

# Personal Data Management – Handling of Data Breach Incidents for Banking Sector

9 August 2024

Ms Clemence WONG  
Senior Legal Counsel (Acting)

Ms Ayee MAN  
Senior Personal Data Officer (Acting)  
(Compliance & Enquiries)



# Relevant Requirements under the PDPO - Six Data Protection Principles (DPPs)



# DPP4: Security of Personal Data

- **All practicable steps** shall be taken to protect personal data from unauthorized or accidental access, processing, erasure, loss or use (DPP4(1))
- If a **data processor** is engaged to process personal data, the data user must adopt **contractual or other means** to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing (DPP4(2))



# DPP4: Security of Personal Data

- **All practicable steps** shall be taken to protect personal data from unauthorized or accidental access, processing, erasure, loss or use having particular regard to – (DPP4(1))
  - (a) the kind of data and the harm that could result if any of those things should occur;
  - (b) the physical location where the data is stored;
  - (c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;
  - (d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
  - (e) any measures taken for ensuring the secure transmission of the data



# DPP4: Security of Personal Data

What are all practicable steps?

General and  
Organisational  
Preventive  
Measures

Technical Security  
Measures

Mitigating Steps  
after the Data  
Breach

Other  
Considerations

# What are all practicable steps?

## General and Organisational Preventive Measures

- Embrace personal data privacy protection as part of the corporate governance responsibility, covering business practices, operational processes, policies and training
- Comprehensive and on-going review and monitoring process; build a robust privacy infrastructure
- Open and transparent information privacy policies and practices
- Demonstrate organisational commitment to personal data privacy protection with a top-down approach



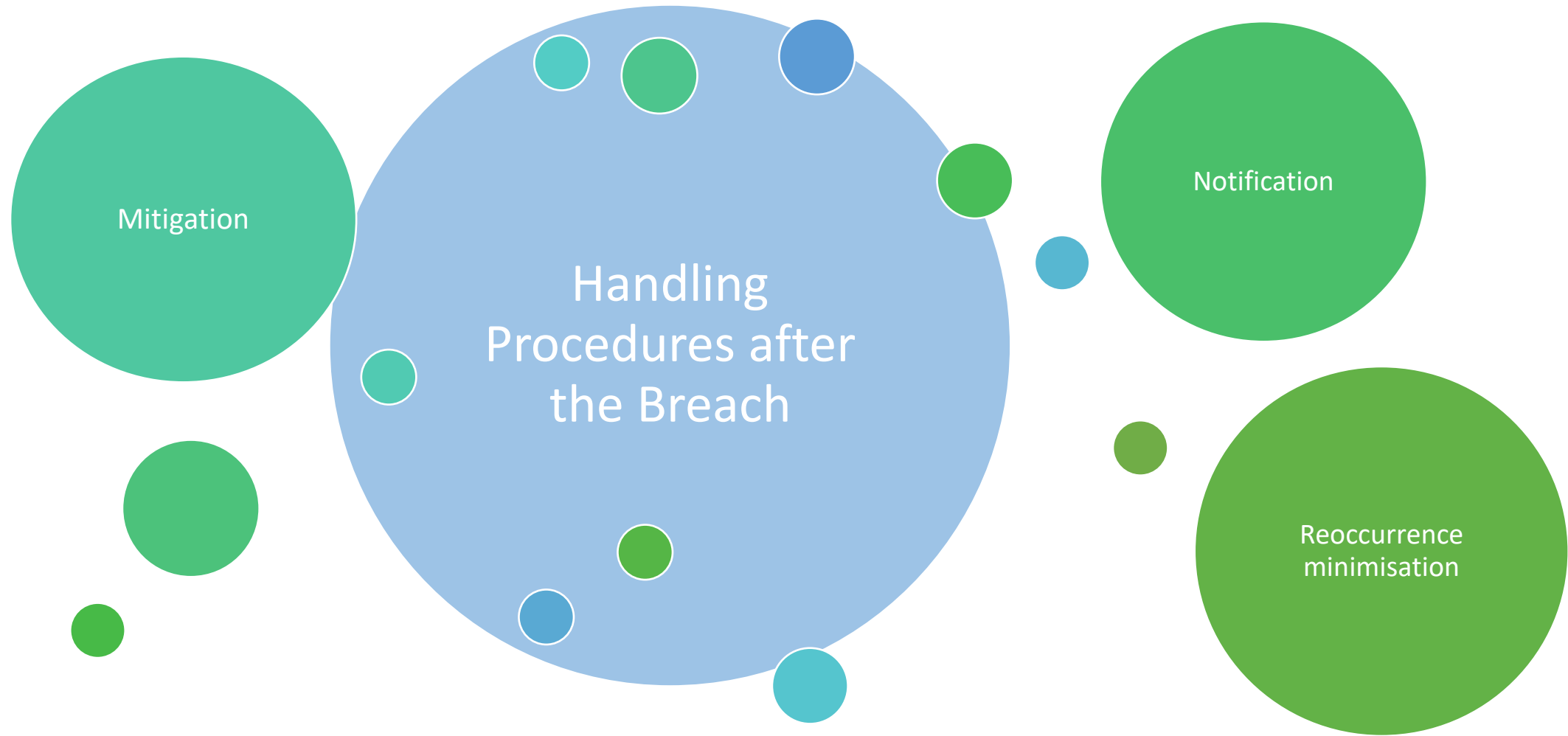
# What are all practicable steps?



