

The 23rd Annual Corporate and Regulatory Update ACRU 2022 - 9 June 2022

Compliance with personal data privacy regulations, Hong Kong and beyond

Mr Dennis Ng, Assistant Privacy Commissioner for Personal Data (Acting)
Ms Clemence Wong, Legal Counsel (Acting)

The Significance of Personal Data Protection for Governance Professionals and Businesses



Handling of Data Breaches

Safeguarding Personal Data When Working From Home

Doxxing Offences under the Personal Data (Privacy) Ordinance

Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data

Handling of Data Breaches




6 保障資料原則 Data Protection Principles

PCPD.org.hk

1 收集目的及方式 Collection Purpose Et 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 Et 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成原來目的之實際所需。

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或間接的目的，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 Et 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.

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

6 Data Protection Principles (DPPs)

- 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

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 complies with the data security requirement.

Handling of Data Breaches

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



What constitutes 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**.
- The PCPD **has always encouraged data users to give data breach notifications** to affected individuals and the PCPD to minimise the potential damage which might be caused to individuals.

7

Common Causes of Data Breaches

- Loss of documents or portable storage devices
- Hacking/ system misconfiguration
- Inadvertent disclosure
- Misconduct of employees
- Improper/ accidental disposal



Recommended Practices for Handling Data Breaches

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



Investigation Report: Hacker's Intrusion into the Email System of Nikkei China (Hong Kong) Limited

- **Data breach notification received by PCPD on 17 March 2021**
- **Personal data of over 1,600 customers were reportedly leaked through intrusion into email accounts of Nikkei**

NIKKEI Nikkei Group Asia /
Nikkei China (Hong Kong)

To: Privacy Commissioner for Personal Data, Hong Kong

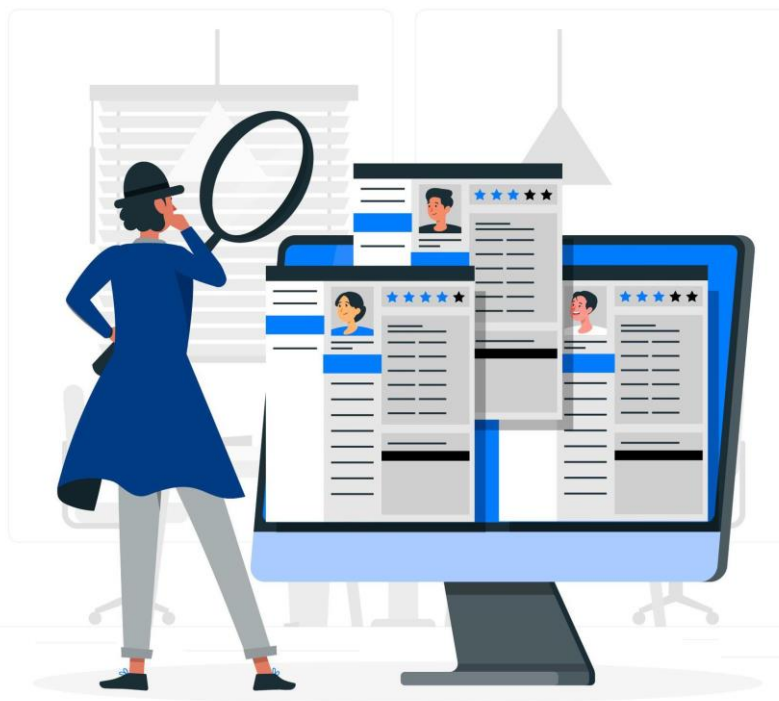


Data Breach Notification Form

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.

Hacker's Intrusion into the Email System of Nikkei China (Hong Kong) Limited



During the **investigation**, the Commissioner:

- Reviewed **the information** provided in the data breach notification and **the announcement made on Nikkei's website**;
- Made 7 rounds of **enquiries** regarding the **security measures** used in Nikkei's information and email systems;
- Examined the **investigation report** provided by the independent consultant engaged by Nikkei; and
- Considered the **follow-up and remedial actions** taken by Nikkei

Hacker's Intrusion into the Email System of Nikkei China (Hong Kong) Limited

INVESTIGATION FINDINGS

- The hacker initially obtained the password of one of Nikkei's email accounts
- The hacker then set up a forwarding function for that email account and 5 other accounts which shared the same password
- All incoming emails in these 6 accounts were automatically forwarded to 2 unknown email addresses between Oct 2020 to Feb 2021
- The data leaked included the names, email addresses, company names, telephone numbers and credit card data of customers



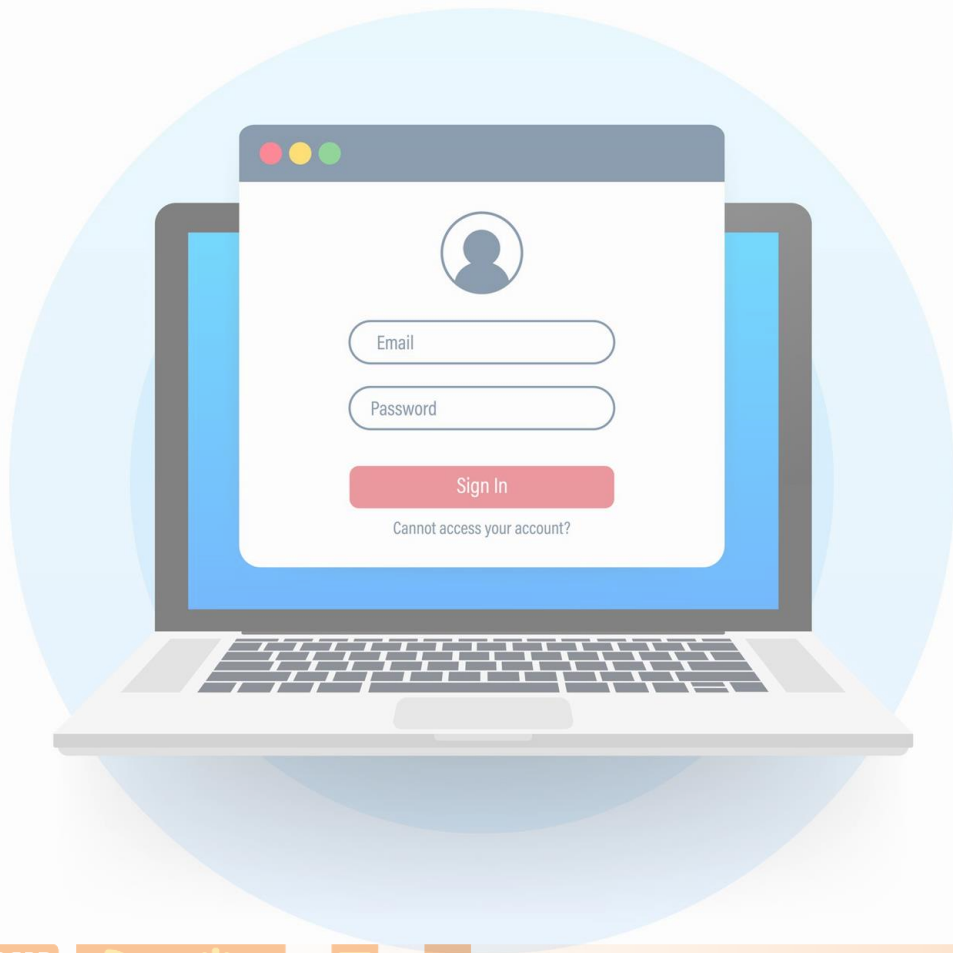
Hacker's Intrusion into the Email System of Nikkei China (Hong Kong) Limited

