BREACH MANAGEMENT AND REPORTING

VIDA ZORA G. BOCAR
Compliance and Monitoring Division

DP 5
FOR THE BPO INDUSTRY

NATIONAL PRIVACY COMMISSION

WHAT IS A DATA BREACH?

Sec. 3 (k), (s), IRR, R.A. 10173
Sec. 3, NPC Circular 16-03

DP 5
FOR THE BPO INDUSTRY

NATIONAL PRIVACY COMMISSION

DEFINITIONS

Security Incident

A **security incident** is:

- An event or occurrence that **affects or tends to affect** data protection; or
- An incident that compromises the **availability**, **integrity**, or **confidentiality** of personal data.

DEFINITIONS

Data Breach

A **data breach** is a **security incident** that:

- Leads to **accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access** of or **unauthorized processing** of personal data
- Compromises the **availability**, **integrity**, or **confidentiality** of personal data

DP 5 FOR THE DPO INDUSTRY

NATIONAL PRIVACY COMMISSION

TYPES OF DATA BREACHES

Availability Breach
Due to loss, accidental or unlawful destruction of personal data

Integrity Breach
Due to alteration of personal data

Confidentiality Breach
Due to the unauthorized disclosure of or access to personal data

NATIONAL PRIVACY COMMISSION

HOW TO HANDLE DATA BREACHES

Sec. 20, R.A. 10173
RULE IV, Secs. 8-9, NPC Circular 16-03

DP 5 FOR THE BPO INDUSTRY

NATIONAL PRIVACY COMMISSION

SECURITY INCIDENT MANAGEMENT POLICY

A **security incident management policy** is implemented by the Personal Information Controller or Processor for the purpose of managing security incidents, including personal data breaches.

DP 5

NATIONAL PRIVACY COMMISSION

REQUIREMENTS

Every Personal Information Controller or Processor should have policies and procedures for:

1. The **creation of a data breach response team**

2. Implementation of **security measures and privacy policies**

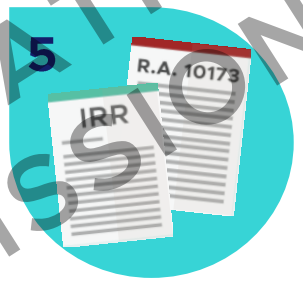
3. Implementation of an **incident response procedure**

DP 5 FOR THE DPO INDUSTRY

NATIONAL PRIVACY COMMISSION

REQUIREMENTS

4. **Mitigation of possible harm** and other negative consequences of a data breach
5. **Compliance with the Data Privacy Act** and other data protection laws and regulations

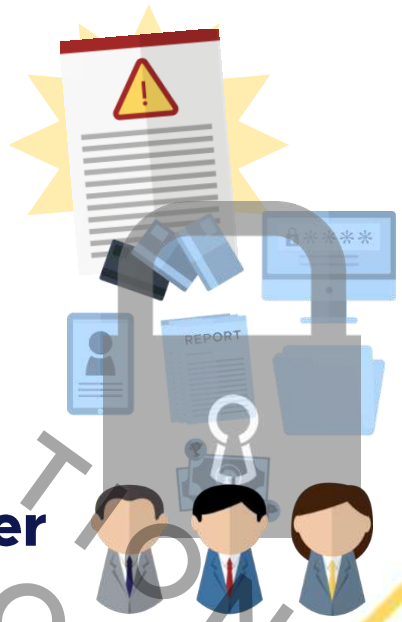


DATA BREACH RESPONSE TEAM

The data breach response team must have at least **one member** with the authority to make immediate decisions on critical actions.

The team shall be responsible for:

- Compliance with the **security incident management policy**
- **Management** of security incidents and personal data breaches
- Compliance with the **data privacy law and other issuances**



***This may be outsourced by the Personal Information Controller or Processor**

DPO5

NATIONAL PRIVACY COMMISSION

IMPLEMENTATION OF SECURITY MEASURES AND PRIVACY POLICIES

Recommended **best practices** in personal data breach prevention:

1. Regularly conduct a privacy impact assessment
2. Have a working data governance policy
3. Implement security measures
4. Make sure personnel are trained
5. Regularly review policies and procedures
6. Be aware of threats

MANDATORY NOTIFICATION

Sec. 20, R.A. 10173

Rule V, Sec. 11, NPC Circular 16-03

DP 5

NATIONAL PRIVACY COMMISSION

REQUISITES

Notification of a data breach is **mandatory** when:

1. The personal data involves a. **sensitive personal information** or b. any 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.

REQUISITES

All three elements must be present!

