HKICS Annual Corporate and Regulatory Update
11 June 2021

Data Protection for Governance Professionals

Ada Chung Lai-ling

Privacy Commissioner for
Personal Data, Hong Kong

Data Breach Is on the Rise: Major data breaches in recent years and individuals affected

2020	Estée Lauder	440 million
	Microsoft	250 million
	Instagram, TikTok, Youtube	235 million
2019	Capital One (Bank)	160 million
	Zynga (Online game developer)	218 million
	Facebook	419 million
2018	Marriott Hotel	383 million
	Twitter	330 million
	Facebook	140 million
	Uber	57 million
	Cathay Pacific Airways	9.4 million

Reference: Nord VPN, Forbes

Major data breaches in 2021

Platforms	Affected individuals	Individuals in Hong Kong
Facebook	533 million	2.93 million
LinkedIn	500 million	280,000 (All Hong Kong users)
Clubhouse	1.3 million	Unknown
Air India	4.5 million	Unknown

Over 1 billion users affected

Personal Data (Privacy) Ordinance, Chapter 486 (PDPO)

6 Data Protection Principles (DPP)

- Represent the core requirements of the PDPO
- Cover the entire lifecycle of personal data from collection, holding, processing, use to deletion
- Data users have to comply with the DPPs

DPP1 – Purpose and manner of collection of personal data

- Must be directly related to a function or activity of the data user
- The means of collection must be lawful and fair
- The data is adequate but not excessive in relation to the purpose of collection
- Be transparent as regards the purpose of collection and the potential transferees, etc.

DPP2 – Accuracy and duration of retention of personal data

Data users should take all practicable steps to ensure:

- the accuracy of the personal data
- the personal data is deleted after fulfilling the purpose of collection

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 subjects, be used for a new purpose

"New purpose" means any purpose which is unrelated to the original purpose when collecting the data

- 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

DPP4 – Security of personal data

- DPP4 requires that data users should take all practicable steps to protect the personal data they hold against unauthorised or accidental access, processing, erasure, loss or use.
- Adequate protection must be given to the storage, processing and transfer of personal data.
- If a data processor is engaged, the data user must adopt contractual or other means to ensure that the data processor comply with the data security requirement.

DPP5 – Information to be generally available

Transparency

Data users must provide information on: -

i. the policies and practices in relation to personal data;

ii. the kinds of personal data held; and

iii. the main purposes for which personal data is used.

DPP6 – Access to personal data

Data subject's rights

A data subject is entitled to:

i. Request access to his/her personal data at a fee (if any) that is not excessive

ii. Request the correction of his/her personal data

A data user must comply with a data access/correction request within 40 days after receipt of the request

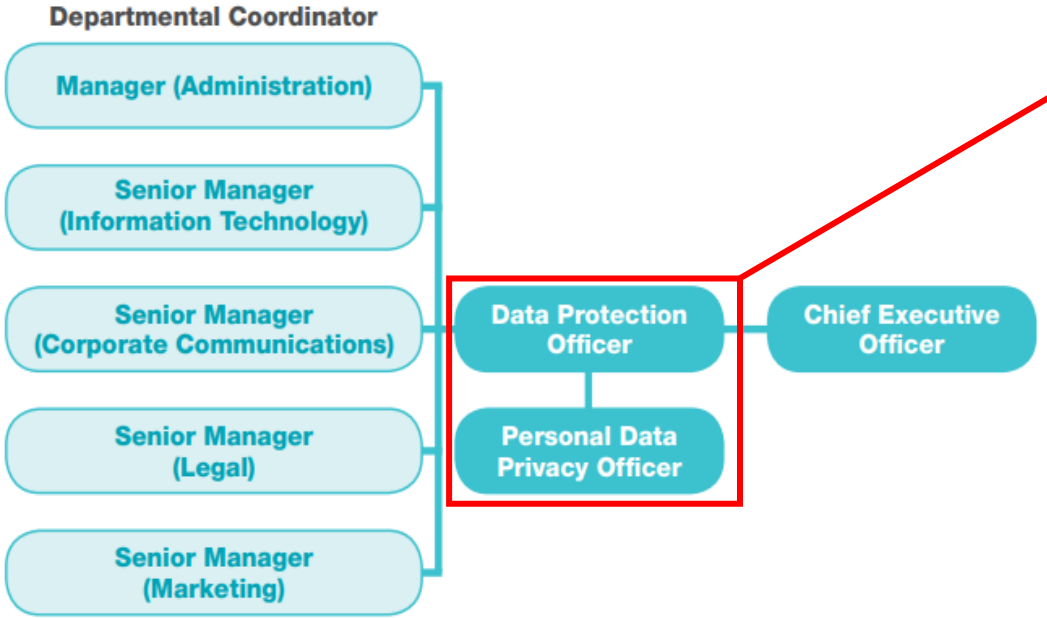
Privacy Management Programme (PMP)

