Cyber Security: New Challenges to Data Protection and Data Breaches

7 September 2022

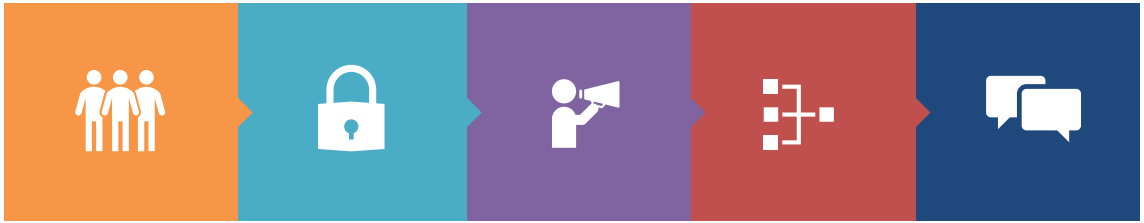
Mr Brad KWOK

Acting Chief Personal Data Officer
(Compliance & Enquiries)

01
PDPO Overview

03
Data Security Risk under WFH Arrangements and Practical Guidance

05
Q&A



02
Data Security and Data Breach Notification

04
Privacy Management Programme

1. PDPO Overview

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

2. Data Security and Data Breach Notification

DPP4: Security of Personal Data

- **All practicable steps** should be taken to protect personal data from unauthorised or accidental access, processing, erasure, loss or use
- If a **data processor** is engaged to process personal data, data user must use **contractual or other means** to ensure that the personal data transferred to the data processor is protected against unauthorised or accidental access, processing, erasure, loss or use

DPP4: Security of Personal Data

- **All practicable steps** should be taken to protect personal data from unauthorised or accidental access, processing, erasure, loss or use having particular regard to –
  - (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 is **all practicable steps**?

- General and Organisational Preventive Measures
- Technical Security Measures
- Mitigating Steps after the data breach
- Other Considerations

What is **all practicable steps**?

General and organisational preventive measures

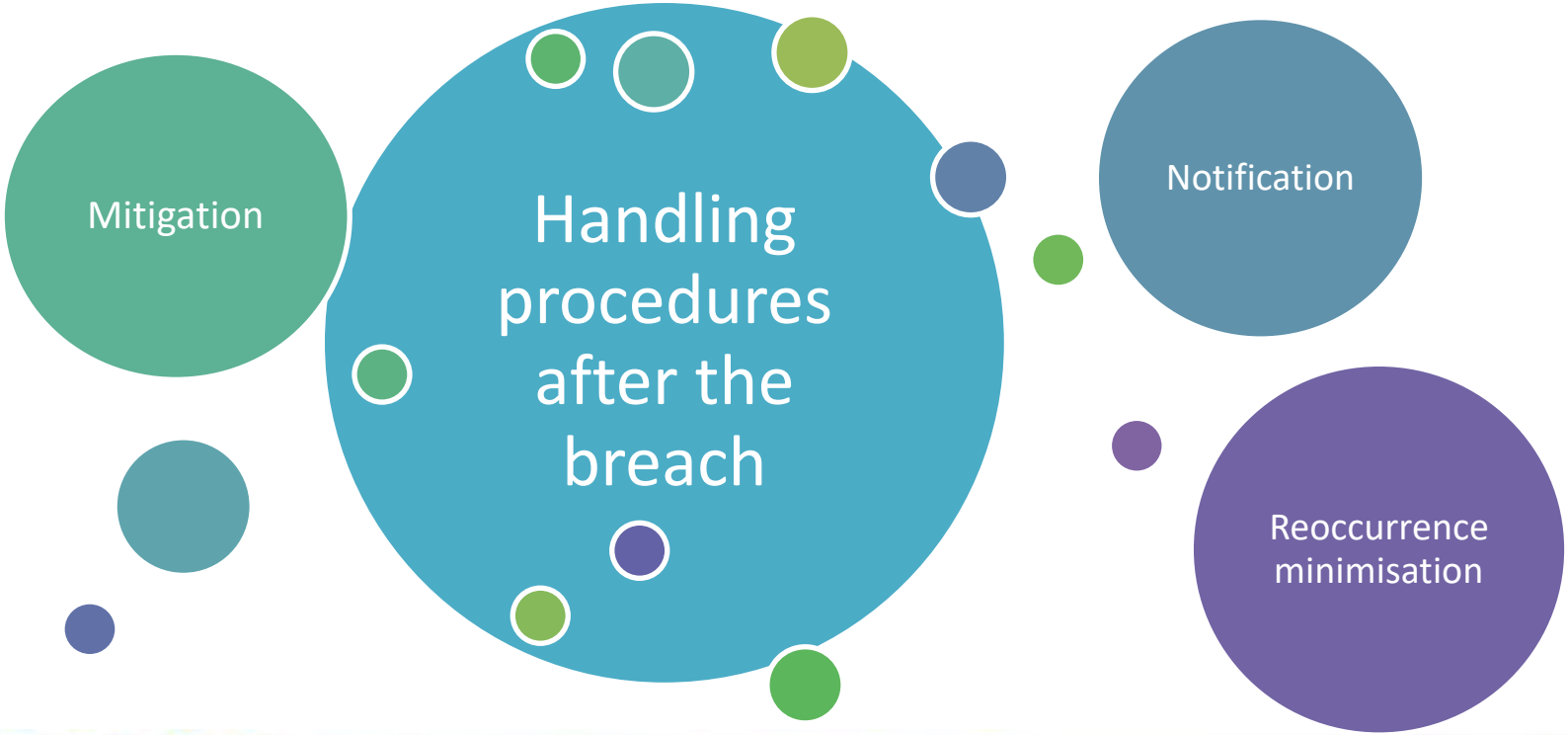
- Embrace personal data privacy protection as part of the corporate governance responsibility, covering business practices, operational processes, policies and training
- Comprehensive and on-going review and monitoring process; build a robust privacy infrastructure
- Open and transparent information privacy policies and practices
- Has top management commitment, a top-down business imperative throughout the organisation

