Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-23

21 June 2017

[redacted]

Re: ASSOCIATION OF BANK COMPLIANCE OFFICERS, INC. REQUEST FOR CLARIFICATION AND COMMENTS

Dear [redacted]

This pertains to the summary of queries you forwarded to the National Privacy Commission (NPC), by email, relating to Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), and its Implementing Rules and Regulations (IRR).

Relative thereto, please find below our responses:[1]

Section 3(b), DPA; Section 19, IRR

Can the consent of a data subject be in the form of a deemed, implied, passive or negative consent (e.g. notice with a period for objecting, the lapse of which will be deemed consent)? How specific must the time-bound characteristic of the consent be? Please provide suggested wording for such notice or consent.

Section 3(b) of the DPA provides:

> "(b) Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal

[1] This advisory opinion is based on the limited information provided in the questions, and may vary based on additional information or when the facts are changed or elaborated.

> 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, it is clear that consent given by a data subject must be evidenced by written, electronic, or recorded means. An implied, passive, or negative consent does not meet such a requirement, including means that merely provide an opt-out option (i.e., a data subject is merely notified of the period within which he or she can object to the processing of his or her personal data).

As regards Section 19(a)(1) of the IRR wherein it is stated that consent must be time-bound vis-à-vis the declared, specified and legitimate purpose, 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 personal information controller (PIC) and the data subject may be a valid stipulation. 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. It is worth noting that 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. At any rate, the validity of the period declared, when challenged, will have to be assessed on a case-to-case basis.

Section 3(h) and (i) and Section 4, DPA;
Section 3(m) and (n), IRR

Please confirm if the provisions of the DPA and its IRR apply to banks with corporate clients only, to the extent that we process personal data of (a) the authorized signatories, officers, directors, stockholders of our clients, (b) our employees, and (c) our candidates/applicants for employment.

The DPA and its IRR apply to the processing of personal data by any natural and juridical person in the government or private sector.[2] Personal data refers to all types of personal information[3], which, in turn, 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".[4]

In the case of banks, whenever one engages in the processing of personal data, it is subject to the provisions of the law, unless otherwise provided in the DPA. This includes processing the personal data of its corporate clients' authorized signatories, officers, directors, and stockholders, and that of its own, including job applicants and other natural persons it may have transactions and/or dealings with.

[2] IRR of RA 10173, §4.

[3] RA 10173, §3(j).

[4] *id.*, §3(g).

Please confirm that for purposes of processing the personal data of its client's relevant authorized signatories, officers, directors, and/or stockholders, since the personal data are collected by the client, the bank will not be considered a PIC or personal information processor (PIP) but will only need to comply with the data sharing requirements under Section 20 of the IRR.

A PIC is defined under Section 3(h) of the DPA as a person or organization that 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. There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.[5]

A bank is considered a PIC relative to all personal data it processes, regardless of the situs for collection. The data involved may have been sourced from its own personnel, job applicants, third-party service providers, etc., or from those of its corporate clients. In all instances, the bank would still be a PIC with respect to those personal data, provided it exercises control over their processing.

As a PIC (and in some cases, even as a PIP), a bank is expected to comply with all the requirements laid out in the DPA, its IRR, and all other relevant issuances of the NPC. Those pertaining to data sharing is but one of them.

Section 4 and 6 DPA; Section 4 and 5, IRR

Please give guidance on the extent of DPA and IRR compliance needed where a foreign company has a Philippine branch. Please confirm that compliance with the DPA and IRR is limited to the Philippine branch, and not the foreign bank in its entirety.

The DPA applies to the processing of personal data, even if those engaged in it only maintain an office, branch, or agency in the Philippines.[6] This extra-territorial application of the law is further emphasized in Section 6 thereof, which states, in part, that the law applies to an act done or engaged in outside of the Philippines by an entity having a link with the country (i.e., it has a branch, agency, office or subsidiary here).

In view of the foregoing, a foreign company and its Philippine branch will both be subject to the provisions of the DPA and its IRR, except for those that apply only to processing activities carried out in the country.

That said, note that a branch office of a foreign company has been defined as an entity that

[5] IRR of RA 10173, §3(m).

[6] *see*: RA No. 10173, §4.

carries out the business activities of the head office and derives income from the host country.[7] As such, it has no separate and independent personality from the head office. The latter merely obtains a license to do business in the host country prior to establishing a branch.[8]

If the foreign head office and/or other branches process the personal data of the Philippine branch's clients' authorized signatories, officers, directors, stockholders who are Philippine residents or citizens, to what extent does it need to comply with the DPA and IRR? Please confirm if such foreign head office or other branches only need to comply if the processing involves the personal data of Philippine residents or citizens.