1.1 Buy-in from the Top

1.2 Appointment of Data Protection Officer/Establishment of Data Protection Office

1.3 Establishment of Reporting Mechanisms

1.2 Appointment of Data Protection Officer /Establishment of Data Protection Office



Duties of a DPO, e.g.-

- **Establish** and **implement** PMP
- **Review** the effectiveness of PMP
- **Report to top management** periodically

Privacy Management Programme (PMP)

2.1 Personal Data Inventory

2.2 Internal Policies on Personal Data Handling

2.3 Risk Assessment Tools

2.4 Training, Education and Promotion

2.5 Handling of Data Breach Incident

2.6 Data Processor Management

2.7 Communication

2.1 Personal Data Inventory

WHY – Personal data inventory helps organisations to:

a) understand the type of consent needed from data subjects;

b) determine how personal data is protected;

c) comply with data access and correction requests; and

d) respond to data leakage incidents efficiently.

HOW - Sample of a Personal Data Inventory (P.1)

Department	Administration
Category of record	Personnel records
Items of personal data contained in the record	Employees' personal data: - Name - HKID copy - Contact information (including address, mobile number and email address)
Means of collection of the data	Employee Information Form
Purpose of collection and use of the data	Handle employment-related matters
Retention period of the data	7 years after the employee has left the service
Location for data storage	Physical: Filing cabinets in Personnel Record Room

Source: PCPD's Privacy Management Programme – A Best Practice Guide

HOW - Sample of a Personal Data Inventory (P.2)

Department	Administration
Disclosure of data to any third parties including data processors and the names and relevant details of third parties (Yes/No)	No
Possible location of transfer (e.g. cloud server location)	N/A
Purpose of disclosing the data and whether the disclosure complies with the Ordinance	N/A
Date of return or destruction by the data processor (if applicable)	N/A
Security measures adopted	Filing cabinets are locked and the key is kept by Head of Personnel Department and Personnel Officer

Source: PCPD's Privacy Management Programme – A Best Practice Guide

2.1 Personal Data Inventory

WHEN – Personal data inventory should be updated at least annually

WHO – Personal data inventory should be updated by respective departments and submitted to the DPO

2.3 Risk Assessment Tool #1: Periodic Risk Assessment

DPO provides the risk assessment questionnaire to coordinators of all/selected departments annually

Departmental coordinators complete the questionnaire

DPO reviews the completed questionnaire for any non-compliant issues

Departmental coordinators draw up mitigating measures for all identified risks

DPO signs and files the questionnaire after the risks have been mitigated

2.3 Risk Assessment Tool #2: Privacy Impact Assessment

Conducted when:

- Regulatory requirements or the organisation's personal data process changes significantly
- Introducing a new personal data handling process
- Engaging data processors to handle personal data

Organisations should:

- Devise internal policies and procedures regarding PIA
- If possible, upload the PIA to its website to enhance transparency

PIA Questionnaire:

