Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Advisory No. 2017-03

DATE : 31 July 2017

SUBJECT : GUIDELINES ON PRIVACY IMPACT ASSESSMENTS

Preamble

WHEREAS, Article II, Section 11 of the 1987 Constitution declares that the State values the dignity of every human person and guarantees full respect for human rights, and Article XIII, Section 21 states that Congress shall give highest priority to the enactment of measures that protect and enhance the right of the people to human dignity. At the same time, enshrined in jurisprudence is the recognition of the right to privacy as a right fully deserving of constitutional protection;

WHEREAS, Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), provides that it is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth. The State also recognizes its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected;

WHEREAS, Section 20(c) of the DPA and Section 29 of its Implementing Rules and Regulations (IRR) provide that the determination of the appropriate level of security for an agency or organization processing personal data shall take into account the nature of the personal information to be protected, the risks represented by the processing to the rights and freedoms of data subjects, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation;

WHEREAS, pursuant to Section 7 of the DPA, the National Privacy Commission (NPC) is mandated to administer and implement the provisions of the DPA, monitor and ensure compliance of the country with international standards set for data protection, and coordinate with government agencies and the private sector on efforts to formulate and implement plans and policies that strengthen the protection of personal information in the country;

WHEREAS, Sections 4, 5, and 6 of NPC Circular 2016-01 requires government agencies to conduct a Privacy Impact Assessment (PIA) for each program, process, or measure within the agency that involves personal data. At the same time, Section 6 of NPC Circular 2016-03 recommends the conduct of a PIA as part of any organization's security incident management policy.

WHEREFORE, in consideration of the foregoing premises, the NPC hereby issues this Advisory that prescribes guidelines for the conduct of a Privacy Impact Assessment:

Scope

This Advisory shall apply to all natural or juridical persons, or any other body in the government or private sector engaged in the processing of personal data within and outside of the Philippines, subject to the applicable provisions of the DPA, its IRR, and other relevant issuances of the NPC.

Definition of Terms

For the purpose of this Advisory, the following terms are defined, as follows:

A. "Act" or "DPA" refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;

B. "Commission" or "NPC" refers to the National Privacy Commission;

C. "Compliance Officer for Privacy" or "COP" refers to an individual that performs some of the functions of a DPO, as provided in NPC Advisory No. 17-01;

D. "Control Framework" refers to a comprehensive enumeration of measures a PIC or PIP has established for the protection of personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination;

E. "Data Protection Officer" or "DPO" refers to an individual designated by the head of agency or organization to be accountable for its compliance with the Act, its IRR, and other issuances of the Commission: *Provided*, that, except where allowed otherwise by law or the Commission, the individual must be an organic employee of the government agency or private entity: *Provided further*, that a government agency or private entity may have more than one DPO;

F. "IRR" refers to the Implementing Rules and Regulations of the DPA;

G. "Personal data" refers to all types of personal information, including privileged information;

H. "Personal information" refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual;

I. "Personal information controller" or "PIC" refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

1.) a person or organization who performs such functions as instructed by another person or organization; or
2.) an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs;

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;

J. "Personal information processor" or "PIP" refers to any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject;

K. "Privacy Impact Assessment" is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a PIC or PIP program, project, process, measure, system or technology product of a PIC or PIP. It takes into account the nature of the personal data to be protected, the personal data flow, the risks to privacy and security posed by the processing, current data privacy best practices, the cost of security implementation, and, where applicable, the size of the organization, its resources, and the complexity of its operations;

L. "Privacy Management Program" refers to a process intended to embed privacy and data protection in the strategic framework and daily operations of a personal information controller or personal information processor, maintained through organizational commitment and oversight of coordinated projects and activities.

M. "Privileged Information" refers to any and all forms of data which, under the Rules of Court and other pertinent laws, constitute privileged communication;

N. "Processing" refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data;

O. "Risk" refers to the potential of an incident to result in harm or danger to a data subject or organization;

P. "Risk Rating" refers to a function of the probability and impact of an event;

Q. "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;

R. "Threat" refers to a potential cause of an unwanted incident, which may result in harm or danger to a data subject, system, or organization;

S. "Vulnerability" refers to a weakness of a data processing system that makes it susceptible to threats and other attacks.

