its collection agents, as PIPs, to ensure compliance with the DPA and related laws. Metrobank remains responsible for the outsourced processing of personal information and will be held accountable for any data breach, even if the personal data involved was outsourced to its collection agents for processing.

100 Data Privacy Act of 2012, § 34.

101 *Id.* Emphasis supplied.

**WHEREFORE**, premises considered, this Commission resolves that the instant Complaint filed by JBZ against Metropolitan Bank & Trust Company and CDR as VP Cards and Personal Credit Sector is hereby **DISMISSED** for lack of merit.

This is without prejudice to the filing of an appropriate civil, criminal, or administrative case before any other forum or tribunal, if any.

**SO ORDERED.**

City of Pasay, Philippines.  
19 January 2023.

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

**Sgd.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**Sgd.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

Copy furnished:

**JBZ**  
*Complainant*

**METROPOLITAN BANK & TRUST COMPANY**  
**OFFICE OF THE GENERAL COUNSEL**  
*dataprotectiondept@metrobank.com.ph*

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

**MCD,**

*Complainant,*

**NPC 19-758**

For: Violation of the  
Data Privacy Act of  
2012

-versus-

**VICTORIAS MILLING COMPANY,  
MOC, EVR, GEK,  
AND SC,**

*Respondent.*

X-----X

**JJD,**

*Complainant,*

**NPC 19-1846**

For: Violation of the  
Data Privacy Act of  
2012

-versus-

**VICTORIAS MILLING COMPANY,  
MOC, EVR, GEK,  
AND SC,**

*Respondent.*

X-----X

## **DECISION**

### **AGUIRRE, D.P.C.;**

Before this Commission are the consolidated cases filed by Spouses MCD and JJD (collectively, Complainants) against Victorias Milling Company (VMC), MOC, EVR, GEK, and SC (Respondents) for alleged violations of Section 25 (Unauthorized Processing), Section 26 (Access due to Negligence), Section 28 (Processing for Unauthorized Purposes), Section 29 (Unauthorized Access or Intentional Breach), Section 31 (Malicious Disclosure), Section 32 (Unauthorized Disclosure), and Section 33 (Combination or Series of Acts) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

### **Facts**

Complainants were employees of VMC.<sup>1</sup> MCD narrated that during his employment as Head of the Asset Management Department from January 2016 to May 2018, VMC required him to submit a Disclosure Statement of all his financial interests and that of the members of his family up to the second degree of consanguinity or affinity.<sup>2</sup> This included a declaration of “the sugarcane farms [he] owned, leased, or managed, and the businesses that [he] and [his] family members may have an interest in that deals

<sup>1</sup> Complaint-Affidavit of MCD y C, 27 June 2019, at 1, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

<sup>2</sup> *Id.*

with VMC.”<sup>3</sup> JJD, as the Administrative Assistant of the Asset Protection and Safety Department, was also required to submit a Disclosure Statement with the same contents.<sup>4</sup>

Complainants explained that “the Disclosure Statement is a highly sensitive document which contained [their] private matters which could not be disclosed or published without [their] knowledge and consent.”<sup>5</sup> He further stated that the submission of the Disclosure Statement does not give VMC the right to process their personal data contained in the document.<sup>6</sup>

In January 2018, Complainants claimed that Respondents conducted field investigations, verifications, inspections, interviews, and inquiries to validate the sugarcane farms that they declared in their Disclosure Statements.<sup>7</sup> Complainants alleged that GEK, one of the respondents, surreptitiously took and carried away the sugarcane that they already harvested.<sup>8</sup> They also contended that GEK submitted to VMC her observations and findings that two haciendas located in the municipality of E.B. Magalona were not declared in the Disclosure Statements of the Complainants.<sup>9</sup> They further alleged that GEK discovered that Complainants are “in the business of financing the farming activities of certain sugarcane planters who bring their produce to VMC for milling.”<sup>10</sup>

As a result, Complainants received Notices to Explain directing them to explain the alleged violations of the VMC Employee Code of Conduct and Discipline and other VMC Policy and Procedures.<sup>11</sup> As stated in the Notices, Complainants, as VMC employees, held “positions that can exert influence on other VMC employees and workers to [their] benefit and advantage, hence at the least, [their] disclosures became imperative as [their] personal business transactions could have run in conflict with [their positions].”<sup>12</sup>

In their Written Explanations, Complainants stated that when they submitted their Disclosure Statements in October 2017, the two haciendas were no longer leased nor operated by them.<sup>13</sup> They explained that the contracts of lease for both farms had already expired in 2013.<sup>14</sup> MCD also explained that financing the farming activities of sugarcane planters, buying standing and cut sugarcanes, and delivering them to VMC for milling does not amount to a conflict of interest.<sup>15</sup> In his Complaint-Affidavit, MCD added that as far as he knows, VMC does not engage in buying standing sugarcanes.<sup>16</sup>

Despite their explanations, Complainants received Notices of Suspension from VMC, suspending them for seven (7) days for “blatant disregard or any deviation from estab-

---

3 *Id.*  
4 Complaint-Affidavit of JJD y J, 27 June 2019, at 1, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).  
5 Complaint-Affidavit of MCD y C, 27 June 2019, at 2, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 2, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).  
6 *Id.* at 3; *Id.*  
7 *Id.* at 2; *Id.*  
8 *Id.*  
9 *Id.*  
10 *Id.* Annex C; *Id.* Annex C;  
11 Complaint-Affidavit of MCD y C, 27 June 2019, at 3, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 2, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).  
12 *Id.* Annex C; *Id.* Annex C;  
13 *Id.* Annex D; *Id.* Annex D;  
14 *Id.* at 3; *Id.* at 3.  
15 Explanation of MCD Complaint-Affidavit of MCD y C, 27 June 2019, Annex D, in Sps. MCDJJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).  
16 Explanation of MCD Complaint-Affidavit of MCD y C, 27 June 2019, Annex D, in Sps. MCDJJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).



lished control and other VMC Policies and Procedures.”<sup>17</sup> They were also not allowed to mill their sugarcanes with VMC.<sup>18</sup>

Because of this, MCD requested a grievance conference.<sup>19</sup> In his Request for Grievance, MCD argued that it was not clear in the Notice of Suspension what specific policies and procedures were disregarded by him that would merit his suspension.<sup>20</sup> He further argued that the Disclosure Statement “does not even state the corresponding sanction in case of incomplete or erroneous statement.”<sup>21</sup> Finally, he argued that the investigation in relation to his Disclosure Statement was performed without his knowledge and consent.<sup>22</sup>

Complainants explained that despite the valid grounds they alleged, VMC disregarded their explanations and decided to suspend them and disallow them from milling sugar until further notice.<sup>23</sup> Because of this, Complainants claimed that they were “forced to render [their] voluntary resignation from employment.”<sup>24</sup>

Due to the incident, Complainants filed their respective ComplaintAffidavits dated 27 June 2019, against Respondents for violations of the DPA.<sup>25</sup>

Complainants alleged that VMC violated the DPA when Respondents conducted an investigation and validation of the sugarcane farms that they stated in their Disclosure Statements without their knowledge and consent.<sup>26</sup> They prayed for the Commission to find Respondents guilty of violations of the DPA.<sup>27</sup> They also claimed that they are entitled to moral damages, exemplary damages, and attorney’s fees.<sup>28</sup>

On 18 December 2020, the National Privacy Commission (NPC), through its Complaints and Investigation Division (CID), consolidated the two (2) cases and directed the parties to Confer for Discovery.<sup>29</sup>

On 11 March 2021, Respondents filed their Entry of Appearance.<sup>30</sup>

On 23 March 2021, only Complainants, through their representative, appeared for the discovery conference, while Respondents failed to appear.<sup>31</sup> Complainants manifested that they are not willing to reset the discovery conference.<sup>32</sup> Thus, in view of Complain

---

17 *Id.* at 4; *Id.* at 4.

18 *Id.*

19 Request for Grievance dated 17 February 2018, Complaint-Affidavit of MCD y C, 27 June 2019, Annex F, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

20 *Id.*

21 *Id.*

22 *Id.*

23 Complaint-Affidavit of MCD y C, 27 June 2019, at 4, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

24 Complaint-Affidavit of MCD y C, 27 June 2019, at 4, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 3-4, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

25 *Id.*

26 *Id.*

27 *Id.* at 5; *Id.* at 4-5.

28 *Id.*

29 Order to Confer for Discovery, 10 February 2021, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

30 Order to Confer for Discovery, 10 February 2021, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

31 Order to Confer for Discovery, 10 February 2021, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

32 *Id.*

ants’ manifestation and the effectivity of NPC Circular 2021-01 (2021 NPC Rules of Procedure),the CID ordered Respondents to file their verified comment within fifteen (15) days from receipt of the Order.<sup>33</sup>

On 30 September 2021, the CID issued an Order stating that it has not received a verified comment from Respondents.<sup>34</sup> As a result, to give due course to the cause of both parties, it gave Respondents a final period of fifteen (15) days from receipt of the Order to file its verified comment to the complaint.<sup>35</sup>

On 18 October 2021, Respondents filed their Consolidated Comment.<sup>36</sup>

In their Consolidated Comment, Respondents explained that in the course of its business operations, it collects, uses, and processes the personal data of its employees, consultants, visitors, clients, and other stakeholders.<sup>37</sup>

Respondents claimed that VMC believes in the importance of good corporate governance as part of sound strategic management.<sup>38</sup> Therefore, they undertake the necessary efforts to create awareness and ensure compliance with the same, which includes the creation of the Manual on Corporate Governance.<sup>39</sup>

Further, Respondents explained that VMC, as a publicly listed corporation, must comply with the Securities and Exchange Commission Code of Corporate Governance for Publicly Listed Companies under SEC Memorandum Circular 19 Series of 2016 which provides for “the adoption of programs that mitigate corrupt practices such as but not limited to bribery, fraud, extortion, collusion, conflict of interest and money laundering.”<sup>40</sup>

Respondents stated that as part of its compliance with the SEC’s Memorandum Circular 19 Series of 2016, guided by its Manual on Corporate Governance and pursuant to good corporate governance, it required all of its employees and consultants to execute the VMC Disclosure Statement yearly or as often as required.<sup>41</sup> The disclosure was designed “to prevent and address any actual or potential conflict of interest that may adversely affect the interest of the company and its stakeholders, such as personal dealings between employees, consultants and VMC.”<sup>42</sup>

Through its Disclosure Statements, Respondents explained that it collects from each employee and consultant his or her name, position, VMC ID number, other positions held outside VMC, names of family members related to any director, officer, employee, or consultant of VMC group, relationships, and signature.<sup>43</sup>

Respondents then narrated that in early 2018, VMC conducted a validation of the in-

---

33 *Id.*

34 Order (To File Verified Comment and Appear Virtually for Preliminary Conference), 27 September 2021, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

35 *Id.*

36 Order (To File Verified Comment and Appear Virtually for Preliminary Conference), 27 September 2021, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

37 *Id.*

38 *Id.*

39 *Id.*

40 *Id. at 3*

41 *Id. at 2.*

42 Consolidated Comment, 18 October 2021, at 2, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

43 *Id. at 3*

formation contained in the submitted Disclosure Statements.<sup>44</sup> It then discovered that “there were certain sugarcane farms and financing activities linked to Complainants that were not divulged in their Disclosure Statements.”<sup>45</sup> Hence, in accordance with its company procedures and the Labor Code of the Philippines, it initiated its internal administrative process which resulted in the suspension of Complainants.<sup>46</sup>

Respondents alleged that during the entire process of investigation, assessment, and action about Complainants, they complied with the DPA and other applicable laws.<sup>47</sup> They explained that “to maintain the confidentiality of personal data, only authorized personnel whose functions included participation in the conduct of internal administrative proceedings under the Labor Code (i.e., HR, Legal, Audit) were given access to information which includes the other respondents.”<sup>48</sup> They further alleged that the individual respondents only carried out their tasks by virtue of their positions as officers or employees of VMC.<sup>49</sup>

For her part, Ms. GEK has authority to access personal information in relation to the Disclosure Statement as Head of the Transformation Department and Internal Audit being that she is responsible in auditing information/processes and providing reports thereon that could adversely affect the business of VMC, one of which is the violation of the company’s policy on conflict of interest. For their part, Ms. MOC, Ms. EVR and Ms. SC have authority to access personal information being signatories of the Notice to Explain and other necessary processes by the company.<sup>50</sup>

They claimed that prior to the effectivity of Complainants’ resignation, they had amicable discussions and considered their demands.<sup>51</sup> After negotiation, both Complainants received a sum of money, that is One Million Five Hundred Thousand Pesos (Php 1,500,000.00) for MCD and Five Hundred Thousand Pesos (Php 500,000.00) for JJD.<sup>52</sup> On 26 April 2018, Complainants also executed a Release, Waiver and Quitclaim on account of the received settlement.<sup>53</sup>

On 28 June 2019, the Respondents disclosed that VMC filed before the Regional Trial Court of Silay a complaint for breach of contract against Complainants.<sup>54</sup> It was after the filing of the aforementioned complaint that the Respondents discovered the present case filed before the Commission.<sup>55</sup>

Respondents argued that the complaint should be dismissed on the grounds that Complainants are guilty of forum shopping, that the claim or demand set forth in the complaint has been paid, waived, abandoned, or otherwise extinguished, and that the complaint lacks merit.<sup>56</sup>

Respondents contended that the information contained in the Disclosure Agreement

---

44 *Id.*  
45 *Id.*  
46 *Id.*  
47 *Id. at 4.*  
48 Consolidated Comment, 18 October 2021, at 4, in *Sps. MCD-JJD v. Victorias Milling Company*, NPC 19-758 & 19-1846 (NPC 2021).  
49 *Id. at 3.*  
50 *Id. at 19.*  
51 *Id. at 4.*  
52 *Id.*  
53 *Id.*  
54 *Id.*  
55 *Id. at 6.*  
56 *Id.*

only pertained to personal information as defined under the DPA and their processing was based on contracts under Section 12 (b), compliance with a legal obligation under Section 12 (c), and legitimate interest under Section 12 (f) of the DPA.<sup>57</sup>

They explained that the processing of personal data was based on a contract.<sup>58</sup> Further, they stated that at the time of processing, an employment relationship existed between them and Complainants which is governed by an employment contract.<sup>59</sup> This allows them to process certain information that are necessary and related to the fulfilment of the contract:

*Processing of personal data based on contract*

It is of no issue that there is an employment relationship between Complainants and VMC at the time when the processing of the personal information was done. Such relationship is governed by the contract entered into by the parties. In an employment relationship, certain information are processed which are necessary and is related to the fulfillment of the contract between the parties. Such information includes personal data which is needed to benefit the employee like those data needed to process salary as well as those for the benefit of the employer, VMC in this case, needed to protect its interest such as disclosures of information involving conflict of interest. When the Complainants entered into a contract with the respondent VMC, they were made aware that certain information will be collected and processed by the company, failure of which may result in the severance of their employment contract.<sup>60</sup>

They further stated that as a Personal Information Controller (PIC), VMC has a legal obligation to process personal data to comply with the law, especially since it is a publicly listed company subject to compliance with regulatory requirements, particularly SEC Memorandum Circular 19 Series of 2016:

*Processing of personal data based on legal obligation*

VMC, being a publicly listed company, is subject to certain legal obligations set out by its regulators. Regulatory requirements also qualify as a legal obligation.

In relation to the Disclosure Statement which is the subject of this present case, the pertinent issuance of the Securities and Exchange Commission, i.e., SEC Memorandum Circular No. 19, Series of 2016 applies. The said memorandum requires that the Company must adopt programs that mitigate corrupt practices such as but not limited to bribery, fraud, extortion, collusion, conflict of interest and money laundering. As previously stated, the VMC Disclosure Statement is part of VMC's compliance to the said SEC-mandated Code of Corporate Governance for Publicly-Listed Companies which is designed to prevent and address any actual or potential conflict of interest that may adversely affect the interest of the company and its stakeholder such as personal dealings between employees, consultants and VMC.<sup>61</sup>

They also stated that VMC has a legitimate interest in processing Complainants' personal information, being a publicly listed company with a responsibility towards its in-

---

57 *Id. at 13.*

58 *Id. at 14.*

59 *Id.*

60 Consolidated Comment, 18 October 2021, at 14, in *Sps. MCD-JJD v. Victorias Milling Company*, NPC 19-758 & 19-1846 (NPC 2021).

61 *Id.*

vestors.<sup>62</sup> Also, part of its good corporate governance initiatives is “to ensure that all possible conflicts of interest of its employees and consultants are addressed.”<sup>63</sup> They explained that VMC processes personal information in relation to the Disclosure Statement to protect its legitimate interest of preventing fraud and violations of its policies which may affect the business:

*Processing of personal data based on legitimate interest*

In this case, the processing of the personal information contained in the Disclosure Statement is necessary for the purposes of the legitimate interest of VMC. VMC as a publicly listed company has a responsibility towards its investors. It holds its shareholders’ best interests as a priority and is committed in maintaining stockholder confidence and optimism at all times. Part of its good corporate governance initiatives is to ensure that all possible conflict interest of its employees and consultants are addressed. Hence, it has mandated all those connected to the company to submit their Disclosure Statements.

...

In this case, the processing of the personal information contained in the Disclosure Statement is based on the legitimate interest of the organization to prevent fraud and violation of its policies which may affect the business.<sup>64</sup>

Respondents argued that assuming the Disclosure Statements contained sensitive personal information, they still have lawful basis in processing the information because it is necessary for the protection of its lawful rights and interest pursuant to Section 13 (f) of the DPA.<sup>65</sup>

The act of Complainants in withholding information which VMC requires from all its employees and consultants gave rise for VMC to process the information in order to protect its lawful rights and interest and implement company policies.<sup>66</sup>

Respondents added that there was a need to assess whether Complainants can reasonably expect their data to be processed in such manner.<sup>67</sup> They argued that because of the employment contract entered into between the parties and VMC’s legitimate interest, Complainants have a lesser expectation of privacy in relation to the disclosures made by Complainants to VMC and its authorized persons.<sup>68</sup>

Respondents also contended that Complainants failed to particularly identify which information was processed and how the individual respondents were able to unlawfully access or disclose their information as they were performing such in their official capacity.<sup>69</sup>

Aside from mentioning Ms. GEK performing her function to validate the contents of the Disclosure Statement, Ms. EVR and Ms. SC as issuer and signatory of the Notice to Explain, Complainants did not give any material information which can substanti

---

62 *Id. at 15.*

63 *Id.*

64 *Id. at 15.*

65 *Id. at 16-17.*

66 Consolidated Comment, 18 October 2021, at 17, in *Sps. MCD-JJD v. Victorias Milling Company*, NPC 19-758 & 19-1846 (NPC 2021).

67 *Id.*

68 *Id. at 18.*

69 *Id. at 19.*

ate their allegation that respondents MOC, EVR, GEK and SC unlawfully processed, used or disclosed their personal data.<sup>70</sup>

Finally, Respondents alleged that “the allegations lack the necessary information to establish [Complainants’] claims and that indeed the crime alleged has been committed.”<sup>71</sup>

In relation to Sections 25, 28, and 32, Respondents stated that they have clearly explained that there was lawful basis in the processing of the information based on contract, legitimate interest and/or protection of lawful rights and interests, or the establishment, exercise, or defense of legal claims.<sup>72</sup> Therefore, the allegations that Respondents committed unauthorized processing, processing personal data for unauthorized purpose/s, and unauthorized disclosure must not prosper.<sup>73</sup>

As to Sections 26, 29, and 31, Respondents contended that the allegations do not provide for the acts or facts that result in a violation of these sections.<sup>74</sup> They argued further that the imputation that Respondents maliciously and fraudulently conducted the investigation to validate Complainants’ sugarcane farms is not within the purview of Sections 26, 29, and 31 of the DPA.<sup>75</sup> There was no allegation of disclosure of unwarranted or false information with malice or bad faith on the part of Respondents.<sup>76</sup>

Respondents thus averred that they did not violate Sections 25, 26, 28, 29, 31, 32, and 33 of the DPA and prayed for the dismissal of the complaint with prejudice for failure to substantiate and prove the allegations.<sup>77</sup>

During the 26 October 2021 preliminary conference, only Respondents appeared.<sup>78</sup> The CID noted the receipt of Complainants’ Urgent Motion for Postponement and the preliminary conference was reset for the last time.<sup>79</sup>

On 16 November 2021, during the Preliminary Conference, Complainants manifested that they are requesting for the minutes or records of the grievance proceedings held on 01 March 2018. Respondent’s counsel, however, raised the relevance which the document may serve as the same had nothing to do with the allegations in the complaint.<sup>80</sup> Complainants, through counsel, answered that the minutes of the grievance proceedings will show the basis of Complainants’ suspension and that some of Complainants’ vital records were violated.<sup>81</sup> Respondents opposed the production of the document considering that the grievance proceedings tackled a different matter and is not connected with data privacy.<sup>82</sup> As a result, the CID ordered Respondents to submit a Comment/Opposition to the Discovery of the Document.<sup>83</sup>

---

70 *Id.*

71 *Id. at 20.*

72 Consolidated Comment, 18 October 2021, at 20, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

73 *Id.*

74 *Id.*

75 *Id.*

76 *Id.*

77 *Id. at 2.*

78 Order, 26 October 2021, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

79 Fact-Finding Report, 29 December 2022, at 3, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

80 Order (After the Preliminary Conference on 16 November 2021), 16 November 2021, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

81 *Id.*

82 *Id.*

83 *Id. at 2.*

During the Preliminary Conference, both parties, however, manifested that they are willing to undergo mediation proceedings.<sup>84</sup> Therefore, the proceedings were suspended.<sup>85</sup>

On 19 and 20 November 2021, Respondents<sup>86</sup> and Complainants<sup>87</sup> respectively, signed and submitted their Applications for Mediation.

On 05 January 2022, the CID issued an Order to Mediate and for the parties to appear for a preliminary mediation conference.<sup>88</sup> The CID, however, ordered the termination of the mediation proceedings due to the parties' repeated delays in rescheduling the preliminary mediation conference for more than two (2) months.<sup>89</sup>

On 10 March 2022, the Mediation Officer issued a Notice of NonSettlement to the parties.<sup>90</sup> On 15 March 2022, the CID lifted the suspension of the complaints proceedings and ordered the parties to file their memoranda.<sup>91</sup> The CID also ordered Respondents to submit their Comment/Opposition to the Discovery of the Document.<sup>92</sup>

On 30 March 2022, Respondents submitted their Comment/Opposition to the Discovery of the Document dated 30 March 2021.<sup>93</sup> Respondents argued that the disclosure of the internal documents and communications, specifically the minutes of the grievance meeting, was "irrelevant, protected by a form of privilege, and must be excluded for legitimate reasons such as but not limited to internal policies, labor relations policy, dispute resolution rules, among others."<sup>94</sup>

The fact in issue in the instant case is the alleged violation sometime on or before 23 January 2018 and the Disclosure Statements. The minutes of the grievance meeting was on 18 March 2018 in relation to work suspension. Thus, the request has no bearing on the allegations in the complaint.<sup>95</sup>

On 01 April 2022, the CID noted the Respondents' Comment/Opposition to the Discovery of the Document.<sup>96</sup>

On 18 April 2022, Respondents filed their Memorandum.<sup>97</sup> They reiterated that aside from the bare allegations of Complainants, nothing in the complaint "provided any detail as to who among the Respondents processed personal data, what kind of personal

---

84 *Id.*

85 *Id.*

86 Application for Mediation, 19 November 2021, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

87 *Id.*

88 Order to Mediate, 05 January 2022, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

89 Notice of Non-Settlement of Dispute, 10 March 2022, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

90 *Id.*

91 Order (for Resumption of Complaints Proceedings, Requiring Respondents to Submit their Comment/Opposition to the Discovery of the Document, and Requiring the Parties to Submit their Simultaneous Memoranda), 15 March 2022, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

92 *Id.*

93 Comment/Opposition to Discovery of Document, 30 March 2022, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

94 *Id.* at 2.

95 *Id.* at 3.

96 Order (Noting the Comment/Opposition to Discovery of Document filed by Respondents), 01 April 2022, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

97 Memorandum for the Respondents, 18 April 2022, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

data, and how could they have used [the] personal data.”<sup>98</sup> Further, they restated their arguments that there was lawful processing based on contract, legal obligation, legitimate interest, and protection of lawful rights and interest <sup>99</sup>

On 11 August 2022, Complainants filed their Memorandum.<sup>100</sup> They maintained that the acts of Respondents in “processing, validating, spying, [and] publishing the contents of the Disclosure Statements of the complainants is a gross violation of the [DPA]” because the submission of their Disclosure Statements do not give Respondents absolute authority to process its contents.<sup>101</sup> Complainants further alleged that Respondents conducted their investigations and inquiries with bias because “they came up with an unverified report that is grossly erroneous, having no factual basis but hearsays and assumptions, full of malice and ill-intent.”<sup>102</sup>

### Issues

- I. Whether there is substantial evidence to find Respondents liable for a violation of the DPA;
- II. Whether Respondents’ act of processing the contents of the Disclosure Statements is a violation of the DPA.

### Discussion

The Commission dismisses the case for lack of substantial evidence.

Complainants failed to substantiate their allegations on how the Respondents violated the DPA. Other than the general statements made in their complaints and Memorandum, the Complainants neither specified the personal data that was unlawfully processed nor alleged the Respondents’ specific acts that amount to a violation of the DPA.

Nevertheless, Respondents’ acts of processing the contents of Complainants’ Disclosure Statements was pursuant to its legitimate interest and did not go beyond what Complainants can reasonably expect upon submission of their Disclosure Statements.

#### **I. There is no substantial evidence to find Respondents liable for a violation of the DPA.**

Respondents, who are VMC and its officers and employees, cannot be held liable for a violation of the DPA based on the allegations of and evidence submitted by Complainants.

Complainants claimed that Respondents violated Sections 25, 26, 28, 29, 31, 32, and 33 of the DPA by processing their personal data without their authority and consent.<sup>103</sup> To

---

98 *Id.* at 16.

99 *Id.* at 20-22.

100 Memorandum for Complainant, 20 July 2022, in *Sps. MCD-JJD v. Victorias Milling Company*, NPC 19-758 & 19-1846 (NPC 2022).

101 *Id.*

102 Memorandum for the Respondents, 18 April 2022, at 7, in *Sps. MCD-JJD v. Victorias Milling Company*, NPC 19-758 & 19-1846 (NPC 2022).

103 Complaint-Affidavit of MCD y C, 27 June 2019, at 5, in *Sps. MCD-JJD v. Victorias Milling Company*, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 5, in *Sps. MCD-JJD v. Victorias Milling Company*, NPC 19-758 & 19-1846 (NPC 2019).



substantiate their complaint, Complainants submitted their Disclosure Statements,<sup>104a</sup> a copy of the blotter report that records the incident where Respondent GEK surreptitiously took and carried away their sugarcane for milling,<sup>105</sup> the Notices to Explain issued by Respondents to MCD and JJD,<sup>106</sup> the written Explanations of MCD and JJD,<sup>107</sup> the Notices of Suspension,<sup>108</sup> the Request for Grievance submitted by MCD,<sup>109</sup> the Letter giving VMC the opportunity to reply before filing a complaint with the NPC,<sup>110</sup> the Certification from Negros Del Norte Planters Association that JJD informed them about the expiration of the lease of one of the undisclosed haciendas,<sup>111</sup> and the Letter from VMC stating that they are referring the matter to their legal counsel.<sup>112</sup>

Section 1 of Rule 131 of the 2019 Amendments to the Revised Rules on Evidence provides:

Section 1. *Burden of proof and burden of evidence.* **Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim** or defense by the amount of evidence required by law. Burden of proof never shifts.

Burden of evidence is the duty of a party to present evidence sufficient to establish or rebut a fact in issue to establish a prima facie case. Burden of evidence may shift from one party to the other in the course of the proceedings, depending on the exigencies of the case.<sup>113</sup>

Section 6 of Rule 133 of the 2019 Amendments to the Revised Rules on Evidence provides:

Section 6. Substantial Evidence. In cases filed before administrative or quasi-judicial bodies, a fact may be deemed established if it is supported by substantial evidence, or that amount of relevant evidence which a reasonable mind might accept as adequate to justify a conclusion.<sup>114</sup>

In this case, Complainants, had the burden of proof in alleging a violation of the DPA. Complainants, however, did not discharge this burden as they failed to support their allegations with substantial evidence.

In *BSA Tower Condominium Corporation v. Reyes*,<sup>115</sup> the Supreme Court held that:

The basic rule is that mere allegation is not evidence and is not equivalent to proof.

104 *Id.* Annex A; *Id.* Annex A.

105 *Id.* Annex B; *Id.* Annex B.

106 *Id.* Annex C; *Id.* Annex C.

107 *Id.* Annex D; *Id.* Annex D.

108 *Id.* Annex E; *Id.* Annex E.

109 Complaint-Affidavit of MCD y C, 27 June 2019, Annex F, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

110 Complaint-Affidavit of MCD y C, 27 June 2019, Annex G, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of MCD y C, 27 June 2019, Annex F in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

111 Complaint-Affidavit of MCD y C, 27 June 2019, Annex F in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

112 Complaint-Affidavit of MCD y C, 27 June 2019, Annex H, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of MCD y C, 27 June 2019, Annex G in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

113 2019 AMENDMENT TO THE 1989 REVISED RULES ON EVIDENCE, A.M. No. 19-08-15-SC, rule 131, §1 (1 May 2020). Emphasis supplied.

114 *Id.* rule 133, §6.

115 *BSA Tower Condominium Corp. v. Reyes II*, A.C. No. 11944 (2018).

Likewise, charges based on mere suspicion and speculation cannot be given credence.<sup>116</sup>

As correctly stated by Respondents, nothing in the complaint “provided any detail as to who among the Respondents processed personal data, what kind of personal data, and how could they have used [the] personal data.”<sup>117</sup>

In their submissions, Complainants only mentioned that Respondent GEK validated the contents of the Disclosure Statements by conducting a field investigation.<sup>118</sup> They failed to prove how Respondents MOC, EVR and SC, as issuers and signatories of the Notice to Explain, unlawfully processed their information.

Further, they failed to particularly identify which information Respondents processed and how Respondents unlawfully accessed or disclosed Complainants’ personal data. They neither specified nor discussed the provisions of the DPA that Respondents supposedly violated.

In sum, Complainants failed to discharge their burden and to submit substantial evidence to support their claim against Respondents. Thus, the case must be dismissed for lack of substantial evidence.

II. Respondents’ act of processing and validating the contents of Complainants’ Disclosure Statements was pursuant to its legitimate interest.

While it has been established earlier that Complainants failed to identify which information Respondents processed, a perusal of the records shows that the personal data in the Disclosure Statements only involves personal information.

Section 3 (g) of the DPA defines personal information:

Section 3. *Definition of Terms.* Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

...

(g) Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.<sup>119</sup>

The Disclosure Statements included the names, positions, I.D. numbers, employment information, personal relationships, and financial interests of the employees and consultants of VMC.<sup>120</sup> The employees and consultants’ names clearly fall under the definition

<sup>116</sup> *Id.*

<sup>117</sup> Memorandum for the Respondents, 18 April 2022, at 20-22, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2022).

<sup>118</sup> Complaint-Affidavit of MCD y C, 27 June 2019, at 2, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 2, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

<sup>119</sup> An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (g) (2012).

<sup>120</sup> Complaint-Affidavit of MCD y C, 27 June 2019, Annex A, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, Annex A, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

of personal information. Further, these information, when put together, can directly and certainly identify the members of VMC. Thus, they are considered personal information under the DPA.

Nevertheless, Respondents processed the personal information involved according to a lawful criterion under Section 12 (f) of the DPA. Section 12 (f) of the DPA allows for the processing of personal information when it is necessary for the purposes of the legitimate interests pursued by the PIC:

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

...

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.<sup>121</sup>

Processing based on legitimate interest requires the fulfillment of the following conditions: (1) the legitimate interest is established; (2) the means to fulfill the legitimate interest is both necessary and lawful; and (3) the interest is legitimate and lawful and it does not override fundamental rights and freedoms of data subjects.<sup>122</sup>

In this case, Respondents have clearly established that the processing and validating of the Disclosure Statements were done pursuant to the VMC's legitimate interest of preventing and addressing any actual or potential conflict of interest that may adversely affect the interest of the company in its stakeholders, such as dealings between employees, consultants and VMC.<sup>123</sup>

### **A. Respondents established their legitimate interest in processing Complainants' Disclosure Statements.**

The first requisite of processing based on Section 12 (f) of the DPA is that the legitimate interest is established.<sup>124</sup> This focuses on what the PIC seeks to accomplish with the specific processing activity. To determine whether this has been established, the PIC must comply with the general privacy principles of (1) legitimate purpose and (2) transparency.

Section 11 of the DPA discusses legitimate purpose as follows:

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.

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

122 MAF v. Shopee, NPC 21-167, 22 September 2022, at 9, available at <https://privacy.gov.ph/wpcontent/uploads/2023/05/NPC-21-167-2022.09.22-MAF-v.-Shopee-Decision-Final.pdf> (last accessed 05 July 2023).

123 Consolidated Comment, 18 October 2021, at 2, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

124 MAF v. Shopee, NPC 21-167, at 9

Personal information must, be:

(a) **Collected for specified and legitimate purposes** determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;

...

(e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or **for legitimate business purposes, or as provided by law**.<sup>125</sup>

Elaborating on this, Section 18 of the Implementing Rules and Regulations of the DPA (IRR) provides:

Section 18. Principles of Transparency, Legitimate Purpose and Proportionality. The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.

...

b. Legitimate purpose. The processing of information shall be compatible with a declared and **specified purpose which must not be contrary to law, morals, or public policy**.<sup>126</sup>

The legitimate purpose principle requires that: (1) the purpose of processing must be specified; and (2) that purpose must not be contrary to law, morals, or public policy.<sup>127</sup>

The first element requires that there should be a specific purpose, such that the purpose of processing is clearly defined and not vague or overbroad. While this does not require an exhaustive enumeration of each and every purpose, the purpose must be specific enough for the data subject to understand the purpose of processing. The second element requires the purpose to be within the limitations of the law, which should be understood to include the entire body of laws, rules, and regulations.<sup>128</sup> Additionally, the purpose of processing should not go against prevailing morals or run counter to public policy.<sup>129</sup>

Both elements of legitimate purpose are satisfied in this case. The processing of Complainants' information was done pursuant to a legitimate purpose, which was to comply with existing regulations and to ensure that there were no deviations from the company's policies that could be detrimental to the business of VMC. Further, such purpose is not contrary to any law, rule, or regulation or against morals and policy.

VMC, as a publicly listed corporation, has a responsibility towards its investors and must comply with the Securities and Exchange Commission Code of Corporate Governance

<sup>125</sup> Data Privacy Act of 2012, § 11 (a)(e). Emphasis supplied.

<sup>126</sup> National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule IV, § 18 (a)(b) (2016) Emphasis supplied.

<sup>127</sup> See Data Privacy Act of 2012, § 11; Rules and Regulations Implementing the Data Privacy Act of 2012, rule IV, § 18 (a)(b).

<sup>128</sup> *MLF v. MyTaxi.PH Corp.*, NPC 19-142, 31 March 2022, at 8, available at <https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-19-142-MLF-v.-Grab-Philippines-2022.03.31.-Decision.pdf> (last accessed 24 August 2023).

<sup>129</sup> *Id.* at 8.

for Publicly Listed Companies under SEC Memorandum Circular 19 Series of 2016.<sup>130</sup> The SEC Memorandum Circular requires such corporations “to establish corporate disclosure policies and procedures that are practical and in accordance with best practices and regulatory expectations.”<sup>131</sup> This includes the adoption of anti-corruption programs to mitigate corrupt policies which include conflict of interest.<sup>132</sup>

Further, VMC has legitimate business interest to prevent and address conflicts of interest that may adversely affect the company and its stakeholders.<sup>133</sup> VMC, in compliance with the SEC Circular and pursuant to good corporate governance, required all of its employees and consultants to execute the Disclosure Statements. Clearly, Respondents have a real and present interest in the processing of the Disclosure Statements of its employees.

Further, the transparency principle requires that the claimed interest is declared to the data subject.<sup>134</sup> The PIC should inform the data subject of the nature, purpose, and extent of the processing, using clear and plain language that is easy to access and understand.<sup>135</sup>

In this case, Respondents clearly and adequately communicated to the employees, including Complainants, VMC’s legitimate interest in processing Complainants’ information through the provisions found in the Disclosure Statements. As stated in the Disclosure Statements, the disclosure is done “in accordance with the VMC Group policy on good corporate governance to ensure transparency in (the) working relations with all parties.”<sup>136</sup> Further, the Disclosure Statements stated who are covered and what would amount to a conflict of interest.<sup>137</sup>

### **1. Coverage**

This statement is to be accomplished by employees and consultants of Victorias Milling Company, Inc. (VMC) and its subsidiaries (the VMC Group).

### **2. Definition of Terms**

...

**Conflict of Interest** – any personal or financial interest, actual or apparent, that is in conflict with VMC Group duties and responsibilities.

Areas wherein conflict of interest may arise:

1. Dealings with/as suppliers, contractors, business partners, consultants, or third parties
2. Dealings with directors, employees, consultants, and prospective employees and consultants

130 Consolidated Comment, 18 October 2021, at 3, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

131 Consolidated Comment, 18 October 2021, at 3, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

132 *Id.* Recommendation 15.2.

133 Consolidated Comment, 18 October 2021, at 2, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2021).

134 Data Privacy Act of 2012, § 11 (a).

135 Rules and Regulations Implementing the Data Privacy Act of 2012, rule IV, § 18 (a).

136 Complaint-Affidavit of MCD y C, 27 June 2019, Annex F, in Sps. MCD-JJD v. Victorias Milling Company, NPC 19-758 & 19-1846 (NPC 2019).

137 *Id.*

...

3. In accordance with the VMC Group policy on good corporate governance to ensure transparency in my working relations with all parties, I hereby declare and disclose the following:<sup>138</sup>

Thus, Respondent established their legitimate interest and satisfied the first requisite of processing based on Section 12 (f) of the DPA. They have communicated their specific purpose in processing Complainants' Disclosure Statements and such purpose is not contrary to law, morals, or public policy.

**B. The means that Respondents used to fulfill its legitimate interest were both necessary and lawful.**

The second requisite of processing based on Section 12 (f) of the DPA is that the means to fulfill the legitimate interest is both necessary and lawful.<sup>139</sup> For this requisite, the PIC must evaluate how it is accomplishing its legitimate interest as previously established. The PIC must show that the means or the specific processing activity undertaken is (1) necessary and (2) lawful.<sup>140</sup>

As the Commission previously held, the qualifier “necessary” refers to the general privacy principle of proportionality.<sup>141</sup> Following this principle, the processing must be adequate, relevant, suitable, and necessary, such that it is not excessive in relation to the declared and specified purpose.<sup>142</sup>

Section 11 of the DPA provides:

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:

...

(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;

(d) **Adequate and not excessive in relation to the purposes for which they are collected and processed[.]**<sup>143</sup>

Section 18 of the Implementing Rules and Regulations of the DPA (IRR) elaborates on proportionality:

Section 18. *Principles of Transparency, Legitimate Purpose and Proportionality*. The

138 *Id.*  
139 MAF v. Shopee, NPC 21-167, at 9.  
140 See Data Privacy Act of 2012, § 11 (b)(c)(d).  
141 EA and TA v. EJ, EE, and HC, NPC 17-018, 15 July 2019, at 10, available at <https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-17-018-EA-and-TA-v-EJ-Decision2019.07.15-.pdf>, (last accessed 24 August 2023).  
142 Data Privacy Act of 2012, § 11 (c)(d).  
143 *Id.* § 11 (b)(c)(d). Emphasis supplied.

processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and **proportionality**.

. . .

c. Proportionality. The processing of information shall be **adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose**. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.<sup>144</sup>

Given this, processing is deemed proportional when (1) processing is adequate, relevant, and necessary to the declared and specified purpose; and (2) the means by which processing is performed is the least intrusive means available.<sup>145</sup>

In *Philippine Stock Exchange Inc. v. Secretary of Finance*, the Supreme Court explained “necessary” to mean that “the personal data sought by the State must be acquired through ‘narrowly tailored’ means, which are only necessary to accomplish the regulatory agencies’ given mandate.”<sup>146</sup> As applied in this case, the PIC must adopt means that are only necessary to accomplish its legitimate interest to prevent abuses.

In this case, Respondents’ act of validating the VMC employees’ Disclosure Statements was necessary to verify the accuracy of the entries and detect discrepancies in the Disclosure Statements. Respondents conducted field investigations, verifications, inspections, interviews, and inquiries simply to verify the entries of Complainants on their Disclosure Statements.<sup>147</sup> By doing so, Respondents can ensure that all possible conflicts of interests of the VMC employees and consultants are addressed. Further, as stated by Respondents, the validation was done with utmost confidentiality as “only authorized personnel whose functions included participation in the conduct of internal administrative proceedings under the Labor Code were given access” to Complainants’ information.<sup>148</sup>

Specifically, GEK, as the Head of the Transformation Department and Internal Audit, is responsible for auditing information and providing reports thereon that could adversely affect the business of VMC.<sup>149</sup> Thus, it was necessary for her to process the information in the Disclosure Statements.

The second element is also present as the means chosen by Respondents were lawful. For this element, it requires that the means chosen to accomplish the legitimate interest is itself lawful.<sup>150</sup> The PIC cannot violate any law in the process of accomplishing its legitimate interest. Considering that the determination of lawfulness goes into the means chosen to accomplish the legitimate interest, it is different from the lawfulness of the purpose under the general privacy principle of legitimate purpose (i.e. purpose must not be contrary to law, morals, and public policy). Section 11 of the DPA provides:

---

144 Rules and Regulations Implementing the Data Privacy Act of 2012, rule IV, § 18 (c). Emphasis supplied.

145 *MAF v. Shopee*, NPC 21-167, at 14.

146 *Philippine Stock Exchange v. Secretary of Finance*, G.R. No. 213860 (2022).

147 Complaint-Affidavit of MCD y C, 27 June 2019, at 2, in *Sps. MCD-JJD v. Victorias Milling Company*, NPC 19-758 & 19-1846 (NPC 2019); Complaint-Affidavit of JJD y J, 27 June 2019, at 2, in *Sps. MCD-JJD v. Victorias Milling Company*, NPC 19-758 & 19-1846 (NPC 2019).

148 Consolidated Comment, 18 October 2021, at 4, in *Sps. MCD-JJD v. Victorias Milling Company*, NPC 19-758 & 19-1846 (NPC 2021).

149 *Id.* at 19.

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

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:

...

(b) Processed fairly and **lawfully**;

Respondents' adopted means for validating the information in the Disclosure Statements were lawful. The field investigation and the inquiries done by Respondents did not violate any existing law or regulation, company policy, or contractual agreement between VMC and Complainants.

### **C. Respondents' interest is legitimate and lawful and it does not override fundamental rights and freedoms of data subjects.**

The third requisite is that the interest is legitimate and lawful and it does not override fundamental rights and freedoms of data subjects.<sup>151</sup> This requisite focuses on the effect of accomplishing the legitimate interest such that it does not override the fundamental rights and freedoms of the data subjects.

A determination of the effect of accomplishing legitimate interest requires an analysis of the totality of the three (3) requisites. Given that the legitimate interest of the PIC has been established (first requisite) and the PIC's means to fulfill that legitimate interest is both necessary and lawful (second requisite), it must now be determined whether the processing undertaken does not override the Complainants' fundamental rights and freedoms (third requisite).

In determining the effect of the PIC's legitimate interest on the data subject, aside from the categories of personal information that is processed, the Commission considers the general privacy principle of fairness and the reasonable expectation of the data subjects with regard to the processing of their personal information.

Section 11 (b) of the DPA states that the personal information must be processed fairly.<sup>152</sup>

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:

...

(b) Processed **fairly** and lawfully[.]<sup>153</sup>

Section 19 of the Implementing Rules and Regulations of the DPA (IRR) elaborates on

151 MAF v. Shopee, NPC 21-167, at 9.

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

153 *Id.* Emphasis supplied.



fairness:

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:

...

b. Personal data shall be processed **fairly** and lawfully.

1. Processing shall uphold the rights of the data subject, including the right to refuse, withdraw consent, or object. It shall likewise be transparent, and allow the data subject sufficient information to know the nature and extent of processing.
2. Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.
3. Processing must be in a manner compatible with declared, specified, and legitimate purpose.
4. Processed personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
5. Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards.<sup>154</sup>

As discussed, Respondents processed Complainants' personal data in compliance with the SEC Circular and pursuant to good corporate governance.<sup>155</sup> The validation of the Disclosure Statements did not go beyond what can be reasonably expected by Complainants, as employees, when they submitted their Disclosure Statements to VMC. It is not unreasonable to expect that these Disclosure Statements would be subject to verification and validation as a necessary consequence.

The interest of Respondents to comply with regulatory requirements and protect its business from conflicts of interest that may adversely affect the company is legitimate and does not override the fundamental rights and freedoms of the data subjects, including Complainants. This legitimate interest does not, in any way, disregard the fundamental rights and freedoms of Complainants.