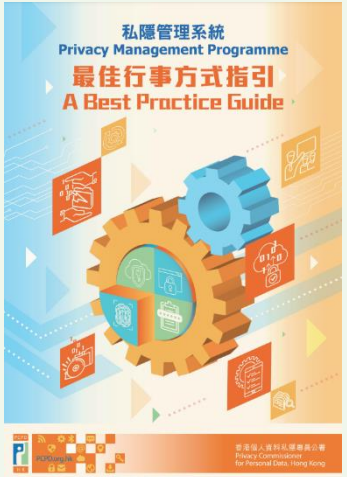
- Analyses the privacy risks according to the six DPPs and other PDPO requirements
- Devises mitigation actions for any privacy risks identified
- Should be completed by departmental coordinators and signed by the DPO

Privacy Management Programme (PMP)

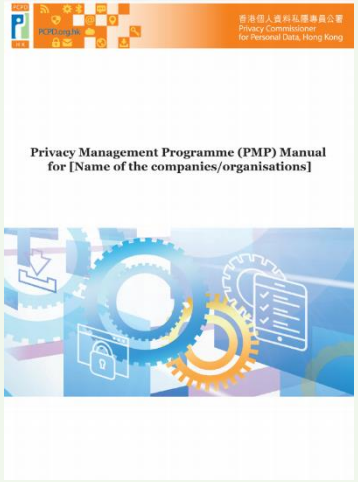
3.1 Develop an Oversight and Review Plan

3.2 Assess and Revise Programme Controls

Privacy Management Programme: A Best Practice Guide



General Reference Guide – Privacy Management Programme (PMP) Manual



New Inspection Regime of the Companies Register

Documents filed after commencement

- Public: correspondence addresses of directors and *company secretaries*, and partial identification numbers of directors, *company secretaries* and relevant individuals
- Specified persons (upon application): usual residential addresses and full identification numbers of the individuals

Documents registered before commencement

- Usual residential addresses and full identification numbers of the individuals withheld from inspection upon application made by the individuals concerned

Public Records in Overseas Jurisdictions – Company Officers

	Directors and Company Secretaries
The UK	• Identification number: N/A • Address: Correspondence / service address
Australia	• Identification number: N/A • Address: Usual residential address (unless with separate application)
Singapore	• Identification number: Yes • Address: Usual residential address (or alternate address)

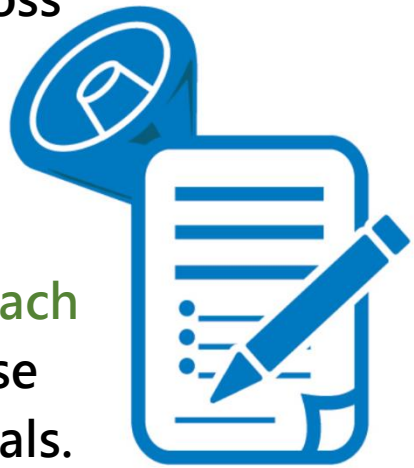
Handling Data Breaches

- What is a data breach?
- How to handle a data breach
- Common causes
- Case sharing