General Principles

A Privacy Impact Assessment (PIA) helps a PIC and PIP navigate the process of understanding the personal data flows in the organization. It identifies and provides an assessment of various privacy risks, and proposes measures intended to address them.

The identification of risks and the use of a control framework for risk management should consider existing laws, regulations, and issuances relevant to privacy and data protection, as well as the rights of data subjects. The most appropriate standard recognized by the sector or industry of the PIC or PIP, as well as that of the information and communications technology industry shall also be considered.

Key Considerations

In general, a PIA should be undertaken for every processing system of a PIC or PIP that involves personal data. It may also be carried out vis-à-vis the entire organization of the PIC or PIP with the involvement or participation of the different process owners and stakeholders.

A PIA should be conducted for both new and existing systems, programs, projects, procedures, measures, or technology products that involve or impact processing personal data. For new processing systems, it should be undertaken prior to their adoption, use, or implementation. Changes in the governing law or regulations, or those adopted within the organization or its industry may likewise require the conduct of a PIA, particularly if such changes affect personal data processing.

A PIC may require a PIP or a service or product provider to conduct a PIA. For this purpose, the report prepared by the PIP or the service or product provider may be considered by the PIC in determining whether the former is able to provide a comparable level of protection to the processing of personal data.

A PIC or PIP may choose to conduct a single PIA for multiple data processing systems that involve the same personal data and pose similar risks. A single PIA may also be conducted on a data processing system where two or more PICs or PIPs are involved.

The PIC or PIP may forego the conduct of a PIA only if it determines that the processing involves minimal risks to the rights and freedoms of individuals, taking into account recommendations from the DPO. In making this determination, the PIC or PIP should consider the size and sensitivity of the personal data being processed, the duration and extent of processing, the likely impact of the processing to the life of data subject and possible harm in case of a personal data breach.

Objectives

The conduct of a PIA is intended to:

A. identify, assess, evaluate, and manage the risks represented by the processing of personal data;

B. assist the PIC or PIP in preparing the records of its processing activities, and in maintaining its privacy management program;

C. facilitate compliance by the PIC or PIP with the DPA, its IRR, and other applicable issuances of the NPC, by determining:
   a. its adherence to the principles of transparency, legitimate purpose and proportionality;
   b. its existing organizational, physical and technical security measures relative to its data processing systems;
   c. the extent by which it upholds the rights of data subjects; and

D. aid the PIC or PIP in addressing privacy risks by allowing it to establish a control framework;

In conducting a PIA, it is important that its results are properly documented in a report that includes information on stakeholder involvement, proposed measures for privacy risk management, and the process through which the results of the PIA will be communicated to internal and external stakeholders.

Responsibility

The PIC or PIP is primarily accountable for the conduct of a PIA. This responsibility remains even when it elects to outsource or subcontract the actual conduct of the activity. For this

purpose, the PIC or PIP may lay down a policy, which establishes the circumstances under which a PIA shall be carried out, including the personnel involved, the resources available, and the review process that will be undertaken.

A recommendation for the conduct of a PIA may also come from the DPO of the PIC or PIP. Part of the functions of a DPO is to ensure the conduct of PIA relative to activities, measures, projects, programs, or systems of the PIC or PIP. In case of disagreement between the DPO and its principal on the conduct of a PIA, this should be properly documented, particularly the reason for the conflicting views.

The extent of the involvement of the DPO in the PIA is left to the discretion of the PIC or PIP. The PIC or PIP may allow the DPO to actively take part in the PIA, or it may simply consult and seek his or her recommendations based on the results of the PIA.

Where the PIC or PIP has a COP, the involvement of the latter in the PIA shall also be determined by the PIC or PIP.