In sum, for processing based on Section 12 (f) of the DPA to apply, the PIC must comply with three (3) requisites.<sup>156</sup> The first requisite focuses on what the PIC is accomplishing and the legitimate purpose that has been communicated to the data subject. The second requisite refers to how the PIC is accomplishing the legitimate interest, such as the means chosen or the specific processing activity undertaken, which should be necessary and lawful. Finally, the third requisite considers the effect of accomplishing the legitimate interest, such that it does not override the fundamental rights and freedoms of the data subjects.

In this case, Respondents complied with all three requisites for processing based on legitimate interest. Respondents have clearly established the legitimate interest in pro

<sup>154</sup> Rules and Regulations Implementing the Data Privacy Act of 2012, rule IV, § 19(b). Emphasis supplied.

<sup>155</sup> Consolidated Comment, 18 October 2021, at 2, in *Sps. MCD-JJD v. Victorias Milling Company*, NPC 19-758 & 19-1846 (NPC 2021).

<sup>156</sup> *MAF v. Shopee*, NPC 21-167, at 9.

cessing the Disclosure Statements. The investigations and interviews lawfully conducted were necessary to verify the accuracy of the entries in the Disclosure Statements. Further, their acts did not go beyond what could be reasonably expected by Complainants, as employees, when they submitted their Disclosure Statements. Thus, even if Complainants had presented substantial evidence to support their claims, Respondents would still have lawful basis under Section 12 (f) of the DPA when they processed Complainants' personal information.

Given the foregoing, the Commission cannot find Respondents liable for violating Section 25 (Unauthorized Processing), Section 26 (Access due to Negligence), Section 28 (Processing for Unauthorized Purposes), Section 29 (Unauthorized Access or Intentional Breach), Section 31 (Malicious Disclosure), Section 32 (Unauthorized Disclosure), and Section 33 (Combination or Series of Acts) of the DPA.

**WHEREFORE**, premises considered, this Commission resolves that the case filed by Spouses MCD and JJD against Victorias Milling Company, MOC, EVR, GEK, and SC is **DISMISSED** for lack of substantial evidence.

This is without prejudice to the filing of appropriate civil, criminal, or administrative cases before any other forum or tribunal, if any.

**SO ORDERED.**

City of Pasay, Philippines.  
30 June 2023.

**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

**JOHN HENRY D. NAGA**  
Privacy Commissioner

(on official leave)  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

Copy furnished:

**D-S & I LAW OFFICES**  
*Counsel for Complainants*

**KAB**  
*Counsel for Respondents*

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission



# RESOLUTIONS



X-----X

## **RESOLUTION**

### **NAGA, D.P.C.:**

Before this Commission is a request made by Sun Life of Canada Philippines Inc. (Sun Life) to be exempted from notifying affected data subjects from a data breach incident that occurred last 29 November 2017.

#### The Facts

On 01 September 2017, Sun Life's Unit Manager (UM) was transferred from Eucalyptus New Business Office (NBO) to Empress NBO. By reason of such transfer, the Licensing Department updated her Agent Information System (AIS). On 26 November 2017, the UM reported to their Helpdesk that she was able to generate the production report that belongs to her Branch Manager (BM) and her direct advisors when she used her personal laptop via Google Chrome browser.

On 27 November 2017, the incident was escalated to the Advisor Technology Support (ATS) and Compliance. It was identified that because of the update, the code of her new BM was saved as the UM's Team Lead Code which allowed her to generate the production report.

Sun Life reported that one hundred one (101) accounts with one hundred (100) policy owners were affected by the breach. The personal data involved are as follows: Due Date; Policy Number; Insured Name; Submitted Applications; Settled Applications; Net Sales Credit; First Year Premium; and Renewal Premium Income.

In response, Sun Life mentioned that they have taken the following measures to address the breach:

- a. On 27 November 2017, the UM was requested to delete the production report that she has downloaded from the agent's portal and send confirmation that the same was deleted;
- b. The UM code was updated to her own team code in the Agent's Information System;
- c. The Licensing Department will file a maintenance request to update the AIS. The Team code field will not accept the code if it does not belong the advisor/ UM whose account is being updated; and
- d. IT will be requested to sweep or check the system for another similar occurrence.

On 29 November 2017, Sun Life submitted the breach notification report before the Commission with a request to be exempted from notifying its clients and advisors that were affected by the breach, on the ground that the breach will not cause real risk of serious harm to the rights and freedoms of the policy holders considering that it was the

UM herself who reported the said breach.

### Discussion

As provided by Section 11 of the NPC Circular 16-03, notification to the affected data subjects shall be required upon knowledge of or when there is reasonable belief by the Personal Information Controller (PIC) or Personal Information Processor (PIP) that a personal data breach requiring notification has occurred, under the following conditions:

- A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, “other information” shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
- B. There is reason to believe that the information may have been acquired by an unauthorized person; and
- C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

The Commission recognizes that Sun Life has premised its request for exemption on the ground that the incident does not meet the third condition laid down by the abovementioned provision as the personal data were disclosed only to the UM.

However, Sun Life failed to take into account that the number of affected data subjects is more than one hundred (100) individuals which falls under the mandatory breach notification as provided by Section 13 (B) of NPC Circular 16-03.

According to Section 38 of the Data Privacy Act of 2012 (DPA), “Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.” Thus, the DPA and the rules and regulations in relation to data privacy should be interpreted in a manner that will uphold the data privacy rights of the individual. Hence, the Commission does not see any reason to disturb the general rule for the PIC to notify the data subjects affected by a personal data breach.<sup>1</sup>

The Commission then deems it wise to order Sun Life to notify the affected data subjects to provide them the reasonable opportunity to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.

On another matter, the Commission notes that as of the date of the promulgation of this Resolution, it has yet to receive its full breach report as required under NPC Circular 16-03. The Commission reminds Sun Life that the DPA requires two (2) different reports in case of a data breach.

As held by the Commission in the case of In re: SLGF (NPC BN 19115):

---

<sup>1</sup> Section 18 of the NPC Circular 16-03

Section 17 of the NPC Circular 16-03 speaks of two notification requirements to be submitted to the Commission in case a data breach cases. First is the initial notification<sup>2</sup> that informs to the Commission that a personal data breach has occurred. This has no particular form or content as it merely requires that the Commission to be notified within seventy-two (72) hours. The second notification<sup>3</sup> is the Full Breach Report which contains a more specific and concrete narration of facts surrounding the incident, the effect of such incident and the remedial actions taken by the PIC. The full breach report that the Commission requires must include, but not be limited to:

1. Nature of the Breach

- a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
- b. a chronology of the events leading up to the loss of control over the personal data;
- c. approximate number of data subjects or records involved;
- d. description or nature of the personal data breach;
- e. description of the likely consequences of the personal data breach; and
- f. name and contact details of the data protection officer or any other accountable persons.

2. Personal Data Possibly Involved

- a. description of sensitive personal information involved; and
- b. description of other information involved that may be used to enable identity fraud.

3. Measures Taken to Address the Breach

- a. description of the measures taken or proposed to be taken to address the breach;
- b. actions being taken to secure or recover the personal data that were compromised;
- c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
- d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
- e. the measures being taken to prevent a recurrence of the incident.<sup>4</sup>

The foregoing content and information is needed by the Commission in order to determine if the PIC has acted adequately in order to protect the rights of the affected data subject and to see if the PIC has undertaken measures to avoid further damage. These two documents are very much different from one another not only as to its form and content but also as to its purpose.

Sun Life submitted before the Commission a breach notification dated 29 November 2017. The breach notification submitted can only be considered as a notification as prescribed under Section 17 (A) of NPC Circular 16-03 as it lacks the necessary content and information required in a full breach report. Therefore, Sun Life is not yet compliant in terms of the submission of the required full breach report.

**WHEREFORE**, premises considered, this Commission **DENIES** the request of Sun Life to be exempted from notifying data subjects affected by the breach.

---

2 Section 17 (A) of the NPC Circular 16-03

3 Section 17 (D) of the NPC Circular 16-03

4 Section 17 (A) of NPC Circular 16-03

Sun Life is hereby **ORDERED** to comply within ten (10) days from receipt of this Resolution with the following:

(1) **NOTIFY** with dispatch the affected data subjects, including proof of compliance consistent with NPC Circular 16-03; and

(2) **SUBMIT** a full breach report detailing the measures it has since undertaken to prevent, avoid or reduce the recurrence of a similar personal data breach.

**SO ORDERED.**

Pasay City, Philippines;  
15 October 2020.

**(Sgd.)**

**JOHN HENRY D. NAGA**

Deputy Privacy Commissioner

WE CONCUR:

*(On Official Business)*

**RAYMUND ENRIQUEZ LIBORO**

Privacy Commissioner

**(Sgd.)**

**LEANDRO ANGELO Y. AGUIRRE**

Deputy Privacy Commissioner

**COPY FURNISHED:**

**JSC**

*Data Privacy Officer*

**COMPLAINTS AND INVESTIGATION DIVISION**

**ENFORCEMENT DIVISION**

**GENERAL RECORDS UNIT**

National Privacy Commission

X-----X

RESOLUTION

AGUIRRE, D.P.C.:

This Resolution refers to the Letter<sup>1</sup> of the Commission on Elections (COMELEC) providing notice to this Commission of a possible personal data breach concerning the registered voters of Talavera, Nueva Ecija, and its request for extension of time to notify the data subjects.

The Facts

On 10 November 2020, COMELEC received an unsigned memorandum dated 04 November 2020 from JBR, Election Officer (EO), Office of the Election Officer (OEO) of Talavera, Nueva Ecija, reporting that on 30 October 2020, a burglary incident happened at the OEO of Talavera, Nueva Ecija.<sup>2</sup>

After the inventory was conducted, the following items were found missing:

- (1) One portable hard drive which contains the voter registration records and VRS backups (COMELEC property);
- (2) One Lenovo Think Pad Laptop with SN R90JD1J8 (COMELEC property) which contains the voter registration system program, other VRS reports and data backup;
- (3) One Acer laptop (LGU property);
- (4) One Samsung Notebook (LGU property);
- (5) Php 350.00 hidden inside an employee’s drawer; and
- (6) Two hundred pieces of face shields.<sup>3</sup>

JBR also reported the following:

- (1) The lock of the office vault was smashed and destroyed;
- (2) The incident was immediately reported to the local police and investigation is on-going;
- (3) The concerned officers of COMELEC were informed; and
- (4) Inventory of all office documents is on-going.<sup>4</sup>

Furthermore, COMELEC requested that since such notice has been submitted beyond the seventy-two (72) hour period, within which the Commission should be notified, the same be considered justified and reasonable considering the consecutive work suspensions that followed after the receipt of JBR’s report, thus:

---

1 Letter dated 16 November 2020.  
 2 *Ibid.*  
 3 *Ibid.*  
 4 *Ibid.*



Please note that while this Office received the report of JBR on 10 November 2020, work in government offices in the National Capital Region as well as in Region III, among other regions, was suspended effective 3:00 o'clock in the afternoon of 11 November 2020 (Thursday) until 13 November 2020 (Friday).<sup>5</sup>

COMELEC informed this Commission of their security measures, thus:

Relatedly, undersigned respectfully informs the NPC that, as a security feature, all the data encoded in the computers of all OEOs involved the voters of their respective cities and municipalities only, and are already encrypted in AES 256. The portable hard disks containing said data are likewise encrypted.<sup>6</sup>

According to the letter, the COMELEC Executive Director and Data Protection Officer issued a memorandum dated 10 November 2020 for the Director IV of COMELEC's Information Technology Department, as well as Director III of the Finance Services Department and Data Compliance Officer, informing them about the report of JBR with a directive to investigate the incident.<sup>7</sup>

Lastly, COMELEC claims that since the investigation is on-going and the challenges posed by the threat of COVID-19, it is not reasonably possible to notify the data subjects within the prescribed period. For these reasons, COMELEC requests for an extension of time to comply with the notification of data subjects<sup>8</sup> without stating a specific timeline for such.

### Discussion

This Commission denies the request for an indefinite extension of COMELEC to notify the affected data subjects.

Section 18(B) of NPC Circular 16-03 provides that:

**If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification.** A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects. **The Commission may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach,** taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.<sup>9</sup>

In this case, COMELEC requests for an extension to comply with the notification of data subjects on two (2) grounds, namely, (1) that an investigation is on-going, and (2) the challenges posed by the threat of COVID-19.<sup>10</sup>

A careful scrutiny of the records reveals that there are two (2) investigations referred to in this case. First, the on-going investigation conducted by the local police. Second,

5 *Ibid.*

6 *Ibid.*

7 *Ibid.*

8 *Ibid.*

9 Emphasis supplied.

10 *Supra* note 1.

the investigation under the directive of COMELEC through its Information Technology Department and Finance Services Department.

As to the on-going investigation by the local police, there is no showing how the notification to data subjects will hinder the investigation on robbery or other relevant crime thereto. Not all criminal investigations, even those conducted as a result of the breach as in this case, can be considered as a ground for postponement of notification of data subjects. Simply mentioning that a criminal investigation is being undertaken is not sufficient. The burden is on the party requesting for postponement to show that the notification will indeed affect the outcome of the investigation.

As to the investigation within the COMELEC, this is not the investigation contemplated by Section 18 of NPC Circular 16-03, which specifically refers to criminal investigations.

Furthermore, while the challenges posed by the threat of COVID19 pandemic was raised by the COMELEC as a reason for its postponement to notify the data subjects, it was not explained how it is not reasonably possible to notify the data subjects within the prescribed period. More importantly, it did not state what period of additional time is requested for. The request for an indefinite extension of notification of the affected data subjects is hereby denied.

The Commission, however, notes that no mention was made about the COMELEC's concrete steps for the retrieval of the affected data subjects' information which may have been stored in the stolen equipment. In order to effect the notification of the data subjects which will enable them to take the necessary precautions, the Commission directs the COMELEC to conduct notification through alternative means under Section 18(D) of NPC Circular 16-03<sup>11</sup>, thus:

Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: Provided, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.<sup>12</sup>

This Commission likewise brings to the attention of COMELEC the required submission of its Full Breach Report. Section 17(C) of NPC Circular 16-03 provides that:

There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days,

<sup>11</sup> NPC Circular 16-03, Personal Data Breach Management. Dated 15 December 2016.

<sup>12</sup> Emphasis supplied.

unless the personal information controller is granted additional time by the Commission to comply.<sup>13</sup>

While COMELEC has requested for additional time to notify the data subjects herein, no request for additional time to submit the full report has been made. The COMELEC is reminded that the notification of data subjects and notification of the Commission are two (2) different requirements to be complied with by personal information controllers (PICs).

**WHEREFORE**, premises considered, the Commission on Elections is **ORDERED, within ten (10) days** from receipt of this Resolution, to: (1) Submit its Full Breach Report, and (2) Notify the data subjects through alternative means and submit proof of compliance thereto.

**SO ORDERED.**

Pasay City, Philippines  
26 November 2020.

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

**Sgd.**  
**RAYMUND ENRIQUEZ LIBORO**  
Privacy Commissioner

**Sgd.**  
**JOHN HENRY D. NAGA**  
Deputy Privacy Commissioner

**COPY FURNISHED:**

**BJS**  
Executive Director and Data Protection Officer  
Commission on Elections

**THRU: MRA**  
Representative  
Commission on Elections

**COMPLIANCE AND MONITORING DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

---

<sup>13</sup> Emphasis supplied.

CNI,

*Complainant,*

**CID No. 17-K-004**  
For: Violation of the  
Data Privacy Act

**-versus-**

XXX,

*Respondents.*

X-----X

## **RESOLUTION**

### **NAGA, D.P.C.:**

This refers to the Compliance Letter dated 02 December 2020, with an attached XXX Cards Complaint Management Process submitted by the XXX in relation to the 21 September 2020 Order of this Commission.

### **The Facts**

On 21 September 2020, the Commission issued a Resolution disposing, thus:

**WHEREFORE**, premises considered, this Commission hereby **DENIES** Complainant CBI's Urgent Motion for Reconsideration. Furthermore, the case of CBI vs. XXX is hereby considered **CLOSED**. Furthermore, XXX is **ORDERED** to submit **within thirty (30) days** from receipt of this Decision a complete report on the measures it has undertaken or will undertake to address the issue of delayed response to their customers' request in relation to their rights as data subjects.

Respondent manifested that they received the abovementioned Resolution on 04 November 2020. Thus, on 02 December 2020, XXX submitted its Compliance with an attached XXX Cards Complaint Management Process as Annex 1 of the Compliance. The Annex 1 provides the step-by-step process in the handling of complaints from their clients. The Respondent also indicated therein turnaround time of seven (7) days for simple complaints and forty-five (45) for complex complaints.

### **Discussion**

The Commission finds XXX submission to be substantially compliant with the 21 September 2020 Order of this Commission.

The 21 September 2020 Order was based on the inaction of the Respondent to the request for correction of the Complainant. Such request should be acted upon with reasonable turnaround time considering that the request is one of the rights provided in the Data Privacy Act (DPA) to every data subject<sup>1</sup>. Further, this obligation is in relation to Section 28 (d) of the Implementing Rules and Regulations of the DPA.

While the Commission opines that the Complaint Management Process of the

Respondent herein can be written in a more comprehensive and detailed manner, we find it to substantially comply with the requirements of the abovementioned provisions of the DPA, its IRR, and with the Commission's 21 September 2020 Order. As jurisprudence provides, the substantial compliance rule is defined as, "compliance with the essential requirements, whether of a contract or of a statute."<sup>2</sup>

**WHEREFORE**, premises considered, this Commission hereby **NOTES** the submission made by the XXX dated 02 December 2020 in compliance with the Commission Order dated 21 September 2020.

**SO ORDERED.**

Pasay City, Philippines;  
17 December 2020.

**(Sgd.)**

**JOHN HENRY D. NAGA**

Deputy Privacy Commissioner

WE CONCUR:

**(Sgd.)**

**RAYMUND ENRIQUEZ LIBORO**

Privacy Commissioner

**(Sgd.)**

**LEANDRO ANGELO Y. AGUIRRE**

Deputy Privacy Commissioner

COPY FURNISHED:

**CBI**

Complainant

**XXX**

Respondent

**COMPLAINTS AND INVESTIGATION DIVISION  
ENFORCEMENT DIVISION  
GENERAL RECORDS UNIT**

JCR,

*Complainant,*

**NPC 17-K-001**

For: Violation of the provisions of the Data Privacy Act of 2012

**-versus-**

**GLOBE TELECOM, INC.**

*Respondents.*

X-----X

## RESOLUTION

### **AGUIRRE, D.P.C.:**

This Resolution refers to the Compliance Report dated 03 February 2020<sup>1</sup> 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 Decision<sup>2</sup> 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 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)<sup>3</sup> 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

1 Compliance Report dated 3 February 2020.

2 Decision dated 5 December 2019.

3 *Ibid.*

System, and failure to provide correct answers to any of the six (6) account verification questions.<sup>4</sup>

On 03 August 2020, the Enforcement Division of this Commission issued an Enforcement Letter<sup>5</sup> 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.<sup>6</sup>

On 20 August 2020, Respondent submitted a Comprehensive Report<sup>7</sup> 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.<sup>8</sup>

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.<sup>9</sup>

## **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 inci-**

---

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.

8 *Ibid.*

9 *Ibid.*

- dents 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;
- g. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.<sup>10</sup>

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 Decision<sup>11</sup> 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.

(sgd)  
**LEANDRO ANGELO Y. AGUIRRE**  
*Deputy Privacy Commissioner*

WE CONCUR:

(sgd)  
**RAYMUND ENRIQUEZ LIBORO**  
*Privacy Commissioner*

(sgd)  
**JOHN HENRY D. NAGA**  
*Deputy Privacy Commissioner*

<sup>10</sup> Emphasis supplied.

<sup>11</sup> Supra note 1.



**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

X-----X

## **RESOLUTION**

### **AGUIRRE, D.P.C.:**

In an Order dated 23 July 2020, the Commission required Sun Life of Canada (Philippines), Inc. (“Sun Life”) to show cause why it should not be subject to contempt proceedings and other actions available to the Commission for failing to comply with the Commission’s decision, thus:

**WHEREFORE**, the above premises considered, the Commission resolves to **ORDER** Sun Life of Canada (Philippines), Inc. to show cause in writing, within fifteen (15) calendar days from receipt of this Order, why it should not be liable for Failure to Notify under Section 20 of NPC Circular 16-03 and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.

In response to the Show Cause Order, Sun Life sent a letter dated 26 August 2020 explaining that:

1. A notification two years after the incident would cause undue alarm on the part of the data subjects.
2. The December 2019 Letter is not prohibited under NPC Circular 16-03.
3. Sun Life merely tried to exhaust all administrative remedies.
4. Sun Life believed in good faith that the Honorable Commission had yet to resolve the December 2019 Letter.
5. Sun Life did not willfully violate the Resolutions of this Honorable Commission.

### **A. Requirements for exemption from notification of data subjects**

At the outset, it should be emphasized that notification of data subjects of data breaches is the general rule and exemption will only be allowed in exceptional circumstances when the Commission determines that “such notification would not be in the public interest or in the interest of the affected data subjects.”<sup>1</sup> It is a basic rule of evidence and procedure that the Commission, in making this determination, cannot simply rely on bare allegations. It looks at the available evidence on record to see whether these are sufficient to overcome the presumption that notification is in the best interest of the data subjects.

In this case, in seeking to be exempted from notifying its data subjects, Sun Life alleged in its 19 October 2017 breach notification that the breach is unlikely to give rise to a real risk of serious harm to data subjects since controls are in place to prevent the takeover

---

<sup>1</sup> National Privacy Commission Circular 16-03, Sec. 18(b).

of the account or any amendment, withdrawal or cancellation.<sup>2</sup> It also alleges that “notification would not be in the best interest of the affected policy holders and may cause undue alarm.”<sup>3</sup> No evidence being submitted to support Sun Life’s claims, this Commission denied its request for exemption.

Seeking the reconsideration of the Commission’s 29 July 2019 Resolution, Sun Life filed a letter dated 5 September 2019 reiterating its earlier submissions emphasizing the measures it has taken to prevent a recurrence of the incident, the controls it has in place to prevent any fraudulent use of the information on its system, and the lack of any concern or complaints received in relation to the information that was disclosed. Despite the Commission’s finding in its previous Resolution regarding Sun Life’s failure to submit any evidence to support its claims, Sun Life again chose not to provide this Commission with any evidence to support its assertions. Instead, it simply asserts that “there is no vulnerability pertaining to access in this case that may be exploited by others.”

While Sun Life may have taken the necessary steps to secure its system and prevent a recurrence of that incident, these remain mere assertions in the absence of any evidence to support them. In addition, the steps outlined by Sun Life are only with regard to the risks that may arise in relation to its own system. It did not consider the other risks, such as phishing or social engineering attacks, that its data subjects may be subjected to as a result of the breach.

When the Data Privacy Act (“DPA”) states as one of the criteria for notification that the “unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject,”<sup>4</sup> it does not qualify that the risks and harms that should be considered are only those within the control of the personal information controller that was breached. Instead, the risks and harms that data subjects may face must be viewed holistically taking into consideration all the relevant circumstances.

## **B. The procedure followed by Sun Life is improper**

In response to this Commission’s Show Cause Order, Sun Life explained that the procedure it followed was not prohibited under this Commission’s rules and that it was merely trying to exhaust all administrative remedies when it met with our Enforcement Division to submit additional documents in support of its request for reconsideration. These will be discussed in *seriatim*.

### *i. A second Motion for Reconsideration is not allowed.*

Sun Life asserts that: “there is nothing in NPC Circular 16-03 that prohibits a second motion for reconsideration. Absent such prohibition, the Honorable Commission cannot categorically state that ‘a second request or motion for reconsideration is not allowed under NPC Circular 16-03.’”<sup>5</sup>

Sun Life correctly states that NPC Circular 16-03 does not contain any prohibition on the filing of a second motion for reconsideration. It also does not contain anything on the

---

2 See, 19 October 2017 letter of Sunlife.

3 *Id.*

4 Republic Act No. 10173, Sec. 20 (f).

5 Sun Life’s letter dated 26 August 2020, p. 4.

process of filing a motion for reconsideration. As Sun Life is undoubtedly aware, NPC Circular 1603 only provides for the obligation of personal information controllers in relation to breaches, including the obligation to notify the Commission and data subjects in the event of a breach.<sup>6</sup> The Commission’s Rules of Procedure are contained in NPC Circular 1604, Section 2 of which states:

**SECTION 2. Scope and Coverage.** – These rules shall apply to all complaints filed before the National Privacy Commission or such other grievances, requests for assistance or advisory opinions, and other matters cognizable by the National Privacy Commission

The proceedings involving personal data breach notifications clearly fall under “other matters cognizable by the National Privacy Commission.” Hence, the determination whether a personal information controller such as Sun Life may be exempted from the requirement of notifying its data subjects is a matter falling within the scope of NPC Circular 16-04.

It is a basic rule of statutory construction that statutes must be construed and harmonized with other statutes to form a uniform system of jurisprudence.<sup>7</sup> Simply because NPC Circular 16-03 does not contain a provision prohibiting the filing of a second motion for reconsideration does not mean that it is allowed, as Sun Life claims, especially since it is expressly prohibited by NPC Circular 16-04:

**SECTION 30. Appeal.** – The decision of the National Privacy Commission shall become final and executory fifteen (15) days after the receipt of a copy thereof by the party adversely affected. **One motion for reconsideration may be filed**, which shall suspend the running of the said period. Any appeal from the Decision shall be to the proper courts, in accordance with law and rules.<sup>8</sup>

On the basis of this same provision, this Commission’s 28 October 2019 Resolution denying Sun Life’s Motion for Reconsideration has already become final and executory. As Sun Life itself admitted in its response to the Show Cause Order:

4. On 04 December 2019, Sun Life received the Honorable Commission’s Resolution dated 28 October 2019 (the “October Resolution”) denying the request for reconsideration in the September 2019 Letter.

5. On 23 December 2019, Sun Life responded to the October Resolution by submitting a letter dated 23 December 2019 (the “December 2019 Letter”) requesting for the deferment of the running of the period within which to comply with the requirements of the July Resolution pending a meeting with the Honorable Commission’s Enforcement Division.<sup>9</sup>

Even assuming Sun Life’s filing of the 23 December 2019 letter is allowed, it was filed beyond reglementary period having been filed nineteen (19) days after Sun Life received a copy of this Commission’s resolution denying its request for reconsideration.

*ii. Sun Life’s reliance on the doctrine of exhaustion of administrative remedies is misplaced.*

6 See, NPC Circular 16-03, Sec. 2. Emphasis supplied.  
7 See, Akbayan-Youth v. Commission on Elections, G.R. No. 147066, 26 March 2011.  
8 Emphasis supplied.  
9 Sun Life’s letter dated 26 August 2020, p. 2.

Its second request for reconsideration having been filed out of time and in clear contravention of the prohibition on the filing of second motions for reconsideration, Sun Life cannot now claim that it was merely exhausting administrative remedies when it sought to meet with this Commission's Enforcement Division and submit additional evidence.

In the first place, the proper time to submit evidence to substantiate its request for exemption was when it first filed the same or, at the very least, when this Commission called its attention to this deficiency in the 29 July 2019 Resolution. In both instances, Sun Life either failed or chose not to.

If Sun Life believes that this Commission's decision denying its request for exemption did not consider all the relevant factors, it only has itself to blame for not submitting all the necessary evidence and raising all of its arguments when it had numerous opportunities to do so.

Similar to parties coordinating with the sheriff in the execution stage of a court case, it should be stressed that there is nothing wrong with meeting with the Enforcement Division to clarify how compliance with this Commission's resolution should best be carried out. It is an altogether different matter, however, to attempt to get the sheriff to intercede on a party's behalf to reverse the decision of the court. This is what Sun Life attempted to do in this case. While this Commission endeavors to keep an open line of communication with its stakeholders, this does not mean that proper procedure can be dispensed with especially in pending cases and more so in cases, such as this one, where a decision has already been rendered. This is not what the doctrine of exhaustion of administrative remedies contemplates.

In addition, Sun Life attempts to justify its refusal to comply with this Commission's decision by pointing to the length of time that has passed from the time it requested for exemption until the denial, stating: ‘

Without a doubt, it heightened Sun Life's earlier concern that a notification would cause undue alarm on the part of the data subjects.

Considering the foregoing factual antecedents, it was reasonable for Sun Life to be persistent in seeking a reconsideration of the July Resolution and the October Resolution, hence, the submission of the October 2019 Letter and the December 2019 Letter.<sup>10</sup>

To reiterate, the notification of data subjects is the general rule. In asking for exemption from this general rule, personal information controllers like Sun Life bind themselves to comply with this Commission's Decision on their request. They cannot impose as a condition to such compliance that the Decision must be rendered within a period of time convenient to them. In the absence of a change in circumstances that would render compliance impossible, and Sun Life has not alleged much less submitted any evidence in this regard, it is subject to the requirements of the DPA and NPC Circular 16-03, as clarified by the Commission in its Decision.

Nevertheless, at its core, the notification requirement under NPC Circular 16-03 is for the protection and benefit of data subjects. This Commission acknowledges the efforts

---

<sup>10</sup> Sun Life's letter dated 26 August 2020, p. 3.

Sun Life made to address the breach when it occurred and, although delayed, the efforts it has since undertaken to properly notify and protect its data subjects as shown in its 07 July 2020 and 28 July 2020 letters.

Despite the issues discussed herein being straightforward, rooted as they are in express provisions and clear principles of the Data Privacy Act and its related issuances, this Commission recognizes that misconceptions and misapplications of these doctrines still persist. Considering that the factual antecedents of this case all occurred during the time of Sun Life’s previous data protection officer, hopefully Sun Life will take stock of the circumstances of this case and the Commission expects it to take the necessary steps to ensure not only that this situation will not be repeated but, more importantly, that it will be in a better position to safeguard its data subjects. Compliance with the DPA entails more than simply ticking off boxes on a checklist such as the registration of a Data Protection Officer, conduct of a privacy impact assessment, creation of a data protection policy, or the exercise of breach reporting procedures. Companies must realize that compliance with the DPA involves doing such activities within a framework of protecting the data subjects from very real risks, such as what the affected data subjects faced in this case.

Guided by the principle that the power of contempt should be used sparingly, judiciously, and with utmost self-restraint,<sup>11</sup> this Commission resolves to consider Sun Life as having satisfactorily complied with the Show Cause Order. Sun Life is warned, however, that any violation of a similar nature will be dealt with more severely.

**WHEREFORE**, the above premises considered, the Commission resolves to consider this matter **CLOSED**. Sun Life of Canada (Philippines), Inc. is hereby given a **STERN WARNING** that a repetition of this conduct or a similar infraction shall be dealt with more severely.

**SO ORDERED.**

City of Pasay, Philippines;  
10 September 2020.

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
*Deputy Privacy Commissioner*

WE CONCUR:

**Sgd.**  
**RAYMUND ENRIQUEZ LIBORO**  
*Privacy Commissioner*

---

<sup>11</sup> See, *Baustista v. Yujuico*, G.R. No. 199654, 03 October 2018.

**Sgd.**  
**JOHN HENRY D. NAGA**  
*Deputy Privacy Commissioner*

**COPY FURNISHED:**

**JSC**  
*Data Protection Officer*

**ENFORCEMENT DIVISION**  
**COMPLIANCE AND MONITORING DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

X-----X

RESOLUTION

AGUIRRE, D.P.C.:

This Resolution refers to the request for Postponement of Notification to affected data subjects of Batangas Bay Carriers, Inc. (Batangas Bay), a subsidiary of Magsaysay Shipping & Logistics, dated 01 September 2020,<sup>1</sup> involving a personal data breach caused by a ransomware attack.<sup>2</sup>

The Facts

On 26 August 2020, some users reported that their files stored in the company’s shared network drive could not be opened. This was reported to the IT Servicedesk and upon checking, they discovered that the files have been encrypted and the file extensions have been changed to .ROGER. The research showed that the incident was caused by a certain strain of ransomware virus. Around the same time, they realized that other servers at the Time Plaza Data Center, which hosts other systems, applications or databases, were infected by the same ransomware virus.<sup>3</sup>

On 01 September 2020, Batangas Bay was able to determine that the availability of personal data in its payroll database was compromised due to encryption as a result of the ransomware attack. In its report, the officers stated that they remain hopeful that the data’s availability can be restored through decryption without paying a ransom.<sup>4</sup>

As it was unclear what vulnerabilities in the data processing system allowed the breach, Batangas Bay engaged cybersecurity experts to learn more about the incident during the investigation.<sup>5</sup>

As to the number of individuals or personal records affected, the officers of Batangas Bay claim that it is yet to be determined. Nonetheless, they believe the number to be more than one hundred (100) individuals.<sup>6</sup>

Batangas Bay believes that the most likely consequence of this incident is data loss arising from an inability to decrypt the affected files since the security incident involves a ransomware. In the report, the officers state that there is no indication that personal data has been acquired by unauthorized persons. However, they expect that the data loss will be minimal and temporary as it backs up data constantly and the same are intact.<sup>7</sup>

The report indicated the following as the personal data possibly involved in this breach: name, birthday, age, marital status, number of dependents, home address, salary and

1 Possible availability breach due to ransomware affecting Payroll Database dated 1 September 2020.  
2 Ibid., at p. 2.  
3 Ibid., at pp. 1-2.  
4 Ibid., at p. 2.  
5 Ibid., at p. 2  
6 Ibid., at p. 2  
7 Ibid., at p. 2



allowance, government ID numbers, bank account numbers, contact numbers, and employment information.<sup>8</sup>

Batangas Bay reports that it has undertaken the following measures to address the breach:

- (1) All servers were shut down to contain the virus and allow the IT team to inspect each server;
- (2) An incident advisory was sent to all users and management on 27 August 2020, and all units were advised to apply business continuity plans and workarounds while the servers or systems are down;
- (3) Security patches for the ransomware were applied to nonaffected servers; (
- 4) Cybersecurity vendors were tapped to assist on the containment, clean-up, and possible decryption of affected files; and
- (5) The network traffic from and to the network was stopped, thus disconnecting the internet access in Times Plaza on 27 August 2020. The internet connection was diverted to Antonino building, the back-up center. This enabled the cybersecurity vendor and IT to monitor the link, and determine any suspicious and virus-related activities.<sup>9</sup>

However, Batangas Bay stated that it has yet to notify the affected data subjects since it still needs to determine precisely who were affected, and that it is not reasonably possible to notify them all individually within a span of seventy two (72) hours.<sup>10</sup> It also claims that it has no reason to believe at the time that any data has been acquired by an unauthorized person or that the breach is likely to give rise to a real risk of serious harm to the affected data subjects.<sup>11</sup>

Hence, the instant request for postponement of notification of data subjects until such time that it has ascertained the identities of the affected data subjects.<sup>12</sup>

## **Discussion**

This Commission denies the herein request for postponement of notification to data subjects of Batangas Bay in accordance with NPC Circular No. 16-03 (Personal Data Breach Management).

At the outset, it should be emphasized that notification of data subjects of data breaches is the general rule. Under Section 18(A) of NPC Circular No. 16-03, it provides that:

**The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.** The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.<sup>13</sup>

---

8 *Ibid.*, at p. 2

9 *Ibid.*, at p. 2

10 *Ibid.*, at p. 2

11 *Ibid.*, at p. 1.

12 *Ibid.*, at p. 2.

13 Emphasis supplied.

The exemption or postponement will only be allowed in exceptional circumstances under Section 18(B) of NPC Circular No. 16-03, which provides that:

**If it is not reasonably possible to notify the data subjects within the prescribed period**, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification. A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects. The Commission may authorize the postponement of notification **where it may hinder the progress of a criminal investigation related to a serious breach**, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.<sup>14</sup>

The report of Batangas Bay does not contain any narration of a “criminal investigation related to a serious breach that may hinder the progress thereof, taking into account circumstances provided in Section 13 of the said Circular, and other risks posed by the personal data breach” in order for the Commission to consider its request for postponement. Following this, the instant request for postponement is not proper and must be denied.

The Commission notes that Batangas Bay also asserts that it has yet to determine the identities of the affected data subjects, as the ground for their request for postponement of notification of data subjects. This is not plausible as Batangas Bay has categorically reported that it has ascertained that the subject ransomware attack affected the availability of personal data in the company’s payroll database. Considering that the affected database is the payroll system, it should be able to readily identify the data subjects as the persons therein are its own employees.

Batangas Bay’s report and request also contains a contention that, since the security incident involves ransomware, it has no reason to believe that any data has been acquired by an unauthorized person or that the breach is likely to give rise to a real risk of serious harm to the affected data subjects.

On this issue, the Commission finds that no evidence was presented to support this claim. It is a basic rule of evidence and procedure that the Commission cannot simply rely on bare allegations and must look at the available evidence on record to see whether these are sufficient to overcome the presumption that notification is in the best interest of the data subjects.

The Commission also notes that Batangas Bay seems to connect the fact that the security incident involved ransomware with the lack of any indication that personal data has been acquired by unauthorized persons.

Section 11 of NPC Circular 16-03 states the conditions for notification, thus:

**SECTION 11. When notification is required.** Notification shall be required upon knowledge of or when there is reasonable belief by the personal information

controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

<sup>14</sup> Emphasis supplied.

1. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, “other information” shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject

Certain misconceptions about Section 11(2) of NPC Circular 16-03 (Section 11(2)) must be clarified. A loss of control over personal data held in custody should be enough for a personal information controller to have “reason to believe that the information may have been acquired by an unauthorized person.” An indication of exfiltration of data is not a requirement in Section 11(b). Absolute certainty of acquisition by an unauthorized person is not required by either the Circular or the Data Privacy Act (DPA), considering that the condition only provides for a determination based on the existing circumstances that can give a “reason to believe.”

This liberal interpretation of the conditions necessitating mandatory breach notification is rooted in Section 20(f) of the DPA itself, which provides:

The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.<sup>15</sup>

The infection of the system by a ransomware should be sufficient to form a reasonable belief for the personal information controllers.

Ransomware is defined as “a type of malicious software that infects a computer and restricts users’ access to it until a ransom is paid to unlock it... Typically, these alerts state that the user’s systems have been locked or that the user’s files have been encrypted. Users are told that unless a ransom is paid, access will not be restored.”<sup>16</sup> While ransoms primarily cause availability breaches, it is different from other availability breaches because a malefactor intentionally causes them. This is unlike other types of availability breaches that are caused by accidents or system glitches. In these cases, the total exercise of control over the data is removed from the personal information controller and is taken by the malefactor. Without this control, the personal informa-

<sup>15</sup> Emphasis supplied.

<sup>16</sup> UC Berkeley Information Security Office (n.d).Frequently Asked Questions- Ransomware. Retrieved from <https://security.berkeley.edu/faq/ransomware/>.

tion controller will be unable to exercise its obligations in processing the personal data according to the provisions of the DPA. Recent ransomware attacks have also shown a capability to release the encrypted data over the internet upon non-payment of the ransom, potentially leading to a confidentiality breach contemplated in Section 11(2). For the protection of the data subjects, such incidents must be notified both to the Commission and the affected data subjects.

This construction of Section 11(2) is guided by the Interpretation Clause in the DPA which states:

Section. 38. *Interpretation.* – Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.

**WHEREFORE**, premises considered, the request for Postponement of Notification to Data Subjects filed by Batangas Bay Carriers, Inc. is hereby **DENIED**.

Batangas Bay Carriers, Inc. is **ORDERED** to notify the affected data subjects of the breach incident in accordance with the provisions of NPC Circular 16-03 and to **SUBMIT** proof of compliance thereto **within fifteen (15) days** from receipt of this Resolution.

**SO ORDERED.**

Pasay City, Philippines;  
21 September 2020.

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

**Sgd.**  
**RAYMUND ENRIQUEZ LIBORO**  
Privacy Commissioner

**Sgd.**  
**JOHN HENRY D. NAGA**  
Deputy Privacy Commissioner

**COPY FURNISHED:**

**CRD**  
*Data Protection Officer*

**COMPLIANCE AND MONITORING  
DIVISION ENFORCEMENT DIVISION  
GENERAL RECORDS UNIT**  
National Privacy Commission

X-----X

**RESOLUTION****AGUIRRE, D.P.C.:**

Before the Commission is the Compliance dated 12 May 2021 submitted by ABS-CBN Corporation (ABS-CBN) in fulfillment of the directive in the Order dated 11 March 2021.<sup>1</sup>

**The Facts**

On 26 August 2020, some users reported that their files stored in the company's shared On 11 March 2021, the Commission issued an Order instructing ABSCBN to submit proof of its notification to the affected data subjects:

**WHEREFORE**, the Commission **ORDERS** ABS-CBN Corporation to submit proof of notification to the two-hundred eight (208) data subjects who were affected by the breach, **within fifteen (15) days** from receipt of this Order.

**SO ORDERED.**<sup>2</sup>

ABS-CBN, through its newly appointed Data Protection Officer (DPO), acknowledged that it received the Order dated 11 March 2021 through e-mail on 05 April 2021.<sup>3</sup> Further, it informed the Commission that according to its former DPO, it provided an update on the notification of data subjects to the Commission in September or October 2018.<sup>4</sup> Thereafter, ABS-CBN forwarded to the Commission the e-mail threads that showed the internal reports regarding the notification of affected data subjects.<sup>5</sup>

The National Privacy Commission's Enforcement Division (EnD) sent a Compliance Letter dated 22 April 2021 to ABS-CBN acknowledging receipt of the copy of e-mail threads.<sup>6</sup> The EnD, however, found the submissions insufficient and inadequate since the submissions did not contain proof that the data subjects were actually informed of the breach.<sup>7</sup> ABS-CBN's report only mentioned that it notified the data subjects through e-mails, phone calls, and letters sent through couriers.<sup>8</sup> The EnD instructed ABS-CBN to submit a copy of the breach notification sent to the affected data subjects and proof that the notification was received by the respective data subjects.<sup>9</sup>

On 12 May 2021, ABS-CBN submitted the following documents:

- 1 Compliance, 12 May 2021, in In re: ABS-CBN Corporation, NPC BN 18-179 (NPC 2022).
- 2 Order, 11 March 2021, at 8, in In re: ABS-CBN Corporation, NPC BN 18-179 (NPC 2022).
- 3 E-mail from LSA, Data Protection Officer of ABS-CBN Corporation, to National Privacy Commission (06 April 2021).
- 4 *Id.*
- 5 *Id.*
- 6 Letter Re: Order of the Commission En Banc dated 11 March 2021 (CID BN 18-179 "IN RE: ABS-CBN CORPORATION"), 22 April 2021, in In Re: ABS-CBN Corporation, NPC BN 18-179 (NPC 2022).
- 7 *Id.*
- 8 *Id.*
- 9 *Id.*

1. A template of the notification sent to the affected data subjects;<sup>10</sup>
2. Online Store Report – Summary of Actions Taken;<sup>11</sup>
3. Copy of the actual e-mails sent to affected data subjects;<sup>12</sup>
4. Outbound Call Log Results;<sup>13</sup>
5. Status of E-mails and Callouts;<sup>14</sup>
6. Recordings of the phone calls to affected data subjects;<sup>15</sup>
7. Certification from Slash.PH;<sup>16</sup> and
8. Delivery Status Report of Couriered Mail.<sup>17</sup>

The EnD acknowledged the receipt of ABS-CBN’s submissions, but it determined that there were still insufficiencies in the submissions.<sup>18</sup> It stated that the copy of the e-mails sent to affected data subjects failed to prove that they received the notification since there were no acknowledgments from the recipients that were included.<sup>19</sup> The EnD further noted the discrepancy between the number of recorded successful call-outs and the number of data subjects actually notified by phone call.<sup>20</sup> According to the EnD, the Online Store Report identified a total of sixty (60) successful call-outs, while ABS-CBN only sent thirty-four (34) call recordings.<sup>21</sup> The EnD also stated that in relation to the notification of data subjects by mail, the tracking numbers provided by ABS-CBN from the courier could not be verified on the courier’s website.<sup>22</sup>

The EnD, thus, reiterated its instructions for ABS-CBN to submit a copy of the breach notification sent to the affected data subjects and proof of receipt of the notification.<sup>23</sup> It further ordered ABS-CBN to submit a complete status report of the notification to affected data subjects, which should specify the number of data subjects notified through e-mail, phone, or courier.<sup>24</sup>

On 22 October 2021, ABS-CBN explained that it sent a copy of the emails sent to the affected data subjects because it no longer has a copy of the return receipts in its system.<sup>25</sup> As to the discrepancy with the number of data subjects successfully notified by phone call, ABS-CBN stated that it submitted four (4) e-mails containing the call recordings to the Commission on 12 May 2021.<sup>26</sup> In relation to the tracking numbers from the courier, ABS-CBN explained that old tracking numbers could no longer be accessed from the courier’s website.<sup>27</sup> It manifested that it would submit a certification from the

---

10 E-mail from LSA, Data Protection Officer of ABS-CBN Corporation, to National Privacy Commission (12 May 2021), Annex A.

