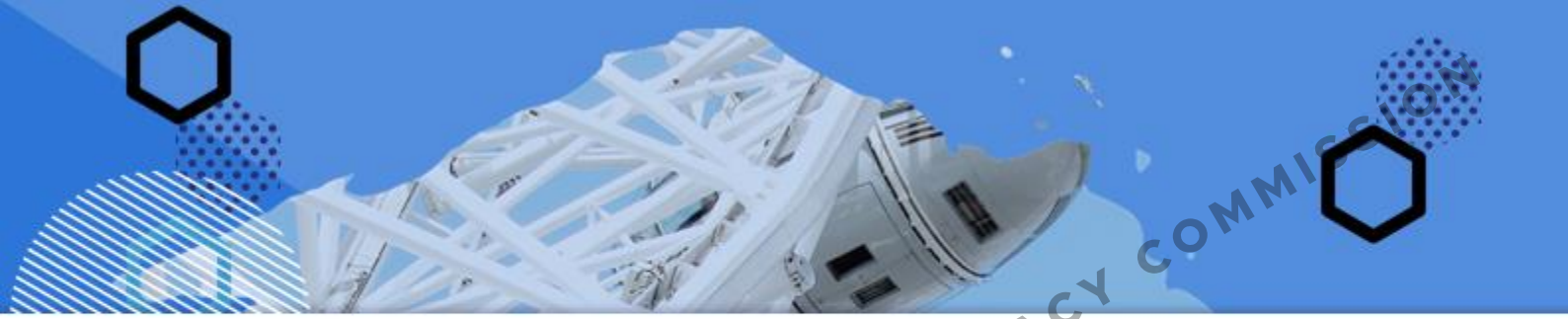


Data Breach Management and Threats to Data Protection

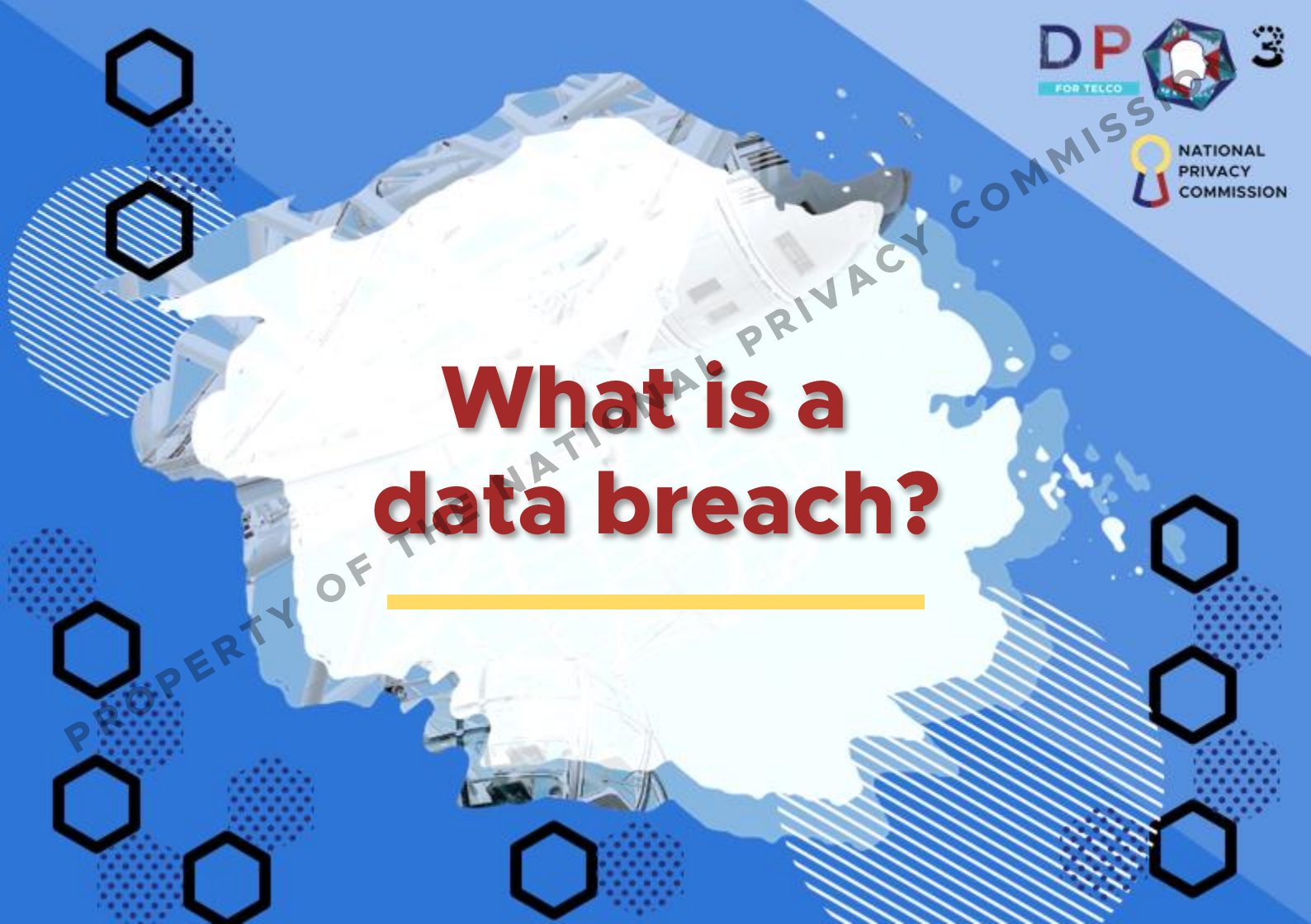
Francis Euston R. Acero
Complaints and Investigations Division
National Privacy Commission

