Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Advisory No. 18-02

DATE : 26 JUNE 2018

SUBJECT : UPDATED TEMPLATES ON SECURITY INCIDENT AND PERSONAL DATA BREACH REPORTORIAL REQUIREMENTS

SEC. 1. *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 Data Privacy Act of 2012, its implementing rules and regulations, and other relevant issuances of the National Privacy Commission (NPC).

SEC. 2. *Updated Templates*. - This Advisory provides updated templates for the reportorial requirements of the NPC on security incidents and personal data breaches:

1. Annual security incident reports to be submitted to the NPC by the PIC[1] and PIP,[2] *Provided*, that entities that are both PICs and PIPs shall submit both reports to the NPC (both Annex "A" and Annex "B"); and

2. Mandatory notification for the NPC[3] and for data subjects[4] for personal data breach events with mandatory notification requirements under the Data Privacy Act of 2012.

SEC. 3. The templates pertaining to the Annual Security Incident Reports and Mandatory Breach Notification may be updated in subsequent issuances.

SEC. 4. *Online Filing*. – Those wishing to submit through the internet may fill out the form at the NPC website; submission through this electronic Form shall be considered as sufficient compliance with the required Annual Security Incident Report. An annual report is not necessary for those who do not experience any security incident within a calendar year.

SEC. 5. *This Advisory*. – This advisory supersedes and takes precedence over any other prior advisories and issuances inconsistent therewith.

---

[1] Annex "A" –Annual Security Incident Reports for PICs
[2] Annex "B" –Annual Security Incident Reports for PIPs
[3] Annex "C" – Mandatory Notification: Personal Data Breach for National Privacy Commission
[4] Annex "D" – Mandatory Notification: Personal Data Breach for Data Subjects

APPROVED:

(sgd.) IVY D. PATDU
Deputy Privacy Commissioner
Policies and Planning

(sgd.) LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner
Data Processing Systems

(sgd.) RAYMUND E. LIBORO
Privacy Commissioner

ANNEX A

Annual Security Incident Reports for PICs

SUMMARY
Annual Security Incident Reports
January to December 2017

Sector: _____City/Municipality: _____ Province: _____

PIC (Individual or Organization) _____

Name of DPO _____

PERSONAL INFORMATION CONTROLLER

A. Personal Data Breach, Mandatory Notification	<#>
B. Personal Data Breach, not covered by mandatory notification requirements	<#>
C. Other Security Incidents	<#>
D. Total Security Incidents (D = A+B+C)	<#>

How Security Incidents Occurred

Types	***Number***	**Types**	***Number***
Theft	<#>	Communication Failure	<#>
Fraud	<#>	Fire	<#>
Sabotage/Physical Damage	<#>	Flood	<#>
Malicious Code	<#>	Design Error	<#>
Hacking/Logical Infiltration	<#>	User Error	<#>
Misuse of Resources	<#>	Operations Error	<#>
Hardware Failure	<#>	Software Maintenance Error	<#>
Software Failure	<#>	Third Party Services	<#>
Hardware Maintenance Error	<#>	Others	<#>

Personal Data Breaches

	Confidentiality	**Integrity**	**Availability**
Mandatory Notification Required	<#>	<#>	<#>
Mandatory Notification Not Required	<#>	<#>	<#>

PREPARED BY : _____ E-MAIL: _____

DESIGNATION : _____ CONTACT NO .: _____

DATE : _____

ANNEX B

Annual Security Incident Reports for PIPs

SUMMARY
Annual Security Incident Reports
January to December 2017

Sector: _____City/Municipality: _____ Province: _____

PIP (Individual or Organization) _____

Name of DPO _____

PERSONAL INFORMATION PROCESSOR

This form applies to personal data processing performed on behalf of PICs

A. Personal Data Breaches, reported to PICs	<#>
B. Personal Data Breaches, not reported to PICs	<#>
C. Other Security Incidents	<#>
D. Total Security Incidents (D = A+B+C)	<#>

How Security Incidents Occurred

Types	***Number***	**Types**	***Number***
Theft	<#>	Communication Failure	<#>
Fraud	<#>	Fire	<#>
Sabotage/Physical Damage	<#>	Flood	<#>
Malicious Code	<#>	Design Error	<#>
Hacking/Logical Infiltration	<#>	User Error	<#>
Misuse of Resources	<#>	Operations Error	<#>
Hardware Failure	<#>	Software Maintenance Error	<#>
Software Failure	<#>	Third Party Services	<#>
Hardware Maintenance Error	<#>	Others	<#>

PREPARED BY : _____ E-MAIL: _____

DESIGNATION : _____ CONTACT NO.: _____

DATE : _____

ANNEX C

Mandatory Notification: Personal Data Breach for the National Privacy Commission

<NAME OF ENTITY>
<ADDRESS>
<CONTACT INFORMATION>

<DATE>

<PRIVACY COMMISSIONER>
National Privacy Commission
Pasay City, Metro Manila
Philippines

Subject: <DATA BREACH> dated <DATE> of <DATABASE>
<NPC REGISTRATION NO.>

Gentlemen:

I write in behalf of <ENTITY>, in relation to the data breach of <DATE>, involving <BRIEF DESCRIPTION OF DATA>. This notification is made pursuant to the mandatory data breach notification procedure in Philippine law to the National Privacy Commission.

