

**Practising Governance Annual Conference 2023**

26 October 2023

# How to Uphold Data Governance Standards in a Data Breach

**Joyce LAI**









**Assistant Privacy Commissioner for Personal Data  
(Corporate Communications and Compliance)**


**Office of the Privacy Commissioner for Personal Data, Hong Kong**



# Some recent data breaches

Breaches with millions of affected users have occurred

Industry	Company	Reported number of affected individuals
Telecom	 (2023)	37 million 
	 (2022)	9 million 
	 (2022)	9 million 
Health insurance	 (2022)	9 million 

1x  = 2 million

# Personal Data (Privacy) Ordinance, Cap 486

Enacted in 1995, came into effect on 20 December 1996

1st comprehensive personal data protection law in Asia

Covers both public (government) and private sectors

Technology-neutral and principle-based

# Six Data Protection Principles of the PDPO



# A data breach may amount to a contravention of Data Protection Principle (DPP) 4(1) and (2) in Schedule 1 to the PDPO

## *DPP 4(1)*

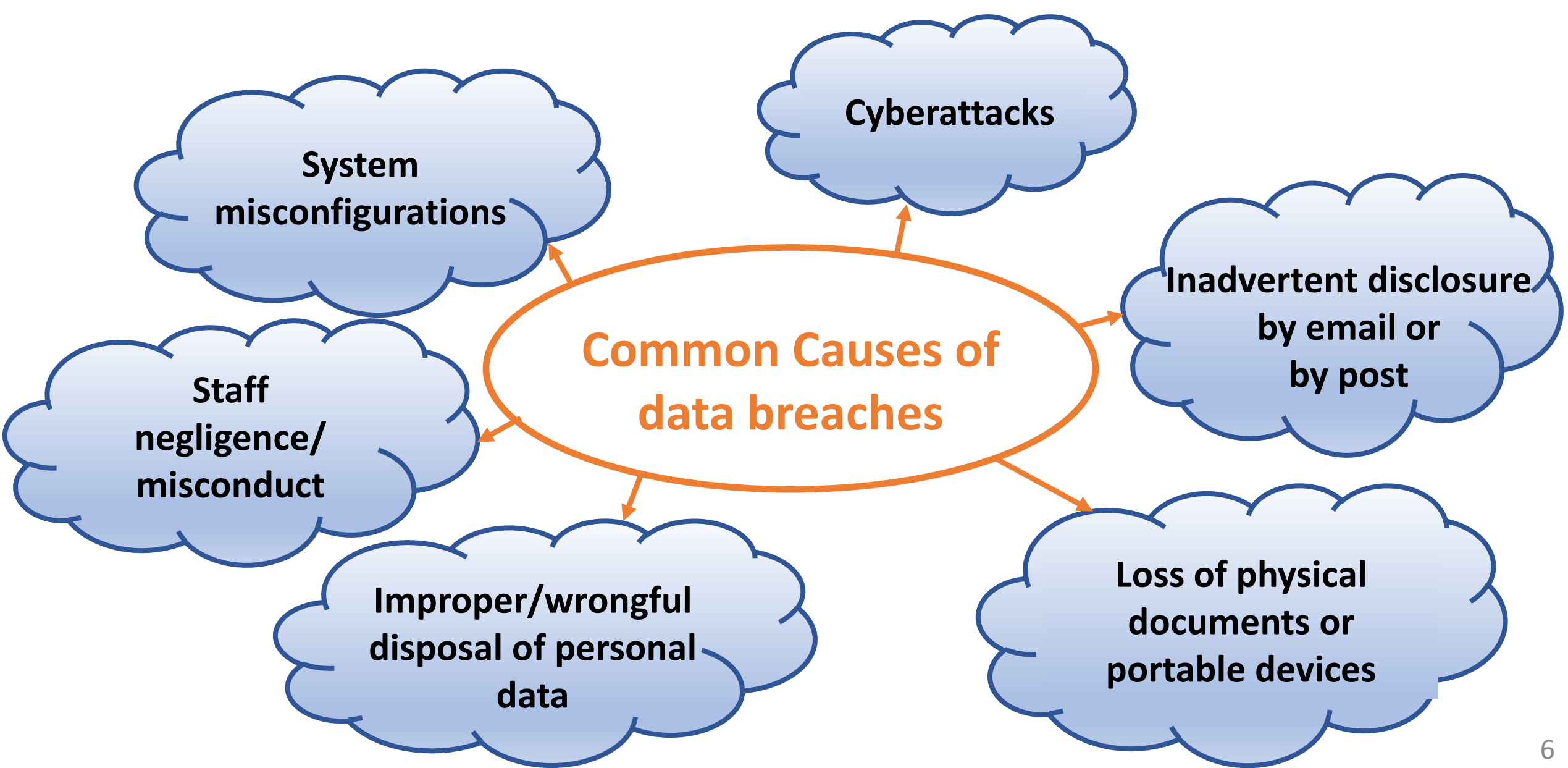
A data user shall take **all reasonably practicable steps** to ensure that the personal data it holds is protected against unauthorised or accidental access, processing, erasure, loss or use



## *DPP 4(2)*

If a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the **data user must adopt contractual or other means**, to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.





