PCPD H K

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

CityU School of Law
香港城市大學
City University of Hong Kong

Safeguarding Data Security Amid Increasing Cyberattacks

School of Law, City University of Hong Kong
Course: Law and Technology (PLE5031/LW566H)
16 February 2024

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data

Content

This presentation covers…

1. Overview of the Data Protection Principles as specified in the Personal Data (Privacy) Ordinance (PDPO)

2. Cyberattacks and data breaches

3. PCPD's initiatives to promote data security

Definition

Personal data means any data –

(Section 2(1) of the PDPO)

Relating directly or indirectly to a living **individual**;

From which it is practicable for the **identity** of the individual to be directly or indirectly **ascertained**; and

In a form in which **access to or processing of** the data is **practicable**

Who?
Three groups are involved

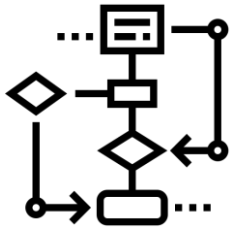
Data Subject

The individual who is the **subject** of the data

Data User

A person who, either alone or jointly or in common with other persons, **controls** the **collection, holding, processing or use** of the data

Data Processor



A person who –

a) Processes personal data **on behalf of another person**; and

b) Does **not** process the data for any of the person's **own purposes**

6 Data Protection Principles

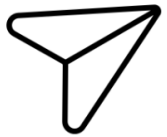
(Schedule 1 to the PDPO)

Represent the core requirements of the **Personal Data (Privacy) Ordinance (PDPO)**

Cover the **entire lifecycle** of the handling of personal data, from **collection, holding, processing, use to deletion**

Data users must comply with the DPPs

DPP1
Purpose and Manner of Collection of Personal Data



Must be collected for a **lawful purpose directly related to a function or activity** of the data user

The data is **necessary, adequate but not excessive** in relation to the purpose of collection

The **means of collection** must be **lawful** and **fair**

All practicable steps shall be taken to **inform** the data subject whether it is obligatory to supply the personal data, the **purpose** of data collection, and the **classes of persons to whom the data may be transferred**, etc.

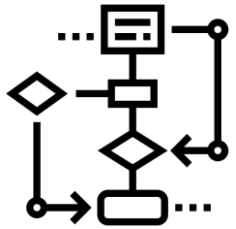
DPP2
Accuracy and duration of retention

Data User

Should take **all practicable steps** to ensure:

- the **accuracy** of the personal data
- the personal data is **not kept longer than is necessary** for the fulfilment of the purpose for which the data is used

Data Processor

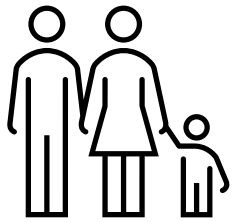


If a **data processor** is engaged to process personal data, the data user must adopt **contractual or other means** to prevent the personal data from being kept longer than is necessary

DPP3
Use of personal data

Personal data shall not, without the **prescribed consent** of the data subject, be used for a new purpose.

> "***Prescribed consent***" means *express consent given voluntarily which has not been withdrawn in writing*



Minors

Under certain circumstances, a relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using the data subject's personal data for a **new purpose**.

> "***New purpose***" means any purpose which is *unrelated to the original purpose or its directly related purpose* when the data is collected

DPP4
Security of personal data

Data users should take **all practicable steps** to ensure the personal data that they hold is **protected against unauthorised or accidental access, processing, erasure, loss or use**

If a **data processor** is engaged, 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

DPP5
Openness

All practicable steps should be taken to ensure that a person can:

Ascertain a data user's **policies and practices** in relation to personal data

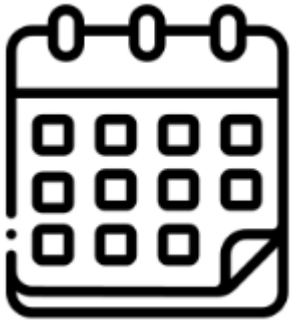
Be informed of the **kind of personal data** held by a data user

Be informed of the main **purposes** for which personal data held by a data user is or is to be used

DPP6
Data access and correction

A data subject must be given **access to his personal data**

A data subject must be **entitled to the right to request corrections** where the data is inaccurate.