Responsible Officers. The pertinent details of <ENTITY>, and the responsible persons thereof, are as follows:

Head of the Organization	<NAME> <OFFICE ADDRESS> <E-MAIL ADDRESS> <TELEPHONE> <OTHER CONTACT INFO>
Data Protection Officer	<NAME> <OFFICE ADDRESS> <E-MAIL ADDRESS> <TELEPHONE> <OTHER CONTACT INFO>
Process Owner	<NAME> <OFFICE ADDRESS> <E-MAIL ADDRESS> <TELEPHONE> <OTHER CONTACT INFO>

Nature of the Breach. In brief, we describe the nature of the incident, thus:

- *Describe the nature of the personal data breach.*
  - *Be as specific as possible. Indicate if the details provided are sensitive to the entity, which may cause unwarranted damage to the entity if disclosed to the public.*

- *Provide a chronology that describes how the breach occurred; describe individually the events that led to the loss of control over the personal data.*
- *Provide a description of the vulnerability or vulnerabilities that of the data processing system that allowed the breach.*
- *Include description of safeguards in place that would minimize harm or mitigate the impact of the personal data breach.*
- *Indicate number of individuals or personal records affected. Provide an approximate if the actual impact has not been determined.*
- *Describe the likely consequences of the personal data breach**. Consider effect on company or agency, data subjects and public.***

Personal Data Possibly Involved.

- *List all sensitive personal information involved, and the form in which they are stored or contained.*
- *Also list all other information involved that may be used to enable identity fraud.*

Measures taken to Address the Breach.

- Describe in full the measures that were taken or proposed to be taken to address the breach.
- Describe how effective these measures are.
- Indicate whether the data placed at risk have been recovered. Otherwise, provide all measures being taken to secure or recover the personal data that were compromised.
- Indicate actions of the organization to minimize/mitigate the effect on the affected individual. Provide all actions being performed or proposed to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident.
- Indicate of the affected individuals are aware that the incident has occurred. Include all the actions being taken to inform the data subjects affected by the incident or any reasons for delay in the notification.
- Describe the steps the organization has taken to prevent a recurrence of the incident.

Should you require further information on this matter, contact us using the information above. Any information that later becomes available shall be reported within five (5) days, or as further required by the Commission.

Sincerely,
<ENTITY>

<HEAD OF AGENCY/
DATA PROTECTION OFFICER>

ANNEX D

Mandatory Personal Data Breach Notification to Data Subjects

<NAME OF ENTITY>
<ADDRESS>
<CONTACT INFORMATION>

<DATE>

<DATA SUBJECT>
<ADDRESS>

Subject: <DATA BREACH> dated <DATE>
<NPC REGISTRATION NO.>

Dear <DATA SUBJECT>

I write in behalf of <ENTITY>, regarding your data in <BRIEF DESCRIPTION OF DATABASE>.

We regret to inform you that your data has been exposed in this data breach. To our understanding, your exposure is limited to: <DATA INVOLVED IN THE DATA BREACH>.

Nature of the Breach

- *Provide a summary of the events that led up to the loss of control over the data. Do not further expose the data subject.*
- *Describe the likely consequences of the personal data breach.*

Measures taken to Address the Breach.

- **Provide information on** *measures taken or proposed to be taken to address the breach, and to secure or recover the personal data that were compromised.*
- *Include actions taken to inform affected individuals of the incident. In case the notification has been delayed, provide reasons.*
- *Describe steps the organization has taken prevent a recurrence of the incident.*

Measures taken to reduce the harm or negative consequences of the breach.

- **Describe** *actions taken to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident.*

Assistance to be provided to the affected data subjects.

- **Include information on** *any assistance to be given to affected individuals.*

Do not hesitate to contact our Data Protection Officer for further information:

Data Protection Officer <DATA PROTECTION OFFICER>
<OFFICE ADDRESS>
<E-MAIL ADDRESS>

<TELEPHONE>
<OTHER CONTACT INFORMATION>

We undertake to provide more information to you as soon as they become available.

Sincerely,
<ENTITY>

<HEAD OF AGENCY/
DATA PROTECTION OFFICER>