DEFICIENCIES IDENTIFIED

- Weak password management
- Retention of obsolete email accounts
- Lack of security controls for remote access
- Inadequate security controls on information system



Hacker's Intrusion into the Email System of Nikkei China (Hong Kong) Limited



CONTRAVENTION

- Nikkei had failed to take **all practicable steps** to ensure that its customers' personal data was protected against unauthorised or accidental access, processing or use
- **Contravention of the requirements of DPP 4(1)** relating to the security of personal data

14

Hacker's Intrusion into the Email System of Nikkei China (Hong Kong) Limited

The Commissioner issued an enforcement notice to direct Nikkei to take the following steps:

Revise the information security policy

Devise effective measures to ensure staff's compliance with the revised policy

Engage an independent data security expert to conduct regular reviews and audits

Develop up-to-date training and education for staff members on information security

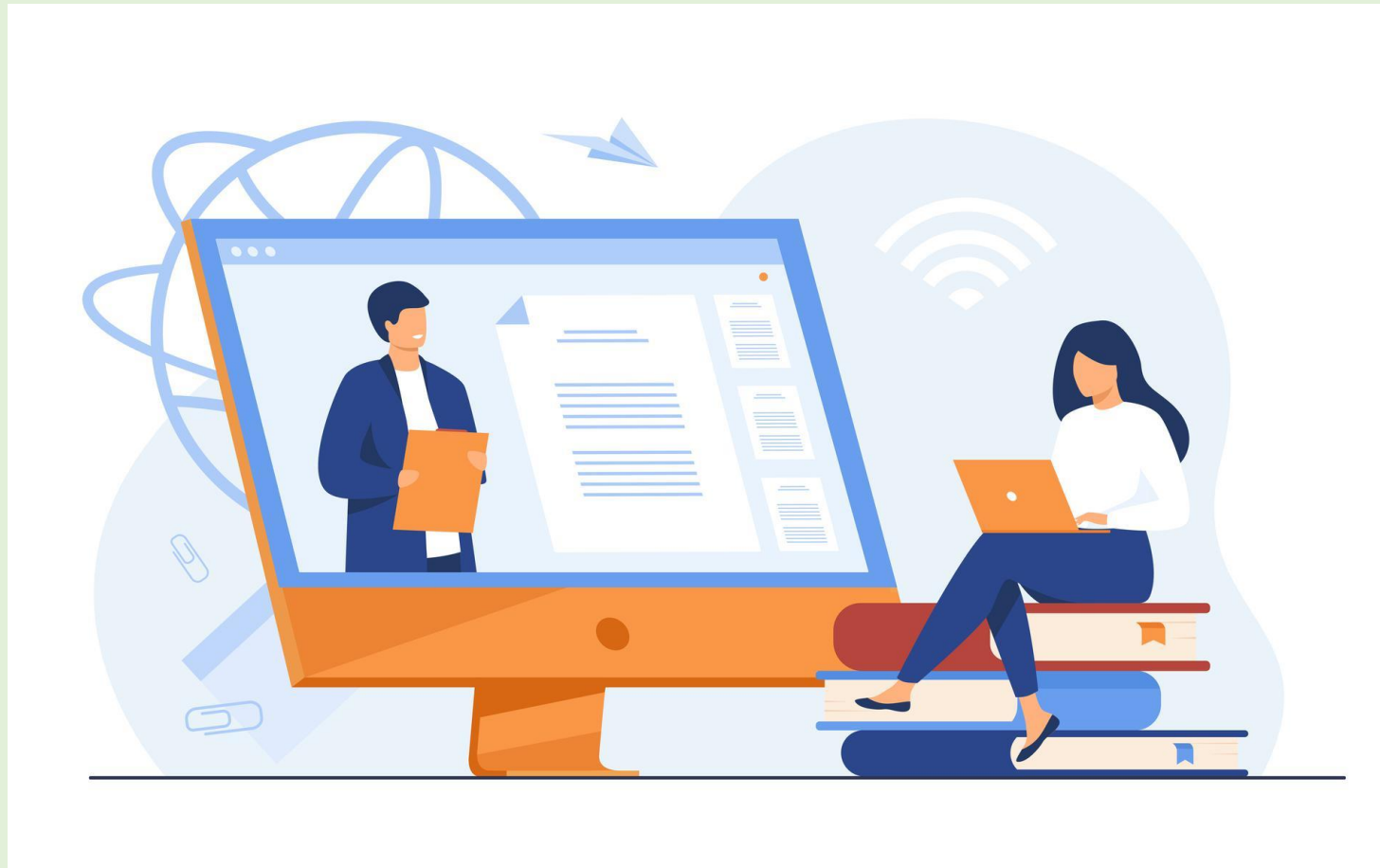
Provide documentary proof within two months to show the completion of the items above

Recommendations for Governance Professionals and Businesses

- ✓ a) Establish a Personal Data Privacy Management Programme
- ✓ b) Appoint Data Protection Officer(s)
- ✓ c) Devise policy on email communications
- ✓ d) Adequate security measures
- ✓ e) Instil a privacy-friendly culture in the workplace



Safeguarding Personal Data When Working From Home



Safeguarding Personal Data When Working From Home

Between

- (i) the companies' networks and employees' home networks
- (ii) the corporate devices and employees' personal devices
- (iii) office premises and employees' homes