# Preparing for Contingency – Data Breach Response Plan

- A document setting out how an organisation will **respond in the event of a data breach**
- Helps **ensure a quick response** to and **effective management** of a data breach
- The plan should outline:
  - ① **a set of procedures** to be followed in the event of a data breach
  - ② **strategy for identifying, containing, assessing and managing** the impact brought about by the incident from start to finish



# Data Breach Response Plan

*Aspects to be covered (non-exhaustive):*

- **Description** of what constitutes a data breach
- Internal incident **notification** procedure
- Designation of the **roles and responsibilities** of members of the dedicated breach response team
- **Risk assessment** workflow
- **Containment** strategy
- **Communication** plan
- **Investigation** procedure
- **Record-keeping** policy
- Post-incident **review** mechanism
- **Training** or drill plan





# 5 Steps for Handling Data Breaches

*Immediate gathering of essential information*

*Containing the data breach*

*Assessing the risk of harm*

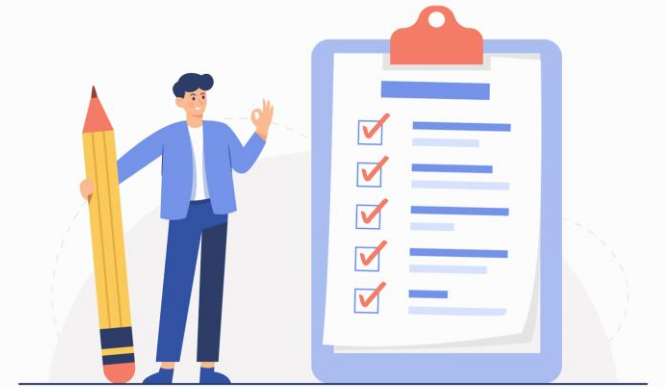
*Considering giving data breach notifications*

*Documenting the breach*

# Step 1: Immediate gathering of essential information

The data user shall promptly gather all relevant information of the data breach:

- **When** did the breach occur?
- **Where** did the breach occur?
- **How** was the breach **detected** and by whom?
- What was the **cause** of the breach?
- What kind of **personal data** was **involved**?
- How many **data subjects** might be affected?
- What **harm** may have been caused to those affected individuals?



Staff members who first discover the breach should escalate the incident to the senior management, according to the procedures.

## Step 2: Containing the data breach

- After conducting an initial assessment, the data user should immediately take steps to **contain the breach** according to the **categories of personal data involved** and **the severity** of the breach.
- Remedial actions to **lessen the harm or damage** that may be caused to the affected data subjects should be taken.



# Step 3: Assessing the risk of harm

## The possible harm caused by a data breach may include:

- Threats to personal safety
- Identity theft
- Financial loss
- Humiliation or loss of dignity, damage to reputation or relationships
- Loss of business or employment opportunities



## The extent of the harm suffered by the affected data subjects depends on:

- The **kind**, **sensitivity** and **amount** of the personal data being leaked
- The **circumstances** and **duration** of the data breach
- The **nature** of harm
- The likelihood of **identity theft** or **fraud**
- Whether a **backup** of the lost data is available
- Whether the leaked data are adequately **encrypted**, **anonymised** or otherwise rendered **inaccessible** (e.g. password protected)

# Step 4: Considering giving data breach notifications

When deciding whether to report a breach to the affected data subjects, the PCPD and other law enforcement agencies, the data user should take into account:

- the **potential consequences** of a breach for the affected individuals
- how **serious** or **substantial** these are
- how **likely** they are **to happen**
- The **consequences** of failing to give notification



The data user should **notify the PCPD and the affected data subjects as soon as practicable** after becoming aware of the data breach, particularly if the data breach is likely to result in a real risk of harm to those affected data subjects.



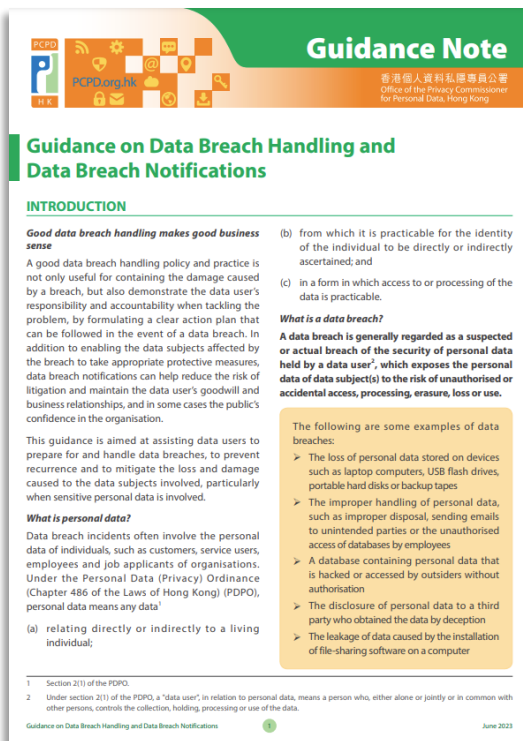
# Step 5: Documenting the breach

- A data user should maintain a **comprehensive record**, including all facts relating to the breach, ranging from **details of the breach and its effects to the containment and remedial actions**
- Organisations that are required to comply with the laws and regulations of other jurisdictions should also consider whether there are any **mandatory documentation requirements** under those laws and regulations

