

**Practising Governance Annual Conference
Getting Ready for 2023**

28 October 2022

Managing Privacy Risks, Adopting Best Practices and Way Forward

Dennis Ng

*Assistant Privacy Commissioner for Personal Data (Acting)
(Legal, Global Affairs and Research)*

Office of the Privacy Commissioner for Personal Data, Hong Kong



Recent Notable Data Breaches – September 2022

Optus

- The 2nd largest telecommunications company in Australia
- Caused by a **cyberattack**
- The personal information of up to **10 million customers** including home addresses, drivers' licenses and passport numbers had been compromised.

Uber

- A popular global platform for rides, delivery of meals and packages
- Caused by a **cyberattack**
- Several internal systems were accessed

Shangri-La

- An international hotel group
- 8 of its hotels suffered **cyberattacks**, including 3 hotels in Hong Kong
- The personal data of over **290,000 Hong Kong customers** might have been affected

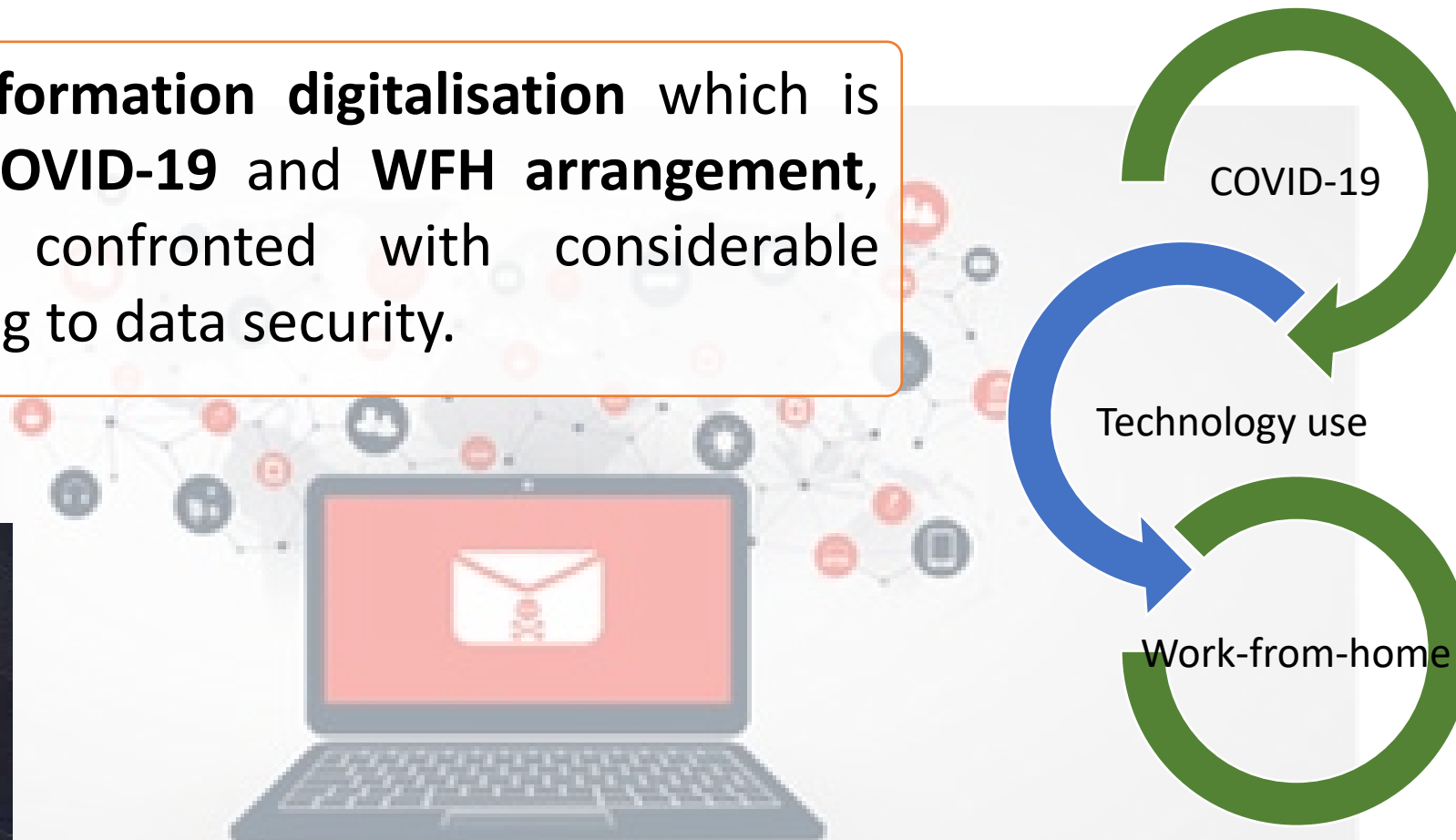
Other Notable Data Breaches with Number of Individuals Affected