A data user must comply with a **data access/correction request (DCR) within 40 days** after receipt

Content

We now turn to…

1. Overview of the Data Protection Principles as specified in Personal Data (Privacy) Ordinance (PDPO)

2. Cyberattacks and data breaches

3. PCPD's initiatives to promote data security

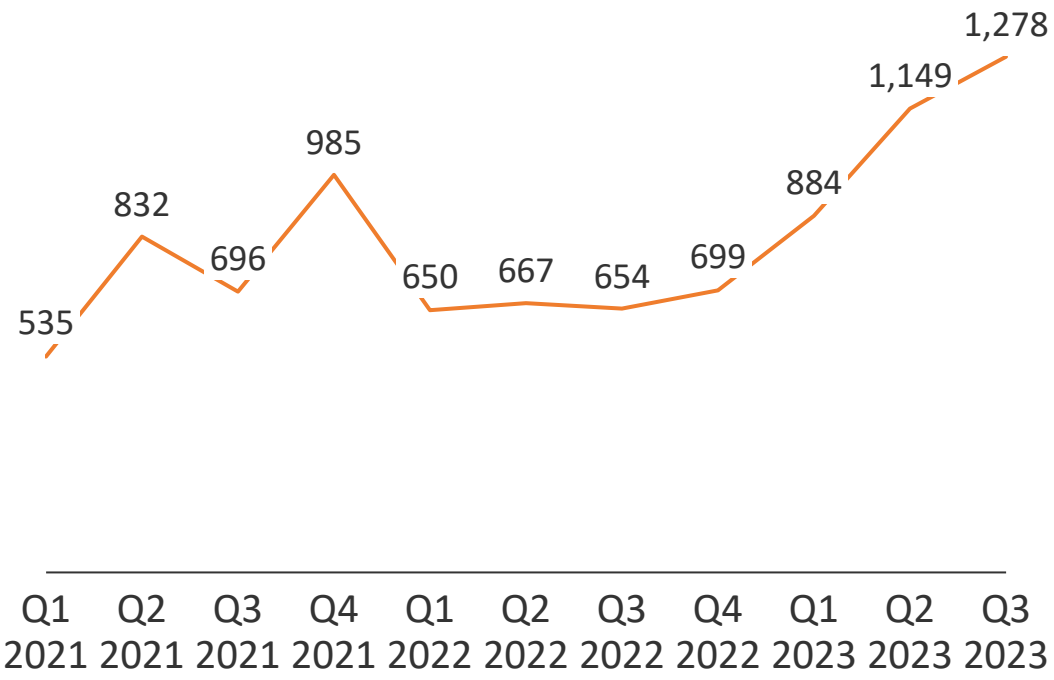
Global Situation

The bad news is that cyberattacks are rising

Cyberattacks around the world

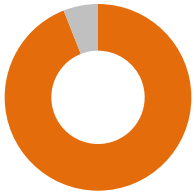
Ransomware victims

Q1 2021 – Q3 2023



Source:Corvus

State of play in 2023



94%

of **organisations** experienced **cyberattacks** in a global survey

57%

of **IT professionals lose sleep** worrying about the organisation being hit by a cyberattack

Source: Sophos

Global Examples

The Medibank and social media cases – why we need to be worried

Medibank (2022)

- Hackers used the credential stolen from an employee account with preferential access to the internal system of the insurer
- Health data of over 9 million customers breached

Source: Reuters (2022)

Global Data Breach Involving Social Media Platforms (2024)

- Reports that researchers uncovered global data breach incidents affecting various online platforms involving 26 billion records of personal data

Source: PCPD (2024)