NATIONAL PRIVACY COMMISSION

DP FOR TELCO

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION



What is a data breach?

What is a **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.

DP FOR TELCO

NATIONAL PRIVACY COMMISSION

What is a **data breach**?

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

- Leads to **unlawful** or **unauthorized processing** of personal data
- Compromises the **availability**, **integrity**, or **confidentiality** of personal data

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Management begins with prevention

Do I need a **security incident management policy**?

A **security incident management policy** is implemented by the controller or processor for the purpose of managing security incidents.

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Do I need a **security incident management policy**?

The security incident management policy has 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**

DPO FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Do I need a **security incident management policy**?

The security incident management policy has policies and procedures for:

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

Do I need a **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 is responsible for:

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

DP FOR TELCO

NATIONAL PRIVACY COMMISSION

What are **best practices** in 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**

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

DP FOR TELCO

NATIONAL PRIVACY COMMISSION

Top Threats to Data Protection

What are my **top threats**?

Threats to an organization's data protection can be classified into two general categories:

1. **Technical** Threats
2. **Physical/Organizational** Threats

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

What are the **top technical threats**?

1. Phishing (especially targeted phishing attacks)
2. Unpatched software and applications
3. Non-existent security architecture
4. Malicious code
5. Poor configuration/Backdoor vulnerability
6. Removable media
7. Botnets
8. No immediate backup systems
9. Cloud computing without safeguards

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

What are **top physical/organizational threats**?

1. Home invasions/robberies
2. Insider jobs
3. Poor password strength
4. Poor physical safeguards
5. Social engineering
6. Insistence on paper-based systems
7. Lack of data disposal policies
8. No organizational support/tone from the top
9. Cultural issues

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Mandatory Notification

Notification becomes **mandatory** when:

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

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

The unauthorized acquisition is likely to give **rise to a real risk of serious harm** to any affected data subject.

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION


DP
FOR TELCO
3
NATIONAL
PRIVACY
COMMISSION
All three elements must be present!
PROPERTY OF THE NATIONAL PRIVACY COMMISSION

In **doubt**? Consider:

The **likelihood of harm or negative consequences** on the affected data subjects.

How notification, particularly of the data subjects, could **reduce the risks arising from the personal data breach** reasonably believed to have occurred.

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

In **doubt**? Consider:

If the data involves:

- Information that would likely affect:
  - National security
  - Public safety
  - Public order
  - Public health
- At least one hundred (100) individuals are affected
- The information is required by all applicable laws or rules to be confidential
- Personal data of vulnerable groups

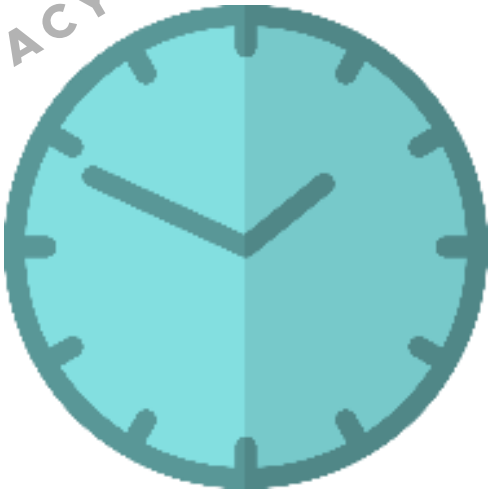
DP FOR TELCO

NATIONAL PRIVACY COMMISSION

Who and **when** must 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.

The obligation **remains with the personal information controller** even if the processing of information is outsourced or subcontracted.