11 *Id.* Annex B.

12 *Id.* Annex C.

13 *Id.* Annex D.

14 *Id.* Annex E.

15 *Id.* Annex F.

16 E-mail from LSA, Data Protection Officer of ABS-CBN Corporation, to National Privacy Commission (12 May 2021), Annex G.

17 *Id.* Annex H.

18 Letter Re: Order of the Commission En Banc dated 11 March 2021 (CID BN 18-179 “IN RE: ABS-CBN CORPORATION”), 11 October 2021, in In Re: ABS-CBN Corporation, NPC BN 18-179 (NPC 2022).

19 *Id.*

20 *Id.*

21 *Id.*

22 *Id.*

23 *Id.*

24 Letter Re: Order of the Commission En Banc dated 11 March 2021 (CID BN 18-179 “IN RE: ABS-CBN CORPORATION”), 11 October 2021, in In re: ABS-CBN Corporation, NPC BN 18-179 (NPC 2022).

25 E-mail from LSA, Data Protection Officer of ABS-CBN Corporation, to National Privacy Commission (22 October 2021).

26 *Id.*

27 *Id.*

courier that the tracking numbers were valid and the mails were successfully delivered.<sup>28</sup>

On 14 February 2022, the EnD sent another letter to ABS-CBN informing it that the submitted copy of the contents of the breach notification still failed to show proof that all affected data subjects received the notification.<sup>29</sup> According to the EnD, ABS-CBN reported that it sent e-mail notifications to two hundred one (201) out of two hundred twenty-five (225) data subjects.<sup>30</sup> The screenshots submitted by ABS-CBN, however, did not show that the data subjects acknowledged that they received the e-mail.<sup>31</sup> The EnD found that the e-mail notification failed to prove that the data subjects were actually notified or that they received the notification.<sup>32</sup> It instructed ABS-CBN to submit proof that all affected data subjects received the notification, which may include “e-mail tracking showing the status of the e-mail sent, sworn affidavit of the person who sent the e-mail notifications, sworn affidavit of the person who called the data subjects through phone, or proof of receipt from the private courier.”<sup>33</sup>

As to the submitted call recordings, the EnD reiterated that it was able to extract only thirty-four (34) call recordings.<sup>34</sup>

On 03 March 2022, ABS-CBN further clarified certain matters in relation to its submissions.<sup>35</sup> It explained that it could not provide a sworn affidavit of the person who sent the notification to affected data subjects by e-mail because the person is no longer connected with ABS-CBN’s third-party service provider.<sup>36</sup> Hence, ABS-CBN manifested whether it could submit a certification from iCONN, ABS-CBN’s third-party service provider, attesting that all e-mails were successfully delivered and that there were only seven (7) undeliverable receipts.<sup>37</sup> As to the call recordings, ABS-CBN explained that sixty-four (64) call-outs were actually made, but four (4) of the call recordings were no longer on file; thus, only sixty (60) call recordings were submitted through e-mail on 12 May 2021.<sup>38</sup> Lastly, ABS-CBN stated that it submitted a copy of the certification from the courier to prove that seven (7) mails were successfully delivered to the recipients who had no e-mail addresses nor contact numbers on record.<sup>39</sup>

The EnD, through its Compliance Letter dated 01 August 2022, instructed ABS-CBN to submit proof that the two hundred eight (208) affected data subjects indicated in the Order dated 11 March 2021 received the breach notification and submit the remaining recordings of successful callouts.<sup>40</sup>

On 18 August 2022, ABS-CBN clarified that there were actually two hundred nine (209)

---

28 *Id.*  
29 Letter Re: Order of the Commission En Banc dated 11 March 2021 (CID BN 18-179 “IN RE: ABS-CBN CORPORATION”), 14 February 2022, in In Re: ABS-CBN Corporation, NPC BN 18-179 (NPC 2022).  
30 *Id.*  
31 *Id.*  
32 *Id.*  
33 *Id.*  
34 *Id.*  
35 E-mail from LSA, Data Protection Officer of ABS-CBN Corporation, to National Privacy Commission (03 March 2022).  
36 *Id.*  
37 *Id.*  
38 *Id.*  
39 *Id.*  
40 Letter Re: Compliance with Order dated 11 March 2021 (CID BN 18-179 “IN RE: ABS-CBN CORPORATION”), 01 August 2022, in In Re: ABS-CBN Corporation, NPC BN 18-179 (NPC 2022).

affected data subjects.<sup>41</sup> According to ABS-CBN, out of the two-hundred nine (209) affected data subjects, twohundred two (202) were notified by e-mail.<sup>42</sup> ABS-CBN manifested that it submitted copies of the two hundred one (201) e-mails to the Commission on 12 May 2021, while the remaining e-mail was missing from its records.<sup>43</sup> The remaining seven (7) out of the twohundred nine (209) affected data subjects were notified by mail sent through a private courier.<sup>44</sup> ABS-CBN specified that it submitted on 18 November 2021 the private courier’s certification that the mails were received by the appropriate recipients.<sup>45</sup>

ABS-CBN further manifested that it has successfully notified by phone call sixty (60) data subjects out of eighty-one (81) affected data subjects whose contact numbers were found on record.<sup>46</sup> It reported that it submitted the recordings of the sixty (60) successful callouts in three (3) separate e-mails to the Commission.<sup>47</sup>

In its e-mail to the Commission dated 18 August 2022, ABS-CBN attached the Sworn Affidavit of RSC, the team lead who was directly involved in sending the notification to affected data subjects by e-mail.<sup>48</sup> Further, ABS-CBN re-sent the recordings of the sixty (60) successful callouts.<sup>49</sup>

### **Issue**

Whether the submissions of ABS-CBN sufficiently complied with the Order dated 11 March 2021.

### **Discussion**

The Commission resolves to close the case upon finding that ABSCBN has complied with the Order dated 11 March 2021.

In concurrence with the EnD’s assessment,<sup>50</sup> the Commission finds that the documents submitted by ABS-CBN are sufficient to prove that it adequately notified the affected data subjects of the details of the breach.

ABS-CBN’s notification to affected data subjects included the information required under NPC Circular 16-03 (Personal Data Breach Management).

Section 18 (C) of NPC Circular 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:

---

41 E-mail from LSA, Data Protection Officer of ABS-CBN Corporation, to National Privacy Commission (18 August 2022).

42 *Id.*

43 *Id.*

44 *Id.*

45 *Id.*

46 *Id.*

47 E-mail from LSA, Data Protection Officer of ABS-CBN Corporation, to National Privacy Commission (18 August 2022).

48 *Id.* Annex A.

49 *Id.*

50 Enforcement Assessment Report, 27 September 2022, at 4, in In re: ABS-CBN Corporation, NPC BN 18-179 (NPC 2022).



...

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.<sup>51</sup>

The notification stated that there was a report of a data breach of ABS-CBN's online shopping facility and identified that the credit card details of the affected data subjects may have been exposed.<sup>52</sup> The notification also specified that ABS-CBN temporarily took down the ABS-CBN Store and the UAAP Store websites.<sup>53</sup> It also advised the data subjects to change their usernames and passwords and to not provide any personal data to anyone who claims to be an ABSCBN representative.<sup>54</sup> The notification also provided an e-mail address where the data subjects could send their questions or concerns.<sup>55</sup>

In addition, the copies of the e-mails sent to the affected data subjects,<sup>56</sup> the Sworn Affidavit of Raymond Joseph S. Cerbas,<sup>57</sup> the recordings of phone calls to affected data subjects<sup>58</sup> and the delivery status report from the courier<sup>59</sup> substantially prove that ABS-CBN notified the affected data subjects regarding the breach. The EnD found that these submissions comply with the requirements provided under Section 18 (A) and Section 18 (D) of NPC Circular 1603.<sup>60</sup> Hence, it is recommended that the case be closed.<sup>61</sup> The Commission affirms the EnD's recommendation and closes the case.

Nonetheless, the Commission stresses that the determination of whether ABS-CBN's acts or omissions contributed to the breach or gave rise to other violations of the DPA are beyond the scope of NPC Circular 16-03 and the matters currently before the Commission.

**WHEREFORE**, premises considered, the Commission resolves that NPC BN 18-179 – In re: ABS-CBN Corporation is hereby **CLOSED**.

51 National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §18 (C) (15 December 2016).

52 E-mail from LSA, Data Protection Officer of ABS-CBN Corporation, to National Privacy Commission (12 May 2021), Annex A.

53 *Id.*

54 *Id.*

55 *Id.*

56 *Id.* Annex C.

57 *Id.* Annex A.

58 E-mail from LSA, Data Protection Officer of ABS-CBN Corporation, to National Privacy Commission (12 May 2021), Annex F.

59 E-mail from LSA, Data Protection Officer of ABS-CBN Corporation, to National Privacy Commission (12 May 2021).

60 Enforcement Assessment Report, 27 September 2022, at 6, in In re: ABS-CBN Corporation, NPC BN 18-179 (NPC 2022).

61 *Id.*

Further, pursuant to Rule X, Section 1 of NPC Circular 2021-01 (2021 NPC Rules of Procedure), the Commission **ORDERS** its Complaints and Investigation Division (CID) to conduct a sua sponte investigation on possible violations under Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, that may have been committed by ABS-CBN Corporation.

**SO ORDERED.**

City of Pasay, Philippines.  
12 October 2022.

**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

I CONCUR:

**JOHN HENRY D. NAGA**  
Privacy Commissioner

Copy furnished:

**LSA**  
*Data Protection Officer*

**ABS-CBN Corporation**  
8th floor, ELJ Building,

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

X-----X

## **RESOLUTION**

### **AGUIRRE, D.P.C.:**

Before the Commission is the Compliance dated 29 December 2020 submitted by the University of the Philippines – Visayas (UP Visayas) in fulfillment of the Commission’s directive in its Order dated 15 December 2020.

### **Facts**

On 07 April 2018, UP Visayas submitted its Data Breach Incident Report dated 05 April 2018, informing the Commission of a confidentiality breach where unauthorized individuals gained access to its system using an existing username without administrative privileges:

SQL Injection attempts in the University’s Research, Creative Works, Public Service and Publication System (RCWPSPS). Hackers were able to gain access to the system by guessing the password of existing users with easy guess password.<sup>1</sup>

UP Visayas stated that the hackers logged in to the system on 29 March 2018 at around 10:02 PM and “lasted for only 15 seconds.”<sup>2</sup> It claimed that the data was not compromised since the “attempts to query data on the database were blocked by the firewall.”<sup>3</sup> Further, it alleged that the hackers were not allowed access to the personal data since the username was not allowed for that kind of operation.<sup>4</sup>

According to UP Visayas, only one account was compromised, and based on the assessment of its system developer and system and network administrators, no data was copied or taken out of the system.<sup>5</sup>

Further, UP Visayas identified that the following personal data may have been involved:

1. Description of sensitive personal information involved

The system contains records of research, creative work, and public service project, as well as publications and other outputs of faculty and researchers [sic] from the various units and colleges of the University of the Philippines Visayas. The system also records email address, phone numbers, high school degree, awards, general and specific experience, roles on project and image of personnel.

2. Description of other information involved that may be used to enable identity fraud

---

1 Data Breach Incident Report, 05 April 2018, at 1 in In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).

2 *Id.*

3 *Id.*

4 *Id.*

5 *Id.*

Part of the records kept at the system is the list of private sectors and the government institution partners/collaborators of projects, certificates of projects and completion, certificates of participation in research, creative works, public service, and publications projects. Reports, documentations, and other relevant certificates are also recorded and stored by the system.<sup>6</sup>

To address the breach, UP Visayas shut down access to the database of the involved system and disabled all usernames with easy passwords.<sup>7</sup>

On 25 October 2018, the Commission, through its Complaints and Investigations Division (CID), sent a letter inviting UP Visayas to a meeting on 03 December 2018 to discuss the breach.<sup>8</sup>

On 19 December 2018, along with additional documents, UP Visayas submitted a copy of the notification it sent to the affected data subject, DJB. The notification informed DJB of the SQL injection attempts in UP Visayas' RCWPPS, that her username and password were used to log into the system, and that "possible access to [her] name, address and research work titles were compromised."<sup>9</sup> Further, UP Visayas informed her that her username and password were disabled and subsequently modified after the incident.<sup>10</sup>

On 15 December 2020, the Commission issued an Order requiring UP Visayas to submit a Post-Breach Report within fifteen (15) days from receipt of the Order.<sup>11</sup>

In response, UP Visayas submitted its Post-Breach Report dated 29 December 2020.<sup>12</sup> It emphasized that in addition to the measurements it took regarding passwords, users must now connect to UP Visayas' internet connection in order to access the website.<sup>13</sup> UP Visayas claimed that, as a result, "there has been no recurrence of a similar incident after the University has undertaken the security measures and breach management."<sup>14</sup>

### **Issue**

Whether UP Visayas has complied with the directives of the Commission in its 15 December 2020 Order.

### **Discussion**

The Commission resolves to close the case considering that UP Visayas has sufficiently complied with the Commission's directive in its 15 December 2020 Order.

In its Post-Breach Report dated 29 December 2020, it sufficiently explained the nature

---

6 *Id.* at 2.

7 Data Breach Incident Report, 05 April 2018, at 2 in In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).

8 Breach Notification of UP Visayas, 25 October 2018, at 1 in In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).

9 Unauthorized Access to RCWPPS dated March 29, 2018, 19 December 2018, at 1 in In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).

10 *Id.*

11 Order, 15 December 2020, at 1 in In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).

12 Post-Breach Report, 29 December 2020 in In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).

13 *Id.* at 2.

14 *Id.*

of the incident and the circumstances regarding its discovery.<sup>15</sup> It also enumerated and submitted proof of the security measures it executed as a response to the incident, such as conducting a system audit, automatically shutting down access to the database, disabling and re-setting the passwords, and making the site available only through its university intranet.<sup>16</sup> Lastly, in compliance with the notification requirements, it informed DJB of the unauthorized access to the RCWPPS through her account.<sup>17</sup>

More importantly, the Commission stresses that the SQL injection attempts were not subject to mandatory breach notification since it was a security incident. There is a distinction between a security incident and a personal data breach.

Section 3 (F) of NPC Circular 16-03 defines a personal data breach:

*Section 3. Definition of Terms.*

...

F. "Personal Data Breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. It may be in the nature of:

1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
2. Integrity breach resulting from alteration of personal data; and/or
3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.<sup>18</sup>

On the other hand, Section 3 (J) of NPC Circular 16-03 defines a security incident:

*Section 3. Definition of Terms.*

...

J. "Security Incident" is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place[.]<sup>19</sup>

In this case, the SQL injection attempts are considered security incidents considering that there is no personal data that was compromised. As a matter of fact, attempts to query data and access personal data were not permitted and blocked by the firewall because the username DJB was not allowed to perform those kinds of operations.<sup>20</sup> Therefore, other than the access of DJB username, no other personal data was involved in the security incident. Given that there was no accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data in this case since access to personal data was not permitted through DJB username, it is not a personal data breach; rather, it is a security incident.

---

<sup>15</sup> *Id.* at 1.

<sup>16</sup> *Id.*

<sup>17</sup> *Id.* at 2.

<sup>18</sup> National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16- 03], § 3 (F) (15 December 2016).

<sup>19</sup> *Id.* § 3 (J).

<sup>20</sup> Data Breach Incident Report, 05 April 2018, at 1 in In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022); Post-Breach Report, 29 December 2020, at 1 in In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).

Moreover, UP Visayas' swift actions and security measures ensured that the security incident would not result into an eventual personal data breach. The actions and measures executed after the incident proved successful since there has been no recurrence of any similar incident up to this date.<sup>21</sup>

Thus, UP Visayas faithfully complied with the procedures under NPC Circular 16-03 and successfully executed its obligations as a Personal Information Controller. Further, it has sufficiently complied with the Orders and immediately implemented security measures to protect its data subjects' personal information.

**WHEREFORE**, premises considered, Commission resolves that NPC BN 18-045 In re: University of the Philippines – Visayas is hereby **CLOSED**.

**SO ORDERED.**

City of Pasay, Philippines.  
10 November 2022

**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

I CONCUR:

**JOHN HENRY D. NAGA**  
Privacy Commissioner

Copy furnished:

WLP  
*Data Protection Officer*  
**University of the Philippines - Visayas**

**NAT**  
*Data Protection Officer*

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

---

<sup>21</sup> See Post-Breach Report, 29 December 2020, at 2 in In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022)

X-----X

**RESOLUTION**

**AGUIRRE, D.P.C.:**

Before the Commission is the Full Breach Report dated 15 August 2022 submitted by Business World, Inc. (Business World) in compliance with the directive of the Commission in the Order dated 30 June 2022.<sup>1</sup>

**Facts**

Business World submitted its Initial Report dated 12 January 2018 informing the Commission that on 09 January 2018, it found a Facebook post of the group “Cyber-Chaos team” entitled “BusinessWorld database dump by Cyberchaos”.<sup>2</sup> The Cyber-Chaos team claimed that it “played with [sic] online security” of Business World’s online resource, www.bworldonline.com.<sup>3</sup>

According to Business World, it found that the list in the “data dump” included email addresses with the extension, “@bworldonline.com”, and email addresses associated with other companies.<sup>4</sup>

Upon Business World’s further investigation, it found that its new WordPress Content Management System (CMS) may have been compromised, including the personal details of thirty (30) of its employees.<sup>5</sup> Business World reported that the compromised personal details were the employees’ username, password, email address, first and last names, and administrative identification number.<sup>6</sup>

Business World also reported the following initial remediation steps to address the incident:

1. We contacted the Paste Bin site (where the relevant data was ‘dumped’) and, pursuant to our request, the lists that contain the personal data of the data subjects affected by this incident were taken down;
2. We initiated contacting the group Cyber-Chaos team and requested that they take down their post on the subject ‘data dump’. At the same [time], we submitted a report to Facebook requesting that the relevant post on the subject ‘data dump’ be removed/taken down. To date, we are awaiting the response of Facebook to our take-down request;
3. We changed the root passwords and other related access rights/tools to the servers/systems that cater to our online resource/portal;
4. We are currently reviewing our online resource/portal to check whether there are other data ‘missing’, and/or have other ‘malicious content’;

---

1 Full Breach Report, 15 August 2022, in In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).  
 2 Initial Report, 12 January 2018, at 1, in In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).  
 3 *Id.*  
 4 *Id.*  
 5 *Id.* at 1-2.  
 6 *Id.* at 2.

5. We are currently crafting and implementing ‘heightened security measures’ on our servers and systems; and
6. Our breach management and response team already reached out to the affected data subjects concerning this incident.<sup>7</sup>

The Commission, through its Complaints and Investigation Division (CID), issued an Order dated 30 June 2022 directing Business World to submit its Full Breach Report within fifteen (15) days from receipt of the Order.<sup>8</sup>

On 29 July 2022, Business World requested an extension to submit its Full Breach Report until 14 August 2022.<sup>9</sup> It claimed that since the incident, there were manpower changes in the company and that the employee who reported the incident to the Commission is no longer connected with the company.<sup>10</sup>

On 01 August 2022, the CID resolved to grant Business World’s request and directed it to submit the Full Breach Report within fifteen (15) days or until 15 August 2022.<sup>11</sup>

On 15 August 2022, Business World submitted its Full Breach Report.<sup>12</sup> It reported that on 08 January 2018 it received an email about the incident from “an affected user outside of Business World,” who claimed that only her email address was exposed due to the breach.<sup>13</sup>

Upon investigation, Business World discovered that the WordPress version it was using “became the entry point of the hackers to conduct a Structured Query Language (SQL) Injection.<sup>14</sup> Thereafter, the Cyber-Chaos team reportedly posted the “data dump” on pastebin.com.<sup>15</sup>

Further, Business World reported that the incident occurred when it was migrating its database from the old BusinessWorld website to the new WordPress-based site.<sup>16</sup>

Business World informed that the incident affected thirty (30) employees and one thousand four hundred seventy-five (1,475) individuals outside Business World.<sup>17</sup> It identified that as to the affected employees, the data exposed included the employees’ username and password for the old website, their email address with the extension “@bworldonline.com”, and the employees’ first and last name.<sup>18</sup> As to the affected individuals outside Business World, their email addresses were exposed.<sup>19</sup>

With regard to the measures it took to minimize harm or mitigate the impact of the breach, Business World reported the following:

---

7 *Id.* at 2.  
8 Order (To submit Full Breach Report), 30 June 2022, at 1, in In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).  
9 Email from JNC, Business World, Inc., to Complaints and Investigation Division, National Privacy Commission (29 July 2022).  
10 *Id.*  
11 Resolution of Motion for Extension, 01 August 2022, at 1, in In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).  
12 Email from ASD, Business World, Inc., to Complaints and Investigation Division, National Privacy Commission (15 August 2022).  
13 Full Breach Report, 15 August 2022, at 1, in In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).  
14 *Id.*  
15 *Id.*  
16 *Id.*  
17 *Id.* at 2.  
18 *Id.*  
19 Full Breach Report, 15 August 2022, at 2, in In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).



- i. We have built our own Wordpress site that is no longer dependent on 7th Media's customizations, enabling us to set updates to automatic, helping ensure that we are protected from exploits discovered of the said CMS
- ii. Usernames and passwords were randomly generated so that anyone trying to do a brute force attack will have a very difficult time
- iii. Passwords of users are reset every month
- iv. The URL of the login screen is changed every month
- v. The login screen has been geo-blocked and can only be accessed by Philippine IP addresses
- vi. We have changed hosting services to Conversant Content Delivery Network (CDN) and Web Application Firewall (WAF)...we have not been hacked since.
- vii. We have installed Wordpress plugins such as Sucuri Security and Blackhole for Bad Bots as additional layers of protection for our website.
- viii. Plugins are updated every Friday
- ix. The Wordpress Database is cleaned and optimized every Friday
- x. The old database that was compromised has been taken offline immediately after the incident has been discovered
- xi. Server credentials are changed every month.
- xii. No users from outside BusinessWorld are registered in the Wordpress CMS[.]<sup>20</sup>

According to Business World, it informed affected employees personally and sent notification letters to affected non-employees about the incident and the measures that must be done.<sup>21</sup> As proof of its notification to the affected individuals outside the company, Business World submitted a copy of the notification letter dated 17 January 2018.<sup>22</sup>

### **Issue**

Whether Business World sufficiently complied with the Order dated 30 June 2022.

### **Discussion**

The Commission resolves to close the case upon finding that Business World sufficiently complied with the Order dated 30 June 2022. Business World sufficiently notified the affected data subjects and implemented measures to prevent the recurrence of the breach.

The notification letter dated 17 January 2018 that Business World sent to its affected individuals included the information required under NPC Circular 16-03 (Personal Data Breach Management). Section 18 (C) of NPC Circular 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:

. . .

C. Content of Notification. The notification shall include, but not be limited to:

1. nature of the breach;
2. personal data possibly involved;

---

20 *Id.* at 2-3.  
 21 *Id.* at 3.  
 22 *Id.* Annex.

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.<sup>23</sup>

In the letter-notification dated 17 January 2018, Business World informed the affected data subjects of the nature of the breach by reporting that the hacker group Cyber-Chaos team claimed that it gained access to Business World’s data and posted the data online.<sup>24</sup> It further identified that the incident involved the email addresses of Business World’s subscribers.<sup>25</sup>

Business World assured the affected data subjects that the website, where the email addresses were posted, has been immediately taken down.<sup>26</sup> It also informed the affected data subjects that it has taken action “to further strengthen the security of [its] system” and advised them to regularly change their passwords.<sup>27</sup>

The letter dated 17 January 2018 also specified Business World’s email address, where affected data subjects can ask for further information regarding the breach.<sup>28</sup>

Given the foregoing, the Commission finds that Business World has sufficiently notified the affected data subjects of the breach.

In addition, the Commission notes the remedial measures taken by Business World. Business World built its own WordPress site that enables automatic updates and it implemented additional layers of security on its website for protection against vulnerabilities it has identified.<sup>29</sup> It also took down the old database that was compromised immediately after the discovery of the incident.<sup>30</sup>

Business World’s random generation of usernames and passwords and the monthly resetting of the passwords provide more security and protection to the personal data of the data subjects.<sup>31</sup> These measures are sufficient to address the breach and prevent the recurrence of the incident.

**WHEREFORE**, premises considered, Commission resolves that NPC BN 18-006 – In Re: Business World, Inc. is hereby **CLOSED**.

**SO ORDERED.**

---

23 National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §18 (C) (15 December 2016).

24 Full Breach Report, 15 August 2022, Annex, in In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).

25 *Id.*

26 *Id.*

27 *Id.*

28 *Id.*

29 *Id.* at 2.

30 Full Breach Report, 15 August 2022, at 3, in In Re: Business World, Inc., NPC BN 18-006 (NPC 2022).

31 *Id.* at 2.

City of Pasay, Philippines.  
10 November 2022.

**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

I CONCUR:

**JOHN HENRY D. NAGA**  
Privacy Commissioner

Copy furnished:

**ASD**  
*Data Protection Officer*  
**Business World, Inc.**

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

X-----X

RESOLUTION

AGUIRRE, D.P.C.:

Before the Commission is a request for postponement from the requirement of notification of affected data subjects dated 01 July 2022 filed by Equicom Savings Bank (Equicom) in relation to an unauthorized transfer of funds from the bank accounts of Equicom’s depositors.

Facts

On 01 July 2022, Equicom submitted to the Commission an initial report of a data breach through the Data Breach Notification Management System (DBNMS).<sup>1</sup>

On 29 June 2022 at around 10:58 A.M., a complaint for an unauthorized debit on the account of Delictable, Inc. (Delictable) was received by the Sales Officer of Equicom-Dilliman Branch.<sup>2</sup> Upon inquiry of Delictable’s bank account, it was revealed that fund transfers were made via Instapay.<sup>3</sup>

Equicom noted that a total amount of one hundred fifty thousand pesos (Php 150,000.00) was transferred to three (3) GCash recipients crediting fifty thousand pesos (Php50,000.00) to each.<sup>4</sup>

At 11:00 AM, an internet banking transaction report was generated to verify the transactions allegedly made by Delictable.<sup>5</sup> It was noted that the account name AJM bore Delictable’s account number “instead of the legitimate account name of Delictable.”<sup>6</sup>

Further, it was also reported that several Equicom branches “were also appearing to be used by AJM.”<sup>7</sup> Equicom stated that it deactivated AJM’s account at the branch level.<sup>8</sup>In the report, it was stated that Branch Head JL and Service Officer RDL called the other branches to inform them of the possible unauthorized debits of their depositors.<sup>9</sup>

Equicom claimed that the perpetrator managed to use the “Inspect Elements” feature of the Chrome web browser, and that “the account number of the Source Account was eventually changed to other account number[s] of existing [Equicom] depositors.”<sup>10</sup>Consequently, a simulation test was made by the IT Department of Equicom to mimic

1 In re: Equicom Savings Bank, NPC BN 22-094, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Date of Notification of Equicom Savings Bank (01 July 2022).

2 Id., 1.b Chronology of Equicom Savings Bank.

3 Id.

4 Id.

5 In re: Equicom Savings Bank, NPC BN 22-094, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.b Chronology of Equicom Savings Bank (01 July 2022).

6 Id.

7 Id.

8 Id.

9 In re: Equicom Savings Bank, NPC BN 22-094, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.b Chronology of Equicom Savings Bank (01 July 2022).

10 Id., 1.a How breach occurred + DPS vulnerability.

the process.<sup>11</sup>

As for personal data involved, Equicom mentioned in its Initial Report that the depositors' account numbers may be used to identify fraud.<sup>12</sup> The possible sensitive personal information involved was reported as "to be determined" by Equicom.<sup>13</sup>

Equicom identified nineteen (19) affected data subjects from four (4) Equicom branches and noted that there are sixty-seven (67) unauthorized fund transfers through Instapay involving the total amount of Three Million Seventy-Seven Thousand Four Hundred Fifty-Six pesos (Php3,077,456.00).<sup>14</sup>

In terms of the measures to address the breach, Equicom stated that it "strengthen security measures process both in front end and API".<sup>15</sup> Further, to secure/recover the personal data and to mitigate harm, it stated that the "internet banking facility [was] immediately shut down",<sup>16</sup> and that the "internet banking facility will be down for 10 days due to deployment of other authentication procedures in the front end and API".<sup>17</sup> In order to prevent the reoccurrence of the incident, Equicom indicated in its Initial Report "tighter security measures in the internet banking facility."<sup>18</sup>

Equicom also declared in its Initial Report that it will only conduct actions to inform the affected data subjects once a complaint is received, and that there is an "[o]ngoing thorough investigation."<sup>19</sup>

Equicom is then requesting the postponement of notification of the affected data subjects. It stated that the reason for the request is "currently undergoing evaluation".<sup>20</sup>

## **Discussion**

The Commission resolves to close the case upon finding that Business World sufficiently complied with the Order dated 30 June 2022. Business World sufficiently notified the affected data subjects and implemented measures to prevent the recurrence of the breach.

The Commission resolves to deny the request for postponement of notification of data subjects.

### *1. The incident falls within the scope of the mandatory breach notification requirements.*

The Commission finds that the case falls under the mandatory breach notification requirement and notification of the affected data subjects is necessary in order to protect them from the risk of serious harm. As provided in Rule V, Section 11 of NPC Circular No.

---

11 *In re: Equicom Savings Bank*, NPC BN 22-094, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Brief Summary of Equicom Savings Bank (01 July 2022).

12 *Id.*, 2.b Other info that may enable identity fraud.

13 *Id.*, 2.a SPI.

14 *Id.*, 1.c Number of DS / Records.

15 *In re: Equicom Savings Bank*, NPC BN 22-094, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.a Measures to address the breach of Equicom Savings Bank (01 July 2022).

16 *Id.*, 3.b. Measures to secure/recover personal data

17 *Id.*, 3.c. Actions to mitigate harm

18 *Id.*, 3.e Measures to prevent recurrence of incidence

19 *In re: Equicom Savings Bank*, NPC BN 22-094, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.d Actions to inform data subjects of Equicom Savings Bank (01 July 2022).

20 *Id.* Type of Request.

## 16-03 (Personal Data Breach Management):

**SECTION 11.** *When notification is required.* Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

A. The personal data involves sensitive personal information or **any other information that may be used to enable identity fraud. x x x**

B. There is **reason to believe that the information may have been acquired by an unauthorized person; and,**

C. The personal information controller or the Commission believes that the **unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.**<sup>21</sup> (Emphasis Supplied)

Based on the records, all the conditions for mandatory breach notification are present. The account numbers involved are considered as information that may be used to enable identity fraud since it relates to financial information of the data subjects.<sup>22</sup> Further, Equicom itself admitted in its Initial Report that the use of depositors' account number may enable identity fraud.<sup>23</sup>

Additionally, Equicom stated that there was indeed unauthorized debit on Delictable Inc.'s account including fund transfers via Instapay and three (3) transactions amounting to one hundred fifty thousand pesos (Php 150,000) was transferred via GCash.<sup>24</sup> In this case, it is thus evident that the account numbers of the depositors have been acquired by an unauthorized person.

Consequently, the unauthorized acquisition will give rise to a real risk of serious harm to the nineteen (19) clients of Equicom whose bank accounts are compromised. Moreover, based on the DBNMS Report submitted, the total amount subject of the unauthorized transfer of funds is Php3,077,456.00.<sup>25</sup>

Equicom stated that it will only conduct actions to inform the affected data subjects once a complaint is received.<sup>26</sup>

This Commission reiterates Equicom's obligations as the Personal Information Controller (PIC) to notify the affected data subjects in cases of breach that fall under the mandatory notification rule. Also, Equicom should have taken into account the likelihood of harm or negative consequences of the incident given the fact that the account numbers were already acquired by an unauthorized person.

This Commission stresses that Equicom need not wait for a complaint before notifying the affected data subjects, especially in this case, where harm had already materialized through the unauthorized acquisition of account numbers. Further, there's still a con-

<sup>21</sup> NPC Circular No. 16-03, Rule V, § 11.

<sup>22</sup> *Id.*

<sup>23</sup> *In re: Equicom Savings Bank*, NPC BN 22-094, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 2.b Other info that may enable identity fraud (01 July 2022).

<sup>24</sup> *Id.* 1.b. Chronology

<sup>25</sup> *In re: Equicom Savings Bank*, NPC BN 22-094, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.c Number of DS / Records of Equicom Savings Bank (01 July 2022).

<sup>26</sup> *Id.* 3.d Actions to inform data subjects

tinuing risk of serious harm posed to other data subjects given that Equicom has yet to notify its data subjects.

This Commission finds that the notification to the affected data subjects is necessary in order to allow them to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.<sup>27</sup> Equicom must notify the data subjects affected by the hacking incident of their bank accounts to reduce the risks arising from the breach and to prevent further unauthorized fund transfers from their bank accounts.<sup>28</sup>

*II. The postponement of notification  
is not warranted by mere “investigation.”*

Equicom’s justification for postponement is anchored on its claim that the breach is “currently undergoing investigation.”<sup>29</sup> However, the Commission is not persuaded by the justification.

Rule V, Section 18(B) of NPC Circular No. 16-03 provides that the Commission “may authorize the postponement of notification if such notification **may hinder the progress of a criminal investigation related to a serious breach**, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.”<sup>30</sup> (Emphasis supplied)

Here, Equicom has not provided enough proof to show that there is an ongoing criminal investigation. The mere mention that it is “currently undergoing investigation”<sup>31</sup> does not suffice. Thus, the Commission cannot grant its request to postpone the notification to the nineteen (19) clients whose bank accounts are subject to unauthorized fund transfers.

*III. Equicom as a PIC must submit its Full Breach Report*

In its initial report, Equicom stated that it undertook measures to address the breach including correctional actions, remediation, and preventive steps that would mitigate and remediate the incident.<sup>32</sup>

However, Equicom has yet to submit its Full Breach Report which includes the description of the personal data breach, actions and decisions of the incident response team, outcome of the breach management, and difficulties encountered and compliance with notification requirements.<sup>33</sup> Moreover, in this case, the Commission finds it necessary for Equicom to submit the proof of security measures it undertook to address the breach as stated in its initial report.

**WHEREFORE**, premises considered, the Commission resolves that the request to

27 NPC Circular No. 16-03, Rule V, § 18(A).

28 NPC Circular No. 16-03, Rule V, § 18(B).

29 In re: Equicom Savings Bank, NPC BN 22-094, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Justification for postponement of Equicom Savings Bank (01 July 2022).

30 NPC Circular No. 16-03, Rule V, § 18(B).

31 In re: Equicom Savings Bank, NPC BN 22-094, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Justification for postponement of Equicom Savings Bank (01 July 2022).

32 In re: Equicom Savings Bank, NPC BN 22-094, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), ¶¶ of Equicom Savings Bank (01 July 2022).

33 NPC Circular 16-03, Rule IV, § 9.

postpone the notification of the affected data subjects filed by Equicom Savings Bank (Equicom) is hereby **DENIED**.

Equicom is hereby **ORDERED**, within fifteen (15) days from receipt of this Resolution, to comply with the following:

1. **NOTIFY** the affected data subjects, pursuant to Section 18 of the NPC Circular No. 16-03, and submit proof of compliance thereof, including the proof of receipt of the data subjects of such notification;
2. **SUBMIT** a Full Breach Report pursuant to Sections 17(D) in relation to Section 9 of NPC Circular No. 16-03; and
3. **SUBMIT** proof of security measures.

**SO ORDERED.**

City of Pasay, Philippines.  
14 July 2022.

**SGD.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

WE CONCUR:

**SGD.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

**SGD.**  
**DUG CHRISTOPHER B. MAH**  
Deputy Privacy Commissioner

Copy furnished:

**JTF**  
*Data Protection Officer*  
Equicom Savings Bank

**COMPLIANCE AND MONITORING DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission



X-----X

**RESOLUTION**

**NAGA, P.C.;**

Before the Commission is the compliance of La Salle Green Hills School (LSGH) dated 29 July 2022 (Compliance) in relation to the 21 May 2020 Resolution of the Commission (Resolution).

**Facts**

On 01 June 2018, LSGH sent a data breach report to notify the Commission about a data breach caused by one of its employees.<sup>1</sup> LSGH stated that an employee brought home some work documents that were left in a tricycle.<sup>2</sup> LSGH alleged that the lost documents include forms of seven (7) school employees which contained the Social Security System (SSS) Salary Loan Application Form, SSS Sickness Benefit, and Pag-IBIG Multi-Purpose Loan Form.<sup>3</sup> The forms contained the following personal and sensitive personal information of the employees:

- a) Name;
- b) Date of Birth;
- c) Tax Identification Number (TIN);
- d) SSS Number;
- e) Pag-IBIG Number;
- f) Contact Number (mobile or landline); and
- g) Electronic mail address.<sup>4</sup>

In line with the incident, LSGH stated that it immediately notified the affected employees through its Human Resource Department (HRD).<sup>5</sup> LSGH also released a memorandum which prohibits the school personnel to bring home documents containing personal data.<sup>6</sup> The school administration likewise scheduled a re-orientation of all personnel regarding the matter.<sup>7</sup>

Moreover, LSGH stated that the concerned employee exerted possible efforts to locate the documents but failed to do so.<sup>8</sup>

On 21 May 2020, the Commission issued a Resolution with a dispositive portion stating:

**WHEREFORE,** premises considered, this Commission orders La Salle Green Hills School to submit the result of its PIA, together with the revised Privacy Policy and Security Incident Management Policy one (1) week from the receipt of this Resolu-

---

1 Electronic Mail dated 01 June 2018 from La Salle Green Hills School.  
2 *Id.*  
3 *Id.*  
4 *Id.*  
5 Electronic Mail dated 01 June 2018 from La Salle Green Hills School.  
6 *Id.*  
7 *Id.*  
8 Supplemental Breach Report received 03 August 2018 of La Salle Green Hills School.

tion.

**SO ORDERED.**<sup>9</sup>

Records show that LSGH only received a copy of the Resolution on 06 January 2021.<sup>10</sup> Consequently, the Enforcement Division (EnD) of the National Privacy Commission sent a compliance letter requiring LSGH to submit the required documents within ten (10) days from receipt of the letter.<sup>11</sup>

On 27 April 2021, LSGH requested for an extension of thirty (30) days to submit the required documents due to the appointment of its new Data Protection Officer (DPO) who was not given the pertinent documents for the proceedings by its previous DPO.<sup>12</sup> LSGH also stated that due to the implementation of a skeletal workforce caused by the pandemic, all other employees were in a work from home setup.<sup>13</sup>

Pending the resolution of its Motion for Extension, LSGH submitted the following documents as part of its compliance:

1. LSGH Revised Data Privacy Policy
2. LSGH Revised Privacy Security Incident Policy
3. LSGH Offices Personal Data Inventory and Privacy Impact Assessment
4. LSGH Data Privacy Security Incident Reporting Form
5. LSGH Privacy Management Plan
6. LSGH Social Media Policy for Students
7. LSGH Social Media Policy for Personnel and Partners<sup>14</sup>

Subsequently, the Commission issued a Resolution dated 06 May 2021:

**WHEREFORE**, premises considered, this Commission hereby **GRANTS** La Salle Green Hills School an extension of ten (10) days to comply with the 21 May 2020 Resolution of the Commission reckoned from the date of the Motion for Extension. The Commission also **NOTES** the submission of compliance dated 05 May 2021 pending the Final Enforcement Assessment Report from the Enforcement Division.

The La Salle Green Hills School is **STERNLY WARNED** that their similar conduct shall be dealt with accordingly.

**SO ORDERED.**<sup>15</sup>

Subsequently, the EnD sent a letter dated 28 July 2021 ordering LSGH to submit the following:

- A. Excel files stating the PIA results for:
1. Associate Principal for Academic Affairs
  2. Associate Principal for Student Affairs

---

9 *In Re: La Salle Greenhills School*, CID BN 18-085, Resolution dated 21 May 2020, at p. 3.  
10 Electronic Mail dated 19 April 2021 from Mega Manila Customer Service.  
11 Compliance Letter dated 20 April 2021 from Enforcement Division, at pp. 1-2.  
12 Motion for Extension dated 27 April 2021 from La Salle Green Hills School, at ¶¶ 2-4.  
13 *Id.*, at ¶ 6.  
14 Compliance dated 05 May 2021 from La Salle Green Hills School.  
15 *In Re: La Salle Greenhills School*, CID BN 18-085, Resolution dated 06 May 2021, at p. 3.

B. Files with complete entries in the PIA results of:

1. Finance Resource Department
2. Guidance Education and Intervention Services
3. Health and Services Unit
4. Lasallian Mission Office
5. Learning Resource Center
6. Sports Program and Development Office
7. Quality Assurance and Research Office
8. Human Resource and Development Office
9. Safety and Security Office.
10. Admissions Office
11. Registrar's Office.<sup>16</sup>

On 06 August 2021, LSGH submitted its Compliance by attaching the documents required by the EnD in its 28 July 2021 Letter.<sup>17</sup>

On 05 April 2022, the EnD sent a letter to LSGH in relation to its submissions. The EnD stated:

While the PIA was found compliant with the requirements in identifying attendant risks in the processing of personal data, it was also found that its implementation is yet to be fully made in other offices such as the Finance Resource Department, Office of the Associate Principal for Academic Affairs, Office of the Associate Principal for Student Affairs, Quality Assurance and Research Office and Sports Program Development Office.<sup>18</sup>

The EnD also made the following evaluation:

As to the other documents submitted by LSGH, the Commission observed that the: 1) Revised Data Policy; 2) Revised Privacy Security Incident Policy; 3) Offices Personal Data Inventory and Privacy Impact Assessment; 4) Data Privacy Security Incident Reporting Form; 5) Privacy Management Plan; 6) Social Media Policy for Students; and 7) Social Media Policy for Personnel and Partners, are too general and do not contain the necessary specificity to be considered compliant with the requirements of the Data Privacy Act of 2012 (DPA).<sup>19</sup>

Thus, the EnD ordered LSGH to submit “(1) Report on the full implementation of the PIA, specifically on the aforementioned offices, and (2) Revised policies in compliance with the requirements of DPA.”<sup>20</sup>

On 19 April 2022, LSGH submitted the required documents in compliance with the EnD's 05 April 2022 letter.<sup>21</sup>

In another letter dated 08 June 2022, the EnD stated that LSGH “failed to submit the requested revised policies,” thus, it ordered the school to furnish a copy of the revised policies.<sup>22</sup> LSGH thereafter submitted “[t]he digital copies of the Revised Data Privacy

---

16 Compliance Letter dated 28 July 2021 from Enforcement Division, at p. 2.

17 Compliance dated 06 August 2021 from La Salle Green Hills School.

18 Compliance Letter dated 05 April 2022 from Enforcement Division, at p. 1.

19 *Id.*, at p. 2

20 *Id.*

21 Compliance dated 19 April 2022 from La Salle Green Hills School.

22 Compliance Letter dated 08 June 2022 from Enforcement Division, at p. 1.

Policy, Revised Data Privacy Security Incident Policy and Revised Security Incident Report Form.”<sup>23</sup>

On 19 July 2022, EnD sent a compliance letter to LSGH which serves as a “final demand to comply with NPC’s Order dated 21 May 2020.”<sup>24</sup> EnD stated that:

Upon assessment, LSGH still failed to submit the following revised policies: (1) Office Personal Data Inventory and Privacy Impact Assessment; (2) Data Privacy Security Incident Reporting Form; (3) Privacy Management Plan; (4) Social Media Policy for Students; and (5) Social Media Policy for Personnel and Partners.<sup>25</sup>

In compliance thereto, LSGH provided the documents that the EnD ordered the school to submit.<sup>26</sup>

### **Issue**

Whether La Salle Green Hills School complied with the Resolution dated 21 May 2020.

### **Discussion**

LSGH was ordered by this Commission to submit the result of its PIA and its Revised Privacy Policy and Security Incident Management Policy.<sup>27</sup>

Based on records and EnD’s evaluation, this Commission finds that LSGH has sufficiently complied with the Resolution dated 21 May 2020.

*LSGH sufficiently complied with the requirements under NPC Advisory No. 17-03 in the conduct of its PIA*

NPC Advisory No. 17-03 (Guidelines on Privacy Impact Assessment) defines a PIA as:

[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 [Personal Information Controller] or PIP [Personal Information Processor] 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.<sup>28</sup>

Moreover, NPC Advisory No. 17-03 also states that:

In general, a **PIA should be undertaken for every processing system** of a PIC or PIP that involves personal data. It may also **be carried out vis-à-vis the entire organization** of the PIC or PIP with the involvement or participation of the different process owners and stakeholders.<sup>29</sup> (Emphasis supplied)

<sup>23</sup> Compliance dated 18 June 2022 from La Salle Green Hills School.

<sup>24</sup> Compliance Letter dated 19 July 2022 from Enforcement Division, at p. 2.

<sup>25</sup> Id., at p. 1.

<sup>26</sup> Compliance dated 29 July 2022 from La Salle Green Hills School.

