NATIONAL PRIVACY COMMISSION

THE 2019 COMPENDIUM OF NPC ISSUANCES

NATIONAL PRIVACY COMMISSION

THE 2019 COMPENDIUM OF NPC ISSUANCES

PRIVACY COMMISSIONER'S MESSAGE

The National Privacy Commission annually releases a compendium of its guidance in the year that was to provide an easy reference to dedicated Data Protection Officers, privacy advocates, students and anyone interested in data protection issues and privacy governance.

The 2019 Compendium of Issuances compiles 46 Advisory Opinions, and 9 Commission-issued Orders.

The compedium is part of NPC's broader campaign to raise awareness on data privacy rights. An effort like this must be sustained amid the public's growing need to keep abreast with data privacy and protection policies and standards. This, as most of us now operate in environments that take steps toward full digitization and automation.

Guidance on the use of technology and data have intensified. This means greater safekeeping of personal data must be implemented. Indeed, if businesses and government agencies aim to establish with their stakeholders a relationship that is built on trust, these organizations must add another dimension to their core operations, and that is setting a policy regime that builds trust by promoting privacy and security of Filipinos.

While this compendium offers a glimpse of the concerns and issues that influenced our decision-making in 2019, it may also offer useful lessons on emerging trends that can help us anticipate challenges in the future.

More ambitiously, we hope that by offering this compendium, we can spark the interest and curiosity of many and eventually turn them into partner-advocates of personal data privacy rights.

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

TABLE OF CONTENTS

15 ADVISORY OPINION

248 DECISIONS

315 RESOLUTIONS

353 ORDER

NATIONAL
PRIVACY
COMMISSION

5th Floor Delegation Building, PICC Complex, Roxas Boulevard

NPC Trunk line No: 8234-2228
For registration & compliance concerns– 118
For complaints– 114
For advisory opinions– 110
For other inquiries– 117

ADVISORY OPINIONS

ADVISORY OPINION NO. 2018-032

26 November 2018

[redacted]

Re: PPP CENTER PRIVACY MANUAL

Dear [redacted],

We write in response to your letter request received by the National Privacy Commission (NPC) for the review of the Public-Private Partnership Center's (PPP Center) Privacy Manual in relation to its compliance with the Data Privacy Act of 2012 (DPA)[1] and its Implementing Rules and Regulations (IRR).[2] A copy of the draft Privacy Manual provided is attached herewith as Annex "A."

Please see comments below on the draft PPP Center Privacy Manual:

PPP Center Privacy Manual	Remarks
Privacy Manual Logo	As the Privacy Manual pertains solely to the PPP Center's privacy policies, kindly remove the NPC seal and retain the PPP seal.
I. Introduction	It should be "Data Privacy Act of 2012".

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

II. Definition of Terms "Data Protection Core Team or DPCT – refers to the team that would assist the Data Privacy Officer..."	DPO pertains to the *Data Protection Officer.*
III. Scope **Third paragraph**: "... as well as the Personal Data under the control or custody of a private entity that is being shared with or transferred to a Government Agency, shall be protected in compliance with the Act."	Please clarify. Perhaps the intention was to refer to the personal data being with or transferred to the PPP Center shared by a private entity and not just any other Government Agency. In that case, the inclusion of such in the scope is accurate since the personal data will then be under the custody of the PPP Center thus calling for the application of the Privacy Manual.
Fourth paragraph: "The Center may use this Privacy Manual to issue and implement more detailed policies and procedures, which reflect its specific operating requirements."	We suggest to include the term "technical": "The Center may use this Privacy Manual to issue and implement more detailed policies and procedures, which reflect its specific **TECHNICAL AND** operating requirements."
IV. Processing of Personal Data	As a matter of form, we suggest to remove the examples in the parentheses for the subsections as it was merely for drafting guidance.

A. Collection	Please clarify as it seems that based on the current provision, the collection of all personal data will be through the consent form (Annex 1). Note that there will be collection and processing of personal data which is not based on consent, i.e. fulfillment of a contract, processing provided for by existing laws and regulations, among others. Hence, it advisable to provide for the other modes and basis for collecting personal data.
B. Use "Personal Data collected shall be used by the Center for identification, documentation and other legal purposes."	"Other legal purposes" is vague. The DPA mandates that the processing of data shall have a specific and defined purpose. Expound or enumerate the specific uses of the data collected from guests, employees of the PPP Center, etc.

C. Storage, Retention and Destruction "All information gathered shall not be retained for a period longer than one (1) year, unless advised otherwise by the DPO."	Note that there are existing rules and regulations governing the retention period of certain records, i.e. tax purposes, Republic Act No. 9470 (National Archives of the Philippines Act of 2007), etc. Hence, it may be advisable to include a statement that the general rule for the retention period is one (1) year, subject to existing laws, rules and regulations on retention of specific records and documents, and as may be otherwise advised by the DPO in specific instances.
V. Control Framework for Data Protection **B. Physical Measures** **3. Encryption of Personal Data digitally processed** "The CBKMS shall develop a password policy that will be enforced through a system management tool."	Please define what CBKMS is.
B. Physical Measures **8. Retention and disposal procedure**	See comments above on retention.

C. Technical Measures "Each PIC and PIP must implement technical security measures..."	The PIC must pertain to the PPP Center as the PIC in this manual. Thus, it may be rephrased as "The Center shall implement technical security measures..." Should the PPP Center mean that it has PIPs under its control, please specify.
VI. Breach and Security Incidents "Every PIC or PIP must develop and implement policies and procedures..."	Same comment as above.
2. Measures to prevent and minimize occurrence of breach and security incidents "... In particular, the DPO shall monitor the compliance of the Personal Information Processors (PIP) and Personal Information Controllers (PIC) with the DPA."	Same comment as above. Rephrase to: "... the DPO shall monitor the compliance of the Center and its PIPs with the DPA."
5. Documentation and reporting procedure of security incidents or a Personal Data breach "The DPCT shall ensure proper data breach and security incident management by the PIPs and PICs..."	Same comment as above. Rephrase to: "The DPCT shall ensure proper data breach and security incident management by the Center...." Should the PPP Center mean that it has PIPs under its control, please specify so.

VII. Inquiries and Complaints "Every Data Subject has the right to reasonable access to his or her Personal Data being processed by the Personal Information Controller or Personal Information Processor."	Same comment as above. Rephrase to: "Every Data Subject has the right to reasonable access to his or her Personal Data being processed by the Center."

OTHER COMMENTS:

1. Annex 1 – Consent Form

   Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. There is a need to revise this form as consent has to be specific in relation to a particular processing of personal data.

   We reiterate that there are lawful processing activities that is not based on consent. Please refer to Sections 12 and 13 of the DPA for the criteria for lawful processing of personal and sensitive personal information.

2. Annex 2 – Inquiry Summary Form

   As stated in the form, it may be submitted via fax, courier or hard copy mail.

   Please note that pursuant to Section 28 of NPC Circular No. 16-01 - Security of Personal Data in Government Agencies, facsimile technology shall not be used for transmitting documents containing personal data. Hence, the PPP Center should consider revising the method of transmitting Annex 2

Also, the terms *"Data Privacy Officer"* and "*Data Protection Officer"* were used in this form. Please choose the appropriate nomenclature and be consistent in all documentation.

3. Annex 4 – Access and/or Alteration Request Form

   On Section 7 – Disclaimer, please correct the title of the law from Data Protection Act of 2012 to Data Privacy Act of 2012.

4. If you have additional questions or require further clarification, please contact the NPC Privacy Policy Office at 02-510-7836.

For your information.

Very truly yours,

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

Noted by:

(Sgd.) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

ADVISORY OPINION NO. 2018-033

26 November 2018

[redacted]

Re: DATA SHARING, CONSENT, AND COMPLIANCE WITH THE DATA PRIVACY ACT OF 2012

Dear [redacted]

This is in response to your request received by the National Privacy Commission (NPC) concerning various inquiries and clarifications regarding Republic Act No. 10173,[1] known as the Data Privacy Act of 2012 (DPA), particularly, the following:

1. If two PICs agree to share data with a data sharing agreement signed stating that compliance to the Data Privacy Act will be separate responsibilities, will both PICs be held responsible for a violation committed by only one of them if violation involves the shared data (e.g., non-encryption, processing without consent)?
2. Is there any standard as to how a recipient of personal data will ensure that the data to be received is being shared with consent from the data subject? Is a certification/ contract stating that consent from data subjects were obtained sufficient?
3. Is there a benefit in obtaining new consent via SMS or other means of communication (purpose is processing with another PIC/PIP) if the same data subject has

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

previously signed a consent form for the same purpose? Is there any timeline on the validity of a signed consent if nothing is stated in the consent form? As context to the above, a data partner of the company sends SMS opt-in confirmation to potential clients before our company's loan approval. The SMS asks the data subject whether he consents to data partner giving its score to HCPH based on its transaction data with Company A (not the data partner). These data subjects have already signed the HCPH consent form where it states HCPH may collect data from described third-parties.

4. In the context of mobile operators sending SMS messages to its subscribers with direct marketing offers for third party products and services, it is understood that prior consent from the subscribers is required. What practical methods/channels is considered acceptable for obtaining such consent from the existing subscriber base of such mobile operators?

We provide the following clarifications:

Data sharing and compliance with the DPA

To clarify, all personal information controllers (PICs) and personal information processors (PIPs) are mandated to comply with the provisions of the DPA, its Implementing Rules and Regulations (IRR) and issuances of the NPC.

PICs that share personal data under a data sharing agreement (DSA) are mandated to put in place adequate safeguards for data privacy and security in compliance with applicable laws and regulations. The DSA should include a general description of the security measures that will ensure the protection of the personal data of data subjects. The DSA, considering its terms, allows PICs to use contractual and reasonable means to provide safeguards for data protection to the personal data being shared.

Where a PIC fails to put in place the security measures required by law, regulations and the DSA, the said PIC may be solely accountable in the absence of fault or negligence on the other PIC. If no security measures are put in place by both parties or the DSA fails to provide

for the same, both parties may be held accountable. Nonetheless, the determination of liability, if any, will be based on the particular facts and circumstances of the case.

Data sharing and consent of the data subject

In relation to data sharing arrangement, the DSA or the pertinent contract may stipulate such fact or guarantee that the PIC sharing the personal data has collected or processed such on the basis of any of the criteria for lawful processing of personal and sensitive personal information under Sections 12 and 13 of the DPA, and that the data subject consented to the data sharing, unless consent is not required for the lawful processing of personal data.

Consent

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

From the definition provided above, it is clear that consent must be evidenced by written, electronic, or recorded means.[2] Any of the three (3) formats provided may be adopted by a PIC. Nonetheless, it is worth emphasizing that, regardless of the format of the consent given by the data subject, it must be freely given, specific, and informed.[3]

In line with the foregoing discussion, implied, implicit or negative consent is not recognized under the law.

Further, as to whether there is a timeline on the validity of a signed consent if nothing is stated in the consent form, the IRR states that when consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose.[4] The time-bound element does not necessarily mean that a specific date or period of time has to be declared. Thus, for instance, declaring that processing will be carried out for the duration of a contract between the PIC and the data subject may be a valid stipulation.

[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §3(c).
[3] Id.
[4] Id. § 19 (a) (1).

Also, as long as the purpose, scope, method and extent of the processing remains to be the same as that disclosed to the data subject when consent was given, the consent remains to be valid.

Where applicable, such as in cases where the period of processing can be reasonably ascertained at the time of collection, a PIC may specifically provide for the period of validity of a consent obtained from a data subject. The limitation merely emphasizes that consent cannot be overly broad and perpetual for this would undermine the very concept of consent as defined in the law.

We understand that as far as HCPH is concerned, the basis of processing personal data would be the consent of the data subject and/or the contractual relation with the data subject or taking steps at the request of the data subject prior to entering into a contract.

It must be clearly conveyed to the data subject that prior to the loan approval, HCPH would be conducting due diligence and/or further investigation on the applicant-data subject, which will involve collecting further information from third-party sources, and the data subject must consent to the same. Further, these third-party sources must be identified, and the data subject must authorize them to share information with HCPH. Finally, the data subject has to be notified of the transfer of transaction data from Company A to the data partner, the processing done by the data partner and the relationship between the data partner and HCPH, and data subject has to specifically consent and authorize such transfer and processing.

Direct marketing through SMS messages and consent of the data subject

You mentioned that mobile operators would send direct marketing offers for third party products and services via SMS messages to its existing subscriber base. In relation to the same, you inquired on the acceptable practical methods or channels for obtaining consent from the said subscribers.

If consent is the appropriate basis for processing made by the said mobile operators, it is possible for them to obtain consent through an SMS request. For postpaid subscribers, there is an option of sending hardcopy consent forms. Lastly, for those with online accounts with these mobile operators, sending consent forms online through their

respective account dashboards or email may also be considered.

The mobile operators should come up with the most efficient and effective way of obtaining consent, taking into consideration the type of processing they will do.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

ADVISORY OPINION NO. 2018-036

23 July 2018

[redacted]

RE: DATA SHARING WITH THE MANILA INTERNATIONAL AIRPORT AUTHORITY (MIAA)

Dear [redacted],

We write in response to your letter dated 6 June 2018 requesting for clarification regarding data sharing under Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA). Specifically, you seek to clarify whether air carriers may transfer personal information of ticket holders for the purpose of refunding terminal fees, without securing ticket holders' consent and without executing a data sharing agreement with the Manila International Airport Authority (MIAA).

We understand that since August 2012, members of the Air Carriers Association of the Philippines (ACAP), namely: Air Philippines Corporation (PAL Express), Cebgo, Inc. (Cebgo), Cebu Air, Inc. (Cebu Pacific), Philippine Airlines, Inc. (PAL), and Philippines AirAsia, Inc. (AirAsia), have been collecting terminal fees directly from prospective passengers for their flights from the Ninoy Aquino International Airport.

The carriers then remit the collected terminal fees to the MIAA after the passengers have taken their flights. The carriers submit the following to MIAA:

1. List of flights covered;
2. Number of passengers for each flight; and

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

3. Amount of terminal fees collected.

Thus, under the current system, carriers do not provide any personal information to the MIAA.

MIAA is currently looking into a possible transfer from the carriers to MIAA of the terminal fees collected, including unused and unrefunded fees, with the intention to refunding the same to the ticket holders unable to take their flights. This proposed system will necessarily entail the transfer of personal information of ticket holders from the carriers to MIAA.

Data Sharing

The Implementing Rules and Regulations (IRR) of the DPA defines data sharing as the disclosure or transfer to a third party of personal data under the control or custody of a personal information controller.[2]

A data sharing agreement (DSA) refers to a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more personal information controllers.[3]

NPC Circular No. 16-02 sets out the guidelines for data sharing and DSAs involving government agencies. The circular covers personal data under the control or custody of a private entity that is being shared with or transferred to a government agency, and vice versa.[4] Furthermore, the issuance states that a DSA is required when personal data is shared or transferred for the purpose of performing a public function or providing of a public service.[5]

As mentioned above, the contemplated transfer of terminal fees collected, including unused and unrefunded fees for refunding the ticket holders, to MIAA, will necessarily entail the transfer of personal data of each ticket holder (i.e., names, birthdates, contact details, bank details, credit card details, flight details, other personal information) to MIAA.

[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §3(f) (2016).
[3] NPC Circular No. 16-02, §3(E)
[4] Id., §2.
[5] Id., §1.

Considering the foregoing, the contemplated transfer of collected fees and personal data from the air carriers to MIAA falls squarely under the meaning of data sharing. Thus, a data sharing agreement is required.

Subject to the separate determination of whether this proposed transfer of responsibility in refunding terminal fees to the MIAA is operationally feasible, it is recommended that an amendment of the existing Memorandum of Agreement between MIAA and the air carriers regarding the Passenger Service Charge (PSC) be made to include the required contents of a DSA pursuant to NPC Circular No. 16-02, and incorporate the data privacy principles, enforcement of the rights of data subjects, and implementation of appropriate security measures.[6]

Furthermore, it should be noted that bookings of ticket holders prior to the effectivity of the DPA is still covered by the DPA. As we understand, the air carriers still store and retain personal information in relation to the said bookings and transfer thereof is yet to be done. The storage, retention, and transfer thereof are considered processing[7] under the DPA and such processing is still ongoing until the present. As such, the DPA applies.

Consent of ticket holders to the data sharing

NPC Circular No. 16-02 provides that the consent of the data subjects to the data sharing is required except when such consent is not required for lawful processing[8] of personal data.[9]

Section 5 of Executive Order No. 903[10] states the following powers and functions of MIAA, among others:

- To control, supervise, construct, maintain, operate and provide such facilities or services as shall be necessary for the efficient functioning of the Airport;
- To promulgate rules and regulations governing the

[6] Id., §6.
[7] Republic Act No. 10173, § 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.
[8] See: Republic Act No. 10173, §12 and 13.
[9] See: NPC Circular No. 16-02, §4.
[10] Executive Order No. 903, Providing for a Revision of Executive Order No. 778 Creating the Manila International Airport Authority, Transferring Existing Assets of the Manila International Airport to the Authority, and Vesting the Authority with Power to Administer and Operate the Manila International Airport (July 21, 1983).

planning, development, maintenance, operation and improvement of the Airport and to control and/or supervise as may be necessary the construction of any structure or the rendition of any service within the Airport;

- To perform such other acts and transact such other business, directly or indirectly necessary, incidental or conducive to the attainment of the purposes and objectives of the Authority, including the adoption of necessary measures to remedy congestion in the airport;

As stated in MIAA Memorandum Circular No. 06, series of 2017, the refund of terminal fees for unused tickets is anchored on the abovementioned powers and functions of MIAA. Thus, the data sharing is considered necessary for compliance with a legal obligation to which the personal information controller is subject and is pursuant to existing laws and regulations. Considering the foregoing, the data sharing agreement may proceed without the need to obtain the consent of ticketholders.

Nevertheless, the ticket holders should be duly informed that their personal information will be shared with the MIAA for purposes of refunding of the terminal fees, pursuant to the right of data subjects to be informed of the processing of their personal information.[11]

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[11] See: Republic Act No. 10173, §16(a).

ADVISORY OPINION NO. 2018-037

8 August 2018

[redacted]

RE: APPLICABILITY OF THE DATA PRIVACY ACT OF 2012 TO PHYSICAL OR ONLINE ARCHIVES AND LIBRARIES

Dear [redacted],

We write in response to your inquiry received by the National Privacy Commission (NPC) regarding the applicability of Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA), to physical or online archives and libraries. Particularly, you are inquiring whether the DPA applies to access to archival records which contain information of deceased individuals as well as church records used for historical research.

Scope of the DPA

At the outset, there is no conflict between the DPA and Republic Act No. 9470[2] or the National Archives of the Philippines Act of 2007 (NAP). It should be noted that the DPA has the twin task of protecting the fundamental human right of privacy and ensuring the free flow of information to promote innovation and growth.[3] Thus, the law will not operate to curtail the applicability of laws and regulations relative to archives and libraries.

As such, the pertinent provisions of the NAP will primarily apply as to the management and administration of all public records with archival value, held by either government offices or private collections, for the protection of public documents and records for the preservation of

[1] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission and for other Purposes [DATA PRIVACY ACT OF 2012], Republic Act No. 10173 (2012).
[2] An Act to Strengthen the System of Management and Administration of Archival Records, Establishing for the Purpose the National Archives of the Philippines, and for other Purposes [NATIONAL ARCHIVES OF THE PHILIPPINES ACT OF 2007], Republic Act No. 9470 (2007).
[3] Republic Act No. 10173, §2

the country's cultural heritage and history.

Nevertheless, when libraries and archives process personal information, the DPA will apply. As stated in Section 4 of the DPA, it applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. Processing has a very broad definition and includes essentially anything which one can do with personal information, including, but not limited to its collection, storage, use, retrieval, disclosure, and disposal.[4]

In this regard, the DPA, its IRR, and other related issuances of the NPC shall apply to archives and libraries when they use, store and provide access to archival records which contain personal information.

Libraries and archives are then obliged to comply with the provisions of the DPA, its IRR and other NPC issuances that are relevant to their operations and to the nature of information that they are processing. They must adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.[5] Libraries and archives are also mandated to uphold the rights of the data subjects[6] and implement security measures for the protection of personal data.[7]
Processing for historical research purposes

As to historical research, it is important to note that personal information processed for research purposes is outside of the scope of the DPA.[8] The same is reiterated in the IRR, which further states that the Act shall not apply to personal information processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations or ethical standards.[9] This encompasses access to archival records and church records that may contain personal information for historical research.

This exemption, however, applies only to the minimum extent necessary to achieve the specific purpose, function, or activity. Also, this entails the concomitant responsibility of ensuring that appropriate organizational, physical and technical security measures are in place to protect the personal data being processed for historical research purposes.

[4] See: Republic Act No. 10173, §3(j).
[5] Republic Act No. 10173, §11.
[6] Id., §16
[7] Id., §20
[8] Id., §4(d).
[9] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §5(c) (2016).

Although the consent of the data subjects may not be required in certain instances, the person or organization conducting the research must recognize the rights of the data subjects, including the right to be informed, among others.[10] The data subjects must be aware of the nature of the processing activities, the purpose of processing, the retention period of personal data and the enforcement of their rights.[11]

Likewise, Section 11(f) of the DPA provides that personal information must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed, provided that personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law, may be stored for longer periods.

We note also that pursuant to the EU General Data Protection Regulation, the processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected.[12] Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is considered to be processing that is lawful and compatible to the original purpose for which such information were collected or processed.[13]

Further, the law does not prescribe a specific retention period, but rather, applies the laws, rules, or regulations pertinent to a specific industry or sector. In the absence of such, retention of personal data shall only be for as long as necessary for the fulfillment of the declared, specified, and legitimate purpose.[14]

These provisions should complement the NAP specifically on provisions applicable to records stored with permanent and enduring archival value. Thus, libraries and archives should strive to strike a balance in order to determine on a case-to-case basis whether access to archival records containing personal information for historical research meets both the requirements of the NAP and those of the DPA.

[10] Maldoff, Gabe. How GDPR changes the rules for research, available at https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/ (last accessed 16 July 2018).
[11] Id.
[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [EU GENERAL DATA PROTECTION REGULATION], Recital 50 (2016).
[13] Id.
[14] See: Republic Act No. 10173, §11(e).

Deceased individuals

While the DPA does not explicitly provide for its applicability on personal information of deceased individuals, Section 17 thereof specifically grants the lawful heirs and assigns of the data subject the right to invoke the rights of the data subject at any time after death or when the data subject is incapacitated or incapable of exercising his or her rights. Hence, when personal data of deceased individuals are processed, they are still considered as data subjects and the lawful heirs and assigns may exercise the rights of the deceased as a data subject.

Consequently, processing of personal information of deceased individuals requires the concomitant responsibility to observe general data privacy principles of transparency, legitimate purpose, and proportionality, as well as the implementation of appropriate security measures as required by the DPA. Note, however, considering the foregoing discussion on processing for historical research, personal information of deceased individuals processed for research purposes may be exempt from the coverage of the DPA.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2018-075

8 November 2018

[redacted]

Re: BARANGAY TANYAG ORDINANCE NO. 03 "ORDINANSANG NAG-AATAS SA LAHAT NG MAY-ARI NG APARTMENT, BAHAY-PAUPAHAN, PAUPAHANG KUWARTO AT LAHAT NG URI NG PAUPAHAN PARA SA PANINIRAHANG PANG-INDIBIDWAL, PAMPAMILYA AT PANGKOMERSYAL NA IPAREHISTRO SA TANGGAPAN NG BARANGAY TANYAG ANG LAHAT NG NANINIRAHAN SA KANILANG PAUPAHAN AT ANG PAGTATAKDA NG KAUKULANG MULTA SA LALABAG DITO."

Dear [redacted],

We write in response to your letter seeking clarification regarding the Paupahan Form (Form) required by Barangay Bagong Tanyag, Taguig City in accordance with Barangay Ordinance No. 03[1] on the registration of tenants of leased residential spaces as a pre-requisite for the issuance of Barangay Clearance for Business Permit and the renewal thereof.

As we understand, you are inquiring whether the Form complies with the provisions of the Data Privacy Act of 2012 (DPA).[2] Particularly, you raised the following questions:

1. Whether the Form is valid when it does not have a clear provision stating the specific purpose of collecting the information;

[1] Barangay Tanyag, Ordinansang Nag-Aatas Sa Lahat Ng May-Ari Ng Apartment, Bahay-Paupahan, Paupahang Kuwarto At Lahat Ng Uri Ng Paupahan Para Sa Paninirahang Pang-Indibidwal, Pampamilya At Pangkomersyal Na Iparehistro Sa Tanggapan Ng Barangay Tanyag Ang Lahat Ng Naninirahan Sa Kanilang Paupahan At Ang Pagtatakda Ng Kaukulang Multa Sa Lalabag Dito, Ordinance No. 03 series of 2017.

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

2. Whether the Form collects an excessive amount of personal information;
3. Whether the Form is valid when it does not contain any statement on the protection of personal information collected;
4. Whether a point person who will take charge in the safekeeping of the data and the liability in case of a data breach must be designated;
5. Whether the barangay can compel its constituents to sign the Form and whether it can sanction them for not following the ordinance; and
6. Whether residents may refuse to fill up the Form due to the barangay's lack of security measures to protect their personal information.

An ordinance enjoys the presumption of validity and can only be nullified in a direct action assailing its validity or constitutionality.[3] Under this presumption, Barangay Bagong Tanyag can mandate its constituents to comply with the provisions of Ordinance No. 03 and provide penalties for non-compliance.

In collecting personal data from its constituents, the barangay now assumes the role of a personal information controller (PIC),[4] and thus becomes subject to the DPA and the general data privacy principles of transparency, legitimate purpose, and proportionality. Likewise, they should implement security measures to maintain the confidentiality, integrity and availability of personal data, and ensure that the rights of data subjects are protected in the implementation of this ordinance.

Transparency

The principle of transparency states 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 the personal information controller, and the rights of the data subjects and how these can be exercised.[5] The purpose of the data collection need not be included in the form itself, provided that the purpose is shared with the data subjects through other means

[3] Social Justice Society v. Atienza, Jr., G.R No. 156052 (13 February 2008).
[4] Data Privacy Act of 2012, § 3 (h).
[5] See: Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (a) (2016).

that are equally effective.

In this case, the ordinance states that the purpose for the submission of the list of tenants is for the maintenance of peace and order in the barangay and the effective management of its constituents. Likewise, it provides an exhaustive list of personal information required to be submitted. The constituents were, however, not informed as to the extent of processing, the risks and safeguards involved, and their rights as data subjects and how they may be exercised. Both the ordinance and the form does not provide for such information. For instance, it must be clear to the data subjects how and to what extent does the barangay intend to use their personal data for maintenance of peace and order, including whether such personal data will be shared with any other government or private entities.

Legitimate purpose

The principle of legitimate purpose[6] states the processing of personal information shall be compatible with a declared and specified purpose, which is not contrary to law, morals or public policy. With Barangay Tanyag, the basis for processing is the mandate of cities and barangays to enact measures on how to protect its territorial jurisdiction and maintain peace and order.[7] Thus, as long as the barangay is able to provide its legal basis, and has ensured that its purpose is consistent with its statutory or constitutional mandate, then it may be considered as within its rights to issue an ordinance like Ordinance No. 03.

Proportionality

Even with a legitimate purpose, the authority of the barangay to process personal data is limited and not absolute. The principle of proportionality states that the processing of information shall be adequate, relevant, suitable, necessary and not excessive in relation to a declared and specified purpose.[8] Under this principle, there is a need to examine whether every item of personal data required to be submitted is necessary and relevant to the stated purpose. It must be emphasized that personal data must only be processed if the purpose of processing could not be reasonably fulfilled by other means. For instance, the barangay may consider collecting "number

[6] IRR of DPA, § 18 (b) (2016).
[7] See: An Act Providing For A Local Government Code Of 1991 [Local Government Code of 1991], Republic Act No. 7160 § 16 (1991).
[8] Id. § 18 (c).

of occupants - adults and children" instead of collecting the names of all the occupants, to fulfill the purpose of determining the total number of constituents covered by the jurisdiction of the barangay.

This means that the barangay should be able to readily explain why a particular item of personal data is collected and the why its processing is necessary to achieve the objectives of the ordinance. The barangay should strongly consider whether collecting statistical or aggregate data is already sufficient to fulfill these objectives.

In addition, the data collected must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed, unless the personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods. In either case, the DPA requires that adequate safeguards are guaranteed by said laws authorizing their processing.[9] No such safeguards exist in the ordinance, such as provisions on retention periods and records disposal.

Data Subject Rights

As the barangay is now a PIC, it 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.

The barangay should have a person in charge of ensuring that the barangay complies with such obligation. The barangay should have a designated Data Protection Officer (DPO). They may instead appoint a Compliance Officer for Privacy (COP), provided that the latter shall be under the supervision of the Data Protection Officer (DPO) of the corresponding province, city, or municipality that the barangay is a part of. For further guidance, it would be helpful to look into NPC Circular No. 2016-01 which provides guidelines on security of personal information in government agencies, and NPC Advisory 2017-01 on the designation of a Data Protection Officer.

On the part of data subjects, those with concerns about how their personal data is handled under this ordinance may refer the matter

[9] DPA § 11 (f)

to the Data Protection Officer of the barangay, or if there is no such officer in the barangay, to the Data Protection Officer of the City of Taguig. The barangay should have procedures in place to ensure that data subjects can exercise their rights.

The risk involved in the collection of personal information is a valid concern, particularly with the amount of data collected by the barangay and the lack of information on existing safeguards for personal data protection in the provisions of the ordinance.

Upon complaint of a data subject, or the discovery of a data breach occurring due to negligence, a personal information controller or its responsible officials may be subject to penalties specified in Chapter VII (Sections 25-37) of the DPA should they be found to have failed to comply with provisions of the law and to take adequate precautions to protect personal information they collect and hold.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-001[1]

3 January 2019

[redacted]

Re: PRIVATE DETECTIVE SERVICES

Dear [redacted],

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC). You disclosed that Eyespy Detectives and Investigators Co. (Eyespy) is a duly registered partnership with the Securities and Exchange Commission, and a duly registered and licensed to operate detective agency with the Supervisory Office of Security and Investigation Agencies of the Philippine National Police, pursuant to Republic Act No. 5487, as amended,[2] or the Private Security Agency Law.

Eyespy offers several services including background checks or investigation, records verification, property checks or verification, surveillance operation, service of summons (from foreign courts), assistance in locating missing persons, insurance claim investigation or verification, polygraph examination and lifestyle check upon the request of clients.

As stated in your letter, Eyespy has adopted measures to ensure that client requests for services are supported by legal and justifiable purposes, such as gathering of evidence for a pending case of or a suit to be instituted by the client. You further stated that there are, however, instances where services, such as surveillance operations

[1] Tags: Private detective services, background investigation, right to privacy.
[2] An Act to Regulate the Organization and Operation of Private Detective, Watchmen or Security Guards Agencies [Private Security Agency Law], Republic Act No. 5487, as amended (1969).

and background checks, are requested for the sole purpose of enabling the client to make better personal decisions.

The conduct of a discreet surveillance operation, background check or investigation, or record verification are often requested: a) by a party in a dating relationship, on their partner; b) by a foreigner, on his Filipino fiancée to determine if she is indeed single, has the capacity to marry and without derogatory record; and c) by parents, on the girlfriend, boyfriend, fiancé or fiancée of their child.

You now wish to clarify whether the abovementioned activities of Eyespy are permissible by the provisions of Republic Act No. 10173,[3] or the Data Privacy Act of 2012 (DPA), particularly on the processing of sensitive personal information of individuals in cases when the request is not pursuant to a pending case or in preparation for the filing of one.

Activities in Private Investigation Subject to the DPA

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.[4]

Moreover, the law defines personal information as information which the identity of 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 and individual.[5] On the other hand, what is considered as sensitive personal information is clearly enumerated as:

- About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- 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

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

person, the disposal of such proceedings, or the sentence of any court in such proceedings;

- Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licenses or its denials, suspension or revocation, and tax returns; and
- Specifically established by an executive order or an act of Congress to be kept classified.[6]

While private investigation is a duly recognized field, there being the Private Security Agency Law, the activities and services involved therein, such as records verification on birth, marital status and education, would necessarily involve the processing of personal information and sensitive personal information, thus subject to the provisions of the DPA. For processing of personal information, the Section 12 of the law provides the following conditions for lawful processing:

(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 an freedoms of the data subject which require protection under the Philippine Constitution.

[6] Id. § 3 (j).

Meanwhile, under the Section 13 of the law, the processing of sensitive personal information is prohibited unless specific conditions under the law are met:

(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.

Furthermore, the general data privacy principles of transparency, legitimate purpose, and proportionality must always be adhered to in the processing of personal data.

Expectation of privacy

On another perspective, while the 1987 Philippine Constitution guards the right to be let alone of individuals against unreasonable State intrusion, the Civil Code of the Philippines holds liable individuals for violating another person's right to privacy. The Code states:

> 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.[7]

Our Supreme Court had the chance to delve on the right to privacy in relation to the abovementioned provision and held:

> 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."
>
> XXX XXX XXX

[7] An Act to Ordain and Institute the Civil Code of the Philippines [CIVIL CODE OF THE PHILIPPINES], Republic Act No. 386, art. 29 (1949).

> Thus, an individual's right to privacy under Article 26(1) of the Civil Code should not be confined to his house or residence as it may extend to places where he has the right to exclude the public or deny them access. The phrase "prying into the privacy of another's residence," therefore, covers places, locations, or even situations which an individual considers as private. And as long as his right is recognized by society, other individuals may not infringe on his right to privacy.[8]

Furthermore, in our Advisory Opinion No. 2018-090 – Data Privacy and Office-Issued Mobile Devices, we discussed on the expectation of privacy and how the passage of the DPA affects it, to wit:

> The ruling in Ople v. Torres also expounded on the "reasonable expectation of privacy" test in ascertaining whether there is a violation of the right to privacy. This test determines whether a person has a reasonable or objective expectation of privacy and whether the expectation has been violated. The reasonableness of a person's expectation of privacy depends on a two-part test:
>
> (1) whether by his conduct, the individual has exhibited an expectation of privacy; and
> (2) whether this expectation is one that society recognizes as reasonable.
>
> The factual circumstances of the case determine the reasonableness of the expectation. Similarly, customs, community norms, and practices may, therefore, limit or extend an individual's reasonable expectation of privacy. The reasonableness of a person's expectation of privacy must then be determined on a case-to-case basis.
>
> XXX XXX XXX
>
> It is noteworthy to mention that the reasonable expectation test was used at a time when there were no laws on data protection and informational privacy.
>
> XXX XXX XXX
>
> Yet, with the DPA now in place, the reasonable expectation test should be revisited and interpreted in the context of the law.

[8] Spouses Bill and Victoria Hing v. Alexander Choachuy Sr. and Allan Choachuy, G.R. No. 179736, June 26, 2013. Citations omitted.

> 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.[9]

General guidelines to consider

In your letter, it is unclear what means and methods are used by Eyespy in the conduct of its services. Thus, the NPC is unable to make a categorical determination on the legality of its activities as circumstances may also differ.

However, in the conduct of the contemplated services, Eyespy may examine its activities through the framework below:

- The type of personal data is involved, i.e. personal information and/or sensitive or privileged personal information;
- The lawful basis to process such personal data given the situation, if any (Eyespy may look into Sections 12 (b) and (f) and/or 13(f) of the DPA); and
- The means and methods used, taking into consideration proportionality and expectation of privacy.

Given the foregoing discussion, it is also for Eyespy to determine whether its acts, such as records verification and background investigation, would: (a) constitute a violation of an individual's expectation of privacy, and (b) violate existing laws, including the DPA.

It is worth noting that the DPA dictates its provisions shall be liberally interpreted in a manner mindful of the rights and interests of the data subject.[10] Thus, it is the burden of Eyespy to ensure that any processing of personal data is in accordance with the law.

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

[9] National Privacy Commission, NPC Advisory Opinion No. 2018 – 090 (Nov. 28, 2018). Citations omitted
[10] Data Privacy Act of 2012, § 38.

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-002[1]

4 January 2019

[redacted]

Re: DISCLOSURE OF IDENTITY IN CONFIDENTIAL REPORTS AND INVESTIGATIONS

Dear [redacted],

We write in response to your inquiry on whether the management of your agency violated your rights or existing laws when they maliciously disclosed your identity to the persons involved in the alleged corruption in your office, which you have earlier reported through a letter captioned "CONFIDENTIAL REPORTS."

The Data Privacy Act of 2012 (DPA)[2] provides the criteria for lawful processing of personal information and sensitive personal information in Sections 12 and 13, respectively. Disclosure of personal data may be permitted where one of the criteria provided in said sections is met. In this instance, given the limited information, it is difficult to determine whether such lawful criteria exists.

Hence, the determination of the propriety of the disclosure of your identity would have to depend on the circumstances of the particular case, including information on the internal rules and regulations of your agency and that of the Presidential Complaint Center on the handling of corruption accusations. Laws and regulations other than the DPA would also be applicable.

Should you wish to pursue a complaint with the National Privacy Commission, you may compile all the supporting documents and send the complaint to complaints@privacy.gov.ph. For further information,

[1] Tags: disclosure; confidential report; criteria for lawful processing; complaint
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

kindly refer to our website at https://www.privacy.gov.ph/mechanics-for-complaints/.

This opinion is rendered based on the information you have provided, considering that an advisory opinion does not serve to adjudicate issues between parties or provide a standing rule in an actual controversy.[3]Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[3] See: National Privacy Commission, Rules of Procedure on Requests for Advisory Opinions, Circular No. 18-01 [NPC Circular 18-01], § 2 (September 10, 2018).

ADVISORY OPINION NO. 2019-004[1]

4 January 2018

[redacted]

Re: DATA SHARING ARRANGEMENTS WITH OFFSHORE COMPANIES

Dear [redacted],

We write in response to your request for guidance on data-sharing arrangements entered into by PLDT with entities outside of the Philippines.

We understand that PLDT frequently enters into agreements with offshore companies to be able to provide products and services to its clients. These offshore companies either act as a personal information controller (PIC) or a personal information processor (PIP) depending upon the nature of service that they provide and the purpose of engagement.

We understand further that contractual discussions on compliance with the Data Privacy Act of 2012 (DPA)[2] have been a challenge for PLDT as these offshore companies may be unwilling to agree to data privacy commitments. Hence, you ask for guidance on possible courses of action or any framework that has been agreed upon by data privacy authorities to address the matter.

[1] Tags: data sharing, outsourcing, personal information controller, personal information processor, compliance
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

Scope of the DPA; contractual agreements involved

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

An entity may either be a PIC who controls the collection, holding, processing or use of personal data or instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, or it may be a PIP to whom a PIC may outsource the processing of personal data, whereby it is directed by the PIC to perform any of the processing activities in accordance with its instructions.

Where an offshore company acts as a PIC with its own purpose of processing, completely separate from the declared purpose of PLDT, a data sharing agreement is required.

On the other hand, where an offshore company acts as a PIP, contracted by PLDT to perform particular processing activities on its behalf, the outsourcing or sub-contracting agreement shall reflect the security measures involved in processing, including the transfer of data, use, storage and retention.

Data sharing and compliance with the DPA

All PICs and PIPs are mandated to comply with the provisions of the DPA, its Implementing Rules and Regulations (IRR) and issuances of the National Privacy Commission (NPC).

PICs that share personal data under a data sharing agreement are mandated to put in place adequate safeguards for data privacy and security in compliance with applicable laws and regulations. The DSA should include a general description of the security measures that will ensure the protection of the personal data of data subjects. The DSA, considering its terms, allows PICs to use contractual and reasonable means to provide safeguards for data protection to the personal data being shared.

Where a PIC fails to put in place the security measures required by law, regulations and the DSA, the said PIC may be solely accountable in the absence of fault or negligence on the other PIC. If no security

measures are put in place by both parties or the DSA fails to provide for the same, both parties may be held accountable. Nonetheless, the determination of liability, if any, will be based on the particular facts and circumstances of the case.

For data sharing between PLDT and another PIC, Section 20 of the IRR of the DPA should be followed and NPC Circular No. 16-02[3] may be referred to for guidance.

Duty of the PIC to ensure that the PIPs comply with the DPA

It is recognized under the DPA that PICs may enter into agreements with other entities to process personal data on their behalf. Section 14 of the DPA states:

> "SECTION 14. Subcontract of Personal Information. —A PIC may subcontract the processing of personal information, provided, that the PIC shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of 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."

In addition, Section 21 on accountability states as follows:

> "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."

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

As can be gleaned from the provisions above, it is the ultimate responsibility of the PIC to engage PIPs that are compliant with all applicable laws. The PIC is duty-bound to place the pertinent data privacy and protection provisions in the contract. The agreement with the PIP must comply with Section 44 of the IRR of the DPA, to wit:

> (a) The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement.
>
> (b) The contract or other legal act shall stipulate, in particular, that the personal information processor shall:
>
> (1) Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;
>
> (2) Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data;
>
> (3) Implement appropriate security measures and comply with the Act, these Rules, and other issuances of the Commission;
>
> (4) Not engage another processor without prior instruction from the personal information controller: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implement, taking into account the nature of the processing;
>
> (5) Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;

(6) Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor;

(7) At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services relating to the processing: Provided, that this includes deleting existing copies unless storage is authorized by the Act or another law;

(8) Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter;

(9) Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission.

Failure to comply with the provisions of the DPA and the IRR on outsourcing agreements will be duly considered by the NPC in case there is a compliance check, personal data breach, complaint, or an investigation, among others. This may result into findings where both the PIC, PLDT in this case, and the PIP, are liable for any of the punishable acts under the DPA.

As a PIC, PLDT has control over which entities to engage and contract with and it has the prerogative to continue the contractual relationship. It must determine internally if continuing contracts with non-compliant entities is viable for the business, taking into consideration the attendant risks of such relationship vis-à-vis the requirements of the DPA and the expectations of its data subjects.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-005[1]

4 January 2019

[redacted]

Re: REQUEST FOR INFORMATION FROM THE BUREAU OF INTERNAL REVENUE AND THE MANILA ELECTRIC COMPANY

Dear [redacted],

We write in response to your request for assistance in relation to your various requests for documents and other information from the following:

1. Bureau of Internal Revenue (BIR) – documents relating to a certain corporation under the name Eastern Park View Neighborhood Association, Inc., specifically, the certified true copy of the following:
    a. BIR Form No. 1903 – Application for Registration For Corporations/Partnerships (Taxable/Non-Taxable), Including GAIs and LGUs
    b. BIR Form No. 1906 – Application for Authority to Print Receipt and Invoices
    c. BIR Certificate of Registration (COR)
2. Manila Electric Company (MERALCO) – information on the following:
    a. Person who allowed the MERALCO customers to apply for electric service;
    b. Names of MERALCO customers; and
    c. Who are the actual occupants of the subject property.

[1] Tags: data sharing, outsourcing, personal information controller, personal information processor, compliance

We understand that the above requests stemmed from your predicament in dealing with alleged informal settlers in your property in [redacted], Antipolo City.

Scope of the DPA

The Data Privacy Act of 2012 (DPA)[2] applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.

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.

With this, the information in the various BIR forms and BIR COR pertain to corporations or juridical entities. As such, this is corporate information and not personal information.

Nonetheless, the disclosure of such forms is still regulated by other applicable laws and regulations, specifically the 1997 Tax Code, as amended, and Executive Order No. 2, s. 2016, and the Inventory of Exceptions to the same. We understand that the BIR denied your request based on the above.

As to the request for information with MERALCO, this pertains to personal information. We understand that MERALCO likewise denied your request as this will allegedly be contrary to the provisions of the DPA as well as the Distribution Services and Open Access Rules (DSOAR), promulgated by the Energy Regulatory Commission (ERC) pursuant to RA No. 9136 or the Electric Power Industry Reform Act of 2001.

Pursuant to the DPA, the processing of personal information, which includes the disclosure thereof, should be based on any of the following criteria for lawful processing under Section 12, to wit:

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

"SECTION 12. Criteria for Lawful Processing of Personal Information. – xxx

(a) The data subject has given his or her consent;

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

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

(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;

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

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

Based on the above, MERALCO's disclosure to you can be considered as processing necessary for the legitimate interest of the third party to whom the data is disclosed under Section 12 (f) above.

To determine if there is "legitimate interest" in processing personal information, personal information controllers (PICs) such as MERALCO must consider the following: [3]

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] See generally, Data Privacy Act of 2012, § 12(f); United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ (last accessed on June 11, 2018).

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.[4]

However, similar to the BIR request, it is recognized that other applicable laws and regulations applies to the disclosure of MERALCO's customer information, such as the DSOAR. Also, MERALCO mentioned that it has no information on the identity of the actual occupants of the property in question.

While we understand the challenges you have encountered, requesting for such information from MERALCO may be moot and academic at this point.

Nevertheless, you may continue with your current efforts with the local government unit and the Philippine National Police, and require assistance from the Housing and Urban Development Coordinating Council (HUDCC) and the Department of Justice (DOJ) as these are the primary government agencies spearheading the drive against professional squatters and squatting syndicates.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[4] See: National Privacy Commission, Advisory Opinion No. 2018-080 (Nov. 5, 2018).

ADVISORY OPINION NO. 2019-006[1]

4 January 2019

[redacted]

RE: USE OF CLINICAL DATA IN RESEARCH

Dear [redacted],

We write in response to your letter requesting the National Privacy Commission (NPC) to allow you to use the following clinical data of stroke patients of Our Lady of Lourdes Hospital (OLLH) for your research study:

- Age
- Sex
- Body Mass Index
- Diabetes
- Asthma
- Hypertension
- Heart Diseases (coronary heart disease, cardiomyopathy, heart failure, and atrial fibrillation)
- Personal or family history on TIA
- Brain aneurysm or arterioveous malformations

[1] Tags: Health Research, Clinical Data, Health information

- Smoking

We would like to clarify that NPC is not mandated to grant permission, nor compel any institution to allow any request of a researcher when using clinical data. A researcher must comply with the requirements of applicable laws, regulations, or ethical standards for research.[2]

The Data Privacy Act of 2012[3] (DPA) applies only to the processing of personal data.[4] Statistical, aggregate, or anonymous data are no longer in the purview of the law.

With this, you may consider requesting for the abovementioned clinical data from the OLLH sans all information that may lead to the identity of the patient. If there is a need for any personal data of the patient, it is best to obtain consent. Lastly, it is recommended that you submit your research protocol to a recognized research ethics committee/ ethics review board to ensure that ethical standards are observed.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

---

[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (c) (2016).
[3] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[4] Id. § 4.

ADVISORY OPINION NO. 2019-007[1]

4 January 2019

[redacted]

Re: CREDIT VERIFICATION

Dear [redacted],

We write in response to your inquiry regarding credit verification in relation to know-your-customer (KYC) requirements vis-à-vis the provisions of the Data Privacy Act of 2012 (DPA).[2] In particular, you are seeking to use the existing government databases to confirm vital information submitted by credit card applicants.

The use, including access thereto, of government databases is primarily subject to laws and regulations governing the respective databases. The purpose of access and use of the requesting party, as well as the particular information required to be obtained, depends upon the policy of the government agency, the purpose of the establishment of such database, and other relevant regulations.

As such, it is not within the authority of the National Privacy Commission (NPC) to grant permission as to the use of these databases.

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.[3] This includes databases containing personal data managed and maintained by government agencies. The use of government

[1] Tags: KYC; lawful processing; consent
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission and for other Purposes [Data Privacy Act Of 2012], Republic Act No. 10173 (2012).
3 Id. § 4.

databases to confirm vital information of credit card applicants comes under the scope of the law and is subject to the general principles of legitimate purpose, transparency, and proportionality.[4]

We understand that for credit card applications, applicants provide both personal and sensitive personal information. Lawful processing of these personal data should be in accordance with Sections 12 and 13 for personal information and sensitive personal information, respectively.

As stated in your letter, part of a bank's responsibility prior to issuing a credit card is to perform proper credit verification to confirm the identity and financial capability of the applicant. Likewise, the verification is important to strengthen KYC and credit underwriting processes and mitigate fraud.

When personal information is involved, the verification may fall under the following basis for processing:

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

On the other hand, if it concerns sensitive personal information, processing is allowed when the data subject has given consent, specific to the purpose prior to the processing, or when processing is provided for by existing laws and regulations.

Likewise, you mentioned that the consent of applicants shall be secured before disclosing all declared information to third parties, including

[4] Id. § 11

government agencies, for KYC purposes. As consent is a criterion for processing both personal and sensitive personal information, banks may disclose personal data to government agencies for verification purposes pursuant to such consent obtained. The consent from the data subjects should include an authorization given to the bank to request information from a government database, subject to that particular agency's governing law and internal policies.

We emphasize that consent of the data subject as defined under Section 3(b) of the DPA refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so.

The consent contemplated by the law is an express consent wherein the data subject voluntarily assents to the collection and processing of personal information, rather than an implied or inferred consent resulting from the data subject's inaction or continued use or availment of services offered by a particular entity.[5]

While the verification for KYC purposes is allowed under the DPA, banks still have the obligation to observe the principles of transparency and proportionality while taking the necessary steps to protect the rights of the data subject.

The principle of transparency dictates that the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised.[6]

Moreover, the proportionality principle requires that "the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means."[7]

[5] See: National Privacy Commission, NPC Advisory 2017-42 (August 14, 2017).
[6] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §18(a) (2016).
7 Id. § 13 (c).

Hence, upon application, applicants should be informed when their personal data will be verified with specific government databases and that only information relevant and necessary to the attainment of the purpose of processing will be collected, used and stored for verification purposes.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-009[1]

14 January 2019

[redacted]

Re: APPLICATION FOR EXEMPTION UNDER THE DATA PRIVACY ACT OF 2012

Dear [redacted],

We write in response to your request which sought for the exemption of the Judiciary Savings and Loans Association, Inc. (JUSLA) from the coverage of Republic Act No. 101731[2], also known as the Data Privacy Act of 2012 (DPA), it being a non-bank financial institution, based on Section 4 (f)[3] the law.

Scope of the DPA

We understand that JUSLA is a non-bank financial institution (NBFI) having 4,710 members nationwide.[4] It is a non-stock, non-profit corporation engaged in the business of accumulating the savings of its members and using such accumulations for loans to members to serve the needs of households by providing long term financing for home building and development and for personal finance.[5]

[1] Tags: Scope, exemption, special cases, registration of data processing systems
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] Id. § 4. This Act does not apply to the following: (f) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws. (Emphasis supplied).
[4] Judiciary Savings and Loans Association, Inc., About Us, available at https://jusla.com.ph/about_us.html.
[5] Judiciary Savings and Loans Association, Inc., Frequently Asked Questions, available at https://jusla.com.ph/forms/JUSLA%20FAQs.pdf.