DP FOR TELCO

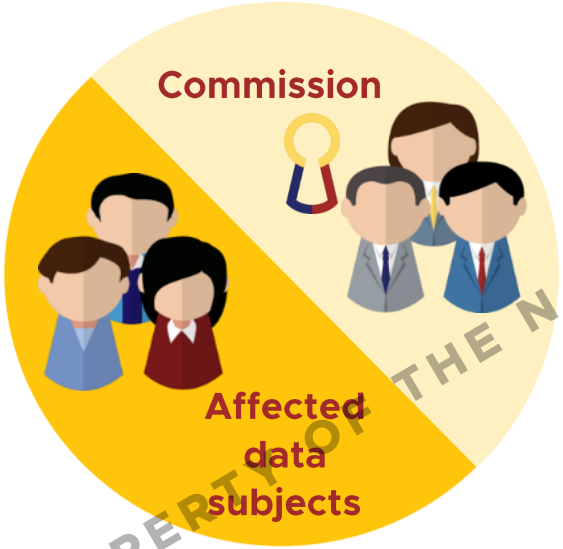
NATIONAL PRIVACY COMMISSION

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Notification Requirements

Who must we notify?



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

How do we notify the 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.

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

How do we notify the 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.

How do we notify the data subjects?

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.

DP FOR TELCO

NATIONAL PRIVACY COMMISSION

Content is king. **Substance** matters.

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 FOR TELCO

NATIONAL PRIVACY COMMISSION

Content is king. **Substance** matters.

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.

DPO FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Content is king. **Substance** matters.

Personal Data Possibly Involved

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

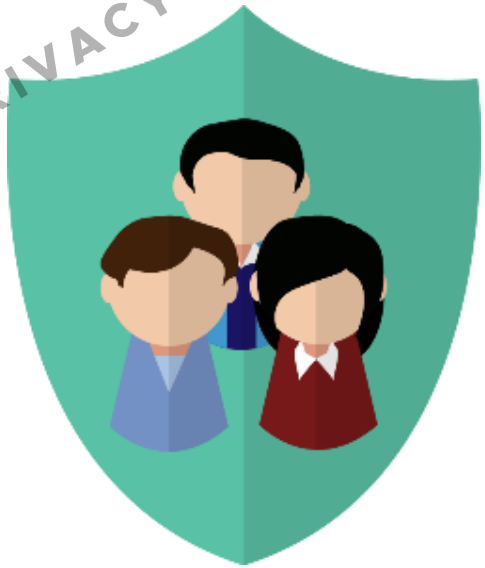
DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Content is king. **Substance** matters.

Remedial Measures to Address Breach

- 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



DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Content is king. **Substance** matters.

Remedial Measures to Address Breach

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

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Content is king. **Substance** matters.

Remedial Measures to Address Breach

- 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.

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Additional information for data subjects

Remedial Measures to Address Breach

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

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Delay and Exemption from Notifications

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 FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Delay in notifications?

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 FOR TELCO

NATIONAL PRIVACY COMMISSION

Exemption 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 FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Exemption 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.

DP FOR TELCO

NATIONAL PRIVACY COMMISSION

The **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 FOR TELCO 3

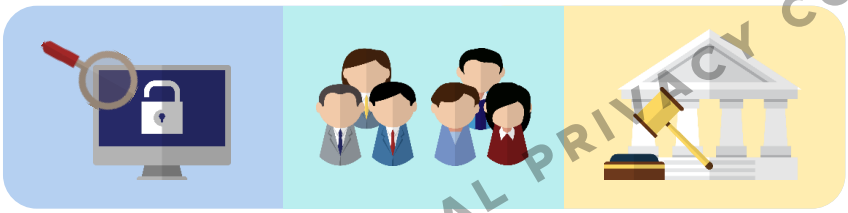
NATIONAL PRIVACY COMMISSION

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

Concealment is a crime

The **failure** to disclose leads to prison



The NPC can investigate data breaches further:

On-site examination of **systems and procedures**.

If necessary, the Commission can:

require the cooperation of concerned parties, or **compel appropriate action therefrom** to protect the interests of data subjects.

The **failure** to disclose leads to prison

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 FOR TELCO

NATIONAL PRIVACY COMMISSION

The **failure** to disclose leads to prison

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 FOR TELCO

NATIONAL PRIVACY COMMISSION

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

The Annual Report

The **annual** report

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.

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

The **annual** report

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 FOR TELCO 3

NATIONAL PRIVACY COMMISSION

The **annual** report

All security incidents and personal data breaches shall be documented.

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

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION

The **annual** report

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

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION


DP
FOR TELCO
3
NATIONAL
PRIVACY
COMMISSION
In
Conclusion
PROPERTY OF THE NATIONAL PRIVACY COMMISSION

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.**

Have **questions**?

Contact us!

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

DP FOR TELCO 3

NATIONAL PRIVACY COMMISSION