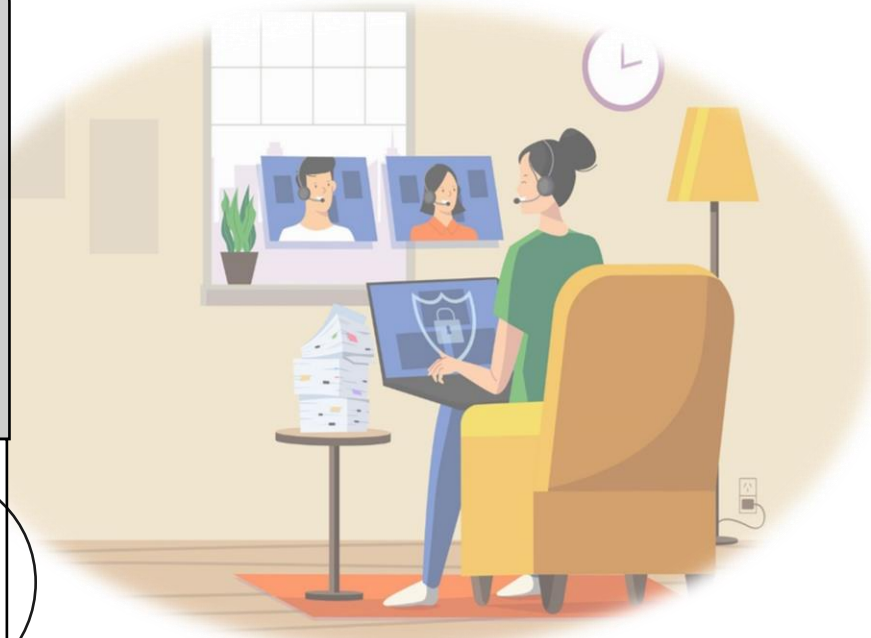
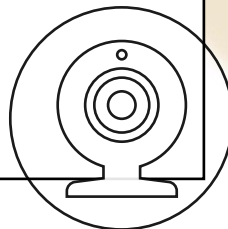
Increase in access/transfer of data & documents



New risks to data security and personal data privacy

- (i) intrusion into online meeting rooms
- (ii) unauthorised recording of meetings
- (iii) exposure of participants' private information

Increased popularity of video conferencing software



Personal Data Protection for WFH Arrangements



Regardless of whether one works in the office or works from home, the **same standard** should apply to the security of personal data and the protection of personal data privacy

Practical Advice to Organisations and Businesses



Risk assessments

- On data security and employees' personal data privacy
- Formulate appropriate safeguards



Policies and guidance

- Review and adjust existing policies based on the results of risk assessments
- Provide sufficient guidance regarding transfer of data, remote access, data destruction, etc.

Practical Advice to Organisations and Businesses



Staff training and support

- Provide sufficient training on data security
 - ✓ Data security techniques, cybersecurity threats and trends
- Deploy designated staff to provide support



Device management

- Ensure the security of data (including personal data) stored in the devices (if provided)
 - ✓ Install anti-malware software, encrypt information, control access, enable remote wipe

Practical Advice to Organisations and Businesses



Use of Virtual Private Network (VPN)

- Choose the appropriate protocol and type of VPN
- Keep the security setting up-to-date
- Require multi-factor authentication for connection
- Block connection from insecure devices



Practical guidance on the use of video conferencing (VC) software

When choosing VC software

- Assess the software's policies and measures on data security and privacy
- Choose a software with **end-to-end encryption** if discussion of confidential matters cannot be avoided

When Using VC software

- Set up strong passwords and **change passwords regularly**
- Activate **multi-factor authentication** if available
- Ensure software is up-to-date with latest security patches installed
- Use secure internet connection



Practical guidance on the use of video conferencing (VC) software



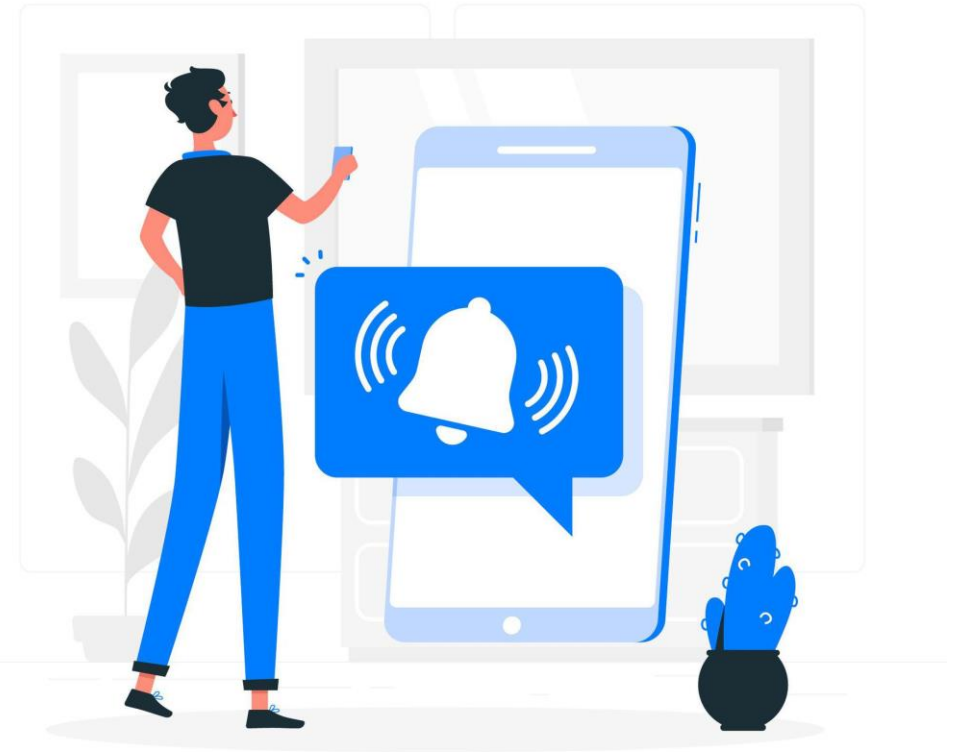
When hosting a video conference

- Set up unique meeting ID and password
- Provide meeting ID and password only to invited participants and, where possible, through different means (e.g. emails and instant messages)
- Arrange one more “host” to handle administrative, technical and ad hoc matters during the video conference
- Use virtual waiting room to validate participants’ identities before allowing entry
- Lock the meeting after all participants are admitted
- Allow only presenters to share screens or documents
- Inform participants and obtain consent before recording meeting; prohibit others from recording
- Store recorded videos and chats securely with password and encryption, delete the records when no longer necessary

Practical guidance on the use of video conferencing (VC) software

When participating in a video conference

- Beware of **background revealing personal information**
- Use **virtual background** if needed
- **Turn off microphone or camera** when not speaking
- **Avoid discussing personal or sensitive information**
- **Close unnecessary documents and windows** before sharing screen



Protecting Personal Data under Work-from-Home Arrangements: Guidance for Organisations

Introduction

1. Work-from-home (WFH) arrangements have been made from time to time during the COVID-19 pandemic. Under WFH arrangements, organisations may have to access or transfer data and documents through employees' home networks and employees' own devices, which are less secure than the professionally managed corporate networks and devices. This inevitably increases risks to data security and personal data privacy.
2. This Guidance serves to provide practical advice to organisations (including business entities) to enhance data security and the protection of personal data privacy under WFH arrangements.