Stakeholder Involvement

Stakeholder involvement is important in the conduct of a PIA. This may be accomplished through their direct participation in the process, through consultations in a public forum or focus group discussions, or through the use of surveys and feedback forms.

Stakeholders may be involved in the whole process, or may be consulted for specific stages, such as in preparatory stage, during risk analysis and evaluation, or after the process during review that leads up to the preparation of the report.

The results of a PIA should be communicated to the stakeholders via a written report.

Structure and Form

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, [1] provided the latter is acceptable based on the following criteria:[2]

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;

[1] Acceptable methodologies include ISO/IEC 29134, which provides standards for the conduct of the PIA.

[2] This takes into consideration Art 29 Data Protection Working Party "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" (4 April 2017) and the provisions of the DPA.

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.

Planning a PIA

The following should be considered when planning the conduct of a PIA:

1. The PIC or PIP should signify its commitment to the conduct of a PIA. This means:

   a. deciding on the need for a PIA;
   b. assigning a person responsible for the whole process;
   c. providing resources to accomplish the objectives of the PIA; and
   d. issuing a clear directive for its conduct.

2. The program, project, process, measure, system or technology product on which a PIA will be conducted should be identified. The scope of the PIA must be clearly delineated.

3. The process owners, participants, and the persons in charge of conducting the PIA,

including the preparation of its report, should be identified. When the scope of the PIA is determined to be broad and/or comprehensive, a taskforce or secretariat may be necessary. The PIC or PIP may also outsource the conduct of the PIA, but great care should be taken in evaluating the adequacy and propriety of the methodology that will be utilized, and the expected outputs.

4. The PIC or PIP should determine how internal and external stakeholders will be involved.

5. Other matters that should be established:

    1.) objectives, schedules, and available resources;
    2.) means of communicating the results of the PIA to stakeholders; and
    3.) procedure for integrating the recommendations of the PIA into the control framework of the organization.

Preparatory Activities

The following should be considered in the preparatory activities leading up to the conduct of a PIA:

1. There should be records of the processing activities of the PIC or PIP, and an inventory of the personal data involved in such activities. For this purpose, a personal data flow should be created, starting from the collection of personal data, all the way up to its deletion or disposal, including storage. The process owners may be assigned to provide these documents prior to conduct of the PIA.

2. A preliminary assessment should be undertaken to determine baseline information, including existing policies and security measures of the organization. It is critical that this be carried out in coordination with the different units or offices of the organization, such as those in charge of compliance, quality management, records and information management, information technology, administration and planning, customer relations, and legal concerns.

3. Stakeholders may be consulted during the preparatory stage to identify their concerns, expectations, and perception of the risks posed by the processing activities of the organization. Existing reports may be considered, such as customer satisfaction surveys, internal audits, and other assessment activities.

4. The objectives, scope, and methodology of the PIA should be established. A control framework should be selected. For agencies that process the personal data records of more than one thousand (1,000) individuals, including agency personnel, the Commission recommends the use of the ISO/IEC 27002 and ISO/IEC 29151 control set as the minimum standard to assess any gaps in the agency's control framework.

5. The detailed plan for the conduct of the PIA should be prepared, including:

    1.) schedules and timelines for the completion of preparatory activities, conduct

of the PIA, and reporting or publication of results;
2.) approval of resource and budget allocations;
3.) participants and methods for stakeholder involvement;
4.) documentation and review process;
5.) other supporting documents.

Conduct of the PIA

The following should be considered in the conduct of a PIA:

1. The records of processing activities, the personal data inventory, and the personal data flows should all be evaluated to determine whether additional information are necessary for the proper conduct of a PIA. Taken together, these constitute the baseline information, along with the following:

    1.) purpose and legal basis of the processing activities, including data sharing and other forms of data transfers.;
    2.) persons responsible for processing personal data, including a list of those individuals with access thereto;
    3.) list of all information repositories and technology products used;
    4.) sources and recipients of personal data; and
    5.) existing policies, procedures and security measures relevant to personal data protection.

2. Once baseline information is complete, the processing activities should be evaluated against the legal obligations of the PIC or PIP, and the latter's chosen control framework.

