National Privacy Commission
Office of the President, Jose P. Laurel St.,
San Miguel,Manila, Metro Manila, Philippines
E-mail: privacycommissioner@privacy.gov.ph

Republic of the Philippines
NATIONAL PRIVACY COMMISSION
Metro Manila

NPC Circular 16-001
June 10, 2016

Re: Data Breach Notification

Pursuant to Section 20(f) of the Data Privacy Act, the National Privacy Commission promulgates the Rules of Procedure for Data Breach Notification and Other Responsibilities:

Sec. 1. What is subject to notification requirements.

a. Definition of breach. A breach is a security incident that leads to unlawful or unauthorized processing of personal, sensitive or privileged information, or that otherwise compromises the availability, integrity or confidentiality of information processed under the control of a personal information controller. This includes accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to information transmitted, stored or otherwise processed.

b. A breach shall be subject to notification requirements under the following conditions:

1. The compromised data involves sensitive personal information or other information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

c. 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,
4. Specifically established by an executive order or an act of Congress to be kept classified.

d. Other information that may be used to enable identity fraud shall include: data about the financial or economic situation of the data subject; user names, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or similar information which may be made the basis of decisions concerning the data subject, including grant of rights or benefits.

f. The claim that information involved in the breach is public information will not automatically exempt a personal information controller from notification requirements. When the level of availability or publicity of the data is changed by the security breach, it should be considered as a security breach requiring notification.

g. A discovery of a vulnerability in the system that would allow access to information about data subjects should prompt the personal information controller to evaluate for possible breach.

h. In cases where the personal information controller is unsure whether notification is required, the primary consideration would be likelihood of adverse effects and how notification, particulary of the data subjects, could reduce risks arising from the circumstances of the breach. The personal information controller shall also consider:
1. If the possible breach would tend to affect national security, public safety, public order, or public health;
2. If the unlawful or unauthorized access involves at least one hundred individuals;
3. If it involves sensitive information required by law or rules to be confidential;
4. If it includes personal data of vulnerable groups.

Sec. 2. Who should notify.

a. The personal information controller shall notify the National Privacy Commission and the affected data subjects in case of breach.

b. The personal information controller shall identify an individual responsible for ensuring compliance with notification requirements,

who should ideally be the designated data protection officer of the personal information controller.

c. The responsibility to notify remains with the personal information controller even if the processing of information is outsourced to a personal information processor.

d. The personal information controller shall use use contractual or other reasonable means to ensure that the processor reports the discovery of a breach or security incident to the personal information controller in order to allow timely reporting of data breach.

Section 3. When should notification be done.

a. National Privacy Commission
   1. The Commission shall be notified within 72 hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a security breach has occurred.
   2. Notification may be delayed only 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.
   3. The personal information controller need not be absolutely certain of the scope of the breach prior to notification. The personal information controller shall not use its inability to immediately secure or restore integrity to the information and communications system to delay notification, if it would be prejudicial to the data subjects.
   4. If there is an indication that the breach involves at least one hundred data subjects, or involves disclosure of sensitive personal information that would adversely affect the data subject, the notification should not be delayed. In this case, the Commission should be notified within the 72 hour period based on available information.
   5. If it is not reasonably possible to provide complete information, the full report of the security breach must be submitted within three days, unless the personal information controller is allowed by the Commission additional time to comply.
   6. Delay in notification shall not be excused if the delay is used to perpetuate fraud or conceal the security breach.

b. Data Subjects-

1. Data Subjects should be notified within 72 hours if the information breach is likely to result in a high risk to their rights and freedoms in order to allow them to take the necessary precautions. Data subjects may be notified based on the information available at that time, if this will allow data subjects to take measures to protect themselves against the effects of the data breach, and to supplement this information at a later stage on the basis of further investigation.

2. If it is not reasonably possible to notify the data subjects within the time period, the personal information controller shall request the Commission for exemption or postponement of notification of individual data subjects. This shall be allowed only under specific circumstances:

    i. The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.
    ii. The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

3. The following factors shall be considered in determining whether a personal information controller is allowed to be exempted from notification:

    i. the security measures implemented by the Data Controller and applied to the data at the time the breach is reasonably believed to have occurred, including measures that would render the data unintelligible to any person who is not authorised to access it;
    ii. the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialise;

4. Based on age or capacity of affected data subjects, notification may be done through legal representatives.

5. Failure to notify. In case of failure to notify the Commission or data subjects, or there is unreasonable delay, the Commission shall determine if notification is unwarranted or delay is justified. Failure to notify shall be presumed if the Commission does not receive notification from the personal information controller within 5 days from knowledge or reasonable belief that a security breach occurred.