It is important to note that the DPA applies to the processing of all types of personal information[6] and to any natural and juridical person involved in personal information processing.

JUSLA is principally engaged in the processing of personal and sensitive personal information (collectively, personal data) of its members. As provided for in Section 3(j) of the law, processing involves 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.

Accordingly, the collection, organization, storage, and use of the personal data of JUSLA members for their savings and loans, among others, are considered as processing activities undertaken by JUSLA as a personal information controller[7] (PIC). Thus, it is covered by the law.

Exemption from the coverage of the law

Section 4 of the DPA and Section 5 of its Implementing Rules and Regulations[8] (IRR) exempt specific *types or classes of information* from its scope - in particular, paragraph (e) of the latter states:

> "Section 5. Special Cases. The Act and these Rules shall not apply to the following specified information, only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned:
>
> xxx xxx xxx
>
> (e) Information necessary for banks, other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas, and other bodies authorized by law, to the extent necessary to comply with Republic Act No. 9510 (CISA), Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act, and other applicable laws;
>
> xxx xxx xxx

[6] Id. § 3 (g).
[7] Id. § 3 (h).
[8] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016)

> 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*** ." (Emphasis supplied).

From the provision above, it is evident that the non-applicability of the law will only apply to the specified information to the minimum extent of collection, access, use, disclosure or other processing activities performed upon such personal information. The natural or juridical entity processing the specified personal information remains to be covered by the law and other relevant issuances of the National Privacy Commission (NPC).

The non-applicability does not extend to the duties and responsibilities of the entity or organization as a PIC or personal information processor[9] (PIP), such as the duty to uphold the rights of data subjects, adhere to the data privacy principles (transparency, legitimate purpose and proportionality), to designate a data protection officer, and to ensure implementation of security measures to protect personal data, among others.[10]

Based on the foregoing, JUSLA as a PIC is covered by the law and is then obliged to comply with the provisions of the DPA, its IRR and other NPC issuances applicable to its processing activities.

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

For your reference.

Very truly yours,

[9] Id. § 3 (i).
[10] National Privacy Commission, NPC Advisory Opinion No. 2017-44 (16 August 2017).

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

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-010[1]

14 January 2019

[redacted]

Re: ACCESS TO EMPLOYEE 201 FILES AND MEDICAL RECORDS

Dear [redacted],

We write in response to your request for clarification received by the National Privacy Commission (NPC) via email regarding access to employee 201 files and medical records by a company's internal auditor.

We understand that in line with the promotion of the development of a strong corporate governance culture, your company, a publicly-listed corporation, has an Audit Committee that was created to enhance the Board of Directors' oversight capacity over the company's financial reporting, internal control system, internal and external audit processes and compliance with applicable laws and regulations.

The Audit Committee is also responsible, among other functions, for overseeing the Senior Management in establishing and maintaining an adequate, effective and efficient internal control framework. We understand as well that the Audit Committee recommended and approved the creation of an Internal Audit Department as part of their oversight function. The internal auditors, as well as external auditors, are granted independence and unrestricted access to all records, properties, and personnel to be able to perform their respective functions.

[1] Tags: Access to employee records, 201 Files, Medical Records, Internal Audit

The issue at hand is whether internal auditors may be restricted to access the 201 files of employees, given that such records are required for the following procedures:

a. Review of employees requirements if compliant to company policy (including detection of submission of falsified documents, with criminal records, and hiring of unqualified personnel);
b. Review of payroll for re-computation and accuracy of payouts (including unauthorized payouts);
c. Review of Medical Records if really fit-to-work and does not have any communicable disease (the Company belongs to the food industry); and
d. Review of other employee benefits provided to employees related to their home address.

Moreover, you sought clarification on the right of the company to access employee records related to their medical benefits provided by a third-party HMO.

You stated that the HMO sends the company monthly summaries of the amounts of money used by employees in their hospitalization. According to your narration, there are no medical records, hospital billings, itemized hospital charges nor certifications from employees that the amount billed by the HMO is the same amount that was charged to them.

Because of the increase in billings to the company, it is now looking into the possibility of fraudulent padded charges by the HMO, undue hospital charges by the hospital, and unauthorized hospital charges from dependents of employees who are not covered. However, the HMO refuses the company's review of charges because of the Data Privacy Act of 2012.

You now seek clarification on the company's right to inspect medical records, including hospital billings, in the given situation.

Access to 201 files; proportionality

Under Data Privacy Act of 2012[2] (DPA), the processing of personal information is considered lawful when the any of the conditions set in Sections 12 and 13 of the law are met.

The processing of personal information shall be allowed, subject to compliance with the requirements of the DPA and other laws allowing disclosure of information to the public, and adherence to the principles of transparency, legitimate purpose and proportionality.[3] The principle of proportionality dictates that the processing of personal information, including collection and access thereto, shall be adequate and not excessive in relation to the declared and specified purpose.

We acknowledge that companies are required to submit reportorial documents to different regulating agencies and bodies including, the Securities and Exchange Commission (SEC), the Bureau of Internal Revenue (BIR), and in the case of publicly-listed companies, the Philippine Stock Exchange (PSE).

To the extent that these reports are required under law or regulation and are necessary for compliance with the company's legal obligation, such processing of personal information of the employees related to the accomplishment of such reports are allowed under the pertinent provisions under Section 12 and 13 of the DPA. Furthermore, reasonable processing of personal information may be allowed to further the company's legitimate interests, which may include the development of a strong corporate governance culture.

In the situation at hand, internal auditors may be allowed access to the 201 files of employees which may contain personal information, only in so far as may be necessary for their functions, which may include the inspection and examination of employee requirements, payroll, and benefits.

Because employees' 201 files may contain sensitive personal information, and thus, access to which must be regulated by institutionalized policies on authority to access. Under Section 20 of the DPA, "a personal information controller must implement

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012] Republic Act No. 10173 (2012).
[3] Data Privacy Act of 2012, § 11.

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."

In relation to compliance with the provisions of the DPA, its IRR and the issuances of the NPC, the company may look into NPC Circular No. 16-01 on Security of Personal Data in Government Agencies[4] as guidance in the establishment of its policies on security of personal data, including access thereto. While the Circular relates to government bodies and entities, the NPC has used it as a benchmark for best practices in privacy policies in the workplace for the private sector.

Specific to the given situation, the company must establish access controls, particularly granting limited authority to access such 201 files by the Internal Audit Department. In Section 15 of the NPC Circular 16-01, a security clearance to access personal data is required, viz:

> SECTION 16. Security Clearance. A government agency shall strictly regulate access to personal data under its control or custody. It shall grant access to agency personnel, through the issuance of a security clearance by the head of agency, only when the performance of official functions or the provision of a public service directly depends on such access or cannot otherwise be performed without such access.
>
> A copy of each security clearance must be filed with the agency's Data Protection Officer.

Thus, the company must institute policies and procedures such as the above for the protection of personal data in its custody.

With respect to medical records, however, access thereto should always be justified as such are classified as sensitive personal information as specifically enumerated under the DPA. Should there be other means to accomplish the purpose, i.e. if the employee is fit to work or does not have any communicable disease, access to the full medical records of the employee may no longer be proportional. The company should consider if fit-to-work certifications would be sufficient. Otherwise, the company should fully inform the employees and seek their consent for access to their medical records.

[4] National Privacy Commission, Security of Personal Data in Government Agencies, Memorandum Circular No. 16-01 [NPC Circular 16-01] (October 10, 2016).

Consent needed for review of hospital charges

As mentioned, health records are a data subject's sensitive personal information which may not be processed unless the conditions set forth under the DPA are present. In relation to the issue with the HMO's charges, an employee's record of hospital billings, itemized hospital charges, and other medical related expenses, may still be considered as part of his or her health records because these may expose relevant information relating to the employee's health.

The fact that the company shoulders the premium for medical benefits coverage is not one of the conditions contemplated by the law that would justify access of employer to the health information of their employees. In order for the company to have access, it may obtain the consent of the employee for such purpose.[5]

The company may likewise consider asking for a certification from the employees that the amount billed by the HMO is the same as that shown or charged to them.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[5] See: National Privacy Commission, NPC Advisory Opinion NO. 2017-25 (June 22, 2017).

ADVISORY OPINION NO. 2019-011[1]

14 January 2019

[redacted]

Re: INSPECTION OF CORPORATE RECORDS CONCERNING AN INDIVIDUAL

Dear [redacted],

We write in response to your request for an advisory opinion on the interpretation of the provisions of the Data Privacy Act of 2012[2] (DPA) and its Implementing Rules and Regulations (IRR)[3] in relation to Section 74 of the Corporation Code of the Philippines (Corporation Code), specifically the following:

1. Whether case files involving a member of a corporation constitute personal information or sensitive personal information under the DPA; and
2. Whether the disclosure of the case files to inspecting members of a corporation would constitute lawful processing under the DPA or unlawful disclosure giving rise to liability under the DPA.

[1] Tags: scope, personal information, sensitive personal information, lawful processing, Corporation Code, inspection of corporate books and records

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

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

Scope of the DPA; personal information; sensitive personal information

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

As defined in Section 3(g) of the DPA, personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

Thus, the files regarding a case before a company's ethics committee, which includes the committee report/s, minutes of the committee and Board of Directors' meetings, and any pertinent board resolution/s on the matter, which necessarily identifies the individual or data subject concerned, is considered as personal information.

Moreover, information "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"**[4] are considered sensitive personal information.
In your letter, you have requested for clarification on whether the emphasized statement above pertains only to judicial proceedings and not to any other type of proceedings.

After a careful reading of the provision above, it is worthy to note that the items are separated by commas and the last phrase is conjoined by the word or which signals disassociation or independence of the words and ideas enumerated.[5]

The provision clearly states that information pertaining to any: (1) proceeding for any offense committed or alleged to have been committed by the data subject; (2) the disposal of the proceedings; OR (3) the sentence of any court in such proceedings, qualifies such information as sensitive.

[4] Data Privacy Act of 2012, § 3 (l).
[5] Microsoft Corporation v. Rolando D. Manansala and/or Mel Manansala, G.R No. 166391 (21 October 2015).

It then covers any of the three (3) items involving a data subject, not limited to court proceedings.

The omission of the term *judicial* to specify the type of proceeding under Section 3(l) of the DPA reflected the view of the legislators not to limit the scope of proceedings to judicial proceedings. Thus, case files of every data subject, in all types of proceedings, shall be provided a higher degree of protection "as the context of their processing could create significant risks to the fundamental rights and freedoms."[6]

Case files, whether judicial or non-judicial in nature, may contain evidence in the form of affidavits, photographs, confidential documents, or objects that may endanger an individual, cause undue prejudice or cloud judgement that will violate the rights and interests of the data subject/s involved.

Records of other types of proceedings may comprise of minutes of the meetings, notes, opinions and committee resolutions. These may be akin to those documents related to the deliberative process of reaching a decision.

In *In Re: Production of Court Records and Documents and the Attendance of Court officials and employees as witnesses under the subpoenas of February 10, 2012 and the various letters for the Impeachment Prosecution Panel dated January 19 and 25, 2012*[7], the Supreme Court ruled that certain information contained in the records of cases before them are considered confidential and are exempt from disclosure due to the dictates of the integrity of the decision-making function of the body which may be affected by the disclosure of particular information.[8]

Similarly, records of other types of proceedings may be treated with utmost protection, where the disclosure of such documents will hinder free discussion of issues, exchange of opinions, and positions of the individuals involved.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119, Recital 51 (4 May 2016)

[7] Supreme Court En Banc Resolution (14 February 2012).

[8] Id.

Further, Section 38 of the DPA provides that any doubt in the interpretation of any provision of the Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.

Hence, the protection of case files, which includes not only the resolution but the deliberations, evidence, notes, opinions or any other documentation relevant to the proceeding, is incumbent upon the personal information controller for these are sensitive personal information, as defined in the DPA.

Lawful processing of sensitive personal information; Section 74 of the Corporation Code

The DPA generally prohibits the processing of sensitive personal and privileged information, except in the following cases in Section 13:

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 membership 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. That 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.

You have cited in your letter that the processing of sensitive personal information of the data subject concerned may fall under Section 13(b) of the DPA in relation with Section 74 of the Corporation Code, which provides for the right of any director, trustee, stockholder or member of the corporation to inspect the records of all business transactions of the corporation and the minutes of any meeting.

In the case of Philippine Associated Smelting and Refining Corporation vs. Lim,[9] the Supreme Court had the occasion to rule on Section 74 of the Corporation Code, to wit:

> "Specifically, stockholders cannot be prevented from gaining access to the (a) records of all business transactions of the corporation; and (b) minutes of any meeting of stockholders or the board of directors, including their various committees and subcommittees.
>
> The grant of legal personality to a corporation is conditioned on its compliance with certain obligations. Among these are its fiduciary responsibilities to its stockholders. Providing stockholders with access to information is a fundamental basis for their intelligent participation in the governance of the corporation as a business organization that they partially own.
>
> xxx xxx xxx
>
> **The phraseology of the text of the law provides that access to the information mentioned in Section 74 of the Corporation Code is mandatory. The presumption is that the corporation should provide access. If it has basis for denial, then the corporation shoulders the risks of being sued and of successfully raising the proper defenses.** The corporation cannot immediately deploy its

[9] Philippine Associated Smelting and Refining Corporation v. Lim, 804 SCRA 600, G.R. No. 172948 (October 5, 2016).

resources — part of which is owned by the requesting stockholder — to put the owner on the defensive."

From the foregoing, the disclosure of the case files to inspecting members may fall under the criterion for lawful processing provided for in Section 13(b) of the DPA, in relation to Section 74 of the Corporation Code.

Nevertheless, Section 13(b) of the DPA requires basis under law or regulation for the processing of sensitive personal information. It is the duty of the corporation to determine whether Section 74 of the Corporation Code suffices for the purpose of allowing the disclosure contemplated by the requesting party.

We note that such disclosure intended, although seemingly mandatory, is also limited by the conditions set forth in Section 74, i.e. "it shall be a defense to any action under this section that the person demanding to examine and copy excerpts from the corporation's records and minutes has improperly used any information secured through any prior examination of the records or minutes of such corporation or of any other corporation, or was not acting in good faith or for a legitimate purpose in making his demand."[10]

Likewise, such disclosure shall also be duly limited by any other applicable laws, rules, regulations, policies, contractual obligations on the matter, i.e. those requiring non-disclosure and confidentiality of documents and records, etc. Finally, the disclosure of the case files, if indeed warranted, shall also consider the general privacy principles of transparency, legitimate purpose, and proportionality set forth in the DPA and its IRR.

The data subject concerned has the right to be informed of the request for disclosure. Moreover, the corporation has the obligation to examine or inquire about the particular demand thereby disclosing only those personal information that are necessary, not excessive, relevant and adequate to fulfill the legitimate purpose of the demand, as required by Section 74 of the Corporation Code.

[10] The Corporation Code of the Philippines, Batas Pambansa Blg. 68, § 74 (1980).

This opinion is based on the limited information you have provided. The NPC was not provided with the details of the nature of the case in question deliberated upon by the ethics committee. Additional information may change the context of the inquiry and the appreciation of facts.

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-012[1]

17 January 2019

[redacted]

Re: NATIONALITY OF DATABASE HOST

Dear [redacted],

We write in response to your letter to the National Privacy Commission (NPC) requesting for guidance on the database utilized by the Firearms and Explosives Office (FEO).

Based on your letter, the FEO already processes online the applications for License to Own and Possess Firearm (LTOPF) and Firearm Registration for individuals and juridical entities. Currently, the FEO database for said application and registration is hosted by a foreign entity. You now seek clarity on the following questions:

1. Is there a legal impediment when the database is hosted by a foreign entity?
2. Is there a requirement in the law that government databases should be hosted only by a Filipino owned company?
3. Should the FEO opt to change the hosting of its databases to a Filipino owned company, is there a clearance requirement from the NPC?

[1] Tags: Government database, nationality requirement

No legal impediment for foreign host of database

The Data Privacy Act of 2012[2] (DPA) does not prohibit hosting of government databases by a foreign entity. There is no requirement in the DPA relating to the nationality of service providers, either for the government or the private sector. In cases where a personal information controller[3] (PIC) subcontracts or outsources the processing of personal data to a personal information processor[4](PIP), such as the engagement of a service provider for hosting services, the PIC remains primarily accountable for the protection of personal data under its control, even when it is already being processed by a PIP. Thus, the FEO is required to "use contractual or other reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the personal data processed, prevent its use for unauthorized purposes."[5] The FEO must also consider the provisions on outsourcing or subcontracting of personal data processing under the law and its Implementing Rules and Regulations[6] (IRR), and relevant provisions in Circular 16-01, "Security of Personal Data in Government Agencies" (2016)[7]

Considerations in the engagement of a database host

With respect to the obligations of the foreign database host as a PIP, the FEO may consider the following elements of the subcontracting or outsourcing contract as indicated in Section 44 of the IRR:

a. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement.
b. The contract or other legal act shall stipulate, in particular,

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] Data Privacy Act of 2012, § 3 (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. xxx.
[4] Id. § 3 (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.
[5] Rules and Regulations Implementing the Data Privacy Act of 2012, § 43.
[6] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).
7 NPC Circular 16-01, Security of Personal Data in Government Agencies, Rule II, § 7 (2016). See also § § 8-13.

that the personal information processor shall:

1. *Process the personal data only upon the documented instructions of the personal information controller*, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;
2. *Ensure that an obligation of confidentiality is imposed on persons authorized* to process the personal data;
3. *Implement appropriate security measures* and comply with the Act, these Rules, and other issuances of the Commission;
4. *Not engage another processor without prior instruction* from the personal information controller: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;
5. Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;
6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor;
7. *At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services* relating to the processing: Provided, that this includes deleting existing copies unless storage is authorized by the Act or another law;
8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, *and allow for and contribute to audits, including inspections,* conducted by the personal information controller or another auditor mandated by the latter;

9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission.

As a government entity, the FEO should also look at NPC Circular No. 16-01 on Security of Personal Data in Government Agencies for guidance on standards relating to data protection. Additionally, there are industry standards which the FEO should consider in determining the adequacy of their database host, such as the following:

a. ISO 27002 (Code of Practice for Information Security Controls) – this provides for general security controls, including databases;
b. ISO/IEC 27040 (Storage Security) – considering that databases are a form of data at rest; and
c. ISO 27018 (Code of Practice for Protection of Personal Identifiable Information "PII" Protection in Public Clouds acting as PII Processors) and ISO 9579 (Remote Database Access with Security Enhancement) – considering that the government is promoting a Cloud First Policy and the FEO is already using cloud computing for their databases.

No clearance requirement needed from the NPC for change of host

Lastly, in case the FEO opts to change the provider or host of its databases to a Filipino owned company, there is no clearance requirement from the NPC. However, the FEO must ensure that the previous host complies with its contractual obligations, significantly those relating to access, retention or deletion of data. The NPC reserves the right to audit a government agency's data center or that of its service provider. NPC may also require the agency to submit its contract with its service provider for review.[8]

Accountability is one of the key principles of data protection under the Data Privacy Act. Government agencies are responsible for personal data under its control, including information that have been transferred to a third-party for processing, whether domestically or internationally. The government agency, as a PIC, must be able to demonstrate that it has ensured a comparable level of protection, consistent with the DPA and other issuances, while personal data is being processed on

8 NPC Circular 16-01, Security of Personal Data in Government Agencies, Rule II, § 7 (2016). See also §§ 8-13.

its behalf by third parties.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-013[1]

1 April 2019

[redacted]

Re: REQUEST FOR A COPY OF TAX DECLARATION OF REAL PROPERTY WITHOUT CONSENT OF REGISTERED OWNER

Dear [redacted],

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) on whether a person, other than the registered owner of real property or his authorized representative, may secure a copy of a tax declaration from the assessor's office of a local government unit (LGUs) without the consent of the registered owner. In the given situation, the person requesting is claiming legal interest over a property (e.g., notice of adverse claim, lis pendens).

The Data Privacy Act of 2012[2] (DPA) applies to all types of processing of personal information in the country or outside, subject to certain qualifications.[3] The disclosure of a tax declaration of real property is considered processing of personal information, and therefore must comply with the requirements under the DPA.

We understand that under the Local Government Code of 1991, owners or administrators of real property, whether natural or juridical persons, are required to prepare and file with the provincial, city or municipal assessor, a sworn statement declaring the true value of their property.[4]

[1] Tags: assessor, sensitive personal information, consent, disclosure, lawful processing, court proceedings, legal claims, real property, tax declaration

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

[3] Id. § 4.

[4] See: An Act Providing for A Local Government Code of 1991 [Local Government Code of 1991], Republic Act No. 7160, § 202 (1991).

Such declaration shall contain a description of the property sufficient in detail to enable the assessor to identify the same for assessment purposes.[5]

We understand further that the tax declaration contains personal information of the individual owner or administrator such as name, address, and Tax Identification Number (TIN).

Under the law, an individual's TIN is classified as sensitive personal information and as such, may only be processed under the limited circumstances provided by Section 13 of the DPA, to wit:

> "SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> a. The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
> b. The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
> c. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
> d. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That

[5] Id.

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."

Without the consent of the registered owner, a copy of a tax declaration of real property may only be disclosed in the instances provided above.

Aside from the aforementioned criteria, processing of personal, sensitive personal, and privileged information (collectively, personal data) requires compliance with the requirements of the DPA and other laws allowing disclosure of information to the public, as well as adherence to the principles of transparency, legitimate purpose and proportionality.[6]

According to your email, the person who is claiming legal interest on real property may have to secure a copy of a tax declaration for certain proceedings involving the annotation of adverse claim and notice of lis pendens. The situation may fall under Section 13(f) where "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..."

As recognized by the EU General Data Protection Regulation (GDPR), the successor of the EU Data Protection Directive (Directive 95/46/EC) which highly influenced the DPA, processing special categories of personal data, sensitive personal information in this case, should be allowed where necessary for the establishment, exercise or defense of legal claims, whether in court proceedings or in an administrative or

[6] Id. § 11.

out-of-court procedure.[7]

Therefore, as long as the requestor may properly establish that there is a pending case in court where the tax declaration of the property is material or that the document is necessary to the establishment, exercise or defense of a legal claim, the assessor's office may grant the request from persons other than the registered owner without the latter's consent. This is subject to the existing policies, regulations, and procedures of the assessor's office relative to the release of such document, i.e. payment of fees, etc.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Recital 52.

ADVISORY OPINION NO. 2019-014[1]

05 March 2019

[redacted]

Re: PROPOSED BANGKO SENTRAL NG PILIPINAS AND DEPARTMENT OF INTERIOR AND LOCAL GOVERNMENT JOINT MEMORANDUM CIRCULAR IN THE ISSUANCE OF BUSINESS LICENSE/PERMIT FOR PAWNSHOPS AND MONEY SERVICE BUSINESSES

Dear [redacted],

We write in response to your request for an advisory opinion on the proposed Joint Memorandum Circular (JMC) which will be issued by the Bangko Sentral ng Pilipinas (BSP) and the Department of Interior and Local Government (DILG).

Specifically, Clause 6.2 thereof provides that each city or municipality shall submit to the BSP a duly certified report, containing the names of Pawnshops (PSs) and Money Service Businesses (MSBs):

1. That were issued new business licenses/permits;
2. Renewed their business licenses/permits;
3. Failed to renew business licenses/permits; and
4. That cancelled/revoked/retired their business permits.

BSP shall then determine and communicate with the pertinent LGUs which PSs and MSBs are:

1. Have BSP registration and with LGU business permit engaged in business activities which are consistent or inconsistent with those stated in the BSP registration;

[1] Tags: Scope, personal information, special cases,

2. With BSP registration but without LGU business permit;
3. Without BSP registration but with LGU business permit – includes those with and without pending application for registration with BSP; and
4. Without BSP registration and LGU business permit.

We understand that the following issues arose in the course of finalizing the JMC:

1. Whether or not the information shared under Clause 6.2 of the proposed JMC is covered by the Data Privacy Act of 2012[2] (DPA);
2. Assuming that the information to be shared is considered personal information, whether or not data sharing between DILG and BSP is allowed under the DPA; and
3. In the affirmative, whether BSP and DILG are required to enter into a separate data sharing agreement or the proposed JMC is sufficient in order to share the information.

Scope of the DPA; personal information; special cases

The information of juridical entities is outside of the scope of the DPA, as the DPA applies solely to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.

While the information of PSs and MSBs operating as sole proprietorships or partnerships may be considered as personal information as the identity of the owner/s can be reasonably and directly ascertained by the BSP and the DILG, their personal information may fall under the exclusions under Section 4(e) and/or 4(f) of the DPA, to wit:

> "SECTION 4. Scope. — xxx xxx xxx
> This Act does not apply to the following: — xxx xxx xxx
>
> (e) Information necessary in order to carry out the functions of public authority which includes the processing

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

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);

(f) Information necessary for banks and other financial institutions under the jurisdiction of the independent central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; xxx."

For Section 4(e), the exclusion particularly pertains to information necessary in carrying out the functions of a public authority, which includes processing for the performance by the independent central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions.

However, the exclusions above are not absolute. The exclusion of the information specified in Section 4 of the DPA is only to the minimum extent necessary to achieve the specific purpose, function, or activity. Thus, the use of the information claimed to be outside the scope of the DPA:

1. Must be necessary in order to carry out the functions of public authority; and
2. The processing of personal data is for the performance of a constitutional or statutory mandate.[3]

Similarly, for Section 4(f), the exclusion applies to information necessary for banks and other financial institutions under the jurisdiction of the BSP to comply with the following:

1. Republic Act No. 9510 - Credit Information System Act

[3] See: National Privacy Commission, NPC Advisory Opinions No. 2018-002 (Jan. 15, 2018), 2018-014 (May 9, 2018), and 2018-060 (Aug. 30, 2018).

(CISA);

2. Republic Act No. 9160 - Anti-Money Laundering Act; and
3. Other applicable laws.

Given this, the personal and sensitive personal information (collectively, personal data) enumerated in Section 4 may be lawfully processed by a PIC, even without meeting the conditions under Sections 12 and 13 of the DPA, but the processing shall be limited to that necessary to achieve the specific purpose, function, or activity. The PIC is still required, however, to implement measures to secure and protect the personal data.[4]

Thus, only the information required to be processed pursuant to the said function are not covered by the law, while the PICs are still covered by the DPA. The BSP and the DILG are mandated under the DPA to adhere to the data privacy principles of transparency, legitimate purpose, and proportionality, implement appropriate security measures for personal data protection, and ensure that data subjects are able to exercise their rights as provided for by law.
Data sharing

Data sharing shall be allowed when it is expressly authorized by law. Further, Section 20 (d) of the IRR recognizes the data sharing between and among government agencies for the purpose of a public function or provision of a public service. The same section provides that the sharing arrangement shall be covered by a data sharing agreement (DSA), and that:

1. All parties to the agreement shall comply with the DPA, its IRR, and issuances of the NPC, including putting in place adequate safeguards for data privacy and security; and
2. The DSA shall be subject to review of the NPC, on its own initiative or upon complaint of a data subject.

The proposed sharing between the BSP and the LGUs is allowed under the DPA and its IRR as the same is necessary in relation to the specific mandates of these government agencies.

[4] See: National Privacy Commission, NPC Advisory Opinion No. 2018-060 (Aug. 30, 2018).

There is legitimate purpose in the sharing of the personal data, as this will aid in the determination of PSs and MSBs' compliance with the pertinent BSP and LGU registrations.

The information to be shared, as described in the JMC, are the minimum information required to determine compliance with existing laws and regulations, and hence, proportional and not excessive in relation to the purpose of the sharing arrangement.

On transparency and upholding the rights of the data subjects to be informed, it advisable that owners of the PSs and MSBs be informed about the sharing arrangement. This may be done through a privacy notice.

Data sharing agreement in a Joint Memorandum Circular

NPC Circular No. 16-02 was enacted to govern data sharing involving government agencies.

As defined in the circular, a data sharing agreement is a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties.[5] With regard to the contents of a data sharing agreement, Section 6 enumerates the terms and conditions that must be complied with and must be included in the agreement.

The proposed JMC, specifically Clauses 6.2, 6.3 and 7.0 thereof, as currently drafted, may not be sufficient for the purposes of complying with the Circular. Clauses 6.2 and 6.3 merely indicate the overview of the operational details of the sharing or transfer of personal data and Clause 7.0 provides for the confidentiality requirement. There are several other items which must be included, to wit:

5 National Privacy Commission, Data Sharing Agreements Involving Government Agencies, Circular No. 16-02 [NPC Circular 16-02] § 3 (E) (October 10, 2016).

ELEMENTS		DETAILS / REMARKS
a.	Term or duration of the agreement	The JMC should specify the term or duration of the sharing arrangement, which may be renewed on the ground that the purpose or purposes of such agreement continues to exist, provided that in no case such term or any subsequent extension exceed five (5) years, without prejudice to entering into a new agreement. A provision on the exact term or duration of the agreement should be added which should not exceed more than five (5) years subject to renewal.
b.	General description of the security measures, including the policy for retention or disposal of records	There is a need to provide a general description of the physical, technical, and organizational security measures that will ensure the protection of the personal data. Likewise, any policies on retention or disposal of records should be reflected in the JMC.

c.	Where online access to personal data will be provided	The following items must be indicated 1. justification for online access; 2. parties granted online access; 3. types of personal data accessible online; 4. estimated frequency and volume of the proposed access; 5. program and middleware; and 6. encryption method
d.	The personal information controller responsible for addressing: (1) information requests; and (2) complaints filed by data subjects and/or is being investigated by the NPC	Not indicated
e.	Method for the secure return, destruction, or disposal of the shared data (including the timeline)	Not indicated
f.	The designated data protection officer or compliance officer	Not indicated

The NPC, the DPA, its IRR, and issuances of the Commission do not limit the agreement of the parties provided that the agreement does not contravene the letter and intent of the law. The Commission fully

subscribes to the fundamental legal tenet ascribing a presumption of regularity in the performance of functions by government agencies.

Finally, please note that a data sharing agreement does not require prior approval from the NPC.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-017[1]

05 March 2019

[redacted]

Re: RESEARCH AND THE DATA PRIVACY ACT OF 2012

Dear [redacted],

We write in response to your inquiry regarding academic research in relation to the Data Privacy Act of 2012.[2] You are seeking clarification as to the implications of the law to the conduct of academic research vis-à-vis access to documents and records in the custody of national government agencies. Specifically, you are inquiring whether you can be granted access to the geocodes of the Labor Force Survey (LFS) administered by the Philippine Statistics Authority (PSA).

DPA and Research

Research is an activity that aims to develop or contribute to knowledge that can be generalized (including theories, principles, relationships), or any accumulation of information using scientific methods, observation, inference, and analysis.[3]

It is the intent of the DPA to grant processing of personal information for research purposes with much flexibility. It recognizes that research is critical to nation-building and serves the interest of the public.

The DPA applies to the processing of all types of personal information[4]

[1] Tags: Research; Access to public documents

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

[3] 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).

[4] 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.

and to any natural and juridical person involved in personal information processing.[5] However, the law provides special cases where the processing of personal information is excluded from its scope. One is the processing of personal information "for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards."[6]

Note, however, that the law does not provide for blanket exemption for research. Such exemption is limited to the minimum extent of collection, access, use, disclosure or other processing necessary to achieve the specific purpose, function or activity.

Hence, researchers have the concomitant obligations to implement the necessary security measures to protect the personal data they process,[7] uphold the rights of data subjects,[8] and adhere to data privacy principles[9] and the other provisions of the DPA.

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

Balancing the right to information to obtain data for research vis-à-vis data privacy

It is a declared policy of the law "to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth."[10] A constant but effective balancing of rights is necessary in the implementation of any State policy, which holds true for the NPC, as with any other government regulatory agency charged with implementing any particular set of laws or policies.[11] This balancing of two equally important rights should be done on a case-to-case basis.

[5] Data Privacy Act of 2012, § 4.
[6] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (c) (2016).
[7] Data Privacy Act of 2012, § 20.
[8] Id. § 16.
[9] Id. § 11.
[10] Id. § 2.
[11] See: National Privacy Commission, NPC Advisory Opinion No. 2017-29 (June 23, 2017).

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

Infrastructure within the National Privacy Commission (NPC) to handle academic research issues; types of data covered by the DPA

The current organizational structure of the NPC does not provide for a specific office or division which specifically handles "non-private sector (academic research) issues on data."

The law covers the processing of all types of personal information and to any natural and juridical person involved in personal information processing.[12] Personal information is broadly 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."[13]

There is no actual listing of all the personal information that the DPA covers. As to sensitive personal information, please refer to Section 3(l) of the law.

Thus, PICs in the public and private sectors should be guided by the provisions of the DPA in determining what particular data in their custody is personal and sensitive personal information which is covered by the law.

Proper process for getting permission for data or requesting for data access

NPC is not mandated to grant permission, nor compel any institution to allow any request of personal data for research purposes. Such requests should be coursed through the agency concerned. National government agencies, as PICs, are the ones who will determine whether data may be disclosed, keeping in mind their specific mandates, their

[12] Supra note 5.
[13] See: Data Privacy Act of 2012, § 3 (g).

charter or governing law, applicable rules and regulations, and data privacy principles enunciated in the DPA.

As to Institutional Review Boards (IRBs), the approval of the IRB means that the research protocol or proposal has been reviewed and found to have met the standards of the board, including ethical considerations. An IRB approval is one of the ways to demonstrate that ethical standards have been considered in the research.

PSA Labor Force Survey

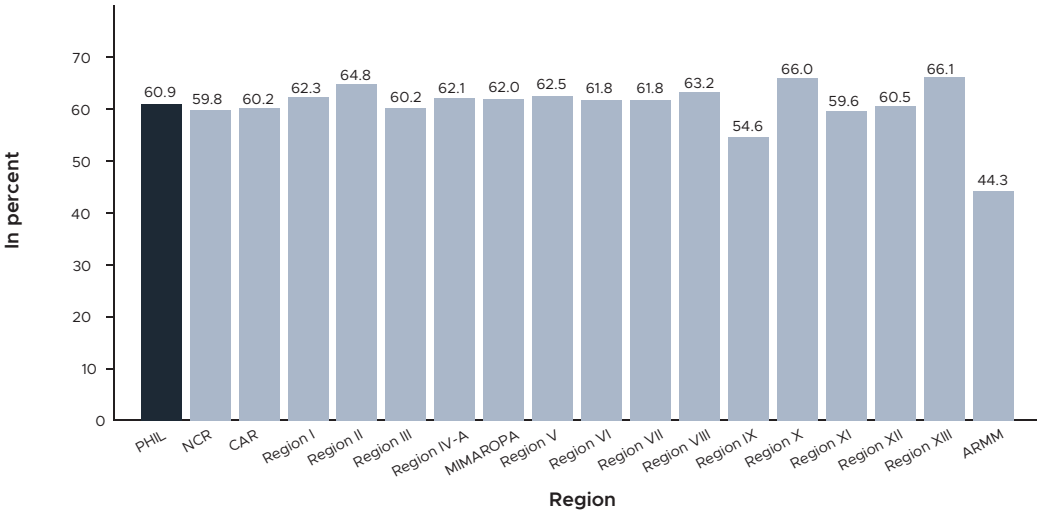
Survey results which are made available to the public do not show any personal data and merely indicate the summary of results gathered from the respondents. Provincial and municipal or city indicators may be considered as personal information from the point of view of the PSA as a personal information controller as they may still have the original raw data from the surveys conducted and hence, may still identify a particular individual respondent.

However, we understand that when released or presented to the public, these indicators are presented as statistics, i.e. for the LFS, the PSA provides an analysis, for instance, of the Employment Situation in April 2018:[14]

> *"More than 60 percent of the population 15 years old and over are in the labor force.*
>
> *In April 2018, the total population 15 years old and over was estimated at 71.0 million wherein the number of persons who were in the labor force was reported at 43.3 million. This placed the labor force participation rate (LFPR) at 60.9 percent, which means that three in five of the population aged 15 years and over were either employed or unemployed.*
>
> *Region XIII (Caraga) had the highest reported LFPR with 66.1 percent while the lowest LFPR reported was in Autonomous Region in Muslim Mindanao (ARMM) at 44.3 percent (Table 1 and Figure 1)."*

[14] Philippine Statistics Authority, Employment Situation in April 2018, available at https://psa.gov.ph/content/employment-situation-april-2018 (last accessed Nov. 22, 2018).

FIGURE 1 Labor Force Particpation Rate by Region: April 2018



Source: Philippine Statistics Authority, April 2018 Labor Force Survey

From the above, the public will not be able to identify an individual from such survey results. Arguably, this may hold true even if the PSA presents a report at the provincial or city/municipal level.

As to you, the researcher, these indicators, when presented as aggregate or statistical data, are not considered as personal information under the DPA since such data no longer contains personal information. Hence, the DPA will not apply to your collection and processing of aggregate or statistical data.

Considering the foregoing, your request for access to the provincial and municipal or city indicators of the aforementioned surveys conducted by PSA do not fall under the coverage of the DPA. The PSA is not proscribed under the DPA to release these data. Nonetheless, this is not withstanding any limitations set by other relevant laws and regulations adhered to by the PSA from disclosing such survey results.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-018[1]

11 March 2019

[redacted]

Re: DATA COLLECTION SURVEYS BY GOVERNMENT AGENCIES

Dear [redacted],

We write in response to your letter which sought guidance from the National Privacy Commission (NPC) with regard to the application of the Data Privacy Act of 2012[2] (DPA) in data collection surveys conducted by the Philippine Statistics Authority (PSA).

We understand that the PSA is a government agency primarily responsible for all national censuses and surveys, sectoral statistics, consolidation of selected administrative recording systems and compilation of the national accounts.[3]

Section 6 of RA No. 10625 or the Philippine Statistical Act of 2013 provides for the following powers of the PSA, among others, to wit:

- Serve as the central statistical authority of the Philippine government on primary data collection;
- Develop and maintain appropriate frameworks and standards for the collection, processing, analysis and dissemination of data;

[1] Tags: Data Sharing Agreement, Data Privacy Principles, Transparency, Legitimate Purpose, Proportionality, Survey, Philippine Statistics Office

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

[3] An Act Reorganizing the Philippine Statistical System, Repealing for the Purpose Executive Order Numbered One Hundred Twenty-One, Entitled "Reorganizing and Strengthening the Philippine Statistical System and for Other Purposes [Philippine Statistical Act of 2013], RA 10625, § 5 (2013).

- Conduct continuing methodological, analytical and development activities, in coordination with the Philippine Statistical Research and Training Institute (PSRTI) to improve the conduct of censuses, surveys and other data collection activities;
- Implement policies on statistical matters and coordination, as directed by the PSA Board.

From the provisions above, PSA issued Resolution No. 5, Series of 2015, establishing the Regional Statistics Committees (RSCs) to provide direction and guidance to regional/local statistical development activities, serve as the policymaking body on statistical matters and shall serve as the venue for discussion and resolution of statistical issues at the local level.[4]

In your letter, you have stated that one of the provisional agendas during the RSC–NCR second quarter meeting was the presentation of "Problems on Data Sharing among Government Agencies and Local Government Units" by the Department of Information and Communications Technology. During the said meeting, concerns on the DPA were raised, especially the issue on response rate to surveys conducted by the PSA.

Hence, it was agreed during the meeting that the committee will seek qualification assistance from the NPC.

Scope of the DPA; response rate to surveys; criteria for lawful processing of personal information

The DPA applies to the processing of all types of personal information[5] and to any natural and juridical person involved in personal information processing.[6] In this case, PSA is considered as a personal information controller (PIC) within the purview of the DPA as it controls the collection, holding, processing or use of personal and sensitive personal information (collectively, personal data) during the conduct of surveys.

[4] Philippine Statistics Authority, Resolution No. 5, Series of 2015, Article 1 (March 20, 2015).
[5] 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.
[6] Id. § 4.

The DPA recognizes several criteria for processing personal and sensitive personal information under Sections 12 and 13 thereof, respectively. In the case of PSA, the processing of personal data of respondents may be based on consent, or to fulfill its functions as a public authority, or when processing is provided for under existing laws and regulations.

We understand that under the Philippine Statistical Act of 2013, there are instances where the National Statistician shall determine whether a survey to be conducted is with or without an obligation to provide information, to wit:

> "SEC. 25. Obligation to Provide Information. – The National Statistician shall determine whether a statistical inquiry or survey to be conducted is with or without an obligation to provide information. **If such obligation is stipulated, all respondents whether natural or legal persons shall be liable to reply to the statistical inquiry or survey. This section applies to all statistical inquiries or surveys conducted by other statistical offices in the PSS.**
>
> The **respondents under this Act are required to give truthful and complete answers to statistical inquiries or surveys of the PSA and other statistical offices of the PSS.** The respondent is considered to have complied with the obligation only upon receipt of the duly completed statistical inquiry or survey forms. The government shall provide franking privileges, charges and postings to the survey offices, unless otherwise disallowed by law.
>
> The PSA is authorized to gather data from other government agencies for statistical purposes." (Emphasis supplied.)

Thus, where a statistical inquiry or survey is determined to be with an obligation to provide information, the same is mandatory and the PSA need not obtain consent of the data subjects for the collection of their personal data.

We wish to emphasize that the DPA, its Implementing Rules and Regulations (IRR), and related issuances of the NPC should be read together with existing laws. The DPA has the twin task of protecting the right to privacy while ensuring the free flow of information, and should not be used as an excuse for non-compliance with other existing laws, rules, and regulations.[7]

[7] See: National Privacy Commission, Advisory Opinion No. 2018-035 (20 July 2018).

General Data Privacy Principles

While the authority of the PSA to process personal data based on its mandate or based on consent is expressly allowed by the DPA, such processing is regulated and should always adhere to the general data privacy principles of transparency, legitimate purpose and proportionality.[8]

The principle of transparency refers to the awareness of the data subjects or the respondents regarding the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the PIC and other recipients of his or her personal data.[9] The PSA is bound to inform the data subjects, either through a privacy notice or some other mechanism, using clear and plain language for easy understanding.

Second, the processing of personal data should be compatible with a declared and specified purpose which is not contrary to law, morals, or public policy.[10] Before even conducting a survey, the PSA should determine its exact purpose and such purpose is relayed to the respondents of the survey.

Lastly, information collected, used and stored shall be adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified purpose. Gathering personal data over and beyond those required to fulfill the objective of the survey violates this principle. Thus, the principle of proportionality should be duly considered in the development of survey questionnaires.

Obligations of a PIC; data sharing; data sharing agreement; sharing of aggregated data

Every PIC should implement reasonable and appropriate organizational, physical and technical security measures for protection of personal data. The appropriate level of security must take into account the nature of the personal data that requires protection, the risks posed by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation, among others.[11]

[8] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (2016).
[9] Id. § 18 (a).
[10] Id. § 18 (b).
[11] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 29 (2016).

As to the sharing of personal data between or among government agencies, it must always be for the purpose of a public function or provision of a public service and should be covered by a data sharing agreement.[12] Relative thereto, the NPC issued Circular No. 16-02[13] which sets out the guidelines for data sharing agreements involving government agencies.

These provisions emphasize that the data sharing may be done to facilitate performance of a public function and to provide public services.[14] Data sharing between government agencies for the above purposes is not prohibited provided that the function or service is consistent with and necessarily required under the general mandate of the agencies concerned.[15]

We wish to emphasize that the data sharing contemplated in the IRR and Circular pertains to sharing of personal data. Hence, the sharing or disclosure of aggregated information in the form of summaries or statistical tables in which a person will no longer be identified need not be covered by a data sharing agreement. Such sharing or disclosure is no longer within the scope of the DPA, but may be subject to the provisions of other applicable laws and regulations, i.e. Philippine Statistical Act of 2013.

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

For your reference.

Very truly yours,

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

Noted by:

[12] Rules and Regulations Implementing the Data Privacy Act of 2012, § 20 (d).
[13] National Privacy Commission, Data Sharing Agreements Involving Government Agencies, Circular No. 16-02 [NPC Circular 16-02] (October 10, 2016).
[14] See: National Privacy Commission, NPC Advisory Opinion No. 2017-54 (11 September 2017).
[15] See: National Privacy Commission, NPC Advisory Opinion No. 2017-52 (11 September 2017).

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-019[1]

12 March 2019

[redacted]

Re: REQUEST FOR EXEMPTION FROM THE COVERAGE OF NPC CIRCULAR NO. 17-01

Dear [redacted],

We write in response to your letter-request received by the National Privacy Commission (NPC) which sought the exemption of the Credit Management Association of the Philippines (CMAP) from the coverage of NPC Circular No. 17-01.[2]

We understand that CMAP is a non-stock and non-profit organization, formed by a group of credit professionals who saw the need for an organization which would promote credit information exchange.[3] It currently has close to more than three hundred members from various industries such as banking, financing, services, trading, manufacturing, and insurance.[4]

Scope of the DPA

The Data Privacy Act of 2012 (DPA)[5] applies to the processing of all types of personal information[6] and to any natural and juridical person

[1] Tags: Scope, Exemption from the Registration of the Data Processing System, designation of Data Protection Officer

[2] National Privacy Commission, Registration of Data Processing Systems and Notifications regarding Automated Decision-Making Operations, Circular No. 17-01 [NPC Circular No. 2017-01] (31 July 2017).

[3] Credit Management Association of the Philippines, About Us, available at http://www.cmaphil.com/portal/AboutCMAP/History.aspx (last accessed 26 February 2019).

[4] Id.

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

[6] Id, §3(g)

involved in personal information processing.

Processing is defined in the DPA as "any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data."[7]

As stated in your letter, CMAP collates public records such as court cases for easy access by members. This act of collating falls squarely on the above definition of processing.

In addition, you mentioned that CMAP members exchange information on loan defaults, past due accounts, bouncing checks, and other unfavorable credit standing of clients. It is not apparent whether these information are also made available to CMAP itself.

However, upon checking CMAP's website, it states the following as its services,[8] among others:

1. Credit Information Exchange is an exchange of credit and collection data through mutual and reciprocal use of quality information.
2. Listing of Court Cases is a compilation of court cased filed in the different courts of Metro Manila, Cebu and Davao in the following categories:
    a. attachment
    b. Batas Pambansa #22
    c. Estafa
    d. Forclosure
    e. Illegal Recruitment
    f. Ejecment
    g. Other Deceits
    h. Falsification of Public Document
    i. Replevin
    j. Sum of Money

[7] Id. § 3 (j)
[8] Credit Management Association of the Philippines, Services, available at http://www.cmaphil.com/portal/AboutCMAP/Services.aspx (last accessed 12 March 2019).

k. Unlawful Detainer
l. Swindling

3. Listing of Returned Checks is a compilation of clients who issued check(s) which was/were dishonored by the drawee bank submitted by CMAP's members.
4. Listing of Accounts Endorsed to Lawyers is a compilation of accounts endorsed to legal submitted by the members of CMAP.
5. Listing of Past Due Accounts from telecommunication companies.
6. Listing of Past Due Accounts from manufacturing companies.

From the foregoing, it is clear that CMAP is a personal information controller[9] (PIC) who is collecting, exchanging, using, storing or processing personal data of its members' clients, and thus, it is covered by the DPA, its Implementing Rules and Regulations (IRR) and other relevant issuances of the NPC.

Appointment of a Data Protection Officer (DPO)

PICs are required to designate an individual or individuals who are accountable for the organization's compliance with the law.[10] This requirement is further clarified in NPC Advisory No. 2017-01 dated 14 March 2017 on the Designation of Data Protection Officers (DPO).

The Advisory applies to all PICs and personal information processors (PIPs) both in the government or private sector. The designation of a DPO is mandatory for PICs and PIPs, regardless of the number of employees, number of sensitive personal information processed, nature of processing or duration or regularity of processing activities.[11] Thus, CMAP is mandated to appoint or designate a DPO to ensure CMAP's compliance with the DPA, its IRR and related issuances of the NPC. Any of the current employees of CMAP who possess the general qualifications of a DPO may perform such role – there is no need hire another person to function as the DPO.

[9] Id. § 3 (h).
[10] Data Privacy Act of 2012, § 21 (b).
[11] National Privacy Commission, NPC Advisory Opinion No. 2018-019 (18 April 2018).

Registration of the Data Processing Systems

To clarify, the registration of the data processing system (DPS) and the designation of the DPO are separate and distinct compliance requirements.

NPC Circular No. 2017-01 dated 31 July 2017 on the registration of DPS provides that in line with Sections 46 and 47 of the IRR, PICs or PIPs that employ fewer than two hundred fifty (250) shall not be required to register unless the processing it carries out is likely to pose risk to the rights and freedoms of the data subject, is not occasional, or includes sensitive personal information of at least one thousands (1,000) individuals.

You stated in your letter that the CMAP does not employ at least 250 persons and does not process 1,000 records involving sensitive personal information. We defer to such conclusion as the CMAP is in a better position of determining such numbers.

Nonetheless, it is advisable to review and re-evaluate the same, given that CMAP may be processing personal data of its members' clients when it provides the services abovementioned. These activities of collating various lists which may contain both personal and sensitive personal information is included in making a determination of the 1,000-record threshold.

It is important to emphasize that the registration of the DPS is just one of the means to comply with the DPA. This means that while a PIC may not be required to register, it is still required to have a DPO, implement reasonable and appropriate security measures intended for the protection of personal information, and uphold the rights of the data subjects by adhering to the principles of transparency, legitimate purpose and proportionality.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-020[1]

18 March 2019

[redacted]

Re: DISCLOSURE OF PERSONAL INFORMATION AND BASIC CREDIT DATA OF INDIVIDUAL BORROWERS FOR AUDIT PURPOSES

Dear [redacted],

We write in response to your request for an advisory opinion on the propriety of disclosing to the Commission on Audit (COA)-LBP State Auditors the personal information[2] and basic credit data[3] of individual borrowers[4] who availed and received loans from the Land Bank of the Philippines (LBP), for audit purposes and pursuant to the powers vested to COA under the 1987 Philippine Constitution and Rule II, Section 3 of its 2009 Revised Rules of Procedures.

In particular, you seek clarification on the propriety of disclosure given the exemption from the scope of the DPA, as claimed by COA.

---

[1] Tags: Audit, Auditors, Borrowers, Credit Data, Commission on Audit, COA, Loans, Scope, Special cases, Public Authority.

[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] Republic Act 9510, 3(b) - "Basic Credit Data" refers to positive and negative information provided by a borrower to a submitting entity in connection with the application for and availment of a credit facility and any information on the borrower's creditworthiness in the possession of the submitting entity and other factual and objective information related or relevant thereto in the submitting entity's data files or that of other sources of information: Provided, that in the absence of a written waiver duly accomplished by the borrower, basic credit data shall exclude confidential information on bank deposits and/or clients funds under Republic Act No. 1405 (Law on Secrecy of Bank Deposits), Republic Act No. 6426 (The Foreign Currency Deposit Act), Republic Act No. 8791 (The General Banking Law of 2000), Republic Act No. 9160 (Anti-Money Laundering Law) and their amendatory laws.