## Technical Security Measures

- Hardware security, e.g. information system, network infrastructure, etc.
- Policies and procedures for regular review of security systems
- Security measures and steps for system login, data transmission and storage, adoption of international standards and technology, e.g. hashing, encryption, etc.

# What are all practicable steps?





# What are all practicable steps?

## Other Considerations

- The nature, size and resources of the data user
- The likelihood of adverse consequences for affected individuals
- The complexity of operations of the data user and its business model
- The amount and sensitivity of personal data held

# Data Breach Incident

## What is a Data Breach

A **suspected or actual breach of the security of personal data** held by a data user, exposing the personal data to the risk of unauthorised or accidental access, processing, erasure, loss or use.

## Examples

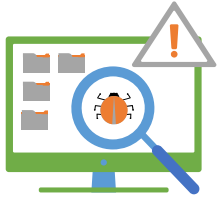
- **Loss of personal data** stored on devices
- **Improper handling** of personal data
- A database containing personal data that is **hacked or accessed by outsiders without authorisation**
- Disclosure of personal data to a third party who **obtained the data by deception**
- **Leakage of data caused by the installation of file-sharing software** on a computer



A data breach may amount to a contravention of  
Data Protection Principle 4 of Schedule 1 to the PDPO

10

# Common Causes of Data Breaches



**1. Cyberattacks**

**2. System misconfigurations**



**3. Loss of physical documents or portable devices**



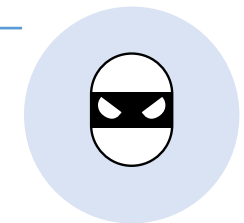
**4. Improper/wrongful disposal of personal data**



**5. Inadvertent disclosure by email or by post**



**6. Staff negligence/misconduct**



# Data Breach Handling



# Data Breach Response Plan

## 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 (Non-exhaustive)



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




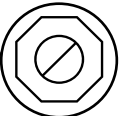
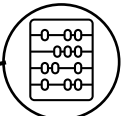


Post-incident review mechanism




Training or drill plan

# Data Breach Handling

## Steps

-  Immediate gathering of essential information
-  Containing the data breach
-  Assessing the risk of harm
-  Considering giving data breach notifications
-  Documenting the breach



**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<sup>1</sup>

(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<sup>2</sup>, 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
- The improper handling of personal data, such as improper disposal, sending emails to unintended parties or the unauthorised access of databases by employees
- A database containing personal data that is hacked or accessed by outsiders without authorisation
- The disclosure of personal data to a third party who obtained the data by deception
- The leakage of data caused by the installation of file-sharing software on a computer

1 Section 2(1) of the PDPO.  
2 Under section 2(1) of the PDPO, a "data user", in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.