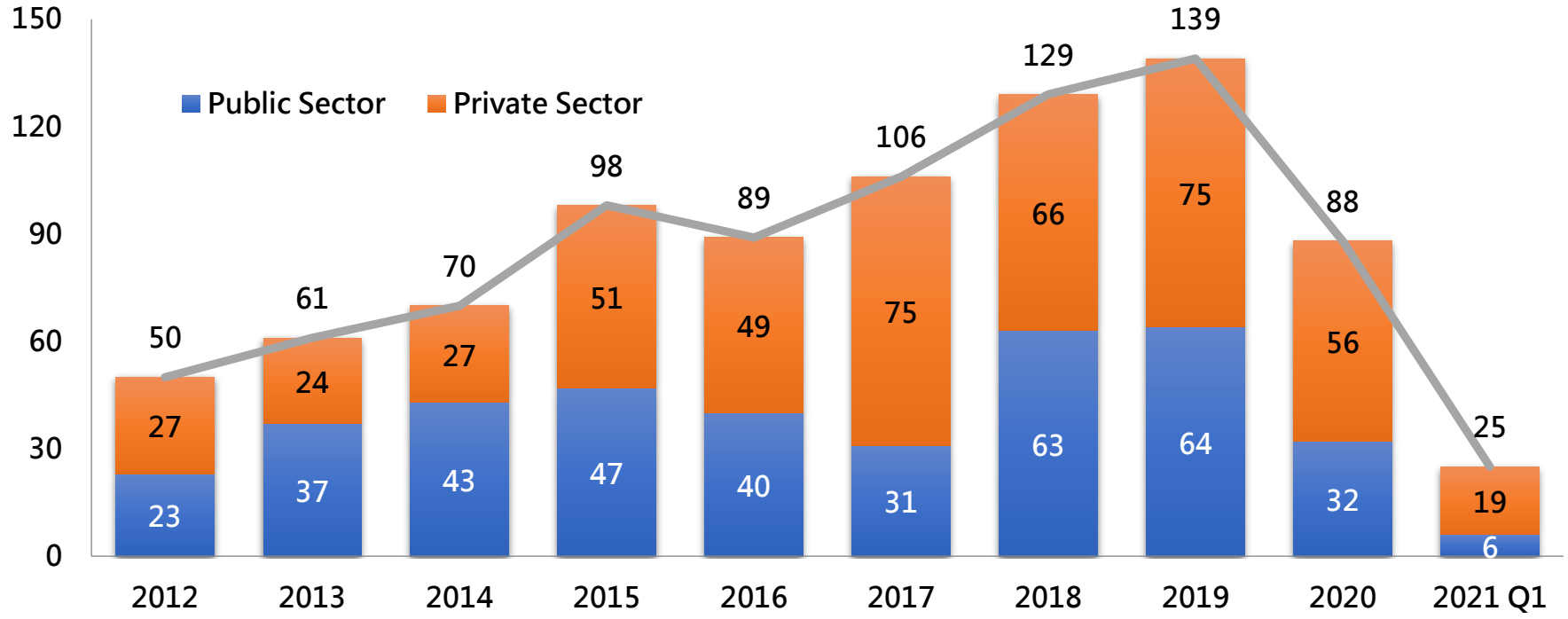
Joyce Lai Chi-man
Assistant Privacy Commissioner for Personal Data (Acting)

What is a Data Breach?

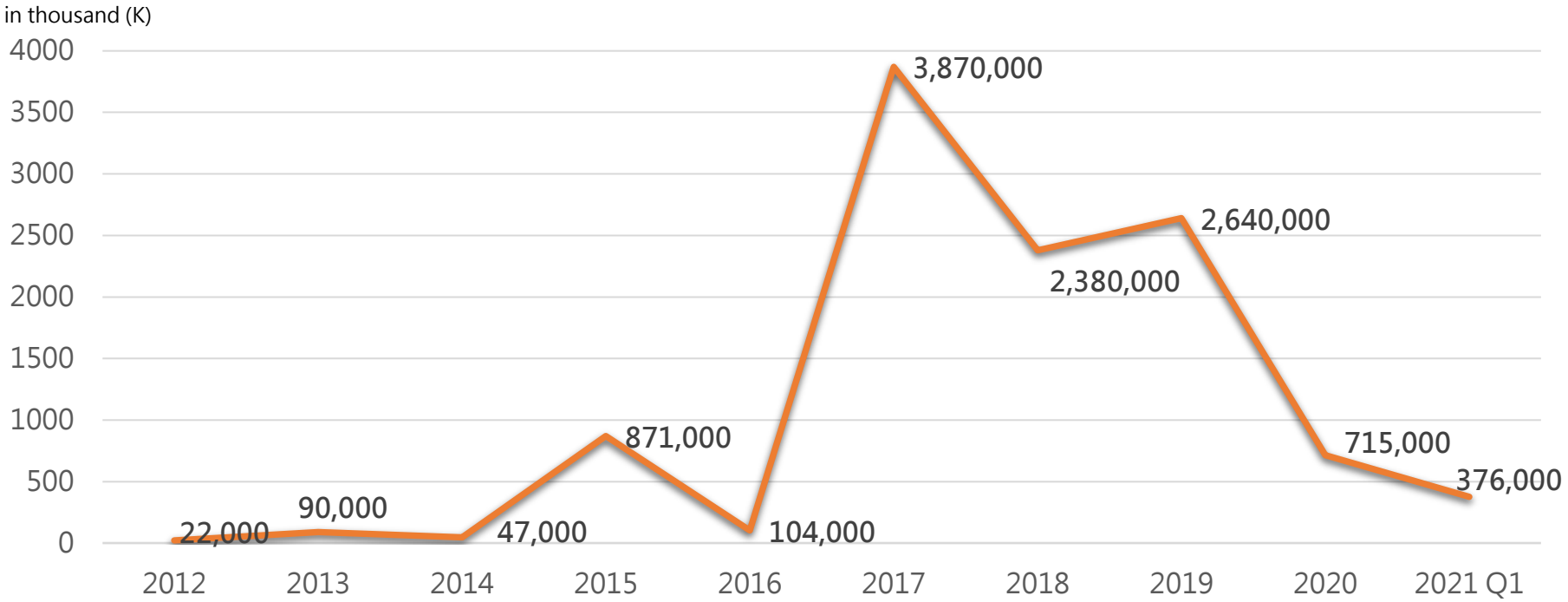
- A suspected breach of security of personal data held by a data user, which results in exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use.
- The breach may amount to a contravention of Data Protection Principle 4 – Security of personal data.
- PCPD has always encouraged data users to give data breach notifications to affected individuals and PCPD to minimise the potential damage which might be caused to individuals.