[4] R.A. 9510, 3(c) - "Borrower" refers to a natural or juridical person, including any local government unit (LGU), its subsidiaries and affiliates, that applies for and/or avails of a credit facility.

Scope of the DPA

The Data Privacy Act of 2012 (DPA)[5] applies to all types of processing of personal data,[6] including disclosure of basic credit data of individual borrowers.

We affirm that Section 4 of the DPA and Section 5 of its Implementing Rules and Regulations (IRR) exempt certain categories of information from its scope and application. However, such exemption applies only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned.[7]

Furthermore, the non-applicability is not absolute because the DPA still requires the personal information controller (PIC) or personal information processor (PIP) to comply with other conditions for personal data processing, including implementing security measures to protect personal data and upholding the rights of the data subjects.[8]

Thus, we emphasize that the requirements under the law, including penalties for violation thereof, will still be applicable to the processing of personal data that involves specific types of information belonging to any of the exemptions.

Criteria for lawful processing of personal information; mandate of the Commission on Audit

We take notice of the provision on confidentiality of information indicated under Part III Section X304.12 of the Manual of Regulations for Banks (MORB) Volume 1, which states:

> Confidentiality of Information. Banks shall keep strictly confidential the data on the borrower or consumer, except under the following circumstances:
>
> a. disclosure of information is with the consent of the borrower or consumer;
> b. release, submission or exchange of customer information with other financial institutions, credit information bureaus, lenders, their subsidiaries and affiliates;

[5] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose, a National Privacy Commission, and for other purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[6] Id. § 4.
[7] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (2016).
[8] *Ibid.*

c. **upon orders of court of competent jurisdiction or any government office or agency authorized by law, or under such conditions as may be prescribed by the Monetary Board;**

d. disclosure to collection agencies, counsels and other agents of the bank to enforce its rights against the borrower;

e. disclosure to third party service providers solely for the purpose of assisting or rendering services to the bank in the administration of its lending business; and

f. disclosure to third parties such as insurance companies, solely for the purpose of insuring the bank from borrower default or other credit loss, and the borrower from fraud or unauthorized charges. (Circular No. 702 dated 15 December 2010)[9]

Based on the foregoing, all information pertaining to borrowers are strictly confidential unless the disclosure to be made by the banks falls under the circumstances enumerated, including disclosure to a government office or agency authorized by law.

On the other hand, the processing of personal and sensitive personal information may be based on the various criteria under Section 12 and 13 of the DPA, to wit:

SECTION 12. Criteria for Lawful Processing of Personal Information. – xxx

(a) The data subject has given his or her consent;

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

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

(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;

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

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

[9] Part III, Section X304.12, Manual of Regulations for Banks (MORB), Volume 1.

the Philippine Constitution.

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

(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

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

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

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

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

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

Pursuant to the 1987 Philippine Constitution, the COA has the authority to define the scope of its audit and examination, establish the techniques and methods required therefor, and promulgate accounting and auditing rules and regulations to ensure the proper and lawful use of government funds and properties.[10]

[10] PHIL.CONST., Article IX-D, § 2 (2).

At the same time, the 2009 Revised Rules of Procedures of COA permits the auditors to exercise such power and functions as provided by law and as may be authorized by COA in the examination, audit and settlement of the accounts, funds, financial transactions of the agencies under their respective audit jurisdiction.[11]

While COA claims that the exemption provided under Section 4(e)[12] of the DPA applies to their request for the names of individual loan borrowers and credit data from LBP, the more appropriate basis for such disclosure is Section 12(e) of the DPA where the processing is necessary in order to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate, or Section 13(b) where the processing is provided for by existing law or regulation, as applicable.

In all instances, however, the processing of personal information should adhere to the principles of transparency, legitimate purpose, and proportionality.[13] We highlight the principle of proportionality which entails that the processing must be necessary to achieve the objectives of the audit and not excessive in relation to the declared and specified purpose.

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

For your reference.

Very truly yours,

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

Noted by:

[11] 2009 Revised Rules of Procedures of the Commission on Audit, Rule II, § 3.
[12] Data Privacy Act of 2012, § 4 (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).
[13] Data Privacy Act of 2012,§ 11; Rules and Regulations Implementing the Data Privacy Act of 2012, § 17-18.

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-021[1]

19 March 2019

[redacted]

Re: ASSIGNMENT OF A NON-RESIDENT DPO AND REQUIREMENTS FOR THE CONTACT DETAILS OF A DPO

Dear [redacted],

We write in response to your inquiry received by the National Privacy Commission (NPC) via e-mail, which sought to clarify matters regarding the Data Privacy Act of 2012,[2] specifically the appointment of a non-resident individual as Data Protection Officer (DPO).

You are inquiring whether it is acceptable to assign a new DPO who is based in the United States, in order to align with company policies and direction. You likewise ask for confirmation on the special requirement to have a local Philippine number to be assigned to the DPO.

Assignment of a non-resident individual as DPO

We had a chance to touch upon on the same matter in our NPC Advisory Opinion No. 2017-018,[3] to wit:

> Given its definition, a DPO need not be a resident of the Philippines. However, he or she must be able to fulfill the functions laid out in NPC Advisory No. 2017-01 (Designation of Data Protection Officers). It is worth noting that such functions would require, as a minimum, being familiar with Philippine laws and regulations on data protection and data security.

[1] Tags: Data Privacy Officer, Data Privacy Principles
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] National Privacy Commission, NPC Advisory Opinion No. 2017-018 (April 21, 2017).

Considering that DPOs are accountable for ensuring compliance of the personal information controller (PIC) with the DPA, its Implementing Rules and Regulations (IRR), issuances of the NPC and other applicable laws and regulations relating to privacy and data protection,[4] a DPO must be familiar with the DPA, IRR, and other pertinent Philippine laws and regulations on personal data processing in the Philippines, in order to lessen the risks of violations of the DPA and other applicable laws and policies.

This is vital since one of the primary duties and responsibilities of a DPO is to inform and cultivate awareness on privacy and data protection within the organization as well as serve as the contact person of the NPC and other authorities in all matters concerning data privacy or security issues.[5]

In addition, the assignment of a DPO familiar with Philippine laws and regulations is critical considering that liability for any violation of the DPA will extend to officers who participated in the commission of the crime and those who, by their gross negligence, allowed the commission of the crime.[6] Thus, if a non-resident individual is assigned as DPO, he cannot interpose as a defense that he does not have any knowledge of Philippine laws and regulations on privacy and data protection.

Requirement of a local contact number for a non-resident DPO

The IRR provides for minimum contents of registration of a PIC, among which is the name and contact details of the compliance or data protection officer which shall be immediately updated in case of changes.[7] The registration form for DPOs likewise incorporates the minimum information required to be submitted to NPC, among which is the DPO's title or designation, postal address, dedicated telephone number, mobile number, dedicated email address, and the industry to which the DPO belongs to.

[4] National Privacy Commission, Designation of Data Protection Officers, Advisory No. 17-01 [NPC Advisory 17-01] (March 14, 2017).
[5] NPC Advisory 2017-01.
[6] Data Privacy Act of 2012, § 34; NPC Advisory Opinion No. 2017-018.
[7] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 47 (a) (10) (2016).

The requirement for the Philippine local mobile number is primarily in connection with the Phase II registration provided in NPC Circular No. 17-01, to wit:

> SECTION 9. Registration Process. A PIC or PIP shall register through the Commission's official website in two (2) phases: xxx
>
> B. *Phase II*. Using the access code provided by the Commission, a PIC or PIP shall proceed to the online registration platform and provide all relevant information regarding its data processing systems. The Commission shall notify the PIC or PIP via email to confirm the latter's successful completion of the registration process

The online registration necessitated the use of a valid email address where a verification email with an activation link will be sent, and upon clicking such link, the access code will be sent to the mobile number, which has to be a Philippine mobile number, otherwise, the access code will not be received.

Considering also that the DPO is the contact person of the NPC, having a local mobile number is advisable as it will enable the NPC to communicate with the DPO with directly in case there is a personal data breach which will necessitate immediate action and response.

Assignment of DPO where there are offices inside and outside the Philippines

While a non-resident individual may be assigned as a DPO, note that each entity that forms part of a group of companies is treated separately and is considered as a PIC or PIP in its own right.[8] Thus, each PIC or PIP must designate a DPO as prescribed by law.

In addition, while a group of related companies may appoint or designate the DPO of one of its members to be primarily accountable for ensuring the compliance of the entire group with all data protection policies, such appointment is still subject to the approval of the NPC and, if so allowed, the other members of the group must still designate a Compliance Officer for Privacy (COP).

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

[5] NPC Advisory 2017-01.

of facts.

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-022[1]

07 May 2019

[redacted]

RE: DISCLOSURE OF MARRIAGE CERTIFICATE FOR INVESTIGATION PURPOSES

Dear [redacted],

We write in response to your request for an advisory opinion which sought to clarify the following matters regarding the Data Privacy Act of 2012[2] (DPA) in relation to the mandate of the Department of Finance - Revenue Integrity Protection Service (DOF-RIPS). Specifically, you request for clarification on the following:

1. Whether the DOF-RIPS, as a public authority which investigates and gathers information necessary to carry out its law enforcement functions, is exempt from the coverage of the DPA;
2. Whether Section 4(e) of the DPA applies to information on marital and filial relations sought to be secured by DOF-RIPS in order to carry out its law enforcement functions; and
3. Whether the DPA applies to information on marriage or filial records of a public officer or employee when there is doubt on the truthfulness of declarations made by the same in his/her Statement of Assets, Liabilities, and Net Worth (SALN) or Personal Data Sheet (PDS), or when it

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

is necessary to carry out DOF-RIPS's law enforcement function.

Investigatory functions of DOF- RIPS

We understand that the DOF-RIPS was created by virtue of Executive Order (EO) No. 259 in December 2003. It is the anti-corruption arm tasked to detect, investigate and prevent corruption in the DOF and its attached agencies. It has the following powers and functions, among others:

- To investigate, upon complaint or motu propio, allegations of corrupt practices of officials and employees of the DOF, the Bureau of Internal Revenue and the Bureau of Customs, and all other agencies under the jurisdiction of the Secretary of Finance.
- To gather evidence and file the appropriate criminal, civil or administrative complaints against government officials and employees within its jurisdiction before the appropriate court of law, administrative body, or agency of competent jurisdiction, and to assist the prosecuting agency or officer towards the successful prosecution of such cases.
- To investigate, upon complaint or motu propio, unusual or unjustified accumulation of wealth disproportionate to the earning capacity of government officials and employees under its jurisdiction and to initiate, and assist in, the prosecution of such cases for recovery or forfeiture of ill-gotten wealth.[3]

Hence, the DOF-RIPS is a public authority, specifically, an investigative body, with the power gather evidence, file the appropriate complaints against government officials and employees, and assist in the prosecution of cases.

Scope of the DPA; special cases

The DPA provides for a list of specified information that are not covered by the law. Section 5 of the Implementing Rules and Regulations (IRR)

[3] Office of the President, Creating the Department of Finance Revenue Integrity Protection Service, and for other purposes, Executive Order No. 259 [E.O. No. 259] (Dec. 17, 2003).

of the DPA[4] provides for the special cases wherein the law and the rules are not applicable:

> "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
>
> d. Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law. Nothing in this Act shall be construed as having amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA); xxx
>
> *Provided*, that the non-applicability of the Act or these Rules do not extend to personal information controllers or personal information processors, who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity." (Underscoring supplied)

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

First, it applies only to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned. Information processed by an agency which does

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

not perform law enforcement or regulatory functions remain subject to the DPA. The processing for law enforcement purpose must also be in accordance with their constitutional or statutory mandate, and strictly adhere to all required substantive and procedural processes. A law enforcement agency must establish its mandate to enforce a particular law, and more importantly, that they are not unreasonably infringing on the rights of individuals guaranteed by the Constitution.

Second, the law is clear that only the specified information is outside the scope of the DPA. This means that the public authority with law enforcement functions remains subject to its obligations as a personal information controller under the DPA, i.e. implementing security measures to protect personal data, upholding the rights of data subjects, and adhering to data privacy principles.

In this case, however, the DOF-RIPS is primarily an investigative agency rather than a law enforcement or a regulatory agency. Hence, its processing does not fall squarely under the special case provided for in the DPA and its IRR.

Criteria for lawful processing of personal and sensitive personal information; certificate of marriage; lifestyle check

A Certificate of Marriage issued by the Office of the Civil Registrar General and/or the Philippine Statistics Authority (PSA) contains both personal and sensitive personal information (collectively, personal data) of the contracting parties.

The processing of personal data by the DOF-RIPS may find support in the DPA, specifically Sections 12 and 13 thereof providing the criteria for lawful processing of personal and sensitive personal information, respectively, to wit:

> "SECTION 12. Criteria for Lawful Processing of Personal Information. — The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
>
> xxx xxx xxx
>
> (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its

mandate;

xxx xxx xxx

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

xxx xxx xxx

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

xxx xxx xxx

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority."[5]

In the case of Carabeo v. Court of Appeals,[6] the Supreme Court held that the creation of an internal body in the DOF is but an essential component in the organized and effective collection of evidence against corrupt DOF officials and employees. The court further expounded on the conduct of lifestyle check by the DOF-RIPS, to wit:

> "The so-called lifestyle check pertains to the evidence-gathering process itself because it is through this method that the DOF-RIPS would be able to collect sufficient evidence to indict a suspected DOF official or employee for graft and corruption. Considering this, the Court finds nothing illegal with the lifestyle check as long as the constitutional and statutory rights of the accused are recognized and respected by the DOF-RIPS."

We wish to highlight the decision in NPC Case No. 16-004,[7] involving the processing of a Certificate of No Marriage (CENOMAR) of an employee subject to an administrative investigation by her employer:

> "Information, such as marital status, is considered sensitive personal information under the Data Privacy Act and should be processed only when necessary and proportional to the purpose of inquiry or investigation, even when prior authority has been obtained

[5] Data Privacy Act of 2012, § 13.
[6] Carabeo v. Court of Appeals, G.R. Nos. 178000 and 178003 (2009).
[7] National Privacy Commission, NPC Case No. 2016-004, Pingol v. Buenaventura (Dec. 15, 2017)

> for verification. It should be shown that obtaining a copy of the complainant's CENOMAR through a PSA request is not excessive in relation to the pending administrative case against complainant. Processing of personal data should not be done if intended merely to satisfy curiosity or to cast a dragnet that would put at risk a data subject to discrimination and any other harm. In this case, it has not been sufficiently shown that the processing of personal data in unrelated to the pending administrative case, or that it is excessive for purposes of the investigation. Thus, we find that the authority provided in the PDS would be sufficient basis for proceeding with verification of its contents for purpose of the administrative case.
>
> xxx xxx xxx
>
> While the evidence before the Commission fail to meet the burden of proof to recommend a criminal prosecution for unauthorized processing against respondents, it is evident that there was little regard for the rights of complainant as a data subject. Her claims of privacy violation were not addressed adequately by the agency, even if only to explain to her the basis of the processing of her personal data.
>
> xxx xxx xxx
>
> Respondents in this case are therefore reprimanded for relying solely on the authority given by complainant through the PDS without due consideration to fairness in the processing of her personal data…Processing of personal data, particularly those of a sensitive nature, should be in accordance with law. This complaint serves as a reminder that anyone involved in the processing of personal data must be cognizant of the obligations imposed by the Data Privacy Act, and that at all times there must be due regard for the rights and freedoms of the data subject."

We are mindful of the mandate of the DOF-RIPS and the necessity of examining the marital records of a person under investigation for corruption as this is crucial in the gathering of evidence on the declarations made in the SALN and/or PDS vis-à-vis possible circumventions on the requirement of full disclosure expected from public officers and employees. We uphold the principle that public office is a public trust, and public officers and employees must at all times be accountable to the people.[8]

The DPA is not meant to prevent government institutions from processing personal data when necessary to fulfill their mandates. Rather, it aims to protect the right to information privacy while ensuring free flow of information. What the DPA does is to promote fair, secure,

[8] PHIL. CONST. art. XI § 1.

and lawful processing of such information.[9]

Nonetheless, we wish to remind the DOF-RIPS that its investigative mandate involving lifestyle checks should at all times strictly adhere to all required substantive and procedural processes and must not unreasonably infringe on the rights and freedoms of individuals guaranteed by the Constitution.

As a government agency, the DOF-RIPS should consider the provisions of NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies, and NPC Circular No. 16-02 regarding the execution of a data sharing agreement between the DOF-RIPS and the PSA, as may be necessary and appropriate.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

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

ADVISORY OPINION NO. 2019-023[1]

13 June 2019

Re: PROCESSING OF CCTV FOOTAGE UNDER THE DATA PRIVACY ACT OF 2012

Dear [redacted],

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) which sought to clarify the following matters regarding Data Privacy Act of 2012[2] (DPA):

1. Whether the use of the closed-circuit television (CCTV) is allowed under the DPA; and
2. Whether the CCTV footage is admissible as evidence in court.

Scope of the DPA; CCTV footage as personal information; lawful processing of personal information

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

Personal information is any information whether recorded in a material form or not, from which the identity of an individual is apparent or

[1] Tags: scope, lawful processing of personal information, privacy notice, CCTV, employee, evidence

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

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]

A CCTV is a camera surveillance system that captures images of individuals or information relating to individuals.[4] Accordingly, 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.[5]

As can be gleaned from the foregoing, the footage and images captured in the CCTV, as a general rule, are considered personal information, and the provisions of the DPA, specifically Section 12, will apply:

(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 (PIC) 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 PIC or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

[3] Data Privacy Act of 2012, § 3 (g)
[4] See: Office of the Privacy Commissioner (New Zealand). Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organizations (2009), available at https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf (last accessed Oct. 16, 2018).
[5] See: Office of the Information Commissioner (Queensland). Camera Surveillance and Privacy (2009), available at https://www.oic.qld.gov.au/__data/assets/pdf_file/0010/28099/guideline-camera-surveillance-and privacy.pdf (last accessed March 21, 2019).

Concomitant to the above, the processing of CCTV footage is allowed under the DPA if the same is necessary under any of the abovementioned criteria, subject to the implementation of a reasonable and appropriate organizational, physical and technical security measures and adherence to the general data privacy principles of transparency, legitimate purpose and proportionality.

In addition, Section 13(f) of the DPA may likewise apply where a CCTV footage or image would reveal sensitive personal information. Thus, the processing of CCTV footage may be allowed if the same 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.

Processing of personal information in the workplace; Legitimate interest of employer

You mentioned in your letter that your client, as the employer, installed CCTV and surveillance cameras in the workplace. Footages then revealed irregularities and fraudulent activities carried out that resulted to the modification of the accounts of postpaid subscribers. Your client then intends to use the video footages as evidence in filing criminal charges against its employees.

Every employer may have a legitimate interest in processing personal information of its employees through the CCTV, particularly in keeping employees safe, preventing crime and detecting employees' misconduct.

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.

In order to use legitimate interest as basis for lawful processing, a PIC must consider the following:

1. Purpose test - The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve;
2. Necessity test - The processing of personal information must be necessary for the purposes of the legitimate

interest pursued by the PICs 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 PIC, considering the likely impact of the processing on the data subjects.[6]

Employee monitoring; right to be informed; privacy notice in the workplace

The DPA imposed obligations on PICs to uphold the rights of the data subject to be informed and notified[7] in the processing operations performed on their personal data. Specifically, every PIC is required to craft and implement policies and procedures regarding the collection, use, access, storage and destruction of footages. The exact purpose of processing and extent of such activities should likewise be indicated.

Employees must likewise be properly informed and oriented about the policy on CCTV and surveillance cameras, including the place, time, and circumstances of such recording. There must be a privacy notice on conspicuous areas to apprise the data subjects, employees in this case, that the premises or particular areas are under surveillance.

Likewise, we wish to emphasize that although employees are within office premises and using company-issued equipment within office hours, they still are entitled to their right to privacy at work.[8] With the emergence of new technologies that provide employers with vast opportunities to monitor and track employees, unbridled checking can damage trust, disrupt professional relationships and disturb workplace peace and performance.[9]

Admissibility of CCTV footage as evidence in court

[6] See: National Privacy Commission, NPC Advisory Opinion No. 2018-061 (Sept. 6, 2018) citing Data Privacy Act of 2012, § 12 (f); United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ [last accessed on September 5, 2018].

[7] Data Privacy Act of 2012, § 16 (a) and (b).

[8] National Privacy Commission, NPC Advisory Opinion No. 2018-084 (Dec. 4, 2018).

[9] Id. citing Privacy Commissioner of New Zealand- Privacy at Work: A guide to the Privacy Act for employers and employees, accessed on 28 November 2018, available at https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-at-Work-2008.pdf

We understand that Rule 11, Section 1 of the Rules on Electronic Evidence provides that audio, photographic and video evidence of events, acts or transactions shall be admissible provided it shall be shown, presented or displayed to the court and shall be identified, explained or authenticated by the person who made the recording or by some other person competent to testify on the accuracy thereof.10 To be admissible, evidence must be competent and relevant. The former requires that the evidence is not excluded by the law or by the Rules of Court while the latter provides that the evidence has a relation to the fact in issue as to induce belief in its existence or non-existence.

Please note however, that the determination of the admissibility of evidence in court is not within the purview of NPC's mandate. This matter is governed by the Rules of Court and other applicable rules of the Supreme Court, such as the Rules on Electronic Evidence.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-024[1]

07 May 2019

[redacted]

Re: DISCLOSURE OF CRIMINAL HISTORY

Dear [redacted],

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) which sought clarify the extent of processing and disclosure of criminal history vis-à-vis the provisions of the Data Privacy Act of 2012[2] (DPA).

Processing of sensitive personal information under the DPA; criminal history; publication in newspapers, media, DOJ website

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in the processing of personal information.[3] Sensitive personal information includes information about any proceeding for any offense committed or alleged to have been committed by an individual, the disposal of such proceedings, or the sentence of any court in such proceedings.[4]

The processing of sensitive personal information is prohibited except in the following cases:[5]

(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;

[1] Tags: lawful processing of sensitive personal information, data privacy principles, criminal history, public notice, employee data; right to information; freedom of the press; prejudicial publicity; right to privacy
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] Data Privacy Act of 2012, § 4.
[4] Id. § 3 (l).
[5] Id. §13.

(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 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;

(f) 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

(g) 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.

The DPA recognizes that journalists process personal and sensitive personal information when reporting on criminal cases on television

and newspapers. As a special case, personal information processed for journalistic, artistic or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations, is outside of the scope of the DPA – but only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned.[6]

In addition, these publishers, editors, or duly accredited reporters, who are considered as personal information controllers (PICs) or personal information processors (PIPs) within the meaning of the DPA, are still bound to follow the law and related issuances with regard to the processing of personal data, upholding rights of their data subjects and maintaining compliance with other provisions that are not incompatible with the protection provided by Republic Act No. 53.[7]

As to the posting of cases in the Department of Justice (DOJ) website, such processing is allowed under Section 13(b) and (f) above as part of their mandate pursuant to the Administrative Code of 1987[8] and other applicable laws and regulations on the matter.

Please note, however, that the said processing is limited only to the minimum extent necessary to achieve the specific purpose, function, or activity of the DOJ, and the agency is not precluded from adhering to the general data privacy principles as well as the requirements of implementing measures to secure and protect personal data.

Particularly on the principle of proportionality, the DOJ is bound to observe and align its practices in order to ensure that only relevant, necessary, and not excessive information is disclosed to the public.

Right to information and freedom of the press vis-à -vis right to privacy; prejudicial publicity; fair and true reporting

The constitutional right to information on matters of public concern is enshrined in Article III, Sec. 7 of the 1987 Constitution. The incorporation of this right is a recognition of the fundamental role of free exchange

[6] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (b) (2016).
[7] Id. 7 (b).
[8] Instituting the Administrative Code of 1987 [Administrative Code of 1987], Executive Order No. 292, BOOK IV, Title III, Chapter 1-General Provisions (1987).

of information in a democracy.[9]

Together with the constitutionally guaranteed right of freedom of the press, the Commission recognizes the vital role of the media in protecting the interest of the public. In fact, newspapers should be given such leeway and tolerance as to enable them to courageously and effectively perform their important role in our democracy.[10]However, we wish to highlight the case of Tulfo v. People of the Philippines,[11] where the Supreme Court ruled that:

"The freedom of the press is one of the cherished hallmarks of our democracy; but even as we strive to protect and respect the fourth estate, the freedom it enjoys must be balanced with responsibility. xxx" (underscoring supplied)

With this, publishers, editors, or duly accredited reporters reporting on criminal cases should process personal and sensitive personal information fairly and lawfully, in a manner that would respect the privacy rights of an individual. The same should avoid prejudicial publicity that may deprive the accused of due process rights to a fair trial.

Further, on the concept of true and fair reporting, the Supreme Court in *People of the Philippines v. Castelo* held that where the publication is a fair and true report of an official investigation it comes within the principle of a privileged communication so that even if the same is defamatory or contemptuous the publisher need not be prosecuted upon the theory that he has done it to serve public interest or promote public good,[12] to wit:

> "Thus, under our law, it is postulated that "a fair and true report, made in good faith, without any comments or remarks, of any judicial, legislative, or other official proceedings which are not of confidential nature, or of any statement, report, or speech delivered in such proceedings, or of any other act performed by public officers in the exercise of their functions", is deemed privileged and not punishable (Article 354, paragraph 2, Revised Penal Code).
>
> The reason behind this privilege is obvious. As it was aptly said, "Public policy, the welfare of society, and the orderly administration of government have demanded protection for public opinion. The

[9] Baldoza v. Dimaano, Adm. Matter No. 1120-MJ, May 5, 1976, 17 SCRA 14.
[10] Lopez v. Court of Appeals, G.R. No. L-26549 (1970)
[11] G.R. Nos. 161032 & 161176 (2008)
[12] People v. Castelo, G.R. No. L-11816 (1962).

> inevitable and incontestable result has been the development and adoption of the doctrine of privilege" (U. S. vs. Bustos, 37 Phil., 731, 742)."[13]

To reiterate, the DPA has the twin task of protecting the fundamental human right of privacy while ensuring the free flow of information to promote innovation and growth. The balancing of the right to privacy of an individual vis-à-vis freedom of the press is worth noting.

Public notice for termination of employee; disclosure of grounds for termination; disclosure of case to current employer

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. In order to use legitimate interest as basis for lawful processing, PICs must consider the following:[14]

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

[13] Id.

[14] See generally, Data Privacy Act of 2012, § 12 (f); United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ [last accessed on September 5, 2018].

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.[15]

From the foregoing, while such public notices may be allowed under the DPA, we wish to emphasize the data privacy principle of proportionality, which requires that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

Hence, it is suggested that only the following details of the former employee be published: full name, facial image, previous designation or position in the company, and effectivity date of the employee's separation from the company. To indicate the grounds for the employee's separation or termination from the company, i.e. cases filed against him or her, and other additional personal information, i.e. home address, email address, mobile number, etc., may no longer be proportional to the primary purpose of the public notice.

As to the disclosure of cases to the current employer of the person, the same may be possible in instances where the current employer asks the former employer as a character reference, when verifying or validating details of employment and other pertinent records submitted by the person, or in general, when the person has given his consent to the current employer to ask former employers about him or her, probably as part of pre-employment requirements or as a continuing requirement during the course of employment.

Companies should have policies in place on how they handle their applicants' and employees' data, and these should be cascaded at the very outset of the relationship with the person, i.e. as a job applicant, and later on, when said person is hired. There is a need to provide clear information about the processing of his or her personal data within the duration of the employment and after separation for whatever

[15] See: National Privacy Commission, NPC Advisory Opinion No. 2018-061 (Sept. 6, 2018).

cause. All these should adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.

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

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-025[1]

07 May 2019

[redacted]

Re: DISCLOSURE OF THE NAMES OF THE UNIT OWNERS/ MEMBERS OF A CONDOMINIUM ASSOCIATION

Dear [redacted],

We write in response to your request for advisory opinion, which sought clarification on the application of the Data Privacy Act of 2012[2] (DPA) to the request received by your client, a condominium association (the Association), from several of its members for a list of the names of members in good standing and delinquent unit owners for purposes of identifying the persons who need to be present to reach a quorum in the Annual General Assembly.

Names of members of the Association as personal information; criteria for lawful processing; legal obligation to which the personal information controller is subject

The names of the members of the Association and their respective membership standing are considered as personal information. Personal information under Section 3(g) of the DPA 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.

[1] Tags: personal information; criteria for lawful processing; legal obligation; Revised Corporation Code

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

Section 12 of the DPA provides the for the various criteria for lawful processing of personal information. Specifically, Section 12(c) appears to be relevant to the issue at hand, which states as follows:

> "Section 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: xxx
>
> (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject; xxx"

In relation to the above provision, Section 73 of the Revised Corporation Code[3] provides:

> "Section 73. Books to be kept; Stocks Transfer Agent. – Every corporation shall keep and carefully preserve at its principal office all information relating to the corporation including, but not limited to: xxx
>
> (b) The current ownership structure and voting rights of the corporation, including lists of stockholders or members, group structures, intra-group relations, ownership data, and beneficial ownership; xxx
>
> Corporate records, regardless of the form in which they are stored, shall be open to inspection by any director, trustee, stockholder or member of the corporation in person or by a representative at reasonable hours on business days, and a demand in writing may be made by such director, trustee or stockholder at their expense, for copies of such records or excerpts from said records. The inspecting or reproducing party, shall remain bound by confidentiality rules under prevailing laws, such as xxx Republic Act No. 10173, otherwise known as the "Data Privacy Act of 2012", xxx."

In your case, the Association has a legal obligation to its members, rooted in Section 73 of the Revised Corporation Code, to provide access to and inspect corporate records and documents.[4] The DPA does not operate to curtail existing rights of members of a condominium corporation, specifically on inspection of corporate books and records, subject to existing laws and regulations on such matters.[5]

[3] An Act Providing for the Revised Corporation Code of the Philippines [Revised Corporation Code of the Philippines], Republic Act No. 11232 (2019).
[4] See: National Privacy Commission, NPC Advisory Opinion No. 2018-011 (Mar. 22, 2018).
[5] Id.

The members of the Association were able to establish the basis for the request for the list of members, i.e. they specified a purpose for requesting for the list, which is to identify those who need to be present to reach a quorum in the Annual General Assembly. Such purpose is not contrary to law, morals or public policy.

It is also worthy to note that under Section 11(e) of the DPA, personal information must be retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained.

It is thus recommended that you advise the members of the Association they must only retain and use such list to determine the quorum necessary for the Annual General Meeting. Subsequently, once the purpose has been fulfilled, the personal data should be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.[6]

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[6] Rules and Regulations Implementing the Data Privacy Act of 2012, § 19 (d) (3) (2016).

ADVISORY OPINION NO. 2019-026[1]

24 April 2019

[redacted]

Re: REDACTED INFORMATION IN REQUESTED PUBLIC DOCUMENTS

Dear [redacted],

We write in response to your letter which sought clarification regarding the redaction of information in requested public documents from the Bureau of the Treasury (BTr) in relation to the Data Privacy Act of 2012 (DPA).[2] Specifically, you are seeking clarification on the following:

a. Whether the BTr can redact information in requested public documents by virtue of them being sensitive personal information under the DPA;
b. If in the affirmative, what information may be redacted; and
c. Proper procedure to be followed by government agencies when redacting information in a public document.

Right to information on matters of public concern; access to public documents; limitations

The people have a fundamental right to information, particularly on matters of public concern.[3] Every Filipino citizen is afforded this right, subject to certain limitations provided by law.

Executive Order (EO) No. 02[4] relates to the operationalization of the people's right to information under the executive branch. EO No. 2 permits the disclosure of information in the possession or under the

[1] Tags: request for public documents; sensitive personal information; redaction; freedom of information
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] PHIL. CONST. art. 3 § 7.
[4] Office of the President, Operationalizing In The Executive Branch The People's Constitutional Right To Information And The State Policies To Full Public Disclosure And Transparency In The Public Service And Providing Guidelines Therefor, Executive Order No. 2 [EO No. 2] (July 23, 2016).

custody of the government unless they fall under any of the exceptions enshrined in the Constitution, existing law or jurisprudence.

In addition, the DPA, having the twin policies of protecting the right to data privacy while at the same time ensuring the free flow of information for innovation and growth,[5] sets certain parameters under which personal data may be processed (e.g., disclosed) in a manner that is consistent with the general data privacy principles.

As you discussed in your letter, public documents include the written official acts, or records of the official acts of the sovereign authority, official bodies and tribunals, and public officers, whether of the Philippines, or of a foreign country, documents acknowledged before a notary public except last wills and testaments, and public records, kept in the Philippines, of private documents required by law to be entered therein.[6]

It has been held that access to public documents may be duly regulated, despite their nature as such. In Legaspi vs. Civil Service Commission,[7] the Court held as follows:

> "The authority to regulate the manner of examining public records does not carry with it the power to prohibit. 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."

EO No. 2 clarifies that "while providing access to information, public records, and official records, responsible officials shall afford full protection to the right to privacy of the individual."[8] For this purpose, it requires that each government office shall ensure that personal information in its custody or control is disclosed or released only if it is material or relevant to the subject-matter of the request and

[5] Data Privacy Act of 2012, § 2.
[6] Supreme Court, Rules of Court, Rule 132, § 19.
[7] Legaspi vs. Civil Service Commission, G.R. No. L-72119 (1987).
[8] EO No. 2, § 7.

its disclosure is permissible under this EO or existing law, rules or regulations, among others.[9]

The above is consistent with the provisions of the DPA which recognizes that certain personal information of public concern is outside of the scope of the law. This pertains to information about any individual who is or was an officer of a government institution that relates to the position or functions of the individual under Section 4(a), including:

a. The fact that the individual is or was an officer or employee of the government institution;
b. The title, business address and office telephone number of the individual;
c. The classification, salary range and responsibilities of the position held by the individual; and
d. The name of the individual on a document prepared by the individual in the course of employment with the government.

While the information may be outside of the scope of the law, this is only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned.

Hence, when a request involves the above information, the concerned government agency may disclose such information. However, where a particular document or form contains personal and sensitive personal information (collectively, personal data) of the government officer or employee which is no longer of public concern, government agencies may redact such personal data.

There is a need to balance, in a case to case basis, the right to information of the public and the right to data privacy of government personnel.

Redacted information in government documents and forms

In all instances, adherence with the general data privacy principles of transparency, legitimate purpose and proportionality is required when

[9] Id.

processing personal data.[10]

The principle of transparency states that the data subject must be aware of the nature, purpose and extent of processing of his or her personal data. This entails giving notice and information to the data subjects using clear and plain language and giving them the procedure and mechanism on how to exercise their rights as data subjects.[11] Second, the processing of personal information shall be compatible with a declared and specified purpose, which is not contrary to law, morals or public policy.[12] Lastly, the principle of proportionality states that only adequate, relevant, suitable and necessary information in relation to your legitimate purpose shall be processed.[13]

The request with the BTr for the certified true copies of the 2010-2018 fidelity bond applications (General Forms 57-A and 58-A) and required supporting documents pertaining to a punong barangay and a municipal mayor should be examined in light of these principles and taking into account relevant laws and regulations on public documents.

We provide our comments as follows:

Redacted Information in General Form 57A of a Punong Barangay and Municipal Mayor	Comment/Remarks
Date when incoming officer assumes accountability (Section 3)	These information forms part of matters of public concern and may be disclosed without redaction, subject to their relevance and necessity to the purpose of the request.
Amounts of maximum accountability or custody (Section 5)	
Salary attached to the position (Section 6)	
Bond fixed by law or by the Chairman of the Commission on Audit (Section 8)	

[10] Data Privacy Act of 2012, § 11.
[11] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (a) (2016)
[12] Id. § 18 (b).
[13] Id. § 18 (c).

Previous experience (Section 9A)	This may be considered as personal information, the disclosure of which should be based upon any criteria under Section 12 of the DPA, and subject to its relevance and necessity to the purpose of the request.
Criminal or Administrative Record (Section 9B)	This is sensitive personal information under the DPA, the disclosure of which should be based upon any criteria under Section 13 of the law, and subject to its relevance and necessity to the purpose of the request. We note that in your letter, you have not stated the purpose of your request for these forms. Considering the principles of legitimate purpose and proportionality, you may not be given access to information on criminal and administrative records, especially if such is still pending with the Ombudsman as you have stated in your letter.

Redacted information in General Form 58A of a Municipal Mayor	**Comment/Remarks**
Place and date of birth	These are considered as personal (place of birth) and sensitive personal information (date of birth from which the age may be computed), the disclosure of which should be based upon any criteria under Section 13 of the law, and subject to their relevance and necessity to the purpose of the request.

Civil status How many persons are dependent for support	Civil status is sensitive personal information, the disclosure of which should be based upon any criteria under Section 13 of the law, and subject to its relevance and necessity to the purpose of the request. The number of dependents is not personal information, hence, outside of the scope of the DPA.
Income other than salary as barangay official, amount and source	These information forms part of matters of public concern and may be disclosed without redaction, subject to their relevance and necessity to the purpose of the request.
If engaged in other business, and names of partners or associations	
Tax Identification Number	This is sensitive personal information under the DPA, the disclosure of which should be based upon any criteria under Section 13 of the law, and subject to its relevance and necessity to the purpose of the request.
Three Character References	These are personal information, the disclosure of which should be based upon any criteria under Section 12 of the DPA, and subject to its relevance and necessity to the purpose of the request.
Have you ever been discharged from any position and particulars	These may be considered as personal information, the disclosure of which should be based upon any criteria under Section 12 of the DPA, and subject to its relevance and necessity to the purpose of the request.
Life insurance, amount, insurance company, and beneficiary	
Criminal or Administrative Record and nature thereof	See comment above for General Form 57A.

Estimated total amount of all monthly living expenses of your family	These may be considered as personal information, the disclosure of which should be based upon any criteria under Section 12 of the DPA, and subject to its relevance and necessity to the purpose of the request.
Date when form was accomplished	This information forms part of matters of public concern and may be disclosed without redaction, subject to their relevance and necessity to the purpose of the request.
Name and Signature of Witness	The names of the witnesses form part of matters of public concern and may be disclosed without redaction, subject to their relevance and necessity to the purpose of the request. As to their signatures, the same may be redacted.
Name and Signature of the Fidelity Bond Applicant	See immediately preceding comment.

Evaluating requests for information; procedure for redacting information in a public document

Government agencies should abide by their Freedom of Information (FOI) Manual when dealing with requests for public document pursuant to EO No. 2. Likewise, it is incumbent upon the government agency to promulgate rules or criteria against which the request for disclosure shall be assessed.

The National Privacy Commission (NPC) issued NPC Advisory No. 2017-02 (Advisory) dated 03 April 2017 to shed light on the nature of processing that is permissible under the DPA while upholding the freedom to access information, public records and official records pursuant to EO No. 02.

Though the Advisory particularly pertains to requests for access to or disclosure of the Personal Data Sheet (PDS) of government personnel, the issuance included considerations that may be taken into account in a request for access to public documents which may also be applicable to the present inquiry. These are:

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

As to the process of redaction, which is defined as the permanent removal of information within a document,[14] the Commission has yet to issue guidelines on the standard manner of redacting public documents.

One may refer to ISO/IEC 27038:2014 - Information technology — Security techniques — Specification for digital redaction for reference on the characteristics of techniques for performing digital redaction on digital documents, and the requirements for software redaction tools and methods of testing that digital redaction has been securely completed.[15]

Redaction tools may likewise be found in software applications, i.e., Adobe Acrobat Pro DC, Microsoft Word Add-In, etc.

For the redaction of documents in hardcopy,[16] methods may include blacking/whiting out which is done by photocopying the original document and using a black marker pen or correction fluid to block out the information. The redacted version should then be photocopied again to produce an access version. Another way is the scalpel, whereby the information is physically removed from the photocopied document using an artist's scalpel or similar tool, leaving a 'doily', which is then photocopied again to provide the redacted document.

[14] International Organization for Standardization, ISO/IEC 27038:2014(en) Information technology — Security techniques — Specification for digital redaction, preview available at https://www.iso.org/obp/ui/#iso:std:iso-iec:27038:ed-1:v1:en (last accessed 24 April 2019).
[15] Id.
[16] See: The UK National Archives, Redaction toolkit, 14-15, available at http://www.nationalarchives.gov.uk/documents/information-management/redaction_toolkit.pdf (last accessed 24 April 2019)

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-027[1]

04 June 2019

[redacted]

RE: DISCLOSURE OF THE NAMES OF THE UNIT OWNERS/ MEMBERS OF A HOMEOWNERS' ASSOCIATION

Dear [redacted],

We write in response to your request for advisory opinion seeking clarification on whether NPC Advisory Opinion No. 2018-011, which recognized the disclosure of unit numbers of members of a condominium association as allowable, is applicable as well to the scenario where the names of the homeowners and tenants occupying the property are requested by members of the Mahogany Place 3 Homeowners' Association, Inc. (the Association). The purpose of the request is for verification if the property in the subdivision is being used for commercial purposes.

We understand from a subsequent email communication that the use of a unit for any business activity for profit is prohibited under the Association's House Rules. We understand further that a neighboring unit owner of the subject unit suspected of engaging in commercial activity, the same allegedly being used as a satellite office without official permits, would like to file a case to determine if there is a violation of this policy. In preparation to pursuing his legal remedies, the property management is requested to provide the list of names of the unit owners and tenants therein.

Names of members of the Association as personal information; criteria for lawful processing; legal obligation to which the personal information

[1] Tags: personal information; lawful processing; general data privacy principle; proportionality

controller is subject

The names of the members of the Association, their respective unit numbers, and the names of their tenants are considered as personal information. Section 12 of the DPA provides for the various criteria for lawful processing of personal information, which includes processing that is necessary for compliance with a legal obligation to which the personal information controller is subject.[2]

In relation to the above, Section 7 of the Magna Carta for Homeowners and Homeowners' Associations[3] (Magna Carta) provides:

> "SEC. 7. Rights of a Member. - An association member has full rights: xxx
>
> (b) to inspect association books and records during office hours and to be provided upon request with annual reports, including financial statements;"

In your case, the Association has a legal obligation to its members, rooted in Section 7 of the Magna Carta, to provide access to, and allow inspection of corporate records and documents. The DPA does not operate to curtail existing rights of members of a homeowners' association, specifically on inspection of association books and records, subject to existing laws and regulations on such matters.[4]

General data privacy principle; proportionality

The above notwithstanding, the pivotal issue is the determination of whether there is any other way the requesting member could verify if the property is being used for commercial purposes and pursue the appropriate legal remedies without necessarily having access to the personal information of the homeowners and tenants of the subject unit.

Pursuant to the general data privacy principle of proportionality, the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.[5] Personal data shall be processed only if the purpose of the

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 12 (c) (2012).
[3] An Act Providing for a Magna Carta for Homeowners and Homeowners' Associations, and For Other Purposes [Magna Carta for Homeowners and Homeowners' Associations], Republic Act No. 9904 (2010).
[4] See: National Privacy Commission, NPC Advisory Opinion No. 2018-011 (Mar. 22, 2018).
[5] Data Privacy Act of 2012, § 18 (c).

processing could not reasonably be fulfilled by other means.[6]

With this, the Association may act on the report or possible complaint of one member for a violation of the Association's House Rules without necessarily providing such member the names of the alleged violators of the House Rules.

Should an investigation, hearing, or any other process be conducted as part of the Association's dispute resolution, the same should follow due process requirements under existing laws and regulations, including the Articles of Incorporation and By-Laws of the Association. In such process, the details of the parties involved would then be necessarily disclosed at the most appropriate time.

We likewise reiterate NPC Advisory Opinion No. 2018-011 – that the more pertinent rules that shall govern your inquiry are the Revised Corporation Code of the Philippines, the Magna Carta, as well as the Articles of Incorporation and By-Laws of the Association. The above may provide more applicable information on the rights of members as to inspection and access to the Association's books and records.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[6] Id

ADVISORY OPINION NO. 2019-028[1]

01 Aug 2019

[redacted]

Re: PUBLICATION OF LIST OF CASES FILED AGAINST EMPLOYERS FOR NON-PAYMENT OF SOCIAL SECURITY CONTRIBUTIONS

Dear [redacted],

We write in response to your request which sought clarification on whether the publication in the newspaper or posting in the Social Security System (SSS) website of a list of cases filed against the employers for non-payment of social security contributions and pending before the Social Security Commission (SSC) will be in violation of the Data Privacy Act of 2012 (DPA).[2]

Condonation Program; publication or posting of docket numbers and names of employers with pending and decided cases involving non-payment of SSS contributions

Pursuant to the Social Security Act of 2018 (SSA), specifically Section 4(a) thereof, the SSC has the power to condone, enter into a compromise or release, in whole or in part, such penalties imposed upon delinquent social security contributions regardless of the amount involved under such valid terms and conditions it may prescribe through rules and

[1] Tags: Scope of the DPA; lawful processing of personal data; posting of cases;
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

regulations when the financial position of the employer demonstrates a clear inability to pay the assessed delinquency arising from economic crisis, serious business losses or financial reverses, or resulting from natural calamity or man-made disaster without fault on the part of the employer.

In connection therewith, Circular No. 2019-004 on the Condonation and Non-Imposition of Penalties on Delinquent Social Security Contributions dated 15 March 2019, provides for the mechanics on how delinquent contributors may remit, in full or through an installment proposal.

To carry out the objectives of the Condonation Program, you intend to publish or post the following:

- cases pending before the SSC which involves collection of contributions; and
- cases with final judgment but pending compliance by employers.

The list to be published will include case docket numbers and names of employers. The purpose of publication is to inform concerned employers so they can avail of the program and for them to verify the status of their cases before the Office of the Executive Clerk of the SSC.

Scope of the DPA; criteria for lawful processing of personal data; general data privacy principles; proportionality

We wish to reiterate that the DPA applies only to processing of personal information pertaining to a natural person. Article 44 of the Civil Code of the Philippines[3] provides:

> "Article 44. The following are juridical persons:
>
> (1) The State and its political subdivisions;
> (2) Other corporations, institutions and entities for public interest or purpose, created by law; their personality begins as soon as they have been constituted according to

[3] An Act To Ordain And Institute The Civil Code Of The Philippines [Civil Code of the Philippines], Republic Act No. 386 (1949)

law;

(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."

Based on the foregoing, corporations are considered as juridical persons. Hence, the processing of a juridical person's information is outside the scope of the DPA. The publication in the newspaper or posting in the SSS website of cases of corporations may be allowed for purposes of availing the condonation program as provided under the SSA.

As to the processing of personal and sensitive personal information (collectively, personal data) of employers who are individuals or natural persons, i.e. sole proprietorships, the processing of the same may find support in the DPA, specifically Section 12(e) – when processing is necessary in order to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate and/or Section 13(b) – when processing is provided for by existing laws and regulations.

Nevertheless, we wish to emphasize that while the processing of personal data in this case is for the fulfillment of a statutory mandate, the SSC, as a personal information controller, is required to observe and adhere to the data privacy principles of transparency, proportionality and legitimate purpose, and uphold the rights of data subjects.

Specifically for proportionality, the principle requires that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.[4] Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[5]

There is a need to determine if publication in a newspaper or posting online the names of individual employers with cases, pending or otherwise, is proportional to the purpose of informing them about the condonation program so that they can avail of the same. In lieu of publication or posting, it may be advisable to send communications directly to such employers to encourage them to avail of the program

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

and to actively disseminate information about the program in all appropriate media.
This opinion is based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts.

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-029[1]

17 July 2019

[redacted]

[redacted]

Re: REQUEST FOR ENDORSEMENT / RULING ON THE USE OF THIRD-PARTY PROCESSOR

Dear [redacted],

We write in response to your letter which sought guidance on the use of the Web-based Census and Accreditation System (Web-CAS) by the Philippine College of Chest Physicians (PCCP) in the processing of personal information. Specifically, you are concerned about the following:

1. Whether or not the decision of PCCP to subcontract its processing of personal information to a third-party under a data processing agreement is allowed by Data Privacy Act (DPA)[2]; and
2. Whether or not sharing of patient's information, limited to hospital's name, date of admittance and discharge, location, medical procedures, and initial and final diagnosis, to PCCP and its third-party processor based on explicit consent of the patient is lawful under the DPA.

[1] Tags: outsourcing, third-party processor, consent, accreditation and training purposes,
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

Web-based Census and Accreditation System; health information for accreditation and training purposes; consent

The PCCP, a subspecialty society of the Philippine Medical Association, is tasked to provide accreditation services to various training hospitals and healthcare providers to ensure effective healthcare delivery in the field of pulmonary medicine.

In order to ensure that a member hospital meets the standards set by the PCCP, such hospital is required to submit personal data of their patients to PCCP through an online system called Web-based Census and Accreditation System (Web-CAS). This system will be used for the efficient and effective monitoring and recording of training activities and quality assurance of training hospitals nationwide.

Relevant to this, we have issued an advisory opinion[3] stating that the use of patient's health information for accreditation and training purposes requires consent from the patient, otherwise, only de-identified information may be lawfully processed.

Accordingly, the PCCP resolved to obtain consent as legal basis when collecting the following personal data of patients:

- Name of hospital
- Data of admittance and discharge
- Location
- Medical procedures
- Initial and final diagnosis

Outsourcing the processing of personal data

Section 14 of the DPA provides that a personal information controller (PIC),[4] PCCP in this case, may subcontract the processing of personal data which includes outsourcing the development and maintenance of the Web-CAS.

[3] National Privacy Commission, NPC Advisory Opinion No. 2018-056 (5 October 2018).
[4] Data Privacy Act of 2012, § 3 Definition of Terms, (h) Personal information controller refers to a person or o 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:

The outsourcing arrangement shall be governed by a contract or other legal document that binds the PCCP and the third party as a personal information processor[5] (PIP). Section 44 of the Implementing Rules and Regulations (IRR) of the DPA sets forth the requirements to be considered in such outsourcing agreements.

Furthermore, both PIC and PIP shall ensure that reasonable and appropriate security 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,6 including having mechanisms in place for the exercise of data subjects' rights, are implemented.

Consent as basis for processing health information for accreditation purposes; general data privacy principles;
advisory opinions as guidance

As stated in Advisory Opinion No. 2018-05[6], personal data of the patient may be lawfully processed by the PCCP and its PIP if the patients or their legally authorized representative has given consent specific to the purpose of accreditation and training.

Correspondingly, the PCCP is required to adhere to the principles of transparency, legitimate purpose and proportionality. The patients must be made aware of the nature, purpose, and extent of the processing of personal data, as well as the risks and safeguards involved, and how they may be able to exercise their rights as data subjects.