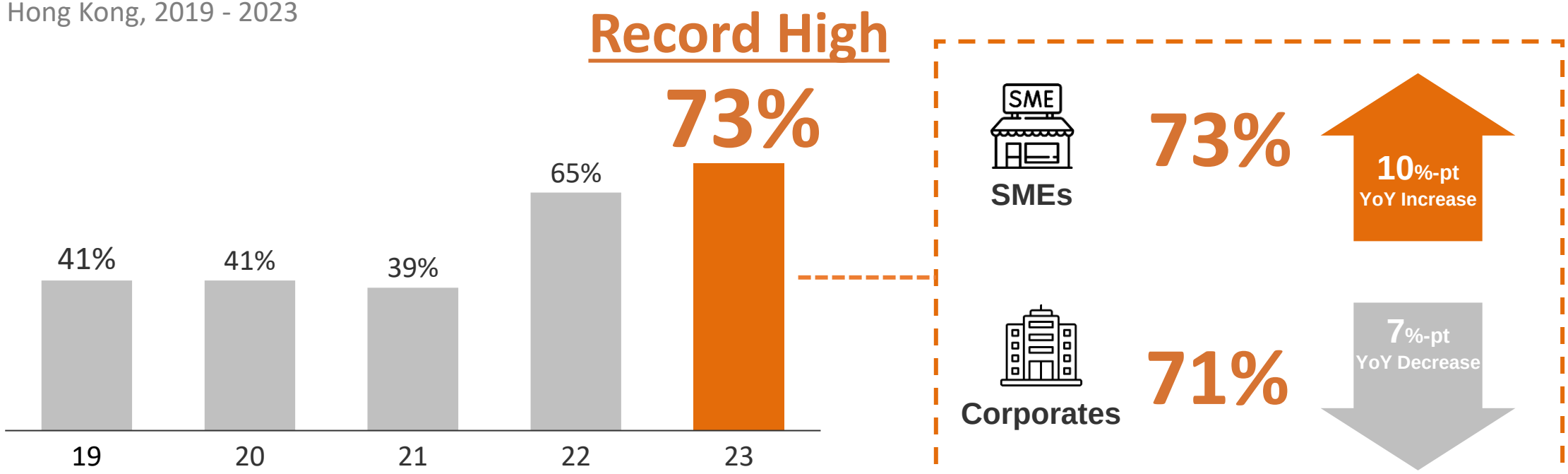
Local Cyber Security Attacks

Cyberattacks are also increasing in Hong Kong

PCPD's survey with HKCERT shows nearly ¾ of enterprises faced cyberattacks in 2023, the highest in five years

% of enterprises that encountered cyberattacks in the past 12 months

Hong Kong, 2019 - 2023



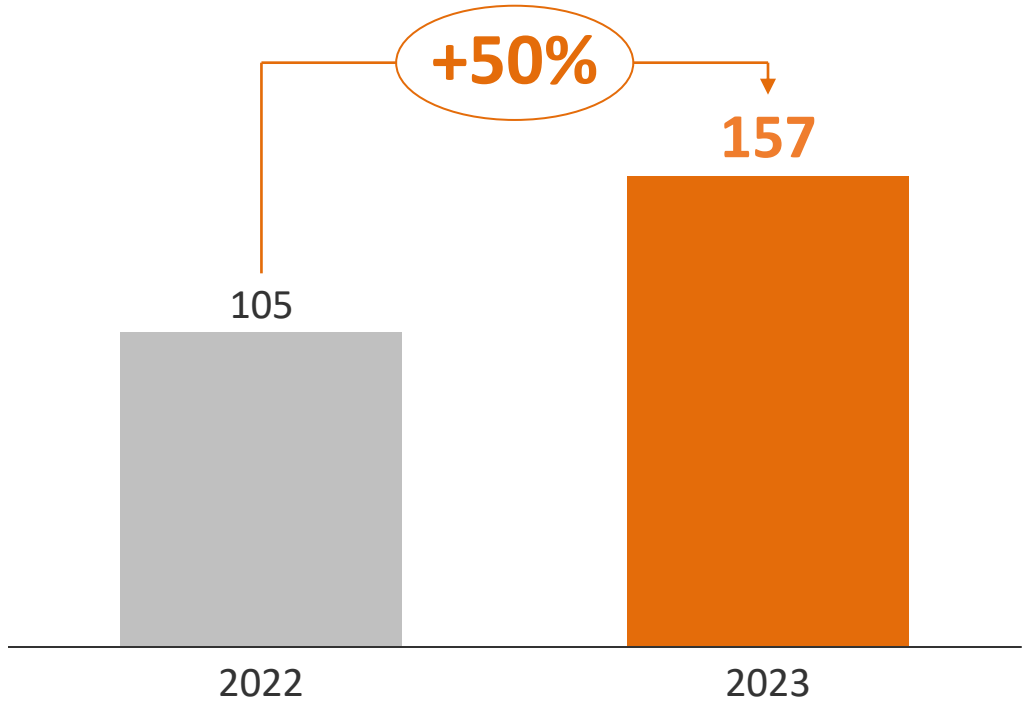
Source: Hong Kong Enterprise Cyber Security Readiness Index