General principles for WFH arrangements

3. Regardless of whether one works in the office or works from home, the same standard should apply to the security of personal data and the protection of personal data privacy. Organisations that implement WFH arrangements should adhere to the following principles:
 - (1) setting out clear policies on the handling of data (including personal data) during WFH arrangements¹; and
 - (2) taking all reasonably practicable steps to ensure the security of data, in particular when information and communications technology is used to facilitate WFH arrangements, or when data and documents are transferred to employees².

¹ Data Protection Principle (DPP) 5 in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) DPP 4

Protecting Personal Data under Work-from-Home Arrangements: Guidance on the Use of Video Conferencing Software

Introduction

1. Work-from-home (WFH) arrangements have been made from time to time during COVID-19 pandemic. As a result, video conferencing has fast become the new normal. The increasingly prevalent use of video conferencing software creates new risks to data security and personal data privacy¹.
2. This Guidance serves to provide practical advice to organisations and their employees to enhance data security and the protection of personal data privacy when they use video conferencing software. This Guidance is also applicable to other users of video conferencing software, such as teachers and students.
3. Organisations (including business entities) should review and assess the policies and measures on security and protection of personal data privacy of different video conferencing software in order to choose the ones that meet their requirements. For example, organisations may wish to use a video conferencing software with end-to-end encryption if they cannot avoid using the software for discussing confidential matters.

¹ Data Protection Principle 4 in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) requires data users to take all practicable steps to protect the personal data they hold against unauthorised or accidental access, processing, erasure, loss or use.

Protecting Personal Data under Work-from-Home Arrangements: Guidance for Employees

Introduction

1. Work-from-home (WFH) arrangements have been made from time to time during the COVID-19 pandemic. Under WFH arrangements, employees may have to access or transfer the data and documents of their employers through their home networks and own devices, which are less secure than the professionally managed corporate networks and devices of their employers. This inevitably increases risks to data security and personal data privacy.
2. This Guidance serves to provide practical advice to employees to enhance data security and the protection of personal data privacy under WFH arrangements.

General principles for WFH arrangements

3. Regardless of whether one works in the office or works from home, the same standard should apply to the security of personal data and the protection of personal data privacy. Employees should adhere to the following principles when they work from home:
 - (1) adhering to their employers' policies on the handling of data (including personal data); and
 - (2) taking all reasonably practicable steps to ensure the security of data, in particular when information and communications technology is used to facilitate WFH arrangements, or when the data and documents are transferred during the work process¹.

¹ Data Protection Principle 4 in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong)



Available for access

Doxxing Offences under the Personal Data (Privacy) Ordinance



27

PCPD



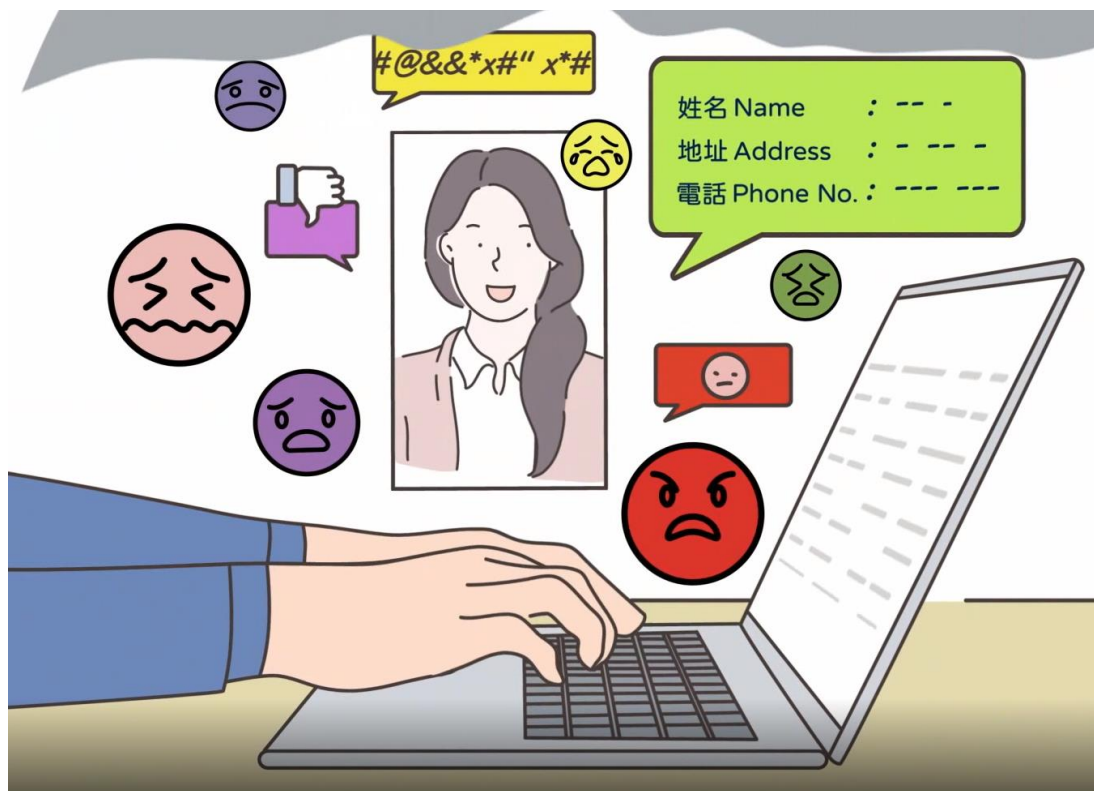
H K



PCPD.org.hk

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

The Personal Data (Privacy) (Amendment) Ordinance 2021 (“Amendment Ordinance”)



- PCPD handled over 6,000 doxxing cases since June 2019
- Weaponisation of personal data
- Serious and far-reaching harms caused to victims and their family members

Three main objectives of the Amendment Ordinance



To create offences to curb doxxing acts

To confer on the Commissioner powers to issue cessation notices

To empower the Commissioner to carry out criminal investigations and institute prosecutions

(I) Section 64 – Create Offences to Curb Doxxing Acts

New section 64(3A) of the PDPO – FIRST-TIER OFFENCE (without actual harm)

A person commits an offence if the person discloses any personal data of a data subject **without the relevant consent** of the data subject –

- (a) with an **intent** to cause **any specified harm** to the data subject or any family member of the data subject; or
- (b) being **reckless** as to whether **any specified harm** would be, or would likely be, caused to the data subject or any family member of the data subject.