As discussed above, the DPA has extraterritorial application and covers personal data processing performed outside the Philippines, subject to the conditions set out in the law (i.e., the PIC or PIP has links to the country).[9] In line with this, a company (e.g., head office or other branch) located outside of the Philippines that is still within the scope of the law must adhere to provisions of the law, except those (i.e., registration of data processing systems) that apply only to entities operating inside the country.

Are personal data which are procured from publicly available sources (for instance, in the GIS, AAFS, PSE or in other public documents/instruments) exempt from DPA and IRR requirements?

The law provides for special cases where it does not apply. They include those information that are matters of public concern, or those necessary for public authorities to carry out their respective mandates or functions.[10] Note, however, that such exemption is not absolute. First of all, the exemption applies only to special categories of "information" in relation to a specific processing activity. The exemption does not extend to PICs or PIPs who remain subject to the requirements of the law, especially the implementation of security measures meant to ensure data protection.[11] Also, the exemption shall only be to the minimum extent necessary to achieve the specific purpose, function, or activity of the processing.[12]

As regards personal data secured from "publicly available sources", that fact alone does not automatically bring them outside the scope of the DPA. Public disclosure of personal data does not equate to a *carte blanche* grant of authorization to use said data for whatever end. Such data, after all, may still be abused or used for purposes other than that for which they were made available. To hold otherwise would undermine the very concept of consent, as defined in the DPA.

[7] IRR of RA No. 7042 – Foreign Investment Act of 1991, §1(c).

[8] *PDIC vs. CITIBANK, N.A. and BANK OF AMERICA, S.T. & N.A*, G.R. No. 170290, April 11, 2012.

[9] RA No. 10173, §6(a).

[10] IRR, §5(a) and (d).

[11] *id.*, §5, last paragraph.

[12] *id.*

Will the compliance of banks with BSP requirements be considered compliance with the DPA and IRR? Some requirements overlap. Will NPC defer to the BSP on this matter? We understand that there is a possibility of a memorandum of agreement between NPC and BSP to align their requirements; is there any update on this?

The BSP is the primary regulator of banks and, as such, it enforces certain laws and regulations that apply directly to the banking sector. The case is different for the DPA, which is a distinct and separate law and which has the NPC as the government agency charged with interpreting and implementing its provisions.[13] With this, compliance with BSP requirements is deemed separate and different from compliance with those imposed by the NPC. In the specific area of data protection at least, the NPC is the primary authority and cannot defer to the BSP.

That having been said, the two agencies are currently reviewing possible overlaps in their functions with a view to harmonizing them for a more efficient regulatory framework. They are in the initial stage of forming a technical working group that will address the issues and other concerns of banks in this matter.

Section 21, DPA; NPC Advisory No. 2017-01

Most of the functions of a data privacy officer are carried out by various officers within a bank (i.e. compliance officer, consumer protection officer, IT security officer, security officer). Will this suffice to comply with the requirement of a data privacy officer?

Under Section 21(a)(b) of the DPA, the PIC shall designate an individual or individuals who are accountable for its compliance with the DPA. More recently, the NPC recently issued Advisory No. 2017-01 (March 14, 2017), which lays down the guidelines for the designation of such individuals, now referred to as data protection officers (DPO) or, in some instances, compliance officers for privacy (COP). Among others, the advisory takes up the mandatory designation, general qualifications, duties and the responsibilities of a DPO.

As per the guidelines, existing officers of a bank may be designated as the DPOs. PICs and PIPs must see to their qualifications and ensure that they are aware of the full range of their duties and responsibilities.

Section 3(f), IRR

When personal data is accessible to the head office or other branches of a bank, is there a need for a data sharing agreement and other requirements notwithstanding that the Philippine branch is not a separate entity from such

[13] *see*: RA 10173, §7.

other head office or other branches? If yes, will internal policies on confidentiality or data protection suffice?

Data sharing is the disclosure or transfer to a third party (one or more PICs) of personal data under the custody of one PIC or PIP.[14] In the case of the latter, data sharing is only possible if it is upon the instructions of the PIC.