Local Data Breaches

Data breach notifications surged in 2023; hacking was a major contributor

Compared with 2022, DBNs in 2023 rose substantially by 50%

Data breach notifications to PCPD



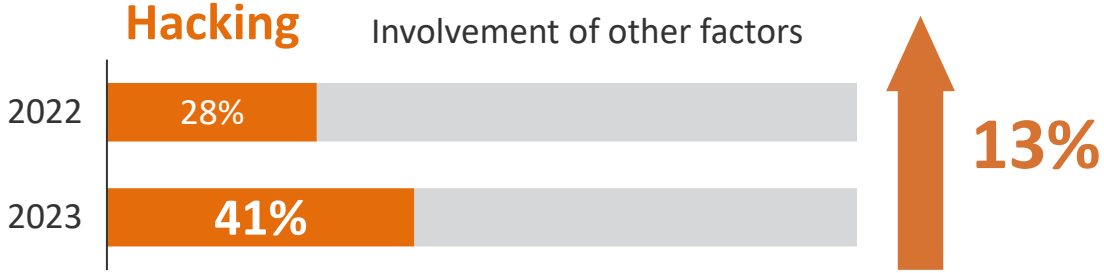
Source: PCPD

DBNs involving hacking rose both absolutely and relatively

Data breach notifications involving hacking

Absolute numbers

As a percentage of total



Legal Liability

A data breach may amount to contravention of DPP4(1) and (2)

DPP4(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.

DPP4(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.

Inspections and Compliance Checks

PCPD takes proactive actions

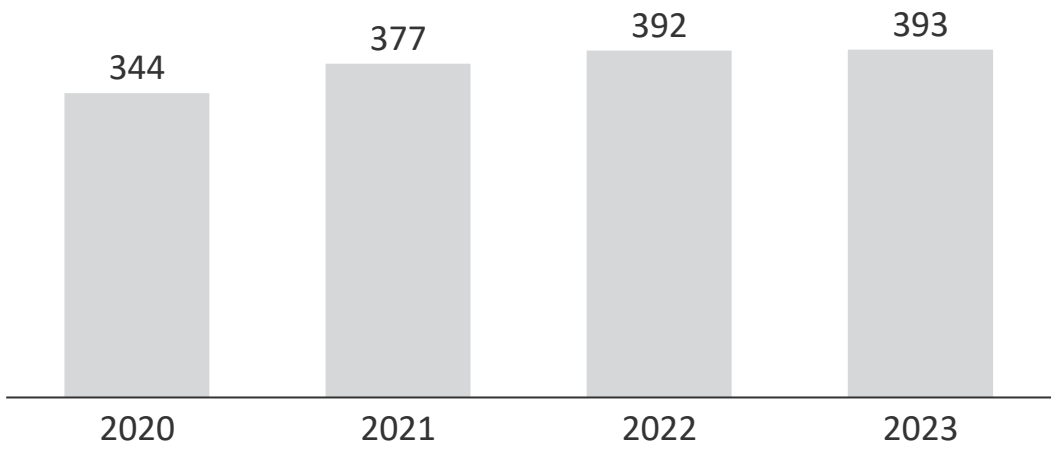
Inspections

Inspections by PCPD in the past three years

Report Date	Companies Inspected
9 Oct 23	ZA Bank Limited
20 Sep 23	The Registration and Electoral Office
20 Dec 22	TransUnion Limited
18 Aug 21	(1) CLP Power Hong Kong Limited and (2) The Hongkong Electric Company, Limited

Compliance checks

Compliance checks initiated by PCPD



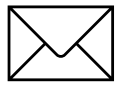
Selected compliance checks launched in 2023

- All credit reference agencies
- Users of AI systems

Investigation against Carousell Limited

Unauthorised scraping of personal data of Carousell users

Background



The investigation arose from **a data breach notification lodged by Carousell Limited**

The company reported that a **listing posted on an online forum offered the sale of the personal data** of 2.6 million Carousell users, including the personal data of **324,232 users in Hong Kong**

Carousell's Explanation

The data breach incident was caused by a **security vulnerability relating to a system migration**

Data User's Obligation

Although Carousell Limited was at all material times using the information systems and database under the centralised model of the Carousell Group, **Carousell Limited as a data user under the PDPO has a positive duty to safeguard the security of the personal data under its control**