<sup>27</sup> In Re: La Salle Greenhills School, CID BN 180-085, Resolution dated 21 May 2020

<sup>28</sup> National Privacy Commission, Guidelines on Privacy Impact Assessment, NPC Advisory 201703, Definition of Terms, at item K (31 July 2017) (NPC Advisory 17-03).

<sup>29</sup> NPC Advisory 17-03, Key Considerations.

Based on the review and evaluation of the EnD, LSGH has submitted the PIA results of the school's various offices and departments.<sup>30</sup> In its Compliance dated 06 August 2021 and 19 April 2022, LSGH sufficiently submitted the reports on the full implementation of the PIA results derived from the school's offices and departments.<sup>31</sup>

In its PIA, LSGH identified the following common privacy risks: the occurrence of unauthorized disclosure, unavailability of data (loss of data), unauthorized alteration of data, and unauthorized access of personal data in the school's programs, projects, processes, measures, systems, or technologies.<sup>32</sup>

Thus, LSGH reported in its PIA the significance of the school's Data Privacy Notice, Data Privacy Consent, Disciplinary Interventions for Data Privacy Breaches, Policy on Confidentiality, and the "No Taking Home of Work Documents" policy.<sup>33</sup>

According to EnD's Report, the PIA of LSGH includes a data inventory tracker for each processing system including the determination of purpose of each and every processing of personal data, its legal basis, type of personal data collected and other systematic description of the personal data flow and processing activities of LSGH.<sup>34</sup>

Moreover, the PIA reports have identified the risks for each processing activity and the likelihood of impact on the rights of data subjects, the existing controls, the risk rating, the remedial measures, risk owner and review date.<sup>35</sup>

In mitigating the further occurrence of risks, LSGH reported that the following actions have been or are being implemented:

- (1) Reinforcement of duties and responsibilities of personnel through regular alignment meetings;
- (2) Strict implementation of the Institutional Office Manual provision on privacy matters and the Code of Ethics and Data Privacy Policy;
- (3) Retention of efficient storage and monitoring of documentation.<sup>36</sup>

For other offices and departments of LSGH, the following mitigation actions are being implemented:

- (1) Regular change of password, control in the access of data, secure disposal of data of unsuccessful applications;<sup>37</sup>
- (2) Two-way authentication;<sup>38</sup>
- (3) Verification and proper information dissemination;<sup>39</sup> and,
- (4) Incident Report with investigation along with CCTV Report.<sup>40</sup>

---

30 Compliance dated 06 August 2021 from La Salle Green Hills School; See Compliance dated 19 April 2022 from La Salle Green Hills School.

31 *Id.*

32 See Compliance dated 06 August 2021 from La Salle Green Hills School.

33 Compliance dated 06 August 2021 from La Salle Green Hills School.

34 Compliance dated 19 April 2022 from La Salle Green Hills School.

35 *Id.*

36 Compliance dated 06 August 2021 from La Salle Green Hills School.

37 *Id.*, in Admissions Office-Privacy Impact Assessment.

38 *Id.*, in Finance Resource Department Privacy Impact Assessment.

39 *Id.*, in Guidance and Education Intervention Services Privacy Impact Assessment.

40 Compliance dated 06 August 2021 from La Salle Green Hills School in Security and Safety Office- Privacy Impact Assessment.

After LSGH evaluated the processing activities conducted by its offices and departments, security and privacy measures were implemented in order to mitigate the occurrence of the identified risks and to better protect the personal data of data subjects. After scrutinizing the various PIA Reports submitted, the Commission finds that LSGH has sufficiently demonstrated its compliance with NPC Advisory No. 17-03.

LSGH's Revised Privacy Policy and Security Incident Management Policy are compliant with the DPA.

Advisory Opinion No. 2018-013 states:

At the outset, it must be clarified that the submitted “privacy policy” should be referred to as the company’s privacy notice. A privacy notice is a statement made to a data subject that describes **how the organization collects, uses, retains and discloses personal information**. A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy.<sup>41</sup>

On 05 May 2021, LSGH submitted its Revised Privacy Policy in compliance with the Resolution dated 21 May 2020.<sup>42</sup> On 05 April 2022, the EnD required LSGH to submit its Revised Data Policy and Revised Privacy Security Incident Policy stating that these submissions were “too general and do not contain the necessary specificity to be considered compliant with the requirements of the [DPA].”<sup>43</sup>

Upon review of the Revised Privacy Policy submitted on 18 June 2022, the Commission notes that it already includes the purpose of the implementation of the Privacy Policy of LSGH, which was not indicated in the previous submission.<sup>44</sup> The revised Privacy Policy also applies to all departments and units, its employees, personnel, students, and personal information processors.<sup>45</sup> Moreover, the scope and coverage of the Revised Privacy Policy specifically provides for the categories of personal and sensitive personal information of data subjects (the students or applicants for admission, parents, guardians and/or alumni/alumnae, employees/personnel and applicants for employment) which are needed to be processed.<sup>46</sup>

Further, the Revised Privacy Policy includes the Guidelines for Students, Parents, Guardians, Alumni/Alumnae, Employees and Personnel on how their personal and sensitive personal information are being processed.<sup>47</sup> Particularly for the employees and personnel, LSGH’s processing of their personal data shall be for purposes of employment application, maintaining personnel records, payroll, benefits, grants, and HMO management, among others.<sup>48</sup> Meanwhile, for students, LSGH’s processing of their personal data is for purposes of application and enrollment, maintaining student records, marketing and publicity of the school, among others.<sup>49</sup>

---

41 National Privacy Commission, Privacy Policy and Consent of Data Subjects, NPC Advisory Opinion 2018-013, (18 April 2018) (NPC Advisory Opinion 2018-013).

42 Compliance dated 05 May 2021 from La Salle Green Hills School

43 Compliance Letter dated 05 April 2022 from Enforcement Division, at p. 2.

44 Compliance dated 18 June 2022 from La Salle Green Hills in Data Privacy Policy, at p. 2.

45 Compliance dated 18 June 2022 from La Salle Green Hills in Data Privacy Policy.

46 Id., at pp. 4-7.

47 Id., at pp. 7-9.

48 Id., at p. 6.

49 Compliance dated 18 June 2022 from La Salle Green Hills in Data Privacy Policy, at p. 5.

Moreover, the Privacy Policy of LSGH contains the following fields:

- (1) Security Measures for Protection of Personal Information;<sup>50</sup>
- (2) Data Subject Rights;<sup>51</sup>
- (3) Record Keeping;<sup>52</sup>
- (4) Data Sharing;<sup>53</sup>
- (5) Disclosure and Direct Marketing;<sup>54</sup>
- (6) Responsibilities of DPO, LSGH, Students and Employees;<sup>55</sup>
- (7) Creation of Data Breach Response Team and Notification Protocol;<sup>56</sup>and,
- (8) Procedure for Recovery and Restoration of Personal Data.<sup>57</sup>

LSGH likewise submitted its social media policies for students, personnel and partners which include the parents, guardians, alumni, among others.<sup>58</sup>These policies provide guidelines on the use of social media platforms, including guidance on how students, personnel, and partners should be mindful of their legal risks and acts.<sup>59</sup>The policies also better ensure that the students, personnel, and partners do not compromise their personal security or the security of the school’s information assets.<sup>60</sup>

LSGH further submitted its Privacy Management Plans for the school years (SY) 2021-2022 and 2022-2023.<sup>61</sup>For SY 2022-2023, LSGH ensures the “Review and Updating of the Implementing Guidelines” of its Data Privacy Policy for students, personnel, and partners.<sup>62</sup>LSGH stated that it shall conduct “Communication Sessions” for the implementation of its privacy policy.<sup>63</sup>

Moreover, LSGH shall draft its “data privacy consent” and shall review and update the “Risk Registry on Data Privacy” per subject area or office.<sup>64</sup>

With regard to the Security Incident Management Policy, the revised submission contains the following details:

1. [The] Purpose and Objectives of the policy;<sup>65</sup>
2. Security Incident/Personal Data Breach Reporting and Incident Reporting Procedure;<sup>66</sup>
3. Initial mitigation to contain the incident/breach to prevent further damage;<sup>67</sup>
4. Creation and composition of the Data Breach Response Team and the actions that it may take to mitigate the incident;<sup>68</sup>

---

50 Id., at p. 11.

51 Id., at p. 18.

52 Id., at p. 21.

53 Compliance dated 18 June 2022 from La Salle Green Hills in Data Privacy Policy, at p. 21.

54 Id., at p. 22

55 Id.

56 Id., at p. 24.

57 Compliance dated 18 June 2022 from La Salle Green Hills in Data Privacy Policy, at p. 25.

58 Compliance dated 19 July 2022 from La Salle Green Hills referred to as Social Media Policy for Personnel and Partners; See also Social Media Policy for Students.

59 Id., at pp. 3-4; See also Social Media Policy for Students.

60 Id., at p. 2; See also Social Media Policy for Students.

61 Compliance dated 19 July 2022 from La Salle Green Hills referred to as Privacy Policy Management Plan.

62 Compliance dated 19 July 2022 from La Salle Green Hills referred to as Privacy Policy Management Plan SY 2022-2023, at p. 1.

63 Id., at pp. 1-2.

64 Id., at p. 4.

65 Compliance dated 18 June 2022 from La Salle Green Hills referred to as Data Privacy Security Incident Management Policy, at p. 2

66 Id., at pp. 3-4.

67 Id., at p. 4.

68 Id., at pp. 4-6.

In addition to the Security Incident Management Policy, LSGH likewise submitted a “Data Privacy Security Incident Reporting Form” which can be accomplished by any individual with knowledge of data privacy security incidents.<sup>69</sup>The said form shall be used “in line with the investigation” and other legitimate purposes.<sup>70</sup>

The accomplished form shall be reviewed and assessed by the school’s DPO.<sup>71</sup>

The fields that are needed to be accomplished are:

- (1) Name and Signature of the person who reports the incident, his or her department or unit;
- (2) Summary of the incident;
- (3) Timeline for the incident;
- (4) Reporting which includes the questions “Were there any controls in place? Who detected the breach? When was the breach isolated?”
- (5) Initial assessment which categorically asks the question if the incident involves sensitive personal information, among others;
- (6) Remedial Measures taken;
- (7) Impact of the incident; and,
- (8) Management of the incident.<sup>72</sup>

Upon review of the documents submitted and based on EnD’s evaluation, LSGH sufficiently complied with the 21 May 2020 Resolution and the subsequent Orders of the Commission. The Commission notes the revisions made by LSGH when it comes to its Privacy Policy and Security Incident Management Policy. These documents are now specific and more concrete policies, guidelines, and practices that help secure the personal data of relevant data subjects and uphold their rights.

**WHEREFORE**, premises considered, this Commission resolves that the matter of NPC BN 18-085, “In re: La Salle Green Hills School” is hereby considered **CLOSED**.

**SO ORDERED.**

City of Pasay, Philippines.  
22 September 2022.

**SGD.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

I CONCUR:

**SGD.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

Copy furnished:

---

69 Compliance dated 19 July 2022 from La Salle Green Hills referred to as Data Privacy Security Incident Reporting Form, at p. 1.

70 Id.

71 Id.

72 Id., at pp. 1-4.



**MMJ**

*Data Protection Officer*

**COMPLAINTS AND INVESTIGATION DIVISION**

**ENFORCEMENT DIVISION**

**GENERAL RECORDS UNIT**

National Privacy Commission

**DVL,**

*Complainant,*

**NPC 22-180**

For: Violation of the Data  
Privacy Act of 2012

-versus-

**ALAMAT CREWSERS MOTORCYCLE  
CLUB,**

*Respondent.*

X-----X

**LAE,**

*Complainant,*

**NPC 22-181**

For: Violation of the Data  
Privacy Act of 2012

-versus-

**ALAMAT CREWSERS MOTORCYCLE  
CLUB,**

*Respondent.*

X-----X

## **RESOLUTION**

**AGUIRRE, D.P.C.;**

Before this Commission are two separate complaints filed by DVL and LAE against Alamat Crewsers Motorcycle Club (Alamat Crewsers M.C.) for an alleged violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

### **Facts**

In their Complaints-Assisted Forms (CAFs) dated 19 August 2022, DVL and LAE respectively claimed that Alamat Crewsers M.C. violated the DPA when it maliciously published, on 11 August 2022, a post on Facebook containing their names and pictures without their consent.<sup>1</sup> The Facebook post containing their pictures states:

IMPORTANT PUBLIC NOTICE:

This is to inform the public that these individuals, LAE and DVL whose pictures are shown here are no longer MEMBERS of ALAMAT CREWSERS M.C. and hereby declared as PERSONA NON GRATA by the club. Please be informed that any transaction or representation made by them using and under the name of ALAMAT CREWSERS M.C. are false pretenses and will not be recognized by the Club.

Though it's not in our nature as a Club to air our laundry out in public, it has come

<sup>1</sup> Complaints-Assisted Form, 19 August 2022, at 3, in DVL v. Alamat Crewsers Motorcycle Club, NPC Case No. 22-180 (NPC 2022); Complaints-Assisted Form, 19 August 2022, at 3, in LAE v. Alamat Crewsers Motorcycle Club, NPC Case No. 22-181 (NPC 2022).

to our attention that these individuals are misrepresenting our club by actively recruiting and using their status as former members as premise. We cannot just let this slide, leaving the Club with no other choice but be obligated to let it be known to the public. One of them was dismissed due to transgressions against the Club and the other one resigned. We have in good faith, tried to settle things under the prying eyes of the public but to no avail.

Also...

\*\*\*ALAMAT CREWSERS M.C. DOES NOT RECRUIT\*\*\*

Again, we would like to reiterate that LAE and DVL are NO LONGER MEMBERS nor are they in any way AFFILIATED with ALAMAT CREWSERS M.C.

PLEASE BE ADVISED ACCORDINGLY!

To all our friends, brothers and sisters on the road, kindly disseminate among your groups to allay any misrepresentation and ill intention in the motorcycle community.<sup>2</sup>

Both DVL and LAE opined that “private entities such as this motorcycle riding club is [sic] devoid of any legal basis to process the personal information of the complainant in any way such as publishing/posting their name and picture without consent[.]”<sup>3</sup>

Further, DVL and LAE stressed that as of the filing of their CAFs, the post is still present and has been liked by thirty (30) individuals and shared by fifty-six (56) individuals, thereby affecting their reputation.<sup>4</sup>

On 22 September 2022, the Commission through its Legal and Enforcement Office (LEO) issued two separate Decisions dismissing the complaints filed by DVL and LAE for lack of merit:

WHEREFORE, the instant complaint is hereby DISMISSED for lack merit, without prejudice to the filing of the appropriate civil, criminal, or administrative cases in the appropriate forum or tribunal, as may be necessary, and without prejudice to the refiling with the National Privacy Commission (NPC) in accordance with the Rules of Procedures of the NPC.

**SO ORDERED.**<sup>5</sup>

The LEO emphasized in its Decisions that “the complaint[s] did not pertain to a violation of the DPA” and, therefore, may be dismissed outright.<sup>6</sup> The LEO argued that Alamat Crewsers M.C.’s processing was allowed pursuant to Section 12 (f) of the DPA and drew a parallel between the circumstances of this case and that of Advisory Opinion No. 2019-024:

In Advisory Opinion No. 2019-024 dated 07 May 2019, the Commission explained that public notices for termination of employees are allowed under the DPA as an exercise of a personal information controller’s legitimate interests. In

2 Id. Annex C; Id. Annex C.

3 Id. at 4; Id. at 4.

4 Id.; Id.

5 NPC 22-180, 22 September 2022, at 4 (NPC 2022) (unreported); NPC 22-181, 22 September 2022, at 4 (NPC 2022) (unreported).

6 Id. at 1-2; Id. at 1-2.

the same Opinion, the Commission explained the criteria to be used to determine the existence of legitimate interest, thus:

‘It has been the common practice for companies to publish notices in newspapers and other media that a certain person appearing in the photograph used to be their employee, but is now no longer connected with the company, and a warning that transactions with the said person on behalf of the company will no longer be honored.[]’

‘The above is still allowed under the DPA. The basis for processing may be Section 12(f) which provides for the processing that 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.[]’

‘Legitimate interest refers to matters that are desired by or important to a PIC, which must not be contrary to law, morals or public policy. This includes business, financial or other reasonable purpose.[]’

...

Applying the foregoing to the instant case, respondent’s act of posting a notice informing the public that complainant was no longer affiliated with respondent may be considered as processing of personal information in furtherance of respondent’s legitimate interests.<sup>7</sup>

DVL and LAE, through their counsel, filed a joint Motion for Reconsideration dated 07 October 2022.<sup>8</sup> They argued that Section 12 (f) of the DPA does not apply in this case:

As stated in the decision under Section 12 (f) of the DPA, the processing of personal information is allowed when pursued by a personal information controller for purposes of legitimate interests, thus: XXX ‘(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.’(emphasis supplied)

In our law, the concept of privacy is enshrined in the Constitution and is regarded as the right to be free from unwarranted exploitation of one’s person or from intrusion into one’s private activities in such a way as to cause humiliation to a person’s ordinary sensibilities.(emphasis supplied) Here we argue that the posting of names and pictures with unsubstantiated claims and tag as ‘persona non grata’ are an unwarranted exploitation of the complainant’s [sic] person and an intrusion to their private life which should not be allowed specially in the guise of a legitimate interest since their posting of the pictures and names are OVERRIDEN by the rights of the complainants as to their privacy.<sup>9</sup>

7 *Id.* at 3-4; *Id.* at 3-4.

8 Motion for Reconsideration, 07 October 2022, in DVL v. Alamat Crewsers Motorcycle Club, NPC Case No. 22-180 (NPC 2022) and LAE v. Alamat Crewsers Motorcycle Club, NPC Case No. 22-181 (NPC 2022).

9 *Id.* at 8-9.

Further, DVL and LAE argued that Alamat Crewsers M.C.'s post which claimed to apprise the public regarding the status of their membership cannot fall within the scope of legitimate interest under Section 12 (f) of the DPA since "aside from providing information to the status of the complainants['] membership the post alluded to an existence of a tag of 'persona non grata' clearly beyond the scope of providing the status of membership of the complainants[.]"<sup>10</sup> In relation to this, it stressed that:

Since the Club does not have any legal personality being a nonregistered entity it does not have any other legal purpose other than being a riders club it cannot legally transact any 'business' aside from motorcycle riding. So, posting the status of membership, alluding malicious tag such as persona non grata serves no purpose at all.<sup>11</sup>

DVL and LAE alleged that Advisory Opinion No. 2019-024, which discusses Section 12 (f) of the DPA, does not apply because Alamat Crewsers M.C. is without juridical personality:

[T]he use of Legitimate Interest Test presupposes that the respondents [sic] on [sic] this case has a lawful purpose and lawful personality to be able to exercise a legitimate interest but since the case has been dismissed *moto proprio* by the Commission it has failed to note that the respondent is a nonentity without any juridical personality for it is not registered in the Securities and Exchange Commission (SEC) and is a mere 'association' of Motorcycle Riders as gentleman's club to say the least without a personality or valid name to protect.

Therefore the application of the Advisory Opinion No. 2019024 [...] should not have any application in this case.

For in the Advisory Opinion the Company who posted a public notice the termination of its employees is validly exercising its rights to protect the business of the Company who has a valid Legal and Juridical Personality granted to it by law through its registration with either the Department of Trade and Industry (DTI) and or the [SEC]. When the Company posted the names and pictures of its former employee it is an extension of the contractual bonds between them covered by an employeeemployer contract and is secured and protected since the Company is mandated to process the information in compliance with the privacy principle of transparency (a privacy policy consented by the former employee), legitimate purpose (for the public not to transact with the separated employee), and proportionality (the information shared ends with the details that the employee is not anymore affiliated with the company and that the post will be available only within a period of retention as identified by the company).

Here since the riders' club [sic] main purpose in existing is to bond as riders, travel the road together, socialize as motorcycle rider, and does not have any other rights and personality other than riding motorcycle as a group therefore there is no valid and legitimate interest to begin with.<sup>12</sup>

Similarly, DVL and LAE averred that the processing was excessive since the public announcement contained malicious imputation and disclosure of unsubstantiated allegations.<sup>13</sup>

---

10 *Id.* at 10.

11 *Id.*

12 *Id.* at 11-13. Emphasis supplied.

13 *Id.* at 13-14.

## **Issue**

Whether Alamat Crewsers M.C. violated the DPA.

## **Discussion**

Alamat Crewsers M.C. did not violate the DPA since its processing of DVL and LAE's personal information falls within the lawful criteria under Section 12 (f) of the DPA. Thus, the Commission denies the Motion for Reconsideration dated 07 October 2022.

Personal information may be processed when it is for a legitimate interest. Section 12 (f) of the DPA provides:

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

...

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.<sup>14</sup>

The Commission has previously enumerated the conditions necessary for the application of legitimate interest under Section 12 (f) of the DPA:

Processing based on legitimate interest requires the fulfillment of the following conditions: (1) the legitimate interest is established; (2) the processing is necessary to fulfill the legitimate interest that is established; and (3) the interest is legitimate or lawful and it does not override fundamental rights and freedoms of data subjects.<sup>15</sup>

As to the first element, Alamat Crewsers M.C. clearly established its legitimate interest. What is deemed "legitimate" in relation to Section 12 (f) is viewed from the perspective of the Personal Information Controller (PIC). The Alamat Crewsers M.C., as an exclusive association, has its own criteria for membership. Thus, it has the legitimate interest of preserving the integrity of its membership to ensure that only official members of its association can claim actual affiliation.

As to the second element, its processing of DVL and LAE's names and pictures by publishing a Facebook post is necessary to fulfill this legitimate interest because Alamat Crewsers M.C. merely used this medium to disseminate the information to the public. As a PIC, it is in Alamat Crewsers M.C.'s legitimate interest to ensure that the public is not misled to believe that certain individuals are still members of its association. To recall, the public notice posted on Facebook specifically stated that it endeavored to inform the public that "any transaction or representation made by [DVL and LAE] using and

<sup>14</sup> 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 (f) (2012).

<sup>15</sup> NPC 20-317 and NPC 20-318, 13 October 2022, at 7 (NPC 2022) (unreported).

under the name of ALAMAT CREWSERS M.C. are false pretenses and will not be recognized by the Club.”<sup>16</sup>

To fall under legitimate interest, it is not necessary that DVL and LAE made actual transactions or misrepresentations in the name of Alamat Crewsers M.C.. It is sufficient that there is a possibility or risk that DVL and LAE, as non-members, may misrepresent and enter into transactions affecting Alamat Crewsers M.C.. Thus, Alamat Crewsers M.C. may, in its legitimate interest, protect itself by ensuring that the public is aware of the status of the membership of DVL and LAE so that they will not be misled should DVL and LAE transact or make representations under the name of Alamat Crewsers M.C. without authority.

Moreover, in considering what it is necessary to achieve the legitimate interests of the PIC, the Commission stresses the importance of the principles of proportionality and fairness. In this case, the Facebook post only disclosed information necessary to achieve Alamat Crewsers M.C.’s purpose of notifying the public that DVL and LAE are no longer affiliated with it and that any false pretenses or transactions made by them would not be recognized.<sup>17</sup> The Facebook post was factual.<sup>18</sup> It neither disclosed any information other than their names and pictures nor did it disclose their supposed transgressions to the club. Although the Facebook post stated that “[o]ne of them was dismissed due to transgressions against the Club and the other one resigned,”<sup>19</sup> this statement is not violative of any privacy violation per se because it did not provide any details regarding the matter.

As to the third element, not only was Alamat Crewsers M.C.’s interest legitimate but the manner in which it was sought to be achieved did not override the fundamental rights and freedoms of DVL and LAE. Alamat Crewsers M.C. has the right to protect its interests by informing the public of DVL and LAE’s membership status. This legitimate interest did not in any way disregard the fundamental rights and freedoms of DVL and LAE. Taking into account the principles of proportionality and fairness, the published factual Facebook post did not go beyond what was necessary to adequately notify the public of DVL and LAE’s current standing with the exclusive association.

Lastly, the Commission emphasizes that contrary to the assertions of DVL and LAE, legitimate interest does not require that the PIC be a juridical entity registered with SEC or DTI. Section 3 of the DPA defines a PIC:

Section 3. *Definition of Terms.* Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

...

(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:

<sup>16</sup> Complaints-Assisted Form, 19 August 2022, Annex C, in DVL v. Alamat Crewsers Motorcycle Club, NPC Case No. 22-180 (NPC 2022); Complaints-Assisted Form, 19 August 2022, Annex C, in LAE v. Alamat Crewsers Motorcycle Club, NPC Case No. 22-181 (NPC 2022).

<sup>17</sup> See Id; Id.

<sup>18</sup> See Id; Id.

<sup>19</sup> Complaints-Assisted Form, 19 August 2022, Annex C, in DVL v. Alamat Crewsers Motorcycle Club, NPC Case No. 22-180 (NPC 2022); Complaints-Assisted Form, 19 August 2022, Annex C, in LAE v. Alamat Crewsers Motorcycle Club, NPC Case No. 22-181 (NPC 2022).

(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.<sup>20</sup>

A PIC, as defined in the DPA, may be an individual or organization so long as it controls the processing of personal information. It does not matter whether the entity is registered with the SEC or DTI because it need not be a juridical entity. An 'association' of gentlemen riders can be considered a PIC for purposes of the DPA.

In determining the applicability of the lawful criteria in Section 12 (f) of the DPA, the Commission examines how the PIC processed personal information and does not look at its juridical personality or registration.

With regard to the procedural aspect of the case, DVL and LAE are barred from submitting a second motion for reconsideration. The Commission, through the LEO, already issued two separate Decisions dated 22 September 2022.<sup>21</sup> DVL and LAE had the opportunity to appeal the Decisions by way of filing one motion for reconsideration following Rule VIII, Section 4 of NPC Circular 2021-01 (2021 NPC Rules of Procedure):

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.<sup>22</sup>

Given that DVL and LAE filed their joint Motion for Reconsideration dated 07 October 2022 in response to the separate Decisions dated 22 September 2022,<sup>23</sup> no further motions for reconsideration or appeals will be entertained.

**WHEREFORE**, premises considered, this Commission hereby **DENIES** the Motion for Reconsideration dated 07 October 2022 filed by DVL and LAE for lack of merit and **AFFIRMS** the Decision dated 22 September 2022.

This is without prejudice to the filing of appropriate civil, criminal, or administrative cases before any other forum or tribunal, if any.

**SO ORDERED.**

City of Pasay, Philippines.  
10 November 2022.

<sup>20</sup> Data Privacy Act of 2012, § 3 (h). Emphasis supplied.

<sup>21</sup> NPC 22-180, 22 September 2022 (NPC 2022) (unreported); NPC 22-181, 22 September 2022 (NPC 2022) (unreported).

<sup>22</sup> National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC 2021 Rules of Procedure], Rule VIII, Section 4 (28 January 2021). Emphasis supplied.

<sup>23</sup> Motion for Reconsideration, 07 October 2022 in DVL v. Alamat Crewsers Motorcycle Club, NPC Case No. 22-180 (NPC 2022) and LAE v. Alamat Crewsers Motorcycle Club, NPC Case No. 22-181 (NPC 2022).



**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

I CONCUR:

**JOHN HENRY D. NAGA**  
Privacy Commissioner

Copy furnished:

**DVL**  
*Complainant*

**LAE**  
*Complainant*

**ALAMAT CREWSERS MOTORCYCLE CLUB**  
*Respondent*  
thelawfirmofisraelcalderon@gmail.com

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

RJC,

*Complainant,*

**NPC 22-012**

For: Violation of the Data  
Privacy Act of 2012

-versus-

DL,

*Respondent.*

X-----X

## RESOLUTION

**AGUIRRE, D.P.C.;**

Before the Commission is the Motion for Reconsideration dated 03 January 2023 filed by RJC.

### Facts

On 10 November 2022, the Commission issued a Decision dismissing the Complaint against Respondent DL on the ground that the processing of RJC’s personal data has lawful basis under Section 13 (f) of the Data Privacy Act of 2012 (DPA):

**WHEREFORE**, premises considered, the Commission resolves that the Complaint filed by RJC against DL is hereby **DISMISSED** for lack of merit.

**SO ORDERED.**<sup>1</sup>

On 03 January 2023, RJC filed his Motion for Reconsideration alleging that the Commission erred in dismissing the Complaint against DL.<sup>2</sup> RJC asserted that the case must not be dismissed because DL was “not able to present evidence that he is innocent.”<sup>3</sup> He claimed that “DL should have provided the evidence that the Ombudsman ordered him to use private data of the complainant without his consent.”<sup>4</sup> He averred that DL, however, was “not able to present evidence in support of his claim that he is allowed to use private data without consent from the owner based on Section 13 (f) [of the DPA].”<sup>5</sup>

RJC stated that the transcript of records that DL previously presented in his counter-affidavit before the Ombudsman is “not an official grade released by the University and since it is not official then it defeats the purpose of rebuking the claims of the complainant that he has a solid background in computer science.”<sup>6</sup> He argued, however, that the transcript “can still profile” him and thus falls within the scope of the DPA.<sup>7</sup>

RJC also questioned how DL obtained a copy of his grades since DL denied having access to the university records of the students during the Second Preliminary Conference before this Commission.<sup>8</sup>

1 Decision, 10 November 2022, at 9, in RJC v. DL, NPC 22-012 (NPC 2022).  
2 Motion for Reconsideration, 03 January 2023, at 1, in RJC v. DL, NPC 22-012 (NPC 2023).  
3 Motion for Reconsideration, 03 January 2023, at 2 & 14, in RJC v. DL, NPC 22-012 (NPC 2023).  
4 *Id.* at 3 & 7.  
5 *Id.* at 3.  
6 *Id.*  
7 *Id.*  
8 *Id.* at 4.

RJC claimed that “the statements presented in the decision of the Commission are contradicting, which is a very strong argument for reconsideration of the decision.”<sup>9</sup> To support his argument, RJC questioned the Commission’s statement:

When determining whether there is lawful processing under Section 13 (f) of the DPA, the Commission clarifies that it cannot rule on the admissibility of evidence or its probative value to a particular case outside its jurisdiction.<sup>10</sup>

...

In this case, however, it is Complainant, RJC, who raised his academic records as an issue in the Ombudsman case. The Commission stresses that DL would not have to present RJC’s transcript of records if it were not for RJC’s presentation of the issue on his academic records. Thus, it was RJC who opened the door for the submission of these types of evidence.<sup>11</sup>

RJC argued that he could not have raised the submission of these types of evidence because “there is no proof that it was [him] who raised his academic records as an issue [before] the Ombudsman.”<sup>12</sup>

RJC also averred that DL disclosed his grades “without his consent and without informing him about the process of his personal sensitive information [sic].”<sup>13</sup> He claimed that DL “has no legal obligation to provide the Ombudsman [with] a copy of [his] grades” absent a subpoena or order from the Ombudsman.<sup>14</sup>

RJC also stated that DL did not present “any measures or guidelines for the lawful processing of [RJC’s] school records or that the same was in adherence to the principles of transparency, legitimate purpose[,] and proportionality when the disclosure was made before the Office of the Ombudsman.”<sup>15</sup> RJC argued that the Commission must adhere to the principles of legitimate purpose and proportionality since it discussed in its Decision the importance of the qualifier ‘necessary’ in Section 13 (f) of the DPA:

[C]onsidering 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 of Section 13 (f) therefore [sic], serves to limit the potentially broad concept of ‘establishment of legal claims’ consistent with the general principles of legitimate purpose and proportionality.<sup>16</sup>

RJC also claimed that the transcript of records was marked “for advising purposes only”<sup>17</sup> and “the act of disclosure of an unofficial copy of school records ... is malicious and unwarranted.”<sup>18</sup> He reiterated his argument that DL processed his transcript of records without his consent, and thus a “direct violation [of] the law.”<sup>19</sup>

9 Motion for Reconsideration, 03 January 2023, at 4, in RJC v. DL, NPC 22-012 (NPC 2023).

10 Decision, 10 November 2022, at 8, in RJC v. DL, NPC 22-012 (NPC 2022).

11 Decision, 10 November 2022, at 9, in RJC v. DL, NPC 22-012 (NPC 2022).

12 Motion for Reconsideration, 03 January 2023, at 5, in RJC v. DL, NPC 22-012 (NPC 2023).

13 *Id.*

14 *Id.* at 7.

15 *Id.*

16 *Id.* at 4.

17 *Id.* at 9.

18 Motion for Reconsideration, 03 January 2023, at 9, in RJC v. DL, NPC 22-012 (NPC 2023).

19 *Id.* at 10.

RJC prayed that the Commission set aside the Decision dated 10 November 2022, prosecute DL for violation of the DPA, and award damages.<sup>20</sup>

On 11 January 2023, Respondent DL submitted his Comment/Opposition to the Motion for Reconsideration.<sup>21</sup>

DL opposed the claims of RJC stating that, “the duty to meet the burden and [to] substantiate his allegations is on the [Complainant], not on the Respondent.”<sup>22</sup>

DL also raised that “it is not within the province of the Ombudsman to authorize or order [DL] in said case what specific evidence he is allowed to present.”<sup>23</sup> He explained that the Ombudsman, nevertheless, ordered him “to file his answer to the complaint by way of Counter-Affidavit and other relevant controverting evidence that he may present in his defense.”<sup>24</sup>

Further, DL reiterated his argument in his Verified Comment dated 08 March 2022 that:

To reiterate, attaching as evidence during the Ombudsman administrative and criminal proceedings a copy of the student’s scholastic record comprises a different context as compared to releasing such record to any third party or publicizing it in a social media platform or website. The former is necessary and proportional to the exercise or defense of legal claims, while the latter is unnecessary and disproportional for any purpose.<sup>25</sup>

Following this, DL prayed that the Motion for Reconsideration filed by RJC be denied for lack of merit.<sup>26</sup>

On 13 January 2023, RJC submitted his Reply to Respondent’s Comment/Opposition<sup>27</sup> reiterating the arguments in his Motion for Reconsideration. He again argued that “it is very clear that [R]espondent DL used the [C]omplainant’s private data without any consent”<sup>28</sup> and that “DL did not provide evidence to prove that he is innocent.”<sup>29</sup> Further, he stressed DL’s supposed admission in his Comment that there was no legal order from the Ombudsman directing DL to present the school records of RJC.<sup>30</sup>

### **Issue**

Whether the Motion for Reconsideration dated 10 November 2022 should be granted.

### **Discussion**

It is a basic rule of evidence that each party must prove his affirmative allegation.<sup>31</sup>If he

---

20 *Id.* at 15.  
21 Comment/Opposition to Motion for Reconsideration, 11 January 2023, at 1, in RJC v. DL, NPC 22-012 (NPC 2023).  
22 *Id.*  
23 *Id.* at 2.  
24 *Id.*  
25 Comment/Opposition to Motion for Reconsideration, 11 January 2023, at 4, in RJC v. DL, NPC 22-012 (NPC 2023).  
26 *Id.*  
27 Reply to Respondent’s Comment/Opposition, 13 January 2023, at 1, in RJC v. DL, NPC 22-012 (NPC 2023).  
28 *Id.*  
29 *Id.* at 2.  
30 *Id.*  
31 Reyes v. Glaucoma Research Foundation, Inc., G.R. No. 189255 (2015).

claims a right granted by law, he must prove his claim by competent evidence, relying on the strength of his own evidence and not upon the weakness of that of his opponent.<sup>32</sup>

In his Motion for Reconsideration, RJC stressed that his complaint against DL for violation of the DPA should not have been dismissed because “in totality, there is no evidence presented by Respondent DL to prove that he is innocent.”<sup>33</sup>

Contrary to what RJC believes, however, it is not for DL to prove that he is innocent. RJC cannot simply wait for the other party to present evidence proving DL’s innocence. As the complainant, RJC must prove his allegation that DL violated the DPA. This, he failed to do.

For this reason, the Commission denies RJC’s Motion for Reconsideration dated 03 January 2023.

RJC argued that DL violated the DPA because DL disclosed his grades “without his consent and without informing him about the process of his personal sensitive information [sic].”<sup>34</sup>

RJC asserted that “the law is very clear that there must be consent from the owner and that the owner must be informed when his data is being processed.”<sup>35</sup>

Based on his arguments, RJC seems to be of the impression that only consent from the data subject can be used to justify the processing of personal information or that consent is the default and the other lawful criteria for processing under the DPA are mere exceptions. To allow this misinterpretation will result in ignoring clear provisions of the DPA that provide for other lawful criteria to process personal information and sensitive personal information.

The Commission has repeatedly held that consent is not the only lawful criteria to process sensitive personal information:

[C]onsent 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.<sup>36</sup>

As discussed in the Decision dated 10 November 2022, the school records of RJC subject of this case are sensitive personal information and they may be lawfully processed for the establishment, exercise, or defense of legal claims.<sup>37</sup>

In this case, DL included RJC’s transcript of records in his counteraffidavit filed before the Ombudsman. According to DL, this was a part of his defense against the claims of RJC and necessary for the protection of his lawful rights and interests in the proceed

---

32 *Id.*

33 Motion for Reconsideration, 03 January 2023, at 15, in RJC v. DL, NPC 22-012 (NPC 2023)

34 *Id.* at 5.

35 *Id.* at 15.

36 ACN v. DT, NPC 18-109, 01 June 2021, at 10, available at <https://www.privacy.gov.ph/wpcontent/uploads/2022/01/Decision-NPC-18-109-ACN-v.-DT.pdf> (last accessed 10 February 2023).

37 Decision, 10 November 2022, at 8, in RJC v. DL, NPC 22-012 (NPC 2022).

ings before the Ombudsman.

The Decision recognized DL’s supposed purpose in using RJC’s transcript of records:

RJC filed the Ombudsman case claiming that the respondents in that case, including DL, ‘were deliberately and/or negligently delaying his graduation for no valid reason’. [DL] claimed that RJC made material allegations in the case, ‘which if not controverted by documentary evidence, may lead to the erroneous conclusion that [the] respondents in said Ombudsman cases [sic] abused their authority and committed grave misconduct in allegedly delaying the graduation of [RJC].’<sup>38</sup>

Following this, the Commission held that the processing of RJC’s personal data had lawful basis under Section 13 (f) of the DPA:

DL alleged that his purpose in using RJC’s transcript of records in his counter-affidavit was to disprove RJC’s ‘false material claims.’ Such purpose may be deemed for the ‘establishment, exercise or defense of legal claims’ under Section 13 (f) of the DPA.<sup>39</sup>

In its Decision, the Commission explained that “DL would not have to present RJC’s transcript of records if it were not for RJC’s presentation of the issue on his academic records.”<sup>40</sup>It was RJC who raised his academic records as an issue in the Ombudsman case thus “it was RJC who opened the door for the submission of these types of evidence.”<sup>41</sup>

RJC argued that “if this [Motion for Reconsideration] can be easily dismissed because of the allegation that it was the complainant who opened the door for the submission of his private personal data, then the statement strongly argues that it is legal to use personal private data without consent from the owner simply because it is open.”<sup>42</sup>

RJC again misinterpreted the statements in the Decision. In its Decision, the Commission explained that the submission of RJC’s transcript of records as part of DL’s defense was necessitated by the issues relating to the academic records of RJC and the supposed reasons for the delay in his graduation. It was RJC who made his academic standing an issue in the Ombudsman case when he claimed that respondents “were deliberately and/or negligently delaying his graduation for no valid reason.”<sup>43</sup> In response, DL presented RJC’s transcript of grades to disprove RJC’s false claims. Given these allegations, RJC cannot now fault DL for presenting evidence to contradict the claims against him.

RJC further asserted that DL, in proving his innocence, should have shown that the “Ombudsman ordered him to use private data of the complainant without his consent.”<sup>44</sup>He argued that “[DL] has no obligation to provide the Ombudsman a copy of the complainant[’s] grades because [DL] failed to present evidence that the Ombudsman issued a subpoena or order [to DL] to release the [his] grades.”<sup>45</sup>

---

38 *Id.* at 2.

39 *Id.* at 8.

40 Decision, 10 November 2022, at 9, in RJC v. DL, NPC 22-012 (NPC 2022).

41 *Id.*

42 Motion for Reconsideration, 03 January 2023, at 12, in RJC v. DL, NPC 22-012 (NPC 2023).

43 Decision, 10 November 2022, at 2, in RJC v. DL, NPC 22-012 (NPC 2022).

44 Motion for Reconsideration, 03 January 2023, at 3, in RJC v. DL, NPC 22-012 (NPC 2023).

45 *Id.* at 7.

RJC maintained that if Section 13 (f) of the DPA will be relied on, then there must be authority to use his grades in the form of an “order from the Ombudsman [which] allowed [DL] to use private data without consent of the owner”.<sup>46</sup>

RJC’s argument is untenable. There is nothing in Section 13 (f) of the DPA that requires the personal information controller (PIC) to present a specific order before lawfully processing sensitive personal information. In fact, the Commission has previously held that an existing court proceeding is not even required before Section 13 (f) can apply.<sup>47</sup>

Since a court proceeding is not required in invoking Section 13 (f) as a lawful criterion for the processing of sensitive personal information, there is less reason to require a specific order before sensitive personal information can be processed for the protection of lawful rights and interests of persons in court proceedings, or the establishment, exercise, or defense of a legal claim.

In his Motion for Reconsideration, RJC also questioned the application of the principles of transparency and proportionality in the use of his transcript of records as evidence.<sup>48</sup> He alleged that the principle of transparency was not adhered to when he was neither informed nor made aware that DL would disclose his school records to the Office of the Ombudsman.<sup>49</sup>

Section 16 (a) of the DPA requires that the data subject “[b]e informed whether personal information pertaining to him or her shall be, are being or have been processed.”<sup>50</sup> The Implementing Rules and Regulations of the DPA further provides that the data subject be informed of the processing before the information is processed or at the next practical opportunity.<sup>51</sup> The “next practical opportunity” depends on the surrounding circumstance of each case. It, however, must always be within a reasonable period to give effect to the data subject’s right to be informed.<sup>52</sup>

In cases where Section 13 (f) is used as basis to process personal information, for practical considerations including the prevention of tampering with evidence, the “next practical opportunity” to inform the data subject can be when the party is furnished or served with a copy of the pleading containing personal data.

The Supreme Court explained that:

Service means the delivery or communication of a pleading, notice or some other paper in a case, to the opposite party so as to charge him with receipt of it and subject him to its legal effect. The purpose of the rules on service is to make sure that the party being served with the pleading, order or judgment is duly informed of the same so that he can take steps to protect his interests.<sup>53</sup>

---

46 *Id.* at 5.

47 A & TA v. EJ, EE, & HC, NPC 17-018, 15 July 2019, at 8, available at <https://www.privacy.gov.ph/wp-content/uploads/2022/04/NPC-17-018-EA-and-TA-v-EJ-Decision2019.07.15-.pdf> (last accessed 02 March 2023)

48 Motion for Reconsideration, 03 January 2023, at 7, in RJC v. DL, NPC 22-012 (NPC 2023).

49 *Id.* at 8.

50 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 (a) (2012).

51 National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, Rule VIII, § 34(a)(2) (2016).

52 ECA v. XXX, NPC 18-103, 23 July 2020, at 5, available at <https://www.privacy.gov.ph/wpcontent/uploads/2020/12/NPC-18-103-ECA-v-XXX-Decision-ADJU1.pdf> (last accessed 27 April 2023)

53 Raoul C. Villarete v. Commission on Audit, G.R. No. 243818 (2022).

Thus, it is during service to the opposing party that a party is provided a practical opportunity to inform the former that the personal data made part of the pleadings and other court submissions was used for the protection of lawful rights and interests, or the establishment, exercise, or defense of legal claims.

In this case, RJC was informed of the use of his sensitive personal information when he received a copy of DL's counter-affidavit in the Ombudsman case along with a copy of his transcript of records in March 2018.<sup>54</sup>

RJC alleged that the principle of proportionality was also not adhered to because "DL failed to explain... why would the entire and complete grades of [RJC is] relevant to his [Maximum Residency Rule] status for his [Master of Science in Computer Science] program."<sup>55</sup> RJC also argued that the copy of Transcript of Records attached by DL is "not an official grade released by the University and since it is not official, then it defeats the purpose of rebuking the claims of the complainant that he has a solid background in computer science."<sup>56</sup>

In its Decision, the Commission already ruled on this argument stating that "when determining whether there is lawful processing under Section 13 (f) of the DPA, ... it cannot rule on the admissibility of evidence or its probative value to a particular case outside its jurisdiction."<sup>57</sup>

The Commission is mandated to administer and implement the DPA,<sup>58</sup> part of this is ensuring the compliance of PICs with the provisions of the DPA.<sup>59</sup> As such, it is within the Commission's mandate to decide if personal or sensitive personal information is processed in accordance with a lawful criterion under the DPA. But in doing so, the Commission is limited to ruling only on the lawfulness of the processing based on the DPA, its IRR, and its other issuances. It cannot rule on the admissibility of evidence submitted to another tribunal outside of its jurisdiction or the propriety of the legal strategy employed by parties in legal proceedings.

