Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Circular 16-03

DATE : 15 December 2016
SUBJECT : PERSONAL DATA BREACH MANAGEMENT

WHEREAS, the Philippine Constitution guarantees respect for the right to privacy, including information privacy, accorded recognition as inherent in the freedoms enjoyed by every Filipino, and at the same time, Article II, Section 11 of the Constitution emphasizes that the State values the dignity of every human person and guarantees full respect for human rights;

WHEREAS, Article II, Section 24, of the Constitution provides that the State recognizes the vital role of communication and information in nation-building, and Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012, 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;

WHEREAS, there are increasing incidents of personal data breaches that impact both public and private entities, entailing significant economic and legal costs for those involved in processing of personal data and putting at risk data subjects for identity theft, crimes and other harm, and that in order to afford protection of personal data, reasonable and appropriate organizational, physical and technical measures should be implemented;

WHEREAS, Section 20(f) of the Act requires prompt notification of the National Privacy Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, which may likely give rise to a real risk of serious harm to any affected data subject;

WHEREAS, in order to ensure compliance of the country and all personal information controllers and personal information processors with the law and international standards set for data protections, and to safeguard against accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing, the management of personal data breach should include prevention, incident response, mitigation and compliance with notification requirements;

WHEREFORE, in consideration of these premises, the National Privacy Commission hereby issues this Circular governing personal data breach management.

RULE I.
GENERAL PROVISIONS

SECTION 1. ***Scope***. These Rules apply to any natural and juridical person in the government or private sector processing personal data in outside of the Philippines, subject to the relevant provisions of the Act and its Implementing Rules and Regulations.

SECTION 2. ***Purpose***. These Rules provide the framework for personal data breach management and the procedure for personal data breach notification and other requirements.

SECTION 3. ***Definition of Terms*****.** For the purpose of this Circular, the following terms are defined, as follows:

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

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

C. "Data Protection Officer" refers to an individual designated by the head of agency to be accountable for the agency's compliance with the Act: *Provided*, that the individual must be an organic employee of the government agency: *Provided further*, that a government agency may have more than one data protection officer;

D. "IRR" refers to the Implementing Rules and Regulations of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;

E. "Personal data" refers to all types of personal information;

F. "Personal data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:

1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
2. Integrity breach resulting from alteration of personal data; and/or
3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.

G. "Personal information controller" refers to a natural or juridical person, or any other body that controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

1. A natural or juridical person, or any other body that performs such functions as instructed by another person or organization; or
2. A natural person who processes personal data in connection with his or her 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;

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

I. "Privacy Impact Assessment" is a process undertaken and used by a government agency to evaluate and manage privacy impacts.

J. "Security incident" is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place;

K. "Security Incident Management Policy" refer to policies and procedures implemented by a personal information controller or personal information processor to govern the actions to be taken in case of a security incident or personal data breach;

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.

RULE II.
GUIDELINES FOR PERSONAL DATA BREACH MANAGEMENT

SECTION 4. ***Security Incident Management Policy*****.** A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure:

A. Creation of a data breach response team, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach;

B. Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident;

C. Implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system;

D. Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach; and

E. Compliance with the Act, its IRR, and all related issuances by the Commission pertaining to personal data breach notification.

SECTION 5. ***Data Breach Response Team*****.** A personal information controller or personal information processor shall constitute a data breach response team, which shall have at least one (1) member with the authority to make immediate decisions regarding critical action, if necessary. The team may include the Data Protection Officer.

The team shall be responsible for the following:

A. Implementation of the security incident management policy of the personal information controller or personal information processor;

B. Management of security incidents and personal data breaches; and

C. Compliance by the personal information controller or personal information processor with the relevant provisions of the Act, its IRR, and all related issuances by the Commission on personal data breach management.

The team must be ready to assess and evaluate a security incident, restore integrity to the information and communications system, mitigate and remedy any resulting damage, and comply with reporting requirements.

The functions of the Data Breach Response Team may be outsourced. Such outsourcing shall not reduce the requirements found in the Act, the IRR or related issuance. The Data Protection Officer shall remain accountable for compliance with applicable laws and regulations.