Investigation against Carousell Limited
Findings

From the evidence collected in the investigation, the Privacy Commissioner considered that the incident had been caused by these deficiencies:

- Failure to check whether a privacy impact assessment was conducted
- Failure to check whether a comprehensive code review process was implemented
- Failure to ensure a thorough security assessment was conducted
- Failure to check and ensure that there was a written policy for the code review process
- Failure to ensure that effective detection measures were implemented

Investigation against Carousell Limited
Decision

DPP4(1) contravention

Carousell Limited had **not taken all practicable steps** in relation to the system migration to ensure that the **personal data held by Carousell were protected from unauthorised or accidental access, processing, erasure, loss or use,** thereby contravening DPP 4(1) concerning the **security of personal data**

The Privacy Commissioner served an Enforcement Notice on Carousell Limited, directing it to remedy and prevent recurrence of the contravention

Content

We now turn to…

1. Overview of the Data Protection Principles as specified in Personal Data (Privacy) Ordinance (PDPO)

2. Cyberattacks and data breaches

3. PCPD's initiatives to promote data security

PCPD's Data Security Initiatives

PCPD is helping data users enhance data security and prevent data breaches

Data Security Thematic Webpage

One-stop access to resources on data security

Data Security Scanner

Self-assessment toolkit for enterprises to assess adequacy of data security measures of ICT systems

Data Security Hotline

Provide SMEs with a channel to make enquiries about compliance with the PDPO

Guidance Materials

- **Data Breach Response Plan**
- **Guidance Note on Data Security Measures for ICT**
- **Privacy Management Programme (PMP)**

Data Breach Response Plan

Putting a plan in place can help minimise impact of a data breach

What?

A document setting out **how** an organisation should **respond in a data breach**

The plan should outline:

- a **set of procedures** to be followed in a data breach
- **strategy for identifying, containing, assessing and managing** the impact brought about by the incident from start to finish

Why?

Help ensure a **quick response** to and **effective management** of a data breach

Elements

- Description of what makes a data breach
- Internal incident notification procedure
- Contact details of response team members
- Risk assessment workflow
- Containment strategy
- Communication plan
- Investigation procedure
- Record keeping policy
- Post-incident review mechanism
- Training or drill plan

Handling Data Breaches

Handling a data breach requires 5 steps, with a preparatory plan in place

PCPD HK PCPD.org.hk

Guidance Note

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Guidance on Data Breach Handling and Data Breach Notifications

INTRODUCTION

Good data breach handling makes good business sense

A good data breach handling policy and practice is not only useful for containing the damage caused by a breach, but also demonstrate the data user's responsibility and accountability when tackling the problem, by formulating a clear action plan that can be followed in the event of a data breach. In addition to enabling the data subjects affected by the breach to take appropriate protective measures, data breach notifications can help reduce the risk of litigation and maintain the data user's goodwill and business relationships, and in some cases the public's confidence in the organisation.

This guidance is aimed at assisting data users to prepare for and handle data breaches, to prevent recurrence and to mitigate the loss and damage caused to the data subjects involved, particularly when sensitive personal data is involved.

What is personal data?

Data breach incidents often involve the personal data of individuals, such as customers, service users, employees and job applicants of organisations. Under the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) (PDPO), personal data means any data[1]

(a) relating directly or indirectly to a living individual;

(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

(c) in a form in which access to or processing of the data is practicable.

What is a data breach?

A data breach is generally regarded as a suspected or actual breach of the security of personal data held by a data user[2], which exposes the personal data of data subject(s) to the risk of unauthorised or accidental access, processing, erasure, loss or use.

The following are some examples of data breaches:

- The loss of personal data stored on devices such as laptop computers, USB flash drives, portable hard disks or backup tapes

1 Section 2(1) of the PDPO.

2 Under section 2(1) of the PDPO, a "data user", in relation to personal data, me other persons, controls the collection, holding, processing or use of the data.