Also, PCCP shall process information that is adequate, relevant, necessary, and not excessive in relation to its purpose of ensuring the quality of training provided by member hospitals. It is likewise paramount to ensure the quality of data collected – that it be accurate, and rectified in case of incomplete or inaccurate data, and that personal data is only retained for as long as it is necessary.

Finally, we wish to emphasize that the advisory opinions of the National Privacy Commission (NPC) provide guidance to the requesting party and the general public[7] on matters relating to the interpretation of

[5] Data Privacy Act of 2012, § 3 Definition of Terms, (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.
[6] Data Privacy Act of 2012, § 20.
[7] National Privacy Commission, Rules of Procedure on Requests for Advisory Opinions, Circular No. 2018-01 [NPC Circular 18-01] (September 10, 2018), § 2.

the provisions of the DPA, its IRR, and NPC issuances, compliance requirements, enforcement of data privacy laws and regulations, and other related matters on personal data privacy, security, and protection.[8] As such, an advisory opinion will not rule on or provide an endorsement of a particular method of processing that a PIC may have chosen.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. Note that the attached agreements and consent form were not reviewed for purposes of this advisory opinion.

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) IVY D. PATDU
*Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

*Per letter issued by the Office of the President dated 12 July 2019.

[8] Id., § 5(a).

ADVISORY OPINION NO. 2019-030[1]

01 Aug 2019

[redacted]

Re: REQUEST FOR LIST OF BUSINESS INDUSTRIES AND THE NAMES OF REGISTERED BUSINESSES IN EACH INDUSTRY IN SORSOGON CITY FOR RESEARCH PURPOSES

Dear [redacted],

We write in response to your letter request seeking clarification on the applicability of the Data Privacy Act of 2012 (DPA)[2] to a request for information made by a graduate student from the Bicol University.

Said student requested for the following data from your office: (1) list of business industries in Sorsogon City and (2) names of businesses in each industry registered with the BPLO from year 2008-2018. The requested data shall be used for the student's thesis on "Assessment on Survival Phase from Introduction to Growth stage of SMEs in Sorsogon City."

You asked for clarification on the following matters in relation to the above and the article which you have read regarding the DPA and the exception for research:

- What does the phrase "provided that no activities are carried out and no decisions are taken regarding the data subject" mean?
- The data being requested are so many, should I issue the

[1] Tags: scope; personal information; research; exceptions; proportionality
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

same even though the research title is tentative?

- Does the thesis warrant that the requested data be issued to the client? Or just the number of establishment per industry?

Scope of the DPA; information on classification of business industries and business names

We wish to reiterate that the DPA applies only to the processing of all types of personal information by any natural and/or juridical person involved in personal information processing.[3] The law 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 reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[4]

Business establishments are juridical persons. Thus, generally speaking, the name of a business establishment and the classification of the nature of its business are a juridical person's information, and not personal information.

Article 44 of the Civil Code of the Philippines define juridical persons, to wit:

"Article 44. The following are juridical persons:

(1) The State and its political subdivisions;

(2) Other corporations, institutions and entities for public interest or purpose, created by law; their personality begins as soon as they have been constituted according to law;

(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."

In this instance, the information requested from your office are not personal information as defined under the DPA. On its face, the lists

[3] Id. § 4.
[4] Id. § 3 (g)

of business industries and business names do not directly identify an individual, save in certain circumstances where the business involves a sole proprietorship.

Nonetheless, the DPA recognizes various criteria for processing personal information under Section 12 thereof, specifically, where 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.[5] This may be a lawful basis for disclosing business names of sole proprietors for research purposes. But there is a need to consider whether trade names will be sufficient without necessarily disclosing the names of the individual sole proprietors.

For guidance, to determine if there is "legitimate interest" in processing personal information, personal information controllers (PICs) must consider the following:[6]

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

Likewise, even if we consider such personal information as being outside of the scope of the DPA as the same will be processed for research, we reiterate NPC Advisory Opinion No. 2019-017,[7] which discussed the implications of the DPA to the conduct of academic research vis-à-vis access to documents and records in the custody of government, to wit:

[5] Id. § 12 (f).
[6] See generally, Data Privacy Act of 2012, § 12 (f); United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ (last accessed on August 1, 2019).
[7] National Privacy Commission, NPC Advisory Opinion No. 2019-017 (March 5, 2019).

> "It is the intent of the DPA to grant processing of personal information for research purposes with much flexibility. It recognizes that research is critical to nation-building and serves the interest of the public.
>
> ... However, the law provides special cases where the processing of personal information is excluded from its scope. One is the processing of personal information "for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards."
>
> Note, however, that the law does not provide for blanket exemption for research. Such exemption is limited to the minimum extent of collection, access, use, disclosure or other processing necessary to achieve the specific purpose, function or activity.
>
> Hence, researchers have the concomitant obligations to implement the necessary security measures to protect the personal data they process, uphold the rights of data subjects, and adhere to data privacy principles and the other provisions of the DPA."

Data subject's rights; limitation on rights; non-applicability

Section 19 of the DPA provides for the non-applicability of the rights of data subjects where the processing of personal information is only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject. The last portion of the provision means that the personal information processed for research shall not be used as a basis for taking measures or making any decisions regarding any particular individual.[8]

Nevertheless, we wish to emphasize that any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research.[9]

General data privacy principles; proportionality

PICs, such as government agencies, are required to adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality when processing personal information. Specifically

[8] See: Directive 95/46/EC of the European Parliament and of the Council, Article 13 (2) (1995).
[9] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 37 (2016).

on proportionality, said principle requires that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.[10] Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[11]

With this, PICs are not precluded from seeking further clarification from researchers as to the purpose of their studies and from there, make a determination of whether the requested information is absolutely necessary for the said purpose, in keeping with the practice of data minimization.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[10] Data Privacy Act of 2012, § 11 and Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (c) (2016)
[11] Id.

ADVISORY OPINION NO. 2019-031

5 September 2019

[redacted]

[redacted]

Re: ACCESS TO AND PROCESSING OF MEDICAL RECORDS FOR CANCER REGISTRIES

Dear [redacted],

We write in response to your letter request for an advisory opinion on whether St. Luke's Medical Center – Bonifacio Global City (SLMC-BGC) and St. Luke's Medical Center, Quezon City (SLMC-QC) (collectively, SLMC) are allowed under the Data Privacy Act of 2012[1] (DPA) to provide access to patient medical records and collection of information from said records by the Department of Health (DOH) – Rizal Cancer Registry of the Rizal Medical Center (RMC) and the Philippine Cancer Society, Inc. (PCS) – Manila Cancer Registry.

In its letter to SLMC-BGC, RMC is requesting access to and collection of pertinent data involving cancer cases occurring among residents of Metro Manila and Rizal Province for the years 2013-2017 gathered from death certificates for the purpose of determining the true incidence of cancer in the population, and for RMC to gather incidence magnitude of the cancer problem and enable to better formulate and evaluate the cancer control program. RMC cited Ministry of Health Circular No.

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

126-A dated 12 December 1983.[2]

To implement the request, research assistants will be sent to SLMC-BGC to review and extract data not only from the chart of patients who died at SLMC-BGC but also relevant Medical Records, Out-Patient Records, Autopsy Records and records of the Department of Pathology, Cytology, Hematology, Radiology, Ultrasound, Nuclear Medicine, CT Scan, MRI and Tumor Registry Board.

On the other hand, PCS requested for access and collection of SLMC-QC's cases of cancer diagnosed from residents of Manila, Pasay, Caloocan, and Quezon cities, the municipalities of Metro Manila and the Rizal Province for the years 2014-2017. PCS will review the chart of patients who died at SLMC-QC collected through death certificates. Pertinent information will be collected from Medical Records, Out-Patient Records, Department of Pathology, Hematology, Radiotherapy and Tumor Registry or Board, wherever appropriate.

You now inquire whether SLMC should allow access and provide the requested data to RMC and PCS given the limitations of the DPA.

Processing of health information allowed based on law and regulation

Medical records, out-patient records, autopsy records, records from the Department of Pathology, Cytology, Hematology, Radiology, Ultrasound, Nuclear Medicine, CT Scan, MRI and Tumor Registry Board contain health information of SLMC patients. As mandated by our data privacy law, any information about an individual's health is classified as sensitive personal information, and the processing of such is prohibited, except in cases stipulated in Section 13 of the DPA. For processing to be lawful, the law requires that at least one of the criteria for processing must exist.

Particularly, Section 13 (b) of the DPA states:

> (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:

[2] Ministry of Health, Population-Based Cancer Registry a. Central Tumor Registry of the Philippines and b. Cancer Control Program in the Rizal Medical Center, Ministry of Health Circular No. 126-A [Ministry Circular No. 126-A] (December 12, 1983).

> 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.

We understand that there is already a law which requires the establishment of a National Cancer Registry and Monitoring System. Republic Act No. 11215 or the National Integrated Cancer Control Act was signed last February 14, 2019.

Section 28 thereof requires the DOH to establish a national cancer registry and monitoring system, which shall be a population-based system, while Section 29 requires hospitals to have their own cancer registries, whereby cancer registry data shall be submitted to the DOH as a requirement for renewal of license to operate a hospital. Both sections of the law recognize explicitly that the processing of the personal data for such registries shall be in accordance with the DPA. The law's Implementing Rules and Regulations (IRR) specifically provides that the national cancer registry shall include existing quality population-based cancer registries and shall expand to other strategically defined geographical areas.[3]

We understand that the RMC and PCS,[4] a government institution and a private institution, respectively, are existing population-based cancer registries in the Philippines. The DOH Rizal Cancer Registry and the PCS Manila Cancer Registry are responsible for collecting and analyzing the cancer data in their respective areas.[5]

From the foregoing, both RMC and PCS may be allowed to collect the relevant health information from SLMC in order to administer their respective population-based cancer registries and in accordance with the provisions of the National Integrated Cancer Control Act.

Since Section 13 (b) allows the processing of sensitive personal information when the same is provided by law and regulation, the consent of the patients or data subjects is no longer necessary.

---

[3] Rules and Regulations Implementing the National Integrated Cancer Control Act, Republic Act No. 11215, § 28 (2019).

[4] We understand PCS-MCR was formerly the "Central Tumor Registry of the Philippines" which is the registry mentioned in Ministry of Health Circular No. 126-A, s. 1983. See: Philippine Cancer Society, Local Publications, available at http://www.philcancer.org.ph/learn-about-cancer/local-publications/ (last accessed May 21, 2019).

[5] Ministry of Health, Ministry Circular No. 126-A, s. 1983 (Dec. 12, 1983).

With the above, it is worth noting that while consent may not be required, by virtue of the principle of transparency, SLMC should make the necessary steps in ensuring that patients are aware their health information is being accessed by the DOH, RMC, and PCS, the purpose and extent of such processing, and how the patient can exercise his or her rights as a data subject. This may be accomplished through a privacy notice.

Furthermore, SLMC should bear in mind the principle of proportionality, such that the processing of health information is adequate, relevant, suitable necessary and not excessive in relation to the declared and specific purpose of the cancer registry. Should SLMC believe that the registries are collecting excessive information, it may seek clarification from RMC and PCS. SLMC should also develop processes and policies to ensure that health information not related to the said purpose is not unduly accessed, collected or processed.

Lastly, it is essential for SLMC to implement reasonable and appropriate organizational, technical and physical security measures to ensure that the personal data to be collected by the research assistants and/or other personnel of RMC and PCS shall receive an adequate level of protection against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

SLMC, together with RMC and PCS, should develop and implement policies and procedures on the method of reviewing and extracting personal data, and the means of securely transmitting these to RMC and PCS. SLMC may also require the mandatory execution of non-disclosure agreements with these research assistants and/or other personnel who shall be processing the medical records.

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

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-032[1]

12 September 2019

[redacted]

Re: STORAGE AND SHARING OF ELECTRONIC MEDICAL RECORDS (EMR)

Dear [redacted],

We write in response to your letter request for an advisory opinion which sought to clarify two issues in your company's business operations:

- What data protection measures that your organization may further take involving the storage of personal and sensitive personal information of patients; and
- What measures should be taken in complying with the Data Privacy Act of 2012[2] (DPA) with respect to the sharing of the analysis and anonymized disease and medical treatment information.

As stated in your letter, MedCheck E-Commerce, Inc. (MedCheck) is a healthcare clinical data company specializing in the collection and analysis of Real World Evidence (RWE), through a cloud-based EMR software, for non-communicable diseases. This is done through working with medical practitioners and researchers to digitally automate the collection of medical data which can be used to produce data registries and research findings to improve patient care.

[1] Tags: electronic medical records; anonymization; security measures

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 13 (a) (2012).

We understand from your letter that medical record information entered by physicians and their staff into the system are stored by MedCheck in a cloud-based system. Medical records include personal and sensitive personal information, such as medical information about the patient and the assessment made by the respective physician on disease diagnosis and recommended treatment/s. MedCheck then encrypts and anonymizes the same and subsequently stores patients' personal information and unidentifiable medical statistics into two separate servers which are both encrypted at rest.

We likewise understand, as per your representation, that MedCheck's business model is focused on aggregating the anonymized medical statistics, specifically anonymized disease and treatment data, from its physicians' practices. Collection of such data is made with the consent of the physicians and is aimed at providing the medical community with medical statistics to improve healthcare practice, such as but not limited to, free access to medical statistics and the creation of databases and health registries.

MedCheck as a personal information controller (PIC)

The DPA defines a PIC as an organization which controls the collection, holding, processing or use of personal information.[3] A personal information processor (PIP), on the other hand, is a juridical person to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject.[4]

If MedCheck serves as an EMR Provider, limited to providing a platform for physicians to process health information for medical treatment purpose, then MedCheck for this particular activity is acting as a Personal Information Processor (PIP). It is clear, however, that data collected by the respective physicians from its patients through the system provided by MedCheck, will be further processed by MedCheck with the intent of using it for statistical and research purposes.

In fact, the data transferred to MedCheck is personal data for anonymization. To the extent that MedCheck has control over the further processing of personal data of the patients, specifically health data, it is acting as a Personal Information Controller (PIC). It is therefore subject to the obligations of a PIC under the DPA such

[3] Data Privacy Act of 2012, § 3 (h)
[4] Id. § 2 (n).

as processing personal data when lawfully allowed,[5] ensuring that reasonable and appropriate safeguards are implemented to protect personal information against any accidental or unlawful destruction, alteration and disclosure, and any other unlawful processing,[6] and upholding data subjects' rights, among others.

Consent of the patients; other lawful criteria for processing

The DPA considers medical and health information as sensitive personal information. Thus, the transfer of patients' medical and health information from a hospital to MedCheck for its further processing, i.e. storage, anonymization, research and/or statistical purposes, requires the consent of the patients.

We understand that when using personal data for medical research purpose, the processing should comply with the requirements of applicable laws, regulations, or ethical standards, including but not limited to obtaining an informed consent from the patient, unless the processing may be justified by some other lawful criteria provided for under the DPA.

It is also worth noting that the data subjects should also be informed on how their data shall be processed. For example, details on how the process of anonymization shall be done, how the data shall be stored, risks involved in the said processes, the safeguards MedCheck has in place to minimize the risks, etc. should be provided.

Additional security measures MedCheck should take regarding the storage of personal data

In the processing personal data, reasonable and appropriate organizational, physical and technical measures must be established by MedCheck to secure its storage.[7] This is pursuant MedCheck's obligation as a PIC to uphold the confidentiality of the personal data and the rights of the data subjects at all times.

We understand that MedCheck continuously encourages its physicians and medical practitioners to register their practice with the National Privacy Commission (NPC) and comply with the DPA and MedCheck's

[5] Id., § § 12-13.
[6] Id. § 20.
[7] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 25. .

data protection policies.

In addition, MedCheck should have technical security measures which may come in the form of policies, procedures, controls, technology and equipment to protect the organization's systems processing personal data. Specifically, the Implementing Rules and Regulations (IRR) of the DPA provide that such measures shall include the following:

a. A security policy with respect to the processing of personal data;
b. Safeguards to protect 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 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 incidents that can lead to 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; and
g. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.[8]

While security measures may not completely eliminate the risks involved in data processing, these minimize the effects of such risks on the data subjects.

Accordingly, MedCheck should be transparent to the data subjects on how these risks shall be addressed and its capacity as a PIC to address

[8] Id. § 28

the same. A privacy impact assessment (PIA)[9] on MedCheck's data processing system should be conducted. A PIA shall, among others, assist the organization in the identification, assessment, evaluation and management of the risks involved in the processing of personal data.[10] For a more comprehensive discussion on the conduct of a PIA, kindly refer to NPC Advisory No. 2017-03.

Security measures in the sharing of anonymized medical data and statistics with third parties

We understand that MedCheck is in the business of collection, analysis and sharing of anonymized medical data. For a more comprehensive discussion on the nature of anonymized data, we refer you to NPC Advisory Opinion No. 2017-27 dated 23 June 2017 on Anonymized Data for Marketing Analytics. To reiterate, anonymized data does not fall within the ambit of the DPA.

However, please duly note that the exclusion from the scope of the DPA shall only apply if all the requirements for the anonymization of data have been met. Otherwise, or if there are factors which may possibly identify the data subjects, the sharing of such data must strictly comply with the DPA considering that the processing involves not only personal but also sensitive personal information.

It is also worth noting that MedCheck receives personal data prior to its anonymization. Hence, such data is subject to the provisions of the DPA. We wish to reiterate that in the processing of medical treatment information where the same is not anonymized, the consent, if this is the basis for processing, should be given by the patients themselves and not the physicians. In all cases, patients as data subjects have the right to be informed and notified about the processing of his or her personal data pursuant to Section 16 of the DPA.

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

For your reference.

[9] National Privacy Commission, Guidelines on Privacy Impact Assessment, Advisory No. 2017-03 [NPC Advisory 17-03] (July 31, 2017)
[10] NPC Advisory No. 2017-03.

Very truly yours,

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

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-034[1]

02 September 2019

[redacted]

Re: CONSENT AND ITS WITHDRAWAL FOR EMPLOYMENT PURPOSES

Dear [redacted],

We write in response to your query which sought to clarify matters regarding the Data Privacy Act of 2012 (DPA),[2] specifically on the consent of job applicants and existing company employees. You sought our opinion on the following scenarios where employers require consent forms:

- as a pre-employment requirement, enumerating the various purposes for the same, i.e. candidate screening, salary offer calculation, as well the submission of police clearance, etc.;
- as an employment requirement where all the required information and purposes of data processing are enumerated including, but not limited to: issuance of a company ID, determination of health conditions and fitness to work, verification of employment history, facilitate processing of ATM payroll, assess, update and provide employee entitlements, approve and verify claims with respect to benefits granted by the company, improve and maintain effective employee administration, manage work activities and personnel, communication, maintenance of employment records, employee data in accounting and tax

[1] Tags: consent; freely given; specific; employees; employment; transparency; privacy notice; lawful processing.
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

system, team building activities, imposition of disciplinary actions, potential legal claims, and HR safety requirements and fire safety instructions; and

- allowing the company to conduct extensive background investigation during the probationary period of employment.

We understand that job applicants who refuse to sign the consent form would not be considered for employment, and those under probationary employment will not be considered for permanent employment.

Relating to the given scenarios, you specifically asked the following:

- What are the criteria applied by the Commission in assessing if the consent of the data subject was "freely given" and "specific"? Is the consent given by the data subjects under the scenarios considered freely given and specific?
- If the consent of the data subjects obtained under the foregoing scenarios fails to satisfy the requirements of the DPA and the Implementing Rules and Regulations (IRR), would the employer be required to divide its purposes for data processing into (a) lawful processing purposes (which do not require consent for processing) and (b) other specific purposes, and obtain the data subject's consent only for those other specific purposes?
- To what extent should an employer apply the requirements under the General Data Protection Regulation (GDPR)? If not applicable, please clarify the differences, if any, between the concept of consent under the DPA and consent under GDPR.
- If consent given by the data subject is not considered as freely given and specific, is it sufficient that they are given an opportunity to withdraw consent?
- Will the withdrawal of consent affect the lawfulness of the processing based on consent before its withdrawal? Should the processing be discontinued immediately or is it sufficient that it be discontinued as soon as practicable, particularly when immediate stoppage is not possible?

- Assuming that a data subject withdraws consent, but the processing may still fall under other instances of lawful processing under Sections 12 and 13 of the DPA, can a personal information controller (PIC) continue to process the personal data?
- Are PICs prohibited from using the terms "consent" or "agree" in the privacy notice or consent form addressed to data subjects with information required under Section 16(b) of the DPA if the PICs know from the very beginning that even if the data subject withdraws consent, they will still process the personal data in accordance with some other lawful purpose under the DPA?

Criteria applied in assessing if consent was "freely given", "specific" and "informed"

Under Section 3(b) of the DPA, consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Thus, the definition of consent indicates three requirements, namely: freely given, specific, and informed indication of will.

In order to assess whether a data subject's consent was "freely given," "specific" and "informed," the DPA requires adherence to the principle of transparency, requiring PICs to inform data subjects 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 PIC, his or her rights as a data subject, and how these can be exercised.[3] Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.[4] Thus, validity of consent will depend on the data subject's comprehension of the disclosures made by the PIC. It is only with sufficient comprehension that a data subject will be able to exercise real choice in providing consent.

Further, we note the pertinent discussions in Opinion 15/2011[5] on the definition of consent of the Article 29 Data Protection Working Party

[3] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (2016).
4 *Id.*
[5] European Commission, Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 13 July 2011, pages 12-13, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (last accessed: 27 May 2019).

of the European Commission, specifically on whether the same may be considered as freely given in the context of an employer-employee relationship, to wit:

> "Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent. If the consequences of consenting undermine individuals' freedom of choice, consent would not be free. xxx xxx xxx
>
> An example of the above is provided by the case where the data subject is under the influence of the data controller, such as an employment relationship. In this example, although not necessarily always, the data subject can be in a situation of dependence on the data controller - due to the nature of the relationship or to special circumstances - and might fear that he could be treated differently if he does not consent to the data processing. xxx xxx xxx
>
> Reliance on consent should be confined to cases where the individual data subject has a genuine free choice and is subsequently able to withdraw the consent without detriment. If, once consent is withdrawn, the data processing continues based on another legal ground, doubts could be raised as to the original use of consent as the initial legal ground: if the processing could have taken place from the beginning using this other ground, presenting the individual with a situation where he is asked to consent to the processing could be considered as misleading or inherently unfair."

In addition, Opinion 2/2017[6] on data processing at work reinforces the above:

> "WP29 has previously outlined in Opinion 8/2001 that where an employer has to process personal data of his/her employees it is misleading to start with the supposition that the processing can be legitimised through the employees' consent. In cases where an employer says they require consent and there is a real or potential relevant prejudice that arises from the employee not consenting (which can be highly probable in the employment context, especially when it concerns the employer tracking the behaviour of the employee over time), then the consent is not valid since it is not and cannot be freely given. Thus, for the majority of the cases of employees' data processing, the legal basis of that processing cannot and should not be the consent of the employees, so a different legal basis is required.
>
> Moreover, even in cases where consent could be said to constitute

[6] European Commission, Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, 8 June 2017, pages 6-7, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 (last accessed: 27 May 2019).

> a valid legal basis of such a processing (i.e. if it can be undoubtedly concluded that the consent is freely given), it needs to be a specific and informed indication of the employee's wishes..."

For the requirement that consent be specific, Article 29 Data Protection Working Party opined[7] that "specific consent is therefore intrinsically linked to the fact that consent must be informed. There is a requirement of granularity of the consent with regard to the different elements that constitute the data processing: it cannot be held to cover 'all the legitimate purposes' followed by the data controller. Consent should refer to the processing that is reasonable and necessary in relation to the purpose."[8]

Granularity of consent necessarily dictates that in the case of multiple purposes, different purposes must be unbundled, and separate consent must be obtained for each purpose. As we stated in our Advisory Opinion 2018-063, "[c]onsent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them."[9] PICs may determine which purposes may be grouped together or separated based on what is reasonable and necessary and obtain separate consent for each accordingly.

Furthermore, consent must be intelligible. It should refer clearly and precisely to the scope and the consequences of the data processing. Consent cannot apply to an open-ended set of processing activities. This means that the context in which consent applies is limited. [10] Considering such, a PIC may ask for more than one consent for every purpose it may have. By doing so, a data subject is given more preference as to how their information will be processed rather than obtaining an "all or nothing" consent which cannot be considered freely given.

In addition, consent shall be evidenced by written, electronic or recorded means. Any of the required formats may be adopted by a

---

[7] European Commission, Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 13 July 2011, page 17, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (last accessed: 27 May 2019).

[8] *Id.*

[9] National Privacy Commission, NPC Advisory Opinion No. 2018-063 (October 23, 2018) citing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119), Recital 32.

[10] *Id.*

PIC as the NPC does not maintain any preference. Nonetheless, it is worth emphasizing that regardless of the format of the consent given by the data subject, it must be freely given, specific, and informed and not necessarily just a positive act showing a data subject has opted in.[11]

Necessity of requiring employer to divide the purposes for data processing; other lawful criteria for processing aside from consent

The processing of personal information is permitted under the DPA when at least one of the conditions provided under Section 12 is present. As to sensitive personal information, its processing is prohibited except when there exists any of the cases enumerated under Section 13 of the DPA.

As enunciated in NPC Advisory Opinion No. 2017-050:

> A Personal Information Controller (PIC), such as your employer, can also process personal information when it is necessary and is related to the fulfillment of a contract with the data subject, such as a contract for employment. This would include computation and payment of salaries and other benefits, determination of career movements, facilitation of work-related requirements, and outsourcing of human resource management functions.
>
> Another instance is when the processing of personal information is necessary for compliance with a legal obligation to which the personal information controller is subject and when processing is provided for by existing laws and regulations. This would include compliance with statutory and regulatory requirements of national government agencies, to which your employer is subject to.
>
> In fact, consent in the abovementioned instances may not even be required by the DPA, since the processing would fall under another criteria for lawful processing.
>
> Note also the special cases where the DPA is not applicable on certain specified information, i.e. information necessary in order to carry out the functions of public authority. Hence, the processing of your personal data as an employee in compliance with labor and tax laws are actually outside of the scope of the DPA, to the minimum extent necessary to achieve the specific purpose, function, or activity of the public authority.[12]

From the foregoing, it is clear that consent is not the only basis for an

[11] National Privacy Commission, NPC Advisory Opinion No. 2017-007 (Jan. 9, 2017).
[12] National Privacy Commission, NPC Advisory Opinion No. 2017-050 (Aug. 29, 2017).

employer to lawfully process personal data. In relation to processing with multiple purposes, PICs should be cognizant of all processing activities by conducting a Privacy Impact Assessment (PIA) to come up with a data inventory, description of the processing operations, assessment of the necessity and proportionality of the processing, and assessment of the risks, among others. Through the PIA, the PIC will be able to determine the most appropriate lawful criteria for such processing, which in the case of employment-related processing need not necessarily be consent.

Consent under the DPA vis-à-vis consent under GDPR

Consent was defined in the European Union (EU) General Data Protection Regulation (GDPR) in the following manner:

> 'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[13]

On the other hand, Section 3(b) of the DPA specifically defines consent thus:

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

The above definitions are essentially the similar. While it is true that the Commission often examines EU opinions, laws, and jurisprudence for analogous cases in interpreting the provisions of the DPA, as the latter was highly influenced by the 1995 EU Data Protection Directive, the predecessor of the GDPR, we reiterate the statement in NPC Advisory Opinion 2017-009[14] that the Philippines is not a member of the European Union and therefore not bound by its policies (1995

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119, Article 4 (11) (2016).

[14] National Privacy Commission, NPC Advisory Opinion No. 2017-009 (Jan. 16, 2017).

EU Directive and its successor, GDPR). Neither is the DPA nor its IRR meant to directly enforce the said EU regulations.

Thus, for processing that is under the scope of the DPA, the requirements relating to consent as provided therein shall prevail. Should an employer be likewise subject to the GDPR, such employer shall adhere to both the DPA and the GDPR.

Data subject's rights; withdrawal of consent

When consent is the lawful basis for processing, data subjects have the right to object and withhold consent to the processing of his or her personal data, unless the processing is under the following conditions:

1. The personal data is needed pursuant to a subpoena;
2. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or
3. The information is being collected and processed as a result of a legal obligation.[15]

Where consent is the proper basis for processing, and the same is withdrawn by the data subject, the same should not affect the lawfulness of the processing before the withdrawal of such consent. However, the same is not true in cases where the consent given does not meet the standards set by the DPA. In such cases, other lawful criteria must serve as basis for the processing of information because merely giving a data subject an opportunity to withdraw an irregularly-given consent will not cure such defect. Consent that is not freely given and specific will be tantamount to an implied consent which cannot be sanctioned by the Commission.

In all instances therefore, PICs are reminded to have policies and processes in place to document the consent obtained, its subsequent withdrawal, as well as the procedure on discontinuing the processing of personal data.

Privacy notices; consent forms; right to be informed

[15] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 34 (b) (2016).

Further in your inquiry, clarification is being sought whether the use of the words "consent" or "agree" in privacy notices or consent forms is prohibited in cases where PICs know from the beginning that even if the data subjects withdraw their consent, personal data will still be processed.

We reiterate NPC Advisory Opinion No. 2018-013[16] which discussed at length the difference between privacy notices and consent:

> "...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.
>
> Having stated that, there is also a need to determine and clarify the distinction between privacy policy and securing the consent of the data subject for the processing of his or her personal information.
>
> Being a mere notice, it is emphasized that the privacy policy or notice is not equivalent to consent. This document is an embodiment of the observance of the data privacy principle of transparency and upholding the right to information of data subjects. xxx
>
> On the other hand, obtaining consent from the data subject for the purposes of processing his or her personal data is a different requirement altogether."

Hence, using such words in a privacy notice is not advisable as the same should be used in a consent form instead.

As mentioned above, PICs should be able to determine the most appropriate criteria for processing personal and sensitive personal information. PICs should not get consent if the same is not appropriate and necessary in relation to the purpose of processing, and especially in instances where the PIC is already aware that such processing will still continue despite the withdrawal of consent.

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

For your reference.

[16] National Privacy Commission, NPC Advisory Opinion No. 2018-013 (April 18, 2018).

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-035[1]

6 November 2019

[redacted]

RE: CONSENT OF DATA SUBJECTS PRIOR TO SHARING OF PERSONAL DATA

Dear [redacted],

This refers to your letter-request received by the National Privacy Commission (NPC) for an advisory opinion on whether it is necessary to secure the consent of data subjects prior to sharing of their personal data in relation to the proposed data sharing arrangement.

Based on your letter, the Department of Human Settlements and Urban Development (DHSUD) and its five (5) attached Key Shelter Agencies (KSAs) namely, the Home Development Mutual Fund (HDMF), National Housing Authority (NHA), Social Housing Finance Corporation (SHFC), National Home Mortgage Finance Corporation (NHMFC) and Human Settlements Adjudication Commission (HSAC) will be signing a Data Sharing Agreement (DSA).

The purpose of the data sharing is to facilitate the Housing Beneficiaries Monitoring and Evaluation System (HBMES) which involves the sharing of the personal information of the beneficiaries of the KSAs with the DHSUD as the central repository of all personal data.

The sharing of personal information shall primarily enable the DHSUD and the KSAs to strictly implement the "one-time availment" policy and to ensure that the limited government allocation for housing shall be given to the underprivileged Filipino families.

[1] Tags: Consent; Department of Human Settlements and Urban Development (DHSUD); social housing; regulatory function; beneficiaries; statutory mandate.

You now inquire on whether the consent of all beneficiaries or data subjects are required prior to the sharing of their personal data, considering the provisions of the Data Privacy Act of 2012[2] (DPA), specifically Section 4 (e) thereof.

Scope of the DPA; special cases; data sharing; compliance with the DPA

The DPA provides for a list of specified information that are not covered by the law. Section 5 of its Implementing Rules and Regulations (IRR)[3] provides for the special cases wherein the law and the rules are not applicable. Specifically, Section 5 (d) may find application in this scenario:

Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law. Nothing in this Act shall be construed as having amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);

Being an exception to the rule, it must be established that the information claimed to be outside the scope of the law is:

1. Necessary in order to carry out the law enforcement or regulatory functions of the public authority;
2. Processing of personal data is for the fulfillment of a constitutional or statutory mandate;
3. Applies only to the minimum extent of collection, access, use, disclosure, or other processing necessary for the purpose; and
4. Presupposes that there is strict adherence to all substantive and procedural processes.[4]

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission and other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 4 (e) (2012).
[3] Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012" (24 August 2016).
[4] See: National Privacy Commission, NPC Advisory Opinion No. 2018-079 (Oct. 23, 2018).

Regulatory Functions of the Public Authority; Constitutional or Statutory Mandate

Section 5(d) of the DPA is interpreted to the effect that a government agency having a constitutional or statutory mandate to collect and process personal data may do so even without the consent of the data subject in the exercise of its regulatory function. But this is with the concomitant responsibility of ensuring that organizational, physical and technical security measures are in place to protect the personal data it is processing.[5]

In relation to the above, Republic Act No. 11201 or the Department of Human Settlements and Urban Development Act provides that the DHSUD shall be the sole and main planning and policy-making, regulatory, program coordination and performance monitoring entity for all housing, human settlement and urban development concerns, primarily focusing on the access to and the affordability of basic human needs.[6]

Said law has also mandated the DHSUD to develop and adopt a national strategy to immediately address the provision of adequate and affordable housing to all Filipinos and ensure the alignment of the policies, programs and projects of its KSAs in achieving the said objectives.[7] Consequently, this includes ensuring that there is no repeat availment of housing services among the beneficiaries.

We understand also that all the KSAs are attached agencies[8] of the DHSUD, having their respective mandates under the Department of Human Settlements and Urban Development Act and their pertinent Charters. The proposed data sharing between should also find constitutional or statutory basis in the charters of the KSAs.

We emphasize that government agencies may share or transfer personal data under its control or custody through a DSA in order to facilitate the performance of a public function or the provision of a public service.[9]

---

[5] Id.

[6] An Act Creating the Department of Human Settlements and Urban Development, Defining Its Mandate, Powers and Functions, and Appropriating Funds Therefor [Department of Human Settlements and Urban Development Act], Republic Act No. 11201, § 4 (2018).

[7] Ibid.

[8] Department of Human Settlements and Urban Development Act, § 12 and 22.

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

Necessity and Proportionality; adherence to substantive and procedural process

Furthermore, government agencies as personal information controllers, must be able to show that the processing of personal data is necessary to their regulatory functions, and that the processing shall be limited to achieving the specific purpose, function or activity. In order to be considered necessary, the data collection should not be excessive as to purpose of processing and the manner of collection should not be unduly intrusive.

PICs remain to be subject to the requirements of implementing measures to secure and protect personal data.[10] Protecting the rights of data subjects should be a consideration in all stages of the processing.

Lawful criteria for processing; law and regulation

The DHSUD may also rely on the other provisions of the DPA, particularly Sections 12 and 13 which provides for the various criteria for lawful processing of personal and sensitive personal information, respectively, i.e. processing is necessary for compliance with a legal obligation, processing is provided for by existing laws and regulations, etc.

Considering that there is a need for DHSUD, as the regulatory authority mandated by R.A. 11201, to ensure one time availment among the beneficiaries of housing services and assuming all the attached agencies have similar mandate, the data sharing may no longer require consent of the data subjects.

As to the form and contents of the proposed DSA, please refer to the provisions of NPC Circular No. 2016-02 - Data Sharing Agreements Involving Government Agencies available at our website at https://www.privacy.gov.ph/memorandum-circulars/npc-circular-16-02-data-sharing-agreements-involving-government-agencies/, for guidance and additional information.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate

[10] See: National Privacy Commission, NPC Advisory Opinion No. 2017-035 (July 27, 2017).

issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-036[1]

3 July 2019

[redacted]

Re: COLLECTION AND USE OF PATIENT CASE NUMBER AND APPOINTMENT OF COMPLIANCE OFFICER FOR PRIVACY

Dear [redacted],

We write in response to your inquiry which sought to clarify matters regarding the requirements of the Data Privacy Act of 2012[2] (DPA) vis-à-vis the collection and use of patients' case numbers for the Philippine Obstetrical and Gynecological Society (Foundation), Inc. (POGS) Nationwide Statistics System (PNSS) and as a requirement for doctors applying for eligibility to take diplomate examinations.

In addition, you sought to clarify if POGS can appoint compliance officers for privacy (COPs) in its eleven (11) Regional Chapters, in lieu of data protection officers (DPOs).

POGS Nationwide Statistics System (PNSS); National Census Project; patients' case numbers; requirements for diplomate examinations; proportionality

We understand that POGS has a National Census Project which involves a nationwide electronic census platform using the PNSS deployed

[1] Tags: personal information controller, personal information processor, proportionality, data sharing agreement, outsourcing agreement, compliance officer for privacy

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

in POGS-accredited hospitals. The project involves two applications developed by LeapFroggr (LF): (a) census application and (b) cloud portal to aggregate and generate reports on the anonymized data collected by the census application.

We understand further that POGS will have an outsourcing agreement with hospitals to share the counts or number of incidents of the following, among others:

- OB diagnosis
- Delivery information
- Neonatal information
- Pediatric age/weight and congenital anomalies
- Gyne diagnosis
- Procedures related to the cases mentioned
- Obstetric and gyne mortality counts and causes

For purposes of accuracy and reliability, the Board of Trustees of POGS suggested the inclusion of the patients' case numbers in the data to be transmitted by the hospitals as this will attest to the transmitted number of counts as true and correct.

In addition, POGS will be able to use the case numbers to verify the authenticity of the submitted requirements of doctors applying for diplomate examinations.

Scope of the DPA; personal information; statistical, aggregated data; lawful processing

The DPA applies to the processing of all types of personal information by any natural and/or juridical person involved in personal information processing.[3] The law 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 reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[4]

[3] Id. § 4.
[4] Id. § 3 (g).

Hence, aggregate or statistical data are not considered as personal information under the DPA since such data cannot identify an individual.

We understand that LF's cloud portal will be used to aggregate and generate reports on the anonymized data collected by the census application. As such, the data that will be processed will be de-identified. Thus, what was previously considered personal and sensitive personal information (collectively, personal data) will be rendered anonymous. Therefore, as previously mentioned, these statistical, aggregate, and de-identified datasets are no longer personal information as defined in the DPA, hence, outside the scope of the law.

However, with the inclusion of the case numbers, the collected information will fall within the purview of personal data since it will be possible to ascertain the identity of each patient.

As such, its processing shall be subject to the provisions of the DPA, making it imperative for data subjects to be notified that personal data pertaining to him or her are being or have been processed, pursuant to their right to be informed. Likewise, data subjects' consent must be obtained prior to collection and use of their data, unless the processing of such personal data will fall under any other criteria for lawful processing under Section 13 of the DPA.

General data privacy principles; privacy by design and default

In developing and implementing the National Census Project, POGS must be mindful of the provisions of the DPA and its Implementing Rules and Regulations (IRR), specifically on adhering to the general data privacy principles of transparency, legitimate purpose and proportionality, implementing reasonable and appropriate organizational, physical, and technical security measures, and upholding data subjects' rights.

As such, POGS must integrate privacy and data protection in all processing activities of the National Census Project, considering the nature of the personal data that requires protection, the risks to the rights and freedoms of the patients as data subjects, current data privacy best practices, among others.[5]

[5] See: Data Privacy Act of 2012, § 20.

As for the purpose of verifying the authenticity of submitted requirements for diplomate examinations, we refer you to NPC Advisory Opinion No. 2018-016, where a hospital asked for guidance on the issue of submitting reports on the actual cases handled by resident physicians for diplomate board exam and accreditation, to wit:

> "CMC's disclosure of the patients' data for purposes of fulfilling the resident physicians' submission requirements for diplomate board exam and accreditation to the PCS and POGS may be allowed under the DPA provided that the patient has provided consent.
>
> The NPC understands that patients' personal data are necessary in order to avoid fraud cases. An option to consider is to pseudonymize the patients' data prior to disclosing the same. Pseudonymization consists of replacing one attribute (typically a unique attribute) in a record by another. While pseudonymization lessens the risks, personal data which have undergone pseudonymization remains to be personal data, hence, consent is still necessary.
>
> In the event that the CMC can no longer obtain consent from the patients, there should be design methods and techniques wherein the PCS and POGS can validate that the cases handled by the resident physicians are true and correct without involving disclosure of personal data to the said professional societies. This may be in form of a certification from the CMC."[6]

From the foregoing, patients' case numbers need not be collected by POGS as the purpose of the processing could be fulfilled by other means, such as a certification from the respective hospitals that the submitted requirements of doctors for diplomate examinations are true and correct.

POGS may likewise consider alternatives in the processing of the census data and verifying the authenticity of submitted requirements for diplomate examinations vis-à-vis the patients' case numbers, i.e. implementing pseudonymization,[7] having the verification process done at the hospital level before the transmission of data to the cloud portal, etc.

[6] National Privacy Commission, NPC Advisory Opinion No. 2018-016 (April 12, 2018), citing the Data Privacy Act of 2012, Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, and the EU General Data Protection Regulation, Recital 26.
[7] See: National Privacy Commission, NPC Advisory Opinion No. 2018-029 (June 6, 2018).

Data sharing; outsourcing; data sharing agreement

As defined in the IRR, data sharing pertains to the disclosure or transfer to a third party of personal data under the custody of a personal information controller (PIC) or a personal information processor (PIP) wherein such transfer was directly instructed by the PIC. The data sharing agreement then refers to the contract which contains the terms and conditions of a dating sharing arrangement between two or more PICs.[8]

On the other hand, Section 3(d) of NPC Circular No. 16-02 defines outsourcing as the disclosure or transfer of personal data by a PIC to a PIP, while an outsourcing agreement pertains to the disclosure or transfer of personal data by the PIC to a PIP in order for the latter to process the data according to the instructions of the controller.[9]

With this, there is a need to clarify the roles of POGS, LF, and the hospitals in order to determine the obligations and responsibilities of the parties under the DPA, its IRR, and issuances of NPC, since there are two key differences that exist between data sharing and outsourcing.

First, all parties to a data sharing agreement are considered as PICs under the law. In a subcontracting or outsourcing agreement, there has to be at least one PIC and one PIP. Second, in terms of purpose or objective, each party to a data sharing agreement has its own reason for processing the personal data involved, while in a subcontracting or outsourcing agreement, a PIP has no other purpose or objective for processing the personal data other than that imposed by the instructions of the PIC.[10]

POGS and LF may enter into an outsourcing or subcontracting agreement as it is commonly understood, and not necessarily as described under Sections 43-45 of the IRR of the DPA, if LF will not be processing any personal data for POGS in the course of the development of the applications and provided that LF will not be using the data for its own purpose. It likewise follows that there is no need for a data sharing agreement as defined above.

[8] National Privacy Commission, NPC Advisory Opinion No. 2017-57 (October 3, 2017).
[9] National Privacy Commission, NPC Advisory Opinion No. 2017-008 (January 9, 2017).
[10] Id

As to the POGS-accredited hospitals, we understand that the data to be shared by them are anonymized data. It is understood that information is anonymous when such information "does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[11]

The sharing of such anonymized data is not an outsourcing activity as contemplated in the definition above. Hence, such sharing arrangement for the anonymized data may be covered by an appropriate contract as determined by the parties. However, if the hospitals will be sharing personal data to POGS, the proper contract to execute is a data sharing agreement.

Appointment of a compliance officer for privacy (COP)

We understand that each of the Regional Chapters of POGS is a separate juridical entity registered with the Securities and Exchange Commission (SEC). Nonetheless, programs of the Regional Chapters are aligned with the purposes and projects of the POGS National Office, and regional activities are subject to the approval of the National Board of Trustees.

As provided for in NPC Advisory No. 2017-01,[12] PICs in the private sector may designate COPs, subject to the approval of the NPC and the provisions of said Advisory. Specifically, a group of related companies may appoint or designate the DPO of one of its members to be primarily accountable for ensuring the compliance of the entire group with all data protection policies. Where such common DPO is allowed by the NPC, the other members of the group must still have a COP.

Under this scenario, the POGS National Office's DPO may be appointed or designated as a common DPO, and each of the Regional Chapters shall have their COPs. The request for approval of the designation of a common DPO may be done by writing a letter addressed to the NPC Compliance and Monitoring Division (CMD). For further information

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119, Recital 26 (4 May 2016).

[12] National Privacy Commission, Designation of Data Protection Officers, Advisory No. 2017-01 [NPC Advisory No. 17-01] (March 14, 2017).

on the above, you may contact the NPC CMD at compliancesupport@privacy.gov.ph and 234-22-28 local 118.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-038[1]

24 October 2019

[redacted]

Re: COLLABORATION WITH INSURANCE COMPANIES FOR ACCESS TO CONTACT DETAILS OF DATA SUBJECTS FOR PURPOSES OF PRODUCT RECALL

Dear [redacted],

We write in response to your inquiry which sought to clarify matters regarding the Data Privacy Act of 2012[2] (DPA), particularly on the legitimate purpose in seeking assistance from and collaborating with insurance companies for access to the updated personal information and contact details of the insured vehicle owners, in relation to the on-going campaign of Honda Cars Philippines, Inc. (HCPI) for the product recall pertaining to the replacement of vehicle parts/components relating to the safety of the vehicle and its passengers.

HCPI has experienced low campaign and completion ratio (CCR) with respect to the product recall because HCPI's customer records are no longer current. Many of the notices sent by HCPI to owners of affected vehicles has been returned unserved.

Hence, HCPI would like to request from insurance agencies or companies for the updated contact details of insurance policy holders with Honda vehicles for the sole purpose of enabling HCPI to reach out to those covered by the product recall. HCPI anticipates that the insurance agencies or companies will be apprehensive about sharing personal data of their insured clients because of the provisions of the

[1] Tags: personal information, legitimate purpose, lawful processing vitally important interests.
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

DPA.

Vitally important interests of data subject; further processing of a data subject's personal information

Based on your representation, HCPI's proposed processing of the personal data of the insured vehicle owners is with the intention of protecting the vitally important interests of the said Honda car owners, pursuant to Section 12(d) of the DPA, thus, there is a need to inform as many of the current vehicle owners as possible of the product recall.

However, the EU General Data Protection Regulation (GDPR),[3] the successor of the EU Data Protection Directive (Directive 95/46/EC) which highly influenced the DPA, provides further insight on this particular lawful criterion for processing, to wit:

> "The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters."[4]

Also, the UK Information Commissioner's Office discussed "vital interest" as intended to cover only interests that are essential for someone's life, and generally only applies to matters of life and death.[5] It is likely to be particularly relevant for emergency medical care.[6] Finally, in order to rely on this criterion, the processing must be necessary - if one can reasonably protect the data subjects' vital interests in another less intrusive ways, this basis will not apply.[7]

---

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Recital 26.

[4] Id., Recital 46.

[5] UK Information Commissioner's Office, Vital interests, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/ (last accessed: 27 August 2019).

[6] Id.

[7] Id.

From the foregoing, it seems that such criterion for lawful processing to protect the vitally important interests of data subjects is not squarely applicable for the HCPI's processing vis-à-vis its product recall campaign.

Other lawful bases for processing; contract; legitimate interest

HCPI may consider the other lawful criteria for processing of personal information as provided for in Section 12, i.e. processing is necessary and is related to the fulfillment of the contract[8] of sale in relation to HCPI's obligation to warrant the goods against any hidden defects or legitimate interest[9] of HCPI. For the insurance companies, they may be able to process and disclose the insured's information based on its duty to fulfill the contract of insurance or even the legitimate interest of the insurance company.

In any case, HCPI and the insurance companies are advised to determine the most appropriate basis for the sharing or disclosure of such personal information, with due consideration of the rights and freedoms of the data subjects.

General data privacy principles; proportionality

The processing of personal information must adhere to the data privacy principles of transparency, legitimate purpose, and proportionality. As such, the data subject must be aware of the nature, purpose and extent of the processing of his or her personal data including the risks and safeguards involved, the identity of the personal information controller, his or her rights as data subject, and how these rights can be exercised. With regard to proportionality, the processing of information must be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.[10] Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[11]

From the foregoing, the proposed HCPI collaboration with the insurance companies for access to the updated personal information of the insured vehicle owners should strictly be limited to the sharing

[8] Data Privacy Act of 2012, §12(b).
[9] Id., § 12 (f).
[10] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).
[11] Id.

of the personal information which is adequate and necessary for the on-going product recall campaign.

In addition, HCPI should also consider the availability of other measures to inform such owners of the product recall, i.e. launching an intensified information campaign through various traditional media and social media, utilizing the resources of its dealerships across the country to intensify the campaign, among others. HCPI may likewise request the insurance companies to check their respective records and determine if there are insured Honda vehicles which are qualified for the product recall. Such insurance companies may then directly inform these insured car owners of the HCPI's product recall campaign.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-039[1]

03 September 2019

[redacted]

Re: REQUEST FOR TAX DECLARATION

Dear [redacted],

We write in response to your letter which sought clarification regarding your request to secure copies of tax declarations, certificates of title, and tax clearances of real properties from the Assessor's Office and the Treasurer's Office of the City of Antipolo vis-à-vis the provisions of the Data Privacy Act of 2012[2] (DPA).

We understand that you are the counsel for Manila Water Company, Inc. (MWCI). Pursuant to the Concession Agreement of Manila Water with the Metropolitan Waterworks and Sewerage System (MWSS), the former acts as an agent of the latter. In line with the relevant provisions of Concession Agreement, MWCI embarked on a pipeline laying project which necessitates the conduct of due diligence on the identity, ownership, possession and valuation of properties that may be duly affected by the project, hence this request for the copies of the abovementioned documents.

We understand that the Assessor's Office and the Treasurer's Office of the City of Antipolo claim that the names and addresses of the property owners are personal information that are protected under the DPA.

[1] Tags: tax declarations; scope; lawful processing of personal data;
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

Scope of the Data Privacy Act of 2012; regulatory function; public authority

The DPA applies to all types of processing of personal information subject to certain qualifications.[3] The disclosure of documents containing personal or sensitive personal information (collectively, personal data) is considered processing. Under the DPA, processing of personal data shall be allowed, subject to compliance with the law and adherence to the principles of transparency, legitimate purpose, and proportionality. By way of exception, the DPA recognizes that certain specified information is outside its scope.