3. The control framework should adhere to the data privacy principles. It should implement security measures and establish procedures for the proper exercise by data subjects of their rights. Privacy and data protection measures, whether planned and existing, should be considered.

4. The data processing systems of the PIC or PIP should be assessed to determine if there are gaps at any stage of the processing. There is a gap when:

    1.) there is a violation of any data privacy principle;
    2.) the organizational, physical, and technical security measures are inadequate to safeguard the confidentiality, availability, and/or integrity of personal data; or
    3.) the exercise of data subjects of their rights is not possible or restricted without legal basis.

5. Gaps should be evaluated to determine the risks involved to personal data, possible threats, and existing vulnerabilities of the systems. Risks include the following:

    1.) unauthorized or unlawful processing;

2.) confidentiality breach;
3.) integrity breach;
4.) availability breach; and
5.) violations of rights of data subjects

6. Risks, in turn, should be assessed to determine whether the breach or privacy violation it poses is likely to happen. The assessment should consider the processing operations of the PIC or PIP, vulnerabilities and threats, as well as existing safeguards, if any. A determination of how the risk will affect the rights and freedoms of data subjects should be done based on the amount and nature of personal data involved, and the impact of possible harm.

7. Measures to address the risks identified should be proposed. They may mitigate, accept, avoid, or transfer the risks posed by the processing, by taking into account the likelihood and impact of a breach or privacy violation, the available resources of the organization to address the risks, current data privacy best practices, and industry or sector standards. The proposed measures should include:

1.) risks and strategies for risk management;
2.) implementing activities, including definite plans and specific projects;
3.) controlling mechanisms to monitor, review, and support implementation;
4.) proposed time frame, expected completion, or schedules;
5.) responsible and accountable persons; and
6.) necessary and available resources.

8. Involvement of stakeholders should be documented.

9. The report featuring the results of the PIA should be reviewed before being finalized and approved. It should include the proposed measures that should serve as basis for implementing changes in the organization (e.g., new policies and procedures, security measures to strengthen data processing systems, etc.). The report should also include recommendations as to when the PIA will be updated and reviewed.

10. Results of the PIA should be reported to management and communicated to internal and external stakeholders. The PIC or PIP can limit the information provided to the public based on its legitimate interests, such as the legal, business operation, or security risks that disclosure may give rise to.

Documentation and Review

A PIA requires documentation and procedures for review. Its results should be contained in a corresponding report.

The PIC or PIP must maintain a record of all its PIA reports. When a report contains information that are privileged or confidential, the PIC or PIP may prepare a PIA Summary that can be made available to data subjects upon request. Other means of communicating the results of the PIA to internal and external stakeholders should be considered, such as

publishing key findings or result summaries in the PIC or PIP website, through newsletters, annual reports, and other similar materials.

A PIA should be evaluated every year. This, however, does not preclude the conduct of a new PIA on the same data processing system, when so required by significant changes required by law or policy, and other similar circumstances.

Compliance and Accountability

The conduct of a PIA is one of the ways a PIC or PIP is able to demonstrate its compliance with the DPA, its IRR, and related issuances of the NPC. It also represents a proactive approach to the management of risks represented by personal data processing by ensuring that the rights of data subjects are protected.

In the event a personal data breach occurs, or a complaint is filed by a data subject against the PIC or PIP, the conduct of a PIA shall be considered in evaluating if the PIC or PIP exercised due diligence in the processing of personal data.

When the NPC determines that a processing system of a PIC or PIP poses a significant risk to the rights and freedoms of data subjects, it may request for a copy of the PIA report regarding such system. When so requested, such copy shall also be made available to the Commission for compliance monitoring purposes.

Approved:

[Sgd] RAYMUND E. LIBORO
Privacy Commissioner

[Sgd] IVY D. PATDU
Deputy Privacy Commissioner

[Sgd] DAMIAN DOMINGO O. MAPA
Deputy Privacy Commissioner

Date: 31 July 2017