Guidance on Data Breach Handling and Data Breach Notifications | 1 | June 2023

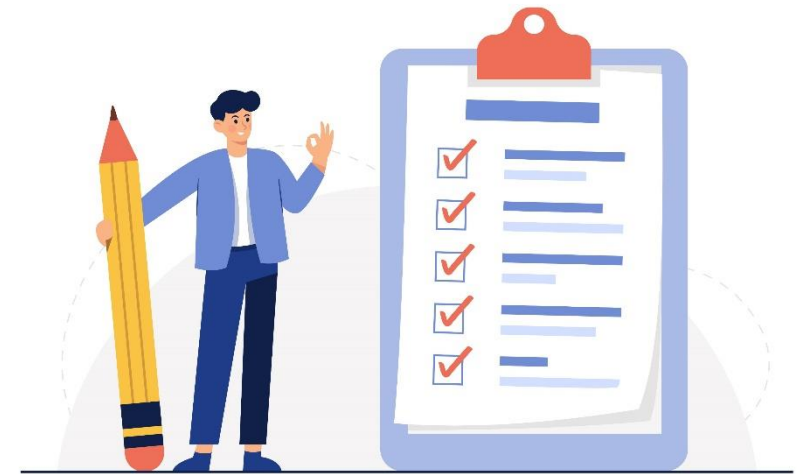


Scan to download the Guidance Note

# Step 1: Immediate Gathering of Essential Information

**Gather all relevant information of the data breach to assess the impact on data subjects and to identify appropriate mitigation measures:-**

- 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?



# Step 2: Containing the Data Breach



**Depending on the categories of personal data involved and the severity of the breach, the following containment measures (non-exhaustive) may be considered:-**

- Conducting a thorough search for the lost items containing personal data
- Requesting the unintended recipients of emails/letters/fax to delete or return the mistakenly sent documents
- Shutting down or isolating the compromised/breached system/server
- Fixing any bugs or errors that may have caused the breach
- Changing users' passwords and system configurations to block any (further) unauthorised access
- Removing the access rights of users suspected to have committed or contributed to the data breach
- Notifying the relevant law enforcement agencies if identity theft or other criminal activities have been or are likely to be committed

16





## 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 depends on the circumstances of the data breach, such as:-

- The **kind, sensitivity and amount** of the personal data being leaked
- The **circumstances 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 is adequately encrypted, anonymised or otherwise rendered inaccessible
- The duration of the breach

17

# 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:**

- Potential consequences of a breach for the affected individuals
- how serious or substantial the consequences are, and how likely they are to happen
- Consequences of failing to give notification

NOTE

The data user should notify the PCPD and the affected data subjects as soon as practicable after becoming aware of the data breach. If notification to overseas regulatory authorities is required, the data user should ensure that the notification is made within the statutory time limit in accordance with the relevant requirements, if any.

# Step 4: Considering Giving Data Breach Notifications

*This can help to:*

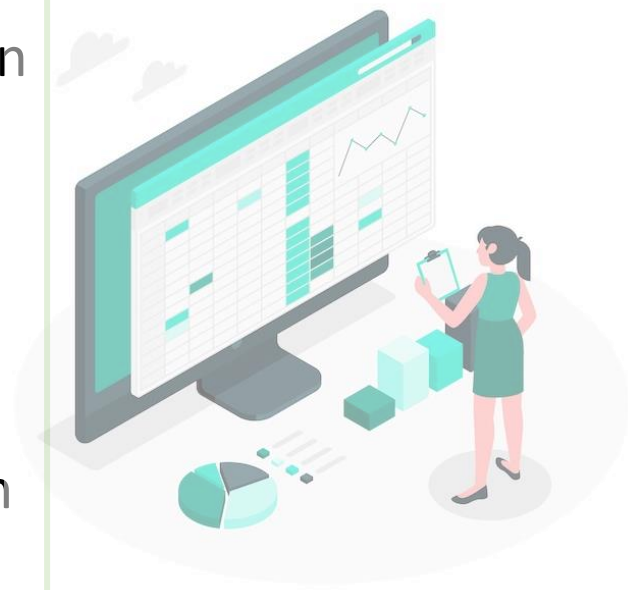
- ✓ Draw the affected data subjects' attention to **take proactive steps or measures to mitigate any potential harm or damage**
- ✓ Enable the relevant authorities to undertake appropriate **investigative or follow-up actions**
- ✓ Demonstrate the data user's commitment to robust personal data privacy management by adhering to the principles of transparency and accountability
- ✓ **Raise public awareness**
- ✓ Obtain appropriate advice from the PCPD in terms of promptly responding to the breach and improving personal data systems and policies, thus **preventing the recurrence of similar incidents**



# Step 4: Considering Giving Data Breach Notifications

*What should be included in the notification?*

- A general description of what occurred
- The **source, date and time** of the breach and its duration (or an estimate)
- The date and time when the breach was detected
- **The types of personal data involved**
- The **categories and approximate number of data subjects** involved
- **An assessment of the risk of harm** that could result from the breach
- A description of the **mitigation measures taken or to be taken**
- **The contact information** of the data breach response team or of a staff member designated to handle the data breach