One of these special categories is "information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the … regulatory agencies of their constitutionally and statutorily mandated functions."[4] In order to apply, it must be established that the information claimed to be outside the scope of the law is:

1. The information is necessary to carry out the regulatory or law enforcement functions of a public authority;
2. These functions are provided for by the Constitution or by law;
3. The processing is only to the minimum extent of collection, access, use, disclosure, or other processing necessary for the purpose; and
4. There is strict adherence to all substantive and procedural processes.[5]

The above is interpreted to the effect that a government agency having a constitutional or statutory mandate to collect and process personal data may do so even without the consent of the data subject in the exercise of its regulatory function.[6] The information requested may be released to MWCI if the same documents may properly be released to MWSS, under its legal mandate. This comes with the concomitant responsibility of ensuring that organizational, physical and technical security measures are in place for data protection.[7]

[3] Id. § 4.
[4] Data Privacy Act of 2012, § 4 (e).
[5] See generally, National Privacy Commission, NPC Advisory Opinion No. 2018-079 (Oct. 23, 2018).
[6] See: National Privacy Commission, NPC Advisory Opinion No. 2017-035 (July 27, 2017).
[7] Id.

In this case, the personal data needed by MWCI, acting as an agent of MWSS, which is a regulatory agency pursuant to RA No. 6234,[8] may be outside of the scope of the DPA, but subject to the above requisites as well as the provisions of their Concession Agreement.

Lawful criteria for processing of personal and sensitive personal information; general data privacy principles

MWCI may rely on the other provisions of the DPA, specifically Sections 12 and 13 which provides the criteria for lawful processing of personal and sensitive personal information, respectively. These sections clarify that consent of the data subject is just one of the possible bases for processing. Personal information controllers (PICs), such as the City of Antipolo and MWCI, should make their own determination of the proper basis for the disclosure, depending on the nature of the personal data being processed.

Property laws vis-à-vis the DPA

The provisions of Presidential Decree No. 1529,[9] Act No. 496,[10] and other applicable laws and regulations on the matter should be read together and harmonized with the DPA. For instance, in order to quiet title to real property or remove clouds therefrom, processing is recognized under the DPA for purpose of the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims.[11]

In Advisory Opinion No. 2018-083,[12] it was emphasized that "the DPA is not meant to prevent government institutions from processing personal data when necessary to fulfill their mandates. Rather, it aims to protect the right to information privacy while ensuring free flow of information. What the DPA does is to promote fair, secure, and lawful processing of such information."

Public documents; publicly available information

The belief that tax declarations and tax clearances are not protected

[8] An Act Creating The Metropolitan Waterworks And Sewerage System And Dissolving The National Waterworks And Sewerage Authority; And For Other Purposes, Republic Act No. 6234 (1971).
[9] Amending and Codifying the Laws Relative to Registration of Property and for other Purposes [Property Registration Decree], Presidential Decree No. 1529 (1978).
[10] An Act to Provide for the Adjudication and Registration of Titles to Lands in the Philippine Islands [The Land Registration Act], Act No. 496 (1902).
[11] Data Privacy Act of 2012, § 13 (f).
[12] National Privacy Commission, NPC Advisory Opinion No. 2018-083 (Oct. 29, 2018).

by the DPA is misguided. A public document, or even publicly available information, by such fact alone, does not lose the protection afforded by the DPA in so far as the processing involves the personal data contained in such documents.

Further, Advisory Opinion No. 2017-030[13] discussed the processing of personal data which is available in the public domain, to wit:

"... the provisions of the DPA are still applicable even for those personal data which are available in the public domain. Note that the law has specified the information which is outside of its scope but only to the minimum extent necessary to achieve the specific purpose, function, or activity in Section 4 thereof.

There is no express mention that personal data which is available publicly is outside of its scope. Thus, "it is a misconception that publicly accessible personal data can be further used or disclosed for any purpose whatsoever without regulation."

... the PIC which collects and processes personal data from the public domain must still observe the requirements under the law, specifically on the criteria for lawful processing of personal, sensitive personal and privileged information found under Sections 12 and 13 thereof."

Likewise, reference to the case of Francisco v. Magbitang,[14] is misplaced. The ruling of the Court does not create an obligation on the part of government agencies to allow unrestricted access to tax declarations. Documents under control and custody of government agencies remain to be subject to the protection of the DPA. Even Executive Order (EO) No. 02 operationalizing Freedom of Information in the Executive Branch[15] admits of certain limitations such as those that pertain to the privacy of individuals and those that may affect security.

The EO clarifies that "while providing access to information, public records, and official records, responsible officials shall afford full

[13] National Privacy Commission, NPC Advisory Opinion No. 2017-030 (June 28, 2017), citing Office of the Privacy Commissioner for Personal Data, Hong Kong, Guidance Note - Guidance on Use of Personal Data Obtained from the Public Domain, August 2013, available at https://www.pcpd.org.hk/english/publications/files/GN_public_domain_e.pdf

[14] G.R. No. 48132 (1989).

[15] Office of the President, Operationalizing In The Executive Branch The People's Constitutional Right To Information And The State Policies To Full Public Disclosure And Transparency In The Public Service And Providing Guidelines Therefor, Executive Order No. 2 [EO No. 2] (July 23, 2016).

protection to the right to privacy of the individual."[16] For this purpose, it requires that each government office shall ensure that personal information in its custody or control is disclosed or released only if it is material or relevant to the subject-matter of the request and its disclosure is permissible under this EO or existing law, rules or regulations, among others.[17]

We note also the provision of Act No. 496 which you discussed, wherein all records and papers relating to registered land in the office of the Register of Deeds shall be open to the public, but the same is subject to reasonable regulations as may be prescribed by the Land Registration Authority. This reinforces the rationale that the public documents are still duly protected and access to the same may still be regulated.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[16] EO No. 2, § 7.
[17] Id.

ADVISORY OPINION NO. 2019-040[1]

17 October 2019

[redacted]

Re: ANTI-MONEY LAUNDERING COUNCIL REQUEST

Dear [redacted],

We write in response to your letter which sought clarification regarding the request from the Anti-Money Laundering Council (AMLC) for documents pertaining to a certain business entity in Antipolo City. The AMLC is requesting for certified true copies of the following:

1. Business Permits;
2. Duly accomplished application form;
3. Payment History;
4. Account Subsidiary Ledger with Gross Receipts and Capital; and
5. Other relevant documentary requirements submitted by the business entity in relation to the application for/ renewal of business permits:
    a. Income statement;
    b. Contract of Lease;
    c. Land Title/Tax Declaration; and
    d. Community Tax Certificate.

You seek clarification if your office may provide such documents of the business entity to the AMLC pursuant to its investigative functions under Republic Act No. 9160 or the Anti-Money Laundering Act of 2001.

[1] Tags: scope; personal information; data subject; lawful processing of personal data;

Scope of the Data Privacy Act of 2012; processing of personal information

The Data Privacy Act of 2012[2] (DPA) applies to the processing of all types of personal information by any natural and/or juridical person involved in personal information processing.[3] The law 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 reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[4]

Business establishments are juridical persons. Thus, generally speaking, the certified true copies of the above listed documents are the juridical person's information, and not an individual's personal information.

Article 44 of the Civil Code of the Philippines defines juridical persons, to wit:

> "Article 44. The following are juridical persons:
>
> (1) The State and its political subdivisions;
>
> (2) Other corporations, institutions and entities for public interest or purpose, created by law; their personality begins as soon as they have been constituted according to law;
>
> (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."

Nonetheless, as there may be personal and/or sensitive personal information (collectively, personal data) in such requested documents, the DPA recognizes various criteria for processing the same under Section 12, i.e. processing is necessary for compliance with a legal

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] Id. § 4.
[4] Id. § 3 (g).

obligation[5] or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate;[6] or Section 13, i.e. processing of the same is provided for by existing laws and regulations[7] or processing concerns 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.[8]

Hence, the BPLO may rely on the above lawful bases for processing, considering that the AMLC is vested with investigative functions under RA No. 9160.

We wish to emphasize that the DPA should not be an obstacle to the collection and processing of personal data by the various government agencies as long as the same is necessary for the fulfillment of their respective mandates. The law promotes fair, secure, and lawful processing of such information.[9] This is with the concomitant responsibility of complying with the requirements of the DPA, its Implementing Rules and Regulations, and other issuances of the National Privacy Commission.[10]

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[5] Data Privacy Act of 2012, § 12 (c).
[6] Id. § 12 (e).
[7] Id. § 13 (b).
[8] Id. § 13 (f).
[9] See: National Privacy Commission, NPC Advisory Opinion No. 2018-083 (Nov. 26, 2018).
[10] Id.

ADVISORY OPINION NO. 2019-041[1]

23 October 2019

[redacted]

Re: CREDIT CARD FRAUD INVESTIGATION

Dear [redacted],

We write in response to your inquiry seeking clarification on the provisions of the Data Privacy Act of 2012[2] (DPA) in relation to the Philippine Credit Card Industry Regulation Law[3] on credit card fraud investigations.

As stated in your letter, we understand that one of the main drivers of credit card fraud losses is the unauthorized or fraudulent transactions in e-commerce platforms or those involving online merchants, whereby credit cards are used by unauthorized persons to purchase goods.

We understand further that in order to combat this type of fraud and launch an investigation, the personal information submitted to the online merchant during the order taking is needed to be able to track the delivery of the goods sold, and thereafter apprehend the perpetrator with the assistance of law enforcement agencies.

You ask whether the disclosure of the personal information provided to the online merchants, such as the name, address, delivery address, email address, and mobile or other contact number, to the credit card issuers for purposes of fraud investigation, is allowed under the DPA.

[1] Tags: credit card fraud; investigations; lawful processing;
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] An Act Regulating The Philippine Credit Card Industry [Philippine Credit Card Industry Regulation Law], Republic Act No. 10870 (2016).

Credit card details; personal information; lawful processing

We consider the above details provided to the online merchants during the order taking as personal information, the processing of which should comply with the provisions of the DPA, its Implementing Rules and Regulations[4] (IRR), and related issuances of the National Privacy Commission (NPC).

Based on the given scenario, the disclosure of the personal information held by the online merchants to the credit card issuers for fraud investigation may fall under Section 12 (f) of the DPA, where processing is necessary for the purposes of the legitimate interests pursued by the personal information controller (PIC) or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[5]

In the determination of legitimate interest, PICs must consider the following: [6]

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

As to the disclosure of such personal information to law enforcement, regulatory, or investigative agencies, the same is also recognized under Section 12 (c) of the DPA, where processing is necessary for

[4] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).
[5] Data Privacy Act of 2012, § 12 (c) and (f).
[6] See generally, Data Privacy Act of 2012, § 12 (f); United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ [last accessed on June 11, 2018].

compliance with a legal obligation to which the PIC is subject, or Section 12 (e) - processing that is necessary to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.

Under any of these provisions, it is understood that the government agencies involved are processing information which is necessary to carry out their respective mandates as provided by law, and there is strict adherence to all substantive and procedural processes.

We also take note of the provisions of the Philippine Credit Card Industry Regulation Law. Section 16 of the law recognizes several instances where credit card issuers may disclose data of cardholders, to wit:

> "Section 16. Confidentiality of information. – Credit card issuers, their officers, employees and agents shall keep strictly confidential the data on the cardholder, except under any of the following circumstances:
>
> a. Disclosure is with consent of the cardholder;
> b. Customer information is released, submitted or exchanged with credit information bureaus, industry association, or card association;
> c. Upon orders of a court of competent jurisdiction or any government office or agency authorized by law, or under such conditions as may be prescribed by the Monetary Board of the BSP;
> d. Disclosure to third party service providers is necessary for the sole purpose of assisting or rendering service to the credit card issuer in enforcing its rights against the cardholder;
> e. Disclosure to third parties such as insurance companies is necessary for the sole purpose of insuring the credit card issuer from cardholder default or other credit loss, and the cardholder from fraud or unauthorized charges;
> f. Disclosure to third parties is for the purpose of investigating fraud or unauthorized activities or mitigating risk involving card issuance, use and acquiring. xxx." (underscoring supplied)

In this instance, disclosures by the credit card issuers of personal information pertaining to the unauthorized persons fraudulently using another person's credit card may be allowed (1) upon orders of a government office or agency authorized by law, or (2) for the purpose of investigating fraud or unauthorized activities.

General data privacy principles; proportionality; data subjects' rights

While the processing of personal information for the above purpose may be allowed under the DPA and relevant laws, online merchants, credit card issuers, as well as the pertinent government agencies still have the obligation to observe the general data privacy principles of transparency, legitimate purpose and proportionality, and take the necessary steps to protect and uphold the rights of the data subject.

Specifically for the proportionality principle, the same 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."[7]

Hence, the disclosure of the personal information should be limited to that which is relevant and necessary to the transaction under investigation, which in this case is limited to the name, address, delivery address, and contact details of the unauthorized person fraudulently using the credit card.

It is further recommended that credit card issuers and their partner-merchants implement reasonable and appropriate security measures to ensure that the personal information of cardholders are properly protected, endeavor to educate them on how to secure their credit cards against fraudulent activities, and have procedures in place whereby cardholders would be able to easily report lost or stolen credit cards and other suspicious transactions.

This is in keeping with the declared policy of the state to institute appropriate mechanisms to protect and educate credit cardholders, thereby ensuring the vibrancy and growth of the credit card industry.[8]

[7] Rules and Regulations Implementing the Data Privacy Act of 2012, § 17 (c).
[8] Philippine Credit Card Industry Regulation Law, § 2.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-042[1]

17 October 2019

[redacted]

Re: TAX DECLARATION

Dear [redacted],

We write in response to your letter which sought clarification on the release of the certified clear and complete copies of tax declarations of certain real properties.

We understand that a certain law firm requested for the abovementioned documents on behalf of its clients (herein referred to as "Spouses") in relation to your letter to the Spouses dated April 3, 2019 wherein you stated that the subject property of the Spouses appears to overlap with portions of several other titled real properties also declared for tax purposes, and that the Spouses may settle the matter of conflict of ownership in a court of proper jurisdiction.

The law firm claims that in order for the Spouses to fully appreciate the situation and to guide them in taking the proper course of action, they are requesting for the copies of the respective tax declarations of the properties which overlaps with the subject property.

You now ask the following:

1. Whether the request of the law firm will require the consent of the several affected declared owners/data subjects whose names and last known addresses are

[1] Tags: tax declarations; scope; lawful processing; data privacy principles; consent; data sharing agreement

printed on the face of the tax declarations; and

2. Regardless of the consent of the data subjects, does the City of Antipolo, through the Office of the City Assessor, still need to enter into a data sharing agreement with the law firm and their clients before processing their request.

Scope of the Data Privacy Act of 2012; lawful criteria for processing

The Data Privacy Act of 2012[2] (DPA) applies to all types of processing of personal information subject to certain qualifications.[3] The disclosure of documents containing personal or sensitive personal information (collectively, personal data) is considered processing. The law sets certain parameters under which personal data may be processed in a manner that is consistent with the general data privacy principles.

The Office of the City Assessor may rely on any of the provisions of Sections 12 and 13 of the DPA which provides the criteria for lawful processing of personal and sensitive personal information, respectively.[4] These sections clarify that consent of the data subject is just one of the possible basis for processing. For instance, the DPA provides that processing of personal information is permitted if necessary to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.[5]

Personal information controllers (PICs), such as the City of Antipolo, should make its own determination of the proper basis for the disclosure, depending on the nature of the personal data being processed.[6] They should evaluate whether the release of information is necessary for the fulfillment of its duties under existing laws and regulations.

Due consideration should also be given to the information requested and whether it is relevant and material to the declared purpose of the requesting party. In this case, the Spouses are requesting information to guide them in taking the proper cause of action. The Office of the City Assessor previously communicated to the Spouses the seeming

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] Id. § 4.
[4] See: National Privacy Commission, NPC Advisory Opinion No. 2019-39 (Sept. 3, 2019).
[5] Id. § 12(e); See also § 13(f).
[6] Id.

overlap of portions of the subject property and other declared properties belonging to other owners and the possible need to settle conflicts of ownership.

Data sharing; data sharing agreement

Data sharing is allowed when it is expressly authorized by law and adequate safeguards are in place, including adherence by the parties thereto to the general principles of transparency, legitimate purpose, and proportionality.[7]

Relative to this, the NPC issued NPC Circular No. 16-02 which sets out guidelines for data sharing agreements involving government agencies. Section 1 of the Circular provides:

> "SECTION 1. General Principle. To facilitate the performance of a public function or the provision of a public service, a government agency may share or transfer personal data under its control or custody to a third party through a data sharing agreement: Provided, that nothing in this Circular shall be construed as prohibiting or limiting the sharing or transfer of any personal data that is already authorized or required by law."

Considering that the request for copies of the tax declarations is in relation to or necessary for compliance with a legal obligation of the Spouses with the Office of the City Assessor, or may be based also on the fulfillment of the functions of your office as a public authority, whereby both instances are considered as lawful bases for processing of personal information under the DPA, the said request may be granted without necessarily executing a data sharing agreement between and/or among the parties concerned.

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

For your reference.

Very truly yours,

[7] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 20 (a) (2016).

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-043[1]

24 October 2019

[redacted]

Re: ACCESS TO PSA CIVIL REGISTRY DOCUMENTS FOR VERIFICATION PURPOSES

Dear [redacted],

We write in response to your letter which sought our opinion on three (3) matters raised by the Armed Forces and Police Savings and Loan Association, Inc. (AFPSLAI) in relation to the processing of the personal and sensitive personal information (collectively, personal data) of AFPSLAI's members.

The issues may be summarized as follows:

1. AFPSLAI offers automatic transmittal of capital contribution, loan, and pension remittances from the respective finance centers of the Armed Forces of the Philippines, Philippine Navy, Philippine Air Force, Philippine National Police, Philippine Veterans Affairs Office, Bureau of Fire Protection, Bureau of Jail Management Protection and other similar military/civilian branch, to facilitate related transactions. Upon knowledge of death of the member, the pertinent finance center notifies AFPSLAI to return the amount of remittances. There are instances, however, that AFPSLAI already knows of the death of a member and is ready to return the overpaid remittances,

[1] Tags: general data privacy principles; criteria for lawful processing; data sharing; data sharing agreement; civil registry documents

but the necessary proof of the fact of death, i.e. death certificate, cannot be acquired by AFPSLAI. Efforts have been made to communicate with the concerned heirs but to no avail. Hence, the over remitted funds kept on accumulating as accounts payable by AFPSLAI;

2. Members' loans are insured. Upon death, the insurance companies require the death certificate to release the insurance proceeds to be applied to the members' accountabilities. As mentioned above, there is difficulty in acquiring the death certificate; and
3. The Bangko Sentral ng Pilipinas (BSP) requires the AFPSLAI to ensure that all members are duly qualified. AFPSLAI's records reveal that there are associate members whose qualifications are in doubt as there are no documents to prove filiation with regular members. AFPSLAI sent letters to a number of these associate members for the submission of their birth and/or marriage certificates. However, many have not complied with the request.

In view of the above, AFPSLAI coordinated with the Philippine Statistics Authority (PSA). There is a draft Memorandum of Agreement (MOA) which contains the terms and conditions of AFPSLI's access to the PSA's Batch Request Entry and Query System (BREQS) and Data Matching of Records scheme.

You now ask for opinion on AFPSLAI's right to process the necessary documents in behalf of the members for the above purposes.

Criteria for lawful processing

AFPSLAI may rely on any of the provisions of Sections 12 and 13 of the Data Privacy Act of 2012[2] (DPA) which provides the criteria for lawful processing of personal and sensitive personal information, respectively.[3]

For all three issues, the processing may be related to a contract between AFPSLAI and the member, a legal obligation on the part of

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] See: National Privacy Commission, NPC Advisory Opinion No. 2019-39 (Sept. 3, 2019).

the AFPSLAI, or a requirement under a specific law, rule or regulation, i.e. Commission on Audit (COA) rules on affecting finance centers of the Armed Forces of the Philippines and/or the Philippine National Police, insurance laws or issuances of the Insurance Commission relating to insured loans, and/or BSP rules governing membership in non-stock savings and loans associations. AFPSLAI may likewise consider whether its processing is based on the establishment, exercise or defense of legal claims.

With the above, AFPSLAI should make a determination of the proper basis for the processing depending on the nature of the personal data being processed.

Data sharing; Memorandum of Agreement with the PSA

As defined in the IRR, data sharing pertains to the disclosure or transfer to a third party of personal data under the custody of a personal information controller (PIC) or a personal information processor (PIP) wherein such transfer was directly instructed by the PIC. The data sharing agreement then refers to the contract which contains the terms and conditions of a dating sharing arrangement between two or more PICs.

We understand that the MOA covers the Data Matching Records Scheme and the use of BREQS scheme (issuance of PSA civil registry documents) for the purpose of verification of status of AFPSLAI pensioners/members and their beneficiaries through the system to be provided by the PSA.

We provide the following general comments on the draft MOA pursuant to the provisions of NPC Circular No. 16-02 governing data sharing involving government agencies:

- There is a need to clarify Section 7.4 of the MOA, which requires AFPSLAI to submit various forms to PSA, i.e. Application Form, Consent Form, and Waiver and Authorization Form. It further provides that "AFPSLAI shall sign and accomplish all forms in behalf of its members/ relatives of members, in connection with the rationale and the legitimate purposes mentioned in the whereas clauses."

Note we were not provided with a copy of the abovementioned forms, and hence, these were not reviewed for purposes of this opinion.

To clarify, consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.
With the above, it is not appropriate for AFPSLAI to accomplish a consent form in behalf of its members/relatives of members, unless it has been specifically authorized by the data subjects for the said purpose.

As we understood it, AFPSLAI is already having difficulty in communicating with the members and/or their relatives with respect to requesting for the pertinent civil registry documents. With this scenario, it may not be feasible to require a consent form. As mentioned above, AFPSLAI's processing may be based on a number of various criteria for processing. Considering the attendant circumstances, consent may not be the most appropriate basis for the status quo.

Nonetheless, if moving forward and based on privacy impact assessment, AFPSLAI makes a determination that indeed, consent of the data subject is the proper basis for processing, it may then implement changes to its data processing systems whereby consent will be obtained from the data subject at the most opportune time.

- The MOA should have provisions on the following matters:

    1. Remedies available to a data subject, in case the processing of personal data violates his or her rights, and how these may be exercised;
    2. The designated data protection officers of AFPSLAI and PSA;

3. The personal information controller responsible for addressing information requests and complaints filed by a data subject and/or is being investigated by the Commission; and
4. Process through which a data subject may access a copy of the MOA.

The NPC, the DPA, its IRR, and issuances of the Commission do not limit the agreement of the parties provided that the agreement does not contravene the letter and intent of the law. The Commission fully subscribes to the fundamental legal tenet ascribing a presumption of regularity in the performance of functions by government agencies.

Finally, please note that a data sharing agreement does not prior approval from the NPC.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-044[1]

6 November 2019

[redacted]

Re: AUTHORITY TO SHARE CUSTOMERS' PERSONAL INFORMATION TO PARTNER LOAN PROVIDER

Dear [redacted],

We write in response to your letter requesting for an advisory opinion on sharing customers' personal information. As stated in your letter, CIS Bayad Center, Inc. (Bayad Center) accepts payments for Social Security System (SSS) contributions and stores the payment details including SSS numbers in the database for purposes such as addressing payment history inquiries, Bayad Center promotions, rewards, loyalty programs, advisories and updates, as well as credit scoring purposes upon a customer's request. These purposes are contained in the Data Privacy Consent Form filled out by your clients.

Further, we understand that there is a proposed contract between Bayad Center and its partner loan provider, Home Credit, for the latter's credit scoring of your customers. In the proposed contract, Home Credit will provide Bayad Center the SSS numbers of its loan applicants, which will then be cross-matched with Bayad Center's database. If a match occurs, Bayad Center will send to Home Credit the following: (1) biller code, (2) transaction amount, (3) transaction date, and (4) SSS number. If otherwise, no data shall be shared.

You now inquire whether Bayad Center customer's consent to the processing of their personal data for credit scoring purposes upon the customer's request and/or Bayad Center's loan provider partner's separate Consent Form clause will be sufficient to vest Bayad Center the authority to share its customers' data to Home Credit for credit

[1] Tags: consent of the data subject; lawful criteria processing; credit scoring; general data privacy principles; transparency; privacy notice; data sharing; data sharing agreement.

scoring.

Consent of the data subject required for processing of personal data for other purposes

Section 3(b) of the Data Privacy Act of 2012[2] 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. The law further provides that consent shall be evidenced by written, electronic or recorded means.

While the NPC was not furnished with Bayad Center's Consent Form, we note that in your letter, it was qualified that credit scoring was made "upon customer's request." This phrase, in effect, limits the consent for the processing of personal data given by the data subject to Bayad Center through the Consent Form such that the processing of customer's personal data for credit scoring shall be allowed only upon a separate request from the customer.

The DPA provides that the purpose for processing must be specific and declared to the data subject. Therefore, the Bayad Center's Consent Form filled out by its client alone, without the separate request for credit scoring is not sufficient to vest Bayad Center the authority to share its customers' personal data to its loan provider partner for credit scoring.

On the other hand, you have quoted paragraphs (2), (3), (4) and (7) of the Home Credit Consent Form. You inquire whether the provisions are sufficient to vest Bayad Center the authority to share its customers' data. You posit that Bayad Center is specifically mentioned as a Partner in the consent form. And even assuming that Bayad Center is not explicitly named as a Partner in the form, it is nonetheless included in the full list of partners in Home Credit's website.

We take note of item (3) of the consent form which provides:

> (3) I allow (loan provider), directly or through the Partners, to collect and process my personal information and sensitive personal information including my name, age,

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

> photographs, fingerprints, other biometric data (facial recognition and voice recognition), employment details, income, financial data, financial profile, credit standing, loan payment history, and other information required in the application form. I allow the use of these information for credit verification, credit scoring, data analytics, collection, automated processing of the loan, collecting, data profiling, direct marketing of products and services of Partners, and offering of existing and new financial services.

Given the above, Home Credit's loan applicants who duly sign the consent form have agreed to the processing of their personal data for credit scoring, and such personal data may be obtained from Home Credit's Partners. Thus, the collection of personal data, including the customer's biller code, transaction amount, transaction date and SSS number from Bayad Center for credit scoring may be allowed.

However, we take this opportunity to emphasize that Bayad Center, as a personal information controller (PIC), is ultimately responsible for compliance to the law, including adherence to the data privacy principles of transparency, legitimate purpose, and proportionality.[3] Under the DPA, each PIC is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing.[4]

In this case, on the part of Bayad Center's customers, it is unclear that the company will be sharing personal data to third parties even without their request. While there is basis for Bayad Center to disclose personal data to Home Credit on the basis of the latter's consent form, Bayad Center should be transparent to its customers and inform them of that their personal data will be processed for credit scoring should they be a loan applicant of Home Credit. At the very least, this information should be stated in Bayad Center's privacy notice.

Execution of a data sharing agreement required

Bayad Center and Home Credit should execute a data sharing agreement in accordance with Section 20 of the Implementing Rules and Regulations (IRR) of the DPA which provides that data sharing for

[3] Data Privacy Act of 2012, § 11.
[4] Data Privacy Act of 2012, § 21

commercial purposes, including direct marketing, shall be covered by a DSA.

The agreement shall establish adequate safeguards for the protection of personal data and uphold rights of data subjects.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-045[1]

6 November 2019

[redacted]

Re: CONFIRMATION OF DEATH BY THE PHILIPPINE STATISTICS AUTHORITY FOR DEBT WRITE-OFF BY THE PHILIPPINE GENERAL HOSPITAL

Dear [redacted],

We write in response to your e-mail received by the National Privacy Commission (NPC) requesting for an advisory opinion regarding data privacy concerns of the Philippine General Hospital (PGH) vis-à-vis its efforts to write-off receivables from private patients.

We understand from your e-mail that in order to write-off the hospital's bad debts, the death of the patient owing such must be established. The Commission on Audit (COA) auditor suggested that a certificate issued by the Philippine Statistics Authority (PSA) will be acceptable for the purpose. PGH submitted a preliminary list of possibly deceased persons for the PSA's confirmation but such request was denied by the PSA, citing the Data Privacy Act of 2012[2] (DPA) as its reason.

Death Certificate; sensitive personal information

A Death Certificate is an official document setting forth particulars relating to a dead person.[3] It contains details such as (a) date and place of death, (b) full name, (c) age, (d) sex, (e) occupation or profession,

[1] Tags: death certificate, sensitive personal information, Philippine Statistics Authority, lawful criteria for processing, law and regulation, COA audit

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

[3] Philippine Statistics Authority, Death Certificate, available at https://psa.gov.ph/civilregistration/requesting-civil-registry-document/death-certificate (last accessed Aug. 27, 2019).

(f) residence, (g) status as regards marriage, (h) nationality of the deceased, and (i) probable cause of death.[4]

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

Processing of sensitive personal information pursuant to existing laws and regulations

Considering that a Death Certificate contains sensitive personal information, disclosure is generally prohibited unless it falls within the cases provided for in Section 13 of the DPA, specifically, if processing is provided for by existing laws and regulations.

In this instance, a Death Certificate may be released by the PSA to PGH pursuant to Section 8.3 (b) (b1), in relation to Section 7.4 (b), of COA Circular No. 2016-005[5] which requires the submission of the death certificate for purposes of writing off dormant receivables of government agencies and instrumentalities arising from regular business transactions. This COA circular is applicable to PGH being the country's largest government tertiary hospital.

Stemming from above, PSA is not precluded from providing a copy of the Death Certificate to PGH since the COA Memorandum specifically enumerates the Death Certificate as one of the relevant documents to validate the existence of the condition allowing write-off.

While we are aware that the Death Certificate is the primary consideration to authorize the write-off of the hospital's bad debts based on the confirmed death of the debtor, only a limited amount of the information therein is actually needed to establish the condition to allow write off. As such, PSA may consider redacting the deceased's sensitive personal information prior to the release of the Death Certificate to PGH as an added security measure.

[4] Law on Registry of Civil Status, Act No. 3753, (1930).
[5] Commission on Audit, COA Circular No. 2016-005 (December 19, 2016).

As an alternative, PSA may opt to issue a separate certification to the effect that the PSA confirms the death of a person based on available records without necessarily issuing a copy of then Death Certificate itself.

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

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-046[1]

17 December 2019

[redacted]

Re: INTER-AGENCY COUNCIL AGAINST TRAFFICKING (IACAT) REQUEST FOR INFORMATION WITH THE PHILIPPINE STATISTICS AUTHORITY (PSA)

Dear [redacted],

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify whether or not the Data Privacy Act of 2012[2] allows for the disclosure of the personal information, specifically the age, of an alleged trafficking victim, by the Philippine Statistics Authority (PSA) to the Inter-Agency Council Against Trafficking (IACAT) for purposes of filing a criminal case for violation of Republic Act No. 9208.[3]

We understand that during the inquest proceedings of the foreign national arrested by the IACAT Region 7, the IACAT experienced difficulty in proving the age of the victim. We note that minority qualifies the offense under Section 6 of Republic Act No. 9208.

With the consent of the victim, IACAT requested the Philippine Statistics Authority (PSA) for the personal details of the victim, including the age. However, PSA refused to divulge any information, stating that it can only provide the requested information through a court-issued subpoena. As explained by the Regional Prosecutor, a request for the issuance of a subpoena from the court is not possible as the case is currently being investigated by the investigating prosecutor.

[1] Tags: Sensitive personal information, consent, lawful processing.
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] An Act to Institute Policies to Eliminate Trafficking in Persons Especially Women and Children, Establishing the Necessary Institutional Mechanisms for the Protection and Support of Trafficked Persons, Providing Penalties for its Violations, and for Other Purposes [Anti-Trafficking in Persons Act of 2003], Republic Act No. 9208 (2003).

Sensitive personal information; criteria for lawful processing; Section 13

Section 3 of the DPA provides the definition of sensitive personal information, which includes an individual's age. As a general rule, the processing of such information is prohibited unless any of the conditions provided for in Section 13 of the DPA is attendant. Specific to this scenario, the following lawful bases should be considered:

- The data subject has given his or her consent to the processing;[4]
- The processing is provided for by existing laws and regulations;[5] or
- The processing concerns such personal information as is necessary (1) for the establishment, exercise or defense of legal claims or (2) when provided to government or public authority.[6]

While Section 13 (a) of the DPA allows for the processing of sensitive information when there is consent of the data subject, the same must be freely given, specific and an informed indication of the will.[7] Only upon the concurrence of the three (3) elements can consent be considered valid.

In this case, however, the consent given by the trafficking victim may not be considered a valid consent because if indeed the trafficking victim is a minor, he or she cannot validly provide the consent needed under the DPA.[8]

*Processing based on law; establishment, exercise or defense of legal claims; information provided to governmen*t

With this, the more appropriate possible basis for the disclosure would be any existing law and regulation. As discussed above, RA No. 9208 qualifies the offense when the victim is a child. To prove the minority of the victim, it follows that the only credible source of information is the records of the PSA, specifically the victim's Certificate of Live

[4] Data Privacy Act of 2012, § 13 (a).
[5] Id. § 13 (b).
[6] Id. § 13 (f).
[7] Id. § 3 (b).
[8] See: National Privacy Commission, NPC Advisory Opinion No. 2017-49 (August 29, 2017).

Birth. Implicit in the law as well is the allowance for disclosure of the victim's personal circumstance, subject to the confidentiality clause provided for by Section 7 of RA No. 9208.

Disclosure may also be made pursuant to Article 7(3) of Presidential Decree No. 603[9] which allows the disclosure of a person's birth information to a court or proper public official whenever absolutely necessary in administrative, judicial or other official proceedings to determine the circumstances surrounding a person's birth. In this case, the disclosure of the birth information of the victim is necessary in the inquest proceeding to determine whether or not the foreign national is guilty of violating Republic Act No. 9208 as well as for the establishment, exercise or defense of legal claims of the victim.

Likewise, processing is also allowed when sensitive personal information is provided to government or public authority. The disclosure of the trafficking victim's age to IACAT may be allowed because such disclosure is pursuant to IACAT's mandate provided for in Section 21 of RA No. 9208. Specifically, IACAT is tasked to assist in the filing of cases against violators of the law as well as secure from any department, bureau, office, agency, or instrumentality of the government such assistance as may be needed to effectively implement the law.

We reiterate that the DPA is not meant to prevent government institutions from processing personal data when necessary to fulfill their mandates. Rather, it aims to protect the right to information privacy while ensuring free flow of information. What the DPA does is to promote fair, secure, and lawful processing of such information.[10]

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

For your reference.

Very truly yours,

[9] The Child and Youth Welfare Code [Child and Youth Welfare Code], P. D. No. 603 (2003).
[10] See: National Privacy Commission, NPC Advisory Opinion No. 2018-083 (Nov. 26, 2018).

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION NO. 2019-048[1]

20 December 2019

[redacted]

Re: DISCLOSURE OF RECORDS UNDER THE CUSTODY OF THE CITY CIVIL REGISTRAR

Dear [redacted],

We write in response to your request for an advisory opinion which sought to clarify whether the City Civil Registry Office (CCRO) of Iloilo may release records that contain personal data to agencies like the Social Security System (SSS), Bureau of Internal Revenue (BIR), Philippine Veterans Affairs Office (PVAO) if there is a formal request, and to the regular courts and other agencies upon issuance of a subpoena, without the consent of the document owner.

Scope of the DPA; processing of personal data by the CCRO

The Data Privacy Act of 2012[2] (DPA) and its Implementing Rules and Regulations (IRR) applies to the processing of all types of personal information and to any natural and juridical person in the government or private sector involved in personal information processing.[3]

We understand that the civil registry was established by law to record the civil status of persons[4] and that the City Civil Registrar has the primary function of keeping and preserving the following books and make the proper entries concerning the civil status of persons:

[1] Tags: disclosure of civil registry documents; scope; lawful processing of personal data;
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 4 (2016).
[4] Law on Registry of Civil Status [Civil Registry Law], Act No. 3753, § 1 (1930).

1. Birth and death register;
2. Marriage register, in which shall be entered not only the marriages solemnized but also divorces and dissolved marriages.
3. Legitimation, acknowledgment, adoption, change of name and naturalization register.[5]

Given the foregoing, civil registry documents contain personal and sensitive personal information. The DPA considers the collection, storage and sharing of records by the CCRO of Iloilo under its custody as processing activities and is thus covered by the DPA.[6] As a personal information controller (PIC), the CCRO must adhere to any of the lawful bases for processing provided under Sections 12 and/or Section 13 of the DPA.

Criteria of lawful processing of sensitive personal information; equest from government agencies and courts; PSA Memorandum Circular

The DPA provides that the processing of sensitive personal information is prohibited, except for certain instances provided by law.[7] In particular, exceptions include processing that is provided for by existing laws and regulations and 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.[8] Public authority is defined as any government entity created by the Constitution or law and vested with law enforcement or regulatory authority and functions.[9]

When processing is based on any of the above criteria, the consent of the document owner is no longer required. Further, the provisions above on the lawful processing of sensitive personal information of the DPA should be read together existing laws, rules, and regulations.

[5] Id. § 4.
[6] Data Privacy Act of 2012, § 4.
[7] Id. § 13.
[8] Id. § 13 (b) and (f).
[9] Rules and Regulations Implementing the Data Privacy Act of 2012, § 3(r).

We understand that the Philippine Statistics Authority (PSA) issued Memorandum Circular No. 2019 – 15 on Guidelines on the Issuance of the Civil Registry Documents (CRDs)/ Certifications including Authentication addressed to all City/Municipal Civil Registrars, among others.[10] The issuance lists down persons who may be allowed to request for the copy issuance of Civil Registry Documents/Certifications other than the document owner. Among those listed are as follows:

1. The court or proper public official whenever absolutely necessary in administrative, judicial or other official proceedings to determine the identity of the person; provided, that there must be a duly issued subpoena duces tecum and ad testificandum for the production of the civil registry document;[11] and
2. Request from other government agencies pursuant to their mandate; provided, that the requesting government agency executed Data Sharing Agreement with PSA in accordance with NPC Circular 16-02.[12]

We reiterate that the DPA is not meant to prevent government institutions from processing personal data when necessary to fulfill their mandates. Rather, it aims to protect the right to information privacy while ensuring free flow of information. What the DPA does is to promote fair, secure, and lawful processing of such information.[13]

We likewise emphasize that NPC Circular 16-02 on Data Sharing Agreements Involving Government Agencies provides that a government agency may share or transfer personal data under its control or custody to a third party through a data sharing agreement to facilitate the performance of a public function or the provision of a public service, and that the Circular shall not be construed as prohibiting or limiting the sharing or transfer of any personal data that is already authorized or required by law.[14]

Please note however, that although the disclosure of personal data is supported by a constitutional or statutory mandate of government agencies, the adherence to the principles of transparency, legitimate

[10] Philippine Statistics Authority, Guidelines on the Issuance of the Civil Registry Documents (CRDs)/ Certifications including Authentication, Memorandum Circular No. 2019-15 [PSA MC 2019-015] (June 11, 2019)
[11] Id. § II (6).
[12] Id. § II (7).
[13] National Privacy Commission, NPC Advisory Opinion No. 2018-083 (Nov. 26, 2018).
[14] National Privacy Commission, Data Sharing Agreements Involving Government Agencies, Circular No. 16-02 [NPC Circular 16-02] (October 10, 2016).

purpose and proportionality must still be complied with.[15] For this purpose, the CCRO shall ensure that personal data in its custody or control is disclosed or released only if it is material or relevant to the subject-matter of the request and its disclosure is permissible under the existing law, rules or regulations, among others.

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

For your reference.

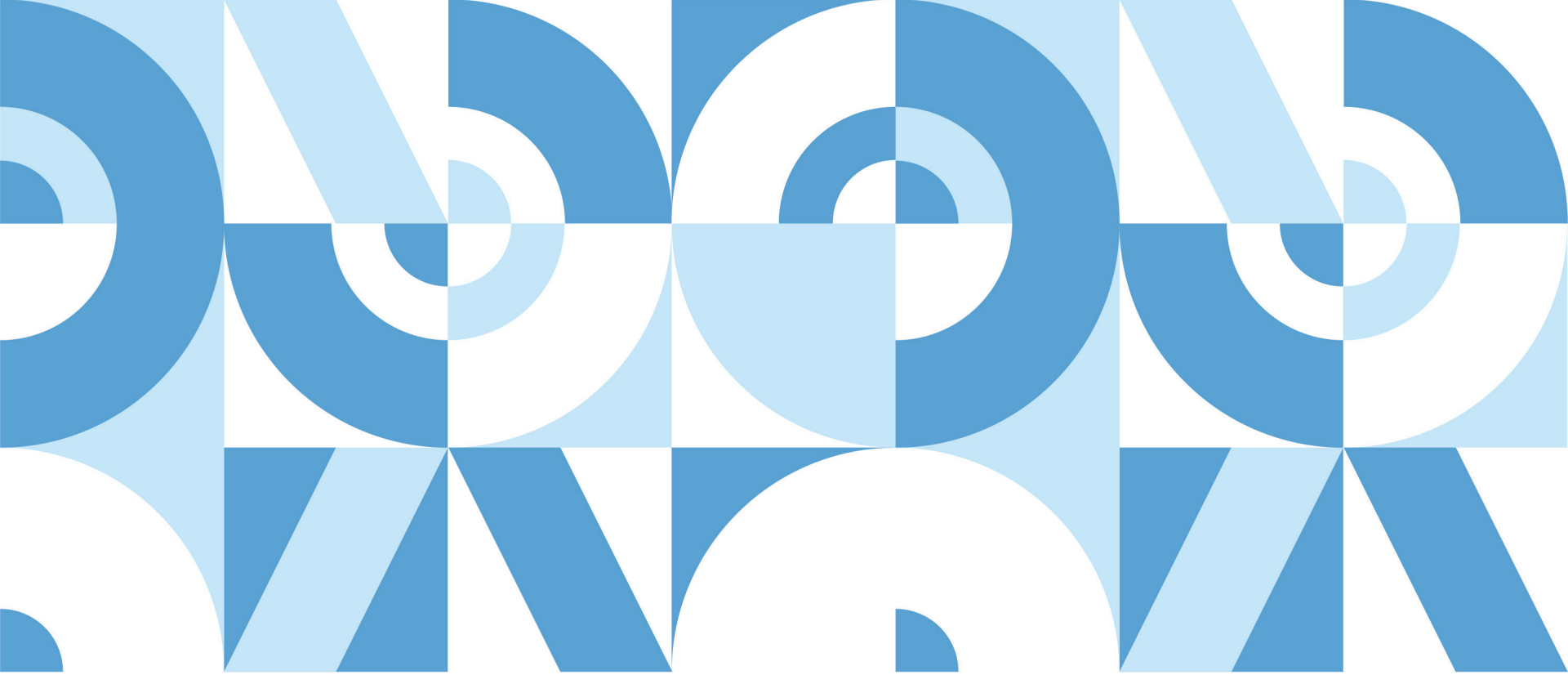
Very truly yours,

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

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[15] Data Privacy Act of 2012, § 11.



DECISIONS

IBC,

Complainant,

-versus-

CID No. 17-K-004
For: Violation of Data Privacy Act of 2012

PBI,

Respondent.

x----------x

DECISION

PATDU, D.P.C.

This Commission is being asked to decide whether a bank may be made liable for claims that certain transactions charged against the credit card it issued was not authorized by the card holder. The card holder in this case is the data subject who requested for the bank to remove the charges in his account relevant to transactions which he claims were unauthorized.

Facts of the Case

From the records of the case, Complainant obtained a credit card from respondent PBI. Under the terms and obligations of obtaining the card, complainant is obliged to pay the purchases to be made and charges to be incurred.

On 09 July 2017, complainant received an email from PBI through email address <customercare@pbi.com.ph>. Said email required him to log-in as a card holder to verify his information on a link provided, under threat of having his card suspended. The email message stated that his credit card would be temporarily suspended until the verification process is complete with a separate reminder not to input any wrong information, otherwise, his account will be suspended.

Complainant, on the belief that it was a legitimate email coming from the respondent bank, felt obliged to comply with the instructions provided in the email.

When complainant tried to use his credit card on 19 July 2017, he was informed that he had already reached his credit limit. Complainant immediately called the Respondent's customer service hotline and was shocked to learn that several transactions were charged against his credit card to which he had no knowledge of.

During his inquiry with the Respondent's customer hotline, complainant learned that there were transactions done on 10 and 11 July 2017, amounting to a total of Php 203, 983. Complainant also received information about additional transactions done on 18 July 2017 amounting to Php 33, 000 pesos. According to the records of the case, all questioned charges were transacted online.

On 20 July 2017, complainant filed a protest on the first series of transactions alleging that it was not authorized. PBI instructed the complainant to fill out and file a "Cardholder's Statement of Disputed Item" (CSDI) form in order to pursue his protest. On the same date, Complainant filed his CSDI form for the first series of transactions and submitted it to the Respondent. On 04 August 2017, complainant filed another CSDI form for the second series of alleged unauthorized transactions as additional disputed items.

Through a letter dated 25 August 2017, respondent PBI sent a response to the complainant stating that after reviewing the complaint filed, the first series of transactions shall remain to be for complainant's account as a cardholder. Respondent stated that the transactions were made online using the cardholder's full credit card details. Furthermore, for security, a One-Time Password (OTP) was sent to the cardholder's registered email address ibc@yahoo.com and that the said transactions were properly authenticated using the OTP sent to the registered address.

Complainant then wrote his letter of protest dated 10 September 2017 to formally require Respondent to make and effect the necessary correction/removal and rectification of his account. However,

complainant did not receive a reply on his letter of protest as well as a response to the second Cardholder's Statement of Disputed Items Form.

Hence, Complainant instituted this complaint before the Commission for violations of the Data Privacy Act.

Allegations of Complainant

Complainant alleges that the Respondent failed to set-up, institute and implement the necessary, appropriate and adequate security measures required under the Data Privacy Act. He further alleges that this enabled unauthorized entities to obtain the personal information of the complainant which was illegally used to make unauthorized and fraudulent transactions charged to his credit card account. In addition, he further alleges that he had suffered sleepless nights, serious anxiety and mental stress which arose from the refusal of the respondent to correct the billing of the unauthorized or fraudulent transactions made on his credit card.

Responsive Comment

Respondent in its responsive Comment admits the following matters:

a. The issuance to the complainant of the above-described credit and the transactions that were charged to it;
b. The two protests of the complainant through the submission of Cardholder's Statement of Dispute Item Forms; and
c. The first protest of the complainant was denied through a letter dated 25 August 2017 while the second protest was received through their Card Fraud Control but was not responded to.

In their defense, Respondent asserts that their Card Fraud Control immediately acted on complainant's protests as evidenced by the denial letter furnished to the complainant.

Respondent maintains that the online transactions are deemed valid because they were properly authenticated through the One-Time Password (OTP) sent to the complainant's email address.

Respondent PBI further maintains that it did not violate the Data Privacy Act (DPA) requiring personal information controllers to take steps to ensure that personal data are legally and properly processed by natural persons under its authority.

They assert that the Complainant, assuming that he was a victim of phishing incident as he claims in his complaint, cannot feign ignorance about such because Respondent regularly sends phishing advisories to its clients' Registered email addresses and mobile numbers, in addition to the posting of said advisories on its website and conduct of periodic awareness campaign.

Respondent maintains that the Complainant was the proximate cause, if not the sole cause of the data breach and not the alleged failure of the respondent to ensure proper and legal processing of complainant's data because he voluntarily disclosed his personal and financial information without verifying the link provided in the email.

Respondent prays that the complaint be dismissed since the Complainant has no cause of action against the respondent under the DPA and its implementing rules and regulations as the data breach was a result of complainant's own acts and not from the failure of respondent to set up, institute and implement the necessary, appropriate and adequate security measures.

Issues

The sole issue to be resolved by this Commission is whether Respondent PBI is liable for unauthorized processing on the alleged illegal transactions charged to the Complainant.

Decision

Rights of Data Subjects

Before the discussion on the issue of unauthorized processing, the Commission deems it necessary to discuss rights accorded to data subjects relevant to this case.

Data subjects under the Data Privacy Act[1] are entitled to rights, including the right to rectification[2] of his or her records, to wit;

> (d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: Provided, That the third parties who have previously received such processed personal information shall he informed of its inaccuracy and its rectification upon reasonable request of the data subject;
>
> € 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; and
>
> (f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

Responsibility rests upon the Personal Information Controller (PIC) in establishing procedures and mechanisms for the exercise of these rights. In this case, the claim of the data subject is that the charges in his credit card are inaccurate or false. The complainant filed 2 protests with the Respondent bank on 20 July 2017 and 04 august 2017, respectively, through the submission of Cardholder's Statement of Disputed Item (CSDI) Form.

We note that while the first protest was addressed, the second protest and the subsequent letter of protest were not. In Respondent's Comment[3], they admitted receiving the CSDI form filed by the

[1] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating For this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 3(c) (2012) [hereinafter, DPA].
[2] DPA, §16(d)
[3] Comment, par. 6-8

Complainant on 20 July 2017 and 04 August 2017. They also admitted to issuing a response denying the request for the first protest on 25 August 2017. While they also admit to receiving the second CSDF abovementioned, and a subsequent letter of protest received on 10 September 2017, there was no mention of any response issued to these requests. Hence, evidence on record shows that the Respondent has not addressed all the concerns of the complainant regarding the rectification of his credit records.

Unauthorized Processing and lawful Basis for processing of personal information

The Complainant anchors his right to have his records rectified and removed from the system of PBI on the claim that the transactions made on his credit card was unauthorized or illegal. Hence, since he did not give his authority to the disputed transactions, PBI should not have processed the same. Since PBI allowed the transaction to push through without his consent, Complainant asserts that the Respondent bank should be made liable for unauthorized processing of his information.

The Commission finds this argument devoid of merit.

For a person or a Personal Information Controller to be held liable for unauthorized processing, the following elements must be present:

1. There must be processing of personal information;
2. That such processing was without the consent of the data subject or that such was not authorized by the Data Privacy Act or any other existing law.

Under the DPA, there are criteria for lawful processing of personal information[4].

The same criteria is applied in this case in determining whether the processing of the alleged unauthorized transaction by the bank was indeed lawful.

[4] DPA, §12

In processing the personal information relevant to the transactions and charges made on the credit card, PBI may find support in section 12(b)[5]:

"**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:

> (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; xxx" (emphasis supplied)

The use of the credit card issued by PBI is governed by the terms and conditions which sets out the obligations of the issuer and recipient of the credit card. As held in the case of *Pantaleon vs American Express International and in BPI Express Card Corporation vs. Armovit*, the relationship between the credit card issuer and the credit card holder is a contractual one that is governed by the terms and conditions found in the card membership agreement.[6] Such terms and conditions constitute the law between the parties.[7]

In the complaint[8] filed by IBC, he admitted that at the time he obtained credit card from PBI, he obliged himself, as the borrower, to pay those purchases and charges which he incurred under the terms and conditions of the contract. This fact is not disputed by the Respondent. Since the same terms and conditions govern the contractual relationship between the parties, the processing of personal information done by PBI pursuant to its contractual obligation is deemed lawful, as provided under the law.