New section 64(3B) of the PDPO – Penalty

(3B) A person who commits an offence under subsection (3A) is liable on conviction to a fine at level 6 (HK\$100,000) and to imprisonment for 2 years.

(I) Section 64 – Create Offences to Curb Doxxing Acts

New section 64(3C) of the PDPO – SECOND-TIER offence (with actual harm)

A person commits an offence if –

- (a) the person discloses any personal data of a data subject **without the relevant consent** of the data subject –
 - (i) with an **intent** to cause **any specified harm** to the data subject or any family member of the data subject; or
 - (ii) being **reckless** as to whether **any specified harm** would be, or would likely be, caused to the data subject or any family member of the data subject; and
- (b) the disclosure **causes any specified harm** to the data subject or any family member of the data subject.

New section 64(3D) of the PDPO – Penalty

(3D) A person who commits an offence under subsection (3C) is liable on conviction on indictment to a fine of HK\$1,000,000 and to imprisonment for 5 years.

(I) Section 64 – Create Offences to Curb Doxxing Acts

	FIRST-TIER - Summary Offence	SECOND-TIER – Indictable Offence
1.	Any personal data of a data subject is disclosed without the relevant consent of the <u>data subject</u>	
2.	Has an <u>intent</u> or is being <u>reckless</u> as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject	
3.	N/A	The <u>disclosure causes any specified harm</u> to the data subject or any family member of the data subject

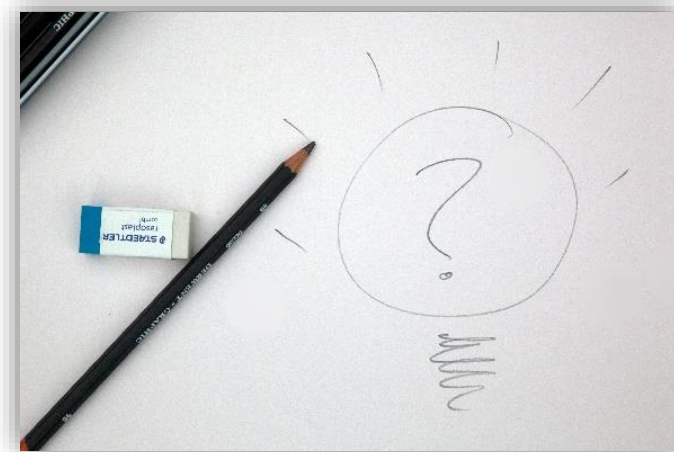


To determine the severity of the offence, the two-tier offence is differentiated by **whether actual harm has been caused to the data subjects or their family members.**

(I) Section 64 – Create Offences to Curb Doxxing Acts

- (a) harassment, molestation, pestering, threat or intimidation to the person;
- (b) bodily harm or psychological harm to the person;
- (c) harm causing the person reasonably to be concerned for the person's safety or well-being; or
- (d) damage to the property of the person

(new section 64(6) of the PDPO)



What constitutes specified harm, in relation to a person?

The Implications of the Amendment Ordinance

- To **criminalise** doxxing acts and **more effectively combat** the crime by **increasing the enforcement powers** of the Commissioner



The Amendment Ordinance will not affect:

- **normal and lawful business activities** in Hong Kong
- **freedom of speech** and **free flow of information** currently enjoyed by the public (as enshrined in the Basic Law and the Hong Kong Bill of Rights Ordinance)

(II) The Commissioner's powers to carry out criminal investigations and institute prosecutions

Issue **written notice** to request any person to provide relevant materials; or to answer relevant questions to facilitate investigation
(new section 66D of the PDPO)



The Commissioner may

Apply for **warrant** to enter and search **premises** and seize materials for investigation; or **access electronic device**
(new section 66G of the PDPO)

To **stop, search** and **arrest** any person who is reasonably suspected of having committed a doxxing-related offence
(new section 66H of the PDPO)

Prosecute **in the name of the Commissioner** a doxxing-related offence **triable summarily** in the Magistrates' Court
(new section 64C of the PDPO)

Failure to comply with the Commissioner's request is a **criminal offence**.

(II) The Commissioner's powers to carry out criminal investigations and institute prosecutions

Powers to require materials and assistance

(New section 66D of the PDPO)

If the Commissioner reasonably suspects that, in relation to a specified investigation, a person –

- **has or may have possession or control of any material** relevant to that investigation; or
- may otherwise be able to **assist** the Commissioner in relation to that investigation,

the Commissioner may, by written notice given to the person, require the person to provide materials and assistance.

Failure to comply with a written notice is an offence (new section 66E(2) of the PDPO).

- On summary conviction – a fine at level 5 (HK\$50,000) and imprisonment for 6 months
- On conviction on indictment – a fine of HK\$200,000 and imprisonment for 1 year



(II) The Commissioner's powers to carry out criminal investigations and institute prosecutions

Powers to require materials and assistance
(New section 66D of the PDPO)



It is an **offence** where, with **intent to defraud**:

- (i) a person fails to comply with a written notice issued pursuant to section 66D; or
- (ii) a person provides any answer or statement that is **false** or **misleading** in a material particular (new section 66E(6) of the PDPO)



- On summary conviction – a fine at level 6 (HK\$100,000) and imprisonment for 6 months
- On conviction on indictment – a fine of \$1,000,000 and imprisonment for 2 years

(II) The Commissioner's powers to carry out criminal investigations and institute prosecutions

Powers exercisable in relation to premises under warrant
(New section 66G(2) of the PDPO)



(a) To enter and search the premises;

(b) To carry out specified investigation in the premises; and

(c) To seize, remove and detain any material in the premises that the Commissioner or any prescribed officer reasonably suspects to be or to contain evidence for the purposes of the specified investigation



Under no circumstances shall the Commissioner or prescribed officers enter and search premises without a warrant.