Further, the first part of Section 13(f) of the DPA requires that the information is "necessary for the protection of lawful rights and interests of persons in court proceedings." In ruling that it was RJC who "opened that door" for the presentation of his grades, which prompted DL to present evidence to discredit the RJC's claims, the Commission already ruled on this issue in its Decision.

Nevertheless, considering that the Commission does not rule on the admissibility of evidence and considering that all the factual circumstances of a proceeding in another tribunal will not and should not be presented before this Commission, the burden was on RJC to prove that the personal data used by DL in his defense was not necessary. While RJC voiced all manner of objections in his Motion for Reconsideration saying that other pieces of evidence such as a certification from the Office of the Registrar could have sufficed,<sup>60</sup> he still failed to show that it was unnecessary.

In assessing what is necessary for the protection of lawful rights and interests of a per-

54 Memorandum for Complainant, 04 August 2022, at 3, in RJC v. DL, NPC 22-012 (NPC 2022).

55 Motion for Reconsideration, 03 January 2023, at 9, in RJC v. DL, NPC 22-012 (NPC 2023).

56 *Id.* at 3

57 Decision, 10 November 2022, at 8, in RJC v. DL, NPC 22-012 (NPC 2022).

58 Decision, 10 November 2022, at 8, in RJC v. DL, NPC 22-012 (NPC 2022).

59 *Id.* § 7 (a).

60 Motion for Reconsideration, 03 January 2023, at 9, in RJC v. DL, NPC 22-012 (NPC 2023).



son in court proceeding, it is not for the complainant to dictate what pieces of evidence are necessary and can be used by the respondent in their defense.

Given the foregoing, the Motion for Reconsideration dated 03 February 2023 failed to present any argument which would warrant a reversal of the Decision dated 10 November 2022.

**WHEREFORE**, premises considered, the Commission resolves to **DENY** the Motion for Reconsideration dated 03 January 2023 filed by RJC. The Decision dated 10 November 2022 is hereby **AFFIRMED**.

**SO ORDERED.**

City of Pasay,  
Philippines. 26 January 2023.

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

**Sgd.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**Sgd.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

Copy furnished:

**RJC**  
*Complainant*

**DL**  
*Respondent*

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

Complainant,

For: Violation of the Data Privacy Act of 2012

-versus-

FNT and NNT

Respondent.

X-----X

RESOLUTION

AGUIRRE, D.P.C.;

This Commission resolves the Motion for Reconsideration (MR) filed by FNT on the Decision dated 22 September 2022.

Facts

On 22 September 2022, the Commission issued a Decision and held FNT liable for a violation of Section 25 (Unauthorized Processing of Personal Information and Sensitive Personal Information) of Republic Act No. 10173 or the Data Privacy Act (DPA):

WHEREFORE, premises considered, this Commission hereby:

- 1. **DISMISSES** the case against NNT for lack of merit; and
- 2. **FINDS** that FNT violated Section 25 of the Data Privacy Act of 2012 (DPA) and **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice. This Commission **RECOMMENDS** the prosecution of FNT for Unauthorized Processing of Personal or Sensitive Personal Information under Section 25 of the DPA.

SO ORDERED.<sup>1</sup>

On 29 December 2022, FNT received the Decision by email.<sup>2</sup>

On 06 January 2023, FNT received the Decision by registered mail.<sup>3</sup>

On 07 January 2023, FNT sent an email inquiry to the National Privacy Commission (NPC) Adjudication Secretariat at adjudication@privacy.gov.ph.<sup>4</sup>She requested clarification on whether to submit a “Motion” or a “comment about the Decision.”<sup>5</sup>

On 20 January 2023, FNT visited the NPC Adjudication Secretariat, specifically Atty. Lee Santos-Javier or the Clerk of the Commission, to clarify the date when she can

1 Decision, 22 September 2022, at 22, in JBA v. FNT and NNT, NPC 20-026 (NPC 2022).  
 2 Statement in Support for the Submission of Motion of Extension of Time and Motion for Reconsideration, 13 February 2023, at 2, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).  
 3 Motion For Extension of Time to Submit the Final Copy of Motion for Reconsideration, 26 January 2023, at 1, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).  
 4 Statement in Support for the Submission of Motion of Extension of Time and Motion for Reconsideration, 13 February 2023, at 3, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).  
 5 *Id.*

submit her MR.<sup>6</sup>

On the same day, FNT stated that she sought to avail herself of the services of the Public Attorney’s Office (PAO), but her request was denied due to “conflict of interest”.<sup>7</sup> She narrated that the PAO declined to represent her because JBA, the Complainant, was already assisted by the same PAO at F.B. Harrison Street, Pasay City.<sup>8</sup>

According to FNT, she also completed the requirements to avail of the legal assistance program of the Integrated Bar of the Philippines (IBP) Cavite, but it was “subject for approval.”<sup>9</sup>

Nonetheless, on 20 January 2023, FNT filed her MR, arguing the following:

1. She denies using nor processing JBA’s personal information after her resignation in 2018.
2. She denies having access to the account in the Sheryna.ph website (Sheryna) and her staff members create the account for her.
3. She denies having knowledge about the accounts relating to the “AUTO-RENEW” ads in Sheryna. She explained that the ads were manually posted only on 2016 and the ads were “system generated” or “system automated.”
4. She did not pay for the subscription of the website’s autorenewal feature.<sup>10</sup>

In her MR, FNT denies having access to Sheryna and clarifies that her staff members are the ones who created the account for her:

Never ko naaccess ang account na Sheryna ph, pero inaaral ko may umulit ang posts pero nagbabago ang DATE ng post. Kaya nasa System to ng Sheryna.ph na nag “AUTO-RENEW” at ENCRYPTED” ito sa Website. Kapag ENCRYPTED” meaning conceal data by converting it into a “code” to prevent unauthorized access. “.<sup>11</sup>

May[sic] STAFF created also my Account. Hundreds of Ads posted Online from different websites, for House and Lot selling and Recruitment. I check my secondary email [ ] and [ ] using keyword: Property and Alexandra to view AD different websites.<sup>12</sup>

FNT likewise explained that the ads in Sheryna were still being posted as late as February and November 2021 even though the ads were originally posted in 2016 because the posting of ads is “automatically renewed” by Sheryna:

Bakit meron listings still “being posted” as late as February and November 2021? My Answer ‘AUTOMATED RENEW’ or ‘AUTO-RENEW’ or “AUTOMATIC RENEWAL”. I analyzed the ADS ID Number each post, ang first FOUR (4) Digits ng ADS ID pareho-pareho at hindi nagkakalayo ang last Two (2) Digits, pero ang Date at year ay iba iba at kung basis ang PRICE pareho ito sa mga ADS posted year 2016.<sup>13</sup>

---

6 Motion For Extension of Time to Submit the Final Copy of Motion for Reconsideration, 26 January 2023, at 1, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).

7 *Id.*

8 *Id.*

9 Motion for Extension of Time to Submit the Final Copy of Motion for Reconsideration, 26 January 2023, at 1, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).

10 Motion for Reconsideration, 20 January 2023, at 1-14, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).

11 *Id.* at 1

12 *Id.*

13 *Id.*

How would I know na may ADS sa Sheryna.ph kung wala akong lists saan nakapost ang Agent? How would I know na may AUTO RENEW “Features” ang Sheryna.ph? If I have the lists, nadelete or deactivated na ang account and posts are deleted also gaya ng mga ibang account sa mga ECOMMERCE Website at ang facebook account na ginagamit ni Agent JBA noon are all DELETED.<sup>14</sup>

To further justify her claim that the ads were “auto-renewed,” FNT explained that the digits of the newly posted ads’ ID numbers are different compared to the ID number of previously posted ads:

Mga analysis ko bakit AUTORENEW ang mga ADS sa Sheryna.ph the following:

1. Two (2) House Model Unit sa Sheryna.ph Posts ay PHASE-OUT na ang Catherine Townhouse since 2018 and Diana Townhouse since 2017. Hindi na Removed kaya activate pa rin. It’s not reasonable ipost ang mga House Model Units that are already SOLD-OUT and PHASEOUT at walang Inventory.

2. Prices are not updated since 2016, hindi ito na-access para ma-update

**3. Check the AD ID, pareho ang first four (4) digits “4083” and ang last two (2) Digit Numbers all ADS hindi nagkakalayo.**

4. May Screenshot na umulit ang AD ID #408339 na Catherine Townhouse at AD ID #408326 an Alexandra House. Ang Catherine Townhouse ay nag AUTORENEW ito ng November 2018 at November 2021, magkaibang year pero same Month “November” Ganun din ang Alexandra House captured sa screenshot ni Ms JBA, Last AUTO RENEW was February 07, 2017 at ang bagong AUTO RENEW date was February 08, 2021 same month “February” pero magkaibang year.<sup>15</sup>

...

4) Are ADS newly posted? NO! **Go to Sheryna.ph website post at least Three (3) ADS at the same day, and check the AD ID, analyze the series or numbers and compare AD ID sa mga ADS sa Account** ni Aqua (Screenshot) versus mga NEWLY POST AD.<sup>16</sup>

...

Ang Series ng mga AD ID sa 151 four digits “4083” pareho lahat ang six (6) ADS at ang last two (2) digits ay hindi nagkakalayo.

Kapag nagposts ng ADS sa Sheryna.ph. the higher the Series Number the newest the AD, and the lowest Series Number the Oldest Posts.

Dahil sa SERIES NUMBER ng AD ID na pareho ang mga 1st Four (4) Digits “4083” at hindi nagkakalayo ang mga last Two (2) Digits, nangangahulugan na ang mga ADS na ito ay naipost sa isang araw sa magkaibang oras at dahil “RANDOM” ang AUTOMATED RENEW ng Sheryna.ph, nagbago ang mga DATE at YEAR pero walang nagbago sa AD ID. **Paisa-isa ang pag AUTORENEW sa Sheryna.ph sa account na ito, tama dahil “RANDOM” ang sagot nila, at kaya tinatawag itong SYSTEM GENERATED OR SYSTEM AUTOMATION, at hindi manual posting.**<sup>17</sup>

...

Wala din proof na may “NEWLY” posts sa iba pang Websites based sa screenshot sa mga ADS Posted and mga DATE from 2015; 2016 only. **Except sa Sheryna.ph**

14 *Id.* at 13.

15 *Id.* at 3.

16 Motion for Reconsideration, 20 January 2023, at 8, in *JBA v. FNT and NNT*, NPC 20-026 (NPC 2023).

17 *Id.* at 6.

**ADS na may AUTO RENEW Feature. Are the ADS at Sheryna.ph [are] NEWLY POSTED? NO. Hindi NEWLY Posted ang mga ADS, inaaral ko base sa AD ID; PRICES; TITLE ADS & details walng nagbabago, unreasonable na mag post ng ADS na hindi updated.** Unreasonable dahil my staff created [me] an account at Sheryn.ph at iba't ibang website na mas marami ADS. Hindi ko din naaccess since 2016 ang mga account ginawa sa akin kaya hindi rin ito updated.<sup>18</sup>

FNT also narrated that she even messaged the Sheryna website to ask the reason for the renewal “every 90 days [sic] or yearly basis”, to which Sheryna replied “Random”.<sup>19</sup>

On 21 January 2023, FNT emailed the NPC Adjudication Secretariat requesting an extension of fifteen (15) days to submit a “FINAL COPY of Motion.”<sup>20</sup> FNT explained that she did not receive any response or acknowledgement from the Adjudication Secretariat.<sup>21</sup>

On 26 January 2023, FNT visited Atty. Santos-Javier for the second time to submit a physical copy of her Motion of Extension of Time.<sup>22</sup>

On the same day, FNT also filed a Motion for Extension of Time to Submit the Final Copy of Motion for Reconsideration by email.<sup>23</sup>FNT prayed that the Commission grant another fifteen (15) days to submit the “FINAL COPY” of her Motion for Consideration [sic].<sup>24</sup> She also prayed that other reliefs that are deemed just and equitable be granted.<sup>25</sup>

On 27 January 2023, FNT again returned to the NPC Adjudication Secretariat “for clarification of days to be counted for the submission [sic] of the Motion for Extension of Time and Motion for Reconsideration.”<sup>26</sup> FNT explained her confusion on the basis on when she should count the deadline for her submission:

Sinabi ko kay Attorney Javier na nalilito ako sa date na pagbabasehan? Kung ang Date ng Decision sent thru email or the data I received the physical copy via courier? Dahil noong nabasa ko ang Decision ng December 31 ng gabi, I anticipated since it was National Holiday up to January 02, 2023, no one from National Privacy Commission (NPC) can assist me or answer my inquiries.<sup>27</sup>

FNT mentioned that she inquired about the deadline of submissions last 07 January 2023 via email:

I informed Attorney Javier that last January 07, 2023, na nagemail ako sa NPC - Adjudication kay sir Joseph the Secretariat, nagtanong ako kung hanggang kailan pwede magsubmit, pero wala akong nareceived na reply. Attorney Lee Ann Santos-Javier explained, the Secretariat is hesitant to give an answer because Adjudication Department [sic] should remain neutral in this case. Baka sasabihin binibigyan ka

18 Decision, 22 September 2022, at 9, in JBA v. FNT and NNT, NPC 20-026 (NPC 2022).

19 Motion for Reconsideration, 20 January 2023, at 2, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).

20 Motion for Extension of Time to Submit the Final Copy of Motion for Reconsideration, 26 January 2023, at 2, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).

21 *Id.*

22 Statement in Support for the Submission of Motion of Extension of Time and Motion for Reconsideration, 13 February 2023, at 1, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).

23 Motion for Extension of Time to Submit the Final Copy of Motion for Reconsideration, 26 January 2023, at 1, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).

24 *Id.* at 2.

25 *Id.*

26 Statement in Support for the Submission of Motion of Extension of Time and Motion for Reconsideration, 13 February 2023, at 2, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).

27 *Id.*

naming ng advice or legal assistance. I replied to Attorney Javier, nag-inquire ako dahil when I received the hardcopy may nakalagay ‘**further inquiries or clarifications**’, kaya sa NPC – Adjudication po ako nagsend ng email.<sup>28</sup>

FNT also asked Atty. Santos-Javier if her submissions are already considered late.

I asked Attorney Javier kung late na ang submission ko ng Motion? Attorney Javier explained, she cannot give the answer, since wala siyang power to decide. Attorney Javier further said, hintayin ko kung anong magiging sagot ng Committee En Banc of [the National Privacy Commission (NPC)] kung tatanggapin nila ang nasubmit mo [sic] Motion for Reconsideration and Motion for Extension of Date. Hindi niya maisagot kung hanggang kailan pwede magsubmit, ang sinabi niya lang ‘naitable’ ko sa Committee lahat ng nasubmit na Motion noong last January 20, 2023 at ang mga email mo.<sup>29</sup>

On 13 February 2023, FNT filed her Statement in Support for the Submission of Motion of Extension of Time and Motion for Reconsideration (Statement).<sup>30</sup>In the Statement, FNT reiterated her prayer that the Commission grant both her Motion for Extension and MR.<sup>31</sup>

### Issue

Whether the MR filed by FNT dated 20 January 2023 should be granted.

### Discussion

The Commission denies FNT’s MR. The Commission finds no reason to overturn the Decision dated 22 September 2022 since the MR was filed out of time, and FNT provided no new or material arguments that could overturn the Decision.

#### **I. FNT filed the MR out of time.**

For cases before the NPC, judgments, orders, or resolutions shall be served either personally, by registered mail, by courier, or by electronic mail.<sup>32</sup> Rule III, Section 6 of the NPC Circular 2021-01 (2021 NPC Rules of Procedure) provides:

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.<sup>33</sup>

The Commission’s judgments, orders, or resolutions shall only be served through cou-

---

28 *Id.* at 2-3.

29 *Id.* at 4.

30 *Id.* at 2.

31 *Id.*

32 National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC Circular No. 2021-01], rule III, § 6 (28 January 2021).

33 National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC Circular No. 2021-01], rule III, § 6 (28 January 2021). Emphasis supplied.

rier when an updated email of the party is unavailable.<sup>34</sup> This is to prevent a situation where an adverse party will insist on computing the period to comply with the Commission's directive from the later date of receipt.

This situation, however, cannot apply to this case. FNT cannot claim that her email is unavailable since she herself admitted that she received the e-mails from the NPC Adjudication Secretariat. In fact, the records show that FNT received the Decision by email on 29 December 2022.<sup>35</sup>

A period of fifteen (15) days from the receipt of the copy of the decision is given to a party for him or her to file an appeal.<sup>36</sup> Section 4, Rule 8 of the 2021 NPC Rules of Procedure provides that the Commission's decision becomes final and executory within fifteen (15) days from receipt of the parties:

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.<sup>37</sup>

Thus, a party may appeal the Commission's Decision by filing a motion for reconsideration within the fifteen-day period. If no motion for reconsideration is filed within the period, then the Decision becomes final and executory.<sup>38</sup>

FNT received the Decision by email on 29 December 2022.<sup>39</sup> Following Section 4, Rule 8 of the 2021 NPC Rules of Procedure, she had fifteen (15) days from 29 December 2022 or until 13 January 2023 to file her MR.

FNT herself acknowledged that she knew that the Decision was already final and executory on 13 January 2023:

*Tinanong ko ulit si Atty. Lee kung paano ang bilangan ng submission ng Motions dahil ang nakasaad sa CERTIFICATION 'The said Decision was delivered to and received by both parties on 29 December 2022, via electronic mail, and the same has become **final and executory on 13 January 2023.**'*<sup>40</sup>

Despite this, FNT only filed her MR on 20 January 2023 or seven (7) days beyond the fifteen-day period for appeal.<sup>41</sup> As a result, FNT's MR filed on 20 January 2023 was filed out of time, and the Decision dated 22 September 2022 became final and executory.

## **II. FNT provided no new or material arguments to warrant a reversal of the Decision dated 22 September 2022.**

Nevertheless, even if the MR was filed on time, FNT still did not provide any new or ma-

<sup>34</sup> *Id.*

<sup>35</sup> Statement in Support for the Submission of Motion of Extension of Time and Motion for Reconsideration, 13 February 2023, at 2, in *JBA v. FNT and NNT*, NPC 20-026 (NPC 2023).

<sup>36</sup> NPC 2021 Rules of Procedure, rule II, § 4.

<sup>37</sup> *Id.* Emphasis supplied.

<sup>38</sup> *Id.*

<sup>39</sup> Statement in Support for the Submission of Motion of Extension of Time and Motion for Reconsideration, 13 February 2023, at 2, in *JBA v. FNT and NNT*, NPC 20-026 (NPC 2023).

<sup>40</sup> *Id.*

<sup>41</sup> Motion for Reconsideration, 20 January 2023, at 1, in *JBA v. FNT and NNT*, NPC 20-026 (NPC 2023).

terial allegations to justify a reversal of the Decision dated 22 September 2022.

In the Decision dated 22 September 2022, the Commission held FNT liable for Section 25 (Unauthorized Processing of Sensitive or Personal Information) of the DPA.<sup>42</sup>FNT processed JBA’s personal information by posting ad listings even after JBA’s resignation.<sup>43</sup>When JBA submitted her official resignation letter, she withdrew her consent and explicitly exercised her right to erasure as a data subject.<sup>44</sup>

In the MR, FNT relies heavily on the allegation that she denies the processing of JBA’s personal information after her resignation because of the “AUTO-RENEW” feature of ads posted on the Sheryna website.<sup>45</sup>

To recall, in her Verified Comment dated 23 December 2021, she explained:

Isang beses lang mag posts, at hindi na binabalikan dahil ang ibang posting naka AUTO RENEW, ibig sabihin after 30 days kapag na-expire may auto renewal posts either 3 months, 6 months, or 1 year.<sup>46</sup>

While the Commission takes note of the explanations provided by FNT on this point in the MR, these arguments, however, are neither new nor material to warrant the reversal of the Commission’s Decision.

The Commission stresses the obligation of Personal Information Controllers (PIC) to remain accountable for personal information in its control.<sup>47</sup>

Section 3(h) of the DPA defines a PIC as:

Section 3. Definition of Terms.

...

(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.<sup>48</sup>

In her Verified Comment, FNT explained how the business of her real estate agency is conducted.<sup>49</sup> FNT described that she orients newly recruited agents while her staff members create “secondary accounts” for the agents to use in selling real estate properties on various platforms for “online marketing.”<sup>50</sup>In her MR, she reiterated that her staff members create the accounts in her name and that she personally has no access to those accounts.<sup>51</sup>FNT also explained that she herself has no copy of any list showing

42 Decision, 22 September 2022, at 22, in JBA v. FNT and NNT, NPC 20-026 (NPC 2022).

43 *Id.*

44 *Id.*

45 Motion for Reconsideration, 20 January 2023, at 1, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).

46 Verified Comment of FNT, 23 December 2021, at 2, in JBA v. FNT and NNT, NPC 20-026 (NPC 2021).

47 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 § 21 (a) and (b) (2012). Emphasis supplied.

48 Data Privacy Act, § 3 (h). Emphasis supplied.

49 Verified Comment of FNT, 23 December 2021, at 5, in JBA v. FNT and NNT, NPC 20-026 (NPC 2021).

50 *Id.*

51 Motion for Reconsideration, 20 January 2023, at 29, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).



where the ads are being posted by her staff.<sup>52</sup>

In this kind of relationship, even if FNT's staff members are the ones tasked with making these secondary accounts, FNT is still considered the PIC. After all, she is the person who instructs another person or organization to collect, hold, process, use, transfer, or disclose personal information on her behalf. Further, because these accounts, as well as the ads posted using those accounts, were not only created following her instructions but, more importantly, all benefit her company, she cannot evade liability as the PIC.

Section 21 of the DPA provides that a PIC is responsible for personal information under its control:

Section 21. *Principle of Accountability.* **Each personal information controller is responsible for personal information under its control or custody**, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(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.<sup>53</sup>

As a PIC, FNT is accountable for overseeing the type of information utilized by her team and ensuring the accuracy of the platform where such information is being published. This also means that it is her obligation to ensure that the processing of personal information being carried out is in accordance with the legal basis provided by law.

In her MR, however, FNT denies that she had access and control over the ads because her staff failed to give her a list of all websites their agency used.<sup>54</sup> Additionally, FNT denied that she had access to the website accounts because her staff member had already resigned prior to JBA's resignation.<sup>55</sup> This argument is a reiteration of one of her claims in her Verified Comment:

I already commented na may mga account and ADS na hindi na-delete noon **dahil hindi ako nabigyan ng listahan ng staff kung saan saan websites siya nag post.** Isa na dito ang Sheryna.ph Website at gaya ng Piliko.com na iisa ang website builder, ay parehong HINDI DELETED ang account. At naunang mag-resign ang Staff ko, Ms. JBA resigned 2018, rason hindi ito naaccess dahil walang lists kung kaya from 2016 the date it was registered and ADS was published at still nag-exists until 2022.<sup>56</sup>

FNT cannot simply evade her obligations by claiming that her staff members did not provide her with a comprehensive list of the websites where the various ads were published. FNT should have taken the appropriate measures to ensure that there are

52 *Id.* at 15.

53 Data Privacy Act, § 21 (a) and (b). Emphasis supplied.

54 Motion for Reconsideration, 20 January 2023, at 1, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).

55 *Id.*

56 *Id.*

designated processes and procedures in place. Since these could have been foreseen, the procedures will be useful when it comes to managing the personal information of her recruited real estate agents.

FNT's actions, or lack thereof, demonstrated her lack of accountability on her part as a PIC.

In the Decision dated 22 September 2022, the Commission ruled that “availing of automatic renewal methods does not remove a [PIC’s] obligation to ensure that personal information is properly processed and that a data subject’s rights are observed.”<sup>57</sup>

Even if FNT argues that the ads are not “newly posted” by her, this does not change the fact that the ads which contain JBA’s personal information keep appearing on the website because of the feature she availed of in 2016. This reinforces the fact that FNT was unable to discontinue such ads. She also failed to do anything from the time the staff member who had access resigned until JBA resigned and exercised her right to erasure and even after that.

Lastly, FNT averred that she did not pay for the subscription of Sheryna’s auto-renewal feature.<sup>58</sup> In her MR, she again failed to provide additional circumstances that would warrant a denial of the request for erasure under Section 10(B)(2) of NPC Advisory 21-01 on Data Subject Rights. Absent any of those circumstances, she should have acted on JBA’s request for erasure.

Upon JBA’s resignation on 30 October 2018, FNT should have initiated the removal of ads containing JBA’s personal information. The ads served a specific purpose which is no longer relevant after JBA’s resignation making its continued presence in the website unnecessary.<sup>59</sup> Thus, FNT should have removed the same since it was specifically requested in JBA’s resignation letter that “all the dummy account [sic] you created in my name will be remove [sic] in [sic] Facebook, [LinkedIn] [and] any website and other online services.”<sup>60</sup>

As emphasized in the Decision, there is no longer any reason to post the ads with JBA’s name since JBA was no longer affiliated with FNT or any of her businesses.<sup>61</sup> Since the dates of the ads in Sheryna were posted after JBA’s resignation on 30 October 2018, JBA’s personal information are no longer necessary for the purposes for which they were collected.<sup>62</sup>

Besides, when JBA exercised her right to erasure, any consent previously given for the use of her name in these ads and for those accounts is no longer valid since she has effectively withdrawn her consent.

Even if FNT did not purchase the auto-renewal method, the fact remains that she took advantage of the feature in advertising her property listings. JBA’s resignation and exercise of her right to erasure should have prompted FNT to act strictly in managing how long those ads would be posted.

---

57 Decision, 22 September 2022, at 21, in JBA v. FNT and NNT, NPC 20-026 (NPC 2022).  
58 Motion for Reconsideration, 20 January 2023, at 1, in JBA v. FNT and NNT, NPC 20-026 (NPC 2023).  
59 Decision, 22 September 2022, at 21, in JBA v. FNT and NNT, NPC 20-026 (NPC 2022).  
60 Complaints-Assisted Form, 20 January 2020, at 11, in JBA v. FNT and NNT, NPC 20-026 (NPC 2020).  
61 Decision, 22 September 2022, at 21, in JBA v. FNT and NNT, NPC 20-026 (NPC 2022).  
62 *Id.*

The DPA imposes stricter obligations on entities processing personal data. PICs or PIPs must protect the personal data in their custody and ensure that any processing undertaken is fair, lawful, and in accordance with the rights of data subjects. The obligations and responsibilities under the DPA are primarily targeted to PICs and PIPs since they are in a better position to ensure the protection of their data subjects' personal data.

Considering the foregoing, the Decision dated 22 September 2022 is maintained. FNT is liable for a violation of Section 25 (Unauthorized Processing of Personal Information and Sensitive Personal Information) of the DPA.

**WHEREFORE**, premises considered, this Commission **DENIES** the Motion for Reconsideration filed by FNT. The Decision dated 22 September 2022 is hereby **AFFIRMED**.

**SO ORDERED.**

City of Pasay, Philippines.  
22 February 2023.

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

**Sgd.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**Sgd.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

Copy furnished:

**JBA**  
*Complainant*

**FNT and NNT**  
*Respondents*

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

X-----X

**RESOLUTION**

**NAGA, P.C.;**

Before the Commission is the Compliance submitted by Leapfroggr, Inc. (Leapfroggr) to the Order of the Commission dated 10 November 2022.

**Facts**

On 10 November 2022, the Commission issued an Order requiring Leapfroggr “to submit an affidavit, sworn oath or its equivalent showing proof of notification to the two affected data subjects, the contents of the notification, and the corresponding receipt of the notification.”<sup>1</sup> The dispositive portion of the Order reads:

**WHEREFORE**, premises considered, LEAPFROGGR, INC. is hereby **ORDERED** to **SUBMIT** proof of notification to the affected data subjects within fifteen (15) days from the receipt of this Order:

**SO ORDERED.**<sup>2</sup>

On 21 December 2022, Leapfroggr submitted its compliance with the Order wherein it attached separate affidavits of LYB<sup>3</sup> and TMR.<sup>4</sup>

**Issue**

Whether Leapfroggr sufficiently complied with Commission’s Order dated 10 November 2022.

**Discussion**

The Commission finds that Leapfroggr has sufficiently complied with the Order dated 10 November 2022.

As reflected in the submissions made by Leapfroggr, the affidavits of LYB and TMR sufficiently proved that it actually notified the affected data subjects.

Rule V, Section 18 (D) of NPC Circular No. 16-03 (Personal Data Breach Management) provides:

*D. Form.* Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. **The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified**, and to safeguard against further unnecessary

1 In re: Leapfroggr, Inc., NPC BN 18-229, Order dated 10 November 2022, at p. 4  
2 Id.  
3 Affidavit dated 21 December 2022 of LYB.  
4 Affidavit dated 21 December 2022 of TMR.

disclosure of personal data. **The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach[.]** x x x *Provided further*, that the personal information controller shall establish means through which the **data subjects can exercise their rights and obtain more detailed information relating to the breach.**<sup>5</sup>

In the Order dated 10 November 2022, the Commission noted that Leapfroggr’s attachment of screenshots of email notifications to TMR and LYB in its Post-Breach Report dated 03 February 2022 were inadequate to prove that the email was received by TMR.<sup>6</sup> Thus, Leapfroggr was ordered to submit an affidavit showing proof of notification to the affected data subjects.<sup>7</sup>

Accordingly, Leapfroggr submitted its compliance containing two (2) separate affidavits from TMR and LYB stating that they received an email from Leapfroggr dated 29 November 2018 notifying them of a data breach incident.<sup>8</sup>

This Commission finds that these affidavits submitted by Leapfroggr, containing statements that the email notifications were received by TMR and LYB, are sufficient proof that it has indeed notified the affected data subjects of the incident.

Moreover, the email notifications dated 29 November 2018 provided detailed information relating to the breach.<sup>9</sup> Leapfroggr explained that in its usual export process, its “system schedules the export and when it can start automatically converting [sic] patient profiles to Word documents.”<sup>10</sup> When the process is done, a zip file protected by a password, is created and a message will be generated which is sent to the “messenger inside the SeriousMD application.”<sup>11</sup>

Further, Leapfroggr explained that the generated message “should have been an automated message but [it] manually sent the generated message instead.”<sup>12</sup>

In addition, Leapfroggr stated that in addressing the breach, the erroneous message and the exported file were deleted immediately,<sup>13</sup> the export process was changed,<sup>14</sup> and the manual sending of files was disabled, changing the process to automated sending.<sup>15</sup>

The Commission reminds the personal information controllers (PICs) like Leapfroggr, and personal information processors (PIPs) of their obligation under the Data Privacy Act of 2012 (DPA). Under the DPA, notification to the affected data subjects is required especially in breach cases that involves sensitive personal information or other information that may be used to enable identity fraud and are reasonably believed to have been acquired by an unauthorized person, which may likely give rise to a real risk of

---

5 National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18(D) (15 December 2016) (NPC Circular 16-03).

6 In re: Leapfroggr, Inc., NPC BN 18-229, Order dated 10 November 2022, at p. 3

7 *Id.*, at p. 4

8 Affidavits dated 21 December 2022 of LYB and TMR.

9 *Id.*

10 *Id.*

11 *Id.*

12 Affidavits dated 21 December 2022 of LYB and TMR.

13 *Id.*

14 *Id.*

15 *Id.*

serious harm to the affected data subjects.<sup>16</sup>

**WHEREFORE**, premises considered, this Commission resolves that the matter of NPC BN 18-229 “In re: Leapfroggr, Inc.” is hereby considered **CLOSED**.

**SO ORDERED.**

City of Pasay, Philippines.  
19 January 2023.

**Sgd.**

**JOHN HENRY D. NAGA**

Privacy Commissioner

WE CONCUR:

**Sgd.**

**LEANDRO ANGELO Y. AGUIRRE**

Deputy Privacy Commissioner

**Sgd.**

**NERISSA N. DE JESUS**

Deputy Privacy Commissioner

Copy furnished:

**SS**

*Data Protection Officer*

**BDC**

*Head of the Organization*

**COMPLAINTS AND INVESTIGATION DIVISION**

**ENFORCEMENT DIVISION**

**GENERAL RECORDS UNIT**

National Privacy Commission

---

<sup>16</sup> An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter V, § 20 (f) (2012).

X-----X

## **RESOLUTION**

### **AGUIRRE, D.P.C.;**

Before the Commission is the breach notification submitted by Cardinal Health International Philippines, Inc.'s (CHI Philippines) involving the disclosure of the home phone numbers of its employees to the Cardinal Health Inc. (Cardinal Health) group of companies as a result of a system glitch.<sup>1</sup>

### **Facts**

Cardinal Health, the parent company of CHI Philippines, is responsible for managing the information security system of its international conglomerates, which includes CHI Philippines.<sup>2</sup> It also manages its directory services where its employees' information is stored.<sup>3</sup>

On 21 October 2018, Cardinal Health retired its single-sign on system and transitioned its directory service protocol from Lightweight Directory Access Protocol (LDAP) to Active Directory (AD).<sup>4</sup> To migrate information from LDAP to AD, one must export the contents of the LDAP from the current environment, configure the directory server to use AD, and finally, import the exported file.<sup>5</sup>

During the process, Cardinal Health reported system errors.<sup>6</sup> The employees' home phone numbers stored in Workday, Cardinal Health's human resource management system, became available on Skype, Outlook, and global address book of the Cardinal Health group of companies.<sup>7</sup>

On 22 October 2018, two of its employees notified Cardinal Health that their home phone numbers were visible on Skype.<sup>8</sup>

On 26 October 2018, Cardinal Health identified that one thousand four hundred sixty-five (1,465) employees of CHI Philippines were affected by the incident.<sup>9</sup>

On 27 October 2018, Cardinal Health notified the National Privacy Commission of the breach.<sup>10</sup> On the same day, it notified CHI Philippines' employees by email.<sup>11</sup>

1 Notification to the Commission, 27 October 2018, at 3, in In re: Cardinal Health International Philippines Inc., NPC BN 18-200 (NPC 2018).

2 Id.

3 Id.

4 Id.

5 How to Migrate from LDAP to Active Directory, available at <https://www.ibm.com/support/pages/how-migrate-ldap-active-directory> (last accessed 31 January 2023).

6 Notification to the Commission, 27 October 2018, at 3, in In re: Cardinal Health International Philippines Inc., NPC BN 18-200 (NPC 2018).

7 Id.

8 Id.

9 Id.

10 Id. at 1.

11 Id. at 5.

As a subsequent measure to address the incident, Cardinal Health declared that it took immediate steps by removing the script that triggered the internal disclosure of employees' home phone numbers.<sup>12</sup>It averred that it "implemented an internal communications protocol requiring coordination between its Identity Management (IDM) and Human Resource (HR) Data Compliance Departments when personal data will be processed to transferred to ensure [that] risks of inadvertent disclosures are identified, and safeguards against potential inadvertent disclosures are put in place."<sup>13</sup> Cardinal Health also maintains that it will require its IT Team to undergo further training to ensure observance of data protection compliance protocols and take the necessary disciplinary actions against the IT Team.<sup>14</sup>

Cardinal Health specified that the exposure is only limited to the employees' home phone numbers.<sup>15</sup>It also maintained that neither sensitive personal information nor information that may be used to enable identity fraud were involved in the incident.<sup>16</sup>It assured that employees' private phone numbers are no longer visible to the best of its knowledge.<sup>17</sup>

### **Issue**

Whether the matter requires mandatory breach notification.

### **Discussion**

The Commission finds that this matter does not fall under mandatory breach notification. Thus, the Commission resolves to close the matter.

Section 11 of NPC Circular 16-03 (Personal Data Breach Management) provides:

Section 11. *When notification is required.* Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.

For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

B. There is reason to believe that the information may have been acquired by an unauthorized person; and

---

<sup>12</sup> Notification to the Commission, 27 October 2018, at 3, in In re: Cardinal Health International Philippines Inc., NPC BN 18-200 (NPC 2018).

<sup>13</sup> *Id.*

<sup>14</sup> *Id.* at 4

<sup>15</sup> *Id.*

<sup>16</sup> *Id.* at 3.

<sup>17</sup> *Id.* at 2.



C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.<sup>18</sup>

Given this, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or other information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.<sup>19</sup>

For the first requisite the personal data involved is the employees' phone numbers.<sup>20</sup> This, however, cannot be considered as sensitive personal information.<sup>21</sup> Section 3 (I) of the Data Privacy Act of 2012 defines sensitive personal information as:

Section 3. *Definition of Terms.*

...

(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.<sup>22</sup>

A data subject's home phone number clearly does not fall within the definition of sensitive personal information. Also, given the circumstances, the data subjects' home phone number, by itself, cannot be considered as information that may be used to enable identity fraud.

<sup>18</sup> National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §11 (15 December 2016).

<sup>19</sup> In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, available at <https://www.privacy.gov.ph/wp-content/uploads/2023/01/NPC-SS-22-001-and-NPC-SS-22008-2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf> (last accessed 31 January 2023).

<sup>20</sup> Notification to the Commission, 27 October 2018, at 4, in In re: Cardinal Health International Philippines Inc., NPC BN 18-200 (NPC 2018).

<sup>21</sup> Id.

<sup>22</sup> 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 (I) (2012).

For the second requisite, this matter involves a confidentiality breach where the employees' home phone numbers became temporarily visible to the entire organization. Because of this, the information could have been acquired by an unauthorized person. Thus, the second requisite is present.

The third requisite that the unauthorized acquisition is likely to give rise to a real risk of serious harm is not present in this case. Taking note of the nature and quantity of the personal data involved and the limited exposure within the confines of the organization, there is neither serious harm to the affected data subjects nor reason to believe that the employees' home phone numbers may have been likely resulted in a real risk to the data subjects.

Considering that the first and third requisites for mandatory breach notification are absent in this case, the Commission finds that the breach pertaining to employees' home phone numbers among the Cardinal Health group of companies does not require mandatory breach notification to the Commission.

Nevertheless, even if the incident is not subject to mandatory notification, Cardinal Health has fulfilled its obligations as a Personal Information Controller by taking immediate precautionary measures to minimize any possible harm or negative consequences to its data subjects.

**WHEREFORE**, premises considered, this Commission resolves that the matter of NPC BN 18-200 In re: Cardinal Health International Philippines Inc. is hereby **CLOSED**.

**SO ORDERED.**

Pasay City, Philippines.  
19 January 2023.

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

**Sgd.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**Sgd.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

Copy furnished:

**JAS**

*Data Protection Officer*

**Cardinal Health International Philippines, Inc.,**

**COMPLAINTS AND INVESTIGATION DIVISION**

**ENFORCEMENT DIVISION**

**GENERAL RECORDS UNIT**

National Privacy Commission

X-----X

**RESOLUTION**

**AGUIRRE, D.P.C.;**

Before the Commission is the breach notification submitted by IRemit, Inc. (I-Remit) involving the disclosure of personal information of its employees to the entire company.

**Facts**

On 21 June 2018, a member of I-Remit’s Human Resources (HR) department accidentally emailed an attachment containing I-Remit’s employees’ personal information to the whole organization.<sup>1</sup> The HR staff intended to send the e-mail only to the members of the HR team.<sup>2</sup>

The personal information involved the employees’ Tax Identification Number (TIN), Social Security System (SSS), and Pag-IBIG number.<sup>3</sup> It also included their emergency contact number, educational background, birthday, address, civil status, and work experience.<sup>4</sup>

Upon realizing the mistake, the HR member immediately clicked the “RECALL” button on Microsoft Outlook, which cancelled the sending of the email.<sup>5</sup>

On the same day, I-Remit’s Data Protection Officer (DPO) held an emergency meeting with the Information Technology (IT) Team.<sup>6</sup> The IT Team reported that all computers have been cleared of any copies of the attachment.<sup>7</sup>

Two advisories relating to the incident were immediately sent to the employees of I-Remit.<sup>8</sup> The first advisory was from their DPO with instructions to immediately delete the email should they receive a copy.<sup>9</sup> The DPO emphasized that failure to comply with the advisory will result in severe disciplinary action and possible criminal liability.<sup>10</sup> The HR Head sent the second advisory reminding the employees to acknowledge and comply with the DPO’s prior advisory or face disciplinary action.<sup>11</sup>

On 4 July 2018, I-Remit notified the Commission of the breach.<sup>12</sup> IRemit submitted an Incident Report stating that one hundred fiftythree (153) out of one hundred eighty-six

---

1 Notification to the Commission, 04 July 2018, at 2, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).  
2 *Id.*  
3 *Id.*  
4 *Id.*  
5 *Id.*  
6 Report, 23 October 2020, at 2, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).  
7 Notification to the Commission, 04 July 2018, at 2, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).  
8 Report, 23 October 2020, at 4, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).  
9 *Id.* Annex B.  
10 *Id.*  
11 *Id.* Annex B-1  
12 Notification to the Commission, 04 July 2018, at 2, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018)

(186) supposed recipients received the email.<sup>13</sup>

On 08 October 2020, the Complaints and Investigation Division (CID) issued an Order requiring I-Remit to submit a Full Breach Report detailing the incident.<sup>14</sup>

On 23 October 2020, I-Remit submitted its Full Breach Report in compliance with the CID's Order.<sup>15</sup>

On 18 January 2022, the CID directed I-Remit to submit a Post-Breach Report detailing the incident that prompted the notification to the Commission. I-Remit was required by the Commission to provide the following:

1. An enumeration of the personal information involved in the attachments (e.g. name, address, cellphone no. etc.);
2. Documentation and proof of the remedial and security measures taken in response to the privacy incident, including the recall and/or deletion of the said mail;
3. Documentation and proof that no further processing was made by the actual recipients of the email;
4. Outcome of the breach management, and the difficulties encountered, if any, as well as the compliance with the notification requirements as to the affected data subjects, and the assistance provided, if any;
5. Documentation/Reports as to the security measures taken before, during, and after the security incident, and the remedial measures taken to prevent its recurrence.<sup>16</sup>

In Compliance with the 18 January 2022 Order, I-Remit sent an email to the CID on 31 January 2022 reiterating the contents of their Full Breach Report dated 23 October 2020.<sup>17</sup>

On 04 February 2022, I-Remit re-sent a copy of the Full Breach Report it submitted on 23 October 2020.<sup>18</sup>

Based on the CID's assessment dated 12 October 2022, I-Remit implemented reasonable and appropriate measures to address the incident.<sup>19</sup>

### **Issue**

Whether I-Remit conducted proper breach management, including the implementation of reasonable and appropriate security measures pursuant to NPC Circular 16-03 (Personal Data Breach Management).

### **Discussion**

I-Remit enumerated in its submissions the measures it took to address the breach following Section 17 (D) (3) of NPC Circular 16-03:

---

13 *Id.*  
14 Order, 08 October 2020, at 1, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).  
15 Report, 23 October 2020, at 2, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).  
16 Order To Submit Post-Breach Report, 18 January 2022, at 1, in In re: I-Remit, Inc., NPC BN 18115 (NPC 2018).  
17 Report, 31 January 2022, at 1, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).  
18 Compliance, 04 February 2022 at 1, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).  
19 Final Breach Notification Evaluation Report, 12 October 2022, at 6, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).

Section 17. *Notification of the Commission.* The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:

...

D. Content of Notification. The notification shall include, but not be limited to:

...

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.<sup>20</sup>

I-Remit narrated that, as an immediate measure, its DPO held an emergency meeting with their IT team to immediately and manually inspect all computers to “ensure that no copies (of the e-mail) were made.”<sup>21</sup>I-Remit also maintained that its IT Team checked all computers and deleted copies of the email, including those from “Junk and Recycle Bin” to ensure that no copies of the email and its attachment were kept or downloaded by unintended recipients.<sup>22</sup> IRemit also emphasized that because of the urgent action of “hitting the recall button” by its HR employee, the IT Team reported that the email could not be opened anymore and that some of the employees could not open the e-mail to begin with.<sup>23</sup>I-Remit also provided proof and documentation that no further processing was made by the actual recipients of the email by attaching a screenshot of the e-mail sent by its Information Security Officer.<sup>24</sup>Employees were likewise required to acknowledge if they have complied with the instructions.<sup>25</sup>

Its HR department and DPO also immediately sent advisories to the employees to delete the email should they receive a copy. The advisory from HR emphasized that “failure to follow such directive will result in severe disciplinary action and possible criminal liability.”<sup>26</sup>

In its efforts to prevent a recurrence of the breach, I-Remit also implemented physical, organizational, and technical security measures.<sup>27</sup>

As a physical measure, I-Remit explained that in order to minimize possible harm or negative consequences and to limit damage or distress to those affected by the

20 National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §17 (D)(3) (15 December 2016).

21 Report, 23 October 2020, at 3, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).

22 *Id.*

23 Report, 23 October 2020, at 3, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).

24 *Id.* Annex B-1.

25 *Id.* Annex E.

26 *Id.* Annex B.

