Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-018

21 April 2017

[redacted]

Re: **VARIOUS QUERIES REGARDING THE IMPLEMENTING RULES AND REGULATIONS (IRR) OF THE DATA PRIVACY ACT (DPA) OF 2012**

Dear [redacted]

This pertains to your queries received by the National Privacy Commission (NPC) on 26 November 2016, via email, that relate to various sections of the Implementing Rules and Regulations (IRR) of the Data Privacy Act of 2012 (DPA).

At the outset, we note that some of the questions relate to provisions, as written in the *draft* IRR, and thus, were mislabeled. We urge inquiring parties to prepare and review their questions thoroughly to avoid any confusion.

Section 3

Sec. 3(c): What would constitute a "lawful representative"? Would "an agent specifically authorized by the data subject" include anyone authorized in writing or other recorded form by the data subject?

A lawful representative or agent, as used in the IRR[1], refers to a person duly authorized by the data subject to act on his or her behalf. As in the case of consent, the grant of authority by the data subject must be evidenced through written, electronic or recorded means.

[1] IRR, §3(c).

Would negative consent be sufficient (e.g., where a data subject returns a signed application form but does not tick an opt-out box)?

Implied, implicit, or negative consent is *not* recognized under the DPA and its IRR. The consent of a data subject is required to be specific and evidenced through written, electronic, or recorded means. Thus, it needs to be express and not subject to conjectures, based on assumptions, or ascertained by mere inference.

Sec. 3(f): Given the definition for "data sharing", will data collected in the Philippines but transferred to a foreign company as part of an outsourcing agreement be exempt from the DPA and IRR?

No. The DPA[2] and its IRR[3] explicitly state that they apply to the processing of personal data, even if the act or practice is performed outside of the country, provided that the personal data relates to a Filipino citizen or a resident of the Philippines, and/or the personal information controller (PIC) or personal information processor (PIP) has an established link to the Philippines. As long as the foregoing conditions are met, processing of personal data, whether or not it is part of a data sharing or a subcontracting/outsourcing arrangement, will be covered by the DPA, the IRR and other applicable issuances by the NPC.

In the case of outsourcing or subcontracting, note that the IRR requires the PIC to use all reasonable means in ensuring that proper safeguards are in place whenever it outsources or subcontracts data processing.[4]

Sec. 3(g): Does the definition for "direct marketing" mean it will only apply the marketing material is addressed to individuals by their names?

Direct marketing refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals.[5] The phrase "directed to particular individuals" does not mean that the material addresses a particular person by name. A merchant and/or advertiser in possession of and using other types of personal data (e.g., email address, home adress, mobile phone number, email, etc.) when sending out marketing materials directly to individuals are also covered under the law.

Given the definition for "personal data", may it be used interchangeably with the term "personal information"?

No. The term, "personal data," is used when personal information, sensitive personal information and privileged information are referred to collectively. It may *not* be used in lieu of personal information (and vice versa), which only forms part of the broader concept of personal data.

[2] DPA, §4.
[3] IRR of the DPA, §4.
[4] IRR, §43.
[5] IRR, §3(g).

Given the definition for "personal information", are identifying information (e.g., business contact information/KYC information) relating to the individual employees/representatives of corporate/institutional clients protected under the DPA/IRR?

Yes. The DPA and its IRR apply to the processing of personal data. Thus, even where a company only has juridical persons for clients, if it processes personal data or information relating to individuals (e.g., employees/representatives of such corporate clients), it is still bound to comply with the DPA, its IRR and other applicable issuances by the NPC.

Section 4

How is the term "affiliate" defined?

The IRR adopts the common or general definition for the term, "affiliate." Under Republic Act No. 10142, also known as the Financial Rehabilitation and Insolvency Act (FRIA) of 2010, it refers to a corporation that directly or indirectly, through one or more intermediaries, is controlled by, or is under the common control of another corporation.[6]

Would the foreign parent or foreign affiliate of a PIC or a personal information processor (PIP) be subject to all the requirements under the IRR (i.e., submission of policies, consent from data subject, etc.)?

If a PIC or PIP operating in the Philippines has a foreign parent company or a foreign affiliate, the latter shall be subject to the requirements under the DPA if it is engaged in the processing of personal data of Filipino citizens or residents of the Philippines, and/or it has an established link to the country.[7] "Access" falls within the definition of the term, "processing".[8]

If there is a security breach in the parent or an affiliate offshore that does not include Philippine residents/citizens, and the Philippine entity is not involved, should it be reported to the NPC?