Taking into account the discussion above regarding the nature of a branch vis-à-vis its head office, the disclosure or transfer contemplated here will only be undertaken within the same organization or entity. Accordingly, with no other party involved—specifically, another PIC—a data sharing agreement is not necessary. The bank must remain mindful that even if a data sharing agreement is not necessary, the processing of its personal data, including that of providing access to the head office and other branches, must adhere to data privacy principles, be adequately secured, and should remain subject to the exercise of data subjects of their rights.

Section 3(m) and (n), IRR

Please confirm: With respect to individual customers, a bank that collects data directly from customers acts as a PIC. On the other hand, a bank that collects data from a corporate client, which provides the personal data of its officers who are authorized to open and/or operate the client's account, is considered a PIP. In the latter case, the corporate client, which instructs the bank to process personal data, is considered the PIC.

A PIC refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.[15] Thus, in the two (2) scenarios provided:

a. Where a bank collects personal data directly from its individual clients or customers, the bank is considered the PIC vis-à-vis such data.

b. Where a bank processes the personal data of its (corporate) client's officers who are authorized to open and/or operate the client's account, the bank remains to be a PIC. A bank is considered a PIC relative to all personal data it processes, regardless of the source of data. The bank presumably received these personal data for purposes of processing activities necessary for the bank to perform its primary functions. It is the bank that retains control over how the personal data of the client's officers will be processed within the bank, and for what purpose. The bank may be considered a PIP if it processes the personal data in behalf of the client or under the client's instructions, where the processing could have been performed by the client for its own purposes had it not been outsourced to the bank. Even in these cases, where the bank merely functions as a PIP, it does not preclude a situation wherein the bank shall be deemed

[14] IRR, §3(f).

[15] IRR, §3(m).

a PIC relative to such data. If, for instance, it uses such data for its own purposes (e.g., marketing activities), then it ceases to be a mere PIP, having exercised control over the processing of the data.

Section 19(a)(1), IRR

The requirement that consent be time-bound needs to be reconsidered given that it is highly impractical for business operations. The time lapse for each relevant client will differ and will require suspension of business once consent expires. Monitoring of the expiration and temporary cessation of business relative to each customer is arduous for business continuity. Adjustment is necessary to align the intention behind this requirement with standard business practices. Also, it is not necessary to make consent time bound as everyone can withdraw consent anytime.

Section 19(a)(1) of the IRR provides that:

> "1. Consent is required prior to the collection and processing of personal data, subject to exemptions provided by the Act and other applicable laws and regulations. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn."

As stated earlier, the time-bound nature of consent does not necessarily mean a specific date or period of time has to be declared relative thereto. The language of the provision is broad enough to accommodate scenarios wherein the duration or term of the consent is determined, *inter alia*, by law, contract, the type of processing involved, or the purpose thereof. This view is adopted for all sectors including that of banking and commercial institutions.

That consent may be withdrawn by the data subject has no bearing on the time-bound limitation thereon. While both are designed to uphold a right of the data subject, they exist independently and the significance of one is, in no way, contingent on the other's. Both afford a data subject control over his or her personal data. One allows a data subject to stop the processing of his or her personal data through an overt or explicit act. The other, while resulting in the same outcome, need not be prompted, triggered or initiated by the data subject.

The purging of data from bank processing systems will require significant resources. In lieu of disposing of data, can banks instead mask personal data in such a way that unmasked data, whether singly or collectively, will not lead to identification of clients?

Among the DPA's general principles on the processing of personal information, are provisions that take up data retention and disposal. In particular, Sections 11(e) and (f) of the law provides that personal data shall be:

> "e. Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and
>
> f. 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 be processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further, That adequate safeguards are guaranteed by said laws authorizing their processing."

These are complemented by Sections 19(d)(3), (e)(2) and (e)(3) of the IRR, *to wit*:

> "3. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.
>
> xxx xxx xxx
>
> 2. Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose.
>
> 3. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined."

In brief, these provisions all serve to underscore a number of key points: (1) retention of personal data shall only be allowed when necessary to the purpose for which they were collected; (2) absent such necessity, the personal data must be disposed of or deleted properly; and (3) longer retention periods may be allowed in a few, specific instances (e.g., for historical, statistical purposes, when required by law, etc.) or when personal data is converted to non-personal data permanently (i.e., aggregated, anonymized) or temporarily (i.e., pseudonymized).