In cases where the Data Protection Officer is not part of the Data Breach Response Team, the Data Breach Response Team shall submit a written report addressed to the Data Protection Officer detailing the actions taken in compliance with these Rules.

RULE III.
GUIDELINES FOR THE PREVENTION OF PERSONAL DATA BREACH

SECTION 6. ***Preventive or Minimization Measures.*** A security incident management policy shall include measures intended to prevent or minimize the occurrence of a personal data breach. Such safeguards may include:

A. Conduct of a privacy impact assessment to identify attendant risks in the processing of personal data. It shall take into account the size and sensitivity of the personal data being processed, and impact and likely harm of a personal data breach;

B. Data governance policy that ensures adherence to the principles of transparency, legitimate purpose, and proportionality;

C. Implementation of appropriate security measures that protect the availability, integrity and confidentiality of personal data being processed;

D. Regular monitoring for security breaches and vulnerability scanning of computer networks;

E. Capacity building of personnel to ensure knowledge of data breach management principles, and internal procedures for responding to security incidents;

F. Procedure for the regular review of policies and procedures, including the testing, assessment, and evaluation of the effectiveness of the security measures.

SECTION 7. ***Availability, Integrity and Confidentiality of Personal Data***. The implementation of security measures shall be in accordance with the Act, its IRR, and other issuances of the Commission. The security measures should be directed to ensuring the availability, integrity, and confidentiality of the personal data being processed, and may include:

A. Implementation of back-up solutions;

B. Access control and secure log files;

C. Encryption;

D. Data disposal and return of assets policy.

RULE IV.
GUIDELINES FOR INCIDENT RESPONSE POLICY AND PROCEDURE

SECTION 8. ***Policies and Procedures***. The personal information controller or personal information processor shall implement policies and procedures for guidance of its data breach response team and other personnel in the event of a security incident. These may include:

A. A procedure for the timely discovery of security incidents, including the identification of person or persons responsible for regular monitoring and evaluation of security incidents;

B. Clear reporting lines in the event of a possible personal data breach, including the identification of a person responsible for setting in motion the incident response procedure, and who shall be immediately contacted in the event of a possible or confirmed personal data breach;

C. Conduct of a preliminary assessment for purpose of:

   1. Assessing, as far as practicable, the nature and scope of the personal data breach and the immediate damage
   2. Determining the need for notification of law enforcement or external expertise; and
   3. Implementing immediate measures necessary to secure any evidence, contain the security incident and restore integrity to the information and communications system;

D. Evaluation of the security incident or personal data breach as to its nature, extent and cause, the adequacy of safeguards in place, immediate and long-term damage, impact of the breach, and its potential harm and negative consequences to affected data subjects;

E. Procedures for contacting law enforcement in case the security incident or personal data breach involves possible commission of criminal acts;

F. Conduct of investigations that will evaluate fully the security incident or personal data breach;

G. Procedures for notifying the Commission and data subjects when the breach is subject to notification requirements, in the case of personal information controllers, and procedures for notifying personal information controllers in accordance with a contract or agreement, in the case of personal information processors; and

H. Policies and procedures for mitigating the possible harm and negative consequences to a data subject in the event of a personal data breach. The personal information controller must be ready to provide assistance to data subjects whose personal data may have been compromised.

SECTION 9. ***Documentation.*** All actions taken by a personal information controller or personal information processor shall be properly documented. Reports should include:

A. Description of the personal data breach, its root cause and circumstances regarding its discovery;

B. Actions and decisions of the incident response team;

C. Outcome of the breach management, and difficulties encountered; and

D. Compliance with notification requirements and assistance provided to affected data subjects.

A procedure for post-breach review must be established for the purpose of improving the personal data breach management policies and procedures of the personal information controller or personal information processor.

SECTION 10. ***Regular Review*****.** The incident response policy and procedure shall be subject to regular revision and review, at least annually, by the Data Protection Officer, or any other person designated by the Chief Executive Officer or the Head of Agency, as the case may be. The date of the last review and the schedule for the next succeeding review must always be indicated in the documentation of the incident response policy and procedure.