To reiterate, a foreign entity, whether it is a parent or an affiliate of a Philippine company, is covered by the DPA—including its provision on breach notification—only if it is engaged in the processing of the personal data of Filipino citizens or Philippine residents, and/or has an established link to the Philippines.

---

[6] §4(b).
[7] IRR, §4(d)(4).
[8] *see*: IRR, §3(o).

Where it is stated that "the parent or affiliate of the Philippine entity has access to personal data", does this only refer to personal data about a Philippine citizen or resident or personal data which originated in the Philippines?

No. As per the cited provision, the DPA and its IRR shall still apply to the processing of personal data performed outside of the Philippines, provided that any or all of the conditions set thereunder are met. One of such conditions is when an entity (foreign parent or affiliate) has a branch, agency, office or subsidiary in the Philippines, and it has access to personal data collected by and/or possessed by the latter.[9] In this particular context, no qualification is made as regards the personal data involved. Nonetheless, it is worth noting that the application of this Rule is "with due consideration to international law and comity."[10]

If the human resources function of a Philippine corporation is performed by an offshore affiliate, will the affiliate be subjected to all the requirements under these rules or will the Philippine entity assume all the requirements under these rules?

If a PIC outsources or subcontracts the processing of personal data to another natural or juridical person, the latter is considered a PIP, regardless of the latter's location or relationship with the PIC.[11] As per the DPA[12] and its IRR, a PIP is required to comply with the applicable requirements of the DPA, IRR, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a PIC.[13]

Section 5(f)

Does the provision mean that personal data lawfully collected in foreign jurisdictions without securing the consent of the data subject can be processed in the Philippines, but that the Philippine company (as PIC or PIP) must implement appropriate security measures in respect of such data?

Section 5(f) of the IRR provides that personal data processed in the Philippines, but which were originally collected from residents of foreign jurisdictions in accordance with the laws thereof, fall outside the scope of the DPA.

[9] IRR, §4(d)(4).
[10] IRR, §4(d).
[11] *see*: IRR, §3(n).
[12] RA 10173, §14, in relation to §21(b).
[13] IRR, §45.

This means the collection itself of the personal data is governed by the laws of the foreign jurisdiction. Other types of processing that the personal data is subjected to here in the Philippines remain covered by the DPA. This interpretation is consistent with Section 38 of the DPA, which reads:

> "Interpretation. – Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed." (underscoring supplied)

It is further reinforced by the proviso in the next following paragraph of Section 5, which states *inter alia* that: (a) the non-applicability of the law does not extend to PICs or PIPs (i.e., they must still implement the appropriate security measures in respect of such data); and, the processing of the personal information is exempted only to the minimum extent necessary to achieve the specific purpose, function, or activity.[14]

Section 19(a)(1)

What would satisfy the requirement that the consent be "time bound"? Would a statement to the effect that the consent applies for the period of the customer relationship be sufficient? Can the period be as long as personal information controller likes, or should it be limited (e.g., one year)?

The requirement that the consent of the data subject be time-bound must be considered relative to the "declared, specified and legitimate purpose" of the personal data processing it refers to. Thus, it would *not* be prudent or proper for the NPC to determine how such requirement may be met, absent any specific circumstances.

If the PIC has the data subject for its customer or client, and the processing of the latter's personal data is contingent on such relationship, indicating that the effectivity of the consent is coterminous with that of the relationship *may* be a considered as consistent with the "time-bound" requirement.

What is not permitted is having the duration of the consent determined solely by the PIC. This directly contravenes the "time-bound" element of consent and undermines the very concept of consent, which, as defined in the DPA and its IRR, is an indication of will of the data subject, and *not* that of the PIC.

Section 20

Section 20(b)(2): Is a data sharing agreement required for a group of companies? If the clients of a group of companies already provided consent that the personal data be shared among the group of companies, do we still

[14] *id.*, §5, last paragraph.

need to execute a data sharing agreement within the group? Would policies/procedures relating to data protection that apply to the relevant affiliates be sufficient?

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.[15]

In the private sector, it is permitted if the consent of the data subject is obtained, and certain conditions provided in the Implementing Rules and Regulations (IRR) of the DPA are complied with.[16] One such condition requires the execution of a Data Sharing Agreement (DSA) if sharing is carried out for commercial purposes.[17] The term "commercial purpose" is read in its ordinary meaning and refers to any activity with the ultimate purpose of gain or profit.