(II) The Commissioner's powers to carry out criminal investigations and institute prosecutions

Powers exercisable in relation to electronic device under warrant

(New section 66G(3) of the PDPO)



(a) To access the device;

(b) To seize and detain the device;

(c) To decrypt any material stored in the device;

(d) To search for any material stored in the device that the Commissioner or any prescribed officer reasonably suspects to be or to contain evidence for the purposes of the specified investigation (relevant material);

(e) To reproduce the relevant material in visible and legible form;

(f) To reduce the relevant material into a written form on paper; and

(g) To make copies of, or take extracts from, the relevant material and take away such copies or extracts.

(II) The Commissioner's powers to carry out criminal investigations and institute prosecutions

Under what circumstances can powers be exercised in relation to electronic device without a warrant (New section 66G(8) of the PDPO)

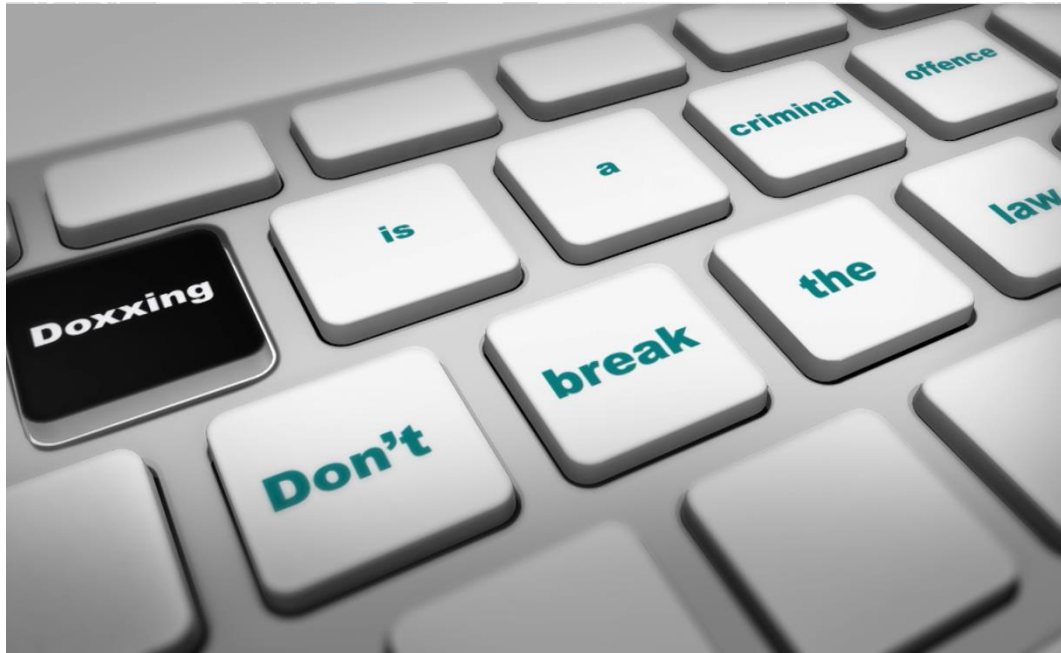
If the Commissioner or any prescribed officer

- (i) **reasonably suspects** that a doxxing or a related offence (i.e. under section 64(1), (3A) or (3C), 66E(1) or (5), 66(I)1 or 66O(1)) has been, is being or is about to be committed;
- (ii) **reasonably suspects** that any material that is or contains evidence for the purposes of a specified investigation is stored in an electronic device; and
- (iii) **is satisfied that** a delay caused by an application for a warrant is likely to defeat the purpose of accessing the device, or for any reason it is not reasonably practicable to make the application.



40

(II) The Commissioner's powers to carry out criminal investigations and institute prosecutions



A person who, without lawful excuse, **obstructs, hinders or resists** any officer in exercising the powers under section 66G or 66H, commits an offence (new section 66I of the PDPO)



On conviction

Subject to a fine at level 3 (HK\$10,000) and imprisonment for 6 months

(II) The Commissioner's powers to carry out criminal investigations and institute prosecutions

Prosecution of offences by the Commissioner (New section 64C of the PDPO)



(1) The Commissioner may prosecute **in the name of the Commissioner**—

- (a) an offence under section 64(1) or (3A), 66E(1) or (5), 66I(1) or 66O(1); or
- (b) an offence of conspiracy to commit such an offence.

(2) Any offence prosecuted under subsection (1) must be tried before a **magistrate** as an offence that is **triable summarily**.

(III) Confer on the Commissioner power to issue cessation notices

New sections 66K and 66M of the PDPO

1. Personal data of a data subject was disclosed **(whether or not in Hong Kong)** without the **consent of the data subject** by means of a **written message** or **electronic message**

2. The discloser had an **intent** or was being **reckless** as to whether any specified harm would be or would likely be, caused to the data subject or any family member of the data subject

3. When the disclosure was made, the data subject was **a Hong Kong resident**; or was **present in Hong Kong**

(III) Confer on the Commissioner power to issue cessation notices

Under what circumstances can the Commissioner serve a cessation notice

(New sections 66K and 66M of the PDPO)

- When the Commissioner has reasonable ground to believe that there is a **“subject message”**, the Commissioner may serve a cessation notice on a person who is **able** to take a cessation action.

Hong Kong Person

- (a) an individual who is present in Hong Kong ;
- (b) a body of persons that is incorporated, established or registered in Hong Kong; or
- (c) a body of persons that has a place of business in Hong Kong

Non-Hong Kong service provider

A person (not being a Hong Kong Person) that **has provided or is providing any service** (whether or not in Hong Kong) **to any Hong Kong person**



Cessation notices have extra-territorial application in respect of electronic messages.