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

Sec. 4. What are the Contents of the Notification.

a. Notification of Commission.
The notification shall include:

1. Nature of the breach
   - description of how the breach occurred and the vulnerability of the system that allowed the breach
   - a chronology of the events leading up to the loss of control of the information
   - approximate number of data subjects or records involved
   - description of nature of information breach
   - description of the likely consequences of the information breach
   - name and contact details of privacy officer or other accountable persons
2. Sensitive personal information possibly involved
   - description of sensitive personal information involved
3. Measures taken by the entity to address the breach
   - a description of the measures taken or proposed to be taken by the controller to address the breach
   - the action being taken to secure or recover the information that has been compromised
   - actions done or proposed to mitigate possible adverse effects and limit damage or distress to those affected by the incident,
   - the action being taken to inform those affected by the incident or reasons for the delay in doing so
   - the measures being taken to prevent repetition of the incident.

The Commission may require additional information.

b. Notification of Data Subjects.

The notification to the data subject should at least include: the nature of the breach, sensitive personal information possibly involves, measures taken to address the breach and reduce negative consequence, the authorities or contact details where the data subject can obtain additional information about the breach, and any assistance to be provided the affected data subjects. Where it is not possible to provide the above information at the same time, the information may be provided in phases without undue delay.

Sec. 5. How will notification be done. –

a. Notification of Commission.

The personal information controller shall notify the Commission by submitting a report, whether written or electronic, containing the required information. The personal information controller shall also include in the report the name of a person and his or her contact information. In case of submission by electronic mail, the personal information controller shall ensure secure transmission.

The personal information controller should receive a confirmation that the notification has been received. Unless there is confirmation, the report is not deemed filed. In case of written document, the received copy kept by personal information controller shall be sufficient confirmation.

b. Notification of Data Subjects.

The personal information controller shall notify the data subjects individually, using a secure means of communication, whether written or electronic. In doing so, the personal information controller shall take the necessary steps to ensure the proper identity of the individual being notified, and to ensure that no further disclosure will be made regarding the data subject's information.

The personal information controller shall put in place all reasonable mechanisms to ensure that all affected individuals are made aware of the breach. In cases where individual notification is not possible or would

require a disproportionate effort, the personal information controller shall seek the approval of the Commission to use alternative means of notification. The personal information controller shall notify by public communication or similar measure whereby the data subjects are informed in an equally effective manner. The personal information controller shall provide a means for the data subjects to obtain more detailed information relating to the breach.

The personal information controller shall report the manner of notification of the data subjects to the Commission.

Sec. 6. When can the Commission Investigate. -

Depending on the nature of the incident, or if there is delay or failure to notify, the Commission may investigate the circumstances surrounding the information security breach. Investigations may include on-site examination of systems and procedures.

If necessary, the Commission may use its enforcement powers to order cooperation of the personal information controller with the investigation or to compel appropriate action to protect the interests of data subjects.

After the investigation, the Commission shall promulgate an order to the personal information controller which may include actions to be taken regarding its security measures, notification of data subjects, and other actions to protect the affected data subject.

Based on the investigation, if there is evidence indicating a violation of the Data Privacy Act, the Commission shall notify the Personal Information Controller and other involved individuals, and allow the filing of an answer, inlcuding any additional evidence or affidavits. In resolving the case, the Commission may award indemnity, issue cease and desist orders, issue a temporary or permanent ban on the processing of personal data, recommend criminal prosecution, impose fines and penalties in accordance with applicable law or rules, or issue orders directing any further action.

Sec.7. Reporting requirements.

All security incidents and security breach shall be documented even if not covered by the notification requirements. For security breach, this should include the facts surrounding the incidents, effects and the remedial action

taken. For security incidents, aggregated data shall constitute sufficient compliance. These reports shall be made available when requested by the Commission. An electronic summary indicating number of incidents and breach, and a classification on whether it tends to affect availability, integrity or confidentiality, shall be submitted to the Commission annually.

Sec.8. Notification and Reporting to the National Privacy Commission. The requirement of notification and reporting shall be complied with by submission through:

a. Mailing Address: National Privacy Commission, Office of the President, Jose P. Laurel St., San Miguel, Manila, Metro Manila, Philippines

b. Electronic Mail: info@privacy.gov.ph

c. The above details for submission may be amended, subject to public announcement through the Commission's website or other comparable means.

Sec. 9. Separability Clause. In the event that any provision or part of this Order is declared unauthorized or rendered invalid, those provisions not affected by such declaration shall remain valid and in force.

Sec. 10. Effectivity. This Order shall take effect fifteen (15) days after publication in a newspaper of general circulation.

Approved:

RAYMUND E. LIBORO
Privacy Commissioner

IVY D. PATDU
Deputy Privacy Commissioner

DAMIAN DOMINGO O. MAPA
Deputy Privacy Commissioner

Promulgated: June 10, 2016

National Privacy Commission
Office of the President, Jose P. Laurel St.,
San Miguel,Manila, Metro Manila, Philippines
E-mail: privacycommissioner@privacy.gov.ph

Summary	
What is subject to 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 outsourced to third party
When should notification of Commission be done.	Within 72 hours from knowledge of security breach, based on available information Follow up report should be submitted within 3 days from knowledge of breach, unless allowed a longer period by the Commission
When should data subjects or individuals be notified.	Within 72 hours from knowledge of breach unless there is 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 personal information controller must have confirmation that 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 in case of an investigation related to the breach. Document all security incidents and submit report to Commission annually.