Data sharing between private sector entities—including that between affiliates, or between a company and its parent or subsidiary—is generally presumed to be in pursuit of some commercial objective or purpose, as is the compliance by such entities with the DSA requirement prior to any data sharing arrangement. 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. Accordingly, it is incumbent upon a private sector entity seeking to exempt itself from the DSA requirement to overcome the aforesaid presumptions.

Section 20(b)(2): How is "commercial purpose" defined?

The term "commercial purpose" is taken in its ordinary meaning. Thus, data sharing for a commercial purpose is one whose ultimate purpose is that of gain or profit.

Section 20(b)(3): Is it necessary to identify the specific processors, or would a general description as to the category of processors (e.g. direct marketing companies, call center operators, telecommunications providers, affiliates within a group of companies, etc.) be sufficient?

The language of Section 20(b)(3) of the IRR clearly imposes a duty to identify the PIP.[18] Unlike Section 34(a)(2)(3), wherein it is possible to refer to the recipients of the personal data by their class, Section 20(b)(3) explicitly calls for the identity of the PIP.

At any rate, under Section 34(c)(3) of the IRR, a data subject may demand access to the names and addresses of the recipients of his or her personal data. Thus, should the PIC fail to identify the PIP, as required, it may later be compelled to do so upon the request of a data subject.

[15] IRR, §20(a).
[16] *id.*, §20(b).
[17] *id.*, §20(b)(2).
[18] IRR, §20(b)(3)(a).

Section 24

Where a company has recorded lines for compliance and quality control purposes, how may it comply with this Section? Is it sufficient to post a notice of such recording in the company's terms and conditions with clients, and in a privacy policy published on its website?

Section 24 of the IRR seeks to elaborate on Section 44 (Repealing Clause) of the DPA, which states:

> "The provision of Section 7 of Republic Act No. 9372, otherwise known as the "Human Security Act of 2007", is hereby amended. Except as otherwise expressly provided in this Act, all other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly." (underscoring supplied)

Both provisions refer to RA 9372, which is the country's primary anti-terrorism legislation. Section 7 thereof relates to the "surveillance of suspects and interception and recording of communications" and states:

> "The provisions of Republic Act No. 4200 (Anti-Wire Tapping Law) to the contrary notwithstanding, a police or law enforcement official and the members of his team may, upon a written order of the Court of Appeals, listen to, intercept and record, with the use of any mode, form, kind or type of electronic or other surveillance equipment or intercepting and tracking devices, or with the use of any other suitable ways and means for that purpose, any communication, message, conversation, discussion, or spoken or written words between members of a judicially declared and outlawed terrorist organization, association, or group of persons or of any person charged with or suspected of the crime of terrorism or conspiracy to commit terrorism.
>
> *Provided*, That surveillance, interception and recording of communications between lawyers and clients, doctors and patients, journalists and their sources and confidential business correspondence shall not be authorized."

As may be gathered from the foregoing provision, it specifically refers to surveillance or the interception of communications as performed by the police or law enforcement officers. It does *not* apply to the recording of conversations by private parties for whatever purpose.

Nonetheless, the recording of phone conversations "for compliance and quality control purposes" is well within the meaning of the term, "processing," as defined under the DPA and its IRR. The conduct thereof must therefore comply with their applicable provisions of the law.

A company measure informing the public of its practice of recording phone conversations made with its representatives may be considered when determining the company's compliance with the duty to inform data subjects of relevant information regarding its processing of their personal data. However, this is but one of many duties and responsibilities that a PIC or PIP must observe in relation to its data processing activities.

Section 26

Does the Data Protection Officer need to be a resident of the Philippines and employed by the data processor?

Given its definition,[19] 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.

Are companies outside of the Philippines which process data covered by Section 4 of the IRR required to appoint their own Data Protection Officers under the IRR?

The designation of a DPO is required for both PICs[20] and PIPs[21]. Since the DPA does not distinguish between entities operating in the Philippines or abroad, an offshore company that meets the criteria set in the law for the latter's extra-territorial application is required to appoint a DPO. For additional guidance on this subject, reference must be made to NPC Advisory No. 2017-01.

For a group of companies where there are offices inside and outside the Philippines, can there be just one appointed Data Protection officer or should one be appointed for each entity?