44

(III) Confer on the Commissioner power to issue cessation notices

Offence for contravening a cessation notice (New section 66O(1) of the PDPO)

On first conviction

- a fine at level 5 (HK\$50,000) and imprisonment for 2 years, and in the case of a continuing offence, a further fine of HK\$1,000 for every day during which the offence continues



On each subsequent conviction

- a fine at level 6 (HK\$100,000) and imprisonment for 2 years; and in the case of a continuing offence, a further fine of HK\$2,000 for every day during which the offence continues

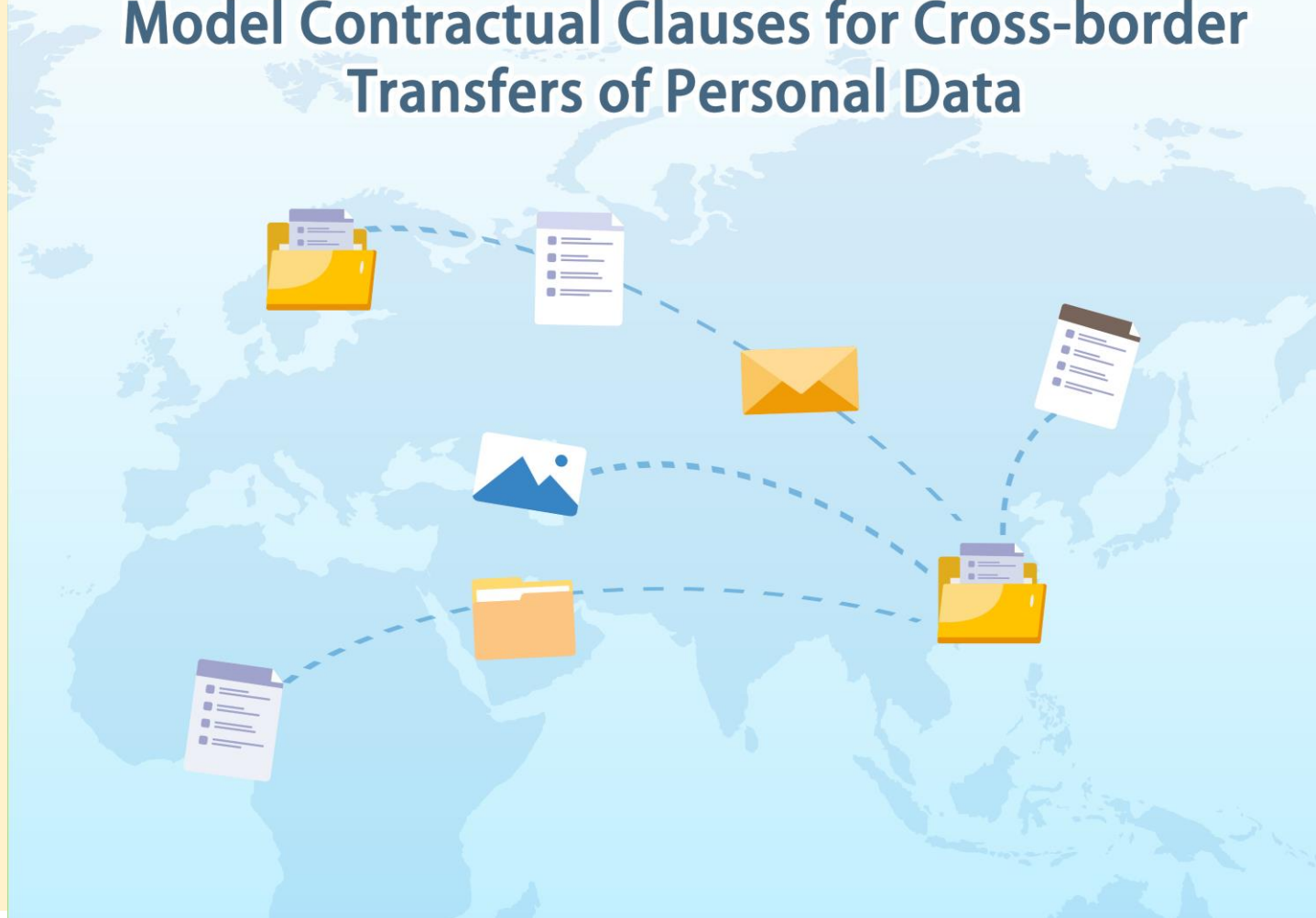
45

Injunctions (New section 66Q of the PDPO)

- The Commissioner may apply to the Court of First Instance for an **injunction**.
- The Court may grant an injunction in any terms that the Court considers appropriate, if it is satisfied that a person (or any person falling within a category or description of persons) **has engaged, is engaging or is likely to engage**, in doxxing offence.



PCPD Issues Guidance on Recommended Model Contractual Clauses for Cross-border Transfers of Personal Data



Regulation of Cross-border Flow of Personal Data

- **General Data Protection Regulation of the European Union**
 - ✓ Transfers on the basis of an adequacy decision; or
 - ✓ Transfers subject to appropriate safeguards (including but not limited to standard contractual clauses promulgated by the European Commission)
- **Personal Information Protection Law of mainland China**
 - ✓ consent of data subjects concerned;
 - ✓ personal information protection impact assessments; and
 - ✓ security assessments/certification/standard contracts/other applicable conditions



Legal Requirements under the PDPO



- The protection should follow the personal data irrespective of the location of the personal data

DPP 1 (Collection of Personal Data)

- All practicable steps shall be taken to ensure that, *inter alia*, the data subject is explicitly informed of the purpose for which the data is to be used and the potential transferees of the personal data concerned

DPP 3 (Use of Personal Data)

- The data subject's prescribed consent would be required if the transfer is for a new purpose, unless it falls within the exemptions under Part 8 of the PDPO

49

Legal Requirements under the PDPO

Engagement of data processors to process personal data outside Hong Kong

- The data user must adopt **contractual or other means to**
 - ✓ prevent any personal data transferred to the data processor from being kept longer than is necessary for the processing of the data (DPP2(3))
 - ✓ prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing (DPP4(2))



50

Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data



Available for access



Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data

PART 1: INTRODUCTION

Given the increasing digitalisation in the handling of personal data and globalisation of business operations in recent years, local enterprises, especially the small and medium-sized ones, may experience practical difficulties in crafting appropriate contractual terms for effecting cross-border transfers of personal data while ensuring that the data concerned be given equivalent protection to the degree provided under the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO). Meanwhile, with the proliferation and advancement of information and communication technology including the big data, cloud computing and data analytics, the challenges and complexities involved in cross-border data transfers are set to mount.

The Office of the Privacy Commissioner for Personal Data has prepared two sets of Recommended Model Contractual Clauses (RMCs) to cater for two different scenarios in cross-border data transfers, namely (i) from one data user to another data user; and (ii) from a data user to a data processor. The RMCs set out the general terms and conditions which are applicable to the transfer of personal data from a Hong Kong entity to another entity outside Hong Kong; or between two entities both of which are outside Hong Kong when the transfer is controlled by a Hong Kong data user, with a view to facilitating the parties to cross-border transfers of personal data to take into account the relevant requirements of the PDPO, including the Data Protection Principles (DPPs) under Schedule 1 thereof.

The RMCs are prepared as free-standing clauses, which may be incorporated into more general commercial agreements between data transferors and data transferees. This Guidance provides detailed elaborations as to the substantive effect of the RMCs, and how adherence to the same ensures that adequate protection be given to the personal data as provided under the PDPO as if the data concerned were not transferred outside Hong Kong.