NOTIFICATION REQUIREMENTS

Rule IX, Secs. 38-42, IRR, R.A. 10173
Rule V, Secs. 15-18, 23 NPC Circular 16-03

DP 5
FOR THE DPO INDUSTRY

NATIONAL PRIVACY COMMISSION

WHO SHOULD NOTIFY?

The **Personal Information Controller** through the data breach response team.

Note: 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.

WHEN SHOULD WE NOTIFY?

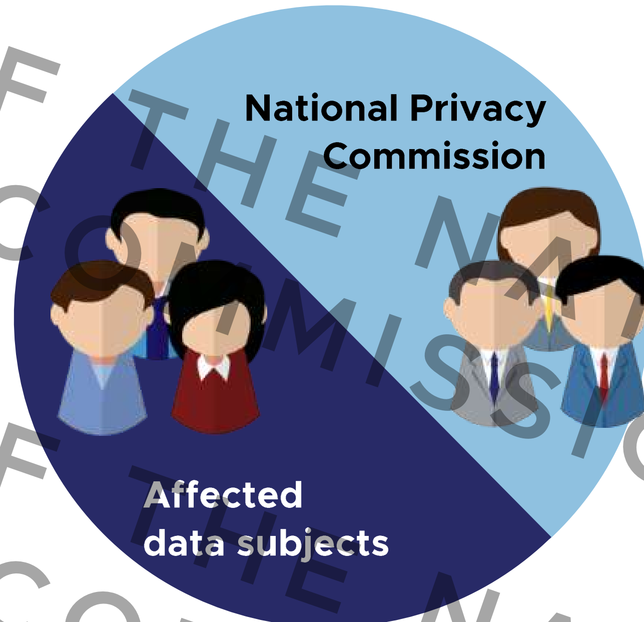
The notification must be made within 72 hours **upon knowledge of**, or when there is **reasonable belief** that a personal data breach has occurred.

DP 5 FOR THE DPO INDUSTRY

NATIONAL PRIVACY COMMISSION

WHO SHOULD BE NOTIFIED?

Notification must be made to the **Commission** and to any **affected data subjects.**



NATIONAL PRIVACY COMMISSION

HOW DO WE NOTIFY NPC?

Notification to the Commission may be done through e-mail at **complaints@privacy.gov.ph** or through **delivering a hard copy to the NPC office.**

Upon receipt of the notification, the Commission shall send a **confirmation message/e-mail** to the Personal Information Controller.

A report is **not deemed filed without confirmation**.

A **read receipt report is not sufficient** confirmation.

HOW TO NOTIFY DATA SUBJECTS

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.

May be supplemented with additional information at a later stage on the basis of further investigation.

HOW TO NOTIFY DATA SUBJECTS

Notification to affected data subjects may be done **electronically** or **in written form**, but **must be done individually**.

The notification **must not involve a further, unnecessary disclosure** of personal data.

If individual notice takes disproportional effort, **NPC authorization is required** for alternative means.

DP 5

NATIONAL PRIVACY COMMISSION

CONTENTS

- Nature of the Breach
- Personal Data Possibly Involved
- Remedial Measures to Address Breach

NATURE OF THE BREACH

- Description of how the breach occurred and the vulnerability of the data processing system that allowed the breach
- Chronology of the events leading up to the loss of control over the personal data
- Approximate number of data subjects or records involved

DP 5 FOR THE DPO INDUSTRY

NATIONAL PRIVACY COMMISSION

NATURE OF THE BREACH

- Description or nature of the personal data breach
- Description of the likely consequences of the personal data breach
- Name and contact details of the data protection or compliance officer or any other accountable persons.

DP 5 FOR THE DPO INDUSTRY

NATIONAL PRIVACY COMMISSION

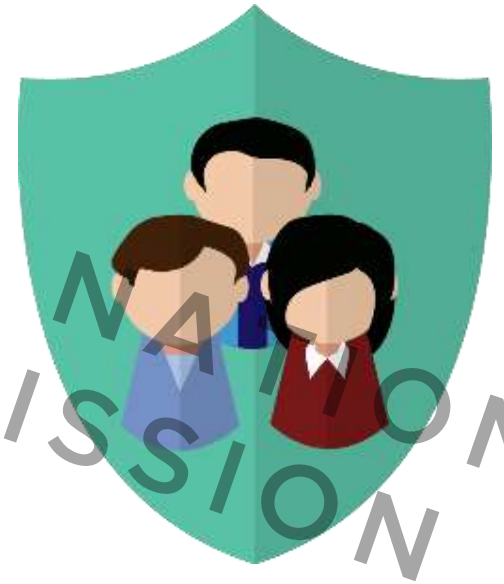
PERSONAL DATA POSSIBLY INVOLVED

- Description of sensitive personal information involved
- Description of other information involved that may be used to enable identity fraud

REMEDIAL MEASURES

- Description of the measures taken or proposed to be taken to address the breach

- Actions being taken to secure or recover the personal data that were compromised



REMEDIAL MEASURES

- Actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident

REMEDIAL MEASURES

- Action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification
- The measures being taken to prevent a recurrence of the incident.