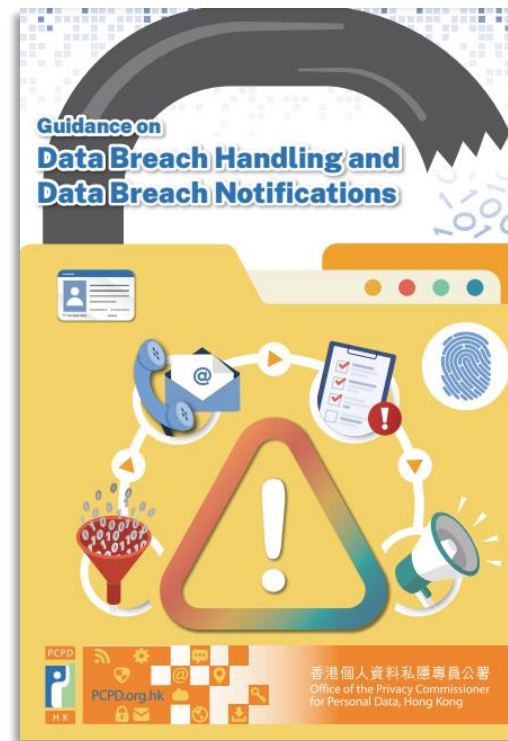


# Lessons Learnt: Preventing Recurrence

The data user should learn from the data breach, review how personal data are handled to **identify the root of the problem** and devise a **clear strategy to prevent the future recurrence** of similar incidents.



Download the  
Guidance Note



Download the  
Pamphlet

15

# Privacy Management Programme (PMP)

## Definition and benefits of adoption

### What's PMP?

- A **management framework**
  - For **responsible collection, holding, processing & use of personal data** by the company
  - To **ensure compliance with Personal Data (Privacy) Ordinance (PDPO)**

### Why PMP?



**Enhance data security**



**Minimise risk of data security incidents**



**Handle data breaches effectively** to minimise damages



**Build trust** with employees and customers, enhance corporate reputation and competitiveness

**“Guide for Independent Non-Executive Directors” published by HKIoD recommends use of PMP as part of ESG management!**

16





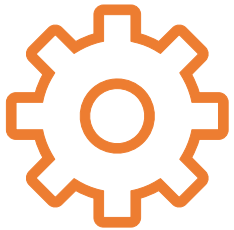
# Privacy Management Programme (PMP)

PMP consists of three parts



## 1. Organisational Commitment

- Buy-in from the top
- Appoint Data Protection Officer
- Set up a reporting mechanism



## 2. Programme Controls

- Personal data inventory
- Internal policies
- Risk assessment tools
- Training, education & promotion
- Handling of data breach incidents
- Data processor management
- Communication



## 3. Ongoing Assessment and Revision

- Develop an oversight & review plan
- Assess and revise programme controls

# Review of the PDPO

*The PCPD is working closely with the Government to comprehensive review the PDPO and formulate concrete proposals for legislative amendments, making reference to relevant laws of other jurisdictions and taking into account the actual situation in Hong Kong. The areas of review include:*

## *1. Establishing a mandatory data breach notification mechanism*

- **DPP 4: Security of personal data**
- Requiring **data users to notify the PCPD and impacted data subjects of data breach incidents**
- To enable the relevant parties to promptly respond to data breaches and take remedial measures

## *2. Requiring formulation of a data retention policy*

- **DPP 2: Duration of retention of personal data**
- Stipulating **the maximum retention period** for the personal data or if that is not possible, **the criteria** used to determine the retention period, and **the time from which retention period commences**

# Review of the PDPO

## 3. Enhancing sanctioning powers

- Introducing an administrative fine regime under the PDPO
- Empowering the Privacy Commissioner to **directly impose administrative fines** for contravention of PDPO requirements
- **Raising the criminal fine levels** under the PDPO to enhance the deterrent effect

## 4. Introducing direct regulation of data processors

- Requiring **data processors** to comply with the relevant requirements under the PDPO
- To enhance the enforcement powers of the PCPD against irregularities involving data processors

# Thank you



2827 2827



[www.pcpd.org.hk](http://www.pcpd.org.hk)



[communications@pcpd.org.hk](mailto:communications@pcpd.org.hk)