What is **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, and adoption of international standards and technology, e.g. hashing, encryption, etc.

What is **all practicable steps**?



What is **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 its operations of the data user and its business model
- The amount and sensitivity of personal data held

What is Data Breach

- Suspected breach of security exposing personal 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.

Data Breach – Common Categories

1. Loss of documents or portable device
2. Misconfiguration of systems or hacking
3. Errors with posts or emails
4. Staff misconduct
5. Improper/wrongful disposal of personal data

Actions for Data Breach Handling

Collecting Information Immediately

Immediate gathering of essential information for assessing the impact on data subjects including:

- When and where did the breach take place?
- How was the breach detected and by whom?
- What was the cause of the breach?
- What kind and extent of personal data was involved?
- How many data subjects were affected?

Actions for Data Breach Handling

Contacting the Interested Parties & Adopting Containment Measures

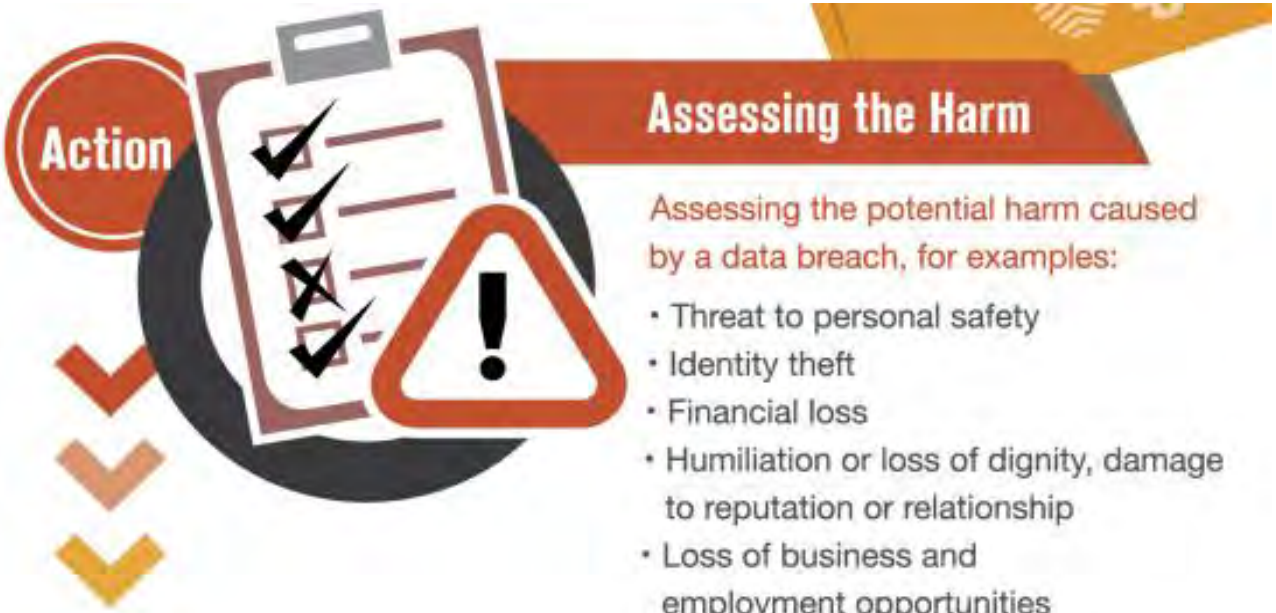
Interested parties may include:

- The law enforcement agencies
- The relevant regulators (e.g. Privacy Commissioner for Personal Data, Hong Kong (the "Commissioner"))
- The Internet companies
- IT experts

Containment measures may include:

- Stopping the system if the data breach is caused by a system failure
- Changing the users' passwords and system configurations to control access and use
- Considering whether technical assistance is needed to remedy the system loopholes and / or stop the hacking
- Ceasing or changing the access rights of individuals suspected to have committed or contributed to the data breach
- Notifying the relevant law enforcement agencies if criminal activities are or likely to be committed
- Keeping the evidence of the data breach to facilitate investigation
- Directing the data processor to take immediate remedial measures and requesting it to notify the data user of the progress, if applicable

Actions for Data Breach Handling



Actions for Data Breach Handling

Considering the Giving of Notification

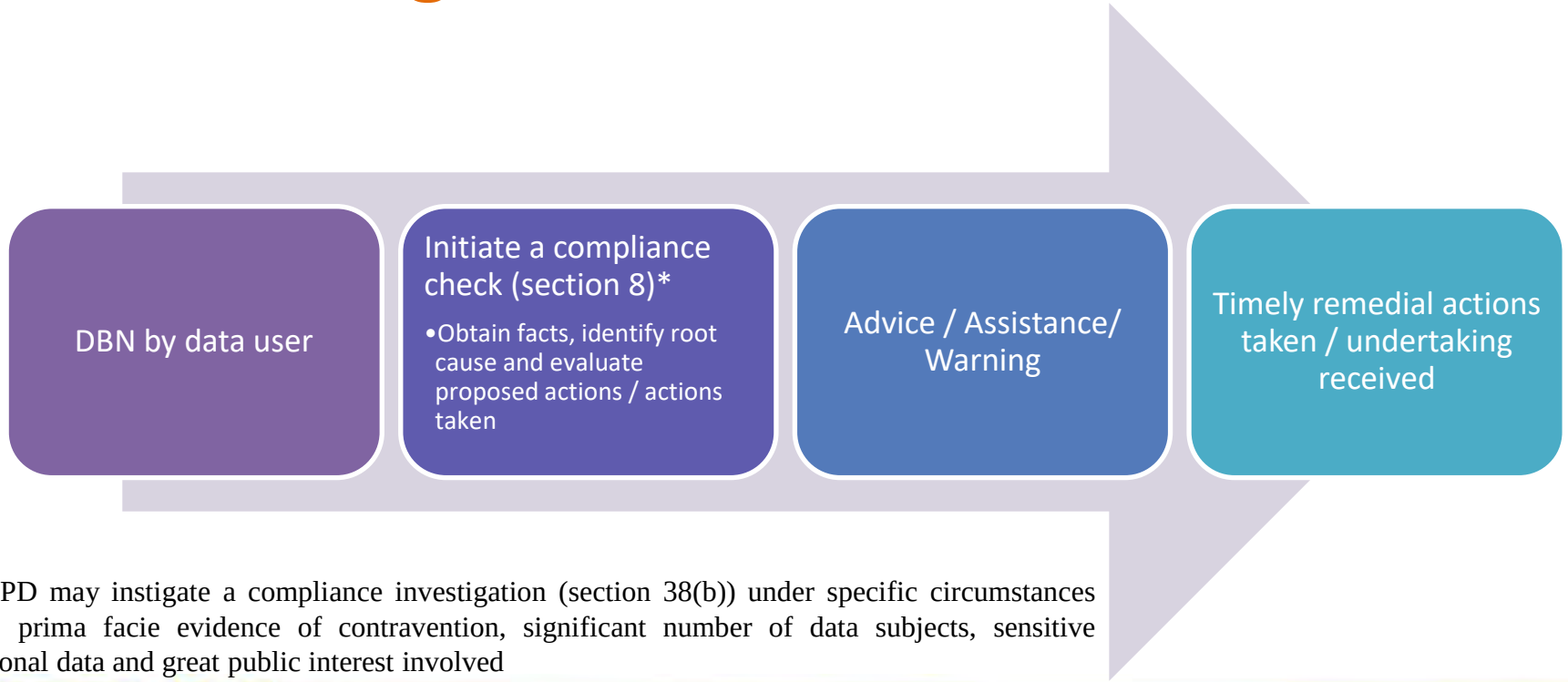
When real risk of harm is reasonably foreseeable in a data breach, the data user should consider:

- Notifying the affected data subjects and the relevant parties
- The consequences for failing to give notification

Data Breach Notification

- Not a statutory requirement on data users to inform PCPD about a data breach incident but data users are advised to do so as a recommended practice for proper handling of such incident

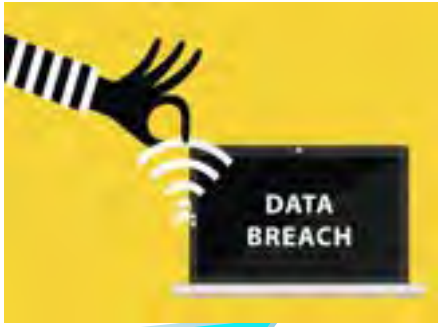
Handling of Data Breach Notifications



*PCPD may instigate a compliance investigation (section 38(b)) under specific circumstances (e.g. prima facie evidence of contravention, significant number of data subjects, sensitive personal data and great public interest involved

Case Sharing (1)
Inadvertent disclosure of personal data via email

- A faculty staff member of an university intended to email the non-local students about the university's quarantine arrangements. However, the staff member mistakenly attached the master list, which contained personal data of about 2,500 students of the faculty, in the email.



- Universities should take reasonably practicable measures to ensure that staff handling such data are properly trained.
- Staff should also observe relevant personal data privacy policies and exercise due diligence in applying those policies. Universities should establish procedures to ensure staff's compliance with those policies.

Case Sharing (2)
Unauthorised access to an international fashion chain's customer personal data system

- An international fashion company's customer personal data system suffered a ransomware attack. About 200,000 customer records were compromised. The company had failed to identify a known exploitable vulnerability, and hence the attacker successfully logged into the customer personal data system with valid credentials and installed ransomware in the company's network.

- Data users should regularly review and monitor security of their networks and test and apply security patches in a timely manner; and limit the retention period of personal data.

Case Sharing (3)
Hacker's intrusion into email system

- A hacker had intruded into six staff email accounts of a company, forwarding the emails that had been sent to those email accounts to two unknown email addresses. The incident led to the leakage of the personal data of over 1,600 customers.

- Adequate policies, measures and procedures covering system security should be put in place, and should cover the following areas:
  - Appoint Data Protection Officer(s);
  - Devise policy on email communications;
  - Adequate security measures;
  - Instil a privacy-friendly culture in the workplace; and
  - Establish a Personal Data Privacy Management Programme.

