Personal Data Breach Management
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
What is a personal data breach

May be in the nature of:

- **Availability** breach – loss or destruction
- **Integrity** breach – alteration
- **Confidentiality** breach – unauthorized disclosure or access
What is a personal data breach

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
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
Guidelines
Management
Security Incident Management Policy ensuring:

Data breach response team creation
Security Incident Management Policy ensuring:

Organizational, physical, technical security measures implementation
Guidelines - Management

Security Incident Management Policy ensuring:

Incident response procedure
Security Incident Management Policy ensuring:

Mitigation of possible harm to data subjects
Guidelines - Management

Security Incident Management Policy ensuring:

Compliance in terms of personal data breach notification
Data Breach Response Team

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
Data Breach Response Team

Functions

1. PIC/PIP’s implementation of security incident management policy
2. Management of security incidents & personal data breaches
3. Compliance
Data Breach Response Team

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
Incident Response Policy & Procedure
Policies & procedures for:

1. Timely discovery of security incidents; person or persons responsible for regular monitoring & evaluation of security incidents
Clear reporting lines
Policies & procedures for:

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
Policies & procedures for:

Evaluation
Policies & procedures for:

Contacting law enforcement
Policies & procedures for:

Conduct of investigations
Notification procedures
Mitigating possible harm to data subjects
Documentation

Description of the personal data breach
Actions & decisions of the team
Outcome & difficulties encountered
Compliance w/ notification requirements & assistance provided to affected data subjects
Notification & Other Requirements
When notification is required

1. Involves sensitive personal information or any other information that may be used to enable identity fraud.
When notification is required

Info may have been acquired by an unauthorized person
Unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.
When in doubt: other considerations

Data that would likely affect national security, public safety, public order, or public health
When in doubt: other considerations

Data of at least 100 individuals
When in doubt: other considerations

Data required by applicable laws or rules to be confidential
Notification of the Commission

When in doubt: other considerations

4

Data of vulnerable groups
Who should notify

1

Personal Information Controller
Who should notify

Need for contractual or other reasonable means – with PIPs
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
Notification of the Commission

When delay is allowed

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

A description of how the breach occurred and the vulnerability of the data processing system that allowed the breach
### Notification of the Commission

#### 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
Notification of the Commission

Content

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.
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
Notification of the Commission

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.
1 Content

4 Additional information may be required
Notification of the Commission

- In the form of a report
- Written or electronic
- Needs receipt confirmation by the Commission
If NPC determines that notification would not be in the public interest or in the interest of affected data subjects.
Failure to Notify

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

Annual Reports

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