# Step 4: Considering Giving Data Breach Notifications

## How to notify?

### Notification to the data subjects

- The data subjects can be notified directly by phone, in writing, via email or in person
- When a direct data breach notification is not practicable in the circumstances, then public announcements, newspaper advertisements or announcements on websites or social media platforms may be more effective

### Notification to the PCPD

- Submit the completed Data Breach Notification Form to the PCPD online, by fax, in person, by post or email
- Oral notifications are not accepted

NOTE

The PCPD does not accept oral notification. The PCPD may carry out compliance actions to investigate a data breach incident regardless of whether the data user has reported the incident to the PCPD.

**Data Breach Notification Form**

A data breach is generally taken to be a breach of the security of the 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. Depending on the circumstances of the case, the breach in question may amount to a contravention of Data Protection Principle 4 of the Personal Data (Privacy) Ordinance (the Ordinance).

Although it is not mandatory under the Ordinance for data users to give data breach notifications, data users are encouraged to give such notifications timely to the Office of the Privacy Commissioner for Personal Data (PCPD), the affected data subjects and other relevant parties when a data breach has occurred.

This notification form is for a data user to report a data breach to the PCPD and it may take about 10-15 minutes to complete. You may refer to our "Practical Tips for Handling Data Breach Incident" at Annex for more information.

**Personal Information Collection Statement**

Please be advised that it is voluntary for you to supply to the PCPD your personal data. All personal data submitted will only be used for purposes which are directly related to this data breach notification and the exercise of the regulatory powers and functions of the Privacy Commissioner for Personal Data.

You have the right to request access to and correction of your personal data held by the PCPD. Request for access or correction of personal data should be made in writing to the Data Protection Officer at the address: 12/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong.

The personal data submitted may be transferred to parties who may be contacted by the PCPD during the handling of this case including agencies who are authorised to receive information relating to law enforcement or prosecution.

I understand the above and I would like to submit a data breach notification on behalf of a data user.\*

\* Mandatory \* Please circle as appropriate

**BASIC INFORMATION OF THE DATA USER**

User Sector :  Private Sector  Public Sector

Company/organisation name\* : \_\_\_\_\_

Hong Kong office's correspondence address : \_\_\_\_\_

**INFORMATION OF THE CONTACT PERSON**

Name of person making this notification\* : Mr / Ms / Miss \_\_\_\_\_

Job Title : \_\_\_\_\_ Email address : \_\_\_\_\_

Country code (for non-Hong Kong phone number) : \_\_\_\_\_

Contact phone number\* : \_\_\_\_\_

Are you the Data Protection Officer for your company/organisation?  Yes  No

Data Breach Notification Form

# Step 5: Documenting the Breach

- Keep a comprehensive record of the incident which should include all facts relating to the breach, including details of the breach and its effects to the containment and remedial actions taken
- Learn from the data breach incident, facilitate a post-breach review and improve personal data handling practices as appropriate
- Organisations that are required to comply with the laws and regulations of other jurisdictions should consider whether there are any mandatory documentation requirements under those laws and regulations



For example, the General Data Protection Regulation of the European Union requires the data controllers to keep documentation of all data breaches

# Case Sharing



## ▶▶ Case (1): Unauthorised download of customers' personal data by a contractor

A contractor of a bank downloaded 964 data files from the bank's computer workstation to his personal mobile device without authorisation, although the contractor was granted access to those raw data under the bank's supervision in a system development project. This incident involved personal data of approximately 210,000 customers.



The incident was caused by misconfiguration of the bank's data loss prevention system, which failed to block the transfer of data from computer workstations to "Windows Portable Devices" such as smartphones and tablets.



## ▶▶ Case (1): Unauthorised download of customers' personal data by a contractor

In the wake of the incident, the bank had:

- **re-configured the data loss prevention system controls to block all data connection with Windows Portable Devices**
- **implemented an Internet cloud-monitoring capability tool to monitor external data transfers through Internet services**
- **Enhanced inadvertent data disclosure tool and end-point security tool to prevent malicious or unauthorised data transfer**
- **Revising its procedures that allow only dummy or masked personal data to be used for the purposes of testing and system development in future.**



Organisations should implement appropriate security measures with regular review so as to protect the personal data held by them from unauthorised or accidental access, processing, loss or use.