As a general rule, 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. Thus, it must designate a DPO in fulfilment of the requirement prescribed by law. However, as clarified in NPC Advisory No. 2017-01, 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, *subject to the approval of the NPC*. Where such common DPO is allowed, the other members of the group must designate a Compliance Officer for Privacy (COP).

Section 34

Section 34(b)(3): Does "legal obligation" extend to legal obligations under foreign law, or only to legal obligations originating in the Philippines?

Section 34(b) of the IRR pertains to the right of a data subject to object or withhold his or her consent to the processing of his or her personal data. By way of an exemption, subsection no.

[19] *see*: NPC Circular No. 16-01, §3(F).
[20] RA 10173, §21(b).
[21] *id.*, §14, in relation to §21(b).

3 thereof states that this right will not apply where the collection or processing is pursuant to a legal obligation on the part of the PIC.

As used in the provision, the term "legal obligation" shall be read to mean obligations borne by either a foreign or domestic law that the PIC may be subject to. This is consistent with the legal maxim, "*ubi lex non distinguit nec nos distinguire debemus*" (when the law does not distinguish, we must not distinguish).[22] Should conflicts arise between obligations imposed by a foreign law and those required by a domestic statute (i.e., DPA), the NPC should be consulted for the appropriate resolution thereof.

Section 34(c)(2): Does this mean that you need to provide access to the source(s) themselves, or is it sufficient to provide information about which sources the data was obtained from?

The provision, which is culled from Section 16(c)(2) of the DPA, means that the data subject has the right to obtain information regarding the sources from which his or her personal data was collected. This is premised on the scenario wherein the entity currently processing the personal data did not directly collect the personal data from the data subject, pursuant to a valid data sharing agreement or some other means authorized by law.

Section 34(d) requires immediate correction. Will organizations be given a reasonable time within which to comply with such request? If so, what period would generally be considered reasonable?

The language of the provision notwithstanding, companies will be given reasonable time to comply with a request for correction or rectification. What may be considered as "reasonable time" given a particular set of circumstances is a question of fact. Recognizing the range of factors that may affect a particular case, the NPC deems it impractical—if not outright improper—to impose a specific and/or uniform timeframe or period within which the obligation to rectify or implement a correction must be complied with.

It is worth noting, nonetheless, that for the public sector, Republic Act No. 6713, otherwise known as the Code of Conduct and Ethical Standards for Public Officials and Employees, provides that all public officials and employees are obliged to act on letters and requests within fifteen (15) working days from receipt of such letter of request.

Does the notification requirement only apply to personal data collected after the IRR comes into effect (i.e., there is no need to provide notifications in respect of data collected prior to this date)?

It must be emphasized that a data subject's right to be informed of certain matters relative to the processing of his or her personal data is enshrined in the DPA,[23] which has been in force

[22] *Amores v. House of Representatives Electoral Tribunal*, G.R. No. 189600 (29 June 2010).
[23] *see*: RA 10173, §16(a) and 16(b).

since 8 September 2012. Accordingly, the obligation on the part of PICs to make the necessary notifications arose beginning on that particular date.

Note further that both the law and the IRR state that notification shall be carried out before the entry of the personal data into the processing system of the PIC, or "at the next practical opportunity".[24] Thus, the fact that the personal data of a data subject was collected prior to the effectivity of the law neither diminishes nor removes the obligation to notify on the part of the PIC. Indeed, while the latter may not have had the duty to notify the data subject prior to enactment of the DPA, it certainly had one as soon as the law became effective.

Can the notification requirement be satisfied by posting a privacy policy containing the required information on the company's website?

It is possible for a PIC to comply with the notification requirement set under the law and the IRR by providing the requisite information in a "privacy notice" or "privacy policy" posted in the PIC's website. However, each PIC will have to make a proper determination whether this method is the most appropriate given its peculiar circumstances. For instance, it may not be prudent or proper for a PIC that collects personal data from people who generally reside in rural areas or regions with little to no access to the internet to comply with the notification requirement through an online privacy notice or policy.

Note further that in order to meet the requirement properly, a PIC must carry out a thorough assessment of its personal data processing system/s. This will ensure that all requisite information are featured in the aforesaid notice or policy.

Section 43-45

If the processing of data is outsourced or subcontracted, what is the liability of the sub-contractor or service provider if there is a breach?