27 *Id.* at 4

incident, it reinforced its “Data Privacy Manual” which it already had in place prior to the incident.<sup>28</sup>A copy of the Data Privacy Manual was attached to I-Remit’s PostBreach Report.<sup>29</sup>

As an organizational measure, I-Remit conducts regular training of its employees on personal data security and privacy awareness.<sup>30</sup>Further, I-Remit reported that advisories and infographics on information security with topics such as “juice jacking” or “phishing e-mails” and data privacy awareness materials are regularly sent to its employees by email.<sup>31</sup>

I-Remit also emphasized that it implemented the following relevant policies in support of its objective to avoid personal breaches, namely: “(i) Email Policy, (ii) Systems Usage Policy & Information Security Guidelines, and (iii) the Employee Hand Book (with Confidentiality Provisions).”<sup>32</sup>These policies are reviewed regularly and updated when necessary.<sup>33</sup>

I-Remit launched a data safety campaign entitled “Think Before You Click” to ensure that such technical accidents will not happen again.<sup>34</sup>

As a technical measure, I-Remit issued an advisory among its employees when sending emails and attachments.<sup>35</sup>I-Remit introduced encryption and password protection and provided instructions when sending files among the organization through Microsoft Word, Excel, and PowerPoint.<sup>36</sup>In the same instructional email, I-Remit emphasized to “(a) use strong passwords, (b) always confirm the identity of the recipient before releasing the passwords, (c) never send out passwords in the same e-mail as the protected files/s, and (d) inform recipients of passwords either in a separate email, face to face or by telephone.”<sup>37</sup>I-Remit also emphasized that after inserting the proper attachments, one must be extra careful that the messages should not go to the wrong recipients.<sup>38</sup>

Based on the foregoing, the measures that I-Remit took after the incident enabled it to strengthen its security measures in compliance with the DPA and the Commission’s issuances. Therefore, pursuant to NPC Circular 16-03, the actions taken by I-Remit are sufficient in closing the case.<sup>39</sup>

As a Personal Information Controller (PIC), I-Remit is reminded of its obligation to continuously update its security measures and ensure that it will be in a position to safeguard the personal and sensitive personal information of its data subjects.

---

28 *Id.* at 2.

29 Report, 23 October 2020, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018), Annex A.

30 *Id.* at 4.

31 *Id.* Annex F and H.

32 Report, 23 October 2020, at 4, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).

33 *Id.*

34 *Id.* at 3.

35 *Id.* Annex C.

36 *Id.*

37 *Id.*

38 Report, 23 October 2020, at 4, in In re: I-Remit, Inc., NPC BN 18-115 (NPC 2018).

39 National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule VI, § 25 (2016).

**WHEREFORE**, premises considered, this Commission resolves that the matter of NPC BN 18-115 In re: I-Remit, Inc. is **CLOSED**.

**SO ORDERED.**

City of Pasay, Philippines.  
26 January 2023.

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

**Sgd.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**Sgd.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

Copy furnished:

**DLA**  
*Information Security Officer/Data Protection Officer*  
**I-Remit, Inc.**

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission



X-----X

RESOLUTION

AGUIRRE, D.P.C.;

Before the Commission is a confidentiality breach involving the misdelivery of a Variable Unit Linked (VUL) Statement of Account (SOA) belonging to a Manufacturers Life Insurance Co. (Manulife) client.

Facts

On 13 November 2018, a Manulife agent emailed its Customer Care to report that his client, VL, received a VUL SOA by mail.<sup>1</sup> The VUL SOA, however, belonged to another Manulife client, LTE.<sup>2</sup>

Manulife sent an Incident Notification dated 30 November 2018 to the National Privacy Commission (NPC). Manulife explained that it learned of the incident on 14 November 2018.<sup>3</sup> The VUL SOA contained the following information: “1) Name of client; 2) Address; 3) Policy number; 4) Name of insured; and 5) Account summary (face amount, units bought/sold, premium amount, balances, charges/fees, current value, payments, etc.).”<sup>4</sup>

Manulife also reported that it discovered that “LTE’s outdated mailing address resulting [sic] to the same being delivered to her old address now being occupied by VL.”<sup>5</sup>

As a result, Manulife immediately requested VL to surrender or return the misdelivered VUL SOA to her agent.<sup>6</sup> Manulife also asked its Information Services (IS) Team to immediately conduct an investigation of the incident.<sup>7</sup>

Manulife’s IS Team initially reported to management that “[t]he old address supplied by the client, which address had already been previously updated, was erroneously tagged as the client’s current mailing address”<sup>8</sup> and that “only VUL SOAs were affected.”<sup>9</sup>

As its measures to address the breach, Manulife reported that the IS Team implemented fixes to ensure the system generating the VUL SOAs would use the correct and updated addresses of its clients.<sup>10</sup> In the meantime, Manulife stated that “no VUL SOAs were

1 Full Report, 21 October 2020, at 1, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).  
2 Incident Notification, 30 November 2018, at 1, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).  
3 Id.  
4 Id.  
5 Id.  
6 Id.  
7 Id.  
8 Incident Notification, 30 November 2018, at 1, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).  
9 Id.  
10 Id.

generated and sent out.”<sup>11</sup> The fixes were reported to have been completely implemented on 16 November 2018.<sup>12</sup> Manulife did not affirm whether VL fulfilled its request to surrender or to destroy the VUL SOA.

Manulife maintained that “[d]espite the information contained in the VUL SOA,” it had appropriate measures in place to minimize the risk of harm or fraud that may arise from the misdelivery.<sup>13</sup> It argued:

Should a person call the Company’s hotline, minimum validation procedures are in place to verify the identity of the client. These validation questions pertain to information that cannot be found in the VUL SOA. For other transactions involving the client’s policy, specific forms have to be filled out and identification documents need to be submitted. In light of the validation requirements in place that sufficiently protect the client from identity theft and fraud, or some other serious harm, it is respectfully asserted that Manulife Philippines is not required to notify the affected client. Nevertheless, rest assured that the Company will make the necessary notification if further investigation reveals that the same is warranted.<sup>14</sup>

On 06 October 2020, the NPC, through its Complaints and Investigation Division (CID), issued an Order directing Manulife to submit its Full Report within fifteen (15) days from receipt.<sup>15</sup> With respect to Manulife’s Incident Notification dated 30 November 2018, the CID concluded that “the notification did not provide the process conducted to notify the affected data subject.”<sup>16</sup> The CID also found that the Incident Notification did not “offer assistance that may be required to mitigate any possible damage that may be caused by the incident.”<sup>17</sup>

On 21 October 2020, Manulife submitted its full report in compliance with the CID’s Order. It reiterated its narration in the Incident Notification dated 30 November 2018, with additional details as to security measures it had taken since the breach occurred.<sup>18</sup> Manulife also submitted a copy of its Data Privacy Manual.<sup>19</sup>

On 14 November 2018, or the day after the breach, the IS Team investigated the VUL SOA generation.<sup>20</sup> It confirmed that LTE’s old mailing address, which was now VL’s current address, was erroneously tagged as LTE’s current mailing address in the Client Administration System (CAS).<sup>21</sup> According to Manulife, the IS Team reported that the CAS “fetched the first address recorded in a policy record instead of the most current one.”<sup>22</sup> The IS Team concluded that this error resulted from a system patch done at the end of October 2018.<sup>23</sup> The issue was then escalated to Manulife’s Data Protection Officer.<sup>24</sup>

After an investigation by its Operations team and IS team, Manulife reported that it dis-

---

11 *Id.*  
12 *Id.*  
13 *Id.*  
14 Incident Notification, 30 November 2018, at 1-2, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).  
15 Order, 06 October 2020, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).  
16 *Id.* at 1.  
17 *Id.*  
18 Full Report, 21 October 2020, at 1, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).  
19 *Id.*  
20 *Id.* at 1-2.  
21 *Id.* at 1.  
22 *Id.* at 1-2.  
23 *Id.*  
24 Full Report, 21 October 2020, at 2, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).

covered the erroneous tagging similarly affected a total of one hundred (100) printed VUL SOAs.<sup>25</sup> Nonetheless, Manulife reported that it was able to stop its courier from sending eighty-nine (89) of the printed VUL SOAs.<sup>26</sup> Manulife explained that:

Out of the 11 delivered VUL SOAs:

- 8 were actually received by the correct clients;
- 1 had the correct address;
- 1 was sent to the client's office address where he was still connected at that time;
- 1 pertained to a client who was outside of the Philippines. This client was contacted by a Manulife agent and did not pose any complaint or issue regarding his non-receipt of the SOA.<sup>27</sup>

As such, Manulife concluded that other than LTE, no other clients were impacted by the incident.<sup>28</sup>

According to Manulife, the personal data of LTE involved and disclosed to VL were: "a) Name of affected client as Policy Owner and Insured; b) Address, old address of affected client which was now the address of the unintended recipient; c) Policy number of affected client; and d) Account summary (face amount, units bought/sold, premium amount, balances, charges/fees, current value, payments)."<sup>29</sup> Nonetheless, Manulife argued that the personal data involved is insufficient for VL to access LTE's Manulife account.<sup>30</sup> Further, Manulife argued that VL remained unaware of LTE's current address.<sup>31</sup>

Manulife also explained why "there is a low likelihood of any adverse impact on the data subject":<sup>32</sup>

a) It is highly unlikely that the data received by the sole unintended recipient, the very same person who reported the incident to her Manulife agent, would be used for identity theft or other nefarious purposes by the recipient.

b) It should also be noted that validation procedures are in place to verify the identity of a client who calls or communicates with the Company. These validation questions pertain to information that cannot be found in the VUL SOA that was sent to the unauthorized recipient. This means that the information the unauthorized recipient got from the VUL SOA would not be sufficient for her to conduct transactions on the policy belonging to the other client.

c) Further, for major transactions involving a client's policy (such as change of address or beneficiary, surrender of policy, policy loans), specific forms have to be filled out and signed by the client, and valid identification documents have to be submitted.<sup>33</sup>

Manulife also reported taking "safeguards to minimize harm or mitigate impact of the breach."<sup>34</sup> It explained that it stopped sending VUL SOAs immediately upon learning

25 *Id.*

26 *Id.* at 1-2.

27 *Id.* at 2.

28 *Id.*

29 *Id.* at 3.

30 Full Report, 21 October 2020, at 3, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).

31 *Id.*

32 *Id.* at 2.

33 *Id.*

34 *Id.* at 3.

of the error and “until the system issue was identified and fixed.”<sup>35</sup> It also stated that it checked LTE’s policy for possible suspicious transactions<sup>36</sup> and that “[t]o date, there has been no red flag for any account takeover or fraud on the data subject’s account.”<sup>37</sup>

Manulife stated that once the issue with its CAS was resolved, it performed a qualitative check and an audit on the VUL SOAs sent out for the next thirty (30) days, “to ensure that the correct information were being picked up in the SOAs” prior to being sent out to clients.<sup>38</sup> Manulife also reported adding “enhancements to the software development lifecycle” to avoid recurrence of the incident.<sup>39</sup> It also stated that “mandatory testing and Quality Assurance were made compulsory prior to the release of any SOA.”<sup>40</sup> According to Manulife, “[a]s far as practicable, taking into consideration the inherent and residual risks, all system enhancements involving clients’ data have undergone the necessary testing and signoffs before they were implemented.”<sup>41</sup>

On remedial measures to address the breach, Manulife reiterated that it advised VL to either return the VUL SOA to Manulife or to destroy it.<sup>42</sup> Similar to its Incident Notification,<sup>43</sup> however, Manulife did not confirm whether VL returned or destroyed the VUL SOA.

Manulife also reported engaging the services of a third-party service provider, KPMG, to “conduct an evaluation of existing processes, systems and controls that impact data privacy.”<sup>44</sup> Manulife explained that this third-party independent evaluation was “supposed to have been done at the early part of [2020] but was delayed due to the current COVID-19 situation.”<sup>45</sup>

Given the foregoing measures, Manulife argued that the incident “has almost no adverse impact on the Company and the public at large.”<sup>46</sup> Manulife maintained that “[i]f at all, the incident led the Company to improve its existing systems and processes to better protect its clients’ information.”<sup>47</sup> Manulife also noted that “to date, it has not received any complaint arising from mis-directed [sic] VUL SOAs.”<sup>48</sup>

Finally, Manulife requested exemption from the notification of the affected data subject.<sup>49</sup> It reasoned:

In determining whether there was a need to notify the data subject of the incident, the primary consideration was the likelihood of harm or negative consequence caused by the misdelivered VUL SOA.

In light of the validation requirements in place that sufficiently protect the client from identity theft and fraud, or some other serious harm, it is respectfully request-

---

35 *Id.*  
36 Full Report, 21 October 2020, at 3, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).  
37 *Id.*  
38 *Id.*  
39 *Id.*  
40 *Id.*  
41 *Id.*  
42 Full Report, 21 October 2020, at 1-2, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).  
43 Incident Notification, 30 November 2018, at 1, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).  
44 Full Report, 21 October 2020, at 3, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).  
45 *Id.*  
46 *Id.* at 2.  
47 *Id.*  
48 *Id.*  
49 *Id.* at 4.

ed that pursuant to Section 19, Rule V of the National Privacy Commission Circular 16-03 on Personal Data Breach Management, the Company be exempted from Notification Requirements. This request is bolstered by the fact that despite the lapse of two years from the incident, there was in fact no suspicious transaction on data subject's account.<sup>50</sup>

On 09 December 2022, the CID assessed that the matter does not fall within mandatory notification under NPC Circular 16-03 (Personal Data Breach Management):

It must be remembered that Manulife specified that they have a validation procedure in place to verify the identity of a client who calls or communicates with their Company. These validation questions pertain to information which cannot be found in the SOA sent to the unintended recipient. But it may not be easily possible since confirmation for such change and account log-in are required.

Although there is reason to believe that the information may have been acquired by unauthorized individuals, we determine **that the limited personal data affected by the subject breach cannot be used to enable identity fraud** to claim any benefits arising from the insurance contract. **Also, when the unintended recipient immediately reported the mixed-up to Manulife, the recipient's action negated any risk which may arise from the incident caused by a system patch.** Thus, the likelihood of giving rise to real risk of serious harm to the affected data subjects is very low, if not, negligible.

Thus, with only two (2) out of three elements for a mandatory breach notification present in this case, it is hereby determined that notification, in this case, is not required.<sup>51</sup>

The CID stated that the incident was addressed, and that Manulife satisfactorily complied with the Order.<sup>52</sup> It concluded that the matter does not fall under mandatory breach notification as provided in NPC Circular 16-03,<sup>53</sup> and as such, Manulife was not required to notify its affected data subject.<sup>54</sup>

### Issue

Whether Manulife sufficiently addressed the breach incident and implemented security measures to prevent its recurrence.

### Discussion

The Commission resolves to close the matter. The incident does not fall under mandatory breach notification under Section 11 of NPC Circular 16-03. Only the first two requisites are present in this case. The third requisite of real risk of serious harm is absent because of prior and subsequent security measures implemented by Manulife.

Section 11 of NPC Circular 16-03 provides:

---

50 Full Report, 21 October 2020, at 4, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).  
51 Final Breach Notification Evaluation Report, 09 December 2022, at 6, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).  
52 *Id.* at 8.  
53 *Id.*  
54 *Id.*

Section 11. *When notification is required.* Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.

A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, “other information” shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

B. There is reason to believe that the information may have been acquired by an unauthorized person; and

C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.<sup>55</sup>

Following this, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.<sup>56</sup>

The first requisite is present. The nature of the information involved may enable identity fraud.

In this case, the information on the VUL SOA is considered “information about the financial or economic situation of the data subject” under Section 11 (A) of NPC Circular 16-03.<sup>57</sup> It contains specific information on LTE’s life insurance policy, namely “Account summary (face amount, units bought/sold, premium amount, balances, charges/fees, current value, payments)”<sup>58</sup>

Further, the information on the VUL SOA is considered information “which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits” under Section 11 (A).<sup>59</sup> The VUL SOA includes a Manulife client’s name, address, policy number, and name of insured,<sup>60</sup> which are necessary considerations for Manulife’s decision to grant insurance claims and release of proceeds, if any.

Other similar information referred to in the last sentence of Section 11(A) of NPC

<sup>55</sup> National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).

<sup>56</sup> In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and other John Does and Jane Does Initiated as a Sua Sponte NPC Investigation on Possible Data Privacy Violations Committed in Relation to the Alleged Hack and Breach of the Commission on Elections System or Servers, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available* at <https://www.privacy.gov.ph/wp-content/uploads/2023/01/NPC-SS-22-001-and-NPC-SS-22008-2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf> (last accessed 31 January 2023).

<sup>57</sup> NPC Circ. No. 16-03, § 11 (A).

<sup>58</sup> Full Report, 21 October 2020, at 3, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).

<sup>59</sup> NPC Circ. No. 16-03, § 11 (A).

<sup>60</sup> 0 Incident Notification, 30 November 2018, at 1, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).

Circular 16-03 need not necessarily be personal information.<sup>61</sup> For mandatory breach notification, Section 20 (f) of Republic Act No. 10173 or the Data Privacy Act (DPA) only requires that the information may enable identity fraud:

Section 20. *Security of Personal Information.*

...

(f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or **other information that may, under the circumstances, be used to enable identity fraud** are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.<sup>62</sup>

Further, Section 11 (A) of NPC Circular 16-03 itself includes the phrase “shall include, but not be limited to,” which means the enumeration is not an exclusive list:

Section 11. When notification is required. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.

A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, **“other information” shall include, but not be limited to:** data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.<sup>63</sup>

In other words, “other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits” does not necessarily refer to personal information, so long as the information may enable identity fraud.<sup>64</sup>

In this case, the name of the insured, and policy number are important—if not the most important—details with respect to a life insurance policy. The outdated address on the VUL SOA provides even more specific details that may be used to assume the policy holder’s identity.

Given the foregoing, and the fact that VL did not surrender or provide confirmation of the destruction of the VUL SOA, unauthorized acquisition of the information on the VUL

61 NPC Circ. No. 16-03, § 11 (A).

62 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 (f) (2012). Emphasis supplied.

63 NPC Circ. No. 16-03, § 11. Emphasis supplied.

64 *Id.* § 11 (A).

SOA may be used to fraudulently assume the identity of the policy holder LTE.

The second requisite is also present. An unauthorized person acquired the information in LTE's VUL SOA.

The Commission held that a loss of control over personal data held in custody is enough for a Personal Information Controller (PIC) to have "reason to believe that the information may have been acquired by an unauthorized person."<sup>65</sup>

In this case, Manulife categorically stated in its Incident Report<sup>66</sup> and Full Breach Report<sup>67</sup> that VL received the VUL SOA. It even stated that VL was advised either to return it or destroy it.<sup>68</sup> Hence, Manulife admitted and confirmed that there was loss of control by the PIC and the acquisition of the affected data subjects' personal data by an unauthorized person.

Nonetheless, the third requisite is not present due to the security measures implemented by Manulife.

The Commission takes this opportunity to discuss the determination of the presence of the third requisite of mandatory breach notification. Section 11 (C) of NPC Circular 16-03 provides:

Section 11. When notification is required. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.

...

C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.<sup>69</sup>

For this purpose, the phrase "likely to give rise to a real risk" in Section 11 (C) means that a link exists between the breach and the possible resulting harm to any affected data subject.<sup>70</sup> The risk must be apparent and not the product of mere speculation.<sup>71</sup> "Serious harm" means that the consequences and effects to any affected data subject is significant based on the surrounding circumstances of the breach.<sup>72</sup>

In determining whether the unauthorized acquisition is likely to give rise to real risk of serious harm, a PIC or the Commission may consider several factors, such as: the nature and amount of information involved in the breach, the period of time that has lapsed since the breach, objective of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of the information.

65 NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).  
66 Incident Notification, 30 November 2018, at 1, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).  
67 Full Report, 21 October 2020, at 1, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).  
68 Incident Notification, 30 November 2018, at 1, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).  
69 NPC Circ. No. 16-03, § 11.  
70 NPC BN 17-028 and NPC BN 18-180, 11 May 2023, at 8 (NPC 2023) (unreported).  
71 *Id.*  
72 *Id.*



In this case, the unauthorized acquisition of information was due to the erroneous delivery to VL.<sup>73</sup> There is no showing that she deliberately intended to obtain LTE's information, as she reported the misdelivery to her agent, who in turn reported the issue to Manulife.<sup>74</sup> Thus, the objective of the unauthorized acquisition was not for fraudulent purposes.

Nonetheless, the nature and amount of information involved in this matter may enable identity fraud. The name of the policy holder, name of the insured, and policy number are important, if not the most important, details with respect to claims on an insurance policy, and the other information such as address and account summary provides even more specific details. Despite Manulife's request to VL, it did not affirm in any of its submissions that VL actually surrendered or confirmed the destruction of LTE's VUL SOA.

Given the foregoing circumstances, including the possibility of fraudulent actions or claims in relation to LTE's insurance policy, there was a real risk of serious harm to the data subject in this case. Manulife itself admitted this risk when it stated that "the appropriate measures in place to minimize the risk of identity theft or fraud that may arise from the misdelivered VUL SOA."<sup>75</sup>

The security measures implemented by Manulife, however, prevented the occurrence of the risk of serious harm to the affected data subject.

Manulife was able to substantiate its claim of "low likelihood of any adverse impact on the data subject"<sup>76</sup> due to the validation measures that it had in place. Manulife stated that "for major transactions involving a client's policy (such as change of address or beneficiary, surrender of policy, policy loans), specific forms have to be filled out and signed."<sup>77</sup> Thus, any person intending to conduct a transaction as to an insurance policy must also submit valid identification documents, in addition to the validation questions, to Manulife.<sup>78</sup>

Manulife also reported continuously monitoring the generation of VUL SOAs.<sup>79</sup> As of 21 October 2020, when Manulife filed its Full Breach Report, it stated that it had continuously monitored LTE's policy for possible suspicious transactions, and that "there has been no red flag for any account takeover or fraud on the data subject's account."<sup>80</sup>

Manulife also flagged the erroneous tagging that similarly affected a total of one hundred (100) printed VUL SOAs.<sup>81</sup> It was able to stop its courier from sending eighty-nine (89) VUL SOAs, and to monitor and resolve the delivery of the remaining eleven (11).<sup>82</sup> In fact, Manulife explained in its Full Report that:

Out of the 11 delivered VUL SOAs:

---

73 Incident Notification, 30 November 2018, at 1, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).

74 *Id.*

75 Full Report, 21 October 2020, at 3, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).

76 *Id.* at 2.

77 *Id.*

78 *Id.*

79 *Id.* at 3.

80 *Id.*

81 Full Report, 21 October 2020, at 2, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).

82 *Id.* at 1-2.

- 8 were actually received by the correct clients;
- 1 had the correct address;
- 1 was sent to the client's office address where he was still connected at that time;
- 1 pertained to a client who was outside of the Philippines. This client was contacted by a Manulife agent and did not pose any complaint or issue regarding his non-receipt of the SOA.<sup>83</sup>

Manulife also reported halting the generation of VUL SOAs altogether while its IS Team implemented fixes for the issue of erroneous tagging of addresses.<sup>84</sup>

To reiterate, the security measures implemented by Manulife—the requirement of answering validation questions and submitting identification documents for any changes or major transactions on a client's insurance policy, halting the generation and delivery of VUL SOAs until the client address tagging issue was fixed, and constant monitoring until 21 October 2020—were sufficient to protect LTE from fraudulent transactions resulting from the disclosure of her information. This removed the real risk of serious harm to the affected data subject.

Given the foregoing, the Commission finds that Manulife was able to address the breach and implement security measures to prevent real risk of serious harm from occurring. As such, the matter does not fall under mandatory breach notification.

**WHEREFORE**, premises considered, this Commission resolves that the matter of NPC BN 18-213 In re: Manufacturers Life Insurance Co. is **CLOSED**.

**SO ORDERED.**

City of Pasay, Philippines.  
29 June 2023.

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

**Sgd.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**Sgd.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

---

<sup>83</sup> Full Report, 21 October 2020, at 2, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).  
<sup>84</sup> Incident Notification, 30 November 2018, at 1, in In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).

Copy furnished:

**JJN**

*Assistant Vice President,  
Head of Risk Management &  
Data Protection Officer*

**Manufacturers Life Insurance Co.**

**COMPLAINTS AND INVESTIGATION DIVISION**

**ENFORCEMENT DIVISION**

**GENERAL RECORDS UNIT**

National Privacy Commission

**IN RE: AIG SHARED SERVICES - BUSINESS PROCESSING INC. AND AIG SHARED SERVICES CORPORATION – MANAGEMENT SERVICES (ROHQ)**

**NPC BN 18-033**

X-----X

**NPC BN 18-076**

**IN RE: MEDICARD PHILIPPINES, INC. - FESTIVAL ALABANG CLINIC**

X-----X

**RESOLUTION**

**AGUIRRE, D.P.C.;**

Before the Commission is the consolidated breach notifications submitted by AIG Shared Services Corporation – Management Services (ROHQ) (AIGSS-MS) by AIG Shared Services – Business Processing Inc. (AIGSS-BPI) (collectively, AIGSS) and by Medicaid Philippines, Inc. - Festival Alabang Clinic (Medicaid).

**Facts**

On 12 March 2018, AIGSS-MS notified the National Privacy Commission (NPC) of a breach:

In accordance with RA. 10173, “Data Privacy Act of the Philippines”, this is to notify the Commission of a recent personal data breach that happened in our organization. Unfortunately, **sensitive personal information of one (1) employee was inadvertently sent to unintended recipients by our medical service provider [i.e. Annual Physical Exam (APE) results were sent to all affected data subjects instead of sending it individually].** The full report of the personal data breach will be sent separately. We will also send the acknowledged notification letter by the data subject to you as soon as we receive it.<sup>1</sup>

It attached a Privacy Risk Incident Report (Report) stating that the following personal data of its employees were involved: full name, employee ID, and medical information.<sup>2</sup>AIGSS-MS explained that “human error” was the “principal root cause,” and that Medicaid was also a responsible party.<sup>3</sup> It stated that the potential harm that may result from the incident was “emotional distress” and “reputational damage.”<sup>4</sup> AIGSS-MS reported that it informed the affected data subjects and obtained confirmation from the recipients that the email was deleted and not reproduced.<sup>5</sup> Finally, it reported that it already informed Medicaid and was waiting for its response on the matter.<sup>6</sup>

On 14 March 2018, AIGSS-BPI also notified the NPC of the breach.<sup>7</sup>

1 Personal Data Breach Notification from AIG Shared Services Corporation - Management Services (ROHQ), 12 March 2018, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018). Emphasis supplied.

2 *Id.*

3 *Id.*

4 *Id.*

5 *Id.*

6 *Id.*

7 Personal Data Breach Notification from AIG Shared Services Corporation - Business Processing Inc., 14 March 2018, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Ser-

On 23 May 2018, Medicaid submitted its breach notification, stating:

1. Nature of the Breach/Incident: Unintended disclosure of Annual Physical Exam (APE) Results
  - a. Appointment Officer voluntarily performed the duty of Records Technician to send APE Results of 6 data subjects the neglecting protocol last March 9, 2018.
  - b. The unencrypted APE Results were sent to unintended recipients within AIG.
2. Personal Data Possibly Involved: APE Results
3. Remedial Measures to Address the Breach/Incident:
  - a. Deletion of all copies of the email containing unencrypted APE Results.
  - b. Disciplinary action for the Appointment Officer.
  - c. Reorientation of all clinic personnel of existing security measures.
  - d. Segregation of duties and limit number of clinic personnel who sends APE Results.
  - e. Company-wide Data Privacy and Information Security Awareness Program.

Kindly see attachments for the details.<sup>8</sup>

Medicaid submitted two email threads to its notification: the first involved the email thread of the breach itself,<sup>9</sup> and the second involved AIGSS and Medicaid's correspondence after the breach.<sup>10</sup> AIGSS initiated the correspondence to inform Medicaid of the breach.<sup>11</sup> It stated that it was expecting Medicaid to perform all measures "to protect [AIGSS'] employees' sensitive personal information."<sup>12</sup> AIGSS also requested an explanation from Medicaid, its next steps in addressing the breach, and its assistance in ensuring the email is deleted.<sup>13</sup> Finally, Medicaid submitted an email apology sent by Medicaid's Alabang Officer to AIGSS.<sup>14</sup>

On the notification of the affected data subjects, Medicaid explained:

We did not perform immediate breach notification because we considered the incident as low/minimal risk and would not cause harm to the 6 data subjects because the recipients of the APE Results were all within AIG. MediCard is committed to complying with RA 10173. We would like to ensure that we are complying with the breach notification requirements even though AIG claimed that they have already reported the breach/incident to the Commission.<sup>15</sup>

On 07 August 2018, the NPC, through the Complaints and Investigation Division (CID), directed AIGSS to submit its Full Report within five (5) days from receipt.<sup>16</sup>

On 21 September 2018, AIGSS requested an additional period of seven (7) days, or until

---

vices (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).  
8 Personal Data Breach Notification from Medicaid Philippines, Inc., 23 May 2018, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018). Emphasis supplied.

9 *Id.*

10 *Id.*

11 *Id.*

12 *Id.*

13 *Id.*

14 Personal Data Breach Notification from Medicaid Philippines, Inc., 23 May 2018, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc., NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

15 *Id.*

16 Memorandum, 07 August 2018, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

28 September 2018, to submit the Full Report.<sup>17</sup> It explained that it needed additional time because of “[t]he volume and nature of the information that it needs to review, as well as AIGSS’s desire to provide [the Commission] a Full Report that is both comprehensive and in full compliance with the Memorandum.”<sup>18</sup>

On 28 September 2018, AIGSS submitted its Full Report in compliance with the Memorandum dated 07 August 2018.<sup>19</sup>

AIGSS explained that between 11 February 2018 and 02 March 2018, the Annual Physical Exam (APE) of six (6) AIGSS employees was conducted in the Medicaid Festival Alabang Clinic.<sup>20</sup> On 09 March 2018, AIGSS’ Human Resources Employee (HR employee) requested scanned copies of the APE results of the six (6) employees from the Medicaid Alabang Officer to comply with the Occupational Health Permit requirements due on the same day.<sup>21</sup>

The HR employee asked the Medicaid Alabang Officer to send the APE results to the Medicaid Nurse based in the AIGSS iHub Clinic (iHub Medicaid Nurse).<sup>22</sup> In turn, the HR employee instructed the iHub Medicaid Nurse to “encrypt and password protect each APE result before sending it individually” to the six (6) employees.<sup>23</sup> The Medicaid Alabang Officer, however, sent all the APE results to four (4) out of the six (6) employees, instead of the iHub Medicaid Nurse.<sup>24</sup> Further, it was sent without following “the agreed process for handling APE results.”<sup>25</sup>

AIGSS stated that on 10 March 2018, one (1) of the four (4) recipient employees reported the incident to the AIGSS Privacy Team.<sup>26</sup> The Privacy Team then initiated a review of the incident and implemented “remediation measures to contain the breach.”<sup>27</sup>

The affected data subjects were five (5) employees of AIGSS–BPI and one (1) employee of AIGSS–MS.<sup>28</sup> The following personal information were affected: “(1) Full Employee Name, 2) Employee ID Number, 3) Age, 4) [Civil] Status, and 5) Medical Information.”<sup>29</sup> AIGSS maintained, however, that other than the AIG Employee ID “there were no other personal information compromised which could enable identity theft.”<sup>30</sup>

On measures to address the breach, AIGSS reported that within seventy-two (72) hours, it obtained email confirmation from the four (4) recipients that “the email had been

---

17 Request for extension, 21 September 2018, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

18 *Id.*

19 Full Report, 28 September 2018, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

20 *Id.* at 1.

21 *Id.*

22 *Id.*

23 *Id.*

24 *Id.* at 2

25 Full Report, 28 September 2018, at 2, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

26 *Id.*

27 *Id.*

28 *Id.*

29 *Id.* at 3.

30 *Id.*

deleted and was not retained or used by them.”<sup>31</sup>

On the notification of the affected data subjects, AIGSS reported that it sent an email to the six (6) affected employees to notify them of the incident.<sup>32</sup> AIGSS explained that this was “because they were AIGSS employees at the time the incident occurred.”<sup>33</sup>

AIGSS also reported sending an email to Medicaid on 13 March 2018 “informing them about the incident and demanding for an explanation on why the agreed process for distributing APE results was not followed.”<sup>34</sup> AIGSS asked for Medicaid’s remedial measures to ensure the incident does not occur again.<sup>35</sup> On 15 March 2018, AIGSS reported that Medicaid responded and advised AIGSS that it had taken the following remedial measures: refresher training for all Medicaid staff, implementation of more stringent protocols to safeguard its clients’ sensitive personal information, and reduction or limitation of the number of staff that can access clients’ sensitive personal information.<sup>36</sup>

On 13 January 2021, the CID issued an Order to Medicaid, directing it to submit a Full Report on the breach notification dated 23 May 2018.<sup>37</sup>

On 02 February 2021, Medicaid submitted its compliance with the Order dated 13 January 2021:

On March 9, 2018, 6:42am, AIG-HR staff Ms. AMB emailed Ms. JL2[sic] (Appointment Officer) of MediCard-Festival Alabang Clinic to send the APE results of 6 employees before 12nn on the same day. From the same email, she then instructed 2 other AIG Personnel (CRN and ihub nurse) to send the said APE results to the 6 employees. At 11:39am of the same day, Ms. JL of MediCard Festival Clinic sent the APE results. However, she included the 6 employees on the said email neglecting the instructions given by Ms. AMB.

On March 10, 2018, 1:18am, upon receiving Ms[.] JL’s email, Ms[.] AMB of AIG replied that the APE results were sent to [ ] unintended recipients and that she [was] clear of her instructions that she only authorized CRN and ihub nurse to send the results to their owners and not her.

Ms. JL sent her apologies to Ms. AMB following the incident (email dated March 10, 9:22am) and explained that she thought it was allowed to send the results to the employees since they need to submit it as part of the requirement for their health permit. She also voluntarily performed the duty of a Records Technician to send the APE results due to the urgency of the request.<sup>38</sup>

Medicaid also submitted the following documents with its compliance: a screenshot of Clause 7 from Medicaid and AIGSS’ contract;<sup>39</sup> an email to AIGSS providing a

---

31 Full Report, 28 September 2018, at 3, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

32 *Id.* at 5.

33 *Id.*

34 *Id.* at 3.

35 *Id.*

36 *Id.* at 4.

37 Order, 13 January 2021, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

38 Full Report, 02 February 2021, at 2-3, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

39 *Id.*

narration of the breach and the countermeasures it implemented;<sup>40</sup> and a copy of the email thread where AIGSS requested its employees to delete the email.<sup>41</sup>

As proof of the security measures it implemented, Medicaid also submitted the following documents: a memorandum from Medicaid’s Clinic Services Department addressed to all personnel, reminding them of minimum requirements in handling personal and sensitive personal information;<sup>42</sup> a Notice of Disciplinary Action to the Medicaid Alabang Officer imposing a ten-day suspension;<sup>43</sup> screenshots of Medicaid’s internal information campaign on procedures to protect personal information;<sup>44</sup> a memorandum requiring attendance of Medicaid employees, contractuals, and consultants to a data privacy and information security awareness training;<sup>45</sup> a memorandum requiring the encryption of digitally processed personal information within Medicaid’s system; and a memorandum announcing the implementation of security features of “Sophos Email Appliance (email gateway)” starting 01 October 2018.<sup>46</sup>

On 26 February 2021, the CID sent another Order to AIGSS, directing it to submit a Full Report on the breach notification in 2018.<sup>47</sup>

On 11 March 2021, AIGSS filed a Motion for Extension to submit its compliance with the Order dated 26 February 2021.<sup>48</sup> It explained:

The current deadline you have provided to us to respond to the Order falls on Monday, 15 March 2021 (given that 13 and 14 March fall on the weekend). However, as the matter that is the subject of the Order occurred sometime ago (the matter occurred three years ago and our last correspondence with your good office was in September of 2018), we require further time to collate the information surrounding this matter.

In the circumstances, we are humbly requesting your good office for an extension of time **until 29 March 2021** to respond to your Order.<sup>49</sup>

On 29 March 2021, AIGSS submitted its compliance with the Order dated 26 February 2021.<sup>50</sup> At the outset, AIGSS argued that any investigations by the NPC should be directed at Medicaid, who was the PIC of the affected data subjects.<sup>51</sup> It noted that the description of the Order dated 26 February 2021 stated the NPC was investigating

---

40 *Id.*  
41 *Id.*  
42 *Id.*  
43 *Id.*  
44 Full Report, 02 February 2021, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).  
45 *Id.*  
46 *Id.*  
47 Order, 26 February 2021, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).  
48 Motion for Extension, 11 March 2021, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines – Festival Alabang Clinic, Inc., NPC BN 18-033 and NPC BN 18-076 (NPC 2021).  
49 *Id.* at 1.  
50 Compliance, 29 March 2021, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).  
51 *Id.* at 1.



“Possible Data Privacy Violations Committed by [AIGSS-BPI] and [AIGSS-MS].”<sup>52</sup> AIGSS explained:

We believe that any investigations which your good office wishes to conduct in this matter should not be directed at either AIGSSBPI or AIGSS-MS as we were not the Personal Information Controllers of the personal information found in the results of the annual physical examinations (“APE”). We have explained below that Medicaid Philippines, Inc. (“Medicaid”) was the Personal Information Controller of the APE results. You may, therefore, wish to contact Medicaid directly (if not already done) should you have any queries regarding this matter as they will be in the best position to provide you with the relevant information relating to this matter.<sup>53</sup>

AIGSS then explained that “Medicaid is a licensed healthcare provider and Health Maintenance Organization which offers Corporate Health Programs.”<sup>54</sup> AIGSS – MS and AIGSS-BPI participated in Medicaid’s Corporate Health Program “for the purposes of offering employees medical benefits.”<sup>55</sup> As part of these medical benefits, employees were entitled to an annual physical examination.<sup>56</sup> According to AIGSS, “six (6) employees (5 from AIGSS-BPI and 1 from AIGSS-MS) attended one of Medicaid’s own free-standing clinics, the Medicaid Alabang Clinic, at Festival Supermall, Alabang, Muntinlupa City between February 11 and March 2, 2018 for their annual physical examinations.”<sup>57</sup>

AIGSS then proceeded to discuss the breach, substantially reiterating its narration in the Personal Data Breach Notification.<sup>58</sup> It added that “[t]he APE results were also not meant to be sent directly to the AIG Shared Services Human Resources officer.”<sup>59</sup> It clarified that “Medicaid ought to have instead sent an email to each of the 6 employees individually, attaching only the APE results of the employee to whom each of the emails was addressed.”<sup>60</sup>

AIGSS also reiterated its position that Medicaid is the PIC.<sup>61</sup> It stated that the notification to the Commission on 12 and 14 March 2018 was made only “as a courtesy and out of an abundance of caution on behalf of [AIGSS’] employees.”<sup>62</sup> It explained:

5. [T]he purposes for which Medicaid collects, uses, discloses and/or processes the personal information found in the results of APEs as well as the methods used by Medicaid in collecting, using, disclosing and processing the said personal informa

tion is entirely in the control of Medicaid. Medicaid provides the APE results directly to the employees and not to either AIGSS-BPI or AIGSS-MS. In the circumstances, Medicaid was the Personal Information Controller in respect of the personal information found in the APE results and was obliged to protect such personal information from, amongst other things, accidental disclosure.

---

52 *Id.*

53 *Id.*

54 *Id.*

55 *Id.*

56 Compliance, 29 March 2021, at 1-2, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

57 *Id.* at 2

58 *Id.* at 1-2.

59 *Id.* at 2

60 *Id.*

61 *Id.* at 1.

62 Compliance, 29 March 2021, at 2, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

7. As AIGSS-BPI and AIGSS-MS were aware of the matter, we informed your good office about the matter through our emails of March 12 and 14, 2018 as a courtesy and out of an abundance of caution on behalf of our employees. For the avoidance of doubt, any obligation to notify your good office of this matter pursuant to the Data Privacy Act of 2012 (“Privacy Act”) falls on Medicaid as the Personal Information Controller which disclosed the APE results of the 6 employees and not AIGSS-BPI nor AIGSS-MS.<sup>63</sup>

### **Issue**

Whether AIGSS and Medicaid were able to sufficiently address the breach and to implement security measures to prevent its recurrence.

### **Discussion**

The Commission resolves to close the matter. The incident does not fall under mandatory breach notification under Section 11 of NPC Circular 16-03 (Personal Data Breach Notification). Only the first two requisites are present in this case. The third requisite of real risk of serious harm is absent because of the security measures that AIGSS implemented.

Section 11 of NPC Circular 16-03 provides:

Section 11. When notification is required. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.

- A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, “other information” shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords, and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
- B. There is reason to believe that the information may have been acquired by an unauthorized person; and
- C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.<sup>64</sup>

Following this, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.<sup>65</sup>

<sup>63</sup> *Id.*

<sup>64</sup> National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], §11 (15 December 2016).

<sup>65</sup> In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, available at <https://privacy.gov.ph/wp-content/up>

The first requisite is present. The information involved is sensitive personal information and other information that may enable identity fraud.

The information inadvertently emailed by the Medicaid Alabang Officer includes the employees' age, civil status, and medical information,<sup>66</sup> and Medicaid ID number.<sup>67</sup> These are considered sensitive personal information under Section 3 (I) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).<sup>68</sup>

Further, the information involved may enable identity fraud, since it may be "made the basis of decisions concerning the data subject, including the grant of rights or benefits."<sup>69</sup> AIGSS stated that "Medicaid is a licensed healthcare provider and Health Maintenance Organization which offers Corporate Health Programs."<sup>70</sup> AIGSS-MS and AIGSS-BPI participated in Medicaid's Corporate Health Program "for the purposes of offering employees medical benefits."<sup>71</sup> This, taken together with the fact that the information compromised included employee information and Medicaid ID number, may enable identity fraud for the purpose of claiming medical benefits.

Medicaid also submitted a screenshot of Clause 7 from Medicaid and AIGSS' Agreement, which provides:

**7. AUTHORITY TO EXAMINE MEDICAL RECORDS.** The COMPANY hereby represents and warrants that, at the time of the **effectivity of this Agreement and effectivity of coverage of each MEMBER and his dependents**, it has obtained from the MEMBER and his dependents the required consents authorizing MediCard and any of its authorized representatives to: (a) obtain, examine and process the MEMBER'S personal information, including the medical records of their hospitalization, consultation, treatment or any other medical advice in connection with the **benefit/claim availed under this Agreement**; and (b) disclose such information to the COMPANY and its representatives[.]<sup>72</sup>

The use of "dependents" and "benefit/claim" in Clause 7 shows that, apart from providing medical examinations for Occupational Health Permit requirements, the Agreement between Medicaid and AIGSS includes Medicaid health insurance coverage for AIGSS employees and their dependents.<sup>73</sup> The name, age, and civil status of the employee, taken together with their employee ID number, are necessary considerations for Medicaid's decision to grant medical benefits or claims of AIGSS' employees.

Given the foregoing, unauthorized acquisition of the personal data and APE results may be used to fraudulently assume the identity of an AIGSS employee covered by Medi-

[loads/2023/05/NPC-SS-22-001-and-NPC-SS-22-0082022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf](#) (last accessed 02 August 2023).

<sup>66</sup> Full Report, 28 September 2018, at 3, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

<sup>67</sup> *Id.* at 3.

<sup>68</sup> See An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (I) (2012).

<sup>69</sup> NPC Circ. No. 16-03, § 11 (A).

<sup>70</sup> Compliance, 29 March 2021, at 1, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

<sup>71</sup> *Id.* at 1.

<sup>72</sup> Full Report, 02 February 2021, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

<sup>73</sup> *Id.*

card's Corporate Health Program.

The second requisite is also present. Unauthorized persons acquired the personal data and APE results in the emailed Excel file.<sup>74</sup> The Commission held that a loss of control over personal data held in custody is enough for a PIC to have “reason to believe that the information may have been acquired by an unauthorized person.”<sup>75</sup>

AIGSS admitted that the Medicaid Alabang Officer sent all the APE results in a single email to four (4) out of the six (6) employees, instead of the iHub Medicaid Nurse.<sup>76</sup> Medicaid reiterated this in its breach notification dated 23 May 2018<sup>77</sup> and in its compliance dated 02 February 2021.<sup>78</sup> Hence, both AIGSS and Medicaid admitted that the PIC lost control and unauthorized persons acquired the personal data of the data subjects.

Further, the HR employee instructed the iHub Medicaid Nurse, and not the Medicaid Alabang Officer, to “encrypt and password protect each APE result before sending it individually” to the six (6) employees.<sup>79</sup> The Medicaid Alabang Officer, however, voluntarily undertook to send the APE results without following “the agreed process for handling APE results.”<sup>80</sup>

Finally, AIGSS submitted a copy of the email from the employee who reported the breach.<sup>81</sup> The employee reported that their x-ray result file was incorrectly placed in another person's APE file, which shows that the recipients were able to open and view the contents of the APE results.<sup>82</sup>

The lack of security measures enabled the viewing of such personal information by the four (4) AIGSS employees, which should be sufficient to form a reasonable belief for the PIC.<sup>83</sup> Nonetheless, the third requisite is not present due to the security measures that AIGSS implemented after the breach.

The Commission takes this opportunity to discuss the factors considered in determining the presence of the third requisite of mandatory breach notification. Section 11 (C) of NPC Circular 16-03 provides:

Section 11. **When notification is required.** Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.