Notwithstanding that section 33 of the PDPO, which imposes restrictions on cross-border transfers of data, is not yet in operation, this Guidance recommends to data users, especially the small and medium-sized enterprises, the best practices to be adopted as part of their data governance responsibility to protect and respect the personal data privacy of data subjects.

This Guidance supplements the Guidance on Personal Data Protection in Cross-border Data Transfer, including the Recommended Model Clauses in the Schedule annexed thereto, issued by this Office in December 2014¹.

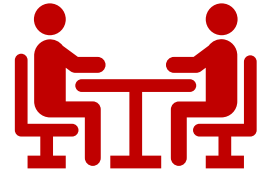
The legal requirements

Data Protection Principle 3 of the PDPO, which is directed against the misuse of personal data, specifies that personal data shall not, without the data subject's prescribed consent, be used for a new purpose. "New purpose" means in essence any purpose other than the one for which the personal data was originally

¹ The Guidance on Personal Data Protection in Cross-border Data Transfer is available at https://www.pcpd.org.hk/english/resources_centre/publications/files/OK_crossborder_a.pdf.

- Containing the core provisions for cross-border data transfers which may be adopted by small and medium-sized enterprises readily in order to comply with the requirements of the PDPO and good data ethics
- The Clauses contained in the “Guidance on Personal Data Protection in Cross-border Data Transfer” published by the PCPD in December 2014 may be more suitable for multinational corporations or organisations which are involved in more complex cross-border transfers of personal data

Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data



Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data

PART 1: INTRODUCTION

Given the increasing digitalisation in the handling of personal data and globalisation of business operations in recent years, local enterprises, especially the small and medium-sized ones, may experience practical difficulties in crafting appropriate contractual terms for effecting cross-border transfers of personal data while ensuring that the data concerned be given equivalent protection to the degree provided under the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO). Meanwhile, with the proliferation and advancement of information and communication technology including the big data, cloud computing and data analytics, the challenges and complexities involved in cross-border data transfers are set to mount.

The Office of the Privacy Commissioner for Personal Data has prepared two sets of Recommended Model Contractual Clauses (RMCs) to cater for two different scenarios in cross-border data transfers, namely (i) from one data user to another data user; and (ii) from a data user to a data processor. The RMCs set out the general terms and conditions which are applicable to the transfer of personal data from a Hong Kong entity to another entity outside Hong Kong; or between two entities both of which are outside Hong Kong when the transfer is controlled by a Hong Kong data user, with a view to facilitating the parties to cross-border transfers of personal data to take into account the relevant requirements of the PDPO, including the Data Protection Principles (DPPs) under Schedule 1 thereof.

The RMCs are prepared as free-standing clauses, which may be incorporated into more general commercial agreements between data transferors and data transferees. This Guidance provides detailed elaborations as to the substantive effect of the RMCs, and how adherence to the same ensures that adequate protection be given to the personal data as provided under the PDPO as if the data concerned were not transferred outside Hong Kong.

Notwithstanding that section 33 of the PDPO, which imposes restrictions on cross-border transfers of data, is not yet in operation, this Guidance recommends to data users, especially the small and medium-sized enterprises, the best practices to be adopted as part of their data governance responsibility to protect and respect the personal data privacy of data subjects.

This Guidance supplements the Guidance on Personal Data Protection in Cross-border Data Transfer, including the Recommended Model Clauses in the Schedule annexed thereto, issued by this Office in December 2014¹.

The legal requirements

Data Protection Principle 3 of the PDPO, which is directed against the misuse of personal data, specifies that personal data shall not, without the data subject's prescribed consent, be used for a new purpose. "New purpose" means in essence any purpose other than the one for which the personal data was originally

¹ The Guidance on Personal Data Protection in Cross-border Data Transfer is available at https://www.pcpd.org.hk/english/resources_centre/publications/files/OK_crossborder_a.pdf.

- The adoption of the RMCs serves to illustrate that the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in the jurisdiction of the transferee, be handled in any manner which, if that took place in Hong Kong, would be a contravention of a requirement under the PDPO
- To ensure that adequate protection be given to the personal data as provided for under the PDPO, as if the data concerned were not transferred outside Hong Kong

Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data

To cater for two different scenarios in cross-border transfers of personal data



(A) From one data user to another data user

(B) From a data user to a data processor

Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data

Containing general terms and conditions which may be incorporated into more general commercial agreements between data transferors and data transferees in transfers of personal data:



(I) From a Hong Kong entity to another entity outside Hong Kong

(II) Between two entities both of which are outside Hong Kong when the transfer is controlled by a Hong Kong data user

54

(A) Data User to Data User RMCs



- **Use:** A transferee should only use the personal data for the purposes of transfer (Note the clauses concerning direct marketing).
- **Onward transfers:** A transferee should not make any onward transfer of the personal data except as agreed by the parties; and should ensure that onward transfers of the personal data meet the requirements of the applicable RMCs.
- **Security:** A transferee should apply agreed security measures to the use of the personal data.
- **Retention and erasure:** A transferee should retain the personal data only for a period which is necessary for the fulfillment of the purposes of transfer and take all practicable steps to erase the personal data once the purposes of transfer have been achieved.
- **Transparency:** A transferee should take all practicable steps to ensure that data subjects should be able to access its personal data policies and practices.
- **Data Access and Correction Requests:** The transferring parties will each comply with their respective obligations in handling such requests.

(B) Data User to Data Processor RMCs



- **Processing:** A transferee should only process the personal data for the purposes of transfer.
- **Onward transfers:** A transferee should not make any onward transfer of the personal data except as agreed by the parties; and should ensure that onward transfers of the personal data meet the requirements of the Data User to Data Processor RMCs.
- **Security:** A transferee should apply agreed security measures to the processing of the personal data.
- **Retention and erasure:** A transferee should retain the personal data only for a period which is necessary for the fulfillment of the purposes of transfer and take all practicable steps to erase the personal data once the purposes of transfer have been achieved.

Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data

Good Data Ethics

- doing what is reasonably expected by data subjects
- being transparent about data processing activities
- By adopting RMCs and observing the principles of transparency and accountability, it will be conducive not only to maximising the value of data but also to developing and sustaining the trust of data subjects



Thank You!

Contact Us

Anti-Doxxing Hotline : 3423 6666

Enquiry : 2827 2827

Website : www.pcpd.org.hk

Anti-Doxxing Thematic Webpage:

www.pcpd.org.hk/english/doxxing/index.html

E-mail :

communications@pcpd.org.hk

complaints@pcpd.org.hk