3. Data Security Risk under WFH Arrangements and Practical Guidance

Data Security Risk under WFH Arrangements

Transfer of personal data from workplace to home

Security of ICT networks and devices

Deviation from standard processes and lack of staff training

The rapid uptake of video conferencing software

Case Sharing (4)
Loss of notebook computer containing work files

- A staff member from a government department lost an official notebook computer on public transport. The computer, provided to the staff member for work-from-home arrangement, contained encrypted personal data of about 400 staff members of the department.

- The department reminded staff to take extra care in handling official portable devices and requested staff to access work files through VPN connection instead of storing work files locally when practicable.

Practical Guidance Relating to WFH Arrangements

Practical Tips for Organisations

Risk assessment

- On data security and employees' personal data privacy

Policies and guidance

- Review and adjust existing policies based on the results of risk assessment
- devise policies and guidance on the transfer of data and documents, remote access to corporate networks, and handling of data breach

Practical Tips for Organisations

Device management

- Provide employees with corporate electronic devices (such as smartphones and notebook computers)
- ensure that appropriate security settings be enabled for the devices

Practical Tips for Organisations

Staff training and support

- Provide sufficient training on data security (e.g. password management, encryption and awareness of cybersecurity threats)
- Deploy designated staff to provide support

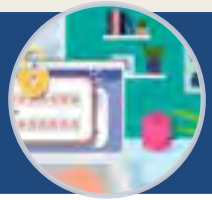
Use of Virtual Private Networks (VPNs)

- Choose the appropriate protocol and type of VPNs, and keep the security setting up-to-date
- Require multi-factor authentication for connection

Practical Tips for Employees

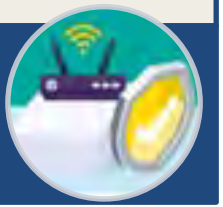
- Use only corporate electronic devices for work
- Secure the devices and the data therein (e.g. strong passwords & change passwords regularly)

Device management



- Refrain from using public Wi-Fi
- Ensure the security protocol and firmware of Wi-Fi routers are up-to-date

Wi-Fi connection



Practical Tips for Employees

- Use only corporate email accounts for sending/receiving work-related documents
- Check the recipient list before sending out messages, and verify suspicious messages

Electronic communications

- Avoid working in public places
- Avoid transferring paper documents out of office premises as far as practicable
- Enhance data security of those documents (e.g. redact or remove personal data)

Work Environment and paper document

Practical Advice on Use of Video Conferencing Software

- choose a platform with adequate data security functions
- Choose a software that provides end-to-end encryption for meetings involving confidential matters
- safeguard their accounts by setting up strong passwords and activating multi-factor authentication

Practical Advice on Use of Video Conferencing Software

- When hosting conferences, set up unique meeting ID and strong password
- Use virtual waiting room to validate participants' identities, and lock the meeting when all participants are admitted
- Any records of the conferences (e.g. video recordings & chat messages) be stored securely with password protection or encryption; they should not be retained for longer than necessary