74 *Id.* at 2-3.

75 NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).

76 Full Report, 28 September 2018, at 2, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc., NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

77 Personal Data Breach Notification from Medicaid Philippines, Inc., 23 May 2018, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc., NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

78 Full Report, 02 February 2021, at 2-3, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

79 Full Report, 28 September 2018, at 1, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

80 *Id.* at 2

81 Compliance, 29 March 2021, Annex 3, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

82 *Id.*

83 NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).

C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.<sup>84</sup>

For this purpose, the phrase “likely to give rise to a real risk” in Section 11 (C) means that a link exists between the breach and the possible resulting harm to any affected data subject.<sup>85</sup> The risk must be apparent and not the product of mere speculation.<sup>86</sup> Serious harm means that the consequences and effects to any affected data subject is significant based on the surrounding circumstances of the breach.<sup>87</sup>

In determining whether the unauthorized acquisition is likely to give rise to real risk of serious harm, a PIC or the Commission may consider several factors, such as: the nature and amount of information involved in the breach, the period of time that has lapsed since the breach, objective of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of the information.

In this case, the unauthorized acquisition of information was due to the inadvertent transmittal of all the APE results to the four (4) AIGSS employees.<sup>88</sup> There is no showing that the AIGSS employees deliberately intended to obtain the information of other employees, as one of the four (4) recipient employees even reported the incident to the AIGSS Privacy Team.<sup>89</sup> The erroneous transmittal stemmed from the Medicaid Alabang Officer’s misunderstanding of the directive to send the results to the iHub Medicaid Nurse,<sup>90</sup> as shown in the Medicaid Alabang Officer’s explanation in the breach’s email thread.<sup>91</sup>

Thus, the objective of the unauthorized acquisition was not for fraudulent purposes.

It must be emphasized that the nature and amount of information involved in the breach—name, employee ID number, age, civil status, and medical information—are important details with respect to availing the medical benefits under Medicaid’s Corporate Health Program.<sup>92</sup>

Nonetheless, the security measures implemented by AIGSS prevented the occurrence of the risk of serious harm to the affected data subjects.

84 NPC Circ. No. 16-03, § 11.

85 NPC BN 17-028 and NPC BN 18-180, 11 May 2023, at 8 (NPC 2023) (unreported).

86 *Id.*

87 *Id.*

88 Full Report, 28 September 2018, at 2, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

89 Compliance, 29 March 2021, Annex 3, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

90 Full Report, 28 September 2018, at 1, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

91 Personal Data Breach Notification from Medicaid Philippines, Inc., 23 May 2018, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

92 Compliance, 29 March 2021, at 1-2, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

AIGSS notified the affected data subjects.<sup>93</sup> After one (1) of the recipient employees reported the incident on 10 March 2018,<sup>94</sup> AIGSS' Privacy Team initiated a review of the incident on the same date and implemented "remediation measures to contain the breach."<sup>95</sup> Thereafter, AIGSS reported that within seventy-two (72) hours it obtained email confirmation from the four (4) recipient employees that "the email had been deleted and was not retained or used by them."<sup>96</sup> Furthermore, AIGSS reported that it sent an email to all six (6) affected employees to notify them of the incident.<sup>97</sup> The notification states:

Dear [],

We very much regret to advise you that we recently became aware of an incident involving your sensitive personal data. In compliance with the Data Privacy Act (Republic Act 10173) and AIG Shared Services Data Privacy Reporting Procedure, we are informing you that your APE Results containing sensitive personal information were inadvertently sent by a Medicaid employee to unauthorized recipients last March 9, 2018.

You may get your own APE results in the attachment then delete all communications pertaining to the subject and its attachments. Please do not forward to any other users and refrain to reproduce it. Rest assured that we are coordinating and in communication with Medicaid to ensure that all measures are being taken to protect your sensitive personal information and ensure that this will not happen again. A request has been sent to unauthorized recipients to delete all communications pertaining to the subject and its attachments. We will also request Medicaid to do the same on the person who sent the email and a confirmation that it has been deleted.

You can reach out to me or to BP Jr. our Data Protection Officer for AIG Shared Services – Business Processing Inc. (email address at [ ] with contact number [ ] ; cell number [ ] ) for additional information regarding the breach, and for any support or clarification.

Lastly, please send us a confirmation that you have deleted the said email.

Thank you[.]<sup>98</sup>

As proof of notification, AIGSS submitted an email notification regarding the breach (sent on 12 March and 13 March 2018), and confirmation of deletion from the four (4) recipients.<sup>99</sup>

Section 18 (C) of NPC Circular 16-03 provides the required content of proper notification of affected data subjects:

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

93 *Id.* Annex 5-A to 5-D.

94 Full Report, 28 September 2018, at 2, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

95 *Id.*

96 *Id.* at 3.

97 *Id.* at 5.

98 Compliance, 29 March 2021, Annex 5-A to 5-D, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

99 *Id.*

procedures:

...

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.<sup>100</sup>

Further, Section 18 (D) of NPC Circular 16-03 provides the required form of proper notification:

Section 18. *Notification of Data Subjects.* The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:

...

D. *Form.* Notification of affected data subjects shall be done **individually, using secure means of communication, whether written or electronic.** The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and **to safeguard against further unnecessary disclosure of personal data.** The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the personal information controller shall establish **means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.**<sup>101</sup>

The notification sent to affected data subjects must contain sufficient information on the nature of the breach incident, the personal data involved, the measures taken by the PIC to address the breach and to reduce harm or negative consequences of the breach, and the assistance it extended to its affected data subjects.<sup>102</sup> Further, the form of notification must be individual and must be made through secure means of communication, whether written or electronic.<sup>103</sup> The PIC must provide the data subject with the means to exercise their rights and obtain more detailed information relating to the breach.<sup>104</sup>

In this case, the Commission finds that the email notification complied with the requirements under Section 18 (C) and Section 18 (D) of NPC Circular 16-03.<sup>105</sup> The email notification contained information on the nature of the breach incident, the personal data

100 NPC Circ. No. 16-03, § 18 (C).

101 *Id.* § 18 (D).

102 NPC BN 18-198, 23 September 2021, at 4 (NPC 2021) (unreported).

103 NPC BN 18-198, 23 September 2021, at 4 (NPC 2021) (unreported).

104 *Id.*

105 *Id.* § 18 (C) - (D).

involved, the measures taken by AIGSS to address the breach and to reduce harm or negative consequences of the breach, and a contact number that data subjects can use to obtain assistance and information.<sup>106</sup> Further, it was sent individually through email.<sup>107</sup> Thus, the notification enabled the affected data subjects to take measures to protect themselves from the consequences of the breach.

The Commission acknowledges the efforts of AIGSS to promptly notify the affected data subjects and implement security measures. In contrast, however, the Commission strongly reprimands Mediacard for its failure to take action and its mere reliance on the measures taken by AIGSS.

The Commission agrees with AIGSS that Mediacard is the PIC. As explained by AIGSS in its Compliance dated 29 March 2021:

5. The annual physical examinations of these 6 employees and any tests for the purposes of these examinations were carried out by Mediacard at its Alabang clinic by Mediacard’s doctors, nurses, and staff based on their professional knowledge, skill, and expertise. AIGSS-MS and AIGSS-BPI naturally ha no input into the conduct of such physical examinations. **The purposes for which Mediacard collects, uses, discloses, and/or processes the personal information found in the results of APEs as well as the methods used by Mediacard in collecting, using, disclosing, and processing the said personal information is entirely in the control of Mediacard. Mediacard provides the APE results directly to the employees and not to either AIGSS-BPI or AIGSS-MS.** In the circumstances, Mediacard was the Personal Information Controller in respect of the personal information found in the APE results and was obliged to protect such personal information from, amongst other things, accidental disclosure.<sup>108</sup>

Clause 7 of the Agreement between AIGSS and Mediacard<sup>109</sup> further confirms that Mediacard is the PIC:

[I]t is hereby agreed that it is the sole responsibility of the COMPANY to obtain from the MEMBERS the consent herein specified and that **MediCard shall have all the right to rely on the representation by the COMPANY that this consent shall have been duly and timely obtained.** The COMPANY shall hold MediCard free and harmless from and against any and all suits or claims, actions, or proceedings, damages, costs and expenses, including attorney’s fees, which may be filed, charged or adjudged against MediCard or any of its directors, stockholders, officers, employees, agents, or representatives in connection with or arising from the **use by MediCard of the MEMBER’S medical records and other personal information pursuant to this Agreement and disclosure of such information to the COMPANY and its representatives pursuant to MediCard’s reliance on the COMPANY’S representation and warranty that MediCard has the authority to examine, use or disclose, as the case may be, said medical records or personal information.**<sup>110</sup>

While there is shared responsibility between AIGSS and Mediacard in that AIGSS was responsible for obtaining its employees’ consent for processing of their information,

106 NPC BN 18-198, 23 September 2021, at 4 (NPC 2021) (unreported).

107 NPC Circ. No. 16-03, § 18 (D).

108 Compliance, 29 March 2021, at 2, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Mediacard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021). Emphasis supplied.

109 Compliance, 29 March 2021, at 2, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Mediacard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021). Emphasis supplied.

110 *Id.* Emphasis supplied.



ultimately it is still Medicaid that processes their personal information to provide health insurance coverage. Moreover, it was Medicaid's own personnel that inadvertently sent the APE results to the four (4) AIGSS employees, neglecting the protocol of encryption and password protection.<sup>111</sup>

There is no showing, however, in any of Medicaid's submissions that it made efforts to notify its affected data subjects. It merely stated in its Full Report that it did not notify because it deemed the incident as "minimal/low risk."<sup>112</sup> It reasoned as follows:

**We did not perform immediate breach notification because we considered the incident as low/minimal risk and would not cause harm to the 6 data subjects because the recipients of the APE Results were all within AIG.** MediCard is committed to complying with RA 10173. We would like to ensure that we are complying with the breach notification requirements even though AIG claimed that they have already reported the breach/incident to the Commission.

MediCard was invited by Deputy Commissioner Ivy Patdu for a meeting last May 22, 2018 to discuss about Data Sharing Agreement and the AIG incident was brought up. We were advised by DepCom Patdu and Atty Mike to perform a breach notification and not to rely on AIG's notification to ensure that Medicaid performed its duty as PIC.<sup>113</sup>

The Commission finds that Medicaid's reasoning is not justified. If Medicaid was truly committed to complying with its obligations under the DPA, as it claims, it should have promptly notified both the NPC and the affected data subjects upon receipt of AIGSS' email informing it of the incident as early as 13 March 2018.<sup>114</sup> Instead, Medicaid sent a notification to the NPC only on 23 March 2018, fourteen (14) days after the breach.<sup>115</sup> Even worse, there is no showing that Medicaid made any effort to notify the data subjects.

The Commission sternly reminds Medicaid that although it was appropriate to implement security measures within its organization, such measures were prospective and insufficient to protect the affected data subjects from the risk they were already exposed to.<sup>116</sup> The purpose of notification is to provide data subjects with an opportunity to take the necessary precautions to protect their own data against the possible effects of the breach.<sup>117</sup> As such, PICs such as Medicaid are required to "establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach"<sup>118</sup>Data subject notification is an essential obligation of a PIC,<sup>119</sup> and Medicaid utterly failed to fulfill such obligation in this case.

**WHEREFORE**, premises considered, this Commission resolves that the matter of NPC

111 Full Report, 28 September 2018, at 1, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

112 Personal Data Breach Notification from Medicaid Philippines, Inc., 23 May 2018, in In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicaid Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018). Emphasis supplied.

113 *Id.* Emphasis supplied.

114 *Id.*

115 *Id.*

116 Resolution, NPC BN 20-149 In re: National Privacy Commission 20 August 2020, at 6 (NPC 2020) available at <https://www.privacy.gov.ph/wp-content/uploads/2022/01/Resolution-NPC-BN-20149-In-re-NPC.pdf> (last accessed 02 August 2023).

117 NPC Circ. No. 16-03, § 18 (D).

118 *Id.*

119 Order, NPC BN 21-035, 01 June 2021, at 4 (NPC 2021) (unreported).

BN 18-033 In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation – Management Services (ROHQ) (AIGSS), and NPC BN 18-076 In re: Medicaid Philippines, Inc. – Festival Alabang Clinic (Medicaid) is **CLOSED**.

The Commission **DIRECTS** the Compliance and Monitoring Division (CMD) to conduct a Compliance Check on the sufficiency of Medicaid’s security measures involved in the processing of personal data.

**SO ORDERED.**

City of Pasay, Philippines.  
02 August 2023

Sgd.  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

Sgd.  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

(on official leave)  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner

Copy furnished:

**SG**  
*Data Protection Officer*  
**AIG Shared Services – Business Processing, Inc.**  
**AIG Shared Services Corporation – Management Services (ROHQ)**

**RCM**  
*Data Protection Officer*  
**Medicaid Philippines, Inc.**

**COMPLAINTS AND INVESTIGATION DIVISION**  
**COMPLIANCE AND MONITORING DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission



# ORDER



*Complainant,*

-versus-

**ORANI WATER DISTRICT**  
*(formerly CDB and SRM),*

*Respondent.*

X-----X

**ORDER**

**AGUIRRE, D.P.C.;**

This Order refers to the compliance of Respondents with this Commission’s Decision<sup>1</sup> involving a Complaint<sup>2</sup> filed by CBP (Complainant) against CDB and SRM who were officers of the Orani Water District (OWD), for the alleged violations of R.A. 10173 (Data Privacy Act). Considering that they are no longer connected to OWD due to the latter’s change in management, SRM and CDB are dropped from the case which shall now continue to proceed with OWD as the Respondent.

**The Facts**

On 15 December 2017, this Commission issued a Decision with the following dispositive portion:

**WHEREFORE**, premises considered, **CDB** and **SRM** are **STERNLY WARNED** that repetition of the same or similar acts will be dealt with more severely. Respondents are hereby further ordered:

1. To coordinate with the head of agency of Orani Water District and submit to the National Privacy Commission the organization’s privacy notice and existing privacy policies pertaining to their employees within fifteen (15) days from receipt of this Decision; and
2. To submit to the National Privacy Commission proof of their attendance or participation in any orientation on the Data Privacy Act or similar events within sixty (60) days from receipt of this Decision.

On 25 January 2018, OWD filed a Compliance<sup>3</sup> with this Commission where it submitted: (1) the office memorandum<sup>4</sup> dated 18 May 2017 from BPA, OWD General Manager, requiring all employees to sign an Employee Non-Disclosure and Confidentiality Agreement; and (2) the signed Employee NonDisclosure and Confidentiality Agreements including those of Ms. Milante and Mr. Buenaventura.

---

1 Decision dated 15 December 2017.  
 2 Complaint Affidavit dated 25 November 2016.  
 3 Compliance with NPC Case No. 16-004 dated 25 January 2018.  
 4 Signing of Employee Non-Disclosure and Confidentiality Agreement dated 18 May 2017.

On 22 July 2019, this Commission, through its Enforcement Division (EnD), sent a letter<sup>5</sup> to SRM and CDB informing them that they have not submitted their organization's privacy notice and existing privacy policies pertaining to OWD's employees, and proof of attendance or participation in any orientation on the Data Privacy Act or similar events. They were also advised to immediately comply with the directives of the Commission En Banc in the Decision dated 15 December 2017 to avoid further liabilities under the law. However, SRM replied to inform the Commission that they are no longer connected with OWD due to a change in management.<sup>6</sup>

On 10 August 2020, the EnD sent a letter<sup>7</sup> to EFS, the new OWD General Manager, advising him to comply with the directives of the Commission En Banc in its Decision dated 15 December 2017 by submitting copies of the organization's privacy notice and existing privacy policies pertaining to its employees, as well as proof of attendance or participation of the employees in any orientation on the Data Privacy Act or similar events within thirty (30) days from receipt of said letter. with the DPO's prior advisory or face disciplinary action.

On 16 September 2020, EFS wrote a letter<sup>8</sup> to this Commission, through the Legal and Enforcement Office (LEO), informing it that there was a change of management within the OWD as a result of a Joint Venture Agreement (JVA). He also stated that there was no proper turn-over of documents by the previous management and that despite having exerted all efforts to locate any existing privacy notice and policies of OWD from the available files in the office, OWD cannot locate the same. Thus, OWD may not be able to submit the required documents. He also admitted that OWD's personnel and employees have not attended any orientation regarding data privacy as of the writing.

On 24 September 2020, the EnD sent another letter<sup>9</sup> to OWD emphasizing its obligation to comply with the orders of the Commission in a Decision dated 15 December 2017. It was also advised to go through this Commission's website to check various resources that could help create their privacy manual and privacy notices. OWD was also urged to comply and submit its compliance report within thirty (30) days from receipt of said letter to avoid further liabilities under the law.

On 16 October 2020, EFS wrote a letter<sup>10</sup> to EnD stating that OWD has started seeking and soliciting information from some of its fellow water districts for references that it can use to design its organization's privacy notice and privacy policies pertaining to their employees. Moreover, OWD has appointed a Data Protection Officer (DPO) as an immediate action to adhere to the legal requirements of the Data Privacy Act. Lastly, it has already checked the Commission's website and browsed over the page on the Creation of Privacy Manual.

---

5 Letter to Mr. CDB and SRM with the subject: Compliance with Decision date 15 December 2017 "CBP v. CDB and SRM" NPC Case No. 16-00. Dated 22 July 2019.

6 Fact-Finding Report dated 09 November 2020.

7 Letter to EFS, General Manger, through the Data Protection Officer with the subject: Compliance with Decision dated 15 December 2017 "CBP v. CDB and SRM" NPC Case No. 16-00. Dated 10 August 2020.

8 Letter to MTP Dated 16 September 2020.

9 Letter to EFS, General Manager with subject Compliance with Decision dated 15 December 2017 "CBP v. CDB and SRM" NPC Case No. 16-00. Dated 24 September 2020.

10 Letter to MTP, Dated 16 October 2020.

OWD states in its letter:

[W]e would like to respectfully appeal for your utmost consideration on our ongoing undertakings to fully comply with the directive set in the decision issued by the Commission En Banc.

xxx

W]e humbly request for your guidance and assistance through the conduct of trainings and capacity building activities for our personnel.<sup>11</sup>

### Discussion

Section 7 of the Data Privacy Act provides for the functions of the Commission, thus:

**(a) Ensure compliance of personal information controllers with the provisions of this Act;**

(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;

(c) 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;

**(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) Monitor the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to this Act;**

(f) Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country;

(g) Publish on a regular basis a guide to all laws relating to data protection;

(h) Publish a compilation of agency system of records and notices, including index and other finding aids;

(i) Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act;

**(j) Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers:** Provided, That the privacy codes shall adhere to the underlying data privacy principles embodied in this Act: Provided, further, That such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller. For this purpose, the Commission shall consult with relevant regulatory agencies in the formulation and administration of privacy codes applying the standards set out in this Act, with respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to the law: Provided, finally, That the Commission may review such privacy codes and

---

<sup>11</sup> *Ibid.*

require changes thereto for purposes of complying with this Act; xxx.<sup>12</sup>

This Commission ordered SRM and CDB to submit OWD's privacy notice and existing privacy policies, and proof of their attendance or participation in any orientation on the Data Privacy Act or similar events as early as 15 December 2017.<sup>13</sup> On 22 July 2019, a letter<sup>14</sup> was sent advising them to immediately comply with the directives of this Commission. On 10 August 2020, this Commission sent another letter<sup>15</sup> to EFS reiterating its directives for OWD. On 24 September 2020, this Commission again sent a letter<sup>16</sup> to Mr. Santos urging OWD to comply and submit their compliance report.

However, despite the Decision and the three (3) letters directing them to comply with the orders of this Commission, OWD has not fully complied to this date. Instead, it submitted documents which are not responsive to this Commission's directives, and explained that there was a change of management<sup>17</sup> and there was no proper turn-over of documents from the previous management.<sup>18</sup>

It is noteworthy that this Commission's Orders to OWD were made almost three (3) years ago. OWD has had more than enough time to comply with those directives. In fact, this Commission sent three (3) additional letters reiterating its previous orders. While this Commission acknowledges that there was a change in management, the new management should have conducted the proper due diligence when it entered into a JVA. OWD should have informed itself of the status of this case so that it could have required the proper turn-over of the necessary documents. Despite all these, the new management of OWD has also had more than enough time to comply with this Commission's Orders. Had the new management started their compliance efforts when EnD wrote to OWD on 22 July 2019<sup>19</sup> or even on 10 August 2020,<sup>20</sup> it could have already come up with the necessary assessments and documents for its privacy manual.

Be that as it may, taking into consideration the latest actions of OWD, it is given a final opportunity to comply with this Commission's directives.

**WHEREFORE**, premises considered, OWD is hereby ordered to **SUBMIT** the final draft of its Privacy Manual and Notices **within thirty (30) days** from receipt of this Order.

**SO ORDERED.**

Pasay City, Philippines  
19 November 2020.

**LEANDRO ANGELO Y. AGUIRRE**  
*Deputy Privacy Commissioner*

---

12      Emphasis supplied.  
13      Supra note 1.  
14      Supra note 5.  
15      Supra note 7.  
16      Supra note 9.  
17      Supra note 8.  
18      *Ibid.*  
19      Supra note 5.  
20      Supra note 7.

WE CONCUR:

**RAYMUND ENRIQUEZ LIBORO**  
*Privacy Commissioner*

**JOHN HENRY D. NAGA**  
*Deputy Privacy Commissioner*

**COPY FURNISHED:**

**CBP**

*Complainant*

**CDB**

**SRM**

*Former Respondents*  
Orani Water District

**EFS**

*General Manager*  
Orani Water District

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission



**MVC,**

*Complainant,*

**NPC 21-010**  
For: Violation of the Data  
Privacy Act of 2012

-versus-

**DSL,**

*Respondent.*

x-----x

**CBP,**

*Complainant,*

**NPC 21-011**  
For: Violation of the Data  
Privacy Act of 2012

-versus-

**DSL,**

*Respondent.*

x-----x

**NMB,**

*Complainant,*

**NPC 21-012**  
For: Violation of the Data  
Privacy Act of 2012

-versus-

**DSL,**

*Respondent.*

x-----x

**RMP,**

*Complainant,*

**NPC 21-013**  
For: Violation of the Data  
Privacy Act of 2012

-versus-

**DSL,**

*Respondent.*

x-----x

**NDL,**

*Complainant,*

**NPC 21-014**  
For: Violation of the Data  
Privacy Act of 2012

-versus-

**DSL,**

*Respondent.*

x-----x

**CBP,**

*Complainant,*

**NPC 21-015**  
For: Violation of the Data  
Privacy Act of 2012

-versus-

**DSL,**

*Respondent.*

x-----x

## ORDER

On 03 February 2022, the Commission issued a Decision finding DSL liable for Section 32 (Unauthorized Disclosure) of the Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).<sup>1</sup> Consequently, the Commission recommends to the Secretary of Justice the prosecution of DSL for the offense of Unauthorized Disclosure under Section 32 of the DPA.<sup>2</sup>

On 05 April 2022, DSL filed a Motion for Reconsideration to the Decision dated 03 February 2022.<sup>3</sup>

In his Motion, DSL argued that the Commission “inadvertently committed palpable error” in holding him liable for Section 32 of the DPA and in recommending for his prosecution.<sup>4</sup> He disagreed with the ruling of the Commission that the publication of the letter dated 23 November 2021 was a processing without lawful basis.<sup>5</sup> DSL claimed that the publication was necessary for compliance with a legal obligation of the GA Tower 1 Condominium Corporation (GAT1CC) in accordance with Section 12 (c) of the DPA.<sup>6</sup> He argued that the House Rules and Regulations of the GAT1CC authorizes the management to disclose the names of the delinquent members and unit owners.<sup>7</sup>

DSL further disagreed with the finding that the letter dated 23 November 2021 was not issued for the interest of GAT1CC.<sup>8</sup> He argued that the Complainants have the burden to prove by substantial evidence that DSL has no authority to issue the letter on behalf of the condominium corporation<sup>9</sup> and that his acts constitute unauthorized disclosure.<sup>10</sup> DSL further argued that the Commission has no jurisdiction over the subject matter of the case.<sup>11</sup> He claimed that since the parties involved are members and officers of the corporation, the case involves an intra-corporate controversy.<sup>12</sup> Hence, according to DSL, it is the Regional Trial Court that has jurisdiction over the case.<sup>13</sup>

DSL also alleged that the Complainants failed to attach a certification against forum shopping to their complaints.<sup>14</sup> According to him, the Complainants also failed to disclose the four (4) pending cases involving the same issues and circumstances as the case at hand.<sup>15</sup> He claimed that the non-compliance of the Complainants with the procedural requirements is “tainted with bad intentions” and is for their own convenience.<sup>16</sup> Considering the foregoing, DSL argued that the Commission should have outrightly dismissed the Complaints.<sup>17</sup>

In order to properly resolve the Motion for Reconsideration filed by Lee, the Commission deems it necessary to require the Complainants to submit their respective Comments on the Motion for Reconsideration.

**WHEREFORE**, premises considered, Complainants **MVC, RRB, NMB, RMP, NDL, and MBN** are hereby **ORDERED** to **COMMENT** on the Motion for Reconsideration filed by DSL **within fifteen**

1 NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015, 03 February 2022, at 13 (NPC 2022) (unreported).

2 *Id.* at 14.

3 Motion for Reconsideration, 05 April 2022, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).

4 *Id.* ¶ 5.

5 *Id.* ¶ 6.

6 *Id.*

7 *Id.* ¶ 8.

8 *Id.* ¶ 10.

9 Motion for Reconsideration, 05 April 2022, ¶ 11, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).

10 *Id.* ¶ 15.

11 *Id.* ¶ 23.

12 *Id.* ¶ 19.

13 *Id.* ¶ 22.

14 *Id.* ¶ 26.

15 Motion for Reconsideration, 05 April 2022, ¶ 28, in MVC, et al. v. DSL, NPC 21-010, NPC 21-011, NPC 21-012, NPC 21-013, NPC 21-014, NPC 21-015 (NPC 2022).

16 *Id.*

17 *Id.*

**(15) days** from the receipt of this Order.

**SO ORDERED.**

City of Pasay, Philippines.  
28 April 2022.

**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

**JOHN HENRY D. NAGA**  
Privacy Commissioner

**DUG CHRISTOPER B. MAH**  
Deputy Privacy Commissioner

Copy furnished:

**MVC**  
*Complainant*

**RRB**  
*Complainant*

**NMB**  
*Complainant*

**RMP**  
*Complainant*

**NDL**  
*Complainant*

**MBN**  
*Complainant*

**CBB**  
*Counsel for Respondent*

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

X-----X

**ORDER**

**AGUIRRE, D.P.C.;**

This Order refers to a breach notification report sent by ABS-CBN Corporation (ABS-CBN) regarding possible unauthorized access and acquisition of personal data of customers of its online store.

**The Facts**

On 18 September 2018, ZDNet published an article<sup>1</sup> entitled “Broadcaster ABS-CBN customer data stolen, sent to Russian servers.” According to the article, the payment skimmer, which intercepts the checkout process through an obfuscated malware hidden within a JavaScript file, has been in operation since 16 August of the same year. According to Dutch security researcher WDG, the malicious code scrapes the financial information of payment cards used by customers attempting to buy merchandise from the store. This information is then transferred to a payment collection server called *adaptivecss.org*, which is registered in Irkutsk, Russia.<sup>2</sup>

On 19 September 2018, the publication of the article was reported to ABS-CBN’s Data Protection Officer (DPO), Mr. Jay C. Gomez, who contacted the company’s Managed Security Service Provider (MSSP) - Symantec, to report the security incident and assist in the immediate investigation and containment procedures. Investigations conducted by the MSSP revealed that a file with a backdoor program was uploaded on ABS-CBN’s website that created a form and submitted the information to the attacker. A total of two-hundred eight (208) unique customers were affected by the breach. Based on the investigation of the MSSP, the malicious code collected the name, complete address (including the city, state, country and zip code), email address, phone number, shop, and credit card details (including credit card name, number, expiration date and CVV) of ABS-CBN’s online store customers. On the same day, ABS-CBN’s DPO sent a formal notification to the Commission.

On 21 September 2018, the MSSP reported that based on the available evidence, Symantec Incident Response can state with high confidence that the attack is consistent with the so-called Magecart<sup>3</sup> campaign. Further, ABS-CBN claimed that the data breach incident is limited only to the ABS-CBN Store website and does not affect other ABS-CBN digital properties.<sup>4</sup>

1 Charlie Osborne, Broadcaster ABS-CBN customer data stolen, sent to Russian servers, available at <https://www.zdnet.com/article/broadcasting-giant-abs-cbn-customer-data-stolen-sent-to-russian-servers/> (Last accessed: 07 January 2021, 10:49PM)

2 *Id.*

3 “Magecart, a threat group which has been active since 2015, specializes in compromising online stores and obfuscating malicious code in JavaScript in order to steal payment card information entered into store checkout pages.” Charlie Osborne, Broadcaster ABS-CBN customer data stolen, sent to Russian servers, available at <https://www.zdnet.com/article/broadcasting-giant-abs-cbn-customer-data-stolen-sent-to-russian-servers/> (Last accessed: 07 January 2021, 10:49PM)

4 Email Notice: Personal Data Breach Incident dated 19 September 2018.

ABS-CBN reportedly took the following measures to address the incident upon knowledge of the compromise:

1. The publication of the article was immediately reported by an IT staff to the ABS-CBN DPO;
2. ABS-CBN engaged its MSSP to assist in the investigation, containment procedures and remediation activities;
3. ABS-CBN also invoked its Incident Response Retainer from the same MSSP;
4. The compromised ABS-CBN online store was taken down on 19 September 2018 at 09:28AM;
5. Upon receipt of additional information from internal Security Analysts, ABS-CBN has also taken down the UAAP Store ([www.uaapstore.com](http://www.uaapstore.com)) as a precautionary measure;
6. An informal notification was sent via SMS by the ABS-CBN DPO to NPC Commissioner Raymond Liboro who acknowledged receipt thereof;
7. A Press Release was published by ABS-CBN Corporate Communications on the data breach;
8. The concerned personnel from IT, Retail and Infosec Head/DPO called for a meeting with the Third-Party Vendor to discuss technical details and remediation plans;
9. On 19 September 2018, the Head of Retail sent the list of affected customers to Head of iConn Operations (Customer Service) for email notification and callouts where two hundred two (202) affected data subjects were notified via email or contact number and six (6) customers were notified via postal mail;
10. ABS-CBN also advised the affected customers to immediately change their account passwords, inform their bank and credit card provider and follow their advice, refrain from providing personal and/or financial information to anyone claiming to be an ABS-CBN representative, and report to ABS-CBN if the aforementioned case was encountered;
11. On 20 September 2018, the MSSP found suspicious logins from one of the administrator accounts of the Third-Party Vendor, the Third-Party Vendor immediately reset administrator passwords and run virus scans on all personnel laptops.

To prevent the recurrence of the incident, ABS-CBN undertook the performance of the following measures:<sup>5</sup>

1. Magento Lockdown:
  - a. Restriction of access to all administrative interfaces to specific systems only;
  - b. Restriction of access to all administrative interfaces based on firewall policies;
  - c. Application of multi-factor authentication for all administrative accounts;
  - d. Removal of the Magento Connector Manager since this is a common target for malicious adversaries;
  - e. Conduct regular vulnerability scanning of the site in order to detect any potential weakness;

---

5 Full Breach Report dated 24 September 2018.

2. For auditing, apply the company’s log retention policies to services hosted by external providers;
3. Devise a backup strategy for the production website and store the backups in a safe location outside of an attacker’s influence; and
4. Notify law Enforcement to take down the infrastructure ‘adaptivecss.org’ since the malicious code is designed to post customer payment card information on the said site.<sup>6</sup>

On 27 September 2018, the Commission, through the Complaints and Investigations Division (CID), met with the ABS-CBN DPO where the Commission requested for a copy of the logs, decoded malware and the basic Magento scanner used by ABS-CBN in addressing the incident. ABS-CBN provided the needed logs and malware samples via email to the NPC.

On 11 October 2018, another meeting was held between the CID and the ABS-CBN representatives, where ABS-CBN was required to submit a supplemental update on ABS-CBN’s and its E-Commerce provider’s additional mitigation and remediation activities.

On 16 October 2018, a supplemental update was sent via email by the ABS-CBN DPO.<sup>7</sup>The update stated that the two-factor authentication for super administrators, as part of its role-based access controls,<sup>8</sup> and an additional IP Whitelisting enabled on production environment on its jump server,<sup>9</sup>were already completed. On E-Commerce hosting, ABS-CBN explained that they will migrate to Sonassi Hosting provider from Nexcess to include additional features such as separate servers for web app and database, web application firewall, extended off-site back-ups and server logs. According to ABS-CBN, the signing of proposal was set on 05 November 2018.

Moreover, ABS-CBN already completed the disabling of Magento Connect and Magento Security Scanning (staging server), while the scanning and remediation of web application server on staging environment prior to restoration and the work with specific business unit and finalization of data retention for its online stores were expected to be completed by 26 October 2018. The scanning of web application server on new production environment pending the migration to new server was set to be completed on 05 November 2018.<sup>10</sup>

On 05 November 2018, another email was sent by the ABS-CBN DPO regarding minor updates on ABS-CBN’s remediation activities. According to ABS-CBN, with regard to E-Commerce hosting, it has completed its migration to Sonassi Hosting provider from Nexcess on 29 October 2018 and that it has decided to host the web application server and Database in an Amazon Web Service (AWS) environment managed and monitored by ABS-CBN. The scanning and remediation of web application server on staging environment prior to restoration was completed on 26 October 2018. The scanning of web application server on new production environment ‘s completion was moved to

---

6 Upon access, the website shows an article entitled “Semalt Expert: Visual Content Tips”. Last accessed: 12:37AM, 08 January 2021.

7 Supplemental update dated 16 October 2018.

8 Role-based access control (RBAC) restricts network access based on a person’s role within an organization.

9 A jump server, jump host or jump box is a system on a network used to access and manage devices in a separate security zone.

10 Supplemental update dated 16 October 2018.

06 November 2018. ABS-CBN also informed this Commission of its target to go live for store website on 08 November 2018.

On 15 November 2018, ABS-CBN submitted their vulnerability scan report for the scenarios prior to restoration and after migration. In their submitted report, the number of vulnerabilities discovered on their web application after restoration and migration were reduced from sixty-one (61) to thirty-one (31). Moreover, of the thirty-one (31) vulnerabilities detected after migration, twenty-nine (29) of these vulnerabilities, which were classified as high risk by the scan, were found to be false positives<sup>11</sup>. ABS-CBN informed this Commission that they planned to relaunch the website on 16 November 2018.

### **Discussion**

Upon careful inspection of the reports and documents submitted by ABS-CBN, the Commission finds the absence of any proof of notification to the affected data subjects as well as proof of receipt of the said notification. NPC Circular 16-03<sup>12</sup> requires that all actions made by a personal information controller should be properly documented. This includes compliance with the notification requirements and assistance to affected data subjects:

**SECTION 9. Documentation.** All actions taken by a personal information controller or personal information processor shall be properly documented. Reports should include:

- A. Description of the personal data breach, its root cause and circumstances regarding its discovery;
- B. Actions and decisions of the incident response team;
- C. Outcome of the breach management, and difficulties encountered; and
- D. Compliance with notification requirements and assistance provided to affected data subjects.

A procedure for post-breach review must be established for the purpose of improving the personal data breach management policies and procedures of the personal information controller or personal information processor.

As to the manner of notification to the affected data subjects, Section 18(A) of NPC Circular No. 16-03 provides that:

The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. **It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.** It may be supplemented with additional information at a later stage on the basis of further investigation.<sup>13</sup>

---

11 A false positive state is when the IDS identifies an activity as an attack, but the activity is acceptable behavior.  
12 National Privacy Commission, Personal Data Breach Management, Circular No. 16-03 (December 15, 2016).  
13 Emphasis supplied.

Moreover, Section 18(D) of same Circular provides that:

Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. **The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach:** *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.<sup>1415</sup>

As stated by the Commission in its Resolution for NPC BN 20-161,

It is noteworthy that the avowed purpose of the required notification to data subjects of a breach incident is for them to take the necessary precautions or other measures to protect themselves against possible effects of the breach. Moreover, personal information controllers (PICs) are required to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach. It therefore follows that PICs should guarantee that the notification they sent to data subjects has been received. Otherwise, it defeats the very purpose of notification of data subjects.<sup>16</sup>

Notification to the affected data subjects in cases of personal data breach is an essential obligation in data privacy protection. Section 20 (f) of the DPA of 2012 states that:

SEC. 20. Security of Personal Information. –

xxx

(f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

The Commission notes that ABS-CBN merely stated the following in its Incident Report:

## REMEDIAL MEASURES

xxx

b. The following security measures were advised to the affected customers:

- Immediately change their account passwords.

14 Emphasis supplied.

15 Supra, Note 2.

16 NPC BN 20-161, 17 December 2021.



- Inform their bank and credit card provider immediately and follow the bank/credit card provider's advice.
- Not provide any personal and/or financial information to anyone who may claim to be an ABS-CBN representative.
- If the aforementioned case was encountered, report the incident to ABS-CBN by emailing [abs-cbnstore@abscbn.com](mailto:abs-cbnstore@abscbn.com).

Pursuant to the requirements of Section 18(A) and Section (D) of NPC Circular 16-03, the Commission orders ABS-CBN to submit proof of notification to the two hundred eight (208) affected data subjects.

**WHEREFORE**, the Commission **ORDERS** ABS-CBN Corporation to submit proof of notification to the two-hundred eight (208) data subjects who were affected by the breach, within fifteen (15) days from receipt of this Order.

**SO ORDERED.**

City of Pasay, Philippines;  
11 March 2021.

**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

WE CONCUR:

**RAYMUND ENRIQUEZ LIBORO**  
Privacy Commissioner

**JOHN HENRY D. NAGA**  
Deputy Privacy Commissioner

**COPY FURNISHED:**

**JCG**  
*Data Privacy Officer*  
ABS—CBN Corporation

**COMPLAINTS AND INVESTIGATION DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

X-----X

**ORDER**

Before this Commission is a request for extension to submit documents filed by Power-Vision EAP, Inc. (PowerVision) dated 04 January 2022, in relation to a phishing incident of its email account. PowerVision also requests guidance from the Commission on a possible exemption from data subject notification.

**Facts**

In the Initial Report sent on 23 May 2021 (Initial Report), PowerVision reported a security incident that happened on 20 May 2021 wherein the password of its administrative email account (help@powervisioneap.com) was cracked and subsequently used to send phishing emails to recipients.<sup>1</sup>

Particularly, emails were sent using the administrative email account containing an audio file that would require the person accessing it to input the Outlook email and password. The Initial Report also contained a request for extension of time of fifteen (15) days to file the Full Breach Report.<sup>2</sup>

PowerVision subsequently submitted a Full Report dated 07 June 2021 (Full Report). In the cover letter of the Full Report, PowerVision related that it had analyzed twenty-five thousand eight hundred eighty-seven (25,887) emails, over which four hundred eighty-two (482) emails contained personal data.<sup>3</sup> The sensitive personal information contained in the emails included “the mental or emotional health condition of the data subject and possibly some isolated number of government identifiers.”<sup>4</sup>

As part of its efforts to address the phishing incident, PowerVision changed the password of their administrative email account, and temporarily deactivated it.<sup>5</sup> Notifications were sent to the three hundred eighty-seven (387) recipients of the phishing email and PowerVision’s client points-of-contact to inform them about the incident, requiring them to change their password, and perform anti-virus scans on their device.<sup>6</sup> On 24 May 2021, multi-factor authentication was required to access all PowerVision-issued email accounts. It also claimed that after investigation, the intruder did not download any emails from the account.<sup>7</sup>

In its cover letter containing the Full Report, PowerVision requested guidance from the Commission on whether an exemption from notifying its data subjects was allowable “since there was no sensitive personal data acquired by the intruder and that the possible emotional and mental effect which may unnecessarily burden the data subject is not proportionate to the minimal possible risk.”<sup>8</sup>

1 Initial Report dated 23 May 2021 filed by PowerVision EAP, Inc.  
2 *Id.*  
3 Cover Letter dated 07 June 2021 of PowerVision EAP, Inc.  
4 Full Report dated 07 June 2021 filed by PowerVision EAP, Inc.  
5 *Id.*  
6 *Id.*  
7 *Id.*  
8 Cover Letter dated 07 June 2021 of PowerVision EAP, Inc.

In an Order dated 08 June 2021 (Order), the Compliance and Monitoring Division (CMD) of the Commission ordered PowerVision to submit the following documents within a period of five (5) days from receipt, to quote:

**WHEREFORE**, premises considered, **the PowerVision EAP Inc.** is **ORDERED: TO SUBMIT** the following documents:

1. Lacking details on the full breach report based on the provisions of NPC Circular 16-03:
  - a. Description how the breach occurred and the vulnerability of the data processing system that allowed the breach.
  - b. Chronology of events.
  - c. Description of the likely consequences of the personal data breach. Provide how will the incident affect both the PIC and its data subjects.
  - d. Measures to secure/recover personal data.
  - e. Actions to mitigate harm.
  - f. Actions taken to inform data subjects. Provide the actual manner of notification. Include the assistance extended to data subjects, if there is any.
  - g. Measures being taken to prevent a recurrence of the incident. Provide the portion of the actual or proposed orientation materials addressing the vulnerability identified.
2. Security Incident Management Policy;
3. Privacy Manual;
4. Copy of the data subject notification; and
5. Policies relating to human Resource security, cryptography, access control, communications security, and compliance

**POWERSHIELD EAP INC.** is hereby given a period of five (5) days from receipt hereof to submit its compliance through email at [breach@privacy.gov.ph](mailto:breach@privacy.gov.ph).

**SO ORDERED.**<sup>9</sup>

PowerVision received the Order on 03 January 2022. Through an email on 04 January 2022, its Data Protection Officer (DPO) requested an extension until 28 January 2022 to submit the documents in the CMD's Order since: 1) the DPO was currently out of the country and had no access to the files needed; and 2) the DPO tested positive for Covid-19 and there was a possibility of delay in returning to the Philippines.<sup>10</sup>

### **Issue**

- I. Whether to grant the request for extension until 28 January 2022 to submit the documents outlined in the Order dated 08 June 2021.
- II. Whether to grant the request for exemption from data subject notification.

### **Discussion**

The Commission grants PowerVision's request for an extension until 28 January 2022 to submit the documents outlined in the CMD's Order dated 08 June 2021. It denies its request for exemption from data subject notification.

<sup>9</sup> Order dated 08 June 2021.

<sup>10</sup> Email Request dated 04 January 2022 of PowerVision EAP, Inc.

*A Personal Information Controller has the obligation to ensure the accessibility of documents and information related to the personal data breach.*

PowerVision, as the Personal Information Controller (PIC), is expected to comply with the periods stated in NPC Circular No. 16-03 (Personal Data Breach Management)<sup>11</sup> and with the corresponding orders of the Commission. Particularly, Section 17(C) of NPC Circular No. 16-03 requires the submission of a Full Breach Report within five (5) days from initial notification, “unless the personal information controller is granted additional time by the Commission to comply.”<sup>12</sup>

Further, Section 18(A) of the same Circular states:

**SECTION 18. Notification of Data Subjects.** The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:

A. When should notification be done. The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred. The notification may be made on the basis of 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.<sup>13</sup>

Considering the abovementioned provisions, the Full Breach Report must be submitted within five (5) days from filing the Initial Report.<sup>14</sup> While, the notification to the affected data subjects must be made based on available information within the 72-hour period.<sup>15</sup>

PowerVision now requests an extension to submit documents given that they are allegedly inaccessible due to the DPO’s physical location and health condition.<sup>16</sup>

The Commission notes that in PowerVision’s cover letter containing the Full Report, it stated that due to the pandemic, “counselling sessions are made through online platform or via audio calls.”<sup>17</sup> As a company that relies on technology, particularly during the pandemic, it would also be reasonable to infer that the documents are digitized and accessible. Thus, the files or documents needed would be accessible regardless of the physical location or health condition of the DPO.

Further, Section 5 of NPC Circular No. 16-03 requires a data breach response team as part of the guidelines for personal data breach management, to quote:

---

11 see NPC Circular No. 16-03, Section 17(A) and (C); Section 18(A).  
12 NPC Circular No. 16-03, Section 17(C).  
13 Section 18(A) of the NPC Circular No. 16-03.  
14 Section 17(C) of the NPC Circular No. 16-03.  
15 Section 18(A) of the NPC Circular No. 16-03.  
16 *Id.*  
17 Cover Letter dated 07 June 2021 of PowerVision EAP, Inc.

**SECTION 5. Data Breach Response Team.** A personal information controller or personal information processor shall constitute a data breach response team, which shall have at least one (1) member with the authority to make immediate decisions regarding critical action, if necessary. **The team may include the Data Protection Officer.**

The team shall be responsible for the following:

- A. Implementation of the security incident management policy of the personal information controller or personal information processor;
- B. Management of security incidents and personal data breaches; and
- C. Compliance by the personal information controller or personal information processor with the relevant provisions of the Act, its IRR, and all related issuances by the Commission on personal data breach management.