Data masking is a type of security measure common in data protection regimes. It is sometimes referred to as "the act of replacing sensitive data with their non-sensitive, 'masked' equivalent while maintaining the quality and consistency needed to ensure that the masked data is still valuable to operational analysts or software developers."[16] It forms part of the broader concept of "pseudonymisation," which is defined as "the processing of personal data in a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."[17] The aim is to protect confidential information that directly or indirectly reveals an individual's identity.[18]

From these, it is clear that data masking is but a tool to protect and secure personal data while still being retained or kept by a PIC or PIP. The personal data itself remains available, once its

[16] Kevin Lonergan, *Why companies need pseudonymisation and data masking for GDPR compliance*, 17 June 2016, http://www.information-age.com/why-companies-need-pseudonymisation-and-data-masking-gdpr-compliance-123461628/

[17] Regulation (EU) 2016/679, §4(5).

[18] *id*.

use is called for. With that, this method will, at best, only allow longer retention periods on certain occasions. It does not provide legal cover for keeping personal data in perpetuity (i.e., even when the purpose of its collection has long been accomplished).

The enumeration of conditions for lawful processing is stated in the alternative; hence, any one of the conditions will support processing by banks of personal data. This said, please confirm if, in a case where processing relates to, or results from, services requested by a client from a bank, the consent of the data subject is not required.

Any one of the conditions for lawful processing may support processing by banks of personal data. Where only personal information, as opposed to sensitive personal or privileged information is involved, processing is permitted unless prohibited by law. This includes processing of personal information necessary and related to the fulfillment of a contract with the data subject, including services requested by a data subject from a bank. This criteria for lawful processing does not apply to sensitive personal or privileged information, where, as a general rule, the processing is prohibited.

On the assumption that the scenario contemplated is one where a corporate client of the bank has given the latter access to the personal data of its personnel, and the bank must process such data to deliver the services requested by the corporate client, both bank and client may be functioning as personal information controllers. On the part of the corporate client, it must establish the legal basis for allowing the bank to access the personal data of its personnel. On the part of the bank, it must establish legal basis for the further processing of personal data for purpose of delivering services. Legal basis may consist of any of the conditions set out in the law, such as securing the consent of the data subject (personnel). In the alternative, if the services requested by the corporate client is limited to processing services that has been outsourced to the bank, the arrangement will be covered by Rule X of the IRR on "Outsourcing and Subcontracting Agreements." In this case, the responsibility for obtaining consent or establishing lawful criteria for processing falls on the corporate client as PIC.

Section 34(a), IRR

Clarification is required to inform PICs/PIPs as to the application of requirements vis-à-vis existing clients whose personal information are already held by the PICs/PIPs. It may be necessary to provide a "grandfathering" clause, which would expressly provide that data collected before the enactment date of the law is exempt if it is used for the same purposes.

Section 16(a) and (b) of the DPA, as implemented by Section 34(a) of the IRR, relates to the right of a data subject to be informed of the processing of his or her personal data, and the concomitant duty of a PIC to make such notification. In general, notification must be undertaken prior to processing; however, if this is not possible, it must be made at the next practical opportunity.

Where the personal data of data subjects have already been processed or are being processed by a PIC or PIP prior to the enactment of the DPA, the duty to notify the affected data subjects arose only when the DPA itself became effective. A "grandfathering clause" is not necessary since the law itself allows for notification to be conducted *a posteriori* or even when data processing is already underway (i.e., at the next practical opportunity).

Section 34(c), IRR

The parameters of or limitations to the right to access have to be made clear. For instance, in the case of banks, does the right apply only in cases of clients with accounts that are open and operational (should not apply to closed accounts)?

A data subject has the right to access specific information relative to the processing of his or her personal data. This, *inter alia*, allows the data subject to determine or verify the lawfulness of the processing being carried out as regards his or her personal data.[19]

Except for the conditions set out in the DPA and its IRR, there are currently no other restrictions to this right. Thus, PICs (i.e., banks) are required to provide a data subject with reasonable access to his or her personal data that are being kept or retained by them. Among others, this allows the data subject to challenge the reason or basis of the data retention, notwithstanding the closure of his or her account.

For consistency, the period for which data is requested should be limited to record retention period.

Consistent with the view above, the right to access a data subject is entitled to under the DPA and its IRR remains while personal data or records relating to him or her are still being processed and retained by the PIC or PIP. To limit such access only within the declared retention period would defeat the objective of giving the data subject the opportunity to challenge the reason or basis for the processing of his or her personal data should it be kept and processed beyond the said retention period.

How often can the data subject access information relative to his or her personal data?

As yet, there are no rules governing the frequency with which a data subject may request access to information relating to the processing of his or her personal data. In some jurisdictions, at least, such request may be made at reasonable intervals.[20] What is considered "reasonable" is reckoned on a case to case basis. Barring any further guidance from the NPC on this matter, PICs or PIPs are accorded the discretion to determine what would constitute a reasonable interval, given the attendant facts of a particular case or request.