Therefore, the claim of IBC that PBI is liable for unauthorized processing for processing without his consent is misplaced. While IBC claims that he did not authorize the transaction, the basis of processing as

[5] DPA, §12 (b)
[6] Pantaleon vs American Express International, G. R. No. 174269, February 23, 2011.
[7] BPI Express Card Corporation vs Armovit, G. R. No. 163654, October 8, 2014.
[8] Complaint, par 3.

discussed above is not simply the explicit consent of the Complainant, but rather, such processing that is related to the fulfillment of the contract that they entered. Online transactions using credit cards do not proceed in the same way as transactions done offline, where the credit card holder affixes his signature to every transaction. In this situation, the manner by which consent will be given by the data subject for the transaction is governed by the agreement between the parties, as provided in the card membership agreement. Part of this are provisions for the use of a One Time Pin (OTP) as further verification.

The question now left for this Commission to decide is whether the Respondent bank should be held liable for processing the credit card transactions charged to Complainant IBC upon the latter's allegations that the same are without his authority and that he was a victim of phishing. Complainant claims that the security measures placed by PBI were insufficient and this resulted to the phishing of his personal information which eventually led to the unauthorized purchases.

Phishing and Access due to negligence

Phishing is defined as the fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication9[9]. The responsibility for the avoidance of falling victim to phishing falls both on the Personal Information Controller and the data subject.

The PIC must be able to implement appropriate security measures[10] provided under the DPA to capture cases of phishing and be able to prevent it from happening for the protection of its data subjects.

In the case at bar, Complainant IBC argues that due to PBI's negligence in not employing security measures, his personal information was illegally obtained through phishing.

This claim has not been sufficiently proven.

[9] ISO/IEC 27032:2012 (en), §4 Terms and definitions
[10] DPA, §20.

While it is true that IBC was able to establish that he fell victim to phishing by presenting a copy of the email pretending to be a legitimate email message from PBI, he was not able to prove that falling for the same email was due to the negligence of the latter. Complainant's claim that PBI did not employ security measures was not supported by any evidence aside from his bare allegations.

On the other hand, PBI presented before this Commission substantial evidence that it has employed security measures to protect its data subjects, including Complainant IBC, from falling for phishing emails.

In the submissions made by the Respondent bank, records show how it regularly sends advisories to its clients' registered email addresses and mobile numbers. They also posted advisories on their website to constantly remind their clients to ignore phishing emails and messages. These advisories were sent to its clients as early as 2014. Furthermore, respondent has shown that it was not remiss in its duties in adopting dynamic consumer awareness program against phishing by utilizing all the available channels to reach their clients[11], through advisories in its website, television commercials and email reminders. As to the sending of email advisories, Respondent also presented proof that the complainant's email address is included as recipient of their advisories on warnings against phishing[12].

The Commission notes that the regular campaigns of the respondent against phishing do not only raise awareness of their customers, but it also provides its clients with precautionary steps to be taken if and when they receive suspicious emails luring them to give their personal information, particularly financial information[13].

Furthermore, in support of Respondent's defense, it submitted evidence that they have enabled multi-factor authentication for their online payments through the implementation of One-Time Password (OTP) to ensure that any access or purchase would need a confirmation from the account owner through an email message before they process the purchase. In fact, in their letter dated 26 August 2017 in

[11] Comment, Annex "5"
[12] Id. P. 67
[13] Ibid

response to the Complainant's first protest, they stated that their Card Fraud Department determined that the transactions were deemed valid since the same were properly authenticated through OTP sent to the complainant's email address. To substantiate this, they presented screenshots from their system that the OTP was successfully sent to the card holder's email address, that their OTP logs showed that the OTP was successfully entered, and that the email address was the same one that the complainant submitted to the bank. The alleged unauthorized purchases were authenticated using the OTP sent to IBC's email. Following authentication, PBI authorized the processing of the purchases[14] and charged the same against the Complainant.

In summary, PBI's continuous awareness campaign and its verification process, through the use of OTP, provides substantial evidence that it was not negligent in employing security measures. The claim of IBC that it was the negligence of PBI that caused the phishing of his personal information is not meritorious.

Anent the issue on the determination of fraud in credit card transactions, the same falls within the ambit of the Central Bank. It has not been sufficiently established before this Commission that the said transactions are indeed illegal or unauthorized.

WHEREFORE, premises considered, the Commission resolves that this case be **DISMISSED** for failure to substantiate and prove the allegations in the Complaint, without prejudice to any action that may be filed to other appropriate agencies or institutions. The Commission, however, **ORDERS** PBI to act on the request for correction which has not yet been addressed, and to provide assistance to complainant to ensure that he is able to exercise his rights as data subject in accordance with law.

SO ORDERED.

(Sgd.)
IVY D. PATDU
Deputy Privacy Commissioner

[14] Records, p. 10

WE CONCUR:

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

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

Copy furnished:

CBI
Complainant

PBI
Respondent

PBI CARDS
Respondent

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
NATIONAL PRIVACY COMMISSION

JV,

Complainant,

-versus-

NPC Case No. 17-047
For: Violation of the provisions of the Data Privacy Act

JR as the Customer Service Manager of **SM STORE** at SM Bicutan,

Respondent.

x----------x

DECISION

AGUIRRE, D.P.C.

For consideration before this Commission is a complaint filed by JV against JR, in her capacity as the Customer Service Manager of the SM Store, for an indeterminate violation of the Data Privacy Act (DPA).[1]

These Proceedings

On 15 March 2018, this Commission, through the Complaints and Investigation Division, conducted a Discovery Conference. At the Conference, this Commission directed the respondent and other representatives of SM Bicutan to submit a responsive pleading within ten (10) days from receipt of the Order dated 16 March 2018.[2]

On 26 March 2018, the respondent filed her Comment containing a narration of incidents and arguments refuting the complainant's allegations.[3]

On 13 April 2018, the complainant filed his Letter-Reply.

[1] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [DATA PRIVACY ACT]
[2] Records, p. 18; NPC Circular No. 16-04, Rule III, Section 15.
[3] Id., at pp. 22-34.

Facts

From these filings, we ascertain these facts.

The complainant filed and paid for a copy of his birth certificate from the Philippine Statistics Authority (PSA) through the Customer Service Center of the SM Store at SM Bicutan.

Upon payment, the cashier collected the complainant's name, address, and phone number. Joselito claims he does not know why this information is necessary, and that no one let him know who can process that information further. [4]

When the complainant returned for his birth certificate, he noted the SM personnel pull his birth certificate from a folder on her desk. He also noted that his birth certificate was kept together with the birth certificates of other people and that another person's Certificate of No Marriage was lying on another table, accessible to any of the other personnel of SM Store.

The SM personnel, JH, then handed the complainant his birth certificate uncovered and in plain sight. Janice was the only person at the counter.

The complainant then asked for an envelope for his birth certificate. Janice told Joselito that no envelopes were to be given, as the PSA did not provide envelopes for the purpose.

When the complainant brought this to the respondent's attention, the respondent informed the complainant that all customer service counters in all SM Stores throughout the country do not provide individual envelopes for their clients' birth certificates.

Nevertheless, the respondent placed the complainant's birth certificate in an envelope and handed over the birth certificate to the complainant. At this point, the complainant was taking photos and videos of JH and the respondent, over their objections.

[4] Id., at p. 3.

Arguments of the Parties

The complainant now comes to us claiming there is a violation of his privacy rights. He claims that his data was not treated with the confidentiality it deserves. He finds it unfair that the persons handling the PSA-issued documents, who are also under the supervision of the respondent, may not be authorized to handle them.[5]

The complainant also feels that any complaint filed with SM Store will not be treated fairly; he acknowledges that he has filed a prior complaint against the same respondent for being arrogant and unprofessional in a previous transaction.[6]

The respondent claims that as a mere conduit of the PSA, she had no obligation to place the birth certificate in an envelope when the PSA provided no such envelope for the purpose; the PSA hands over all documents to be released in just one envelope for every request made in one certain day.

The respondent argues that there is no violation of informational privacy rights or any other violation of the Data Privacy Act.[7] She notes that the Data Privacy Act and its Implementing Rules and Regulations do not define what a "privacy violation" is. Therefore, the respondent concludes, the actions must be measured against the test of what may constitute a reasonable expectation of privacy.

The respondent points to jurisprudence laying down a two-part test: (1) whether by conduct, an individual has exhibited an expectation of privacy; and (2) whether this expectation is one that society recognizes as reasonable.[8] She then contends that as authorized representatives of the PSA, the complainant should have reasonably expected that JH and the respondent can process and facilitate the release of the copy of JV's birth certificate.[9] She argues, further, that this reasonable expectation extends to SM Store and its authorized personnel.[10]

[5] Id., at p. 1.
[6] Ibid.
[7] Id., at p. 30.
[8] Id., at p. 29.
[9] Ibid.
[10] Ibid.

The respondent maintains that there was no data breach, and as such, no criminal liability for unauthorized disclosure under Section 32 of the Data Privacy Act, because only authorized employees of SM Store were at the counter, at all material times in this complaint; Janice released the complainant's birth certificate to the complainant only.[11]

For the respondent, Philippine data privacy laws do not require that every document containing personal data be separated individually from other documents. Neither do these laws prohibit putting different documents in just one envelope. She believes that all that the DPA requires is "appropriate and reasonable" security measures to ensure the confidentiality, integrity and availability of personal data.

The respondent insists that the complainant's birth certificate was never compromised, as SM Bicutan established and implemented appropriate and reasonable security measures, especially following the issuance of PSA Office Memorandum 2017-09, which specified the authorized persons who can be issued the certificates. She points to SM Store policies on the release of requested certificates to its customers:

1. Only authorized personnel, such as Customer Service Assistants, are allowed inside the counters of customer service areas, including those where the customers can request for and receive birth certificates;
2. During the release of certificates, the authorized employee shall search only the requested certificate in the envelope corresponding to the date of request.
3. The requested certificates shall only be released to the owners, or their duly authorized representatives, as enumerated in the guidelines of PSA.
4. If the one claiming the certificate is not the owner, the representative shall be required to submit an authorization letter from the owner, a copy of a valid identification (ID) card of the owner and a valid ID of the representative.
5. The authorized personnel must always maintain all the certificates inside the labeled envelopes.

The respondent claims that the design, including the physical

[11] Id., at p. 30.

arrangement of furniture and equipment, of the counters in the customer service counters in SM Bicutan provides privacy to the personnel handling the personal data.

The respondent also claims that the Non-Disclosure Agreement (NDA) that she and JH were made to sign obliged them to hold personal data under strict confidentiality during and even after their employment.[12] Their NDAs, as presented to this Commission, require them to comply with the provisions of the Data Privacy Act,[13] and prohibit the retention of any copies of any documents that may come into their possession that contain confidential and personal information.

In rebuttal, the complainant argues that as an authorized partner of the government in providing services, it is not just a mere conduit; SM Store is bound to follow the rules of PSA and the Data Privacy Act as a personal information controller.

He maintains that the locations of the folders and envelopes are material: having been placed in a location accessible by all personnel in the customer area, JR had ready access to his birth certificate. The complainant stresses that since respondent was someone whom he had complained about for unprofessional behavior and for discourtesy, he was bothered by the respondent's access to his birth certificate.

The complainant claims that any photo and video taken was for evidentiary purposes;[14] the public nature of the incident removes any reasonable expectation of privacy for Janice and the respondent.

Finally, the complainant points toward a peculiarity in Janice and the respondent's Non-Disclosure Agreements, having been executed only 6 October 2017, two days prior to the incident. The complainant notes that these documents did not exist at the time he filed and paid for his birth certificate.

Issues

The issues to be resolved in this case are:

[12] Id., pp. 48 - 49, 59 – 60.
[13] Ibid.
[14] Id., at p. 102.

1. Whether the Respondent committed any violation of the Data Privacy Act; and
2. Whether the security measures implemented by SM Bicutan are considered reasonable and appropriate.

Discussion

On the procedural aspect of the case, NPC Circular 16-04 provides for the form and content of Complaints, thus:

> 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. The complaint must include any and all reliefs sought by the complainant.[15]

From the narration of events, this Complaint stems from the admitted fact that the birth and other certificates being released at the customer service counter in SM Bicutan were not sealed or covered individually. On the basis of this, complainant alleges that his privacy was violated without specifying either the provisions of the Data Privacy Act that were violated or the acts constituting a violation of those provisions despite what NPC Circular 16-04 requires.

Notwithstanding this deficiency in form, however, the Commission resolves to give due course to the Complaint to clarify important legal concepts on privacy.

Considering that the complainant cites no specific violation of the Data Privacy Act, we must determine whether the processing was done in accordance with some lawful criteria as provided in the law.

The complainant gave his consent for the processing of his birth certificate.

It is undisputed that the birth certificate of the complainant contains personal information and sensitive personal information as defined under the Data Privacy Act.

[15] NPC Circular 16-04, Section 10.

One of the criteria provided under Sections 12 and 13 of the Act for the lawful processing of both personal and sensitive personal information is consent of the data subject. This consent must be specific to the purpose declared prior to the processing.

A person requesting his birth certificate from the PSA is asked to fill out an application form for the issuance of his birth certificate.

In the application form, the requester signifies his consent for the processing of his birth certificate for the purpose of releasing it to him.

The requester also has the option to avail the services of PSA through their accredited partners, in this case, SM Store.[16]

Here, the complainant chose to apply for his birth certificate in SM Store, an accredited partner of the PSA.[17] In doing so, the complainant is considered to have given his consent to SM Store to process his request to get a birth certificate from PSA. He was aware that the processing shall be for purposes of issuing and releasing his birth certificate to him or to his duly authorized representative. Thus, SM Store, as an accredited partner of PSA, processed Complainant's birth certificate according to one of the lawful criteria set out in the Data Privacy Act.

Respondent did not commit any violation of the Data Privacy Act to warrant a recommendation for prosecution.

The respondent argues that since complainant only claimed in general that there was a privacy violation and neither the Data Privacy Act nor its IRR defines what a privacy violation is, the circumstances of the case must be measured against what reasonable expectations of privacy exist. Using the reasonable expectation of privacy test as a measure, she claims that she did not commit any violation of the Data Privacy Act.

The two-part test she cited to determine whether an individual's reasonable expectation of privacy was violated, however, must now be considered within the context of existing laws, specifically the Data Privacy Act.

[16] Application Form – Birth Certificate, https://www.psaserbilis.com.ph/Secure/Files/Birth%20Application%20Form.pdf (last accessed on 08 August 2019)
[17] Ibid.

Quoting the concurring opinion of Justice Harlan in the United States Supreme Court case of *Katz v. US*,[18] the Philippine Supreme Court incorporated the reasonable expectation of privacy test in *Ople v. Torres*,[19] thus:

> The reasonableness of a person's expectation of privacy depends on a two-part test: (1) whether by his conduct, the individual has exhibited an expectation of privacy; and (2) whether this expectation is one that society recognizes as reasonable.[20]

Expounding on the *Katz* test, *Ople* further explained:

> The factual circumstances of the case determines the reasonableness of the expectation. However, other factors, such as customs, physical surroundings and practices of a particular activity, may serve to create or diminish this expectation.[21]

In *Ople v. Torres*,[22] the Supreme Court expressly recognized the right to privacy as a fundamental right guaranteed by the Constitution, identifying in the process several constitutional provisions that protect different facets of such right. Apart from this, the Court explicitly recognized that different zones of privacy are protected under different laws, thus:

> Zones of privacy are likewise recognized and protected in our laws. The Civil Code provides that '[e]very person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons' and punishes as actionable torts several acts by a person of meddling and prying into the privacy of another. It also holds a public officer or employee or any private individual liable for damages for any violation of the rights and liberties of another person, and recognizes the privacy of letters and other private communications. The Revised Penal Code makes a crime the violation of secrets by an officer, the revelation of trade and industrial secrets, and trespass to dwelling. Invasion of privacy is an offense in special laws like the Anti-Wiretapping Law, the Secrecy of Bank Deposits Act and the Intellectual Property Code. The Rules of Court on privileged communication likewise recognize the privacy of certain information.[23]

It is in this context that the Data Privacy Act of 2012 was enacted–

[18] Katz v. United States, 389 U.S. 347 (1967).
[19] G.R. No. 127685, 292 SCRA 141, 23 July 1998.
[20] Ibid.
[21] Ibid.
[22] G.R. No. 127685, 292 SCRA 141, 23 July 1998.
[23] Ibid.

"to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth."[24]

Considering that *Ople* itself recognized the idea of statutory zones of privacy, it follows that with respect to the zone of privacy specifically covered and protected by the Data Privacy Act, the strand of privacy knowns as informational privacy,[25] the determination of the metes and bounds of the right to privacy should necessarily be grounded in the Act itself. Given the specific standards the Data Privacy Act provides with regard to the obligations it imposes on those who process personal data and the rights it gives to data subjects, it follows that reference should first be made to these clear and objective standards[26] before going into an abstract and general examination that is the "reasonable expectation of privacy" test in Katz – a test that was traditionally applied for locational or situational privacy cases to determine when a search can be considered as an intrusion into the right to privacy of individuals.[27]

The Data Privacy Act now grants certain, specific rights to individuals whose personal information and sensitive personal information (collectively, "personal data") is processed. As an overview, these include their right to be informed about the nature and scope of its processing; to access the personal data collected from them; to correct any inaccuracy in the personal data used by other entities; to remove their personal data from another entity's system; and to be indemnified of any damages sustained due to such inaccurate, incomplete, outdated, or unauthorized use of their personal data.[28]

The personal data of individuals can no longer be collected and used by any person or organization without finding basis in the different lawful criteria provided for in the Act. Aside from consent, the processing of personal information is now only permitted if it is

[24] Data Privacy Act, § 2.
[25] See, the discussion on the three strands of privacy in Vivares v. St. Theresa's College, G.R. No. 202666, 29 September 2014, citing Chief Justice Reynato Puno's speech, The Common Right to Privacy.
[26] Canon of statutory construction that a specific law prevails over a general law. See, Lopez v. Civil Service Commission, G.R. No. 87119, 16 April 1991, citing Butuan Sawmill, Inc. v. City of Butuan, No. L-21516, April 29, 1966, 16 SCRA 755.
[27] See generally, Articulating the Complete Philippine Right to Privacy in Constitutional and Civil Law, 82(4) PHIL. L.J. 78 (2008), cited in Pollo v. David, G.R. No. 181881, Oct. 18, 2011 (Bersamin, J., separate opinion).
[28] Data Privacy Act, §16

necessary for the fulfillment of a legal obligation; to protect the life and health of the data subject; to respond to a national emergency, public order and safety; or for a public authority to fulfill its mandate. The Act also considers legitimate interests pursued by an entity, subject to certain provided exceptions. Furthermore, the Act provides a special category of personal information[29] that is prohibited from being processed, except on certain grounds. Subject to qualifications provided for in the law itself, these include: consent of the data subject, existing laws and regulation, the protection of life and health, the achievement of lawful and non-commercial objectives of public organizations, treatment by a medical practitioner or a medical treatment institution, and the protection of lawful interests in court or the defense of legal claims.

These rights and parameters correlate to obligations on the part of other persons and entities who process personal data. These persons and entities must be able to justify their processing of personal data under any of the lawful criteria mentioned. They now have an obligation to provide mechanisms for the access, correction, and removal of personal data upon request, as well as the filing of a complaint. They are further required by the Act to secure the processing of any personal data by documenting and implementing organizational, technical, and physical measures to respect the abovementioned rights.[30] At the core of these obligations are the general data privacy principles[31] of transparency, legitimate purpose, and proportionality. Following this, any person or entity that processes information should collect information only for legitimate purposes that have been made known to the data subject. They should only collect as much information as is needed to achieve business interests or to comply with the law.

All of these constitute objective standards provided by the Data Privacy Act with respect to informational privacy.

In fact, even applying the reasonable expectation of privacy test within the context of informational privacy, the result still points to the Data Privacy Act.

[29] Id., at § 4(l).
[30] Id., at § 20.
[31] Id., at § 11.

The first part asks "whether by his conduct, the individual has exhibited an expectation of privacy."[32] This expectation of privacy has to be examined taking into consideration what the Act itself provides. An individual's expectation of privacy does not depend on a particular action on their part before they are granted the rights provided under the law; these rights are not waived, and the obligations of controllers and processors cannot be ignored simply because there is no overt exhibition of this expectation of privacy. As to the second part, which asks "whether this expectation is one that society recognizes as reasonable,"[33] this determination should be considered as having been made when Congress and the President, as representatives of the people, codified what data subjects should expect with regard to their privacy.

Given these, insofar as informational privacy cases are concerned, the application of the reasonable expectation of privacy test under *Katz* and *Ople* should necessarily result in a determination in accordance with the provisions of the Data Privacy Act. An individual's expectation of privacy should therefore be determined taking into consideration the rights the Act gives to data subjects[34] and the obligations it imposes on those who process personal information by, among others, ensuring they follow not only the general data privacy principles[35] but also that they have lawful basis for that specific processing activity.[36]

This is not to say, however, that the concept of reasonable expectation of privacy no longer applies. While the two-part test under *Katz* and *Ople* should now be construed taking into consideration

the provisions of the Data Privacy Act, this concept of "reasonable expectation" may still be useful in addressing issues concerning informational privacy in relation to what controllers and processors may legitimately do.

In this regard, this concept of "reasonable expectation" is considered to determine the legitimacy of the additional processing

[32] Ople v. Torres, G.R. No. 127685, 292 SCRA 141, 23 July 1998.
[33] Ibid.
[34] Data Privacy Act, § 16.
[35] Id., at § 11.
[36] Id., at §§ 12 and 13.

by examining whether such further processing is compatible with the original business purpose communicated to the data subject and not beyond what the data subject may reasonably expect as to the purpose, scope, manner, and extent of the processing of their personal data.[37]

On the proper usage of publicly available data, for example, this Commission has stated that "the reasonable expectation of the data subject on the purpose for processing of his or her personal information at the time of its collection becomes a crucial consideration... In the absence of a pre-existing relationship, the PIC must demonstrate that the processing can be reasonably expected, particularly if the personal information was collected and obtained from a third party."[38]

In this case, while it is correct to say that the complainant cannot expect that only the PSA will handle his request for his birth certificate, it is incorrect to say that "there is no longer a reasonable expectation that the privacy of his birth certificate extends only to the PSA"[39] and therefore there is no privacy violation under the DPA. Following the discussion above on the application of the reasonable expectation of privacy test to informational privacy cases, determining whether the privacy rights of the complainant were violated or not should be rooted in the provisions of the Data Privacy Act.

From the facts of this case, the complainant clearly consented to the Customer Service Center of the SM Store at SM Bicutan processing his request for a birth certificate as an accredited partner of PSA when he filed and paid for his request through them. Consent under Sections 12 (a) and 13 (a) of the Data Privacy Act served as the lawful basis for the respondent as well as the authorized personnel of SM Bicutan and PSA to process complainant's request.

Having established that there was lawful basis for respondent to process complainant's personal and sensitive personal information, do the circumstances alleged by complainant rise to the level of a violation of the Data Privacy Act to warrant a recommendation for criminal prosecution? We answer in the negative. As will be shown

[37] See, EU General Data Protection Regulation, Recital 47.
[38] NPC Advisory Opinion 2018-050.
[39] Records, p. 29.

hereunder, this does not mean, however, that there was no lapse on the part of respondent or SM Bicutan.

SM Bicutan, as an accredited partner of PSA, has put in place security measures. However, these measures should be strictly implemented.

While the Commission takes note of the security measures set out in the respondent's Comment, it follows that these measures should be strictly implemented by the Company and its personnel and that measures should be taken to ensure this. Also, while not rising to the level of a crime under the DPA, it cannot be said that SM Store's security measures already satisfy the "reasonable and appropriate" standard given the circumstances.

The fact that additional measures are being implemented, as admitted in the counter-affidavit of Janice Herames,[40] is itself a recognition of a deficiency that could have been previously identified and addressed by SM Store. This also shows that the complainant's concern relating to certificates being placed in common envelopes is not entirely unwarranted.

This is all the more true given the pictures taken by the complainant showing a pile of certificates on the counter.[41] This not only goes against the policies of SM Bicutan outlined in the respondent's Comment but, more importantly, potentially endangers the data subjects whose certificates were left where they may be seen by persons transacting near the counter.

The allegations of the complainant do not meet the quantum of evidence required for administrative cases.

The complainant filed this case out of his apprehension that the persons handling his request for birth certificate might misuse the personal data contained in said certificate. He feels threatened because he previously complained to the management of SM Bicutan the person supervising the release his birth certificate.

[40] Id., at p. 55
[41] Id., at p. 5.

In *Morales vs. Ombudsman, et al.,*[42] the Supreme Court held:

> The basic rule is that mere allegation is not evidence and is not equivalent to proof. Charges based on mere suspicion and speculation likewise cannot be given credence. When the Complainant relies on mere conjectures and suppositions, and fails to substantiate his allegations, the complaint must be dismissed for lack of merit.[43]

The complaint shall only be recommended for prosecution if it is supported with relevant evidence which a reasonable mind might accept as adequate to justify a conclusion.[44] The allegations in the complaint must be based on substantial evidence that there is a clear and real violation of the law.

The complainant's allegations are grounded on his fear that the respondent may prejudice his personal data considering her position in SM Store. As the Customer Service Manager of SM Store in SM Bicutan, the respondent exercises supervision over the operations of SM Store in its capacity as an accredited partner of PSA. However, there is nothing in the allegations that the respondent took advantage of her position to the prejudice of the complainant's personal data.

SM Store or PSA's act of not putting each requested certificate in a separate envelope or cover does not prove that a violation of the Act has been committed. The complainant's previous altercation against the persons handling his document also does not add weight to the alleged violation of the Act. The complaint failed to show that the acts of the Respondent amounted to a violation of the DPA.

The prosecution of violations committed under the DPA should not be based on mere suspicion or speculation of the Complainant

that harm may be done to his personal data. Without any evidence or proof to support his allegations, the Complaint should be dismissed for lack of merit.

In PSA's Application Form for Birth Certificate, PSA has accredited

[42] 798 SCRA 609. 17 July 2016.
[43] Id., at p. 627.
[44] Rules of Court, Rule 133, §5

partners extending their services such as delivery of the requested documents through their authorized couriers. It is the option of PSA clients, such as the herein complainant, to secure certifications and copies of civil registry documents from any of PSA's accredited partners.[45]

SM Store is a partner of PSA in accepting and releasing the requested certificates. PSA, a personal information controller, outsources the services of SM Store in SM Bicutan and other SM locations to process the personal data of the requesting data subjects.[46] The processing covers the filing of requests and releasing of the certificates, containing personal data, of the data subjects. SM Store is considered as a personal information processor.

As a personal information processor, SM Store insists that it has adopted reasonable and appropriate security measures including:

1. Company policies with respect to the release of the NSO Birth Certificate;
2. Disciplinary actions to be imposed on the employees who commit a violation of the company policies affecting its obligation as an authorized agent of the PSA;
3. Design of the counters of the customer service areas where the request and release of certificates are made; and
4. Execution of NDAs of the employees handling personal data of the customers.[47]

The mere existence of security measures is not by itself enough to protect the personal data of the subjects.

In this case, the complainant observed that the requested certificates, contained in one folder, were just placed on top of the table at the counter. While only authorized personnel are allowed at the customer service counter, any person transacting at the counter may view some of the details of the certificate appearing first on the folder.[48] Given this, this incident may result in the accidental disclosure of the personal data of any requester whose certificate may appear first on the folder.

[45] Supra note 16.
[46] Data Privacy Act, § 3(i).
[47] Records, pages 22-33.
[48] Id. Pages 3 and 5.

While SM Store already has existing reasonable and appropriate measures, this Commission finds that said establishment is not strictly implementing these measures.

It is also worth noting that the NDAs of Respondent and Herames were only executed two days before the incident.[49] SM Store should require their employees to execute that document or some similar agreement at the beginning of their employment, or at least before they are assigned to handle documents containing personal data of their customers.

Section 26(d) of the Implementing Rules and Regulations of the Data Privacy Act provides:

> d. Management of Human Resources. Any natural or juridical person or other entity involved in the processing of personal data shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data.
>
> The said employees, agents, or representatives shall operate and hold personal data under strict confidentiality if the personal data are not intended for public disclosure. This obligation shall continue even after leaving the public service, transferring to another position, or upon terminating their employment or contractual relations. There shall be capacity building, orientation or training programs for such employees, agents or representatives, regarding privacy or security policies.

SM Store is duty-bound to strengthen the implementation of their privacy and security measures by ensuring that their employees, agents or representatives assigned in the customer service counter of SM Store are contractually-bound to protect the privacy right of their customers.

The management should make their personnel aware of the nature of the data they are handling before they are assigned at the customer service counter. These personnel should also be oriented on the existing measures adopted and implemented by SM Bicutan.

SM Store, as an accredited partner of PSA, should always be mindful that the Data Privacy Act specifically provides that any doubt in the interpretation of any provision of the law shall be liberally

[49] Id. Pages 48-49, 59-60.

interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.[50] As such, SM Store should strictly implement its existing security measures to prevent these incidents in the future.

WHEREFORE, premises considered, the Commission **FINDS** no violation of the Data Privacy Act on the part of Respondent JR as the Customer Service Manager of **SM STORE** at SM Bicutan to warrant a recommendation for prosecution.

This Commission **FINDS**, further, that considering that while **SM STORE** is not a party to this case, there is substantial evidence on record to support a finding that SM Store did not adequately implement their privacy policies with respect to the protection of personal data.

Let the records of this case be forwarded to the Compliance and Monitoring Division for the conduct of a compliance check pursuant to NPC Circular No. 18-02.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against the Respondent before any other forum or tribunal, if any.

SO ORDERED.

Pasay City, 13 August 2019.

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

Concurring:

(Sgd.)
IVY D. PATDU
Deputy Privacy Commissioner

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

[50] Data Privacy Act, § 38.

COPY FURNISHED

JV
Complainant
Parañaque City

JR
Customer Service Manager
SM Store
Shoe Mart Bicutan
Parañaque City

COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

In Re: DATA BREACH INVOLVING THE COMELEC DATA PROCESSING SYSTEM IN WAO, LANAO DEL SUR

NPC CID Case No.: 17-002
For: Violation of the Data Privacy Act f 2012

x----------x

DECISION

PATDU, D.P.C.

Before this Commission is a reported Personal Data Breach involving the Commission on Elections ("**COMELEC**") data processing system in Wao, Lanao del Sur ("**Wao**"), docketed as NPC Case No. 17-002.

COMELEC reported that on 11 January 2017, a desktop computer of the Office of the Election Officer ("**OEO**") of Wao, was stolen by unidentified persons. The desktop computer contained, among other applications, the Voter Registration System ("**VRS**") and the Voter Search ("**VS**") program that utilize the data stored in the National List of Registered Voters ("**NLRV**").

COMELEC notified this Commission about the possible personal data breach through electronic mail on 28 January 2017. The notice to this Commission, included the following statement:

> *"At the outset, the undersigned respectfully informs the NPC that, as a security feature, all data encoded in the computers of all OEOs are already encrypted in AES 256, and that the portable hard disk containing said data are likewise encrypted. Upon completion of the on-going investigation being conducted to determine the scope, including the measures undertaken and still to be undertaken to address and reduce the consequences of such breach, if any, the COMELEC shall be providing the NPC with a detailed report on the matter once all data relative thereto shall have become available. For the meantime, the COMELEC respectfully requests an extension of time to comply with such notifications.*

The initial notification was followed by another report dated 03 February 2017. From the submissions, this Commission found out that the VRS contained a total of 58,364 registration records for the Municipality of Wao. 40,991 of said records (as of 19 October 2016) are intended for the Barangay elections, and 17,373 (as of 13 September 2016) are for the Sangguniang Kabataan ("**SK**") elections. 35, 491 of the Barangay elections data are active voters, while 5,500 are deactivated voters. 17,336 of the SK elections data are active voters, while 37 are deactivated voters.

The NLRV, on the other hand, contains approximately 75,898,336 records as of 17 October 2016. 55,195,674 of which are active voters and 20,703,662 are deactivated voters.

COMELEC also reported on actions they have taken, and other measures for implementation following the incident.[1] For instance,

COMELEC reports that the security feature, encryption in AES 256, of the fields containing personal information has already been implemented since 17 October 2016.

[1] According to COMELEC, part of the measures that have been implemented and/or still for implementation are the following:

Measures already taken:

1. Memorandum dated 23 January 2017 called for installation of CCTV cameras in all field offices, including the hiring of a consultant for the Data Privacy Act compliance.
2. Memorandum dated 01 February 2017 prescribed the interim security measures and controls that will secure and prevent loss, destruction, unauthorized access and misuse of data pending issuance of the key policies related to data security, use, processing, storage and disposal.
3. Conduct of training-seminar on the Data Privacy Act.

Measures to be undertaken:

1. Use of biometrics by the accountable officers to gain access to the VRS and NLRV. The COMELEC Information Technology Department ("ITD") has been directed to develop an application on the matter.
2. Limit the number of personal data in the NLRV deployed in the local field offices and overseas posts. Also under development is the patch that will delete and wipe-out the NLRV storage devices in the offices of the election officer.
3. Drafting of the rules and guidelines on limiting the use of the VS and NLRV in the local field offices to eighty-one (81) Provincial Election Supervisors only, instead of one thousand, six hundred fifty-six (1,656) election officers.
4. Streamline registration forms to cover only personal data required by law (R.A. No. 8189).
5. Execution of Non-Disclosure Agreements ("NDA") with the Job Orders/Contract of Services personnel authorized by the Commission En Banc to be hired. Said NDA shall likewise apply to regular employees of departments and offices that have personal data in their custody.
6. Execution of Data Sharing Agreements with Law Enforcement Agencies.
7. Submission to the Commission En Banc, for its approval, of a Notice to be incorporated in documents containing data requested by data sharing agencies.
8. Drafting of the key policies on the compliance requirements of the Data Privacy Act, for approval by the Commission En Banc.
9. Nationwide training of all the field officials on Data Privacy Act compliance, including the integration of such compliance requirements during the orientation of newly hired employees.
10. Finalization of the Privacy Impact Assessment, for submission to the Commission on or before 27 February 2017.

Considering the seriousness of the possible data breach, involving personal data of millions of Filipinos, and the delay in notification, this Commission conducted further investigations on the circumstances surrounding the personal data breach.[2]

Specifically, an Order for On-Site Examination of Systems and Procedures, dated 07 February 2017, was issued to assess risks to data subjects in a selected field office of COMELEC. The observation and inspection of the personal data processing procedures were carried out at the COMELEC facilities in Taguig City on 08 February 2017.

This Commission, through its investigating officer, also completed a preliminary investigation, where a recommendation for criminal prosecution was made against Casan Tangorac Laguindab (Laguindab), Election Officer of Wao, Lanao del Sur. On 9 February 2018, this Commission directed Laguindab to submit his Responsive Comment on the Preliminary Fact-Finding Report charging possible *Concealment of Security Breaches Involving Sensitive Personal Information,* and *Accessing Personal Information and Sensitive Personal Information Due to Negligence*.

On 13 February 2017, proceeding from the records of the Case, including the onsite examination, this Commission issued a Compliance Order mandating the COMELEC to:

1. Erase all National List of Registered Voters in the computer system in the different municipalities and cities, if it cannot be secured using appropriate organizational, physical and technical security measures;
2. Notify data subjects affected by the personal data breach as soon as possible, but not to exceed two weeks;
    a. Notification by publication in two newspapers of general circulation will be allowed for individuals with records in the National List of Registered Voters (NLRV);

[2] Rule IX, Sec. 38(c) of the IRR of the DPA

b. Individual notification for the individuals with records in the Voters Registration System (VRS) in the Municipality of Wao, Lanao del Sur, in accordance with NPC Circular 16-03 on Personal Data Breach Management;

3. Submit to the National Privacy Commission proposed and implemented revisions in the voter registration process, taking into account the Data Privacy Act, its Implementing Rules and Regulations, and related Issuances of the Commission in two weeks;
4. Include in the submission the status of implementation of part III "Measures Taken to Address the Breach" of the Report on this personal data breach dated February 3, 2017 submitted by the Commission on Elections;
5. Submit a Compliance Report within 15 days from receipt of this Order.

In compliance to the above Order of this Commission, COMELEC submitted its Compliance Report on 28 February 2017.[3] COMELEC reported that the COMELEC en Banc approved the modifications in both local and overseas Voter Registration Systems with the issuance of Minute Resolution No. 17-0092, dated 14 February 2017, entitled "In the Matter of the Proposed Changes on the Voter Registration System (VRS) and Voter Search Systems and Database-Updated".

[3] In response to the order to submit proposed and implemented revisions in the voter registration process in view of the DPA, COMELEC submitted a draft of the Policy on Field Office Systems outlining the policy on data privacy, security and protection; and a draft of the Resolution to align changes in the VRS and the VS with the General Instruction on the conduct of the system of continuing registration of voters.

COMELEC also reported the following: approval on the budget for the installation of CCTV cameras; delay in hiring a consultant due to low budget allocation; dissemination of Memorandum on interim security measures and controls on data processing; addition of a 1-day seminar on data privacy in their Strategic Planning Seminar attended by directors and division chiefs; directive to use biometrics to gain access in the VRS and the VS; development of application to limit the number of personal data in the NLRV and the deployment of application to wipe-out the NLRV from storage devices in the offices of the election officer; finalization of rules and guidelines on limiting the use of VS and NLRV in the local field offices; streamlining of the registration forms to cover only personal data required by Republic Act No. 8189; execution of Non-Disclosure Agreements with COMELEC personnel; planned execution of Data Sharing Agreements with Law Enforcement Agencies; incorporation of Notice in all documents requested by data-sharing agencies; drafting of a Data Privacy Manual; nationwide training of all field officials on DPA compliance; submission of Privacy Impact Assessment to NPC; meeting with PNP to discuss security concerns of COMELEC field offices; the publishing of the required notification to affected data subjects in two newspapers of general circulation and the completion of personal delivery of individual notices to affected data subjects in Wao, Lanao del Sur.

As to the order to notify affected data subjects of the personal data breach, COMELEC reported the publishing of notifications for individuals whose records are included in the NLRV in two newspapers on 24 February 2017. COMELEC also reported shipping individual notifications to those individuals included in the VRS of Wao, Lanao del Sur and the completion of personal delivery to affected voters on 27 February 2017.

On 15 March 2018, this Commission received CTL Responsive Comment on the Preliminary Fact-Finding Report, presenting his defenses to the issues raised before this Commission.

Issues

What remains for Resolution before this Commission are:

1. Whether there was negligence in the safekeeping of the desktop that contained the personal data of registered voters
2. Whether there was concealment of the personal data breach by failing to notify the Commission and the data subjects affected.

Decision

1. Negligence in the safekeeping of the desktop computer that contained the personal data of registered voters.

On 15 March 2018, CTL submitted his Responsive Comment to the Preliminary Fact-Finding report denying the allegation of negligence in the safekeeping of the desktop computer containing personal data of voters. He averred to have implemented physical security measures such as causing the installation of padlocks to every point of ingress and egress of the office. To support his defense, he attached to his Comment photographs of the whole office building where the COMELEC office in Wao is located, and of all doors and windows of the office showing that padlocks were properly installed. Moreover,he

maintained that he assigned his casual employee, to make sure that all points of entry and exit, including the windows, are locked before the last person leaves the office. A sworn affidavit of the casual employee is also attached to his Comment attesting to this claim. CTL maintains that what took place at the COMELEC office in Wao was a robbery with force upon things, whereby the robber gained entry by destroying the back window. He asserted that said robbery was beyond his control.

Section 20 of the DPA mandates personal information controllers (PICs) to implement reasonable and appropriate organizational, physical and technical security measures to protect personal information against natural and human dangers. What is reasonable and appropriate in a given circumstance is determined, in part, by 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 practice, the cost of security implementation and relevant guidelines issued by this Commission. There is negligence if there is failure to implement such reasonable and appropriate security measures.

In this case, CTL cannot be said to have been negligent in implementing reasonable and appropriate security measures to prevent the taking of the desktop computer containing voter personal data. Just like what a reasonable and prudent man would have done to secure the computers inside the office, CTL placed padlocks and gave instructions to make sure that all doors and windows are locked at the end of the working day. He also installed a strong password to said desktop computer and only he and his casual employee knew the said password. The robbery was committed with force upon things, implying that the perpetrator had to break the locks and force his way through the back window into the office of the Election Officer. Further, COMELEC, in their personal data breach report to this Commission, maintains that technical security measures are in place to limit access to the VRS program in the desktop computer and that the VRS and the NLRV data are encrypted in AES 256.

Considering the submissions of COMELEC to this Commission, and the continuing efforts to strengthen its security measures, this Commission holds that the evidence is insufficient to warrant criminal prosecution

for providing access due to negligence.

2. Concealment of the Personal Data Breach.

The reported robbery of the COMELEC field office in Wao, happened on 11 January 2017. COMELEC notified this Commission of the personal data breach only on 28 January 2017.

Section 20 Chapter V on the Security of Personal Information of the Data Privacy Act of 2012 provides:

Section 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. Xxx (Emphasis supplied.)*

The Implementing Rules and Regulations and NPC Circular 16-03 defined what constitutes prompt notification. That is, notification of personal data breach shall be 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.

The IRR allows delay in the notification 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.

In the events leading to the loss of the computer, COMELEC narrated in their breach notification that the loss was discovered at around 8:00 am of 12 January 2017 by MTA, a Job Order casual employee of the Local Government Unit detailed at the COMELEC field office. On the same day, CTL informed, in writing, NDY of the robbery incident and the loss of the desktop computer. The incident was also reported to the Wao police, who immediately conducted its initial investigation of the case.

Upon ascertaining the possibility of a personal data breach, COMELEC ITD issued a memorandum on 24 January 2017 addressed to Executive Director/ Data Protection Officer JMT, advising him that since the lost computer contained personal information, notice of such loss should be submitted to the NPC and affected data subjects. JMT received the memorandum on 26 January 2017. He then immediately submitted the required notification to this Commission two days later on 28 January 2017. COMELEC communicated that its mindset was on the operational aspect of the registration process, thus immediate action was taken to replace the lost computer to ensure the resumption of the conduct of continuing registration of voters in Wao. They also emphasized the implementation of security measures. COMELEC believes that the unauthorized acquisition of the personal data in the desktop computer would not likely present a real risk of serious harm to those affected because of the existing security measures. The VRS is protected from any unauthorized person gaining access to the program. Further, the VRS and the NLRV data are encrypted at par with the standard set by this Commission. It would require a certain degree of technical skill and decryption capability in order to extract the VRS and NLRV data from the desktop computer. There is low probability that real risk of serious harm would befall data subjects because of the security measures in place.

From the records of the case, and considering that NPC Circular 16-03 took effect only on January 13, 2017, or two days after the incident in Wao, this Commission finds that the delay in notification for the particular circumstances in this case do not amount to concealment as defined in the Data Privacy Act.

Section 30 of the DPA provides:

> *SEC. 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.*

CTL reported the incident to his superiors on the same day that the robbery was discovered. Indeed, the determination of the scope of the breach should have been completed faster, and notification of the Commission should have been immediate based only on available knowledge. While COMELEC claims that the security measures are adequate considering the use of encryption and other safeguards, it should have been more circumspect. Such assertion by itself is inadequate basis to support the assumption that notification is not necessary. We take notice, however, that guidelines such as the factors to consider in determining necessity of notification have been provided only in NPC Circular 16-03.

In sum, this Commission finds that there is insufficient evidence to recommend the prosecution of the responsible officers of COMELEC or CTL for the crimes of Access due to Negligence under Section 26, or Concealment of a Security Breach under Section 30 of the Data Privacy Act of 2012.

This Commission considers, however, the need to ensure that existing policies on data privacy and data security are operationalized not just in the Central Office of COMELEC but also in regional and local field offices as well. It is not sufficient to provide documentation of compliance with the DPA, rather, it must be integrated in daily operations and data processing activities. While the evidence is not

sufficient to warrant criminal prosecution, COMELEC must be able to demonstrate compliance with the DPA.

The National Privacy Commission is mandated, under the DPA, to protect personal information. To this effect, NPC Circular 16-03 on Personal Data Breach Management provides guidelines to help PICs prevent and properly manage such breaches when they occur. Further, Section 9 of the same Circular provides for a procedure for post-breach review for the purpose of improving the personal data breach management policies and procedures of the PIC:

> **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.*

In order to ensure that existing breach management policies and procedure are being implemented, this Commission finds it necessary to further require COMELEC to submit its post-breach review report.

WHEREFORE, premises considered, the **COMMISSION ON ELECTIONS** is **ORDERED** to SUBMIT to this Commission, within thirty (30) days from receipt of this Decision:

1. The Designation of Data Protection Officers/ Compliance Officers for Privacy for every Regional Unit and the names and contact information thereof;
2. A copy of its Security Incident Management Policy, pursuant to Sections 4 and 5 of NPC Circular 16-04, including documents demonstrating:
    a. Creation of its Breach Response Team, and the composition thereof;
    b. Dissemination of this Security Policy to all election field offices;
3. Complete Post-Breach Report on its management of this Personal Data Breach in compliance with Section 9 of NPC Circular 16-03.

SO ORDERED.

Pasay City,
15 August 2019.

(Sgd.) IVY D. PATDU
Deputy Privacy Commissioner

WE CONCUR:

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

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

Copy furnished:

JMT
Commission on Elections

CTL
Wao

(x) LEGAL AND ENFORCEMENT OFFICE
(x) GENERAL RECORDS UNIT

CPM,

Complainant,

-versus-

NPC Case No. 19-258
For: Violation of Section 25 (b) of the Data Privacy Act of 2012

GREEN MONEY TREE LENDING CORP. (CASHWAGON),

Respondents.

x----------x

RESOLUTION

For consideration of the Commission is the Motion for Dismissal filed by Respondent Green Money Tree Lending Corp. (Cashwagon) dated 14 August 2019. Its allegations state:

> 1. On 20 June 2019, a discovery conference was set to hear the complaint of herein Complainant against herein Respondent for the latter's alleged violation of data privacy against the former, wherein both parties hereto are required to attend said conference. However, only the Respondent appeared during said discovery conference, thus, said conference was reset to 30 July 2019;
> 2. On 30 July 2019, herein Complainant failed again to appear/attend said discovery conference despite its resetting. Thus, herein Respondent manifested during said conference that it will file the necessary motion to dismiss this present complaint.
>
> WHEREFORE, premises considered, respondent most respectfully moves for the dismissal of this present complaint on the sole ground that Complainant herein failed to appear for two (2) consecutive settings of the discovery conference despite due notice on her part.

At the outset, there is a need to clarify that the Commission's Rules of Procedure[1] does not provide that a party's non-appearance in the Discovery proceedings is a ground for the dismissal of a case. The Rules only provide the following grounds for the outright dismissal of a complaint:

[1] NPC Circular 16-04

> Section 12. Outright Dismissal. – The Commission may dismiss outright any complaint on the following grounds:
>
> a. The complainant did not give the respondent an opportunity to address the complaint, unless failure to do so is justified;
> b. The complaint is not a violation of the Data Privacy Act or does not involve a privacy violation of personal breach;
> c. The complaint is filed beyond the period for filing; or
> d. There is insufficient information to substantiate the allegations in the complaint or the parties cannot be identified or traced.

The grounds in the abovementioned provision not being present in the subject Complaint, the Commission finds that there is no sufficient ground to dismiss the complaint on the sole ground that the Complainant failed to appear for two (2) consecutive settings despite due notice on her part.

WHEREFORE, all these premises considered, this Commission resolves to DENY the Motion for Dismissal filed by the Respondent Green Money Tree Lending Corp. (Cashwagon) and hereby ORDERS the Respondent to submit its responsive Comment to the Complaint within ten (10) days from receipt of this Resolution.

SO ORDERED.

Pasay City, 5 November 2019.

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

We concur:

(Sgd.)
IVY D. PATDU
Deputy Privacy Commissioner

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

COPY FURNISHED:

CPM
Marikina City

GREEN MONEY TREE LENDING CORP. (CASHWAGON)
Data Protection Officer
Makati City

GENERAL RECORDS UNIT
ENFORCEMENT DIVISION
National Privacy Commission

RBG,

Complainant,

-versus-

CID Case No. 18-F-064
For: Violation of the Data Privacy Act of 2012

CB,

Respondent.

x----------x

DECISION

AGUIRRE, D.P.C.

For consideration of this Commission is the Affidavit-Complaint by Complainant RBG dated 01 June 2018 against Respondent CB for an indeterminate violation of the Data Privacy Act (DPA).

These Proceedings

On 24 July 2018, this Commission, through the Complaints and Investigations Division (CID), issued an Order for the parties to confer for discovery on 14 August 2018. On 13 August 2018, the counsel for respondent filed a formal entry of appearance with Motion [to] Reset Hearing due to a prior scheduled hearing of counsel even before he was engaged for this case.[1]

On 14 August 2018, the complainant and her counsel appeared at the Discovery Conference, where the CID gave a verbal order to complainants to file written interrogatories for the respondent to answer. On 20 August, the complainant, through counsel, filed "Proposed Queries of the Complainant for the Respondent to Answer."[2]

Only the complainant's counsel attended the discovery conference on 17 September 2018.[3] The respondent was then ordered to submit his answer to the complainants' written interrogatories within five (5) days

[1] Records, p. 23-25.
[2] Ibid at p. 29.
[3] Ibid at p. 35.

from receipt of the Order.[4] On 26 September 2018, the respondent filed his Responsive Comment to the Complainant's Affidavit-Complaint.[5] On the same day, the respondent filed a manifestation invoking his right against self-incrimination and asked to be excused from answering the written interrogatories.[6]

On 19 October 2018, the complainant filed an Ex-Parte Motion to Declare the Respondent As In Default and to Resolve the Instant Case based on the Pleading Submitted by the Complainant.[7] The motion was grounded on the fact that the respondent failed to file the pleadings required of him within the provided reglementary periods. In the same motion, the complainant attached a judicial affidavit of LBC, the younger sister of the complainant and the respondent.

On 15 November 2018, the complainant filed her reply to the respondent's comment on 15 November 2018.

Facts

On the basis of these, the following facts are established:

The complainant and the respondent are siblings. The complainant resides in New Jersey, United States. On 30 May 2017, the Philippine Statistics Authority (PSA), Sta. Mesa branch, acting on a letter-request allegedly by the complainant, released two (2) marriage certificates which matched the name "RCB" - one between her and a certain JM dated 18 September 1977, and another with a certain VG dated 16 June 1983.[8] Along with the two documents was a certification by National Statistician and Civil Registrar General LSB.[9] The complainant was not in the Philippines for the whole month of May 2017.[10]

Sometime in August 2017, the respondent filed a bigamy case against the complainant and her present husband, VG, with the City Prosecutor's Office of Manila.[11] The counsel of complainant wrote the

[4] Ibid at p. 35.
[5] Ibid at p. 35.
[6] Ibid at p. 35.
[7] Ibid at 44-47.
[8] Ibid at 50-54.
[9] Ibid at 55.
[10] Ibid at 64.
[11] Id.

