Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-017

21 April 2017

[redacted]

Re: CLARIFICATIONS ON REPUBLIC ACT NO. 10173, OTHERWISE KNOWN AS THE DATA PRIVACY ACT OF 2012 (DPA) AND ITS IMPLEMENTING RULES AND REGULATIONS (IRR)

Dear [redacted]

This has reference to the series of queries you forwarded to the National Privacy Commission (NPC) via (3) emails dated 5, 7 and 18 October 2016, respectively, regarding Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), and its Implementing Rules and Regulations (IRR).

Relative thereto, the Commission has prepared a consolidated Advisory Opinion that seeks to address those queries.

Effectivity Date of the IRR

The IRR of the DPA took effect on 9 September 2016, which is fifteen (15) days after it was published in the website of the *Official Gazette* on 25 August 2016. Note that Section 72 of the IRR explicitly provides for its effectivity fifteen (15) days after its publication.

Section 3 of the IRR provides that "consent shall be evidenced by written, electronic or recorded means." Is there a specific format for such consent? What are the acceptable evidence of such consent?

For the purpose of complying with the provisions of the law, any of the three (3) formats prescribed (i.e., written, electronic or recorded) may be adopted by a personal information

controller (PIC) when obtaining the consent of a data subject. Nonetheless, it should be emphasized that, regardless of its format, consent must always be freely given, specific, and informed.

Is an email of a data subject acceptable evidence as electronic means?

It is possible to consider an email as evidence of consent, subject to the rules on authentication provided under the Rules of Court, and the Rules on Electronic Evidence.

As regards a valid retention period for personal data, can consent be given for "any future legitimate use by the business"?

To recall, part and parcel of the definition of consent (of a data subject) is that it must be specific and constitutes an informed indication of will.[1] Permission given for "any future legitimate use by the business" is tantamount to a blanket authorization. This is a clear departure from the requirement that it be specific and informed, thereby removing it from the definition of a valid consent of a data subject.

Note further that consent given to particular processing of personal data must also be time-bound in relation to the declared, specified, and legitimate purpose of such processing.[2] It cannot be perpetual. Consequently, retention of personal data shall only for as long as necessary:

a. for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
b. for the establishment, exercise or defense of legal claims; or
c. for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.[3]

In some specific cases, retention of personal data may be allowed by law.[4]

In Sections 26, 27 and 28 of the IRR, the phrase "where appropriate" was used. When is it appropriate?

The cited provisions relate to the different types of security measures PICs and Personal Information Processors (PIPs) are obliged to adopt in the course of their personal data processing operations. In so doing, they are expected to take into account their respective contexts, with all attendant circumstances.

Corollarily, these same factors would serve as bases for the NPC when evaluating if "reasonable and appropriate" measures are being implemented by a PIC or PIP vis-à-vis its data processing activities.

[1] *see*: RA 10173, §3(b).
[2] IRR of RA 10173, §19(a)(1).
[3] *id*., §19(d)(1).
[4] *id*., §19(d)(2).

In determining the level of security appropriate for a PIC or PIP, the Commission shall 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. [5]

To illustrate, a PIC that does not make use of electronic media or computer systems in its processing activities would have to focus its efforts in developing policies and procedures that relate to manual processing or paper-based systems.

Are all those required to register also obliged to comply with the security measures set forth in Rule VI?

Rule VI of the IRR, which relates to "Security Measures for the Protection of Personal Data", applies to *all* PICs and PIPs.

Section 28(g) vis-à-vis Section 67 of the IRR. Could an overview be provided concerning the obligation by PICs to adopt encryption technology, considering there are no guidelines yet on this subject.

The NPC has issued already Circular No. 16-01, which concerns the security of personal data in government agencies. While the issuance pertains to government entities, its provisions may nevertheless be used as guidance by the private sector.

Some provisions thereof that take up the subject of encryption include the following:

1. *Section 8. Encryption of Personal Data.* All personal data that are digitally processed must be encrypted, whether at rest or in transit. For this purpose, the Commission recommends Advanced Encryption Standard with a key size of 256 bits (AES-256) as the most appropriate encryption standard.
2. *Section 18. Online Access to Personal Data*. Agency personnel who access personal data online shall authenticate their identity via a secure encrypted link and must use multi-factor authentication. Their access rights must be defined and controlled by a system management tool.
3. *Section 24. Emails*. A government agency that transfers personal data by email must either ensure that the data is encrypted, or use a secure email facility that facilitates the encryption of the data, including any attachments. Passwords should be sent on a separate email. It is also recommended that agencies utilize systems that scan outgoing emails and attachments for keywords that would indicate the presence of personal data and, if appropriate, prevent its transmission.
4. *Section 26. Portable Media*. A government agency that uses portable media, such as disks or USB drives, to store or transfer personal data must ensure that the data is encrypted. Agencies that use laptops to store personal data must utilize full disk encryption.

