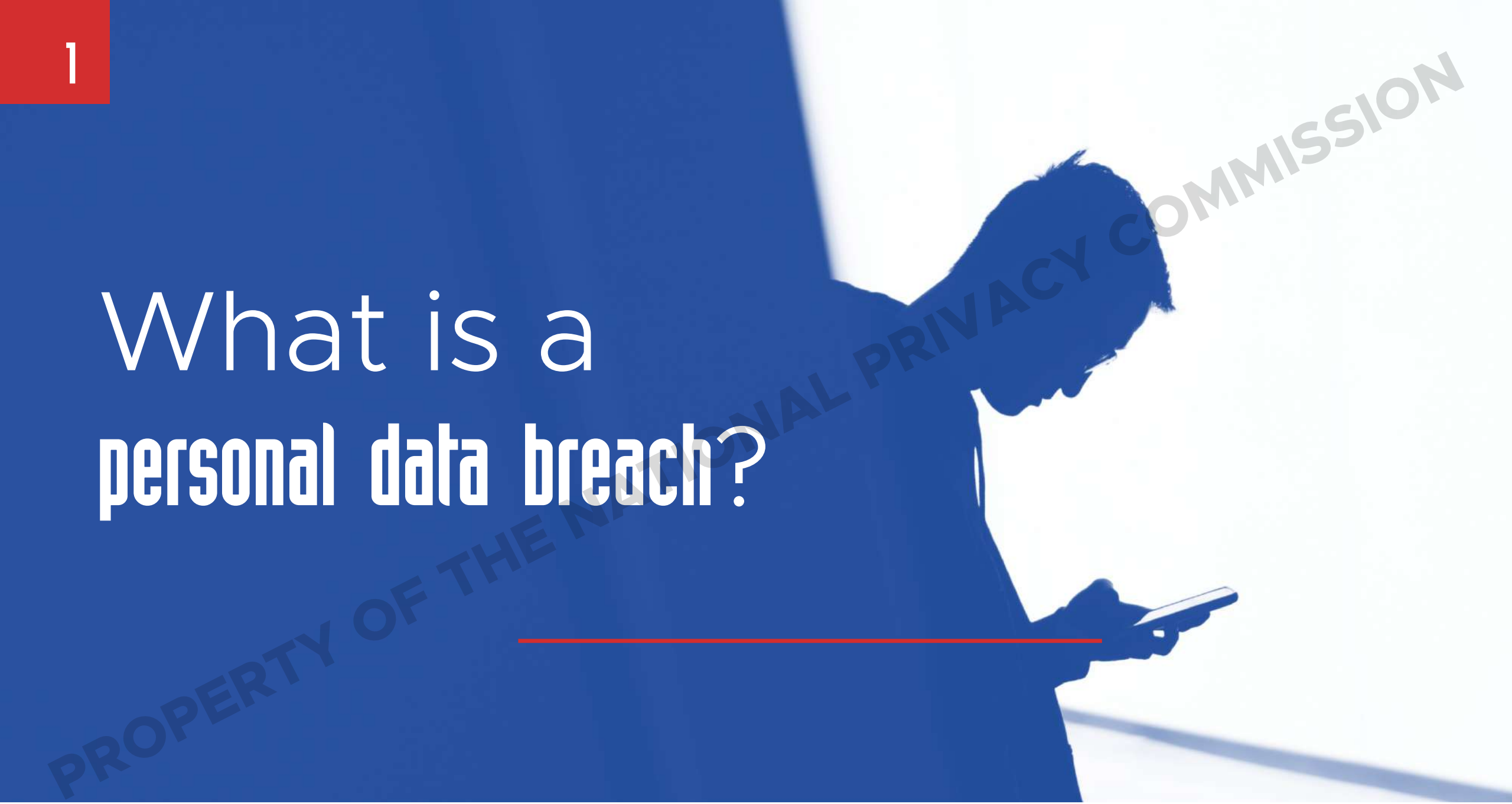
Personal Data Breach Management

NATIONAL PRIVACY COMMISSION

1

What is a **personal data breach**?