Numbers of Data Breach Notifications Received by PCPD



Numbers of Affected Individuals in Hong Kong

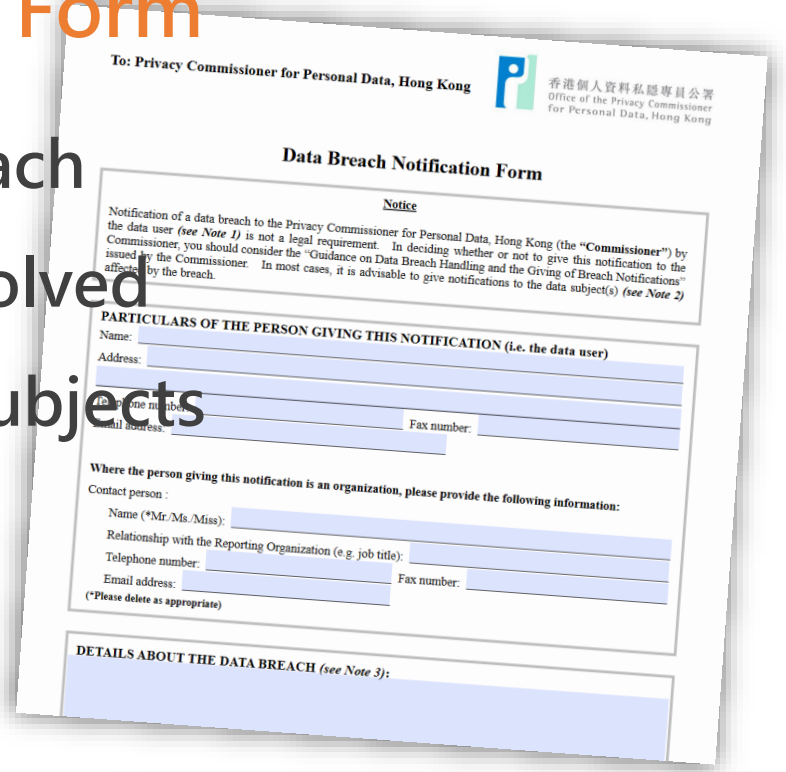


Recommended Practice for Handling Data Breach

- Collect essential information immediately
- Assess the impact on data subjects
- Adopt containment measures
- Contact stakeholders (e.g. services provider, management and affected data subjects)
- Consider giving data breach notification to PCPD