## ▶▶ Case (2): Unauthorised transfer of personal data to a personal computer by a staff member

A financial institution reported that an administrative staff member copied more than 4,000 files from the office desktop computer to his personal laptop via his own USB flash drive without authorisation, in which 51 files contained personal data of around 6,600 customers, 30 staff members and unsuccessful job applicants.



The staff member concerned was the only staff who was granted permission to use USB flash drive with read-and-write functions in discharging his duties. The staff member explained that he copied the files to his personal laptop with a view to cleaning up the space of the hard disk of his office computer which was running slow at the material time.

26

## ▶▶ Case (2): Unauthorised transfer of personal data to a personal computer by a staff member

In the wake of the incident, the financial institution had:

- **revoked the USB write-access right** of the staff member concerned
- **reminded all staff members** the institution's policy on secure use of removable storage devices
- **arranged training for all staff members** in information security risk



Organisations should **attach great importance to data governance** and the **culture of respecting and protecting privacy** and should **regularly review and monitor staff members' access right to personal data.**

# Recommended Data Security Measures for Information and Communications Technology (ICT)



# Recommended Data Security Measures for ICT

Data Governance & Organisational Measures

Risk Assessments

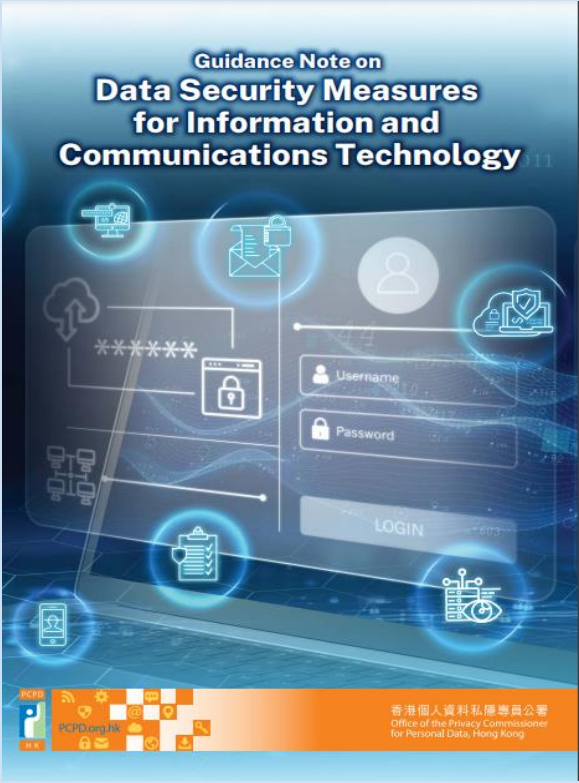
Technical and Operational Security Measures

Data Processor Management

Remedial Actions in the Event of Data Security  
Accidents


Monitoring, Evaluation and Improvement

Other Considerations



The image shows the cover of a guidance note titled "Guidance Note on Data Security Measures for Information and Communications Technology". The cover features a central graphic of a laptop screen displaying a login form with fields for "Username" and "Password", and a "LOGIN" button. The screen is surrounded by various icons representing data security, such as a padlock, a document with a checkmark, a person icon, and a cloud with a shield. The background is a dark blue with glowing lines and icons. At the bottom of the cover, there is a logo for the Office of the Privacy Commissioner for Personal Data, Hong Kong, and the text "PCPD.org.hk".

**Download the Guidance Note**



A large QR code is positioned to the right of the guidance note cover, intended for users to scan and download the document.

# Recommended Data Security Measures for ICT

## 1) Data Governance and Organisational Measures

- Establish clear internal **policy** and **procedures** on **data governance** and **data security**

NOTE

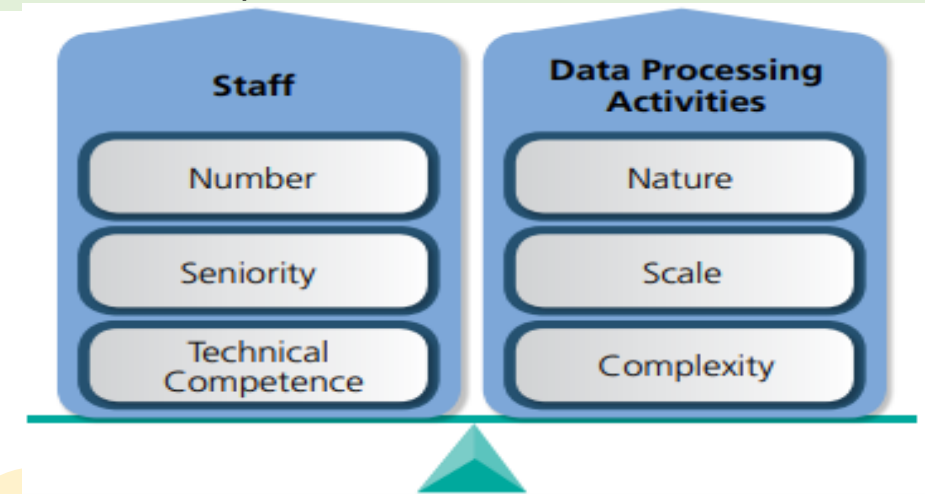
A data user should review and revise its policies and procedures on data governance and data security periodically and in a timely manner based on prevailing circumstances.

- Appoint **suitable personnel** for data security (e.g., CIO, CPO)
- Provide **appropriate staffing levels** for ICT
- Provide **sufficient training** to staff members at induction and on a regular basis

NOTE

A data user should also be mindful of the prudence and integrity of staff members to prevent data breaches caused by human errors or insider attacks. A data user may include confidentiality obligation in employment contracts where appropriate.

### *Proportionate Staff Allocation*



# Recommended Data Security Measures for ICT



NOTE

Results of risk assessments should be regularly reported to senior management and identified risks should be dealt with in a timely manner.

## 2) Risk Assessments

Data users should:

- Conduct risk assessments before product launch, as well as **periodically thereafter**
- **Keep inventory** of the personal data; assess the **nature** of such data and the **potential harm** arising from leakage
- **Conservatively consider** and **minimise** the collection of **sensitive data**
- **SMEs** which may not have the relevant expertise should consider engaging **third party specialists** to conduct security risk assessments

31

# Recommended Data Security Measures for ICT




## 3) Technical and Operational Security Measures



**Securing Computer Networks**




**Database Management**




**Access Control**



**Emails and File Transfers**



**Firewalls and Anti-malware**



**Protecting Online Applications**



**Encryption**



**Backup, Destruction and Anonymisation**



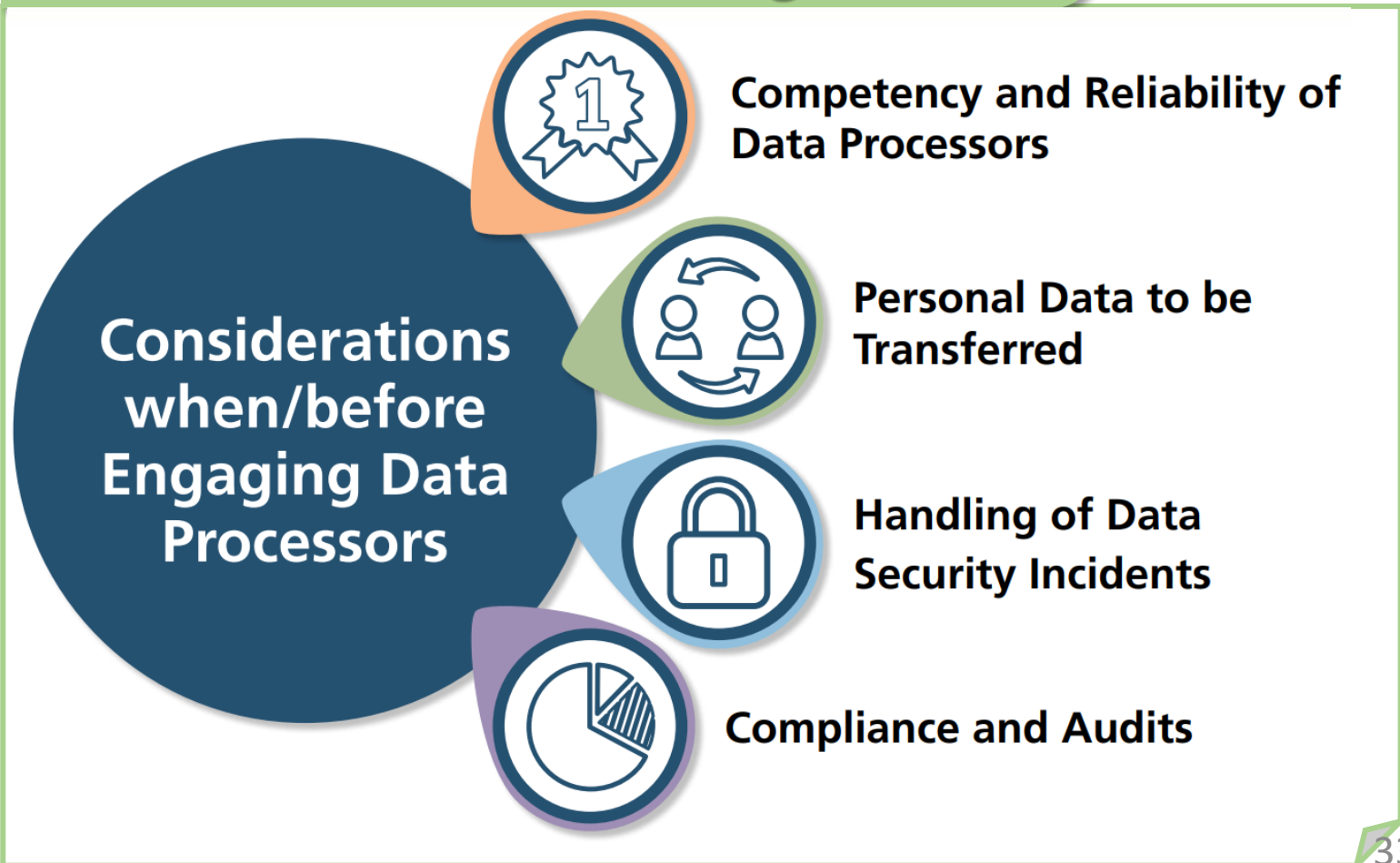
# Recommended Data Security Measures for ICT

## NOTE

Under section 65(2) of the Personal Data (Privacy) Ordinance, a data user may be liable for the acts of its agent (including data processors)

*For more details about data processor management, please refer to the information leaflet "Outsourcing the Processing of Personal Data to Data Processors" issued by the PCPD.*

## 4) Data Processor Management



# Recommended Data Security Measures for ICT

## 5) Remedial Actions in the Event of Data Security Incidents

Stopping and Disconnecting the Affected Systems



Changing Passwords or Ceasing Access



Changing System Configurations



Notifying and Advising the Affected Individuals



Reporting to the PCPD and Other Law Enforcement Agencies/Regulators



Fixing the Security Weakness



Scanning the Systems if Feasible



Following Up on the Lessons Learnt



NOTE

Based on the lessons learnt, the data user should review and strengthen its overall data governance and data security measures.

*For detailed guidance concerning handling of data breaches, please refer to the "Guidance on Data Breach Handling and Data Breach Notifications" issued by the PCPD.*

34

# Recommended Data Security Measures for ICT



NOTE

Improvement actions should be taken for non-compliant practices and ineffective measures.

## 6) Monitoring, Evaluation and Improvement

A data user may commission an independent task force to:

- **Monitor** the **compliance** with data security policy periodically
- **Evaluate** the **effectiveness** of the data security measures periodically

# Recommended Data Security Measures for ICT

## 7) Other Considerations

### Cloud Services

Security Features Available

Capability of Service Providers

Strong Access Control and Authentication Procedures

### Bring Your Own Device (BYOD)

Preventing Storage of Personal Data

Implementing Access Control to Personal Data

Enabling Remote Erasure of Data

Encrypting Personal Data Stored in Devices

### Portable Storage Devices (PSDs)

Setting Out the Permitted Use of PSDs in a Policy

Using End-point Security Software

Keeping Inventory and Tracking of PSDs

Erasing Data in PSDs after use

PCPD



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

HK



**數據安全熱線**  
Data Security Hotline  
2110 1155



**數據安全快測**  
Data Security Scanner



  
**數據安全  
專題網頁**  
Data Security  
Webpage



Follow us to receive  
PCPD's latest updates!



保障、尊重個人資料私隱

*Protect, Respect Personal Data Privacy*





Thank you!

#### Disclaimer

The information provided in this PowerPoint is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance. The Privacy Commissioner for Personal Data (“the Commissioner”) makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information set out in this PowerPoint. The contents provided will not affect the exercise of the functions and powers conferred to the Commissioner under the Ordinance.

保障、尊重個人資料私隱

*Protect, Respect Personal Data Privacy*

 2827 2827

 2877 7026

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

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