Guidance on Data Breach Handling and Data Breach Notifications 1

Handling data breaches

1. Gathering essential information immediately
2. Containing the data breach
3. Assessing the risk of harm
4. Considering giving data breach notifications
5. Documenting the breach

Guidance Note on Data Security Measures for ICT

We recommend best practices in strengthening data security

Background

We have witnessed an **increasing number of data breaches** over the years

Data users should step up their data security measures to **prevent malicious attacks** on their information systems

Robust data security system is a core element of **good data governance**

7 Recommended Measures

Taking the below measures enhances data security of organisations

Data Governance & Organisational Measures

Technical and Operational Security Measures

Remedial Actions in the event of Data Security Accidents

Other Considerations

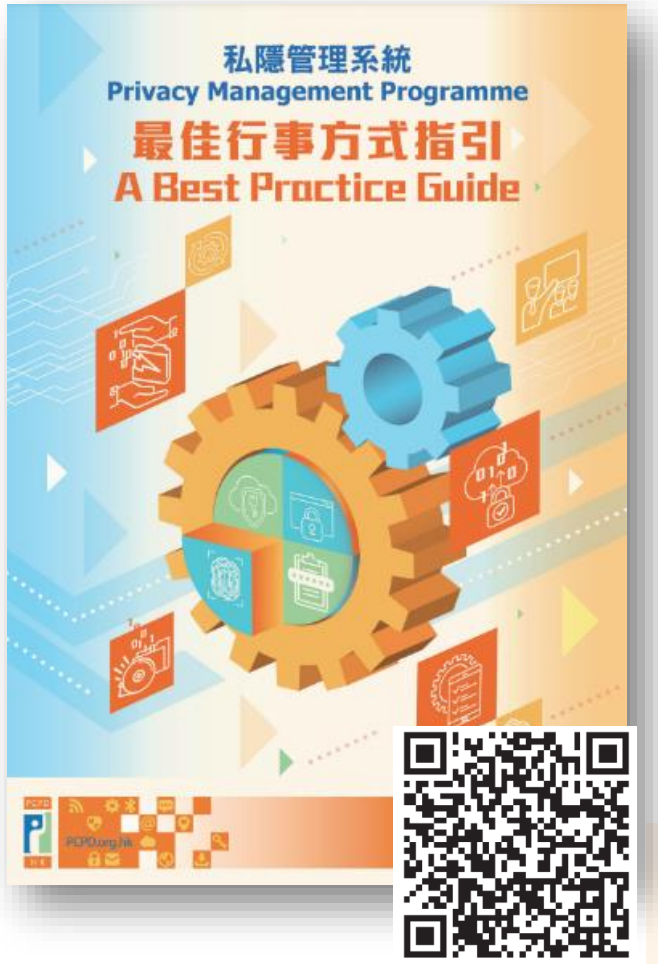
Risk Assessments

Data Processor Management

Monitoring, Evaluation and Improvement

Privacy Management Programme (PMP)

Definition and benefits of adoption



What's PMP?

A **management framework**

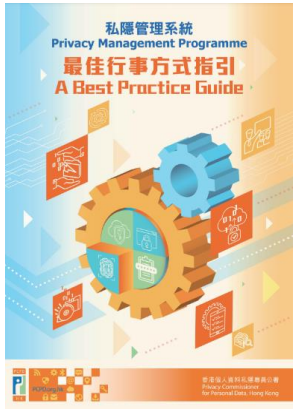
- For the **responsible collection, holding, processing** & **use of personal data** by the organisation
- To **ensure compliance with Personal Data (Privacy) Ordinance** (PDPO)

Why PMP?

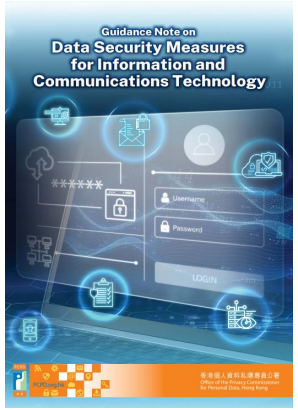
- **Minimise risk of data security** incidents
- **Handle data breaches effectively** to minimise damage
- **Ensure compliance** with PDPO
- **Build trust** with employees and customers, and enhance corporate reputation and competitiveness

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

1 Privacy Management Programme: A Best Practice Guide (revised in Mar 2019)



2 Guidance Note on Data Security Measures for Information and Communications Technology (Aug 2022)



3 Guidance on Data Breach Handling and Data Breach Notifications (revised in Jun 2023)

4 Guidance on the Ethical Development and Use of Artificial Intelligence (Aug 2021)

Thank you

PCPD

H K

2827 2827

www.pcpd.org.hk

communications@pcpd.org.hk