REMEDIAL MEASURES

- Contact information or website containing information on how to mitigate damage arising from the data breach

DELAY AND/OR EXEMPTION FROM NOTIFICATION OF DATA SUBJECTS

Sec. 40, IRR, R.A. 10173
Rule V, Secs. 18-19, NPC Circular 16-03

DP 5

NATIONAL PRIVACY COMMISSION

DELAY IN NOTIFICATIONS

The NPC can grant you a **delay in data subject notification** if:

- There is a **need to determine scope**
- Delay is necessary **to prevent further disclosure**
- There is a need to **restore integrity** to the ICT system
- Notification is going to **hinder a criminal investigation**

DP 5

NATIONAL PRIVACY COMMISSION

NO DELAY IN NOTIFICATION

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 any event, the Commission **must** be notified within the 72-hour period.

DP 5 FOR THE DPO INDUSTRY

NATIONAL PRIVACY COMMISSION

EXEMPTIONS FROM NOTIFICATION

Can't make the 72-hour deadline?
Ask the NPC for an extension.

The NPC can also **exempt you from data subject notification** if notification is not:

- in the **public interest**; or
- in the **best interest** of the data subjects.

DP 5 FOR THE DPO INDUSTRY

NATIONAL PRIVACY COMMISSION

EXEMPTIONS FROM NOTIFICATION

Is the notification not in the best interest of the data subject? **Consider**:

- Security measures implemented and applied to make the data unintelligible to unauthorized persons.
- Subsequent measures taken to ensure high risk of material harm does not materialize.

FULL REPORT!

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.

DP 5

NATIONAL PRIVACY COMMISSION

CONCEALMENT OR FAILURE TO DISCLOSE DATA BREACH

Sec. 30, R.A. 10173
Sec. 57, IRR, R.A. 10173
Sec. 20, NPC Circular 16-03

DP 5

NATIONAL PRIVACY COMMISSION

CONCEALMENT OF BREACH

An intention to conceal is 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 security breach occurred.

DP 5 FOR THE DPO INDUSTRY

NATIONAL PRIVACY COMMISSION

PUNISHABLE ACT

Concealment Is a crime!

Imprisonment from **1 year and 6 months** to **5 years** plus **fine** from ₱500,000 to ₱1,000,000

Imposed on persons who:

- After having knowledge of a security breach and of the obligation to notify the National Privacy Commission
- Either **intentionally** or **by omission** conceals the fact of such breach

DP 5

NATIONAL PRIVACY COMMISSION

ANNUAL REPORT

Sec. 22, NPC Circular 16-03

DP 5

NATIONAL PRIVACY COMMISSION

SUBMISSION

Any or all reports shall be made available when requested by the Commission.

A summary of all reports shall be submitted to the Commission annually.

CONTENTS

In the event of a security incident amounting to a data breach, the report must include:

- The facts surrounding the incident
- The effects of the incident
- Remedial action taken by the PIC

DP 5 FOR THE DPO INDUSTRY

NATIONAL PRIVACY COMMISSION

CONTENTS

All security incidents and personal data breaches shall be documented.

Aggregated data for security incidents not involving a personal data breach suffices.

CONTENTS

The report must contain general information:

- The number of incidents and breaches encountered
- The classification of data breaches according to their impact on the availability, integrity, or confidentiality of personal data

IN CONCLUSION

- Notifications are mandatory only for a **specific form of confidentiality breach.**
- There are two kinds of notifications:
  - Notification to the **data subject**
  - Notification to the **NPC**
- These notifications must be made **within 72 hours of knowledge of a mandatory data breach** has occurred.
- Failure to comply with the notification requirement **can lead to criminal penalties.**

DP 5 FOR THE DPO INDUSTRY

NATIONAL PRIVACY COMMISSION

THANK YOU!!!!

Have **questions?**

Contact us!

privacy.gov.ph
facebook.com/privacy.gov.ph
twitter.com/PrivacyPH

DP 5
FOR THE BPO INDUSTRY

NATIONAL PRIVACY COMMISSION