[19] *see*: REGULATION (EU) 2016/679, Whereas Clause (63).

[20] *see*: DIRECTIVE 95/46/EC, Article 12(a).

Can banks collect a reasonable processing fee should clients require access to information for more than an agreed frequency (e.g., once a year), considering the cost that may be required to retrieve data?

While the DPA is silent as to whether PICs may charge a fee for an access request by a data subject, experience from other jurisdictions[21] suggests that a reasonable processing fee may be collected to defray the administrative cost of addressing or responding to such a request. This is particularly true, if it will entail the reproduction and release of a significant amount of records or documents, and/or the data subject has made multiple requests involving the same data set.

Regarding a data subject's right to order the removal or destruction of his or her personal data, it should be made clear how this requirement will be reconciled with the legal or regulatory requirements on data retention.

Section 16(e) of the DPA, as implemented by Section 34(e) of the IRR, provides for the data subject's right to erasure or blocking upon discovery and substantial proof that his or her personal information is incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected, among others.

As would be the case with other provisions of the DPA, said directives should be read in conjunction with—and reconciled, if necessary—other applicable policies, whether contained in the same law or in another to bring about a result that is most consistent with the rationale for the law. Accordingly, a data subject may not be able to insist on the removal or destruction of his or her personal data in the custody of a PIC, while the latter is obliged to keep or retain the same by law or some other legal authority.

Section 40, IRR

The Rule implies that notification of the Commission and the data subject need not be simultaneously made; it seems that delay in notification vis-a-vis affected data subjects may be allowed in certain instances. Please confirm for proper guidance.

Where a personal data breach warrants notification, a PIC or PIP need not simultaneously notify the NPC and the affected data subjects. This much is evident in the language of IRR, Section 40 and its subsections. Subsection (c) thereof states that the NPC may allow the PIC or PIP to postpone the notification of affected data subjects, if this will negatively affect an ongoing criminal investigation involving the breach. Meanwhile, under subsection (b), the NPC may even authorize the PIC or PIP to dispense altogether with the obligation to notify

[21] REGULATION (EU) 2016/679, Article 15(3).

the affected data subjects, if, in its view, such notification will not be in the interest of the public or that of the data subjects themselves.

How will this determination (whether to delay notification) be made? Will a PIC verbally consult the Commission on the need to delay (formal) notice to both the Commission and data subject?

It is recommended that the PIC notify NPC within seventy-two (72) hours upon knowledge of or reasonable belief that a personal data breach has occurred based on available information. The PIC may then request the NPC additional time to provide the complete report. If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller may also request the Commission for postponement of or an exemption from the notification of data subjects.

Section 17(b) of NPC Circular 16-03 on breach management contemplates a scenario wherein a PIC has been remiss in its duty to promptly notify the NPC regarding a personal data breach incident. On such occasion, once the PIC belatedly notifies the Commission, the latter will make a determination whether the delay was warranted and/or may be excused. The section provides:

> *(b) Delay in Notification*. Notification may only be delayed to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.
>
> The personal information controller need not be absolutely certain of the scope of the breach prior to notification. Its inability to immediately secure or restore integrity to the information and communications system shall not be a ground for any delay in notification, if such delay would be prejudicial to the rights of the data subjects.
>
> Delay in notification shall not be excused if it is used to perpetuate fraud or to conceal the personal data breach.

Under Section 17(c) of NPC Circular 16-03, there shall be no delay if the breach involves at least 100 data subjects or when disclosure of sensitive personal information will harm or adversely affect the data subject

For additional guidance, Section 20 of NPC Circular 16-03 provides:

> **SECTION 20.** ***Failure to Notify***. In case the personal information controller fails to notify the Commission or data subjects, or there is unreasonable delay to the notification, the Commission shall determine if such failure or delay is justified. Failure to notify shall be presumed if the Commission does not receive notification from the personal information controller within five (5) days from knowledge of or upon a reasonable belief that a personal data breach occurred.

Section 41(b), IRR

Security incidents that should be reported to the Commission should be limited to those involving personal data. Incidents not involving personal data are beyond the scope of the DPA. For Banks, this will fall under the jurisdiction of the BSP. Please provide a format for the incident and annual report of breaches.