[5] *id*., §29.

If a PIC employs more than two hundred fifty (250) persons but less than one thousand (1,000), is it automatically required to register?

Yes. Section 47 of the IRR states that PICs or PIPs that employ at least two hundred fifty (250) persons must register their data processing systems with the NPC. Those that maintain fewer employees would ordinarily be exempted from registration, unless any of the conditions set out in the same provision is determined to be present.

If a PIC employs more than two hundred fifty (250) persons but it believes that its processing does not pose a risk to the rights and freedoms of data subjects, is it still required to register?

Yes. Any PIC or PIP that maintains at least two hundred fifty (250) employees is required to register its data processing systems with the Commission. The condition that a processing operation of a PIC or PIP poses a risk to the rights and freedoms of data subjects only comes into play when a PIC or PIP has employees whose number fall below such threshold. In that case, it is one of three possible conditions that would still render as mandatory the registration by the PIC or PIP of its data processing systems with the NPC.

Will a PIC that has separate systems for employee information and healthcare professionals' information be allowed to register only the latter system, or would both systems have to be registered, albeit separately?

Both systems must be registered with the NPC. As per the relevant provision of the IRR, a PIC or PIP that employs fewer than two hundred fifty (250) persons shall not be required to register its data processing systems, unless the processing it carries out is likely to pose a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive personal information of at least one thousand (1,000) individuals.[6] When any of such conditions are met, a PIC or PIP must register *all* its data processing systems. The language of the IRR does not limit the application of the registration requirement to those processing systems that meet any of the three (3) conditions identified.

When is personal data processing likely to pose a risk to the rights and freedoms of data subjects?

The language of the DPA provides little guidance on this subject. It is worth noting, however, that the law is largely based on Directive 95/46/EC of the European Union, which has since been replaced by Regulation 2016/679, also known as the General Data Protection Regulation (GDPR). The GDPR, which is set to take effect in May 2018, offers some illumination in this regard, *to wit*:

> "The risk to the rights and freedoms of natural persons, of varying likelihood

[6] IRR, §47.

> and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects."[7]

What is the consequence of a PIC or PIP's failure to register its data processing systems with the NPC, based on the belief that its processing does not pose a risk to the rights and freedoms of data subjects, and it is later proven that such risk exists? Will the PIC or PIP be held liable for not complying with the registration requirement?

As per the provisions of the DPA, non-compliance with the registration requirement *per se* is not a criminal offense. However, it may lead to administrative penalties and/or fines based on policies that the NPC may develop and implement pursuant to its mandate. Moreover, in the event of a breach or when a data subject files a complaint with the NPC against a PIC or PIP, any ensuing investigation or audit undertaken by the Commission will necessarily involve an assessment of the compliance status of the entity with the provisions of the law, its IRR, and any relevant issuance of the Commission—including those pertaining the registration of data processing systems.

In view of the foregoing, PICs and PIPs are advised to observe due diligence in making an assessment of their data processing systems or operations, particularly their potential impact on the rights and freedoms of data subjects. In case of doubt, the law itself offers guidance as regards the proper approach to adopt when interpreting the law and any of its provisions. Thus:

> "Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed."[8]

[7] Regulation (EU) 2016/679, Whereas Clause (75).
[8] RA 10173, §38.

When is processing not occasional?