PSA to request for a copy of the letter request allegedly signed by the complainant and the copy of the acknowledgment receipt and authorization of the person who received the marriage contracts of the complainant.[12] The PSA, through the Assistant National Statistician, replied that they cannot provide a copy of the requested documents, despite exhausting all efforts.[13]

In a resolution dated 12 December 2017, the Office of the City Prosecutor of Manila dismissed the complaint for bigamy[14] as well as the Motion for Reconsideration.[15]

Arguments of the Parties

The Complainant now comes to the Commission to file a case against the respondent for an unspecified violation of the DPA. In her Affidavit Complaint, she alleges that she was taking a tour in Europe during the time her marriage certificates were requested from the PSA.[16] She alleges that she never requested for a copy of her marriage certificates as she was not in need of it, neither did she authorize the respondent to make the said request. She claims that the respondent forged her signature and later used the marriage certificates to file a bigamy case against her despite his knowledge that her first marriage was annulled. She asserts the respondent intends to malign, besmirch, and destroy her reputation by obtaining the marriage certificates and filing the bigamy case against her. She alleges that the respondent, in falsifying her signature in the letter request, did not just violate the DPA but also the PSA Office Memorandum No. 2017-050 dated 17 April 2017 which provides that a marriage certificate can only be released to the owner or their representative.[17]

The respondent denies any personal participation regarding the alleged falsified letter request and points out that such copy of the alleged falsified letter was not attached to the Affidavit-Complaint.[18] He alleges that numerous cases have been filed before various offices

[12] Ibid at 56.
[13] Ibid at 57.
[14] Ibid at 58-61.
[15] Ibid at 62.
[16] Supra at note 8.
[17] Supra at note 8.
[18] Records, p. 41

and courts involving the parties herein and their other siblings arising out of their disagreements and/or misunderstandings involving co-owned properties. [19]

Issue

The sole issue to be resolved in this case is whether the respondent committed a violation of the DPA to warrant a recommendation for prosecution.

Discussion

The Commission must first resolve the complainant's Ex-Parte Motion to Declare the Respondent as in Default dated 18 October 2018 based on the allegation that he failed to file the pleadings required of him within the provided reglementary periods. Specifically, the complainant asserts that on 17 September 2018, the CID issued an order requiring the respondent to submit his answer to the written interrogatories of the complainant dated 20 August 2018. In the complainant's motion, she alleges that:

> 8. The order dated September 17, 2018 was received by the complainant thru her sister LBC on September 22, 2018 at her given address at Quezon City **so it follows that respondent also received his copy of the order on the same date or even earlier.**
>
> xxx
>
> 10. One month has lapsed from the date of the order and no answer/comment has been filed by the respondent. The deliberate failure of the respondent to file an answer/comment on the written interrogatories of the complainant and the instant complaint is tantamount to a waiver of his right to file an answer/comment therefore it is but fair and proper that the respondent be declared as in default and the instant complaint be finally resolved by the Honorable Commission based on the affidavit complaint of the complainant together with its annexes.[20]

The complainant, through counsel, thus assumed that the respondent received the Order on 22 September 2018 – the same day she received it. In the respondent's Manifestation filed on 26 September 2018,

[19] Ibid, p. 42.
[20] Ibid at 46. Emphasis supplied.

however, he alleges that he received the Order on 24 September 2018 which gave him ten (10) days to file a Responsive Comment and five (5) days to submit Answers to the Complainant's written interrogatories.[21] Such Manifestation is his response in lieu of an Answer to the written interrogatories, alleging that:

> 6. Considering the foregoing and invoking the right of herein respondent against possible self-incrimination, without necessarily admitting anything, with all due respect to the Honorable Commission, herein respondent would beg to be excused from answering the Questions propounded by the complainant. The complainant should prove their allegations against herein respondent with their own evidence and with their own witness.[22]

The respondent's Responsive Comment was also filed on 26 September 2018.

The respondent having submitted the pleadings two (2) days from receipt of the Order, or within the five and ten day reglementary periods provided, and the complainant not having presented any evidence to support her allegations, the Commission finds that there is no ground to grant the complainant's Ex-Parte Motion to Declare the Respondent as in Default.

The respondent did not commit a violation that warrants a recommendation for prosecution under the Data Privacy Act of 2012.

The complaint is premised on the allegation of falsification of the letter-request to the PSA for the release of the two (2) marriage certificates.

In the Affidavit-Complaint, the complainant alleges that:

> xxx In the instant case my signature is forged neither have I authorized CB to obtain my marriage certificates from the Philippine Statistics Office. It is an absurd situation on my part to secure copies of my marriage certificates just to incriminate myself for the crime of bigamy. Since CB has not controverted my denial on the letter request before the city prosecutor of Manila, **he is presumed to be the author of the falsified letter request.**[23]

[21] Ibid at 39.
[22] Ibid at 40.
[23] Supra at note 8. Emphasis supplied.

Contrary to the complainant's position, in administrative proceedings such as this case, it is the complainant who carries the burden of proving their allegations with substantial evidence or such "relevant evidence that a reasonable mind might accept as adequate to support a conclusion."[24]

Such allegation by the complainant remains unsubstantiated. The letter request to the PSA, the document where the forged signature would have been found, has not been included in the record due to PSA's inability to locate it.[25]

In her Reply to Responsive Comment of the Respondent to Complainant's Affidavit-Complaint, the complainant states:

> 2. The fact that the respondent failed to explain how did he obtain said marriage certificates of the complainant from the Philippine Statistics Office he is presumed to be the author of the falsified letter request allegedly signed by the complainant as he benefited from it when the same documents was used by the respondent in filing a case of bigamy against the complainant and her husband VG before the City Prosecutor of Manila.

The Commission cannot rely on presumptions that are unsupported by fact or by law. It is bound to adjudicate following its Rules of Procedure, which provides:

> *Section 22. Rendition of decision.* – The Decision of the Commission shall adjudicate the issues raised in the complaint on **the basis of all the evidence presented** and its own consideration of the law.[26]

As such, on the basis of all the evidence presented, the Commission finds that there is insufficient evidence to support the claim of the complainant that the respondent forged her signature in the letter request to the PSA. There is nothing in the Affidavit-Complaint or its supporting documents that would reasonably connect the respondent to any of the possible violations enumerated under the DPA.

The Commission therefore resolves to dismiss the complaint for lack

[24] Ombudsman v. Fetalvero, G.R. No. 211450, 23 July 2018.
[25] Supra at note 23.
[26] NPC Circular No. 16-04 dated 15 December 2016 ("NPC Rules of Procedure"), Sec. 22, Emphasis supplied.

of substantial evidence required in establishing cases before quasi-judicial bodies.

WHEREFORE, all these premises considered, the Commission resolves to:

(1) DENY the Motion to Declare the Respondent as In Default filed by Complainant RBG; and

(2) DISMISS the complaint of RBG against Respondent CB

SO ORDERED.

Pasay City, 19 November 2019.

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

Concurring:

(Sgd.)
IVY D. PATDU
Deputy Privacy Commissioner

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

COPY FURNISHED

ERY
Counsel for Complainant
Quezon City

CNE
Counsel for Respondent
Quezon City

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

KRL,

Complainant,

-versus-

CID Case No. 17-K-003
For: Violation of the Data Privacy Act of 2012

TRINITY UNIVERSITY OF ASIA, AA, MC, NCB, RG GV, GCT, RR, MR, PB

Respondents.

x----------x

DECISION

AGUIRRE, D.P.C.

For consideration before this Commission is a complaint filed by KRL against Trinity University Of Asia, **AA, MC, NCB, RG GV, GCT, RR, MR, and PB,** for an indeterminate violation of the Data Privacy Act (DPA).[1]

These Proceedings

On 19 April 2018, this Commission, through the Complaints and Investigation Division, conducted a Discovery Conference. At the Conference, the respondents were directed to submit a responsive Comment within ten (10) days from receipt of the Order dated 26 April 2018.[2]

On 30 April 2018, the respondent university, through counsel, filed a Notice of Entry of Appearance with Motion for Clarification of Procedure. The respondent university raised an issue regarding the propriety of the Commission's act of taking immediate action on the complaint without having the complainant exhaust all the administrative remedies available to him. The respondent university also argued that the complaint should have been referred to a Mediation Officer to explore the possibility of first reaching an amicable settlement.

[1] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [DATA PRIVACY ACT].
[2] Records, p. 46; see NPC Circular No. 16-04, Rule III, Section 15.

On 18 May 2018, the respondent university filed a Motion to Admit Comment with Partial Compliance, citing the "amount of documentary evidence being required from the respondent University."[3] The individual respondents, AA, MC, NCB, RG, GV, GCT, RR, MR, and PB have not submitted their individual comments. The Comment of the respondent university contained a narration of the incidents and arguments against the complainant's allegation, and attached as annexes a Privacy Impact Assessment (PIA), DTR and Payroll processes, attendance records of the complainant, as well as affidavits from the Human Resources and Development Unit (HRDU) Director, the Clerk of the College of Business Management and Accountancy (CBMA), the Secretary of the CBMA, a part-time faculty member of the CBMA, the Department Head of the Real Estate Management (REM) of CBMA, and the Finance Director.

Facts

On the basis of these, the following facts were established:

The complainant was a part-time faculty member in the Trinity University of Asia. He was named in a letter-complaint written by the respondents, who are all faculty members of the Trinity University of Asia, informing WUT, president of the university, about alleged unreasonable and oppressive practices of the newly-appointed dean of the College of Business Management and Accountancy (CBMA), CS. Dean CS was the one who informed the complainant about the letter-complaint on 10 November 2017.

Copies of the letter-complaint were also furnished to the Chairman of the Board, the Commission on Higher Education (CHED), and the Regional Director of the Department of Labor and Employment (DOLE).

The pertinent portion of the letter-complaint stated as follows:

Gross ignorance of labor management

She called HR office and asked if [respondent university] follows the principle "no work, no pay." She received an affirmative answer. She did not further inquire as to other

[3] Id, p. 76

details. She has no knowledge that holidays and those declared no classes for reason of fortuitous events and force majeure shall be paid to the employees as provided for by Labor Code provisions. She deducted all the hours/period for the holiday and no classes to the prejudice of the faculty members, and erased the total number of days we reported. But for one of her recruited faculty, by the name of **KRL, this dean, favorably endorsed the former's DTR.** The dates (August 21 and 28) included are the same dates for the other faculty members who were deducted from them but no deduction for Mr. Legaspi. Is she at liberty to make a mockery of the provisions of the Labor Code? To apply the law negatively to those employees, she doesn't like and to apply the same provisions positively to those employees, she likes? Are we changing now the core values of [respondent university]?[4]

Based on those statements, complainant concludes that the respondents were able to access his DTR and pay slip because they are specific about the deductions and have a strong conviction that he was paid for the dated holidays.[5] The letter-complaint did not, however, attach copies of the complainant's daily time record (DTR) or pay slips.

The respondents do not deny having accessed the complainant's DTR. In fact, one of the respondents, RR, a Department Head of Real Estate Management and faculty member, admits that he chanced upon it when he was scanning the bundled DTRs of the entire CBMA for the month of August 2017.[6] According to him, as a Department Head, he is sometimes asked to turn over accomplished DTRs of the faculty to the College Clerk or "attendance-in-charge" from the College Secretary when the latter is not present to personally receive it.[7] He was looking for his DTR in a pile that was alphabetically-arranged when he caught sight of the complainant's DTR.[8]

Complainant wrote a letter-complaint to the NPC to hold the respondents liable for the damages caused to him personally and professionally.[9] He stated that he intentionally did not file the complaint with Trinity University of Asia as he already lost trust and confidence in the institution.[10]

Arguments of the Parties

[4] Id., at p. 6-7. Emphasis in the original.
[5] Id. at p. 1.
[6] Id. at p. 117.
[7] Id. at p.118.
[8] Ibid.
[9] Id., at p.2.
[10] Id., at p. 2.

The complainant now comes to the Commission saying that he feels his right to privacy has been violated.[11] According to him, the respondents' act of copy furnishing CHED with their letter-complaint caused his personal information to be exposed to a more severe extent which caused him dismay.[12] He asserts that as a human resource management professor and someone who has been working in the industry for quite some time, he is fully aware that such information should be confidential.[13] He states that he has experienced sleepless nights from the time he knew about the incident and feels threatened that all the personal information he submitted to the institution is at risk of exposure.[14]

The respondent university, in their Notice of Entry of Appearance with Motion for Clarification of Procedure, argues that the complainant failed to allege that he has exhausted all remedies available to him.[15]Citing the Commission's Rules on the Alternative Modes of Dispute Resolution,[16] it likewise raises that the complaint should have been referred to a Mediation Officer for assistance in reaching an amicable settlement[17] since the complaint is devoid of any serious allegations that would warrant immediate conduct of investigation by the Commission.[18]

In their comment, the respondent university allege that they have substantially complied with the requirements of Republic Act No. 10173 or the Data Privacy Act of 2012 ("DPA"), having completed phases 1 and 2 of the registration process of the Commission. While it has already completed privacy impact assessments for most of its processes, the DTR system is not one of them. The respondent university conducted a privacy impact assessment on the DTR system after the Discovery Conference.[19]

The respondent university asserts that consent of data subjects is not required for the processing of the DTRs, because it is an

[11] Id., at p.1.
[12] Ibid.
[13] Id., at p.1
[14] Id., at p.2
[15] Id., at p.52.
[16] NPC Circular 16-04, Sections 25-27.
[17] Records, p. 55.
[18] Id., at p.55-56.
[19] Id., At p. 92-103.

administrative matter inherent in the operation and legitimate purpose of the university.[20] It vehemently denies that there was unauthorized processing of complainant's personal data, as DTRs contain no personal or sensitive personal information, nor are the DTRs considered confidential by the University and its faculty members.

According to them, the DTRs are processed in the following manner:

1. 1. The full time faculty members with overload, and part-time faculty members fill up the DTRs regularly and turn them over to the designated Attendance-in-Charge (usually, the Secretary/Clerk of the College).
2. On every cut-off date (the 15th and 20th of the month), the designated Attendance-in-Charge will check the DTRs for completeness and accuracy. They will forward the same to the office of the Dean for checking, signature, and endorsement to the HRDU.
3. The HRDU staff will check the data in the DTRs and will determine whether the DTR data match the data gathered from the biometrics. Once confirmed, the HRDU staff concerned forwards the attendance records to the HRDU Director for approval.
4. The HRDU forwards the DTR to Finance Unit for payroll processing.[21]

There are instances when the College Clerk or "attendance-in-charge" in the Office of the College Secretary is not around to personally receive the DTRs, particularly for the part-time faculty members who have limited time in the University and who rarely chance upon the College Clerk.[22] For purposes of meeting the cut-off date for submission of the DTRs, as a matter of practice, faculty members transmit the DTRs to the College Secretary through the following methods: (a) by posting it in the corkboard inside the Dean's Office; (b) by asking a co-faculty to submit it to the College Clerk; (c) by asking their respective personal staff to submit the DTR to the College Clerk; (d) by submitting it through the Department Head, and the latter will transmit the DTR to the College Clerk; (e) by asking the

[20] Id., At p. 85.
[21] Id., At p.107.
[22] Id., At p.109.

class beadle/president to submit the DTR of the faculty concerned to the College Clerk; or (f) course it through the Student Apprentice available.[23]

The respondent university denies that the professors illegally accessed complainant's pay slip. According to them, the payroll system of the University is web-based and can only be accessed through the internet by the employee concerned. The pay slips are downloaded by the Payroll Master for viewing and printing by the concerned employee using his/her unique Employee ID code and password.[24]

Issues

The issues to be resolved in this case are:

1. Whether the Commission erred in taking immediate cognizance of the complaint;
2. Whether the Commission erred in not requiring the parties to submit the complaint to alternative dispute resolution;
3. Whether the complainant's DTR contains personal information; and
4. Whether the respondents committed a violation in relation to the complainant's DTR, warranting a recommendation for prosecution under the Data Privacy Act of 2012.
5. Whether the respondents committed a violation in relation to the complainant's pay slip, warranting a recommendation for prosecution under the Data Privacy Act of 2012.

Discussion

The NPC committed no error in taking immediate cognizance of the complaint.

Section 4 of NPC Circular No. 16-04 provides that no complaint shall be entertained unless it has been shown that the complainant has informed, in writing, the concerned entity of the privacy violation or personal data breach and if there was no response within 15 days or timely and appropriate action on the claimed privacy violation or personal data breach.

[23] Id., at p.109.
[24] Id., at p.124.

In his complaint filed on 28 November 2017, the complainant admitted the following:

> I intentionally did not file the complaint to [respondent university] as I already lost my trust and confidence to the institution knowing that such information was given and exposed to and by the faculty members.[25]

Nevertheless, the following exchange during the discovery conference shows that there was an attempt to comply with the requirement of exhaustion of administrative remedies:

> KRL: Your honor just to answer that, I approach NPC on November 28, 2017 and they advised me to write a letter first to Trinity University of Asia, so I was advised correctly of what the process is all about and then they ask me to wait for 15 days if there will be no action, that's the time that we will pursue it and I informed them that "after 15 days there was no response from the Human Resource Department regarding my complaint, they weren't able to reach out to me: so that's the time I pursued it.[26]

The respondent university indeed received a copy of the complaint on the same day it was received by Commission. The complainant stated for the record that when he submitted his complaint with the Commission, he had been advised to wait at least 15 days to afford the respondent university the opportunity to take appropriate action. However, no action was taken on his complaint.

At any rate, the same Section in Circular 16-04 provides that the Commission may waive any or all of the requirements for exhaustion of remedies, at its discretion, upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to the affected data subject. Considering the allegations on the face of the complaint that the complainant's DTR and pay slips may have been illegally accessed and disclosed by the respondents, it is well within the authority of the Commission to take action on this serious allegation of a violation of the DPA.

The decision to submit a case for alternative dispute resolution lies with the parties.

[25] Id., At p.2.
[26] Id., at p.32.

The Alternative Dispute Resolution Act of 2004 (the ADR Act of 2004) embodies the policy of the state to actively promote party autonomy in the resolution of disputes, or the freedom of the parties to make their own arrangements to resolve their disputes.[27] Mediation, in particular, is an alternative dispute resolution mechanism characterized by the principles of voluntariness, integrity of determination, and the policy that the decision-making authority in the mediation process rests with the parties.[28]

At the onset of the Discovery Conference, the complainant was asked if he was willing to compromise and settle amicably.[29] To this, the complainant answered in the negative.[30] To insist on the conduct of a mediation at this point would have been a violation of not only the ADR Act of 2004 but of the Commission's own alternative dispute mechanisms at that time as well.

The DTR contains personal information.

In their Comment with Partial Compliance, the respondent university attached a Privacy Impact Assessment (PIA) report on the DTR System of Trinity University of Asia.[31] In the submitted PIA, the threshold analysis contained several questions, including: "(a) Will the project or system involve the collection of new information about individuals?"[32] To this, the respondent answered "no."[33]

A perusal of the complainant's DTRs, however, would show that the DTR document contains the complainant's handwritten name, the college or unit where he teaches, and the month covered.[34] The majority of the document is a table of dates with filled-out "time in" and "time out" fields. At the bottom of the document, there is a "prepared by" field with the complainant's handwritten name and signature.[35]

The DPA provides that personal information is any information,

[27] R.A. 9285, Section 2.
[28] Ibid., at Section 8.
[29] Records, p. 27-28.
[30] Id., at p.28.
[31] Records, p. 92.
[32] Records, p. 93.
[33] Records, p. 93.
[34] Records, p. 125-129.
[35] Ibid.

whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[36]

In this case, the complainant's name, college/unit, and signature are information from which his identity can be directly ascertained. The DTRs of the complainant, then, are considered to contain personal information.

In this case, the complainant's name, college/unit, and signature are information from which his identity can be directly ascertained. The DTRs of the complainant, then, are considered to contain personal information.

The failure of the respondent university to treat the information collected in the monthly DTRs as personal information resulted in the lack of clearly documented and implemented policies regarding its processing. In conducting a PIA, the personal information controller – the respondent Trinity University of Asia, in this case - must refer to the law to determine what it should consider as personal information. If such collected information meets the definition or enumeration provided by the DPA for personal or sensitive personal information, then the obligations provided by law should be complied with: its processing must be based on any of the lawful criteria under the law, and it must be accorded the adequate organizational, technical, and physical security measures, to name a few. Hence, even if the personal information controller views certain information as "public knowledge," it should still be properly classified according based on the definition provided by the law in the PIA and treated and protected accordingly.

It should be stressed that a PIA, however, is not an end in itself. In conducting a PIA, a personal information controller is tasked to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a personal information controller.[37] When no PIA has been conducted yet, it should be done on a per-process basis across all the processes of the

[36] R.A. 10173, Section 3(g).
[37] NPC Advisory 2017-03.

of he organization in order to assess the current situation, the existing controls in place, the compliance gaps that have been overlooked, the privacy risks associated with them, and identify the measures needed to address them.

In order to specifically assess these risks, the personal information controllers should carry out their organization's data inventory and data map since both will help in classifying different categories and uses of personal data, and how they flow across the organization.

A PIA should be conducted prior to the deployment of a project, product, or service that involves the collection of personal information. When there are new or revised industry standards, organization policy, law or regulation, or when there are changes to methods in which personal information is handled, a personal information controller should conduct a PIA again on the pertinent process.

To emphasize, it should not only identify the existing controls and risks a project, product, or service may have upon personal data privacy, but it should lead to the identification of remedial actions or mitigation measures necessary to avoid or reduce those risks. These remedial actions and mitigation measures may be incorporated in the organization's Privacy Management Program (PMP).

In this case, the submitted PIA by the respondent university stated the existence of organizational, physical, and technical measures in place for the DTR system. After this, however, the respondent university did not provide details on these or how it intended to address what the Comment referred to as "long-standing practices" of the faculty regarding their submission of DTRs.[38] The affidavits of the College Clerk,[39] the Secretary of CBMA,[40] one of the part-time faculty,[41] and a Department Head from the CBMA,[42] admitted as well that there are several long-standing practices where the DTRs are transmitted through different routes[43] that deviate from the official process in handling the employees' DTR.[44]

[38] Records, p. 86.
[39] Id., at p. 109.
[40] Id., at p.114.
[41] Id., at p. 116.
[42] Supra note 22.
[43] Supra note 24.
[44] Supra note 22.

Nowhere in the respondent university's submitted PIA were these practices even mentioned, despite the fact that these should been considered as compliance gaps resulting in privacy risks that needed to be mitigated by reasonable and appropriate organizational, physical, and technical measures. By simply treating it as a checklist, the respondent university treated the PIA as the ultimate result, when it should have considered it as a tool to improve its processes and systems for the protection of its stakeholder's privacy.

It is incumbent upon the respondent university to revise its PIA in general and on the DTR system in particular to reflect and address the gaps brought about by actual, current practices and as identified in the letter-complaint.

Respondents did not commit a violation in relation to the complainant's DTR to warrant a recommendation for prosecution.

In analyzing whether there are possible violations by the respondent faculty members of the DPA that warrant a recommendation for prosecution, we primarily look into the different stages of processing that the personal information undergoes, and determine whether each one is supported by one or more lawful basis for processing enumerated in the DPA.

The lack of either a uniform policy or process that covers the actual practices in the handling of the employees' DTR, including the ones identified by the aforementioned affiants, cannot by itself give rise to a cause of action for unauthorized or illegal access to personal information as provided by the DPA.[45] It was admitted by respondent RR that as a Department Head, he is sometimes asked to turn over accomplished DTRs of the faculty to the attendance-in-charge from the College Secretary when the latter is not present to personally receive it.[46] This color of authority to access the DTRs, with the acquiescence of the faculty members over time, cannot be overlooked.

[45] SEC. 26. *Accessing Personal Information and Sensitive Personal Infor2mation Due to Negligence.* – (a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.
[46] Supra note 8.

Indeed, the interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.[47] That cannot be said to be the case here, as the complainant and other faculty members could have reasonably expected the further access of their DTRs by different persons in the college upon submission thereof based on the existing practice of the school.

This Commission has previously decided that this concept of "reasonable expectation" is considered in determining the legitimacy of the additional processing by examining whether such further processing is compatible with the original business purpose communicated to the data subject and not beyond what the data subject may reasonably expect as to the purpose, scope, manner, and extent of the processing of their personal data.[48]

Having discussed respondent professors' initial access, the next stage of processing in this case was the use of the information in the DTR to support their claim of "gross ignorance of labor management" in their letter-complaint about Dean CS.

The individual respondents used the complainant's name to give a specific case of "gross ignorance of labor management," which was one of the allegations against Dean CS. The letter-complaint questioned the Dean's alleged unequal treatment regarding holidays and suspended class days due to fortuitous events in the DTRs of faculty members, in relation to the provisions of the Labor Code on holiday pay. To the respondent professors' personal knowledge, the complainant was the only faculty member who did not receive deductions on the holidays of August 21 and 28 of 2017. The use of the complainant's name, therefore, was necessary for the protection of the respondents' lawful rights and interests as contemplated by Section 13(f) of the DPA. The fact that the respondents copy-furnished both the CHED and DOLE does not veer away from that lawful criteria, considering the allegations of the letter-complaint may possibly be

[47] NPC Advisory Opinion 2018-20.
[48] See, Villegas v. Revilles, NPC Case 17-047, citing EU General Data Protection Regulation, Recital 47.

the concern of these agencies as well.

Although Section 13(f) applies to sensitive personal information while the information involved in this case is just personal information, the protection of lawful rights and interests under Section 13(f) by the respondent faculty members in this case is considered as legitimate interest pursuant to Section 12(f) of the DPA. This section provides that it is lawful to process personal information if it is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[49]

The DPA is not intended to cover every possible infraction in the workplace or even society. While the complainant may feel aggrieved with the mention of his name in the letter-complaint, it cannot be said, however, that the complainant incurred actual damage, considering the objective of that letter-complaint was to inform the President of Trinity University of their concerns about the Dean and not the complainant. In the event that the circumstances stated in the letter-complaint about the complainant are untrue, there are other remedies available to him under existing laws, although not the DPA. The merits of the letter-complaint and the truth of their claims are irrelevant to our determination whether there was a violation of the DPA in the processing of complainant's DTR.

The respondents did not commit a violation in relation to the complainants pay slip to warrant a recommendation for prosecution under the Data Privacy Act of 2012.

In the complaint, the complainant alleges that "based on [the statements in the respondents' letter], they were able to access [his] pay slip."[50]

In cases filed before administrative or quasi-judicial bodies such

[49] R.A. 10173, Section 12(f).
[50] Records, p. 1.

as the Commission, a fact may be deemed established if it is supported

In cases filed before administrative or quasi-judicial bodies such as the Commission, a fact may be deemed established if it is supported by substantial evidence, or that amount of relevant evidence which a reasonable mind might accept as adequate to justify a conclusion.[51]

The complainant's allegation in relation to his pay slip remains unsubstantiated. This is all the more true considering the affidavit of the Finance Director that stated "any figures or computation in determining one's payroll is done within the department's office and the finance personnel are the only ones who are authorized to view and do the computation" and that "no other department computes the figure, the HRD only provides the supplementary documents in order to arrive with the figure."[52] There is nothing in the allegations of the complainant that explain how the respondent faculty members could have circumvented the university process on the processing of pay slip to access the same aside from his mere speculation. Notice must also be made that there was no mention of the complainant's salary in the subject letter-complaint to WUT

WHEREFORE, premises considered, the Commission finds no violation of the Data Privacy Act on the part of the respondents Trinity University Of Asia, **AA, MC, NCB, RG GV, GCT, RR, MR, PB,** to warrant a recommendation for prosecution. The complaint filed by complainant KRL is hereby **DISMISSED**.

SO ORDERED.

Pasay City, 19 November 2019.

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

[51] Rules of Court, Rule 133, Section 5.
[52] Records, p. 177

Concurring:

(Sgd.)
IVY D. PATDU
Deputy Privacy Commissioner

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

COPY FURNISHED

KRL
Complainant
Quezon City

ABAD ABAD & ASSOCIATES
Counsel for Respondent
Makati City

COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

RESOLUTIONS

MFS,
Complainant,

- versus -

NPC Case No. 17-003
For: Violation of Data
Privacy Act of 2012

RJJ and SJJ,
Respondents.

x----------x

RESOLUTION

LIBORO, P.C.:

Assailed in this Motion for Reconsideration[1] is the Decision[2] dated 19 March 2018 of the National Privacy Commission (NPC) which declared that Respondents RJJ and SJJ did not violate Sections 25, 28, 29, 31, and 33 of the Data Privacy Act of 2012 (DPA) on unauthorized processing of personal information, processing of personal information and sensitive personal information for unauthorized purposes, unauthorized access or intentional breach, malicious disclosure, and combination of series of acts.

The Facts

MFS, through his Attorney-in-Fact GS, alleged in his complaint that Respondents RJJ and SJJ made use of their authority or connections to access sensitive personal information about the credit standing of complainant, the latter's husband and mother-in-law.

According to the Complainant, Respondents committed unauthorized processing of personal information, processing of personal information for unauthorized purposes, unauthorized access or intentional breach and malicious disclosure, all of which are prohibited by the Data Privacy Act of 2012.

[1] Records, p. 112-116.
[2] Id, at pp. 88-95. Penned by Privacy Commissioner Raymund E. Liboro, with Deputy Privacy Commissioners Ivy Patdu and Leandro Aguirre, concurring.

On 07 March 2017, this Commission received a Supplemental Complaint Affidavit[3] alleging:

> 1. *In June 2016, I personally called RJJ's mother to talk about RJJ and SJJ accessing our credit information and she verbally confirmed that SJJ is indeed looking into financial records, not only of ours, but the records of even another relative of hers named AMR.*
>
> 2. *On February 27, 2017 at 9:10am, I visited BPI AB Branch and VA, verbally confirmed that I am included in the Negative Data list. She also said that pending cases of data subjects can also be viewed in the said data list, which proves, that RJJ and SJJ also looked into my mother's credit information as they emphasized that they are also aware that she has a hit in Makati RTC.*

On 25 May 2017, this Commission received the Joint-Counter Affidavit of Respondents RJJ and SJJ, which stated in part:

> 1. *We both specifically deny the allegations of herein complainant.*
>
> 2. *It is unfortunate that my name (SJJ) is dragged on this mess and the good name of my employer Banco De Oro (BDO) simply because of the assumption herein complainant that I have access to the computer system of BDO that contains sensitive personal information about credit standing, if any.*
>
> 3. *First and foremost, I have no access to the computer system of BDO that contains sensitive personal information about credit standing of BDO's clients, if any. To be honest, I really don't know if BDO has sensitive personal information*

[3] Page 1, Supplemental Complaint-Affidavit of Complainant.

about credit standing of BDO's clients.

4. *Assuming there is such, I could not access the same because it is highly confidential as stated in his own very complaint letter. I am just a TELLER of BDO whose work is basically transacting business in front of a desk of the bank.*

5. *As correctly stated by BDO, I have no authority or access to such Negative Data Bank record.*

6. *Secondly, assuming but without admitting that I have access to the computer system of BDO, again, there is no way I can access their personal details/information since they are not BDO clients. As per answer of BDO, they are non-BDO clients.*

7. *Thirdly, assuming without admitting that they are BDO Clients, still BDO does not have any sensitive personal information about credit standing.*

8. *Also, there is no truth on the allegation in the Supplemental Complaint Affidavit dated February 27, 2017 that there was a confirmation from RJJ's mother that we were checking complainant's financial records and respondent RJJ was aware regarding their unpaid credit cards.*

9. *At the onset, I (RJJ) do not have access to the sensitive personal information of MFS from BDO or any institutions or offices.*

10. *And to simply get back at them or get even in mocking and defaming me, I used two things: 1) My personal knowledge of how the banking system works through my previous affiliations with banks and 2) my personal knowledge of their family background.*

11. *I (RJJ) previously worked for various BPO/ Financial Companies, which provided him with detailed Customer Service Training in terms of Credit Card Transactions, Fraud, Collections, Write Offs and the Negative Data Bank/Negative Data Base, and how the general Credit Card System works across the Globe.*

12. *In response to the complainant's demeaning statements in their FB messenger, I just came up with a believable bluff.*

On 18 June 2017, Complainant sent an email to complaints@privacy.gov.ph with the subject heading "Reply to Counter-Affidavits of Respondents" which states in part:

1. *RJJ has been badgering my mother, for several weeks, to plead to me and ask me to meet with them so he can apologize for what he has done. On April 23, 2017, I agreed on the basis that I would only want to know the truth. During the said meeting, it appears that his real intention is to force me to sign on an affidavit of desistance as he said; he does not want to be investigated further. The said affidavit is signed by my relatives RJJ's mother, RJJ's father and RC that served as witnesses to an agreement that never happened.*

2. *During our meeting with RJJ and SJJ, they showed me a list of his employers in which he has access to the Negative Data list. I took a photo of the document he gave us. However, upon reviewing RJJ' statements in his counter-affidavit, I noticed that there is a clear omission of facts, whether deliberate or not, as details of his employment in BPI is not disclosed in the affidavit he sent you.*

> 3. *We talked with SJJ on May 25, 2017. She told us that she is aware that she signed a second affidavit that counters her statements prior.*

From the pleadings and pieces of evidence submitted by all the parties concerned, this Commission rendered its decision finding that Respondents did not violate Sections 25, 28, 29, 31, and 33 of the Data Privacy Act of 2012 due to the insufficiency of evidence to support the Complainant's claim.

In the said decision, this Commission stressed that while it is a quasi-judicial body and unbound by strict technical rules of procedure, it is not a license to disregard certain fundamental evidentiary rules.[4]

> *While it is true that administrative or quasi-judicial bodies like the NLRC are not bound by the technical rules of procedure in the adjudication of cases, this procedural rule should not be construed as a license to disregard certain fundamental evidentiary rules. The evidence presented must at least have a modicum of admissibility for it to have probative value. Not only must there be some evidence to support a finding or conclusion, but the evidence must be substantial. Substantial evidence is more than a mere scintilla. It means such relevant evidence as a reasonable mind might accept as adequate to support a conclusion.*

On 24 April 2018, the Complainant received a copy of the 19 March 2018 decision of this Commission. Thereafter, Complainant filed its Motion for Reconsideration on 02 May 2018.

In his Motion for Reconsideration, Complainant contends that although admitting that there was no direct evidence of Respondents' actual access to the subject personal information, he was able to present circumstantial evidence to support his allegations.

According to Complainant, on 27 February 2017, the Bank of Philippine Islands (BPI) AB Branch Assistant Manager VA verbally confirmed that

[4] Primo Miro v. Marilyn Mendoza et al., G.R. Nos. 172532 172544-45, 20 November 2013.

he is currently in the Negative Data List. Additionally, Complainant provided a Facebook Messenger conversation with RJJ dated 10 April 2016 where the latter accused the former of being an irresponsible payer based on a Negative Data List, among other things. Complainant likewise claimed that such accusations from the Respondents could only be had if the latter had actual access to the said negative data list.

Further, Complainant attached a copy of text messages sent by Respondent RJJ apologizing to his mother, for all the accusations he made about the complainant.

Further, Complainant attached a copy of text messages sent by Respondent RJJ apologizing to his mother, for all the accusations he made about the complainant.

Lastly, Complainant MFS admitted that he was not a depositor of Banco De Oro (BDO), however, he claimed that the Negative File Information System (NFIS) can be accessed through registered users from different Banker Association of the Philippines (BAP) Member Banks rendering his status irrelevant for the issue on hand.

On 21 June 2018, this Commission received Respondents' Comment/ Opposition dated 16 May 2018. In their Comment/Opposition, Respondents contend that Complainant's Motion for Reconsideration is pro forma for failure to state in particular the error or mistake in fact or law in the decision of the Commission.[5]

Further, the Motion for Reconsideration of Complainant is a mere reiteration or rehash of the complaint filed before the Commission as it contained the very same issues, assignment of errors, and discussions and arguments and that it failed to raise new matters or arguments to warrant the reversal of the assailed decision.[6]

Respondents argue that the Motion for Reconsideration is defective for failure to comply with requirements set forth under Sections 2, 4, 5, and 6 of Rule 15 of the Rules of Court and that the same was already filed out of time.

[5] Records, p. 122.
[6] Ibid.

Lastly, Respondents assert that circumstantial evidence has no place in administrative proceedings since the same is applicable only to criminal proceedings.

The motion lacks merit.

Substantial evidence, quantum of proof in administrative cases

Substantial evidence is defined as such amount of relevant evidence which a reasonable mind might accept as adequate to support a conclusion. It is more than a mere scintilla of evidence. The standard of substantial evidence is satisfied when there is reasonable ground to believe, based on the evidence submitted, that the respondent is responsible for the misconduct complained of. It need not be overwhelming or preponderant, as is required in an ordinary civil case, or evidence beyond reasonable doubt, as is required in criminal cases, but the evidence must be enough for a reasonable mind to support a conclusion.[7]

Complainant avers that he was able to present circumstantial evidence to support his claims against Respondents. However, the Supreme Court has reiterated time and again that in administrative proceedings, complainants carry the burden of proving their allegations with substantial evidence.

Complainant accuses Respondents of processing his personal information without authority and for an unauthorized purpose. This Commission reiterates its ruling that, "A mere claim that one has access to personal information is not enough. Without supporting evidence, this claim resides in the realm of supposition."[8] There is nothing in the complaint nor in the Complainant's motion for reconsideration that would find support to show that Respondents' had actual access to the former's personal information.

In spite the fact that Complainant was able to provide this Commission with screen captures of the messages between him and Respondents,

[7] Primo Miro v. Marilyn Mendoza et al., G.R. Nos. 172532 172544-45, 20 November 2013.
[8] Records, pp. 88-95. Penned by Privacy Commissioner Raymund E. Liboro, with Deputy Privacy Commissioners Ivy Patdu and Leandro Aguirre, concurring.

such claim does not of itself show proof that the Respondents accessed data that would show Complainant and his family are indeed in the negative data bank list.

Motion for reconsideration must be sufficient in form and in substance

Rule 37, Section 1 of the Rules of Court provides for the grounds for filing a motion for reconsideration, applicable provision to wit:

XXX XXX

> Within the same period, the aggrieved party may also move for reconsideration upon the grounds that the damages awarded are excessive, that the evidence is insufficient to justify the decision or final order, or that the decision or final order is contrary to law

A motion for reconsideration must satisfy the requirements of Rule 37 of the Rules of Court. A motion for reconsideration that does not comply with those requirements will be treated as *pro forma* intended merely to delay the proceedings.

In his Motion for Reconsideration, Complainant merely reiterates his arguments and assertions. He enumerates in the said motion his verbal communication dated 27 February 2017 with BPI AB Branch Assistant Manager VA, text message exchange with Complainant MFS' mother RS and Respondent RJJ, paragraph 23 of the Joint Counter-Affidavit of Respondents and the fact that he is not a depositor of BDO where Respondent SJJ is connected as circumstantial evidence to prove that Respondents committed a violation under the Data Privacy Act of 2012.

These pieces of evidence have already been presented to this Commission and have been considered, weighed, and resolved adversely to him when the Commission rendered its Decision dated 19 March 2018.

"Under our rules of procedure, a party adversely affected by a decision of a trial court may move for reconsideration thereof on the following

grounds: (a) the damages awarded are excessive; (b) the evidence is insufficient to justify the decision; or (c) the decision is contrary to law... A motion for reconsideration based on the foregoing grounds is deemed pro forma if the same does not specify the findings or conclusions in the judgment which are not supported by the evidence or contrary to law, making express reference to the pertinent evidence or legal provisions."[9]

Complainant clearly failed to specify which finding of the Commission is not supported by evidence or is contrary to law. He merely attempts to assert his claim in his Motion for Reconsideration by rehashing the pieces of evidence previously ruled upon by the Commission.

The motion filed by Complainant is *pro forma* as it is but a reiteration of reasons and arguments previously set forth in his complaint and supplemental complaint and submitted to this Commission. Although Complainant's Motion for Reconsideration had some flesh on its bones, it is nevertheless *pro forma* as it failed to make reference to pieces of evidence on record or provisions of law that is contrary to the decision of this Commission.

In other words, the movant is also required to point out succinctly *why* reconsideration is warranted. The Supreme Court declared that it is not enough that a motion for reconsideration should state what part of the decision is contrary to law or the evidence; it should also point out why it is so. Failure to explain why will render the motion for reconsideration *pro forma*.[10]

A motion must comply with Sections 4 and 5 of Rule 15 of the Rules of Court

Section 32 of NPC Circular 16-04 states that the Rules of Court shall apply in suppletory character, and whenever practicable and convenient. A motion must comply with the requirements set forth under Sections 4 and 5 of Rule 15 of the Rules of Court.

A motion that does not comply with the abovementioned rule is a

[9] PNB v. Hon. Paneda, et. al., G.R. No. 149236, 14 Feb. 2007.
[10] Marikina Valley Development Corporation et. Al. v. Hon. Napoleon Flojo et.al., G.R. No. 11080, 8 December 1995.

worthless piece of paper. The Supreme Court has held time and again, that under the aforementioned rule; mandatory is the requirement in a motion. As a rule, a motion without notice of hearing is considered *pro forma*.[11]

Complainant's motion for reconsideration, being a written motion must comply with the requirements of Rule 15 of the Rules of Court. Hence, the same is considered a mere scrap of paper for failure to comply with the abovementioned rule.

On-site examination under Section 16 of NPC Circular 16-04 is not mandatory

Complainant alleges the failure of this Commission to comply with the rules and procedure of the NPC pertaining to investigation and examination of systems and procedures. He argues that the decision rendered by the Commission solely relied on the pleadings and pieces of evidence submitted by the parties without undergoing the requisite investigation undertaken by the investigating officer.

NPC Circular 16-04 on the Rules of Procedure of the NPC outlines the procedure in filing complaints with the NPC. Complainant specifically raises in issue compliance with Section 16 of NPC Circular 16-04, pertinent portions reproduced below:

> Section 16. Investigation; Examination of Systems and Procedures. – The investigating officer shall investigate the circumstances surrounding the privacy violation or personal data breach. Investigations may include on-site examination of systems and procedures.[12]

This Commission is well-aware of its own Rules of Procedure and has not been remiss in its duties and the service of justice in this case. This Commission hereby outlines the procedure undertaken in the determination of the presence or absence of any violation of the DPA in this case.

On 13 February 2017, Complainant submitted his Complaint Affidavit

[11] Marylou Cabrera v. Felix Ng, G.R. No. 201601, 12 March 2014.
[12] NPC Circular No. 16-04, Rules of Procedure of the National Privacy Commission.

via email. On 20 March 2017, the Commission through its Complaints and Investigation Division (CID) issued an Order to Confer for Discovery directing all parties to appear before the Commission in accordance with Section 13, NPC Circular 16-04. On 15 May 2017, the Discovery Conference Hearing was held at the office of the Commission.

Pursuant to the Discovery Conference Hearing dated 15 May 2017 where both parties agreed that there will be no additional evidence to be presented, the CID issued an Order dated 23 May 2017 for Respondents to file their responsive pleadings and thereafter, the case will be resolved. This is in full compliance with Section 15 of NPC Circular 16-04.

On 5 January 2018, the CID submitted its Investigation Report on NPC Case No. 17-003, on the alleged violation of the DPA of herein respondents. The said Report recommended for the dismissal of the case for lack of merit, *to wit:*

> "A mere claim that one has access to personal information is not enough, it should be proven. From the evidence that were presented before this Commission, the complainant was not able to substantiate his claim that respondent has access to personal information. A supposition cannot in any way be treated as evidence against respondent if the same is not substantiated as this violates fundamental evidentiary rules."[13]

Clearly, the CID had properly conducted a substantive examination and investigation of the case at hand in accordance with its mandate under NPC Circular 16-04 before submitting its Investigation Report. The same Investigation Report was properly considered by this Commission during adjudication in addition to all the pieces of evidence and pleadings submitted by both parties. Allegations made by Complainant Salipot that no investigation of the privacy violation is completely baseless and unfounded.

This Commission thus reminds Complainant that the on-site examination of systems and procedures is discretionary to the investigating officer. The Supreme Court has ruled that, "where the provision reads 'may,'

[13] Investigator's Report dated 5 January 2018, In re: NPC Case No. 17-003 Salipot v Jimenez, p. 6.

this word shows that it is not mandatory but discretionary. It is an auxiliary verb indicating liberty, opportunity, permission and possibility. The use of the word 'may' in a statute denotes that it is directory in nature and generally permissive only."[14] It is the prerogative of the investigating officer whether to conduct an on-site examination and exercising its option to not undergo one does not, in any way, connote a failure to fulfill its duties and responsibilities.

WHEREFORE, for all the foregoing, Complainant's **MOTION FOR RECONSIDERATION** is hereby **DENIED.**

SO ORDERED.

Pasay City.
25 July 2019.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
IVY D. PATDU
Deputy Commissioner

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Commissioner

[14] Demaala v. COA, G.R. No. 199752, Feb. 17, 2015.

Copy Furnished:

MFS
Complainant

RJJ AND SJJ
Respondents

(x) ENFORCEMENT DIVISION
Legal and Enforcement Office

(x) GENERAL RECORDS UNIT

(x) by personal service

ODC,

Complainant,

-versus-

NPC Case No. 17-001
For: Violation of Data Privacy Act of 2012

ODB & EA,

Respondents.

x----------x

RESOLUTION

LIBORO, P.C.

For this Commission's resolution is the Motion for Reconsideration dated 20 December 2017 assailing the Commission's Decision dated 04 December 2017.

The facts are the following:

On 3 February 2017, Complainant filed a formal complaint before this Commission alleging that Respondent ODB, without consent, deducted from his ODB Savings Account his unpaid balance in his AE Credit Card. According to Complainant, his personal data was processed without his consent, thus, a clear violation of the Data Privacy Act of 2012 (DPA).

On 10 April 2017, Respondent ODB filed a Comment[1] stating therein that the complaint should be dismissed due to several grounds. According to Respondent ODB, Complainant committed forum shopping as a prior complaint before the Bangko Sentral ng Pilipinas (BSP) has been lodged. Further, the complaint does not involve any violation of the DPA as no data sharing to a third party took place considering that Respondent ODB is the issuer of Complainant's AE card. Respondent ODB likewise argued that Complainant was legally and contractually bound to pay his credit card bill.

[1] Records, p. 19.

This Commission, in its 04 December 2017 decision[2], ruled that there was no forum shopping in this case as the right asserted by Complainant in his complaint before this Commission is for violation of the DPA while the one in BSP is for violation of the Bank Secrecy Act. This Commission likewise ruled that although Respondent ODB did not commit unauthorized processing of personal information as this was done with Complainant's consent, it was sternly warned as it violated the Principle of Transparency required by law.

In ruling that Respondent ODB violated the principle of transparency, this Commission stressed that the principle of transparency requires personal information controllers (PIC) to ensure that the data subject must always be able to understand how and why his or her personal information is being processed. For this Commission, Respondent ODB did not properly inform Complainant of its ability and intention to set off its legal claim. While this information can be found within the terms and conditions of the credit card agreement signed by complainant, the way the latter's data was to be processed remained opaque and buried in legalese.

This prompted Respondent ODB to file a motion for partial reconsideration with a prayer that a new decision be rendered reversing the ruling that it violated the principle of transparency and its corresponding penalty. Respondent ODB argued that (1) the Civil Code allows for legal set-off or compensation for as long as the elements under Article 1278 and 1279 are complied with and that the law does not require notification before set-off; (2) the logic behind Article 1290 of the Civil Code as to the non-requirement of notice in case of legal compensation is due to the fact that a party may remove the money against which the set-off would be applied once notice is served; and (3) the ruling that it violated the principle of transparency under the DPA run counter to the provisions of the Civil Code on legal compensation which is provided for in the Civil Code and not under the DPA.

We find no merit in the arguments.

[2] Decision dated December 4, 2017 at p.9; Penned by Privacy Commissioner Raymund E. Liboro with Deputy Privacy Commissioner Ivy Patdu concurring.

While this Commission appreciates Respondent ODB's lengthy discussion on the provisions of the Civil Code on legal set-off or compensation, the same is irrelevant as this was not questioned by the Commission nor did this Commission adjudge Respondent ODB to have violated the Civil Code.

In its 04 December 2017[3] Decision, this Commission in fact acknowledged the relationship between a bank and its depositor- that the bank and the data subject are debtors and creditors of each other, and that a bank has the right to set-off the deposits in its hands for payment of a depositor's indebtedness. In other words, the Commission recognized ODB's right to set-off the debt of Complainant from the latter's savings account.

This Commission is likewise well-aware that the Civil Code imposes no obligation on the part of the bank to notify their client prior to the actual legal compensation or set-off. When this Commission ruled that Respondent ODB should have properly informed Complainant of its ability and intention to set off its legal claim, this Commission did not mean Respondent ODB should have notified Complainant prior the actual set-off. Rather, it meant that the credit card terms and conditions of Respondent ODB should have complied with the principle of transparency.

Under Chapter III, Section 11 of the Data Privacy Act of 2012, the processing of personal information shall be allowed, subject to compliance with the requirements of said act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality[4].

Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted, or otherwise processed and as to the extent their personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible

[3] Id., at p. 9.
[4] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector (Data Privacy Act of 2012) Chapter III Section 11.

and easy to understand, and that clear and plain language be used. Further, the principle of transparency concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. It is imperative that natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.[5]

This simply means that companies must state in clear and plain language how they will handle data, for what purpose and by whom. For example, if a company holds data related to children, then the reading level of the content must be accessible for those children[6]. In the same sense that if a company handles data related to a common person then the reading level should be understood by a common person.

Thus, it is imperative that every personal information controller must remember that transparency is a core principle of the DPA. Adherence to this principle is key to "fairness" which is an equally important criterion set for lawful processing of personal data under the DPA.

It is critical in establishing trust and confidence by a business to a customer and should evoke a sense of fairness and a response that encourages more meaningful participation by data subjects. Transparency is necessary to prove organizational accountability to data subjects. Thus, it is not only a legal tool but an instrument for any business to be trusted in today's personal data driven society.

he Data Privacy Act of 2012, which is based on globally adopted privacy principles, introduces a much broader definition for transparency in that it must not only satisfy a legal mandate but more

[5] Recital 39 of the European General Data Protection Regulation (GDPR) available at http://www.privacy-regulation.eu/en/recital-39-GDPR.htm
[6] Fergal McGovern, The GDPR and Plain Language: What you need to do to comply, available at https://www.cmswire.com/digital-experience/the-gdpr-and-plain-language-what-you-need-to-do-to-comply/, Octorber 18, 2017.

importantly, address the expectations of data subjects. The transparency principle as contemplated in the DPA and as differentiated from what the legal profession have become accustomed to, is centered on the reasonable expectations of the user to be informed and must go beyond legal compliance. Privacy Notices and Terms and Conditions (T & C's for brevity) are prime examples where a company can show its transparency to customers. These are essential for legal purposes and a demonstrable proof of organizational accountability to the DPA. However, the presence of Privacy Notices and T & C's alone, does not automatically translate to being transparent. They could be meaningless to data subjects if they are not concise and easy to understand and do not effectively explain the benefits, risks, potential harm, and even pain of data use and the choices and options available to them.