Section 41(b) of the IRR provides:

> "All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of personal data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the personal information controller. <u>In other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the Commission. A general summary of the reports shall be submitted to the Commission annually</u>." (underscoring supplied)

The determination of whether the security incident involves matters affecting personal data may be done by the NPC pursuant to its primary jurisdiction on privacy and data protection, and its mandate to ensure that PICs and PIPs comply with the DPA, its IRR and related issuances. Reports on security incidents provide insight on the existing security measures within a PIC, as well as documentation of threats that affect a particular industry or sector. As may be gleaned from the foregoing, a security incident that does not involve personal data must still be properly documented by the concerned PIC or PIP through a report containing aggregated data. This report need not be submitted to the NPC, unless specifically requested by the latter. What must be submitted to the NPC on an annual basis is a *general summary* of all reports prepared by the PIC or PIP regarding the data breaches and security incidents that occur on any given year.

Section 46, IRR

The registration requirement is very onerous. It should be removed as it is not included in the DPA. In this jurisdiction, it is a fundamental legal tenet that in case of a discrepancy between a basic law and a rule or regulation issued to implement it, the basic law prevails.[22] *Rules that go beyond the basic law it seeks to implement are declared null and void.*

Sections 46 and 47 of the IRR provide for the requirement to register with the NPC the data processing systems of PICs and PIPs that meet the preset criteria. This mechanism is akin to

[22] *see*: *Commissioner of Internal Revenue v. Bicolandia Drug Corporation (Formerly known as Elmas Drug Co.)*, G.R. No. 148083, 21 July 2006.

the "notification of personal data processing systems" requirement currently found in other jurisdictions with similar data protection regimes. As in most other cases, the purpose thereof is threefold: (1) to ensure that PICs and PIPs provide for adequate safeguards to protect the personal data of data subjects; (2) to promote transparency and public accountability; and (3) to provide data subjects the opportunity to contest inaccurate, unauthorized, or abusive data processing activities.

As the statutory authority charged with administering and implementing the provisions of the DPA,[23] the Commission firmly believes that it is well within its mandate to impose a registration system for data processing systems, in line with its critical function of monitoring and ensuring the compliance by PICs and PIPs with the DPA.[24]

Section 47, IRR

Please confirm that, where a foreign bank has a branch in the Philippines, the registration of data processing systems requirement is limited only to the processing systems of the Philippine branch, and that only the employees of the Philippine branch will be counted in determining whether the 250-employee threshold has been reached.

As per Section 47 of the IRR, when reconciled with the next preceding provision, only data processing systems <u>operating in the Philippines</u> are required to be registered with the NPC, provided they meet the criteria outlined in the Rules.

As stated in Section 47 of the IRR, the registration of data processing systems is required for PICs or PIPs that employ at least two hundred fifty (250) individuals. For those who maintain a smaller workforce, a determination has to be made regarding the processing operations they carry out in order to confirm if they are completely exempt from registration. Indeed, they would still be required to register if the data processing they perform may be characterized as any of the following:

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

When determining the number of personnel for registration purposes, it is first important to ascertain the entity that shall be considered as PIC or PIP. Thus, in the example provided, it must be made clear whether the foreign bank and its Philippine counterpart are treated as one or two separate legal entities. In the case of the latter, only the branch's employees shall be counted in order determine if the 250-person threshold has been reached. Note the discussion above regarding the relationship between a foreign head office and its local branch.

Please confirm if processing by a bank of its employees'

[23] RA 10173, §4.

[24] *see*: RA 10173, §4(a) and (e).

and/or applicants' personal data is occasional and is not likely to pose a risk to the rights and freedoms of data subjects.

For the purpose of data processing system registration, the processing by a bank of its employees' and/or applicants' personal data is not considered an occasional processing activity. Processing will be considered occasional only if the processing is incidental, occurring only under specific circumstances and not regularly performed. In addition, any processing integral to the core activities of the PIC will not be considered occasional. To the extent that the processing of personal data of employees and applicants involve sensitive personal information, and other information that could be used for identity fraud, the processing may likewise pose a risk to the rights and freedoms of data subjects. These are general principles, subject to further evaluation, on a case to case basis.

Section 68, IRR

Are covered entities given a 1-year grace period to be fully compliant with the Rules?

The one-year period provided in Section 67 of the IRR refers only to the registration of data processing systems, and automated processing operations that are subject to the notification requirement[25]. The other provisions and/or requirements of the Rules must be complied with as soon as the Rules became effective on 9 September 2016.

For your reference.

Very truly yours,

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

[25] IRR, §48.