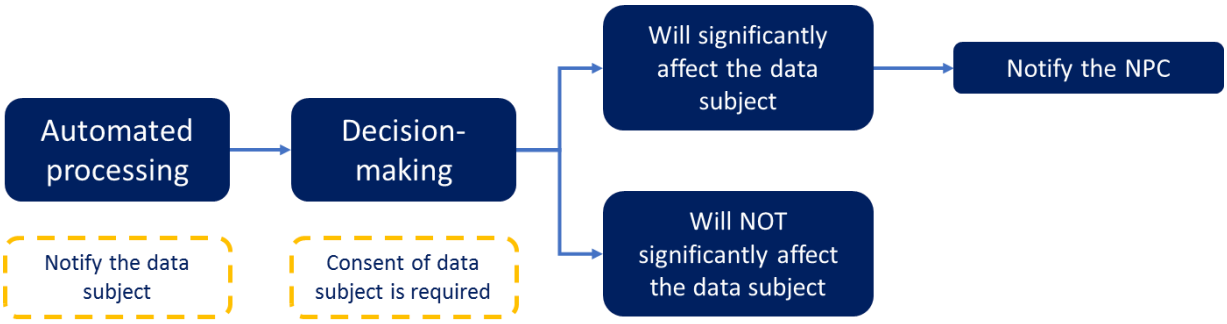
Processing is not occasional when there is regularity and recurrence of the processing.

Section 47 provides that the contents of registration shall include the name and contact details of the compliance or data protection officer, does the data protection officer have to be located in the Philippines?

The NPC has issued its Advisory No. 2017-01 (Designation of Data Protection Officers [DPO]), which provides for guidelines regarding the mandatory designation, general qualifications, position, duties, and responsibilities of a DPO and Compliance Officer for Privacy (COP). While the Advisory is silent as regards the possibility of a DPO/COP being located outside the Philippines, the language thereof allows for such a scenario, provided that the concerned DPO/COP is able to fulfill his or her functions, as laid out in the issuance. Other requirements set out in the Advisory should also be met.

Section 48 of the IRR provides that the NPC shall be notified when the automated processing becomes the sole basis for making decisions about a data subject, particularly when the decisions would significantly affect the data subject. Please clarify and give an example where automated processing will be a basis for making decisions.

Please see diagram below on the requirement for notification:



A possible scenario wherein automated processing is the sole basis for making a decision about a data subject, and where such decision would significantly affect the data subject would be that wherein an individual's loan application—which necessarily includes his or her personal data—is automatically processed by a financial institution or credit facility, such that said automated processing directly results in the approval or denial of the application.

Section 67 of the IRR provides that PICs and PIPs shall register with the NPC their data processing systems or automated processing operations within one (1) year after

the effectivity of the Rules. Further, Section 47(b) provides that procedure for registration shall be in accordance with the Rules and other issuances of the NPC. Is there a specific format or template that may be used for registration?

To date, the Commission does not impose any specific format or template relative to the registration and notification requirements for personal data processing systems and automated processing operations, respectively. For the purpose of determining the compliance by PICs and PIPs with the law and its IRR, adherence to the requirements set out in Sections 47 and 48 of the IRR will be deemed sufficient. As an initial step of the registration of data processing systems, a form requiring information about the data protection officer of the PIC or PIP may be downloaded from the website of the Commission (privacy.gov.ph).

When will the procedure for registration be released?

There is no particular time frame being considered as regards the drafting and release of a more specific procedure concerning the registration of data processing systems. Rest assured, however, that the NPC will come out with the appropriate announcement should any document featuring such a procedure be issued.

Is there a timeframe for monitoring and compliance?

To be sure, the Commission has compliance and monitoring functions to ensure effective implementation of the DPA, IRR and other issuances.[9] At present, these functions are primarily triggered by complaints or reports filed with the Commission, which necessitate the conduct of investigations or audits by its concerned offices. However, it should be emphasized that even absent such initiatives from the Commission, all PICs and PIPs are expected to comply with the provisions of the DPA and its IRR as soon as these policies entered in to force.

Will the NPC issue a certification of compliance with the DPA?

The Commission is currently in the process of developing its monitoring and compliance framework, which could possibly include the issuance of certifications of compliance in favor PICs and PIPs.

Section 5(a) of the NPC Circular 16-01 provides that "[t]he personal information controller shall also include in the report the name of a person and his or her contact information." Whose name shall be included in the report?

[9] IRR, §9(d)

The document in question refers to the *then* draft circular on Data Breach Notification. Please note that the final circular on this subject is now NPC Circular No. 16-03 (Personal Data Breach Management), which was issued on 10 October 2016.

As per the specific provision raised, the person referred therein is the Data Protection Officer (DPO), whose identity and contact information must be included in the notification required to be communicated to the Commission.

For your guidance.

Sincerely,

IVY D. PATDU
Officer in Charge
Deputy Privacy Commissioner
Policy and Planning