If the processing of personal data is outsourced or subcontracted by a PIC to another entity, the latter is considered as a PIP, as defined in the DPA and its IRR.[25] As PIP, an entity is duty-bound to "comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller".[26]

In the event of a breach, the same process for determining any liability on the part of a PIC and/or any of its officers will be undertaken vis-à-vis a PIP and its officers. Accordingly, the extent of liability for either a PIC or PIP will also be governed by Section 61 of the IRR.

[24] RA 10173, §16(b) and IRR, §34a(2).
[25] *see*: DPA, §3(i) and IRR, §3(n).
[26] IRR, §45.

In the event of a breach, will the obligation to report a breach lie with the PIC, or the subcontractor/service provider?

Reference must be made to NPC Circular No. 2016-03 (Personal Data Breach Management) to properly address this query. According to the Section 15 of the Circular, the duty to notify or report a breach remains with the PIC, even if it outsources or subcontracts the processing of personal data to a PIP. To facilitate the timely reporting of a breach, the PIC is obliged to use contractual or other means to ensure that it is given a report by the PIP regarding a breach at the soonest possible time.[27]

Section 47

If a PIC has less than 250 employees but processes data about such employees on an ongoing basis (not just "occasionally") is it required to register? If a Philippine company has less than 50 employees, does it need to register?

The policy provided in Section 47 of the IRR states that, if a PIC or PIP has at least 250 employees, it must register its personal data processing system with the NPC. If its employees are fewer than 250, it may still be required to register in three (3) scenarios. Specifically, if the processing it carries out:

1. is likely to pose a risk to the rights and freedoms of data subjects;
2. is not occasional; or
3. includes sensitive personal information of at least one thousand (1,000) individuals.

Does the 250-employee requirement only include persons employed in the Philippines (as opposed to persons employed by foreign affiliates)?

For the purpose of determining its compliance with the DPA, each juridical person is considered a separate and distinct entity, even if it has a parent company or affiliates, and irrespective of its location, or that of its parent or affiliate. Its nature as a PIC or PIP is determined by the degree of control it exercises over the processing of personal data.[28]

Accordingly, in figuring out whether or not a company should register its personal data processing system with the NPC, as provided in Section 47 of the IRR, one will have to take note of the number of its employees and/or the nature of its processing system. The actual location of the employees themselves is immaterial.

Section 61

[27] NPC Circular No. 16-03, §16.
[28] *see*: IRR, §3(m) and (n).

Would the liability of a corporation extend to: (a) its directors; (b) the data protection officer; and/or (c) other employees involved in the offense?

Where a juridical person is found to be criminally liable under the DPA, Section 61 of the IRR clearly identifies the officers against whom the penalties provided in the DPA may be imposed, namely:

1. officers who participated in the commission of the crime
2. officers who, by their gross negligence, allowed the commission of the crime

Thus, regardless of the designation, title, or position of the officer concerned, what is controlling when making a determination as to which individual/s shall be held liable for the offense is the nature of his/her involvement in the commission thereof.

Section 67

Does the 1-year transition period apply to all requirements in the IRR and the DPA (as stated in the DPA), or only to the registration requirement (as stated in the IRR)? For instance, if there is a breach now, are we required to comply with breach notification requirement?

Section 42 of the DPA states that existing industries, businesses, and offices affected by the Act shall be given one (1) year transitory period from the effectivity of the IRR *or such other period as may be determined by the NPC*, to comply with the requirements of the DPA.

As may be gleaned therefrom, the NPC is given the authority to determine the period of compliance vis-à-vis the requirements of the DPA. The Commission is not bound by the 1-year transitory period mentioned in the law.

The NPC made its determination through the IRR of the DPA. The Rules state that persons involved in the processing of personal data must comply with the personal data processing principles and standards of personal data privacy and security already laid out in the Act.[29] At the same time, they provide that, for purposes of registration, PICs and PIPs are given one (1) year after the effectivity of the IRR within which to register with the Commission their data processing systems or automated processing operations.

Stated otherwise, while PICs and PIPs are given 1 year from the effectivity of the IRR to register with the Commission, they are expected to comply with the rest of the provisions of the IRR immediately upon the effectivity of the latter.

To reiterate, the DPA has been in force since 8 September 2012. It already features provisions that need to be complied with, even sans an IRR. Accordingly, the obligation to notify the

[29] IRR, §67.

NPC regarding a personal data breach arose as soon as the DPA came into force and once the Commission was constituted.
For your reference.

Very truly yours,

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