RULE V.
PROCEDURE FOR PERSONAL DATA BREACH NOTIFICATION AND OTHER REQUIREMENTS

SECTION 11. ***When notification is required*****.** Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.

   For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

B. There is reason to believe that the information may have been acquired by an unauthorized person; and

C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

SECTION 12. ***Public Information*****.** A claim that the data involved in a breach is public information will not automatically exempt a personal information controller from the notification requirements provided herein. When the level of availability or publicity of the personal data is altered by a personal data breach, it shall be considered as a personal data breach requiring notification, subject to the preceding paragraphs.

SECTION 13. ***Determination of the Need to Notify***. Where there is uncertainty as to the need for notification, the personal information controller shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particulary of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred.

The personal information controller shall also consider if the personal data reasonably believed to have been compromised involves:

A. Information that would likely affect national security, public safety, public order, or public health;

B. At least one hundred (100) individuals;

C. Information required by applicable laws or rules to be confidential; or

D. Personal data of vulnerable groups.

SECTION 14. ***Discovery of Vulnerability***. A discovery of a vulnerability in the data processing system that would allow access to personal data shall prompt the personal information controller or the personal information processor, as the case may be, to conduct an assessment and determine if a personal data breach has occurred.

SECTION 15. ***Who should Notify*****.** The personal information controller shall notify the Commission and the affected data subjects upon knowledge of, or when there is reasonable belief that a personal data breach has occurred. The obligation to notify remains with the personal information controller even if the processing of information is outsourced or subcontracted to a personal information processor.

The personal information controller shall identify the designated data protection officer or other individual responsible for ensuring its compliance with the notification requirements provided in this Circular.

SECTION 16. ***Reporting by Personal Information Processors*****.** To facilitate the timely reporting of a personal data breach, the personal information controller shall use contractual or other reasonable means to ensure that it is provided a report by the personal information processor upon the knowledge of, or reasonable belief that a personal data breach has occurred.

SECTION 17. ***Notification of the Commission*****.** The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:

A. *When Notification Should be Done*. The Commission shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.

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.

C. *When delay is prohibited.* There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days, unless the personal information controller is granted additional time by the Commission to comply.

D. *Content of Notification*. The notification shall include, but not be limited to:

   1. Nature of the Breach
      a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
      b. a chronology of the events leading up to the loss of control over the personal data;
      c. approximate number of data subjects or records involved;
      d. description or nature of the personal data breach;
      e. description of the likely consequences of the personal data breach; and

f. name and contact details of the data protection officer or any other accountable persons.

2. Personal Data Possibly Involved
   a. description of sensitive personal information involved; and
   b. description of other information involved that may be used to enable identity fraud.

3. Measures Taken to Address the Breach
   a. description of the measures taken or proposed to be taken to address the breach;
   b. actions being taken to secure or recover the personal data that were compromised;
   c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
   d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
   e. the measures being taken to prevent a recurrence of the incident.

The Commission reserves the right to require additional information, if necessary.

E. *Form.* Notification shall be in the form of a report, whether written or electronic, containing the required contents of notification: *Provided*, that the report shall also include the name and contact details of the data protection officer and a designated representative of the personal information controller: *Provided further*, that, where applicable, the manner of notification of the data subjects shall also be included in the report.

Where notification is transmitted by electronic mail, the personal information controller shall ensure the secure transmission thereof.

Upon receipt of the notification, the Commission shall send a confirmation to the personal information controller. A report is not deemed filed without such confirmation. Where the notification is through a written report, the received copy retained by the personal information controller shall constitute proof of such confirmation.

SECTION 18. ***Notification of Data Subjects***. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:

A. *When should notification be done*. The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.

The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.

B. *Exemption or Postponement of Notification*. If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification.

A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects.

The Commission may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.

C. *Content of Notification*. The notification shall include, but not be limited to:

1. nature of the breach;
2. personal data possibly involved;
3. measures taken to address the breach;
4. measures taken to reduce the harm or negative consequences of the breach;
5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
6. any assistance to be provided to the affected data subjects.

Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.

D. *Form.* Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.

The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.

SECTION 19. ***Exemption from Notification Requirements***. The following additional factors shall be considered in determining whether the Commission may exempt a personal information controller from notification:

A. Security measures that have been implemented and applied to the personal data at the time the personal data breach was reasonably believed to have occurred, including measures that would prevent use of the personal data by any person not authorized to access it;

B. Subsequent measures that have been taken by the personal information controller or personal information processor to ensure that the risk of harm or negative consequence to the data subjects will not materialize;

C. Age or legal capacity of affected data subjects: *Provided*, that in the case of minors or other individuals without legal capacity, notification may be done through their legal representatives.

In evaluating if notification is unwarranted, the Commission may take into account the compliance by the personal information controller with the law and existence of good faith in the acquisition of personal data.

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 21. ***Investigation of a Breach or a Security Incident***. Depending on the nature of the incident, or if there is failure or delay in the notification, the Commission may investigate the circumstances surrounding a personal data breach. Investigations may include on-site examination of systems and procedures.

If necessary, the Commission shall require the cooperation of concerned parties, or compel appropriate action therefrom to protect the interests of data subjects.

The investigation under this Section shall be governed by the Rules of Procedure of the Commission.

Section 22. ***Reportorial requirements***. All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the event of a personal data breach, a report shall include the facts surrounding the incident, the effects of such incident, and the remedial action taken by the personal information controller. For other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation.

Any or all reports shall be made available when requested by the Commission: *Provided*, that a summary of all reports shall be submitted to the Commission annually, comprised of general information including the number of incidents and breach encountered, classified according to their impact on the availability, integrity, or confidentiality of personal data.

Section 23. ***Notification and Reporting to the National Privacy Commission***. The requirements pertaining to notification and the submission of reports shall be complied with through the appropriate submissions to the office of the National Privacy Commission or by electronic mail (complaints@privacy.gov.ph). The foregoing details may be amended, subject to a public announcement made through the Commission's website or other comparable means.

SECTION 24. ***Separability Clause***. If any portion or provision of this Circular is declared null and void or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 25. ***Effectivity***. This Order shall take effect fifteen (15) days after publication in the Official Gazette or two newspapers of general circulation.

Approved:

(Sgd.) RAYMUND E. LIBORO
Privacy Commissioner

(Sgd.) IVY D. PATDU
Deputy Privacy Commissioner

(Sgd.)DAMIAN DOMINGO O. MAPA
Deputy Privacy Commissioner

Date: December 15, 2016

Summary	
What is subject to the notification requirements.	A security breach that: 1. Involves sensitive personal information, or information that may be used to enable identity fraud 2. There is reason to believe that information have been acquired by an unauthorized person 3. The unauthorized acquisition is likely to give rise to a real risk of serious harm
Who should notify.	The personal information controller, which controls the processing of information, even if processing is outsourced or subcontracted to a third party.
When should notification of Commission be done.	Within 72 hours from knowledge of the personal data breach, based on available information. Follow up report should be submitted within five (5) days from knowledge of the breach, unless allowed a longer period by the Commission.
When should data subjects or individuals be notified.	Within seventy-two (72) hours from knowledge of the breach, unless there is a reason to postpone or omit notification, subject to approval of the Commission.
What are the contents of notification to Commision	In general- 1. nature of the breach 2. sensitive personal information possibly involved 3. measures taken by the entity to address the breach 4. details of contact person for more information
What are the contents of notification to data subject	In general, same contents as notification of Commission but must include instructions on how data subject will get further information and recommendations to minimize risks resulting from breach.
How will notification be done?	Commission may be notified by written or electronic means but the personal information controller must have confirmation that the notification has been received. Data subjects or affected individuals shall be notified individually, by written or electronic means, unless allowed by the Commission to use alternative means.
Other requirements	Cooperate with the Commission where there is an investigation related to the breach. Documentation of all security incidents and the submission of an annual report to the Commission.