Data Breach Notification Form

- Details about the data breach
- Types of personal data involved
- Number of affected data subjects
- Risk of harm
- Containment actions



To: Privacy Commissioner for Personal Data, Hong Kong

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

Data Breach Notification Form

Notice

Notification of a data breach to the Privacy Commissioner for Personal Data, Hong Kong (the **"Commissioner"**) by the data user *(see Note 1)* is not a legal requirement. In deciding whether or not to give this notification to the Commissioner, you should consider the "Guidance on Data Breach Handling and the Giving of Breach Notifications" issued by the Commissioner. In most cases, it is advisable to give notifications to the data subject(s) *(see Note 2)* affected by the breach.

PARTICULARS OF THE PERSON GIVING THIS NOTIFICATION (i.e. the data user)

Name:

Address:

Telephone number: Fax number:

Email address:

Where the person giving this notification is an organization, please provide the following information:

Contact person :

Name (*Mr./Ms./Miss):

Relationship with the Reporting Organization (e.g. job title):

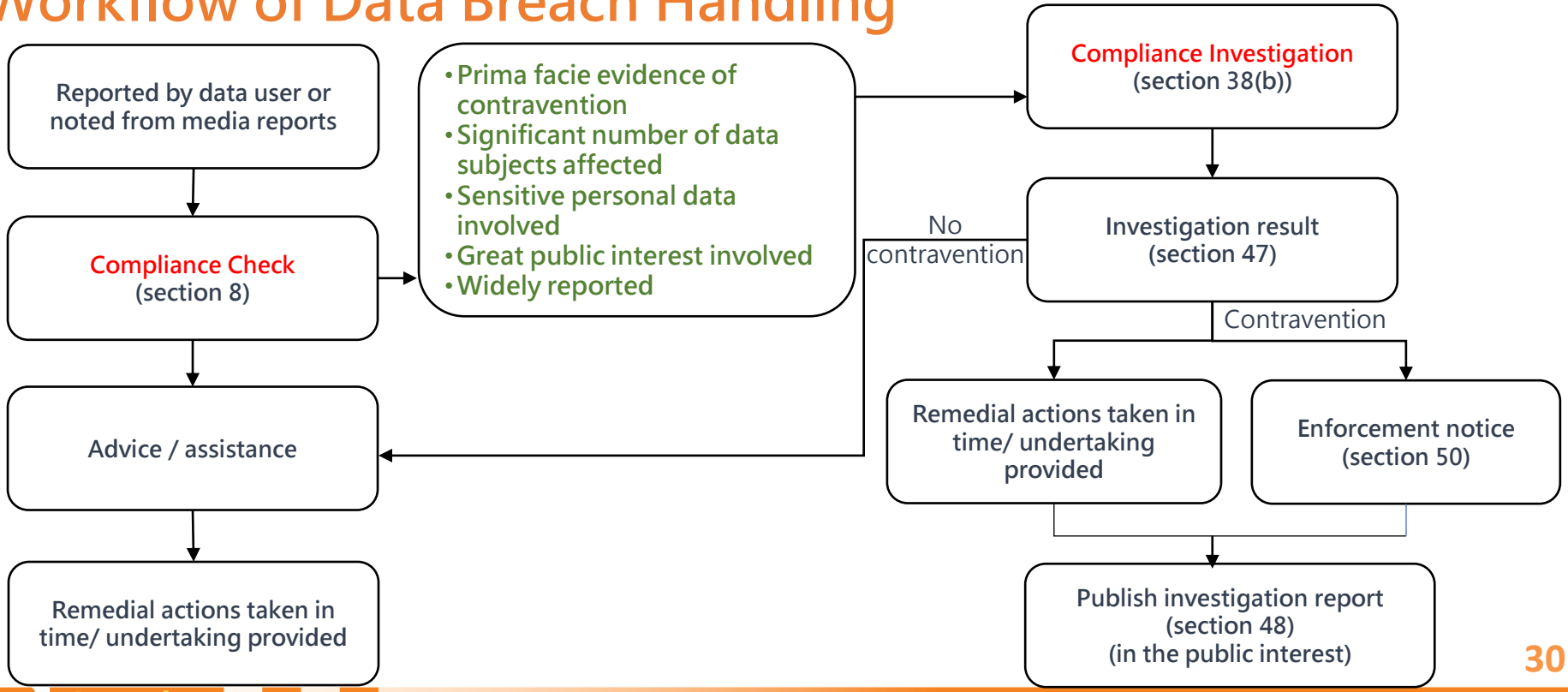
Telephone number: Fax number:

Email address:

(*Please delete as appropriate)

DETAILS ABOUT THE DATA BREACH *(see Note 3)*:

Workflow of Data Breach Handling



Common Causes of Data Breach

Loss of documents or portable storage devices

(34%)

Hacking / System misconfiguration

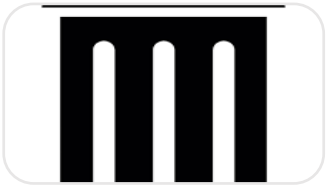
(32%)

Inadvertent disclosure through mail/email

(21%)

Employee misconduct

(10%)



Improper / Accidental disposal

(3%)

Compliance Investigations
(1) Leakage of personal data of electors

Background

A government department lost two notebook computers containing personal data of about 1,200 Election Committee members and about 3.78 million Geographical Constituencies electors during the Chief Executive Election in 2017

Results of Investigation

- Contravened Data Protection Principle 4(1) - security of personal data
- Security measures was not proportional to data sensitivity and associated risks
- Lacked requisite awareness and vigilance as well as effective communication
- Issued an Enforcement Notice – to set internal guidelines and implement effective measures to ensure staff compliance

Compliance Investigations
(2) Intrusion into customer database

Background

An obsolete database (inactive for 6 years) owned by a broadband network company was intruded in 2018 that caused leakage of personal data of about 380,000 customers

Results of Investigation

- Contravened Data Protection Principle 2(2) & 4(1) – retention & security of personal data
- Failed to conduct a comprehensive and prudent review after system migration
- Failed to give due consideration to the retention period of former customers' personal data
- Issued an Enforcement Notice – to devise clear procedures for system migration and data retention and security policies; and to erase personal data retained longer than necessary

Compliance Investigations
(3) Leakage of personal data of airline passengers

Background

Unauthorised access to personal data of approximately 9.4 million passengers of an airline company

Results of Investigation

- Contravened Data Protection Principle 2(2) & 4(1) – retention & security of personal data
- Lax data governance without applying effective authentication to all remote access users
- HKID Card numbers of some affected passengers were kept longer than necessary
- Issued an Enforcement Notice – to implement effective multi-factor authentication, conduct effective vulnerability scans and erase personal data retained longer than necessary

Compliance Investigations
(4) Unauthorised access to credit reports

Background

A local newspaper passed through the online authentication procedures of a credit reference agency and obtained the credit reports of a number of public figures

Results of Investigation

- Contravened Data Protection Principle 4(1) - security of personal data
- Vulnerabilities in online identity authentication process
- Issued an Enforcement Notice – to undergo one-time password verifications for online credit report applications; and to devise clear procedures to ensure that the Q&A for knowledge-based authentications are relevant, functional and up-to-date

JOIN

Data Protection Officers' Club

(Membership Application)

保障資料主任聯會 Data Protection Officers' Club

By becoming a DPOC member, you will:

- **advance your knowledge and practice of data privacy compliance through experience sharing and training;**
- **enjoy 20% discount on the registration fee for PCPD's Professional Workshops;**
- **receive updates on the latest development in data privacy via regular e-newsletter**

As a DPOC member, your organisation's name will be published on DPOC membership list at PCPD's website, demonstrating your commitment on personal data protection to your existing and potential customers as well as your stakeholders.

Membership fee: HK$350 per year
Enquiries: dpoc@pcpd.org.hk

https://www.pcpd.org.hk/misc/dpoc/enrol.html

Thank you!

Telephone： 2827 2827

Website： www.pcpd.org.hk

Email： communications@pcpd.org.hk