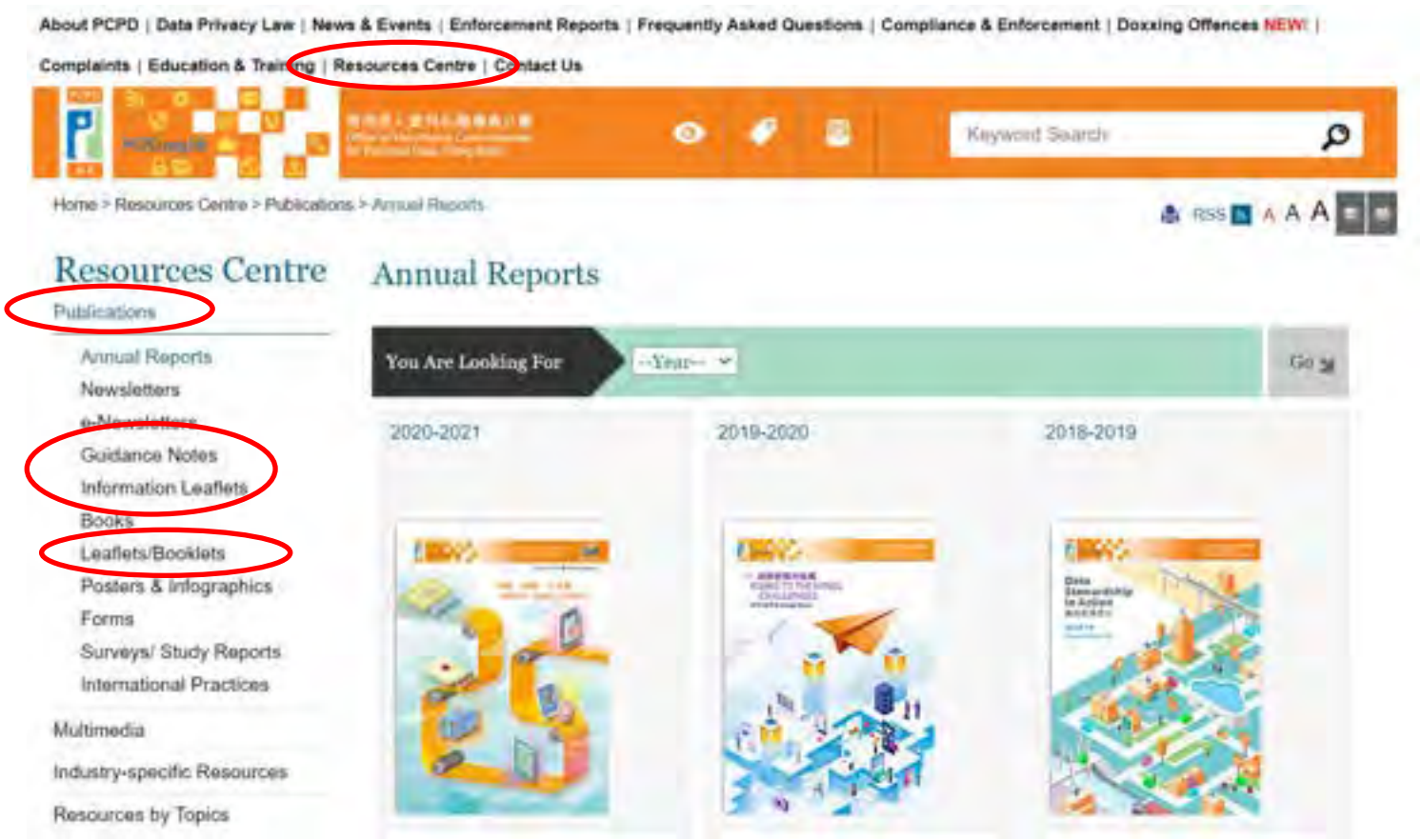
Recommended Data Security Measures for ICT

- 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

4. Privacy Management Programme

Privacy Management Programme

- Encourages organisations to embrace personal data privacy protection as part of their corporate governance responsibilities
- Apply as a top-down business imperative throughout the organisation
- Have in place appropriate policies and procedures that promote good practices
- build trust with clients and also enhance reputation as well as competitiveness


About PCPD | Data Privacy Law | News & Events | Enforcement Reports | Frequently Asked Questions | Compliance & Enforcement | Doxxing Offences NEW! |
Complaints | Education & Training | Resources Centre | Contact Us
Keyword Search
Home > Resources Centre > Publications > Annual Reports
RSS A A A
Resources Centre
Publications
Annual Reports
Newsletters
e-Newsletters
Guidance Notes
Information Leaflets
Books
Leaflets/Booklets
Posters & Infographics
Forms
Surveys/ Study Reports
International Practices
Multimedia
Industry-specific Resources
Resources by Topics
Annual Reports
You Are Looking For
--Year--
Go
2020-2021
2019-2020
2018-2019

Follow us to receive PCPD's latest updates!