Businesses and their lawyers must realize that personal data processing is now set against a milieu that enunciates the rights to privacy and data protection. They must recognize that legal transparency is different from user-centric transparency. The former may be understandable to legal professionals and appreciated by the legal community while the latter should be understandable to the data subject and satisfy their desire to understand how their personal information will be used. The former addresses their broad legal mandate. The latter fulfills compliance to the DPA. The former uses legalese. The latter uses clear and plain language that is easy to understand. Clearly, they must comprehend that the rules in the processing of personal data have changed.

Admittedly, there is transparency tension whenever legalese cross paths with user expectation. This tension often appears in situations where a power imbalance is present. Power imbalance in data privacy parlance is a condition where meaningful information for the data subject becomes more difficult to obtain especially when the controller, like a bank, hold considerable power over a depositor or customer because they are offering financial services that is vital to the needs of an individual. This situation presents itself in other contexts such as in the health sector where a hospital or a health professional wields considerable power over a patient and even in schools where administrators and teachers exercise a significant degree of control over students.

Incidentally, these industries and sectors have been identified by the Commission to belong to a set of personal information controllers and processor that practice larger-scale and a higher-risk type of processing compared to other PICs and PIPs. They are all contained in Appendix 1 of NPC Circular 17-01 on the Registration of Data Processing Systems and Notification Regarding Automated Decision -Making[7]. A bank and a credit card-issuer like Respondent ODB belongs to one of these sectors. Since it practices a higher–risk type of processing that could lead to situations where a data subject may experience risks or threats or exposed to harm or even pain, it is expected that the data subject should be provided with clear, concise, intelligible, and easy to understand information to guide and provide them with a clear picture and a genuine choice about the use of their personal data.

The NPC is aware of these contexts and seeks to reduce this tension. This is the reason why in these imbalanced conditions, the NPC takes a harder look on how controllers adhere to the principles of personal data processing, namely: transparency, legitimate purpose and proportionality. This Commission stands firm that the onus in resolving this transparency tension between legal mandates and user expectation lies with the business or the personal information controller and its processors. By treating data privacy accountability to their customers more seriously and having the data subject's interest in mind, this tension can be reduced and potential transparency violations to the DPA prevented.

Further, this Commission will never tire in calling out personal information controllers to adhere to the data privacy principles. The Commission understands that it takes effort, creativity and innovation to cure this imbalance and strike that equality between clarity and the data subject desire to understand. It is also conscious not to prescribe disproportionate measures that may be too difficult for the controller to implement. We find amending contracts, privacy notices, and terms and conditions elementary practices that should not take disproportionate efforts to implement. We note that Respondent ODB took the first step in this direction by amending its Terms and Conditions in this case. We note further the effort of Respondent

[7] National Privacy Circular 17-01 Registration of Data Processing and Notifications regarding Automated Decision Making (NPC Circular 17-01- registration) 31 July 2017 available at https://www.privacy.gov.ph/npc-circular-17-01-registration-data-processing-notifications-regarding-automated-decision-making/

ODB to resolve and mitigate this imbalance by delivering a better crafted provision in the T & C on the consequences of default by a card holder in pursuit of their legitimate interest to process personal data. It was a manifestation that they completely agree with our determination of the shortcomings of their original Terms and Conditions in providing the clarity sought by the complainant.

In this case, while the terms and conditions of AE Credit Card Card was signed by Complainant, the way the latter's data was to be processed for purposes of legal compensation or set off remained opaque and buried in legalese. The terms and conditions did little to provide Complainant transparency regarding the use of his data.

The Civil Code provides for the elements in order for a legal compensation to take place, however, nothing stops Respondent ODB or any personal information controller from setting out its terms and conditions in a clear, plain, and concise language. This is in fact what Respondent ODB did when it made some changes in its terms and conditions governing the issuance and use of the AE Credit Cards. In the version signed by Complainant, Paragraph 19 (b) of the Terms and Conditions for issuance and use of the AE credit card states:

XXX XXX

> b.) All monies, securities, and things of value that are now or hereafter be in the hands of the ISSUER or any of its related companies or both, on deposit or otherwise to the credit of or belonging to the CARDMEMBER, shall be deemed assigned to the ISSUER effective upon the occurrence of default. The ISSUER is also authorized, without need of notice to the CARDMEMBER to automatically debit his/her deposit account for such amounts may be sufficient to cover full payment of the outstanding balance, or to sell at public or private sale such securities or things of value owned by CARDMEMBER and then to apply the proceeds of such sale to any outstanding obligation of CARDMEMER;
>
> c.) Any Funds of the CARDMEMBER that may now or later be in the hands of the ISSUER or any of its Related Companies will be

applied and set off against any amounts due and payable on the CARDMEMBER's CARD account.

CARDMEMBER hereby gives ISSUER and its Related Companies full power and authority to implement the foregoing acts[8].

XXX XXX

On the other hand, Respondent ODB's new terms and conditions as provided for the use of AE credit card pertaining to consequences of default states:

XXX XXX

ISSUER may, and is hereby authorized by the CARDMEMBER to set off as full or partial payment, and/or withhold, to the extent permitted by law, at ISSUER's option and without need of prior notice, all monies, funds, and/or proceeds of securities, investments or receivables which may come into the possession or control of the ISSUER and/or its Related Companies, to apply the same in satisfying any or all obligations of the CARDMEMBER to the ISSUER, whether left with them for safekeeping or otherwise, or coming into any of their hands in any way, to settle any and all obligations of the CARDMEMBER to the ISSUER. CARDMEMBER irrevocably authorizes ISSUER and/or its Related Companies to debit such amounts as may be necessary to implement this provision from any of the CARDMEMBER's accounts with the ISSUER and/or its Related Companies, immediately after which due notice shall be sent to the CARDMEMBER. In addition, all such properties, receivables or securities in the possession or control of the ISSUER and/or its Related Companies are hereby ceded, transferred and conveyed by way of assignment unto ISSUER in order that the same may be used to satisfy any and all obligations of the CARDMEMBER to the ISSUER in accordance with this provision. For such purpose, and to effectively carry out the powers herein granted, CARDMEMBER hereby unconditionally or irrevocably names and constitutes ISSUER and/or its Related Companies to be his/her true and lawful attorney-

[8] Terms and Conditions for issuance and use of the AE Credit Cards available at https://www.odb.com.ph/sites/default/files/pdf/AE-TCS.pdf / October 2013

> in-fact, with full power of substitution, to do or cause to be done any and all acts that are necessary to carry out the purposes of this paragraph, including the power to sell in accordance with law, based on zonal value or fair market value for real or personal properties, respectively, without the need for any further notice, demand or deed, and to apply the proceeds of the sale to the satisfaction of the CARDMEMBER's obligations to the ISSUER. The appointment of ISSUER and/or its Related Companies is coupled with interest and is, therefore, irrevocable until any and all obligations to the ISSUER are fully settled. For the foregoing purposes, the CARDMEMBER hereby waives his/her rights in favor of the ISSUER and/or its Related Companies under Republic Act 1405 (The Bank Secrecy Act of 1955), as amended, Section 55 of Republic Act 8791 (The General Banking Law of 2000), as amended, Republic Act 6426 (Foreign Currency Deposit Act of the Philippines of 1974), as amended, Republic Act 10173 (Data Privacy Act of 2012) and other laws/regulations, including all subsequent amendments or supplements thereto, relative to the confidentiality or secrecy of bank deposits/accounts, placements, investments and similar or related assets in the custody of the ISSUER and/or its Related Companies. CARDMEMBER shall hold ISSUER and/or its Related Companies, their directors, officers, employees, representatives and agents, free and harmless from any liability arising from ISSUER's, and/or its Related Companies' exercise of their remedies and authorities hereunder, or from any action taken by ISSUER and/or its Related Companies on the basis of and within the framework of the foregoing appointment[9].
>
> XXX XXX

The very fact that Respondent ODB made changes in its terms and conditions is at the very least an acknowledgment of the lack of full transparency in the terms and conditions signed by Complainant. The dispositive portion of the 04 December 2017 decision states that Respondent ODB should SUBMIT their privacy notices and consent form that adequately informs the data subject of his rights within fifteen (15) days from receipt of the Decision. This Commission did not ORDER Respondent ODB to change its privacy notices and consent form. The Commission merely asked Respondent ODB to SUBMIT

[9] Terms and Conditions for issuance and use of the AE Credit Cards available at https://www.odb.com.ph/sites/default/files/pdf/AE-TCS.pdf / March 2019

privacy notices and consent form that adequately informs that data subject of his rights. Thus, if Respondent ODB truly believed that it did not violate the principle of transparency as set forth in its motion for partial reconsideration, it could have simply submitted the terms and conditions signed by Complainant. .

Nevertheless, this Commission finds this an appropriate response by Respondent-ODB to make its Terms and Conditions more understandable to the subject and we expect the business to benefit from this action. This simple step that could be complemented by other accountability measures to be taken by Respondent-ODB, could help mitigate potential tension between them as data controller and the data subjects like the complainant, in the future. This was a response that proves better allocation of time, effort and resources by Respondent-ODB to address age-old transparency matters with fairness to the data subject in mind.

Therefore, this Commission stands by its decision that Respondent ODB violated the principle of transparency. To reverse the same would be to frustrate the operationalizing of the Data Privacy Act of 2012. With the passage of this important law, personal information controllers should put themselves in the shoes of its stakeholders, clients, or customers to ensure that the language used in privacy notices, consent forms, or terms and conditions is at the latter's level. Personal information controllers must be mindful of their clientele and should no longer rely on privacy policies or terms and conditions written in legalese.

This Commission believes that conforming to the principle of transparency will both benefit Respondent ODB's clients and its business.

WHEREFORE, for all the foregoing, Respondent ODB's **MOTION FOR RECONSIDERATION** is hereby **DENIED.**

SO ORDERED.

Pasay City, Philippines.
9 August 2019

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

CONCUR:

(Sgd.)
IVY D. PATDU
Deputy Commissioner

DISSENTING OPINION

AGUIRRE, D.P.C.

This case raises for the Commission's consideration the issue of whether respondent ODB violated the principle of transparency under RA 10173 or the Data Privacy Act of 2012 ("DPA")[10] by not informing complainant ODC when it opted to exercise its right to debit from his ODB Savings Account the outstanding balance from his AE Credit Card.

In its 04 December 2017 Decision ("Decision"),[11] the Commission held that ODB violated the principle of transparency, thus:

> The respondent should have properly informed the complainant of its ability and intention to set off its legal claim. Even though the information required can be found within the terms and conditions of the credit card agreement signed by the complainant, the way the complainant's data was to be processed remained opaque and buried in legalese. What is wanting from the Respondent is the transparency expected from banks when dealing with the public.[12]

[10] "An Act Protecting Individual Personal Information In Information And Communications Systems In The Government And The Private Sector, Creating For This Purpose A National Privacy Commission, And For Other Purposes."
[11] ODC v. ODB and AE, NPC Case No. 17-001, 04 December 2017.
[12] Ibid., at p. 9.

Not satisfied with the Decision, respondent ODB filed their Motion for Partial Reconsideration praying that this Commission reverse its finding that it violated the principle of transparency. As summarized by the majority in their Resolution:

> [R]espondent ODB argued that (1) the Civil Code allows for legal set-off or compensation for as long as the elements under Article 1278 and 1279 are complied with and that the law does not require notification before set-off; (2) the logic behind Article 1290 of the Civil Code as to the non-requirement of notice in case of legal compensation is due to the fact that a party may remove the money against which the set-off would be applied once notice is served; and (3) the ruling that it violated the principle of transparency under the DPA run counter to the provisions of the Civil Code on legal compensation which is provided for in the Civil Code and not under the DPA.[13]

In denying ODB's Motion for Partial Reconsideration, the majority dismissed ODB's discussion on the civil law concept of legal set-off or compensation saying that "the same is irrelevant as this was not questioned by the Commission nor did this Commission adjudge respondent ODB to have violated the Civil Code."[14] The majority then went on to qualify its previous ruling despite the clear implication of the text, saying:

> When this Commission ruled that Respondent ODB should have properly informed Complainant of its ability and intention to set off its legal claim, this Commission did not mean Respondent ODB should have notified Complainant prior [sic] the actual set-off. Rather, it meant that the credit card terms and conditions of Respondent ODB should have complied with the principle of transparency.[15]

Expounding on the general data privacy principle of transparency, the majority further stated:

[13] Resolution, NPC Case No. 17-001, pp. 2-3.
[14] Ibid., at p. 3.
[15] Id.

> The transparency principle as contemplated in the DPA and as differentiated from what the legal profession have become accustomed to, is centered on the reasonable expectations of the user to be informed and must go beyond legal compliance. Privacy Notices and Terms and Conditions (T&C's for brevity) are prime examples where a company can show its transparency to customers. These are essential for legal purposes and a demonstrable proof of organizational accountability to the DPA. However, the presence of Privacy Notices and T&C's alone, does not automatically translate to being transparent. They could be meaningless to data subjects if they are not concise and easy to understand and do not effectively explain the benefits, risks, potential harm, and even pain of data use and the choices and options available to them.
>
> Businesses and their lawyers must realize that personal data processing is now set against a milieu that enunciates the rights to privacy and data protection. They must recognize that legal transparency is different from user-centric transparency. The former may be understandable to legal professionals and appreciated by the legal community while the latter should be understandable to the data subject and satisfy their desire to understand how their personal information will be used. The former addresses their broad legal mandate. The latter fulfills compliance to the DPA. The former uses legalese. The latter uses clear and plain language that is easy to understand. Clearly, they must comprehend that the rules in the processing of personal data have changed.[16]

The principle of transparency is indeed, as the majority has put it, "critical in establishing trust and confidence by a business to a customer and should evoke a sense of fairness and a response that encourages more meaningful participation by data subjects."[17] There is no question about that. As to how the majority interpreted and applied it to this case, however, I respectfully dissent.

In saying that respondent ODB's discussion on the civil law concept of legal set-off is irrelevant, the majority overlooks the significance of respondent ODB's arguments. First, it bears stressing that the Commission is not tasked with and has no authority to examine the

[16] Ibid., at p. 5.
[17] Ibid., at p. 4.

propriety of the legal set-off and determine whether respondent ODB violated the Civil Code. That is a matter for the regular courts to decide, not the Commission. Second, ODB's discussion, premised on the clear implication of this Commission's Decision stating that "respondent should have properly informed the complainant of its **ability and intention to set off** its legal claim,"[18] seeks to show that the matter of the legal set-off is governed by a specific provision of law and, as such, its validity cannot be attacked collaterally using the Data Privacy Act.

In their Motion for Partial Reconsideration, respondent ODB argues:

> To allow the data subject/complainant to question the set-off provision, to which he gave his consent, when he accepted his ODB AMEX Card (see Annex "1" hereof), by ruling that ODB violated the principle of transparency under the Data Privacy Act, runs counter to the provisions of the Civil Code on legal compensation / set-off and the elements required to effect said legal compensation / set-off. It must be noted that the matter of set-off / compensation is governed by a different law, i.e. the Civil Code of the Philippines, and not the Data Privacy Act.[19]

In disregarding the Civil Code provisions on legal set-off and insisting that the DPA is an overarching law the provisions of which supersedes the requirements of other laws governing specific circumstances, the majority is pushing the NPC to play the role of an overbearing regulator. The majority puts the Commission in a position where it acts without any sense of the delicate balance it still has to play in ushering data privacy as a new cog in already functioning mechanisms. Such a position paves the way for creative litigants to weaponize the DPA for purposes not germane to the intent of the law.

The supposed violation of the principle of transparency was neither raised as an issue in the Complaint nor is it supported by substantial evidence.

[18] Ibid., at p. 9. Emphasis supplied.
[19] Motion for Partial Reconsideration dated 19 December 2017, p. 6.

The Complaint hinges on the following assertions of the complainant:

> AE is a credit card company while ODB is in banking. I did not sign any authority for AE to debit my ODB account. Also, the business of AE was only acquired by the ODB group and thus, it is impossible for me to have signed any authority to debit.[20]

As correctly summarized by respondent ODB:

> What the date subject / complainant accused the Bank of is the supposed violation of the Data Privacy Act, in that he was under the mistaken notion that AE and ODB are different entities, and that the sharing of his deposit information is a violation of said law. He only claimed that he did not sign any agreement to debit his account or to auto-debit his account.[21]

In its Decision dated 04 December 2017, the Commission already ruled on the issue of consent stating that the complainant voluntarily gave his consent when he agreed to and signed the terms and conditions.[22] On the issue of data sharing, the Commission also held that since ODB and AE are one and the same entity in this jurisdiction, "the information was not shared with any affiliate or subsidiary of ODB [and as such] there is no need to further discuss consent of the data subject and the absence of a data sharing agreement…"[23]

Since the complainant did not move for the reconsideration of these factual findings of the Commission, these findings are final as to him. Considering also that the Complaint was based on only those two issues, that should have been the end of it. Instead, the majority found respondent ODB to have violated the principle of transparency and gave it a stern warning.

In discussing the substantial evidence requirement for administrative agencies in the exercise of their quasi-judicial powers, the Supreme Court has repeatedly held that "complainants bear the burden of proving the allegations in their complaints by substantial evidence.

[20] Complainant's email complaint to the National Privacy Commission dated 26 January 2017.
[21] Motion for Partial Reconsideration dated 19 December 2017, pp. 5 – 6.
[22] Decision, NPC Case No. 17-001, 04 December 2017, p. 8.
[23] Ibid., at p. 9.

If they fail to show in a satisfactory manner the facts upon which their claims are based, the respondents are not obliged to prove their exception or defense."[24]

In this case, the majority found a supposed violation that was not only never alleged by the complainant but, more importantly, not supported by any evidence on record, much less substantial evidence. Aside from the complainant's bare assertion that he "did not sign any authority for AE to debit my ODB account [and that he] did not enroll said ODB account to any auto-debit facility,"[25] there is nothing else on record to support the majority's finding that ODB violated the principle of transparency.

Denial, without more, cannot rise to the level of substantial evidence. This is all the more true in this case since the very thing the complainant is denying has already been decided by the Commission in favor of the respondent.

To allow, as the majority does in this case, the mere claim of a data subject of supposedly not knowing of or understanding the effects of the contract they signed to result in a violation of the Data Privacy Act would cause great uncertainty in existing contracts with legitimate ends.

Requirements of the Principle of Transparency

The Resolution of the majority perpetuates the misconception that using legal language violates the principle of transparency

While the Data Privacy Act of 2012 does not define "transparency," the Implementing Rules and Regulations provide:

> 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

[24] Re: Letter of Lucena Ofendo Reyes Alleging Illicit Activities Of A Certain Atty. Cajayon Involving Cases In The Court Of Appeals, Cagayan De Oro City, A.M. No. 16-12-03-CA, 06 June 2017.
[25] ODC Affidavit dated 03 February 2017.

> 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.[26]

Contrary to the majority's condemnation of the use of legal language in privacy notices, consent forms, or terms and conditions in its exposition on the difference between legal transparency and user-centric transparency, the requirement to use "clear and plain language" does not prohibit the use of legal language. The principle of transparency does not also require personal information controllers to use layman's terms to replace technical words and concepts at the risk of not capturing the complex concepts they represent.

In explaining the "clear and plain language" requirement in the European Union's ("EU") General Data Protection Regulation ("GDPR"), the independent European working party that dealt with issues relating to the protection of privacy and personal data known as the Article 29 Working Party explained in its Guidelines on Transparency ("Guidelines"):

> The requirement for clear and plain language means that information should be provided in as simple a manner as possible, avoiding complex sentence and language structures. The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear.[27]

It further added that in structuring sentences, language qualifiers such as "may", "might", "some", "often" and "possible" should be avoided.[28]

Aside from the "clear and plain language" requirement, another element of the principle of transparency is that the "information and communication relating to the processing of personal data should be easy to access and understand."[29] To help us understand the meaning of "easy to access and understand," the interpretation of similar language in the GDPR is useful.

---

[26] IRR, Sec. 18.
[27] Guidelines on transparency under Regulation 2016/679 of the Article 29 Working Party, 11 April 2018, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.
[28] Ibid.
[29] IRR, Sec. 18.

Under the GDPR, it is required that the information or communication to be provided to data subjects should be "concise, transparent, intelligible and easily accessible."[30] Although this specific language did not find its way into either the Data Privacy Act or its IRR, it is nevertheless helpful to consider given that the principle of transparency was adopted from the European Commission's Directive 95/46/EC, the predecessor of the GDPR.

In the Article 29 Working Party's Guidelines, which has since been endorsed by the European Data Protection Board,[31] they elaborated on the meaning of each of these additional elements, thus:

> 8. The requirement that the provision of information to, and communication with, data subjects is done in a **'concise and transparent'** manner means that data controllers should present the information/ communication efficiently and succinctly in order to avoid information fatigue. This information should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use…
>
> 9. The requirement that information is **'intelligible'** means that it should be understood by an average member of the intended audience. Intelligibility is closely linked to the requirement to use clear and plain language. An accountable data controller will have knowledge about the people they collect information about and it can use this knowledge to determine what that audience would likely understand. For example, a controller collecting the personal data of working professionals can assume its audience has a higher level of understanding than a controller that obtains the personal data of children.
>
> xxx
>
> 11. The **'easily accessible'** element means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question…[32]

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 27 April 2016.

[31] European Data Protection Board Endorsement 1/2018, 25 May 2018, available at https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0. pdf.

The European Data Protection Board, composed of the data protection authorities of the Member States and the European Data Protection Supervisor, is an independent body with legal personality responsible for ensuring the consistent application of the General Data Protection Regulation.

[32] Guidelines on Transparency under Regulation 2016/679 of the Article 29 Working Party, 11 April 2018, available at https://ec.europa.eu/newsroom/article29/item- detail.cfm?item_id=622227. Emphasis and underscoring supplied.

i. What information is required to be disclosed to data subjects?

In our jurisdiction, we generally recognize the relationship between the credit card issuer and the credit card holder as a contractual one that is governed by the terms and conditions found in the card membership agreement.[33] Such terms and conditions constitute the law between the parties.[34]

To determine the content of the privacy-related information that should be provided to data subjects, we look at the prescribed information covered by the data subject's right to information:

(1) whether personal information pertaining to him shall be, are being, or have been processed;

(2) a description of the personal information to be entered into the system;

(3) scope and method of the personal information processing;

(4) the recipients or classes of recipient to whom they are or may be disclosed;

(5) methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;

(6) the identity and contact details of the personal information controller or its representative;

(7) the period for which the information will be stored; and

(8) the existence of their rights, i.e. to access, correction, as well as the right to lodge a complaint before the Commission.[35]

Following the abovementioned Guidelines on Transparency, the required information should be distinguished, from other non-privacy related information such as contractual provisions or general terms of use.[36] Notably, the list of required information under Section 16

[33] Pantaleon v. American Express International, Inc (2010). GR No. 174269.
[34] BPI Express Card Corporation v. Armovit (2014). GR No. 163654.
[35] Section 16(b), RA 10173.
[36] Guidelines on Transparency under Regulation 2016/679 of the Article 29 Working Party, 11 April 2018, available at

of the DPA does not include legal remedies provided under existing laws, such as the right to set-off under the law on obligations and contracts in the Civil Code that is subject of the present case. As such, the subject provision on the "Consequences of Default" is not one of those contemplated by and intended to be covered by the principle of transparency. *Expressio unius est exlusio alterius.*

Given this, the language for provisions that encompass legal concepts should not be overly burdened with unreasonable impositions of simplification on the supposed reliance on the transparency principle.

ii. What is the required manner of disclosing the required information to data subjects?

Even assuming that it is one of those provisions that is required to be disclosed to data subjects, the other question that needs to be answered is whether the information provided is "intelligible" such that it can be understood by an average member of the intended audience.

At the outset, it should be clarified that compliance with the principle of transparency does not require the personal information controller to determine if the data subject actually understood how their information will be processed. What is required is whether the information provided by the personal information controller, both in terms of the content and manner in which it was provided, would have allowed the data subject to understand if they wanted to.

Elaborating on this, the majority points out in its Resolution, "if a company holds data related to children, then the reading level of the content must be accessible for those children. In the same sense that if a company handles data related to a common person then the reading level should be understood by a common person."[37]

While the majority's statements in its Resolution are not incorrect, they fail to consider that the principle of transparency is context-specific. Simply stating "common person" is not enough because the "common person" for a simple transaction may be different from the "common

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[37] Resolution, NPC Case No. 17-001, p. 4, citing Fergal McGovern, The GDPR and Plain Language: What you need to do to comply, available at https://www.cmswire.com/digital-experience/the-gdpr-and-plain-language-what-you-need-to-do-to-comply/

person" for a complicated transaction. As the Guidelines explain, the important thing to consider is the "**average member of the intended audience…** [such that] a controller collecting the personal data of working professionals can assume its audience has a higher level of understanding than a controller that obtains the personal data of children."[38]

The 2013 version of the AE Terms and Conditions provide:

> 19. **Consequences of Default.** The following shall be consequences of default, whether singly, concurrently, or successively:
>
> xxx
>
> b) All monies, securities, and things of value that are now or may hereafter be in the hands of the ISSUER or any of its Related Companies or both, on deposit or otherwise to the credit of or belonging to the CARDMEMBER, shall be deemed assigned to the ISSUER effective upon the occurrence of default. **The ISSUER is also authorized, without need of notice to the CARDMEMBER, to automatically debit his/her deposit account** for such amount as may be sufficient to cover full payment of the outstanding balance, or to sell at public or private sale such securities or things of value owned by CARDMEMBER and then to apply the proceeds of such sale to any outstanding obligation of CARDMEMBER;
>
> c) Any funds of the CARDMEMBER that may now or later be in the hands of the ISSUER or any of its Related Companies will be **applied and set off against any amounts due and payable** on the CARDMEMBER's CARD account.[39]

From the earlier discussion on the requirement of "clear and plain language," there is no basis to find the 2013 version as violative of the transparency principle. The information provided is definitive; it does not leave room for different interpretations. The sentences do not contain language qualifiers such as "may", "might", or "possibly." Its real intent is evident, by using terms such as "automatically debit", "apply", and "set off." The heading itself, "Consequences of Default" indicates that it talks about the remedial measures that the respondent

[38] Guidelines on Transparency under Regulation 2016/679 of the Article 29 Working Party, 11 April 2018, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227. Emphasis supplied.
[39] Respondent ODB's Comment dated 05 April 2017, Annex "8". Emphasis supplied.

bank may resort to. It is neither ambiguous nor overly broad. The language is that which is typically found in contracts involving credit transactions of similar nature.

Aside from this, the complainant, by his own admission, has been a cardholder of AE Platinum since 2005 and a depositor of ODB since 2014.[40] From the website of AE, it can be seen that complainant's AE card is the highest tier non-dollar charge credit card offered by AE and requires a minimum annual income of Php 1,800,000.00 in order to qualify.[41] It is reasonable to expect that average member of the intended audience, i.e. persons with at least that level of income among others, would have a sufficient level of understanding to appreciate such terms as "default," "credit," "debit," "obligation," "deposit account" as well as the other information being provided to them in the AE Credit Card Terms and Conditions.

The change in the Terms and Conditions is not an acknowledgment of a lack of transparency in the Terms and Conditions signed by the complainant.

In an effort to provide additional justification for respondent ODB's supposed violation of the transparency principle, the majority examined two (2) versions of AE Credit Card's Terms and Conditions: the 2013 version, as attached by respondent ODB, and the 2019 version, as found in the ODB website.[42] Finding variations in the provisions, the majority stated that "the very fact that Respondent ODB made changes in its terms and conditions is at the very least an acknowledgment of the lack of full transparency in the terms and conditions signed by [the] complainant."[43] Although this analysis by the majority is appreciated, I cannot agree with their conclusion after comparing the two provisions.

[40] Complainant's email complaint to the National Privacy Commission dated 26 January 2017.
[41] See https://www.americanexpress.com/ph/network/product-landing/membership-rewards.html.
[42] Terms and Conditions for issuance and use of the AE Credit Cards available at https://www.odb.com/ph/sites/default/files/pdf/AE-TCS.pdf/March2019
[43] Resolution, NPC Case No. 17-001, p. 9.

2013 Version	2019 Version
19. **Consequences of Default.** The following shall be consequences of default, whether singly, concurrently, or successively: xxx b) All monies, securities, and things of value that are now or may hereafter be in the hands of the ISSUER or any of its Related Companies or both, on deposit or otherwise to the credit of or belonging to the CARDMEMBER, shall be deemed assigned to the ISSUER effective upon the occurrence of default. **The ISSUER is also authorized, without need of notice to the CARDMEMBER, to automatically debit his/her deposit account** for such amount as may be sufficient to cover full payment of the outstanding balance, or to sell at public or private sale such securities or things of value owned by CARDMEMBER and then to apply the proceeds of such sale to any outstanding obligation of CARDMEMBER; c) Any funds of the CARDMEMBER that may now or later be in the hands of the ISSUER or any of its Related Companies will be **applied and set off against any amounts due and payable** on the CARDMEMBER's CARD account.[44]	20. **Consequences of Default.** The following shall be the consequences of default, whether singly, concurrently, or successively: xxx b) "the ISSUER may, and is hereby **authorized by the CARDMEMBER to set off** as full or partial payment, and/or withhold, to the extent permitted by law, at ISSUER's option and without need of prior notice all the monies, funds, and/or proceeds of securities, investments or receivables which may come into the possession or control of the ISSUER and/or its Related Companies, to apply the same in satisfying any or all obligations of the CARDMEMBER to the ISSUER, whether left with them for safekeeping or otherwise, or coming into any of their hands in any way, to settle any and all obligations of the CARDMEMBER to the ISSUER. **CARDMEMBER irrevocably authorizes ISSUER and/or its Related Companies to debit such amounts as may be necessary to implement this provision from any of the CARDMEMBER's accounts with the ISSUER and/or its Related Companies, immediately after which due notice shall be sent to the CARDMEMBER.** In addition, all such properties, receivables or securities in the possession or control of the ISSUER and/or its Related Companies are hereby ceded, transferred and conveyed by way of assignment unto ISSUER in order that the same may be used to satisfy any and all obligations of the CARDMEMBER to the ISSUER in accordance with this provision. For such purpose, and to effectively carry out the powers granted herein, CARDMEMBER hereby unconditionally or irrevocably names and constitutes ISSUER and/or its Related Companies to be his/her true and lawful attorney-in-fact xxx **For the foregoing purposes, the CARDMEMBER hereby waives his/her rights in favor of the ISSUER and/or its Related Companies under…Republic Act 10173 (Data Privacy Act of 2012)** and other laws/regulations, including all subsequent amendments or supplements thereto, relative to the confidentiality or secrecy of bank deposits, accounts, placements, investments and similar or related assets in the custody of the ISSUER and/or its Related Companies.[45]

[44] Respondent ODB's Comment dated 05 April 2017, Annex "8". Emphasis supplied.
[45] Terms and Conditions for issuance and use of the AE Credit Cards available at https://www.odb.com.ph/ph/sites/default/files/pdf/AE-TCS.pdf/March2019. Emphasis supplied.

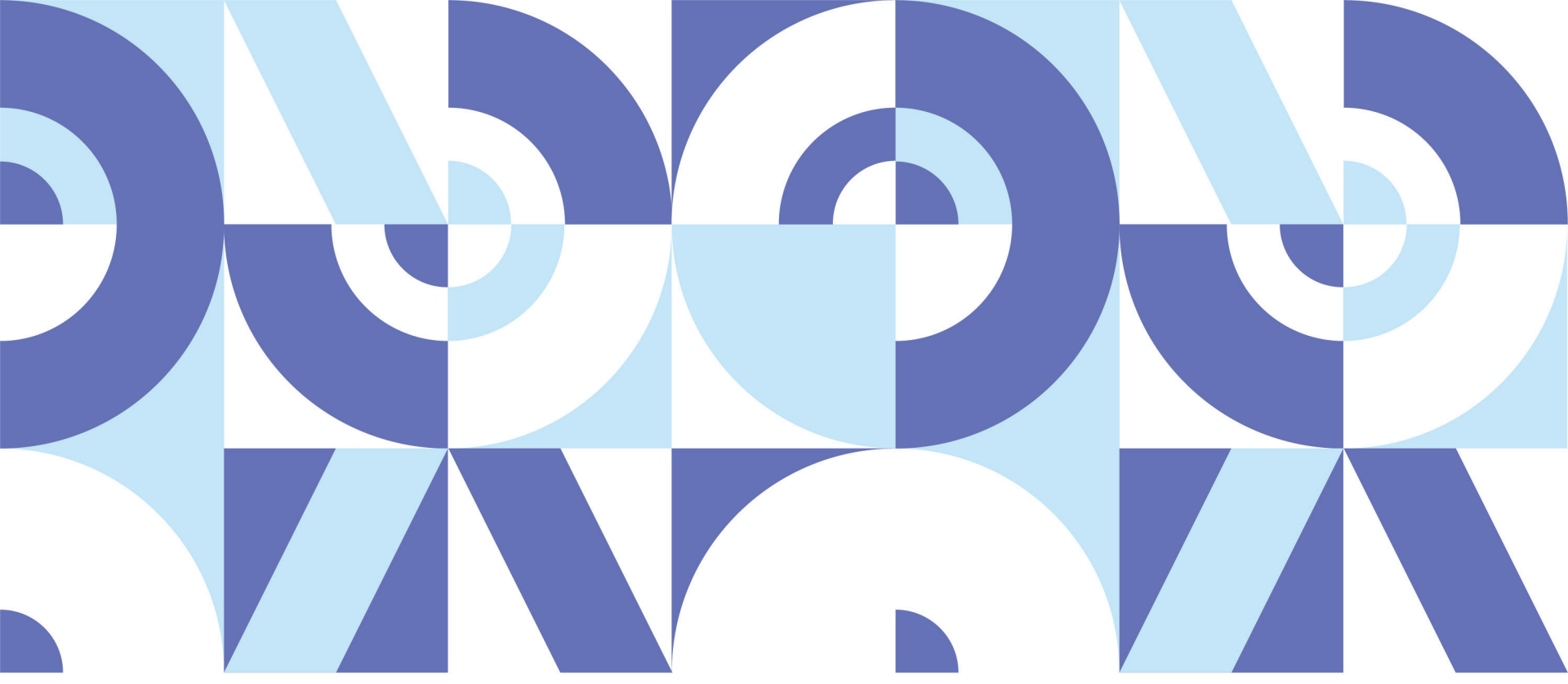
Contrary to how the majority finds the 2019 version as an "appropriate response by Respondent-BDO to make its Terms and Conditions more understandable to the subject [sic],"[46] even a cursory reading of the two versions would show that they are substantially the same on all the important points except that subsections (b) and (c) in the 2013 version have now been merged into subsection (b) in the 2019 version. The terms "debit," "apply," "set-off," and other legal terms are still used such that it can hardly be said that the 2019 version has already cured the supposed issues the majority found in the previous version.

In fact, rather than being the "appropriate response" the majority claims it to be, the 2019 version is more problematic for data subjects since it contains an improper waiver of rights under the DPA. Surely a waiver of the fundamental human right to informational privacy enshrined in the DPA cannot be said to have "fairness to the data subject in mind" as the majority claims.

In light of all these considerations, I vote to **GRANT** the Motion for Partial Reconsideration based on a finding that there was no violation of the principle of transparency.

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

[46] Resolution, NPC Case No. 17-001, p. 10.



ORDER

IN RE: GRAB PHILIPPINES' [1] ROLL-OUT OF THE PASSENGER SELFIE VERIFICATION; [2] PILOT TEST OF THE IN-VEHICLE AUDIO RECORDING; AND [3] PILOT TEST OF THE IN-VEHICLE VIDEO RECORDING

NPC CC 20-001

x----------x

CEASE AND DESIST ORDER

NAGA, D.P.C.:

This resolves the Recommendation of this Commission's Data Security and Compliance Office ("DASCO") to issue a Cease and Desist Order[1] directing Grab Philippines ("Grab PH") to suspend the pilot test and any plans to roll out their three (3) new data processing systems, namely: Passenger Selfie Verification, In-Vehicle Audio Recording, and In-Vehicle Video Recording (collectively referred to as "three (3) new data processing systems") due to the discovered deficiencies that may endanger the privacy rights of the riding public.

FACTS

On 15 January 2020, a conference was held between the Commission and Grab PH to discuss the features, data privacy measures, and other details of its three (3) new data processing systems. During the said meeting, Grab submitted the following documents: Privacy Impact Assessment of the three (3) new data processing systems, Personal Data Review, Grab PH Data Protection Handbook, and Powerpoint presentation on the three (3) new data processing systems.

Based on the submitted documents of Grab PH and their statements during the conference, the features of the three (3) new data processing systems can be described in this wise:

1. Passenger Selfie Verification is a process of identity verification adopted by Grab PH wherein passengers are prompted through the Grab application to follow the onscreen instructions, ultimately requiring them to take a

[1] Dated 31 January 2020

selfie. This is one of the modes by which Grab verifies the identity of its passenger.

According to Grab PH, the selfie generated will be used solely for verification and will not be shared with the driver. However, the data can also be provided as evidence in the event of disputes, conflicts, and or complaints.

During the meeting, Grab PH said that the retention period of the selfies is seven (7) years.

2. The In-vehicle Audio Recording is the process by which conversations transpiring inside the vehicle during the trip are being documented by audio-recording via the driver's Grab application. It is currently implemented as a pilot test that will run for two (2) weeks among ninety (90) Grab PHdrivers.

   The recording starts from the moment the passenger is picked up until drop off at the pinned destination. According to Grab PH, the audio recording is encrypted with AES 256 bits key and asymmetric encryption with a seven (7) day retention period.

3. The In-vehicle Video Recording is the process through which Grab PH documents the passenger and driver experience during the trip with the use of an in-vehicle video camera powered by the electrical system of the vehicle.

   It is currently implemented as a pilot test that will run for six (6) weeks among ninety (90) Grab PH drivers.

For the In-Vehicle Audio and In-Vehicle Video Recording, Grab PH said that these systems are being piloted to promote the safety of both the drivers and passengers.

After reviewing all the submitted documents of Grab PH and the representations they made during the 15 January 2020 conference,

DASCO issued a Notice of Deficiencies to Grab PH in relation to its three (3) new data processing systems, to wit:

1. In June 2019, it was estimated that **one of six Filipinos has installed a Grab app**, all of whom could be potentially affected by risks arising from the aforementioned processing. Despite the possible impact, **Grab did not sufficiently identify and assess the risks posed by its data processing systems to the rights and freedoms of data subjects.** Its PIA methodology states that "The impact to Grab when a risk becomes reality is assessed under the four major categories of operational downtime, people, reputational damage and financial loss", clearly indicating that only the risks faced by the company were taken into account. The sole risk that Grab PH included in its PIA was "regulation action being taken for lack of consent and notification to individuals". **(Emphasis supplied)**

   As a result, the controls identified only corresponded to the said risk. **The PIA did not include controls to secure the photo, audio and video recording from unauthorized disclosure or access, accidental or unlawful destruction, loss, and alteration.** These should have been considered in the PIA given the sensitivity of the data, the use of third party providers, and the fact that Grab collects several other personal data through other systems (e.g. user profile creation/registration, linking Grab account to social media accounts, GrabPay, etc.). Both factors make Grab and its systems a very attractive target of hacking attacks. **(Emphasis supplied)**

2. During the meeting, Grab explained that the photo, audio and video files will be provided to authorities if they get a verified police request after an incident. **According to Grab, the audio and video files will be used as evidence in the event of dispute, conflict, or complaint.** The video recording system will also enable Grab employees to monitor the situation live from the Grab Office and take photos of what is happening inside the vehicle, once the driver prompts the

office through the emergency button. **(Emphasis supplied)**

However, none of these were reflected in its privacy notice (Grabchat message and email) and policy. Affected data subjects only received Grabchat messages and emails that stated a generic purpose—that the processing was "for safety and security purposes", "to improve passenger and driver safety", and "to make riding safer". A link to the second layer information was included in the Grabchat messages, which was supposed to provide the complete and specific details about the processing. The link, however, leads the passenger to Grab's Privacy Policy which only provides a high-level view of all the processing systems of Grab. **(Emphasis supplied)**

3. **Grab did not communicate the basis it uses for the processing to be considered lawful.** It should have indicated if the processing was **pursuant to a regulatory requirement** of another authority or if it is **based on the legitimate interests** of the company and its customers. If the processing was based on the latter, Grab could have cited documented in-vehicle incidents and other related information in the PIA, which may serve as evidence for the existence of a legitimate interest. **(Emphasis supplied)**

4. The **submitted documents were not able to show if the processing was proportional to its purpose.** The PIA lacked the information on whether the benefits of the processing systems were found to outweigh the risks. It had no information if Grab assessed that the passenger selfie verification and the in-vehicle audio and video recording were indeed the best alternatives among all identified means to achieve the underlying purpose. Likewise, it was unclear if Grab assessed whether the personal data it collects from these processing systems are not excessive. **(Emphasis supplied)**

5. **Having the option to withdraw consent was one of the**

controls included in the PIA for the pilot test of the in-vehicle audio and video recording. However, the mechanism to exercise such right during and after the ride was not spelled out in the Grabchat message. It was also not specified if and how the processing will stop if the passenger withdraws consent during the ride, considering that the tech specs prevent the driver from having any control over the device. Further, it was unclear how the consent mechanism will work if Grab decides to roll out the system which may necessitate that all Grab cars be equipped with the recording device. **(Emphasis supplied)**

During the conference, Grab said that they can provide passengers a copy of the audio and video recording when requested. But the Grabchat message was not explicit about this, nor was it clear on how passengers can actually exercise this and other data privacy rights. It also lacked the contact details of the Data Protection Officer of Grab PH. The purpose of the processing may be partly defeated if these information are not provided to the riding public.

6. **The PIA and the notice/email for the passenger selfie verification were silent about the storage and retention period of the photos.** As to the pilot test, Grab stated that the "video recordings will be stored with the provider", and "the encrypted audio is temporarily stored on Grab servers" in its PIA and Grabchat message, respectively. It did not specify, however, whether these servers are located in or outside the country, which should be a consideration when determining the appropriate security measures to implement. Should the servers be located outside the country, Grab simply assumes that the data subject allows such cross-border data transfer since its Privacy Policy states that, "You understand and consent to the transfer of your personal data from your Home Country to the Alternate Country". Under the law, data subjects must be made aware of these information. **(Emphasis supplied)**

Given these deficiencies, Grab PH must adopt the appropriate

measures to correct or remedy the same. As such, Grab PH is hereby **DIRECTED** to comply with the following:

1. Conduct/update the PIA for the processing systems according to NPC Advisory 2017-03, using a methodology that meets the following criteria:

    a. Provides a systematic description of the personal data flow and processing activities including the purpose of the processing, data inventory identifying the types of personal data held, sources and procedures of collection, functional description of the processing including information repositories, data transfers, storage and disposal method of personal data, accountable and responsible persons involved in the processing, and existing organizational, physical and technical security measures;
    b. Includes an assessment of Grab's adherence to the data privacy principles, implementation of security measures, and the provision of mechanisms for the exercise of data subject rights;
    c. Identifies and evaluates the risks posed by the processing, and proposes measures to address the risks; and
    d. An inclusive process that ensures the involvement of interested parties and secures inputs from the DPO and data subjects; and

2. Based on the updated PIAs, update the Privacy Notices and Privacy Manual / Data Protection Handbook.

On a Memorandum dated 31 January 2020, the DASCO recommended to this Commission the issuance of Cease and Desist Order for Grab PH to suspend the [1] roll-out of the Passenger Selfie Verification; [2] pilot test of the In-Vehicle Audio Recording; and [3] pilot test of the In-Vehicle Video Recording until such time that Grab PH fully implements the proper controls to address the deficiencies identified in the Notice of Deficiencies. Further, DASCO emphasized that the issuance of the Cease and Desist Order is in pursuit of protecting public interest by mitigating the risks posed by these processing systems to data subjects.

DISCUSSION

The power of this Commission to issue Cease and Desist Order is explicitly provided in Section 7(c) of the Data Privacy Act ("DPA"), thus:

> "Section 7(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**." **(Emphasis supplied)**

The same power was reiterated in Section 9.f.3 of the Implementing Rules and Regulations of the DPA, to wit:

> "Section 9. *Functions.* The National Privacy Commission shall have the following functions:
>
> xxxx xxxx xxxx
>
> f. Enforcement. The Commission shall perform all acts as may be necessary to effectively implement the Act, these Rules, and its other issuances, and to enforce its Orders, Resolutions or Decisions, including the imposition of administrative sanctions, fines, or penalties. This includes:
>
> xxxx xxxx xxxx
>
> 3. Issuing **cease and desist orders**, or imposing a temporary or permanent ban on the processing of personal data, **upon finding that the processing will be detrimental** to **national security** or **public interest**, or if it is necessary to **preserve and protect the rights of data subjects**;" **(Emphasis supplied)**

From the plain reading of the DPA and its IRR, there are only two (2) elements needed in order for this Commission to validly exercise its power to issue Cease and Desist Order, to wit:

1. There must be a finding or determination; and
2. The processing of personal data will be detrimental to **national security, public interest**, or the **issuance is necessary to preserve and protect the rights of the data subject.**

In DASCO Notice of Deficiencies dated 31 January 2020, it was clearly established that Grab PH's three (3) new data processing systems' risk assessment and mitigation are lacking, the PIA and privacy notice are insufficient, and the purpose of data processing itself is unclear. Further, in DASCO Memorandum dated 31 January 2020, it was stated that, "maintaining the status quo, wherein Grab PH is engaged in the collection and processing of passenger personal information through the processing systems in question, would further expose the fundamental rights and freedoms of the concerned data subjects to detrimental risks."

While this Commission believes that the security of passengers and drivers is a primordial concern, their privacy rights must not be disregarded. It must be protected with earnestness by ensuring that the purpose of data processing is clearly stated, the data flow is secured, and the risks are properly identified and mitigated. Absent these safeguards, this Commission will always adhere in protecting the privacy rights of the data subjects.

WHEREFORE, premises considered, Grab PH is hereby ordered to **CEASE AND DESIST** the [1] roll-out of the Passenger Selfie Verification; [2] pilot test of the In-Vehicle Audio Recording; and [3] pilot test of the In-Vehicle Video Recording until such time that Grab PH fully satisfies the requirements of this Commission as stated in the 31 January 2020 Notice of Deficiencies issued by DASCO.

SO ORDERED.

Pasay City, Philippines
03 February 2020

[SGD.]
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

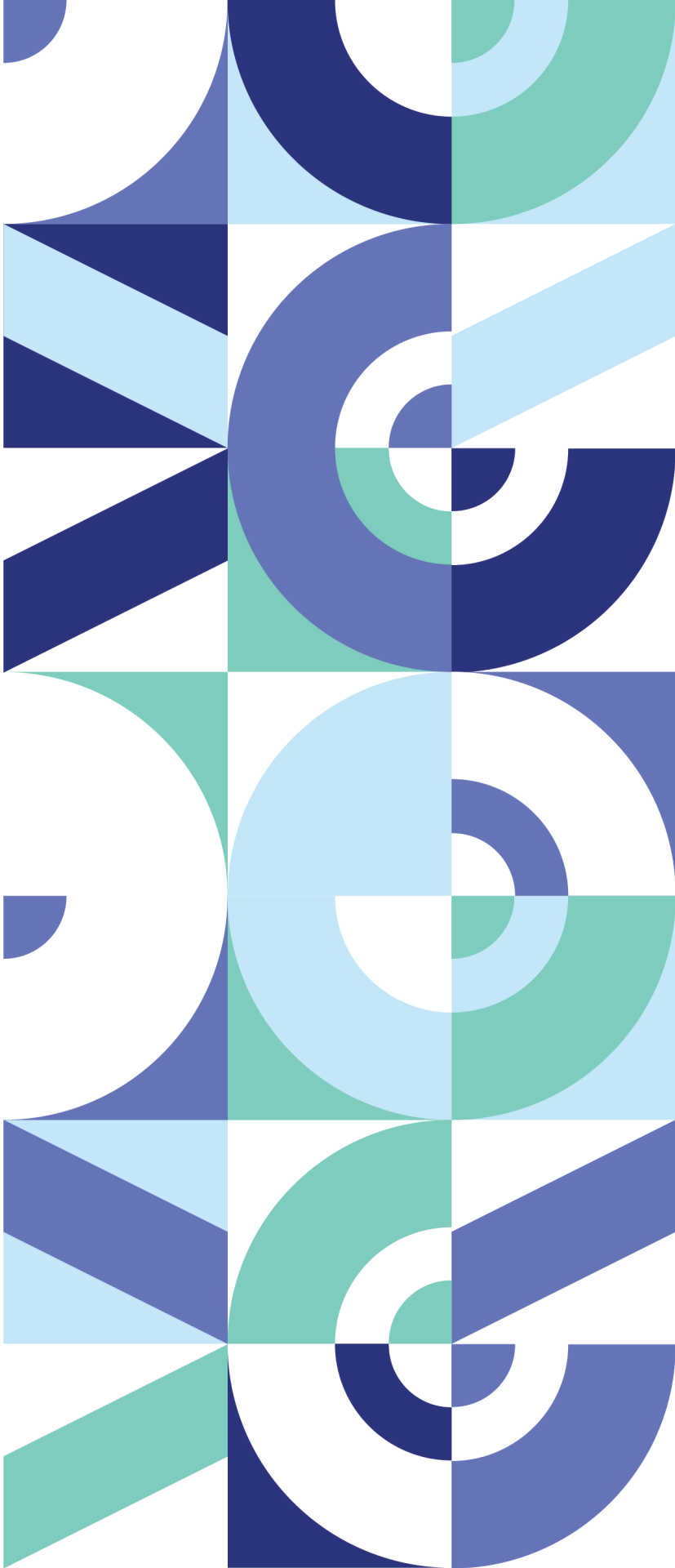
WE CONCUR:

[SGD.]
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

[SGD.]
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

NOTES

NOTES



Trunkline
8234-2228
Local numbers
Compliance 118
Complaints 114
Advisory opinions 110
Other inquiries 117

Website
privacy.gov.ph
Social media
fb.com/privacy.gov.ph
twitter.com/PrivacyPH

Address
5th Floor Delegation Building,
PICC Complex, Roxas Boulevard