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.

**The functions of the Data Breach Response Team may be outsourced. Such outsourcing shall not reduce the requirements found in the Act, the IRR or related issuance. The Data Protection Officer shall remain accountable for compliance with applicable laws and regulations.**<sup>18</sup> (Emphases supplied)

As the quoted provision shows, the responsibility for complying with NPC Circular No. 16-03 does not rest solely with the DPO. The PIC should have a data breach response team in place to handle proceedings related to data breaches. In this case, even though PowerVision's DPO is abroad and has contracted Covid-19, members of PowerVision's data breach response team should be available to comply with the CMD's Order.

Further, the Commission once again reminds PICs that the prompt compliance with the Commission's orders is within their responsibilities and obligations in cases of data breach, especially if the incident involves sensitive personal information<sup>19</sup> and the affected data subjects are more than one hundred (100) individuals.<sup>20</sup>

*The Commission has the authority to grant the PIC an additional period to comply with the submission of documents.*

Nevertheless, in the interest of substantial justice and due process, the Commission now exercises its authority to grant PowerVision's request for extension. In granting PowerVision's request for extension, the Commission applies liberality and shall allow the PIC to submit the additional documents based on its requested period, i.e., 28 January 2022.

The Commission expects that PowerVision will comply in good faith with the period requested. As previously ruled by the Commission: "A PIC is expected to comply with the

---

18 Section 5 of the NPC Circular No. 16-03.  
19 Section 11(A) of the NPC Circular No. 16-03.  
20 Section 13(B) of the NPC Circular No. 16-03.

Commission's Order within the period that the PIC itself requested from the Commission."<sup>21</sup>

*The PIC must notify data subjects in cases which fall under the mandatory breach notification requirement.*

In the cover letter attaching its Full Report, PowerVision requested guidance from the Commission on whether it may be exempted from notifying the affected data subjects.<sup>22</sup> It claims that "there was no sensitive personal data acquired by the intruder and that the possible emotional and mental effect which may unnecessarily burden the data subject is not proportionate to the minimal possible risk."<sup>23</sup> This request for guidance shall be treated by the Commission as a request for exemption from data subject notification.

The Commission finds that the reported breach falls under the mandatory breach notification requirement, and notification is crucial in order to reduce the risks and possible harm to the affected data subjects. Section 11 of NPC Circular No. 16-03 provides:

SECTION 11. When notification is required. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

**A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.** For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

**B. There is reason to believe that the information may have been acquired by an unauthorized person;** and

**C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.**<sup>24</sup> (Emphases supplied)

Further, Section 13(B) and (C) of NPC Circular No. 16-03, in relation to Section 11 of the same Circular provides:

**SECTION 13. Determination of the Need to Notify.** Where there is uncertainty as to the need for notification, the personal information controller shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have

<sup>21</sup> NPC BN 20-129 In re: DB Schenker Global Service Asia Pacific Inc.. Resolution dated 02 September 2021. At page 6.

<sup>22</sup> Cover Letter dated 07 June 2021 of PowerVision EAP, Inc.

<sup>23</sup> *Id.*

<sup>24</sup> Section 11 of the NPC Circular No. 16-03.

occurred. The personal information controller shall also consider if the personal data reasonably believed to have been compromised involves:

xxx

B. At least one hundred (100) individuals;

C. Information required by applicable laws or rules to be confidential;<sup>25</sup>

Here, PowerVision itself identified that the personal data breach involved sensitive personal information since four hundred and eighty-two (482) emails in the administrative email account contained “the mental or emotional health condition of the data subject and possibly some isolated number of government identifiers”.<sup>26</sup> The number of data subjects is more than one hundred (100) since three hundred eighty-seven (387) people were recipients of the phishing email. The two circumstances combined require PowerVision to notify the affected data subjects.<sup>27</sup>

In this case, there are also insufficient grounds for the exemption of notification of affected data subjects. Section 18(B) of NPC Circular No. 1603 provides for situations that may exempt a PIC from notifying data subjects, to quote:

**SECTION 18. Notification of Data Subjects.** The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:

xxx

B. *Exemption or Postponement of Notification.* If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification.

A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects.<sup>28</sup>

Section 19 of NPC Circular No. 16-03 further provides:

**SECTION 19. Exemption from Notification Requirements.** The following additional factors shall be considered in determining whether the Commission may exempt a personal information controller from notification:

A. Security measures that have been implemented and applied to the personal data at the time the personal data breach was reasonably believed to have occurred, including measures that would prevent use of the personal data by any person not authorized to access it;

B. Subsequent measures that have been taken by the personal information controller or personal information processor to ensure that the risk of harm or negative consequence to the data subjects will not materialize;

---

25 Section 13(B) and (C) of the NPC Circular No. 16-03  
26 Full Report dated 07 June 2021 filed by PowerVision EAP, Inc.  
27 *Id.*  
28 Section 18(B) of the NPC Circular No. 16-03.

C. Age or legal capacity of affected data subjects: Provided, that in the case of minors or other individuals without legal capacity, notification may be done through their legal representatives.

In evaluating if notification is unwarranted, the Commission may take into account the compliance by the personal information controller with the law and existence of good faith in the acquisition of personal data.<sup>29</sup>

The Commission notes that the type of sensitive personal information involved may be used to enable identity fraud. Also, the breach of the data subjects' patient records (i.e.- the mental or emotional health conditions) may expose them to harassment, discrimination, or other risks of real and serious harm. Further, PowerVision failed to provide actual proof of the security measures it has implemented during the breach and subsequent measures it has implemented for the risk of harm or negative consequence to the affected data subjects will not materialize. The Commission finds that PowerVision has not sufficiently shown that notification is not reasonably possible, and given the circumstances, an exemption from notification would not be in the best interest of affected data subjects.

Considering the type of personal information involved and the number of affected data subjects, the Commission deems it wise for PowerVision to promptly notify the affected data subjects. This is in order to allow them to take the necessary precautions or other measures to protect themselves against the potential harm or negative consequences resulting from the breach.<sup>30</sup>

**WHEREFORE**, premises considered, PowerVision EAP, Inc.'s (PowerVision) request for an extension to submit the documents enumerated in the Compliance and Monitoring Division's Order dated 08 June 2021, is hereby **GRANTED**. PowerVision is **ORDERED** to submit the required documents as stated in the CMD Order dated 08 June 2021 until **28 January 2022, namely:**

1. Details on the full breach report based on the provisions of NPC Circular 16-03:
  - a. Description how the breach occurred and the vulnerability of the data processing system that allowed the breach.
  - b. Chronology of events.
  - c. Description of the likely consequences of the personal data breach. Provide how will the incident affect both the PIC and its data subjects.
  - d. Measures to secure/recover personal data.
  - e. Actions to mitigate harm.
  - f. Actions taken to inform data subjects. Provide the actual manner of notification. Include the assistance extended to data subjects, if there is any.
  - g. Measures being taken to prevent a recurrence of the incident. Provide the portion of the actual or proposed orientation materials addressing the vulnerability identified.
2. Security Incident Management Policy;
3. Privacy Manual;
4. Copy of the data subject notification; and
5. Policies relating to human Resource security, cryptography, access control, communications security, and compliance

<sup>29</sup> Section 19 of the NPC Circular No. 16-03.

<sup>30</sup> See NPC Circular No. 16-03, Section 18(A).



**PowerVision** is further **ORDERED** to notify the affected data subjects, and submit proof of notification thereof.

**SO ORDERED.**

City of Pasay, Philippines.  
27 January 2022.

**Sgd.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

I CONCUR:

**Sgd.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

Copy furnished:

**RVN.**  
*Data Protection Officer of PowerVision*

**COMPLIANCE AND MONITORING DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

X-----X

**ORDER**

Before the Commission is a request for postponement of notification of data subjects filed by Enchanted Kingdom, Inc. (EKI) regarding a security incident on its online payment gateway on its website, operated by AsiaPay Payment Technology Corporation (AsiaPay).

**Facts**

EKI runs a theme park which has an online store selling its products. Customers are able to settle online purchases through various modes, including credit card payments.<sup>1</sup> The credit card option will direct customers to an online payment gateway, PesoPay, which is operated by AsiaPay. To confirm credit card payments, customers must supply their names, credit card numbers, and card validation values.<sup>2</sup>

In its Initial Report dated 31 August 2021 (Initial Report), EKI reported a possible security incident in the system of its online payment gateway partner, AsiaPay. From the Initial Report, AsiaPay alerted EKI that its payment gateway had been compromised for the period from 04 August 2020 to 02 May 2021. The EKI online store transactions may have been among those affected.<sup>3</sup>

EKI met with AsiaPay’s Chief Operating Officer and its Philippine Senior Accounts Manager on 25 August 2021.<sup>4</sup> In the meeting, EKI was informed that AsiaPay was still investigating the breach and was not in the position to confirm whether EKI transactions, or any specific EKI transaction or customer, were affected.<sup>5</sup>AsiaPay would provide more information to EKI about the breach, and assured them during the meeting and via email that the vulnerability which facilitated the breach had already been addressed.<sup>6</sup>

AsiaPay posted updates on its website regarding the security incident<sup>7</sup> on 11 June 2021, 22 July 2021, and 20 August 2021. In its last update, AsiaPay stated that based on the findings of a forensic investigator, there was a cyberattack that happened between the periods of 04 August 2020 to 05 May 2021 which occurred after its data center migration.<sup>8</sup>

EKI, through its Initial Report, is requesting for the authority to withhold public notification of the breach until such time AsiaPay “renders an actionable report to EKI” given that the information supplied by AsiaPay is nonspecific.<sup>9</sup>

1 Initial Report dated 31 August 2021 of Enchanted Kingdom, Inc.  
2 *Id.*  
3 *Id.*  
4 *Id.*  
5 *Id.*  
6 *Id.*  
7 See Security Incident, accessed at <https://www.asiapay.com/2021.html>, as provided in the Initial Report.  
8 *Id.*  
9 *Id.*

## Issue

Whether EKI's request for postponement of notification of data subjects should be granted.

## Discussion

The Commission denies EKI's request for the postponement of notification of affected data subjects.

*EKI is a Personal Information Controller (PIC).*

A PIC is defined as one "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."<sup>10</sup>Control is present when the entity "decides on what information is collected, or the purpose or extent of its processing."<sup>11</sup>

EKI is the owner and administrator of its website which sells various goods, services and merchandise, and its website provides avenues for online payment.<sup>12</sup>Particularly, customers are required to provide personal information (name, credit card number, and validation value) to confirm credit card payments on its website. This makes EKI a PIC since it determines and requires customers to provide such personal information. EKI is a PIC regardless of having AsiaPay as its online gateway partner, since AsiaPay is processing the personal data for the benefit and on behalf of EKI.

As the PIC, EKI has clear obligations under NPC Circular No. 16-03 (Personal Data Breach Management) relating to the notification of affected data subjects and the Commission, as well as providing crucial information about the data breach to the Commission and to the affected data subjects.

*The data breach falls under mandatory data subject notification.*

Under Section 11 of NPC Circular No. 16-03, notification must be done by the PIC upon knowledge or reasonable belief of a personal data breach that meets particular conditions, to quote:

**SECTION 11. When notification is required.** Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.

For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and

---

10 Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, Section 3(h).

11 Implementing Rules and Regulations of the Data Privacy Act of 2012, Section 3(m).

12 Initial Report dated 31 August 2021 of Enchanted Kingdom, Inc.

other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

B. There is reason to believe that the information may have been acquired by an unauthorized person; and

C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.<sup>13</sup>

Here, EKI reported that confirming credit card payments would require customers to input their names, credit card numbers, and credit card validation values.<sup>14</sup> These types of information relate to the financial and economic situation of data subjects. The information could also be used to enable identity fraud.

The information may also have been acquired by an unauthorized person, as AsiaPay itself publicly stated, through its website announcement, that “it is with regret that the Company now informs stakeholders and supporters that a highly sophisticated cyber-attack on our systems has been discovered.”<sup>15</sup>

It is also reasonably apparent that EKI believed that such unauthorized acquisition would likely give rise to a real risk of serious harm for affected data subjects. From its Initial Report, EKI met with AsiaPay’s top management, and were promised to be updated about the breach.<sup>16</sup> This reveals the clear gravity of the situation. In any case, the Commission finds that the possible acquisition of the names, credit card numbers, and credit card validation values gives rise to serious harm for affected data subjects.

There are only specific instances where the Commission may allow the postponement of notification of affected data subjects. Section 18(B) 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:

xxx

B. *Exemption or Postponement of Notification.* If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification.

xxx

The Commission may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.

<sup>13</sup> Section 11 of the NPC Circular No. 16-03.

<sup>14</sup> Initial Report dated 31 August 2021 of Enchanted Kingdom, Inc.

<sup>15</sup> See Security Incident, accessed at <https://www.asiapay.com/2021.html>, as provided in the Initial Report.

<sup>16</sup> Initial Report dated 31 August 2021 of Enchanted Kingdom, Inc.

In this case, EKI does not allege that there is a pending criminal investigation, and its only reason for seeking postponement is its claim that “the information supplied by AsiaPay is nonspecific”, and therefore, public notification should be withheld “until such time as AsiaPay renders an actionable report to EKI”.<sup>17</sup>

As shown by AsiaPay’s public posts on its website, it has already concluded a forensic investigation and determined the method and period when its systems were breached. EKI need not wait for AsiaPay to provide an actionable report to EKI, and should have been more proactive in seeking information on how the data breach affected EKI’s customers availing of the credit card option for payment during the period relevant to the data breach.

EKI has also not provided the particular security measures it has done after learning about the breach in order to secure the affected data subjects’ personal information. Thus, the Commission finds that with the type of personal data involved and the factual circumstances of the case, EKI shall have to notify the affected data subjects. Such notification to the affected data subjects is urgent and necessary in order to allow them to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.<sup>18</sup>

*EKI has the further obligation to comply with the seventy-two (72) hour period to notify the Commission, and submit its Full Breach Report within five (5) days from notification, as provided under the NPC Circular No. 16-03.*

Under Section 17(A) and (C) of NPC Circular No. 16-03, PICs are required to notify the Commission within seventy-two (72) hours from knowledge or reasonable belief of the data breach, and to submit a Full Breach Report within five (5) days from notification, to quote:

**SECTION 17. Notification of the Commission.** The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:

A. When Notification Should be Done. **The Commission shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.**

xxx

C. *When delay is prohibited.* There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. **The full report of the personal data breach must be submitted within five (5) days,** unless the personal information controller is granted additional time by the Commission to comply.<sup>19</sup> (Emphases supplied)

17

*Id.*

18 Section 18(A) of the NPC Circular 16-03.

19 Section 17(A) and (C) of the NPC Circular No. 16-03

Here, EKI knew about the breach since 20 August 2021. It notified the Commission only on 31 August 2021, or beyond the seventy-two (72) hour-period. Further, EKI has yet to provide its Full Breach Report to the Commission pursuant to Section 9 and Section 17(D) of NPC Circular No. 16-03.

**WHEREFORE**, premises considered, this Commission **DENIES** the request of Enchanted Kingdom, Inc. (EKI) to postpone the notification of affected data subjects.

EKI is hereby **ORDERED within fifteen (15) days** from receipt of this Order to comply with the following:

1. **NOTIFY** the affected data affected subjects pursuant to Section 18 of NPC Circular No. 16-03 and submit proof of compliance thereof, including the proof of receipt of the data subjects of such notification;
2. **SUBMIT** a Full Breach Report pursuant to Sections 9 and 17 (D) of NPC Circular No. 16-03;
3. **SUBMIT** proof of security measures to address the breach pursuant to Section 17(D) of NPC Circular No. 16-03; and
4. **SHOW CAUSE** in writing why it should not be held liable for its failure to submit its Full Breach Report within the prescribed period and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.

**SO ORDERED.**

City of Pasay, Philippines.  
27 January 2022.

**SGD.**

**JOHN HENRY D. NAGA**  
Privacy Commissioner

I CONCUR:

**SGD.**

**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

Copy furnished:

**BMM**

*Data Protection Officer*

**COMPLIANCE AND MONITORING DIVISION**  
**ENFORCEMENT DIVISION**  
**GENERAL RECORDS UNIT**  
National Privacy Commission

-versus-

**PH-CHECK.COM,**

*Respondent.*

X-----X

## **ORDER**

Before the Commission is the Application for Issuance of Cease and Desist Order dated 16 August 2022 (CDO Application) of the Complaints and Investigation Division (CID) of the National Privacy Commission (NPC). The CDO Application is against PH-Check.com (<https://ph-check.com>) for violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA). The PH-Check.com website contains personal data and other information found in the Business Name Registration System (BNRS) website of the Department of Trade and Industry (DTI).

### **Facts**

On 19 January 2022, the DTI endorsed to the CID an e-mail from ASA dated 14 January 2022.<sup>1</sup> The endorsement stated that ASA reported a website with address <https://ph-check.com/> to the DTI and requested that a demand letter be sent to the website in order for it “to stop scraping information” from DTI’s website.<sup>2</sup>

According to ASA, if he searches his full name on Google, then his DTI business details would appear at the top of the search under PHCheck.com.<sup>3</sup> ASA further stated that his data should only be available on DTI’s portal and repository and thus, requested that the DTI developers “stop web scraping from [third] party sites.”<sup>4</sup>

The CID issued its Initial Report dated 21 January 2022 (Initial Report). As explained by the CID:

The [DTI] is a government agency established to address local industry and foreign trade growth. In compliance with Republic Act 38831 as amended, and its Implementing Rules and Regulations, and to facilitate ease of registration, DTI established the online Business Name Registration System (BNRS)[.]

The BNRS Next Gen is a web-based portal that allows end-to-end registration of business name (BN) for sole proprietors. To make BN registration more convenient, applicants may submit applications, pay fees and download their Certificate of BN registration through the BNRS Next Gen. It also contains publicly available informa

1 Department of Trade and Industry (DTI) Endorsement Letter dated 19 January 2022; Initial Report dated 21 January 2022 of the Complaints and Investigation Division, Annex “A”.

2 Department of Trade and Industry (DTI) Endorsement Letter dated 19 January 2022; Initial Report dated 21 January 2022 of the Complaints and Investigation Division, Annex “A”.

3 Electronic mail dated 14 January 2022 of ASA; Initial Report dated 21 January 2022 of the Complaints and Investigation Division, Annex “B”.

4 Electronic mail dated 14 January 2022 of ASA; Initial Report dated 21 January 2022 of the Complaints and Investigation Division, Annex “B”.

tion about DTI-registered BNs that will help both the public and other government agencies check the validity of a particular BN.<sup>5</sup>

The CID also provided the following observations in the Initial Report:

3. A google search of the name 'ASA' will show a result that links his name to 'STT' [ANNEX C].

4. The CID QRSC team investigated the website '<https://phcheck.com/>' and found out that in the homepage of the website, a total of 30 Business Names were listed. [ANNEX D]. Using the website search engine, it will also generate business names not initially listed on its home page.

5. A search for the business name 'STT' will show that it is listed in the website [ANNEX E] and upon clicking the name, will reveal the following business name information: [ANNEX F]

- a. Name
- b. Status
- c. Type of Entity
- d. Business Scope
- e. Business Territory
- f. Certificate No./BNN
- g. Registration Date
- h. Owners/Directors Name and Designation
- i. Additional info: Since Registration

6. A search for the word 'ABC' would display all the business names that starts with the word 'ABC' [ANNEX G]. When the listed business name is clicked, such as the displayed business name 'ABC – ABCFP', the website will redirect to a page where it displays more information like: [ANNEX H]

- a. Name
- b. Status
- c. Type of Entity
- d. Business Scope
- e. Business Territory
- f. Certificate No./BNN
- g. Registration Date
- h. Owners/Directors Name and Designation
- i. Additional info: Since Registration

7. In both searches, the pages has a Contact Details Table that is editable. When the team tried to input a dummy contact detail and then click submit, the website replies with a message 'Thank you! Your information will appear after being reviewed by a moderator'. [ANNEX I]

8. The website <https://ph-check.com/> is devoid of any information pertaining to the company or its owner and has no privacy notice. [ANNEX J]

9. The CID QRSC team also visited the DTI BNRS website and tried to search the Business Name 'STT' and found out that it displays the same information as found in the website <https://ph-check.com/>[.]

xxx

10. The business name 'ABC -ABCFP' was also checked and similarly, it displays the same information [.]

---

<sup>5</sup> Complaints and Investigation Division (CID) Initial Report dated 21 January 2022 , at p. 1



xxx

Based on the foregoing, it shows that the website <https://phcheck.com/> is scraping business name information which is made publicly available by DTI through its website <https://bnrs.dti.gov.ph/>.<sup>6</sup>

The CID wrote a letter dated 21 January 2022 to the DTI detailing that based on its initial investigation, PH-Check.com scrapes data from the BNRS website.<sup>7</sup>

On 07 February 2022, a complaint by KGU was received by the DTI against PH-Check.com, who also requested for the removal of her information from the website.<sup>8</sup>In her complaint, KGU stated that the website “contains information about Philippine companies (Name, Status, Business Scope, Business Territory, Certificate Number/BNN, Registration Date and Time, as well as the Full Name of the Owner).”<sup>9</sup>KGU also stated that “when [her] full name is searched on Google, all [her] business details appear together with [her] full name on PH- Check.com.”<sup>10</sup>

To prove her claims, KGU provided screenshots of: 1) her information found in the BNRS website, 2) the Google search results, and 3) her information found in PH-Check.com.<sup>11</sup>

KGU also noted that PH-Check.com does not contain any contact or owner information, and indicated her lack of consent to the sharing of her information:

PH-Check.com **does not contain contact nor owner information.**

**I also did not give permission for my information to be shared to third party websites and to be made available elsewhere.** DTI’s data privacy notice reads:

xxx

**The reproduction of my information in PH-Check.com are not warranted by the conditions above,** unless the DTI has a data sharing agreement with this website. It is not even a licensing agency nor an entity which facilitates business registration-related transactions.

In this regard, I would like to: **(1) complain against the proprietor of PH-Check.com for replicating my personal information without my consent and (2) request for the removal of my personal data** from this website.<sup>12</sup>

The DTI replied to KGU in a letter dated 08 February 2022.<sup>13</sup> In the letter, the DTI informed KGU that it has endorsed her complaint to the NPC.<sup>14</sup>Further, the DTI stated:

We have taken note of your request the removal of your information on the site PH.check.com. We wish to note however that this is a third-party site and not affiliated with the DTI.

xxx

---

6 Complaints and Investigation Division (CID) Initial Report dated 21 January 2022 , at pp. 2-3.  
7 Letter dated 21 January 2022 of the Complaints and Investigation Division, at p. 1.  
8 Letter dated 07 February 2022 of KGU, at p. 3.  
9 Letter dated 07 February 2022 of KGU, at p. 1.  
10 Letter dated 07 February 2022 of KGU, at p. 2.  
11 Letter dated 07 February 2022 of KGU, at pp. 1-3.  
12 Letter dated 07 February 2022 of KGU, at p. 3.  
13 Letter dated 08 February 2022 of the Department of Trade and Industry.  
14 Letter dated 08 February 2022 of the Department of Trade and Industry.

We wish to likewise note your observation that data from PH.check.com is similar with the information displayed in the public domain of the DTI Business Name Search database. Please be informed however that the DTI does not have an existing partnership or agreement with PH-Check.com, nor has DTI given permission to publish information such as Name, Status, Business Scope, Business Territory, etc. as well as the full name of the owner.<sup>15</sup>

Subsequently, in a Notice to Explain dated 16 February 2022, the CID required the Owner/Administrator of PH-check.com to submit an explanation as to why it should not be liable for violating the DPA<sup>16</sup> since it had received complaints against the website for disclosing “public [personal] information and sensitive personal information.”<sup>17</sup>The Notice to Explain was sent to the following emails: ph-check.comowner-zjoj@customers.whoisprivacycorp.com, ph-check.com-admintl17@customers.whoisprivacycorp.com, and ph-check.com-tech3ysl@customers.whoisprivacycorp.com.<sup>18</sup> The said e-mails were obtained after accessing the website <https://who.is/whois/phcheck.com> where the Registrar Data provided the contact information since the website PH-check.com had no information pertaining to the website’s owner.<sup>19</sup>

However, as of date, PH-Check.com failed to respond to the Notice to Explain issued by the Commission.

In a Supplemental Report dated 05 July 2022 (Supplemental Report), the CID further alleged:

Based on the investigation, it shows that the disclosure of DTI of personal information in its website is pursuant to Act No. 38883 and DAO 18-07, with an undertaking and consent from the data subject to make such information publicly available.

As for the website <https://ph-check.com/>, it has not complied with the [Notice to Explain]. A perusal of the website would show that it does not contain any Privacy Policy or any statement as to the purpose of the website, in violation of the general data privacy principles of transparency, legitimate purpose, and proportionality.

xxx

Moreover, the owners/administrators took means to hide their identity and did not provide any contact details, making it difficult for data subjects to exercise their rights to their personal information, contrary to the requirements set forth in Section 16 of the DPA[.]

xxx

The data scraping activity of the website <https://ph-check.com> and its deliberate intent to hide the identity of its owner or contact details of its administrators is a clear

violation of Sections 11 and 16 of the DPA, which is detrimental to public interest and unless restrained, will cause grave and irreparable injury to a data subject. It is worth noting that as of date, two (2) individuals have already complained regarding this matter.<sup>20</sup>

---

15 Letter dated 08 February 2022 of the Department of Trade and Industry.

16 Notice to Explain dated 16 February 2022 of the Complaints and Investigation Division.

17 Notice to Explain dated 16 February 2022 of the Complaints and Investigation Division.

18 Notice to Explain dated 16 February 2022 of the Complaints and Investigation Division.

19 Complaints and Investigation Division (CID) Initial Report dated 21 January 2022, at p. 2, See: Annex “J”.

20 Supplemental Report dated 05 July 2022 of the Complaints and Investigation Division, at pp. 24.

The Supplemental Report recommended that an Application for Cease and Desist Order (CDO) be filed against PH-Check.com.<sup>21</sup>

Subsequently, in a Technical Report dated 26 July 2022 (Technical Report), the CID stated that based on its examination, “the data is not directly being harvested by the website from the API of bnrs.dti.gov.ph and did not find any website link of the DTI during this interception.”<sup>22</sup> However, the CID noted that it was possible that “a separate web crawler is being used by the [PH-Check.com] website to populate its database causing the data mining to be hidden even when intercepting data from the main website.”<sup>23</sup>

Thereafter, the CID filed its CDO Application, praying that a CDO be issued against PH-Check.com “in order to preserve and protect public interest and the right of the data subjects.”<sup>24</sup>

### Issue

Whether to grant the CDO Application of the CID.

### Discussion

The Commission finds that there are sufficient grounds for the issuance of a CDO against PH-Check.com.

First, the Commission has jurisdiction over the activities of PHCheck.com in relation to privacy matters. PH-Check.com is considered a personal information controller (PIC) that processes personal data.

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.”<sup>25</sup> Sensitive personal information is a subset of personal information which includes information “[i]ssued by government agencies peculiar to an individual.”<sup>26</sup>

Here, the information displayed on the website include the first name, middle name, and last name of the owner or director who is registered in the DTI’s BNRS.<sup>27</sup> Other details found in the website include the DTI Certificate Number or Business Name Number (BNN), status, type of entity, business scope, business territory, and registration date.<sup>28</sup> There are also fields in the website which allow anyone to provide the address, phone number, and website or email address of the business.<sup>29</sup>

---

21 Supplemental Report dated 05 July 2022 of the Complaints and Investigation Division, at p. 4.

22 Technical Report dated 26 July 2022 of the Complaints and Investigation Division, at p. 1.

23 Technical Report dated 26 July 2022 of the Complaints and Investigation Division, at p. 1.

24 Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p. 8.

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, chapter I, § 3 (g) (2012) (Data Privacy Act of 2012).

26 Data Privacy Act of 2012, chapter I, § 3 (l) (2012).

27 Complaints and Investigation Division, Application for Issuance of Cease and Desist Order dated 16 August 2022, at p. 1; See Initial Report dated 21 January 2022, Annex “F”.

28 Initial Report dated 21 January 2022 of the Complaints and Investigation Division, Annex “F”.

29 Initial Report dated 21 January 2022 of the Complaints and Investigation Division, Annex “F”.

Thus, there are personal data displayed on PH-Check.com that can be classified as personal information.

Next, processing is defined in the DPA as “any operation or any set of operations performed upon personal information including, but not limited to, collection, recording, organization, storage...use [and] consolidation” of personal data.<sup>30</sup> Meanwhile, a PIC “refers to as a person or organization who controls the collection, holding, processing or use of personal information.”<sup>31</sup>

In its CDO Application, the CID alleged that PH-Check.com collected “data from [the] DTI[’s] BNRS [website] and displayed it in its website.”<sup>32</sup> These actions thus fall under the definition of processing defined in the DPA.

PH-Check.com is also a PIC given that it is the one that has control over the collection of the personal data displayed. Control is present when a “natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.”<sup>33</sup>

Given that PH-Check.com is a PIC, it is responsible for personal data under its custody or control. Indeed, its “About Us” page states that “PH-Check provides information about Philippines companies. The information is gathered from Philippines public records and Government Data. We try to keep all information up to date.”<sup>34</sup>

Given these circumstances, PH-Check.com, as a PIC, has obligations under the DPA, its Implementing Rules and Regulations (IRR), and related NPC issuances.

The Commission also has the correlative duty to ensure that PICs, like PH-Check.com, comply with the law. This duty includes taking necessary steps to protect and uphold the rights of data subjects, such as the issuance of a CDO when needed.

Section 7(c) of the DPA provides for the power of the Commission to issue CDOs:

Section 7. *Functions of the National Privacy Commission.* – To administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection, there is hereby created an independent body to be known as the National Privacy Commission, which shall have the following functions:

xxx

(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.<sup>35</sup>

As part of its rule-making power and to flesh out its power to issue CDOs, the Commis-

30 Data Privacy Act of 2012, chapter I, § 3 (j) (2012).

31 Data Privacy Act of 2012, chapter I, § 3 (h) (2012).

32 Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p.3.

33 National Privacy Commission, Implementing Rules and Regulations of the Data Privacy Act of 2012, rule I, § 3 (m) (2016) (IRR of the DPA).

34 Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p.3.

35 Data Privacy Act of 2012, chapter II, § 7 (C) (2012).

sion issued NPC Circular No. 2020-02, also known as the Rules on the Issuance of Cease and Desist Orders (NPC Circular No. 20-02).

Rule II, Section 5 of the same Circular provides for the filing of a CDO Application:

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.<sup>36</sup>

The Commission finds that the CID is the proper party to file the CDO application since it conducted a *sua sponte* investigation in relation to PH-Check.com after receiving complaints endorsed by the DTI. The results of the investigation are documented in the CID's Initial Report, Supplemental Report, and Technical Report.

The CID provided the following arguments in its CDO Application: 1) PH-Check.com is doing some act or practice that is in violation of the DPA and its IRR,<sup>37</sup> 2) PH-Check.com is considered an "unknown [(PIC)]",<sup>38</sup> 3) PH-Check.com's act is detrimental to the public interest which would warrant a CDO to protect and preserve the data subjects' rights,<sup>39</sup> 4) unless restrained, PH-Check.com's existence "will cause grave and irreparable injury to the data subjects",<sup>40</sup> and 5) substantial evidence exists for the concurrence of all the grounds to issue a CDO.<sup>41</sup>

The CID in its Application alleged that the quantum of proof to warrant the issuance of a CDO is substantial evidence,<sup>42</sup> or "that amount of relevant evidence that a reasonable mind might accept as adequate to support a conclusion."<sup>43</sup>

Rule II, Section 4 of NPC Circular No. 20-02 provides for the grounds for the issuance of CDO:

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:

<sup>36</sup> Rules on the Issuance of Cease and Desist Order, rule II, § 5.

<sup>37</sup> Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p. 3.

<sup>38</sup> Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p.3.

<sup>39</sup> Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p. 6

<sup>40</sup> Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p. 7.

<sup>41</sup> Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at pp. 7-8.

<sup>42</sup> Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p. 6.

<sup>43</sup> De Jesus v. Guerrero III, G.R. No. 171491, 04 September 2009.

- 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.<sup>44</sup>

The Commission finds that the CDO against PH-Check.com be issued since the grounds provided in NPC Circular No. 2020-02 have been met.

*I. PH-Check.com is doing some act or practice in violation of Section 11 (General Data Privacy Principles) and Section 16 (Rights of the Data Subject) of the DPA.*

The CID argued that PH-Check.com does not adhere to the general data privacy principles in the DPA:

One of the means to show that a PIC complies with the data privacy principles is through the posting of a Privacy Notice that apprises the data subject on the collection, use, purpose, retention, disclosure, and disposal of personal data. The use of a [P]rivacy [N]otice is pursuant to the transparency principle of the DPA in the processing of personal data, which demands that data subjects are afforded a reasonable amount of information about the data processing system of a PIC in possession of their personal information. This is absent in this case.

It also appears that the purpose of Ph-Check.com for processing the scraped personal information is not clear. ‘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 requirement on legitimate purpose is thus not met.

On the matter regarding proportionality, ‘the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not be reasonably be fulfilled by other means.’ As discussed, there is nothing in the website to show the purposes in processing the scraped personal data. Hence, it could not be determined if the processing done by Ph-Check.com is proportionate to its purpose.

Based on the foregoing, it is apparent that Ph-check.com scrapes publicly available information from DTI BNRS, has no privacy policy sufficient to inform the data subjects of the processing of their personal information, has hidden the identity of

its owners or administrators, and has no means for data subjects to exercise their rights under the DPA. As such, it is evident that Phcheck.com is violating the general data privacy principles of transparency, legitimate purpose, and proportionality under Section 11 [of the DPA.]<sup>45</sup>

<sup>44</sup> National Privacy Commission, Rules on the Issuance of Cease and Desist Orders of the National Privacy Commission, NPC Circular No. 2020-02, rule II, § 4 (06 October 2020) (Rules on the Issuance of Cease and Desist Order).

<sup>45</sup> Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at pp. 4-5.

The CID also claimed that the rights of data subjects in Section 16 of the DPA are being violated, particularly the right to erasure:

As already complained by at least two affected data subjects, there is no means in the website for a data subject to request for removal of personal data or exercise any of the data subject rights. This is a patent disregard of Section 16 of the DPA.<sup>46</sup>

A PIC has the obligation to adhere to the DPA's general data privacy principles of transparency, legitimate purpose and proportionality.

Under Section 18 of the IRR of the DPA:

Section 18. Principles of Transparency, Legitimate Purpose and Proportionality. The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.

a. Transparency. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

b. Legitimate purpose. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

c. Proportionality. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.<sup>47</sup>

The CID's investigation revealed that there is no privacy notice on the website, and no other mechanism by which data subjects may be informed on how they will be able to exercise their data privacy rights.<sup>48</sup>

The website does not also provide who the owner, administrator, or Data Protection Officer is.<sup>49</sup> The CID attached in its Initial Report, a screenshot of the website <https://who.is/whois/ph-check.com> showing that PH-Check.com does not provide the contact information of the company or its owner and that the website does not contain any privacy notice.<sup>50</sup> These circumstances provide adequate bases to find that there is a violation of the transparency principle.

The purpose for gathering personal data from the DTI BNRS website is also unclear. To adhere to the legitimate purpose principle, it is required that the PIC actually declares and specifies its purpose which should not be contrary to law, morals or public policy.<sup>51</sup>

---

46 Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p. 6.

47 Data Privacy Act of 2012, chapter III, § 11.

48 IRR of the DPA, rule IV, § 18

49 Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p. 5.

50 Complaints and Investigation Division (CID) Initial Report dated 21 January 2022, Annex "J".

51 RR of the DPA, rule IV, § 18 (b).

Here, PHCheck.com provides no declared purpose other than merely stating that it provides information to the public about Philippine companies.<sup>52</sup>After a review of the evidence presented, the Commission finds that there is substantial evidence to issue the CDO. It has been established from the submissions that PH-Check.com scrapes the personal information from DTI BNRS<sup>53</sup> and no purpose for the same has been established in the website.<sup>54</sup>Moreover, it has been found that no available information as to the owner or administrator can be seen on the website based on the Initial Report of the CID.<sup>55</sup>

Other than the website itself and the fact that it contained scraped information from the DTI’s website, the CID did not find any other information. The Commission is constrained to find that there is insufficient evidence to determine whether the processing done was proportionate to any purpose of PH-Check.com.

There is also substantial evidence to find that the rights of the data subjects to be informed and erasure are being violated. The NPC, through the DTI, received complaints against PH-Check.com, requesting the latter to stop scraping the personal information and remove the personal data from the website.<sup>56</sup>Indeed, the data subjects’ right to information and the right to erasure are not being upheld since there is no privacy notice or available mechanism for data subjects to interact with the PIC for the effective exercise of their rights.

As to the right to information, it has already been established that PHCheck.com scrapes its information from the DTI website.<sup>57</sup> The data subjects were not informed that their personal information would be displayed and available on PH-Check’s website. The right to information of the data subject was not sustained by PH-Check.com for failure to post privacy notice and to furnish the data subjects with necessary information before the processing or at the next practical opportunity. As to the right to erasure, PH-Check’s website failed to provide the contact information of the owners/administrators in order for the data subject to request erasure of its data. Thus, the data subjects has no means to raise and request their right to erasure.

The non-adherence to the data subject’s right to information and erasure were expressed by KGU in her complaint before DTI when she stated that she “did not give permission for [her] information to be shared to third party websites and to be made available elsewhere.”<sup>58</sup> KGU also had to request the DTI for the removal of her personal data from PH-Check.com. This meant that PH-Check.com could not effectively facilitate her right to erasure.

Thus, the CDO Application provides substantial evidence for the existence of the first ground in that PH-Check.com is doing some act or practice in violation of the DPA, its IRR, and other related issuances.

---

52 Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p.3.

53 Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p.3.

54 Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p.5.

55 Complaints and Investigation Division (CID) Initial Report dated 21 January 2022 , Annex “J”.

56 Electronic mail dated 14 January 2022 of ASA; See Initial Report dated 21 January 2022 of the Complaints and Investigation Division, Annex “B”; Letter dated 07 February 2022 of KGU.

57 Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p. 3.

58 Letter dated 07 February 2022 of KGU, at p. 3.



*II. PH-Check.com's act or practice is detrimental to the public interest, and a CDO is necessary to preserve and protect the rights of the data subjects.*

The second ground is likewise present since the processing is detrimental to the public's interests, and a CDO is required for the preservation and protection of the rights of the data subjects.

There does not seem to be any public benefit in the duplication and disclosure of information, including personal data, in PH-Check.com. These information are already found in the DTI's BNRS website.

On the contrary, there are concrete harms that warrant the protection of the data subject. PH-Check.com allows anyone from the public to "edit" the information on the site. From the CID's investigation, the website contains blank fields pertaining to the address, phone number, and website or email.<sup>59</sup> Thus, anyone can enter information regarding these information without any security measure or verification on their accuracy. This may lead to either unauthorized, or even false, disclosure of details linked to the sole proprietor registered with the DTI through the BNRS.

The existence of a website that scrapes the data of sole proprietors and allows for an opportunity to provide false information does not serve the public's interest. There is substantial evidence to find that a CDO must be issued to preserve the rights of data subjects.

It has been established in the CID's Initial Report<sup>60</sup> and Supplemental Report<sup>61</sup> that PH-Check.com was scraping information from DTI's BNRS website.<sup>62</sup> Further, the website is not adherent to the data privacy principles since it does not contain any information as to its purpose in the processing of personal information, nor does it have any privacy notice to apprise the data subjects of their rights.<sup>63</sup> Lastly, since anyone can "edit" the information on the site, the public can be deceived as to the available information on PH-check.com's website.<sup>64</sup>

The continued processing of PH-check.com is detrimental to the public interest since making the personal information publicly available on its website without compliance with the DPA may be harmful to the data subjects.

*III. The commission or continuance of PH-Check.com's acts, unless restrained, will cause grave and irreparable injury to data subjects.*

On the third ground, the CID argued:

<sup>59</sup> Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p. 3.

<sup>60</sup> Complaints and Investigation Division (CID) Initial Report dated 21 January 2022.

<sup>61</sup> Supplemental Report dated 05 July 2022 of the Complaints and Investigation Division.

<sup>62</sup> Supplemental Report dated 05 July 2022 of the Complaints and Investigation Division, at p. 1.

<sup>63</sup> Complaints and Investigation Division (CID) Initial Report dated 21 January 2022, See: Annex "J".

<sup>64</sup> Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p. 3.

The Ph-Check.com website is still active as of this date and its continued existence poses a threat to the personal data collected that can be used for fraudulent means like identity theft, phishing, text blasting, marketing, or other unlawful purposes.

The fact that the website failed to disclose its identity and does not provide data subjects a means to exercise their rights provided under the DPA is proof that the collected personal information is exposed to acts beyond the knowledge and consent of the data subject.

To make matters worse, there is practically no means to hold anyone accountable for any damage done arising from PhCheck.com's processing of personal information. Ph-Check.com does not even reply to a Notice to Explain (NTE) issued by this Commission; how much more when it is to be held accountable for damages caused upon an affected data subject?

Allowing Ph-Check.com to continue its operations increases the risk of exposing the personal data to other grave and irreparable damage and/or injury.<sup>65</sup>

The Commission notes that the owner or administrator of PHCheck.com did not reply to the CID's Notice to Explain. There is also substantial evidence, as discussed, to show that the website's existence may be a vehicle for unlawful purposes, such as false information and identity theft.

It should be emphasized that even DTI itself disclaimed any connection or affiliation with the website. It "does not have an existing partnership or agreement with PH-Check.com, nor has DTI given permission to publish information such as Name, Status, Business Scope, Business Territory, etc. as well as the full name of the owner."<sup>66</sup>

Based on the evidence provided, there are several risks that may cause grave and irreparable injury to data subjects. First, as discussed, there is no apparent purpose for the collection of personal data. Second, there is no contact information of the website's data protection officer (DPO) or owner. Third, PH-Check.com was given an opportunity to explain why the person or entities should not be held liable for violating the DPA, but nevertheless failed to respond to the Notice to Explain by the Commission. Fourth, as discussed, the Commission cannot determine whether the processing complies with the general data privacy principles.

The circumstances point to a possible violation of the DPA, compounded with the fact that data subjects have no proper recourse to the PIC. Thus, the Commission must issue a CDO.

An essential purpose of the DPA is to protect and uphold the rights of the data subjects. Therefore, to avoid grave or irreparable injury to the affected data subjects, PH-Check.com should cease and desist from processing personal data on its website.

WHEREFORE, premises considered, PH-Check.com (<https://phcheck.com>) is hereby ordered to:

- 1) **CEASE AND DESIST** from the processing of personal data on its website, including the collection and display of personal data on its website, pursu-

<sup>65</sup> Application for Issuance of Cease and Desist Order dated 16 August 2022 of the Complaints and Investigation Division, at p. 7.

<sup>66</sup> Letter dated 08 February 2022 of the Department of Trade and Industry.

ant to Section 8 of NPC Circular No. 202002; and

2) **SUBMIT its COMMENT**, within ten (10) days from receipt of this Order, on the allegations in the attached Application for Issuances of Cease and Desist Order dated 16 August 2022, pursuant to Section 9 of NPC Circular No. 2020-02.

The **National Telecommunications Commission** is hereby instructed to take down the website of PH-Check.com immediately upon receipt of this Order.

The Cease and Desist Order shall be immediately executory and enforceable upon the receipt of this Order, through e-mail, by PHCheck.com.

**SO ORDERED.**

City of Pasay, Philippines.  
22 September 2022.

**SGD.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

I CONCUR:

**SGD.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

Copy furnished:

**THE OWNER/ADMINISTRATOR**

*Respondent*

PH-check.com

ph-check.com-owner-zjoj@customers.whoisprivacypcorp.com

ph-check.com-admin-tl17@customers.whoisprivacypcorp.com

ph-check.com-tech-3ysl@customers.whoisprivacypcorp.com

**PMA**

*Data Protection Officer*

Department of Trade and Industry

**NATIONAL TELECOMMUNICATIONS COMMISSION**

BIR Road, East Triangle, Diliman,

Quezon City, Metro Manila, Philippines

**COMPLAINTS AND INVESTIGATION DIVISION**

**ENFORCEMENT DIVISION**

**GENERAL RECORDS UNIT**

National Privacy Commission

## ***Address***

5th Floor Delegation Building  
PICC Complex, Roxas Boulevard

## ***Trunkline***

8234-2228

### **Local numbers**

Compliance - 118

Complaints - 114

Advisory opinions - 110

Other inquiries - 117

## ***Social media***

 [privacy.gov.ph](https://www.facebook.com/privacy.gov.ph)

 [privacy.gov.ph](https://www.instagram.com/privacy.gov.ph)

 [PrivacyPH](https://twitter.com/PrivacyPH)

## ***Website***

 [privacy.gov.ph](https://www.privacy.gov.ph)