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

Contact Us

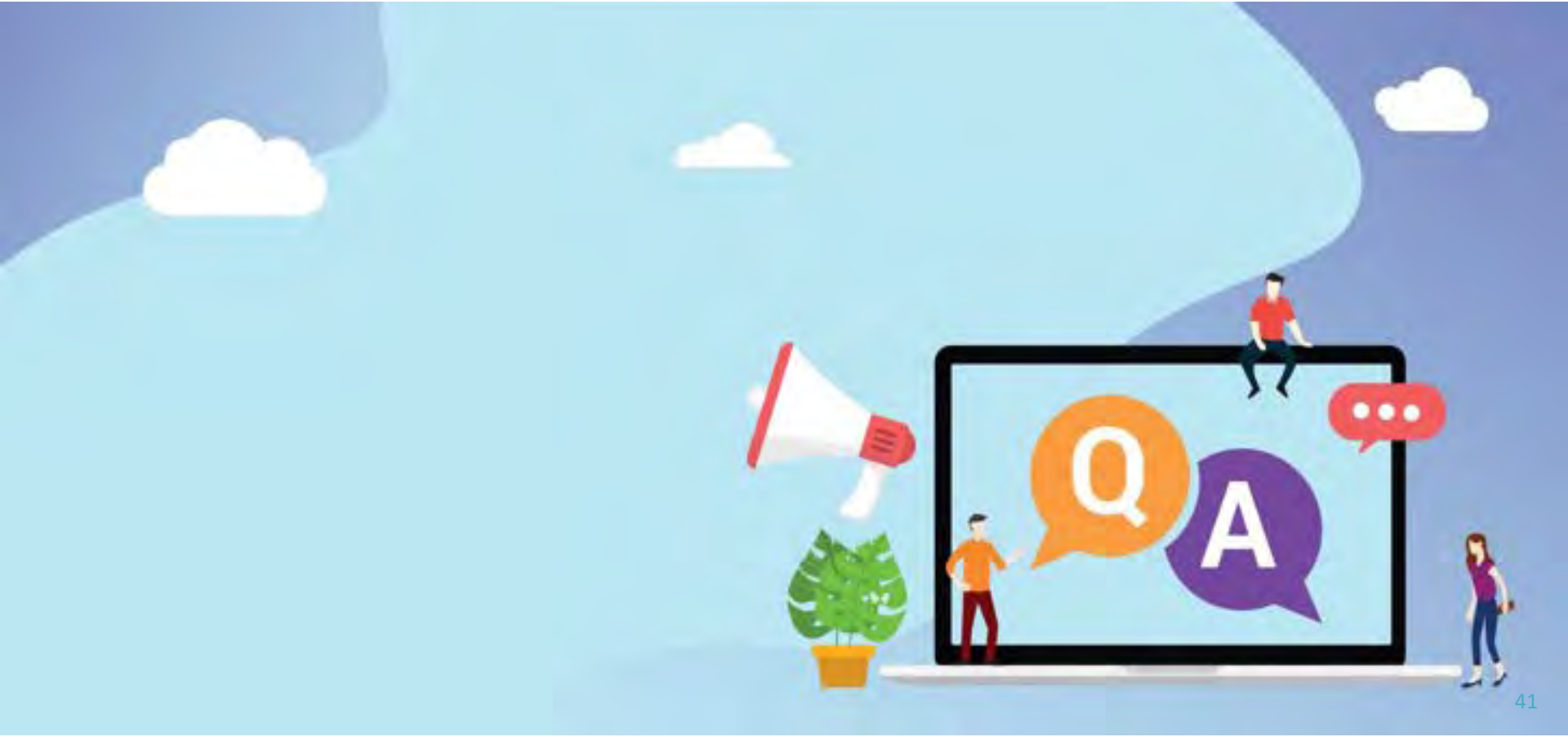
Telephone 2827 2827

Fax 2877 7026

Website https://www.pcpd.org.hk

Email communications@pcpd.org.hk

Address Room 1303, 13/F
Dah Sing Financial Centre
248 Queen's Road East
Wanchai, Hong Kong


Q
A