What is a personal data breach

a breach of security leading the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

May be in the nature of:

- **Availability** breach – loss or destruction
- **Integrity** breach – alteration
- **Confidentiality** breach – unauthorized disclosure or access

Security incident

event or occurrence affecting data protection, or compromises the availability, integrity & confidentiality of personal data; includes incidents that would result to a personal data breach, if not for safeguards that have been put in place

Importance

$3.62 million

average total cost of data breach in 2017

1

10% one-year decrease in average total cost

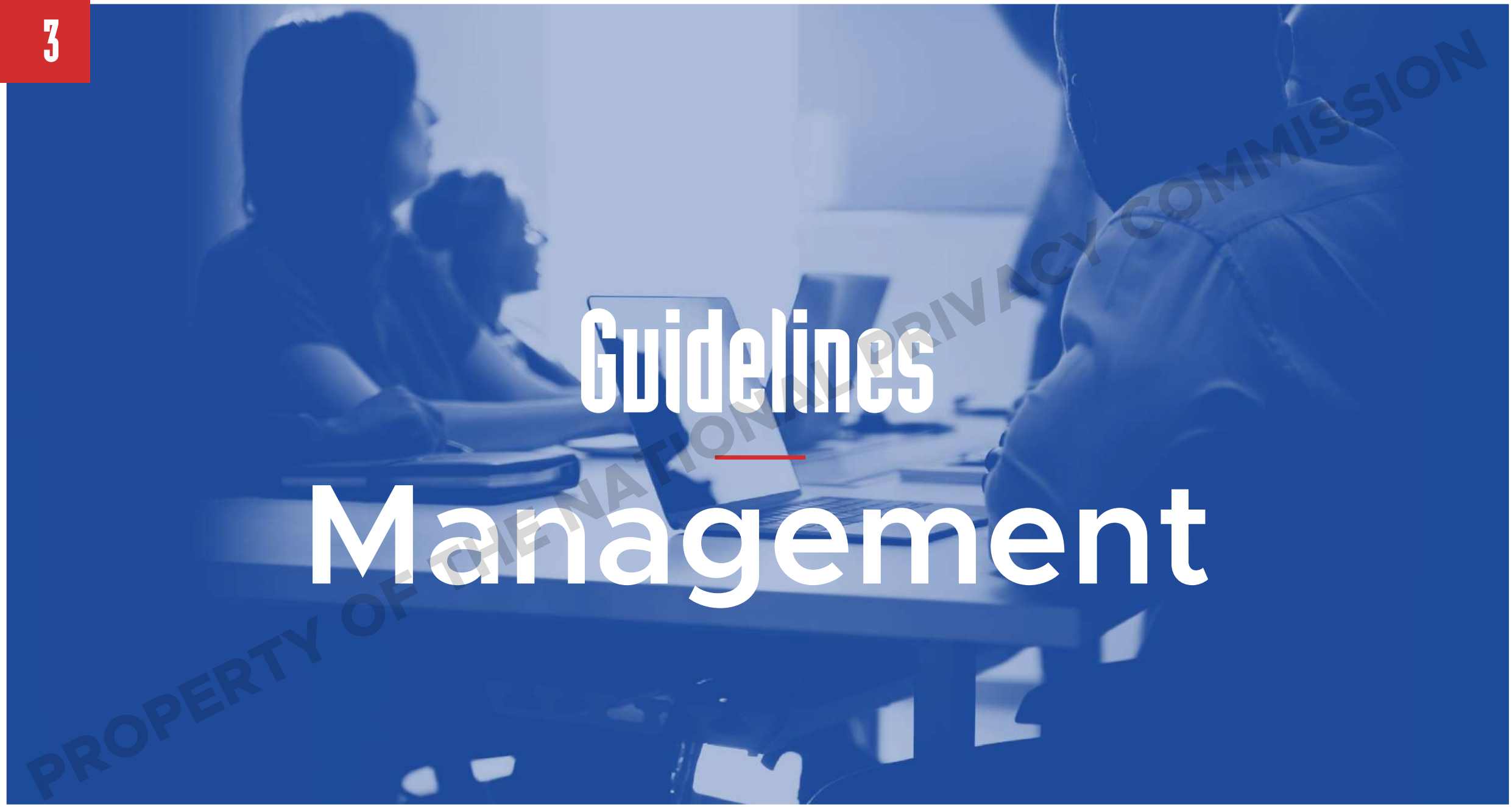
2

$141 is the average cost per stolen record

3

certain industries have more costly data breaches

3



Guidelines

Management

A

Security Incident Management Policy ensuring:

1

Data breach response team creation

A

Security Incident Management Policy ensuring:

2

Organizational, physical, technical security measures implementation

A

Security Incident Management Policy ensuring:

3

Incident response procedure

A

Security Incident Management Policy ensuring:

4

Mitigation of possible harm to data subjects

A

Security Incident Management Policy ensuring:

5

Compliance in terms of personal data breach notification

B

Data Breach Response Team

1

Composition

1

At least 1 member w/ the authority to make immediate decisions regarding critical action

2

May include the DPO

3

Functions may be outsourced, but DPO to remain accountable for compliance

B

Data Breach Response Team

2

Functions

1

PIC/PIP's implementation of security incident management policy

2

Management of security incidents & personal data breaches

3

Compliance

B

Data Breach Response Team

3

Others

1. Ready to assess & evaluate a security incident
2. Restore integrity to info & comms system
3. Mitigate & remedy any resulting damage
4. Comply with reporting requirements

4

Incident Response Policy & Procedure

A

Policies & procedures for:

1

Timely discovery of security incidents; person or persons responsible for regular monitoring & evaluation of security incidents

A

Policies & procedures for:

2

Clear reporting lines

A

Policies & procedures for:

3

Preliminary assessment

1

Nature & scope of breach, and immediate damage

2

Need for notification

3

Immediate measures to secure evidence, contain security incident & restore integrity of system

A

Policies & procedures for:

4

Evaluation

A

Policies & procedures for:

5

Contacting law enforcement

A

Policies & procedures for:

6

Conduct of investigations

A

Policies & procedures for:

7

Notification procedures

A

Policies & procedures for:

8

Mitigating possible harm to data subjects

B

Documentation

1

Description of the personal data breach

B

Documentation

2

Actions & decisions of the team

B

Documentation

3

Outcome & difficulties encountered

B

Documentation

4

Compliance w/ notification requirements & assistance provided to affected data subjects

5

Notification & Other Requirements

A

When notification is required

1

Involves sensitive personal information or any other information that may be used to enable identity fraud

A

When notification is required

2

Info may have been acquired by an unauthorized person

A

When notification is required

3

Unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject

B

When in doubt: other considerations

1

Data that would likely affect national security, public safety, public order, or public health

B

When in doubt: other considerations

2

Data of at least 100 individuals

B

When in doubt: other considerations

3

Data required by applicable laws or rules to be confidential

B

When in doubt: other considerations

4

Data of vulnerable groups

C

Who should notify

1

Personal Information Controller

C

Who should notify

2

Need for contractual or other reasonable means – with PIPs

D

Notification of the Commission

1 When

1. Within 72 hours upon knowledge of or reasonable belief that a personal data breach occurred

2. Based on available information

D

Notification of the Commission

1 When delay is allowed

1. Determine scope of breach
2. Prevent further disclosures
3. Restore reasonable integrity to the system

D

Notification of the Commission

1 Content

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

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

D

Notification of the Commission

1 Content

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.

D

Notification of the Commission

1 Content

3 Measures Taken to Address the Breach

A description of the measures taken or proposed to be taken to address the breach

Measures 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.

D

Notification of the Commission

1 Content

4 Additional information may be required

E

Form

- ✓ In the form of a report
- ✓ Written or electronic
- ✓ Needs receipt confirmation by the Commission

F

Exemption

If NPC determines that notification would not be in the public interest or in the interest of affected data subjects

G

Failure to Notify

- Presumed if NPC is not notified within 5 days
- Triggers an investigation into the breach

G

Annual Reports

- Covers security incidents & personal data breaches
- Submission deadline: 30 June 2018