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

Data Security Risks

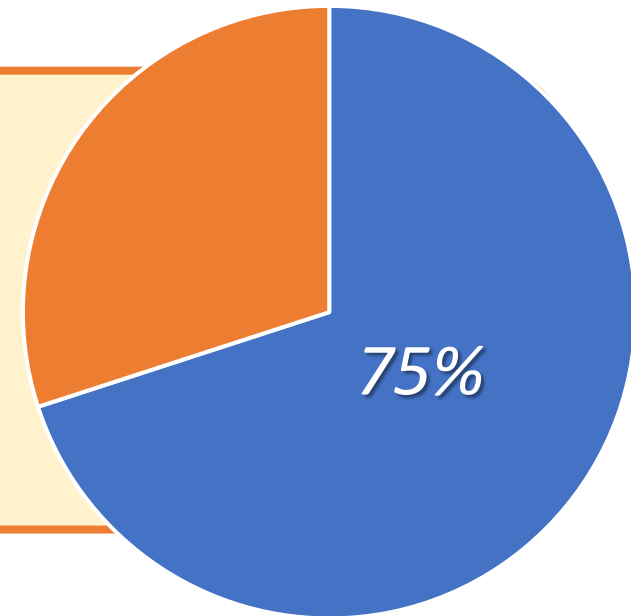
In the era of **information digitalisation** which is accelerated by **COVID-19** and **WFH arrangement**, companies are confronted with considerable challenges relating to data security.



Increasingly Complex Compliance Requirements

According to a study, it is predicted that by **2024, 75% of the global population** will have its personal data covered under privacy regulations.

Coverage of Privacy Regulations



■ Global population covered by privacy regulations

Reference: Gartner

Increasingly Complex Compliance Requirements

Not exhaustive



The proposed American Data and Privacy Protection Act is ready for consideration by the full House of Representatives

The California Privacy Rights Act will take effect in January 2023

The Data Protection and Digital Information Bill was introduced to the Parliament in July 2022



The AI Act is currently being discussed and considered

《深圳經濟特區人工智能產業促進條例》 is expected to take effect on 1 November 2022



Review of the PDPO e.g. direct regulation of data processors, a mandatory data breach notification regime and imposing administrative fines



The Personal Data Protection Law was recently ratified



Review of the Privacy Act 1988 e.g. expanding the definition of personal information, strengthening consent requirements, and introducing the 'right to erasure'.

Increasingly Complex Compliance Requirements



In a recent study, **compliance with recent regulations** was reported as the number one data privacy risk by the respondents from different jurisdictions.

Reference: TurstArc

6 Data Protection Principles (DPPs)

1 收集目的及方式 Collection Purpose & Means



資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。

須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.

All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.

Data collected should be necessary but not excessive.

2 準確性、儲存及保留 Accuracy & Retention



資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的實際所需。

Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used.

3 使用 Use



個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

Personal data is used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject.

4 保安措施 Security



資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5 透明度 Openness



資料使用者須採取切實可行的步驟來公開其處理個人資料的政策和行事方式，並交代其持有的個人資料類別和用途。

A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

6 查閱及更正 Data Access & Correction



資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

A data subject must be given access to his personal data and to make corrections where the data is inaccurate.

Best Practices: Embracing Privacy as a Differentiator and Trust-builder

Embracing a strong **culture of proper data privacy ethics**

Ensuring **privacy is deeply rooted in every product and service**



Data Governance

PERSONAL DATA PRIVACY MANAGEMENT PROGRAMME (PMP)

PMP is a **management framework** for the **responsible collection, holding, processing, and use of personal data** by the company, and to **ensure compliance** with the requirements of the Personal Data (Privacy) Ordinance.

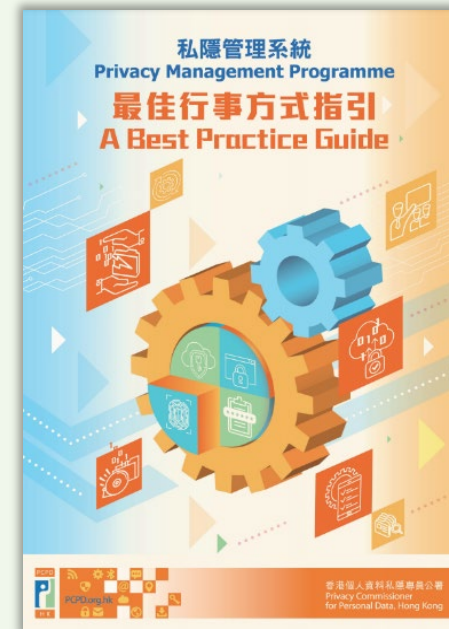
Benefits:

- Minimising the risk of data security incidents
- Effective handling of data breaches to minimise damage
- Ensuring compliance with the PDPO
- Demonstrating the organisation's commitment

The PMP Guide:

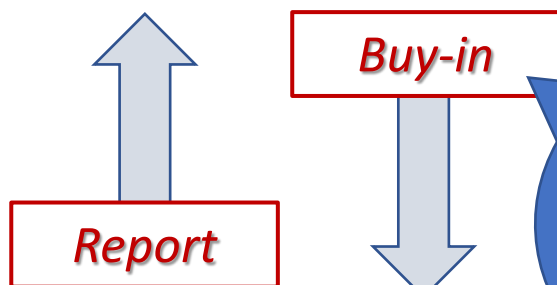
- Recommends organisations to embrace personal data protection as part of their corporate policies and culture

Personal Data Privacy Management Programme: A Best Practice Guide

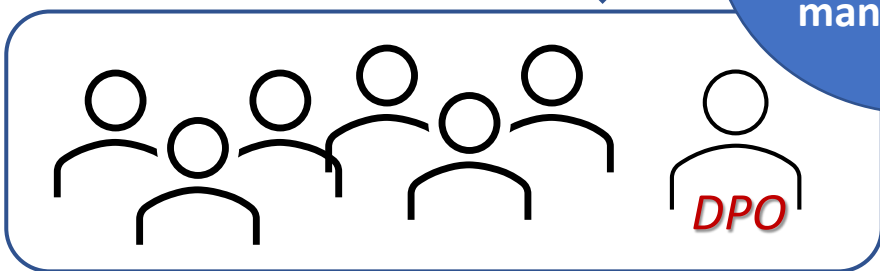


Data Governance

PERSONAL DATA PRIVACY MANAGEMENT PROGRAMME



Ensuring support from top management



1. Organisational Commitment

1.1 Buy-in from the Top

1.2 Appointment of Data Protection Officer

1.3 Establishment of Reporting Mechanism

Data Governance

PERSONAL DATA PRIVACY MANAGEMENT PROGRAMME

2. Programme Controls

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

Data Governance

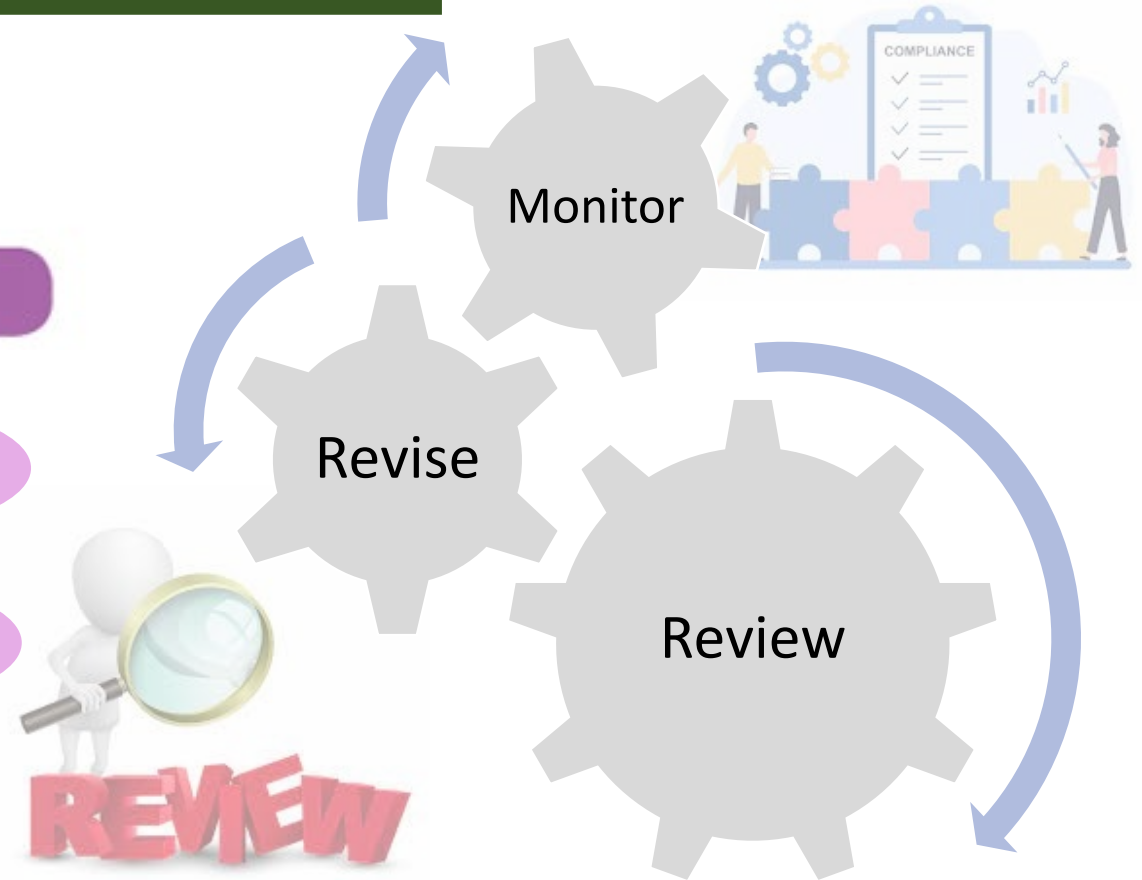
PERSONAL DATA PRIVACY MANAGEMENT PROGRAMME



3. Ongoing Assessment and Revision

3.1 Develop an Oversight and Review Plan

3.2 Assess and Revise Programme Controls



Best Practices: Stepping Up Data Security

Guidance Note on Data Security Measures for ICT: 7 Recommendations

1. Data Governance & Organisational Measures
2. Risk Assessments
3. Technical and Operational Security Measures
4. Data Processor Management
5. Remedial Actions in the event of Data Security Accidents
6. Monitoring, Evaluation and Improvement
7. Other considerations

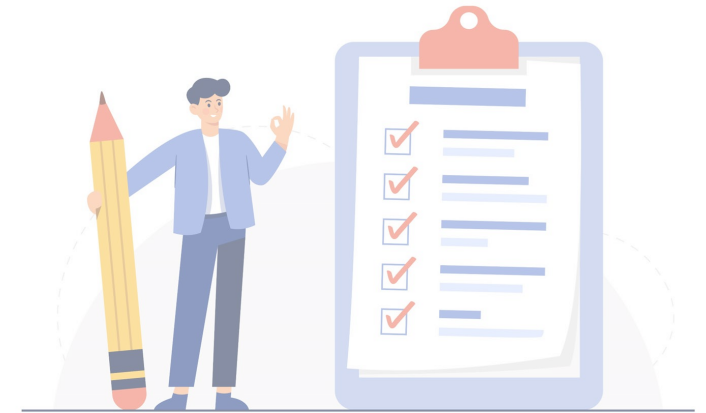


Data Security Measures for ICT

1) Data Governance & Organisational Measures

A data user should:

- establish clear **internal policy** and **procedures** on data governance and data security
- appoint **suitable personnel** in a leadership role to bear specific responsibility for personal data
- provide **appropriate staffing levels** for ICT
- Provide sufficient **training** for staff members at induction and regularly thereafter
- have **guidelines** setting out:



- 1) the life cycle of the personal data handled by the data user, from its collection to its destruction;
- 2) roles and responsibilities of relevant staff;
- 3) lines of authority for decision-making; and
- 4) accountability and power of oversight concerning access and transfer of personal data



Data Security Measures for ICT

2) Risk Assessments

A data user should

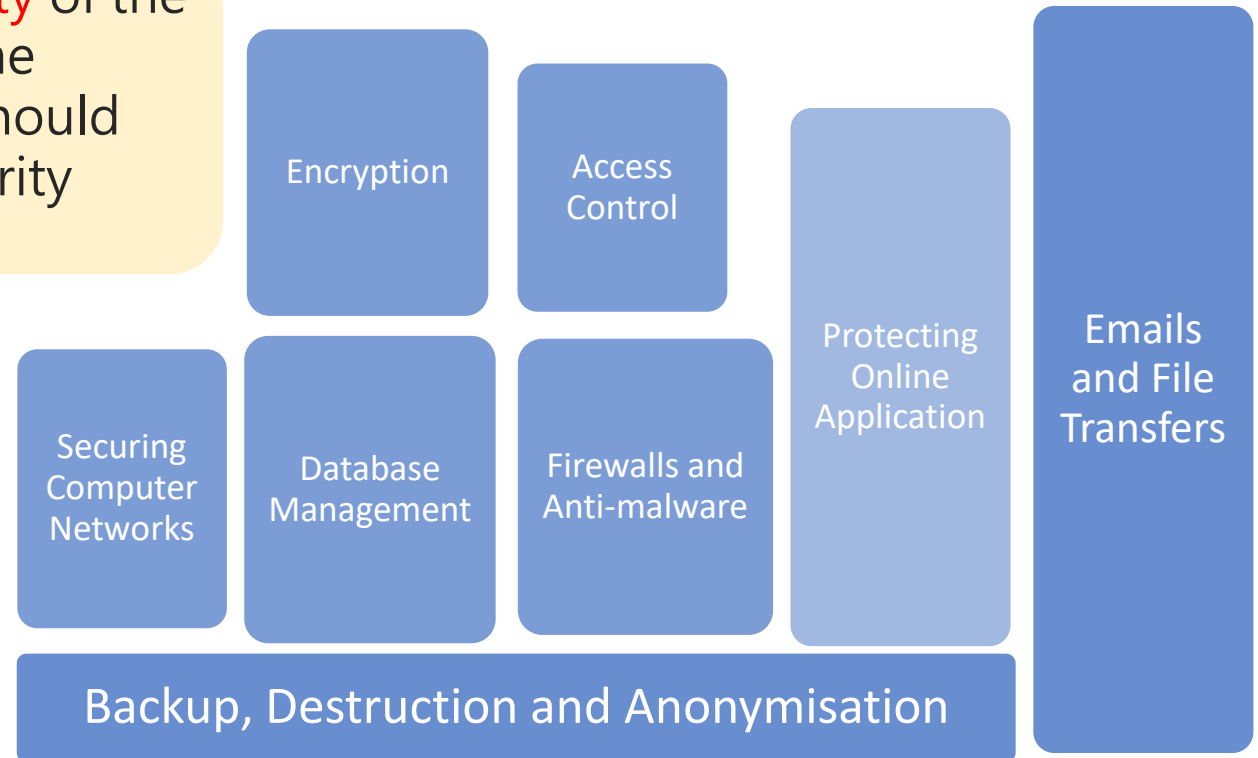
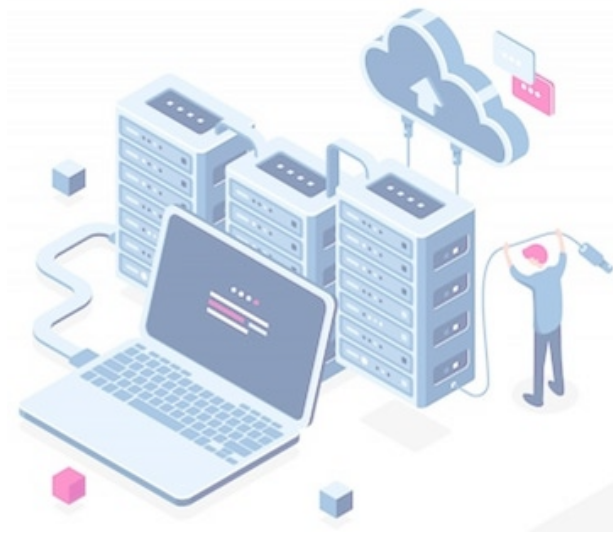
- Keep **inventory of the personal data** under its control, and assess the nature of such data and the potential harm arising from leakage of such data
- Conduct risk assessments on data security for **new systems and applications** before launch, as well as **periodically** thereafter.
- Consider engaging **third party specialists** to conduct security risk assessments
- Report** results of assessments to senior management
- Promptly **address** the identified risks



Data Security Measures for ICT

3) Technical and Operational Security Measures

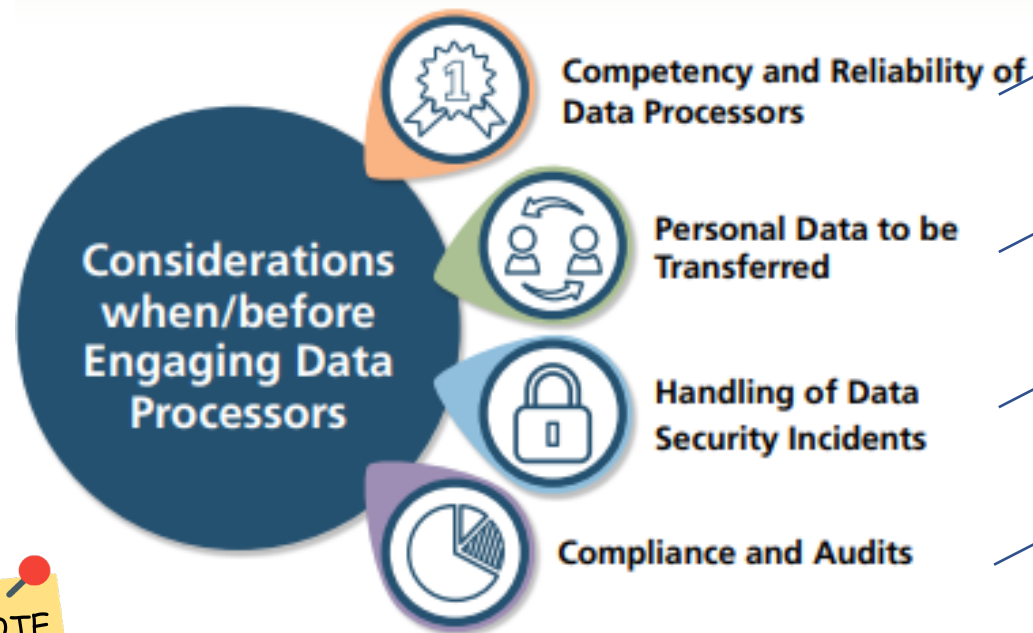
Based on the **nature**, **scale** and **complexity** of the ICT and data processing activities, and the results of risk assessments, a data user should put in place **adequate** and **effective** security measures



Data Security Measures for ICT



4) Data Processor Management



Implementing policy and procedures to ensure data processors' competency and reliability

Conducting assessment to ensure that only necessary personal data is transferred

Requiring the data processor to immediately notify all data security incidents

Conducting field audits to ensure compliance with the data processing contract

NOTE

Under section 65(2) of the PDPO, a data user may be **liable for the acts of its agents** (including data processors such as cloud and data analytics service providers)

Data Security Measures for ICT

5) Remedial Actions in the Event of Data Security Incidents

Timely and **effective** remedial actions taken by a data user after the occurrence of a data security incident may **reduce the risks** of unauthorised or accidental access, processing or use of the personal data affected, thereby **reducing the gravity of harm** that may be caused to the affected individuals



NOTE

A data user should also take into consideration **lessons learnt from a data security incident** to review and strengthen its overall data governance and data security measures.



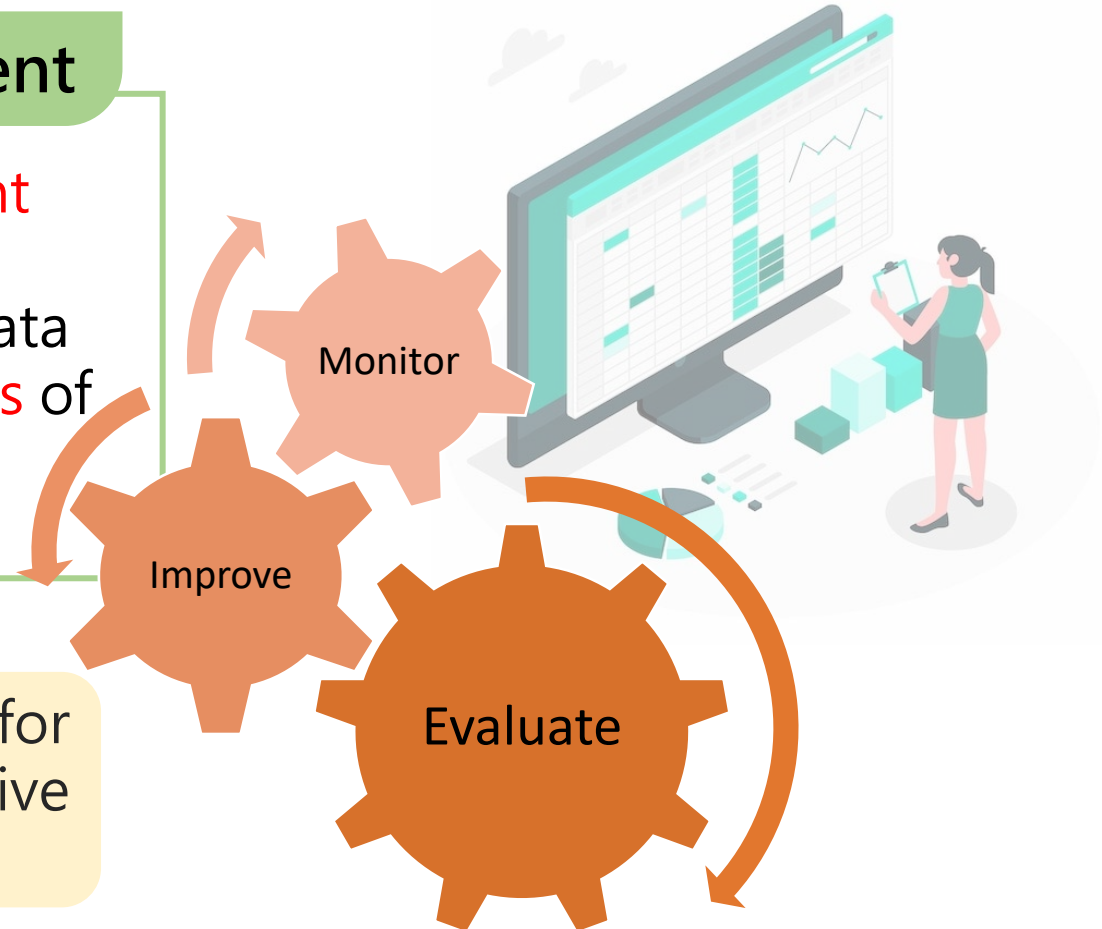
Data Security Measures for ICT

6) Monitoring, Evaluation and Improvement

A data user may commission an **independent task force** (e.g. an internal or external audit team) to **monitor the compliance** with the data security policy and **evaluate the effectiveness** of the data security measures periodically

NOTE

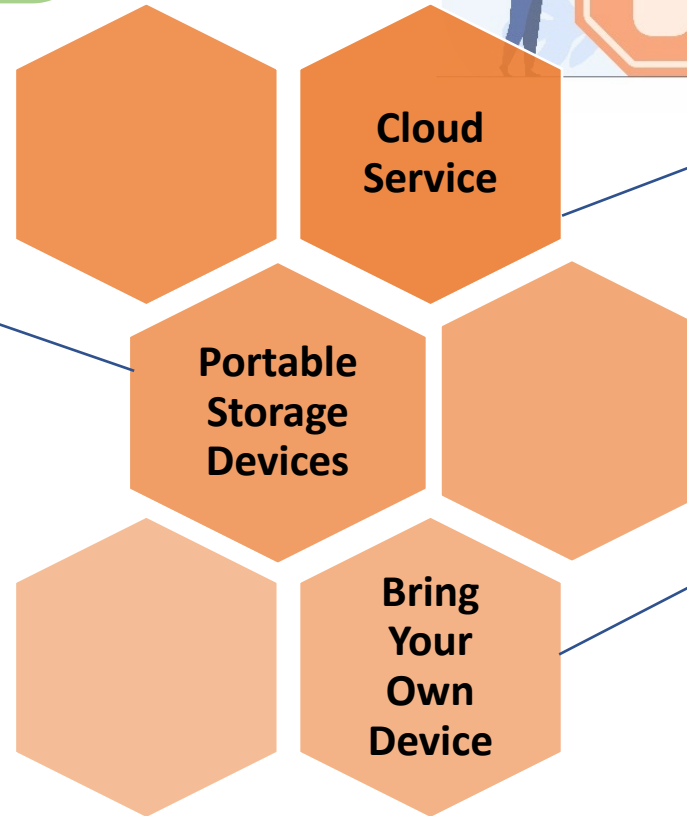
Improvement actions should be taken for noncompliant practices and ineffective measures



Data Security Measures for ICT

7) Other Considerations

- ✓ 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



- ✓ Security Features Available
- ✓ Capability of Service Providers
- ✓ Strong Access Control and Authentication Procedures




- ✓ Preventing Storage of Personal Data
- ✓ Implementing Access Control to Personal Data
- ✓ Enabling Remote Erasure of Data
- ✓ Encrypting Personal Data Stored in Devices



Way Forward

- Comprehensive review of the PDPO with additional regulatory compliance requirements:
 - Mandatory data breach notification regime
 - Direct regulation of data processors

- ✓ Implement the PMP
- ✓ Appoint a DPO
- ✓ Put in place a robust data security system



Understand the **legal requirements**

Study your data and identify **data privacy risks**

Devise and deploy the **data privacy strategy** with regular review



Contact Us

The screenshot shows the PCPD website homepage. At the top, there is a header with the PCPD logo and the text '香港個人資料私隱專員公署 Office of the Privacy Commissioner for Personal Data, Hong Kong'. Below the header is a banner with the slogan '保障、尊重個人資料私隱' and 'Protect, Respect Personal Data Privacy'. The main navigation bar includes links for 'About PCPD', 'Data Privacy Law', 'News & Events', 'Enforcement Reports', 'Frequently Asked Questions', 'Compliance & Enforcement', 'Doxxing Offences', 'Complaints', 'Education & Training', 'Resources Centre', and 'Contact Us'. A search bar is located on the right side of the navigation bar. Below the navigation bar, there are social media icons for Facebook, Instagram, LinkedIn, Twitter, Weibo, and YouTube. The main content area features a large article titled 'PCPD Releases Report on "Comparison of Privacy Settings of Social Media"' with an illustration of a hand holding a smartphone. To the right of this article is a 'What's New' section with several news items, including 'Privacy Commissioner's Office Broadcasts TV Video and Radio Announcement on Doxxing Offences', 'Privacy Commissioner Published an Article on "New Recommended Model Clauses for Cross-border Transfer of Personal Data" at Banking Today, the Bi-monthly Journal of The Hong Kong Institute of Bankers', 'Reaching Out to the Community – Privacy Commissioner Spoke at a Public Seminar of the Media Education Programme Organised by the Hong Kong Press Council', 'PCPD Organised a Webinar on "Protection of Personal Data Privacy for Property Management Sector"', 'Privacy Commissioner's Office Made an Arrest For a Suspected Doxxing Offence', 'Privacy Commissioner Published an Article on "Cross-border transfers of personal data" at the CGJ, the journal of the Hong Kong Chartered Governance Institute', 'Showcasing Hong Kong – Privacy Commissioner Spoke at the Closing General Session of the International Association of Privacy Professionals' (IAPP) Asia Pacific Forum in Singapore', 'Reaching Out to Schools – PCPD Organised the "Learning and Teaching Privacy on Social Media" Online Forum', and 'Reaching Out to the Community – Privacy Commissioner Met with Representatives of RainLily'. At the bottom of the page, there are two buttons: 'For Individuals' and 'For Organisations'.

- ☐ Hotline 2827 2827
- ☐ Fraud Prevention Hotline 3423 6111
- ☐ Anti-doxxing Hotline 3423 6666
- ☐ Fax 2877 7026
- ☐ Website www.pcpd.org.hk
- ☐ E-mail communications@pcpd.org.hk

спасибо
danke 謝謝
ngiyabonga
teşekkür ederim
dank je
gracias
tapadh leat
huala
mauruuru
dziękuję
sagolun
sukriya
kop khun krap
moichakkeram
go raibh maith agat
arigatō
takk
dakujem
merci
obrigado
bedankt
merci
ευχαριστώ
감사합니다
terima kasih