Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-35

27 July 2017

[redacted]

Re: CLARIFICATIONS ON THE DATA PRIVACY ACT (DPA) AND ITS IMPLEMENTING RULES AND REGULATIONS (IRR)

Dear [redacted],

This is with regard to your inquiry received by the National Privacy Commission (NPC) on 1 March 2017, on the following matters:

1. What does the following opening paragraph of Section 5 of the IRR mean? How do we interpret or implement this?

   "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:"

2. How do we interpret the definition of sensitive personal information particularly with respect to offenses committed or alleged to have been committed (Sec. 3(t)(2), IRR)? Are we not allowed to publish reports on cases or complaints filed by PDIC in court or other tribunal? If not, how can we inform the public of such complaints filed by the PDIC?

3. What is the coverage of data sharing agreements? Are directives from other government authorities (e.g. GCG, CSC, BSP, etc.) covered by sharing agreements?

4. Do you have templates of the privacy impact assessment and data privacy manual? Are there other agencies (government or non-government) that have already submitted?

Exemptions to the scope of the DPA

The DPA provides for a list of specified information that are not covered by the law. Section 5 of the IRR[1] provides for the special cases wherein the law and the rules are not applicable:

[1] Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012" (24 August 2016).

"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:

a. Information processed for purpose of allowing public access to information that fall within matters of public concern, pertaining to:

    1. Information about any individual who is or was an officer or employee of government that relates to his or her position or functions, including:
    (a) The fact that the individual is or was an officer or employee of the government;
    (b) The title, office 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 he or she prepared in the course of his or her employment with the government;

    2. Information about an individual who is or was performing a service under contract for a government institution, but only in so far as it relates to such service, including the name of the individual and the terms of his or her contract;

    3. Information relating to a benefit of a financial nature conferred on an individual upon the discretion of the government, such as the granting of a license or permit, including the name of the individual and the exact nature of the benefit: *Provided*, that they do not include benefits given in the course of an ordinary transaction or as a matter of right;

b. 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;

c. Personal information that will be processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards;

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);

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;

f. Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines. The burden of proving the law of the foreign jurisdiction falls on the person or body seeking exemption. In the absence of proof, the applicable law shall be presumed to be the Act and these Rules:

> *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).

The exemptions above are not blanket exemptions. These are limited to the minimum extent necessary to achieve the specific purpose, function or activity.

This is interpreted to the effect that there is a presumption that personal data may be lawfully processed by a personal information controller or processor under the special cases provided above, but the processing shall be limited to achieving the specific purpose, function or activity, and that the personal information controller or processor remains to be subject to the requirements of implementing measures to secure and protect personal data.

For instance, 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. 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.

Processing of sensitive personal information

The processing of sensitive personal information[2] is prohibited except in the following cases:[3]

(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;

[2] RA No. 10173, §3(l) Sensitive personal information refers to personal information:
1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. Issued by government agencies peculiar to an individual which includes, but not limited to social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4. Specifically established by an executive order or an act of Congress to be kept classified.

[3] *Id.*, §13

(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.

From the foregoing, we believe that PDIC's processing of sensitive personal information, which may include the publication of reports containing the same, is allowed under Section 13(b) and (f) above, *i.e.* the processing of the same is provided for by existing laws and regulations, and 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, respectively.

If it is within the mandate of the PDIC to publish reports on cases or complaints filed by the PDIC in order to inform the public, the DPA will not operate to hinder the said mandate.

We note however that there may be a need to check other pertinent laws, jurisprudence, rules and regulations which provide for the confidentiality of records of court proceedings. or information from proceedings.

Data sharing agreements

Data sharing is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor.[4] Data sharing between government agencies for the purpose of a public function or provision of a public service shall be covered a data sharing agreement.[5]

A data sharing agreement 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 parties.[6]

It is possible that directives from government agencies performing regulatory functions will be covered by the data sharing provisions of the IRR and NPC Circular No. 16-02 on data sharing agreements involving government agencies.

However, for a better understanding of the facts, it may be advisable to provide us with additional information on the specific directives and government agencies involved in the sharing of personal data.

Templates of the privacy impact assessment and data privacy manual

There is no prescribed standard or format for a PIA. As such, the PIC or PIP may determine the structure and form of the PIA that it will use. It is not precluded from utilizing any existing methodology, provided the latter is acceptable based on the following criteria:

[4] IRR of RA No. 10173, §3(f)
[5] Id., §20(d)
[6] NPC Circular 16-02 dated 10 October 2016

1. It provides a systematic description of the personal data flow and processing activities of the PIC or PIP. This includes:

    1.) purpose of the processing, including, where applicable, the legitimate interest pursued by the PIC or PIP;
    2.) data inventory identifying the types of personal data held by the PIC or PIP;
    3.) sources of personal data and procedures for collection;
    4.) functional description of personal data processing, including a list of all information repositories holding personal data and their location, and types of media used for storage;
    5.) transfers of personal data to another agency, company, or organization, including transfers outside the country, if any;
    6.) storage and disposal method of personal data;
    7.) accountable and responsible persons involved in the processing of personal data; and
    8.) existing organizational, physical and technical security measures

2. It includes an assessment of the adherence by the PIC or PIP to the data privacy principles, the implementation of security measures, and the provision of mechanisms for the exercise by data subjects of their rights under the DPA.

3. It identifies and evaluates the risks posed by a data processing system to the rights and freedoms of affected data subjects, and proposes measures that address them.

    1.) *Risk identification*. Risks include natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.
    2.) *Risks evaluation based on impact and likelihood*. The severity or extent of the impact of a breach or privacy violation on the rights and freedoms of data subjects must be determined. The probability of the risk happening and the sources of such risk should also be taken into consideration.
    3.) *Remedial measures*. Based on an assessment of risks, measures should be proposed on how to address and manage the said risks.

4. It is an inclusive process, in that it ensures the involvement of interested parties and secures inputs from the DPO and data subjects.

Note that the NPC is not requiring the submission of PIAs or manuals from personal information controllers or processors. However, during the course an investigation or audit, the same may be required to be presented to the NPC pursuant to compliance or enforcement orders which may be issued.

For your reference.

Sincerely,

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman