25th ACRU

Office of the Privacy Commissioner for Personal Data, Hong Kong

3:40pm – 4:40pm, 7 June 2024

Speakers:

Mr Brad KWOK, Chief Personal Data Officer (Compliance & Enquiries)
Ms Clemence WONG, Senior Legal Counsel (Acting)

25th ACRU

1. Data Security Management and Incident Response

2. Cross-boundary Flow of Personal Information within the Greater Bay Area

Data Security Management and Incident Response

Mr Brad KWOK
Chief Personal Data Officer (Compliance & Enquiries)

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

Relevant Requirements under the PDPO

Data Protection Principle 4(1)

All practicable steps shall be taken to protect personal data from unauthorised or accidental access, processing, erasure, loss or use

Data Protection Principle 4(2)

If a **data processor** is engaged to process personal data, the data user must **adopt contractual or other means** to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing

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

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

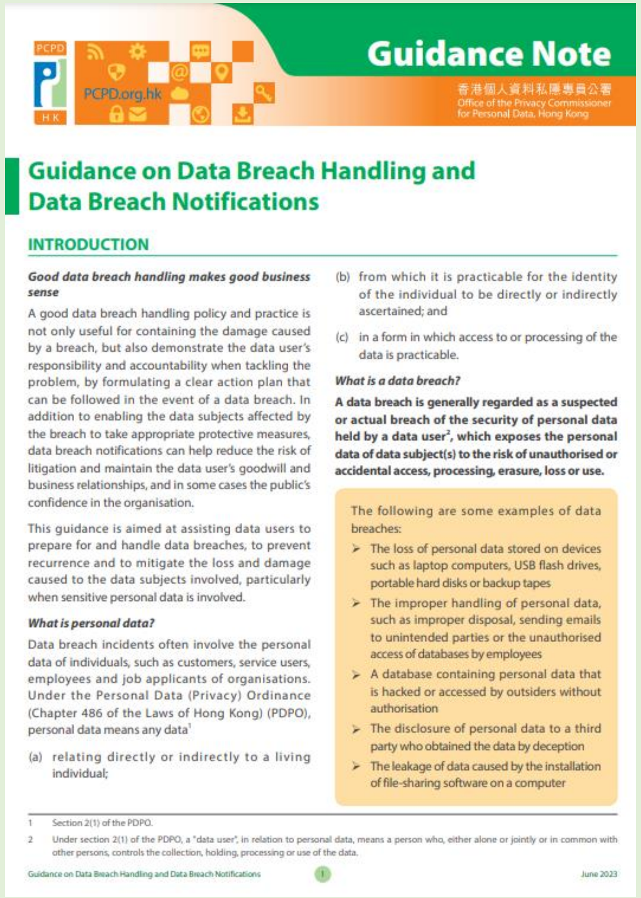
Elements (Non-exhaustive)

- 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

1. Immediate gathering of essential information
2. Containing the data breach
3. Assessing the risk of harm
4. Considering giving data breach notifications
5. 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[1]

(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[2], 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.

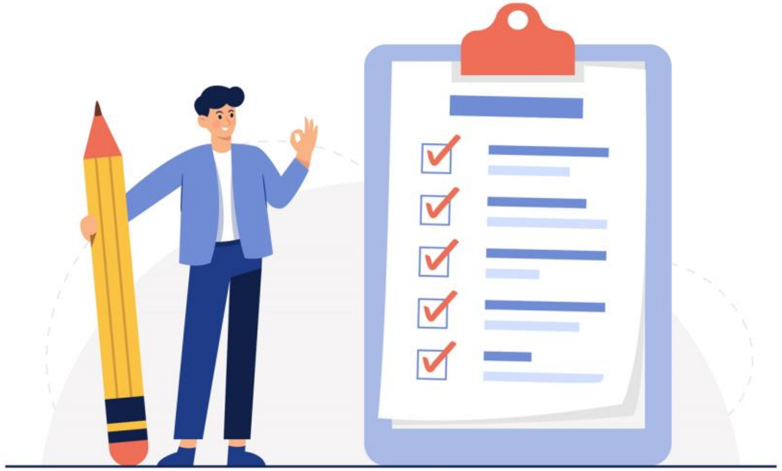
Guidance on Data Breach Handling and Data Breach Notifications 1 June 2023

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

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

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:

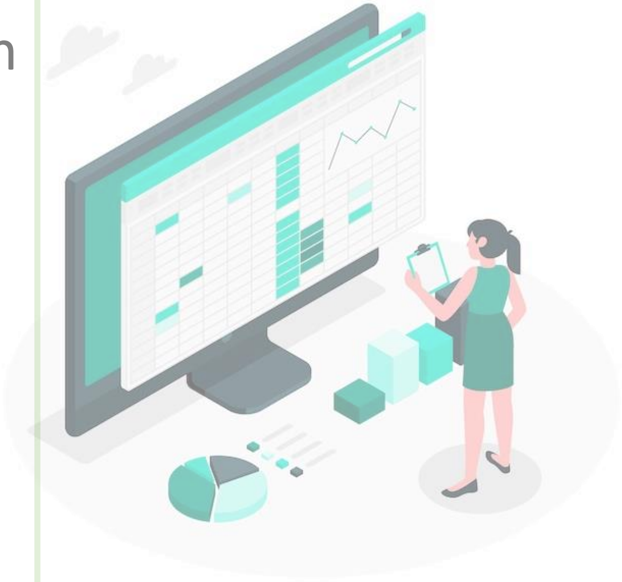
- ✓ Draw the affected data subjects' attention to **take proactive steps or measures to mitigate any potential harm or damage**
- ✓ Enable the relevant authorities to undertake appropriate **investigative** or **follow-up actions**
- ✓ Demonstrate the data user's commitment to robust personal data privacy 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**

Follow the data breach policy / process
The Guidance on Data Breach Handling and the Giving of Data Breach Notifications
Data Breach Information Sheet

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

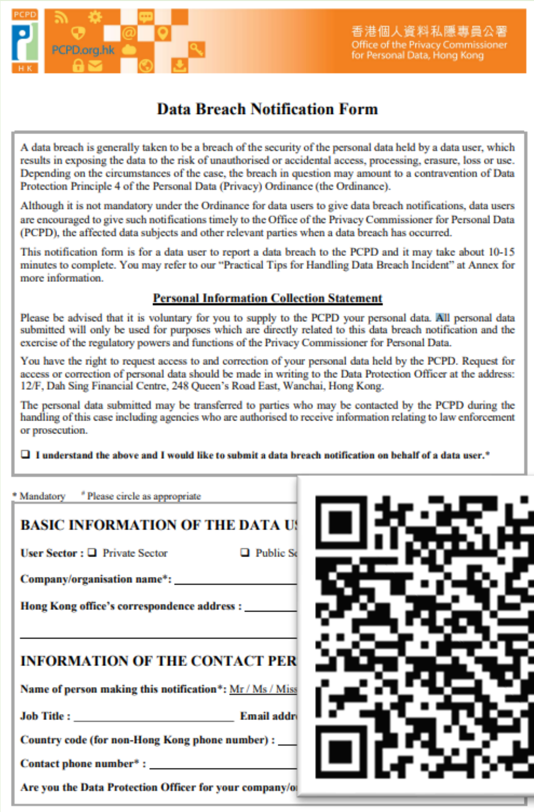
How to notify?

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



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

PCPD.org.hk

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 U

User Sector : □ Private Sector □ Public Se

Company/organisation name*: ____________

Hong Kong office's correspondence address : ____________

____

INFORMATION OF THE CONTACT PER

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

Job Title : ____________ **Email addr**

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

Contact phone number* : ____________

Are you the Data Protection Officer for your company/o

Data Breach Notification Form

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.

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

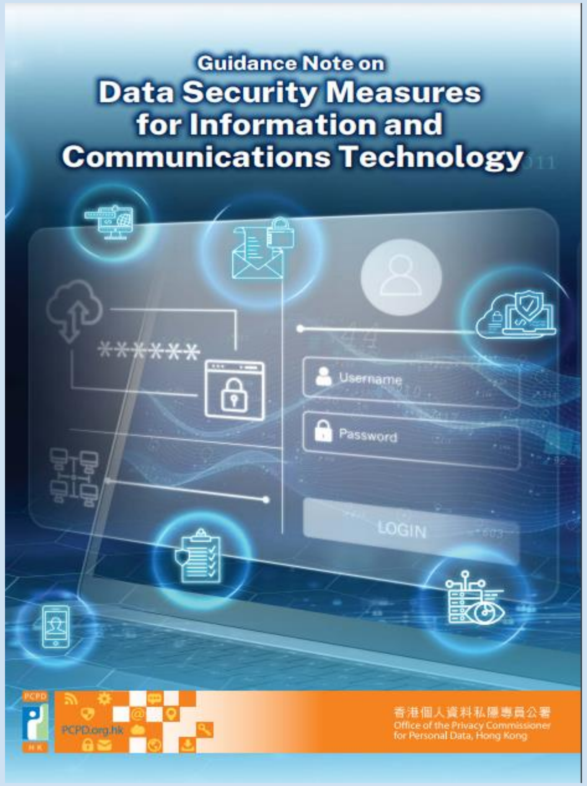
NOTE

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

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



Guidance Note on
Data Security Measures
for Information and
Communications Technology

Username
Password
LOGIN
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

Download the Guidance Note

Recommended Data Security Measures for ICT

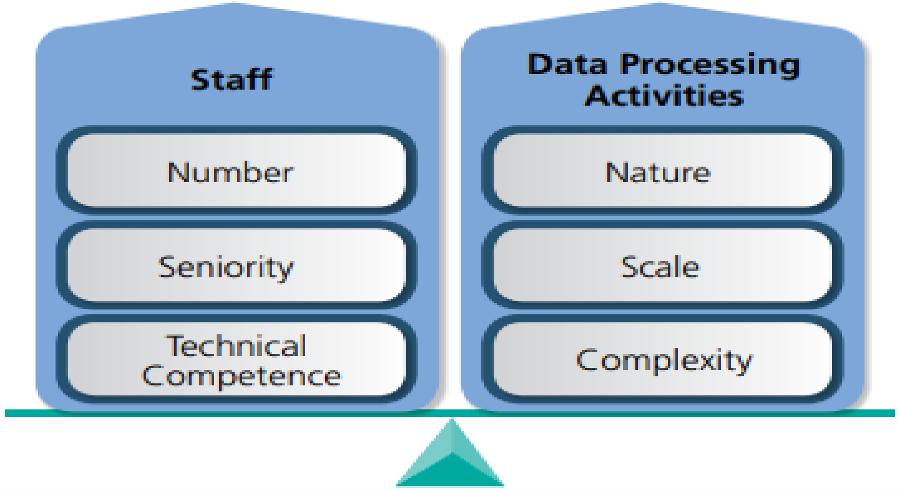
1) Data Governance and Organisational Measures

- 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

Proportionate Staff Allocation



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.

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

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

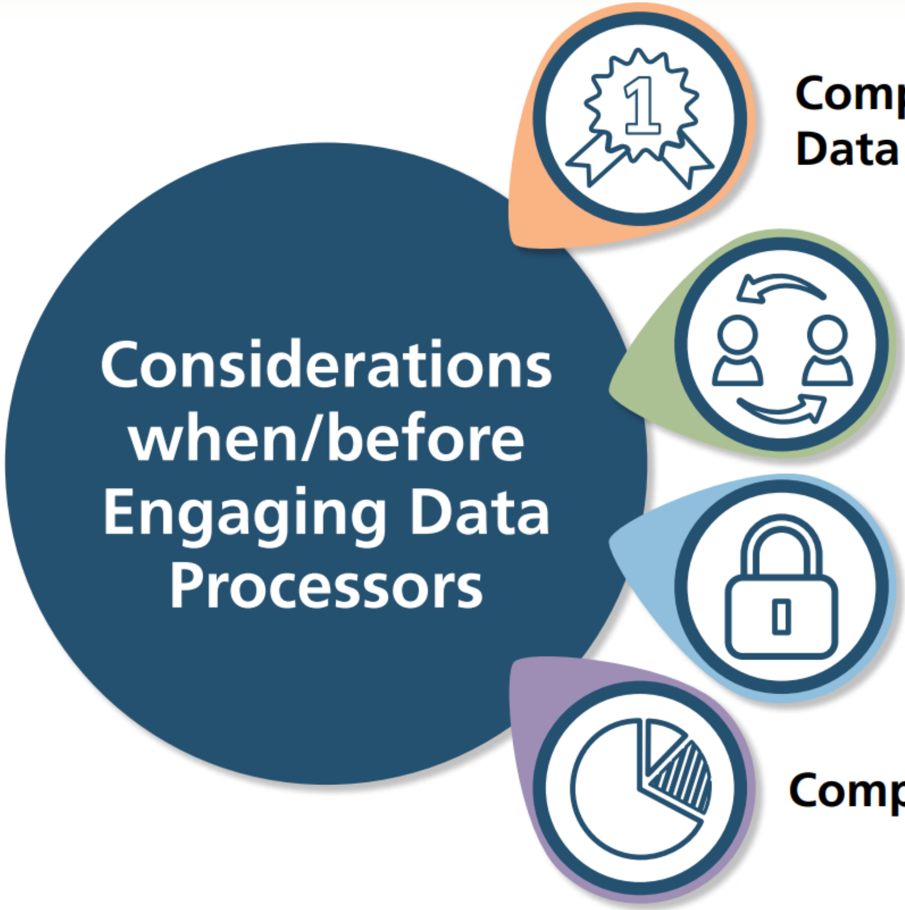
Recommended Data Security Measures for ICT

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



Considerations when/before Engaging Data Processors

- **Competency and Reliability of Data Processors**
- **Personal Data to be Transferred**
- **Handling of Data Security Incidents**
- **Compliance and Audits**

Recommended Data Security Measures for ICT

5) Remedial Actions in the Event of Data Security Incidents

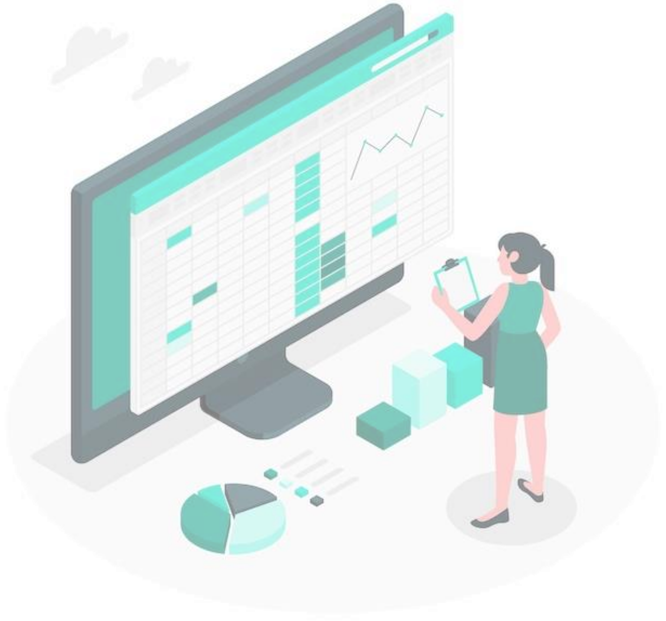
- Stopping and Disconnecting the Affected Systems ✓
- Changing Passwords or Ceasing Access ✓
- Changing System Configurations ✓
- Notifying and Advising the Affected Individuals ✓
- Reporting to the PCPD and Other Law Enforcement Agencies/ Regulators ✓
- Fixing the Security Weakness ✓
- Scanning the 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.

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

數據安全熱線
Data Security Hotline
2110 1155

數據安全快測
Data Security Scanner

About PCPD | Data Privacy Law | News & Events | Enforcement Reports | Frequently Asked Questions | Compliance & Enforcement | Doxxing Offences |
Data Security NEW! | Anti-fraud Tips | Complaints | Education & Training | Resources Centre | Contact Us

Home > Data Security NEW!

Data Security
NEW!

Data Security

7 Recommended
Data Security Measures

Data Governance and Organisational Measures

Risk Assessments

Technical and Operational Security Measures

Data Processor Management

Remedial Actions in the Event of

數據安全專題網頁
Data Security Webpage

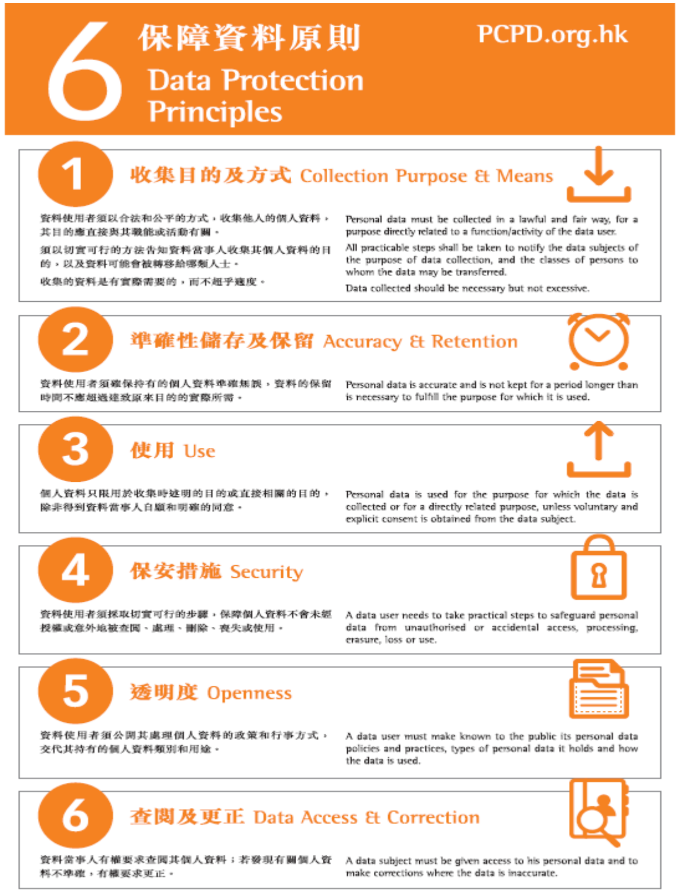
Cross-boundary Flow of Personal Information within the Greater Bay Area

Ms Clemence WONG
Senior Legal Counsel (Acting)

Data Protection Law in Hong Kong

- The Personal Data (Privacy) Ordinance (“PDPO”) is the legal framework for **safeguarding personal data privacy** in Hong Kong

- All data users must comply with the requirements of the PDPO, which include **six Data Protection Principles (“DPPs”)**



6 保障資料原則 Data Protection Principles

PCPD.org.hk

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

資料使用者須確保持有的個人資料準確無誤，資料的保留時間不應超過達致原來目的的實際所需。

Personal data is accurate and is not kept for a period longer than is necessary to fulfill 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 practical steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5 透明度 Openness

資料使用者須公開其處理個人資料的政策和行事方式，交代其持有的個人資料類別和用途。

A data user must make known to the public its personal data policies and practices, 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.

The Requirements under the PDPO in Transferring Personal Data from Hong Kong

DPP1 (Purpose and Manner of Collection of Personal Data)

- All practicable steps shall be taken to ensure, inter alia, that 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

DPP3 (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

The Requirements under the PDPO in Transferring Personal Data from Hong Kong

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))

Facilitation Measures of Using Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong–Hong Kong–Macao Greater Bay Area (Mainland, Hong Kong)

- The PCPD welcomes the facilitation measures of using the Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong) (“**GBA SC**”)

- The PCPD is very grateful to the staunch support of the Cyberspace Administration of China in facilitating the cross-boundary flow of personal information within the GBA

Aligning with the Relevant Laws and Regulations of the Mainland

- The GBA SC adopts the concept of "respective jurisdiction"

- Ensuring that personal information processors and recipients can transfer personal information across boundaries in accordance with the relevant legal requirements of their respective jurisdictions

The PCPD encourages organisations to adopt the GBA SC for cross-boundary flows of personal information within the Greater Bay Area

Key Definitions under the GBA SC

	Mainland	Hong Kong
Personal Information Processor (The party who transfers personal information across the boundary)	an organisation or individual that autonomously determines the purposes and means of processing the personal information	**covers a "data user" in Hong Kong** – a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the personal data
Personal Information Subject	a natural person who can be identified by or is associated with the personal information	**covers a "data subject" in Hong Kong** – the individual who is the subject of the personal data
Personal Information	determined in accordance with the Personal Information Protection Law	determined in accordance with the PDPO

Key Requirements of the GBA SC

Personal information processors and recipients have to comply with the requirements set out in the GBA SC. For instance:

- Obtaining the consent of the personal information subjects prior to the cross-boundary transfer of personal information in accordance with the laws and regulations of the jurisdiction concerned
- Executing agreements that adopt the GBA SC
- Conduct personal information protection impact assessments (which must be completed within 3 months before the filing date), and so on

Relaxation of Requirements as a Facilitation Measure

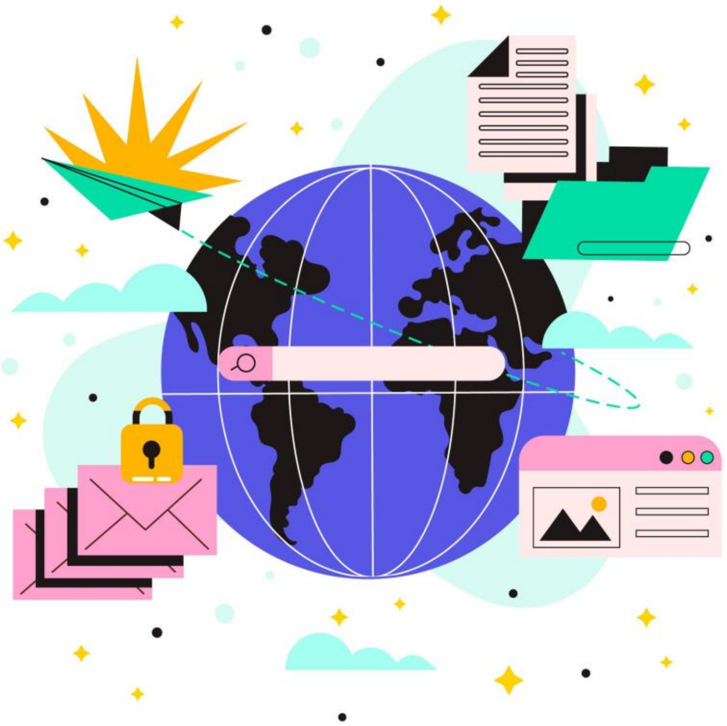
As a facilitation measure, the GBA SC has relaxed some of the requirements set out in the Mainland's Measures on the Standard Contract for Cross-border Transfers of Personal Information out of the Mainland

- The restriction concerning the amount and sensitivity of the personal information that may be transferred across borders was removed
- The parties to the GBA SC are not required to conduct relevant assessments of the personal information protection policies and regulations in the region where the recipient is located
- The scope of the personal information protection impact assessment to be conducted by personal information processors is greatly reduced
- There is no specific requirement regarding sensitive personal information or automated decision-making mechanisms

Additional Requirements Imposed under the GBA SC

The GBA SC imposes additional contractual requirements relative to the requirements under the PDPO

- The personal information processor shall conduct a personal information protection impact assessment on the intended transfer
- The parties shall adhere to the filing procedures of the GBA SC
- Restrictions of further transfer of personal information out of the GBA are imposed upon the recipient



The GBA SC

Article 1 Definition

Article 2 Obligations and Responsibilities of Personal Information Processors

Article 3 Obligations and Responsibilities of Recipients

Article 4 Rights of Personal Information Subjects

Article 5 Remedies

Article 6 Termination of Contract

Article 7 Liabilities for Breach of Contract

Article 8 Miscellaneous

Appendix I Description of Cross-boundary Transfer of Personal Information

Appendix II Other Terms Agreed by Both Parties (If Necessary)

Key Obligations and Responsibilities of Personal Information Processors

Article 2

(2) Inform the personal information subjects (including data subjects) of the requisite information, such as name and contact information of the recipient, purposes and means of processing, etc.

(3) Obtain the consent of the personal information subjects prior to the cross-boundary transfer of personal information in accordance with the laws and regulations of the jurisdiction concerned

Key Obligations and Responsibilities of Personal Information Processors

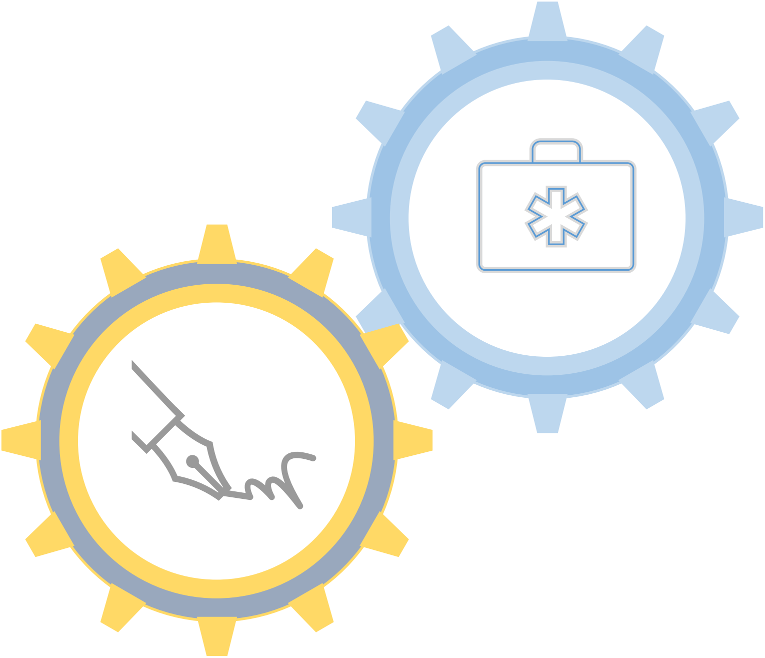
Article 2

(5) Make reasonable efforts to ensure that the recipient adopts technical and management measures (comprehensively considering the personal information risks that may arise), in order to fulfil its obligations and responsibilities under the GBA SC

(7) Respond to enquiries from the regulatory authorities of the jurisdiction concerned regarding the personal information processing activities of the recipient

Key Obligations and Responsibilities of Personal Information Processors

Article 2



(8) Conduct a personal information protection impact assessment on the intended activities of transferring personal information to the recipient, which shall focus on the following:

1. The legality, legitimacy and necessity of the purposes and means, etc. of processing personal information by the personal information processor and recipient;
2. The impact on and security risks to the rights and interests of personal information subjects;
3. Whether the obligations undertaken by the recipient, as well as its management, technical measures and capabilities, etc. to perform the obligations, can ensure the security of personal information transferred across the boundary.

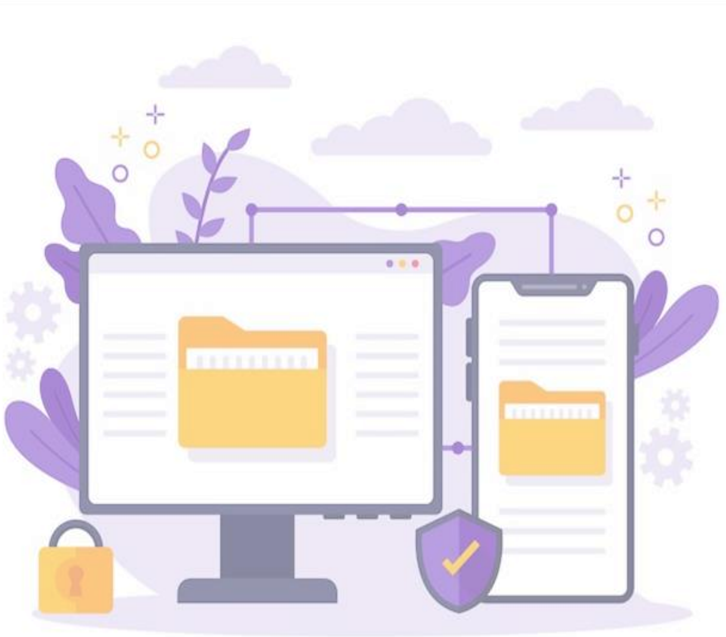
Key Obligations and Responsibilities of Personal Information Processors

Article 2

(11) Provide the regulatory authorities of the jurisdiction concerned with the information referred to in Article 3(10) of the Contract, including all the compliance audit findings in accordance with the requirements under the relevant laws and regulations of the jurisdiction concerned and the Contract

Key Obligations and Responsibilities of Recipients

Article 3



(5) Safeguard security of personal information processing by:

1. Adopting technical and management measures and conducting regular inspections to ensure security of personal information;
2. Ensuring that the personnel authorised to process personal information fulfil their confidentiality obligations and responsibilities, and establishing access control with the least privilege.

Key Obligations and Responsibilities of Recipients

Article 3

(6) If the personal information processed is or may be tampered with, damaged, disclosed, lost, unlawfully used, provided or consulted or accessed without authorisation, the following measures should be adopted:

1. Adopt appropriate remedial measures in a timely manner to mitigate the adverse impact on the personal information subject;
2. Notify the personal information processor immediately and report to the regulatory authorities of the jurisdiction concerned;

Key Obligations and Responsibilities of Recipients

Article 3(6)

3. Where personal information subject shall be notified under the relevant laws and regulations, such notice shall contain:

- the categories of personal information involved as well as the reasons and possible harm
- remedial measures adopted
- measures that the personal information subject may take to mitigate the harm
- contact information of the person or team in charge;

4. Record and retain all related circumstances, including all remedial measures adopted.

Key Obligations and Responsibilities of Recipients

Article 3

(7) Not to provide personal information received under the Contract to individuals and organisations outside the GBA

Key Obligations and Responsibilities of Recipients

Article 3

(8) May only provide personal information to a third party in the same jurisdiction in the Mainland cities within the GBA or Hong Kong if:

1. There is a business need for the transfer;
2. The personal information subject has been informed of the requisite information, such as the third party's name, contact information, purposes and means of processing, etc.;
3. The consent of the personal information subject has been obtained in accordance with the laws and regulations of the jurisdiction of the personal information processor, if the processing is based on the consent of the individual; AND
4. The personal information is provided to a third party in the same jurisdiction in accordance with the terms set out in Appendix I: "Description of cross-boundary transfer of personal information".

Key Obligations and Responsibilities of Recipients

Article 3

(12) Agree to be supervised and managed by the regulatory authorities of the jurisdiction concerned under the relevant supervisory procedures in the course of the implementation of the Contract, such as answering the enquiries of the regulatory authorities of the jurisdiction concerned, complying with the measures taken and decisions made by the regulatory authorities of the jurisdiction concerned, etc.

Key Obligations and Responsibilities of Recipients

Article 3

(13) Where government departments or judicial bodies of the jurisdiction where the recipient is located request the recipient to provide personal information received under the Contract, the personal information processor shall be notified immediately.

The GBA SC – Appendix I:
Description of cross-boundary transfer of personal information

(1) Purposes of processing

(2) Means of processing

(3) The scale of personal information transferred

(4) The categories of personal information transferred

(5) The provision of personal information to a third party in the same jurisdiction (if applicable)

(6) Means of transfer

(7) Retention period after being transferred

(8) Place of retention after being transferred

(9) Other matters (as the case may require)

Details of the cross-boundary transfer of personal information as agreed under the GBA SC

PCPD’s
Guidance on Cross-boundary Data Transfer: Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)

PCPD HK PCPD.org.hk

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 Cross-boundary Data Transfer: Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong – Hong Kong – Macao Greater Bay Area (Mainland, Hong Kong)

Part 1: Introduction

Given the close integration of cities within the Guangdong–Hong Kong–Macao Greater Bay Area (**GBA**), and that data flows between Hong Kong and other cities within the GBA are becoming increasingly frequent, the Cyberspace Administration of China (**CAC**) and the Innovation, Technology and Industry Bureau of the Government of the Hong Kong Special Administrative Region (**ITIB**) signed the Memorandum of Understanding on Facilitating Cross-boundary Data Flow Within the Guangdong–Hong Kong–Macao Greater Bay Area (**MoU**) on 29 June 2023 to jointly promote cross-boundary data flows in the GBA.

The Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong–Hong Kong–Macao Greater Bay Area (Mainland, Hong Kong) (**GBA SC**) (see Appendix) is a facilitation measure under the MoU to foster the cross-boundary flows of personal information[1] within the GBA. It was formulated by the CAC, ITIB, and Office of the Privacy Commissioner for Personal Data, Hong Kong (**PCPD**).

Through this Guidance, the PCPD aims to help organisations in Hong Kong understand the applicability of the GBA SC and the relationship between the GBA SC and other Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data (**RMCs**) issued by the PCPD.

Requirements under the Personal Data (Privacy) Ordinance

Where a data user transfers personal data to places outside Hong Kong, it is required to comply with the relevant requirements under the Personal Data (Privacy) Ordinance (Cap. 486) (**PDPO**), including the Data Protection Principles (**DPPs**) in Schedule 1 of the PDPO.

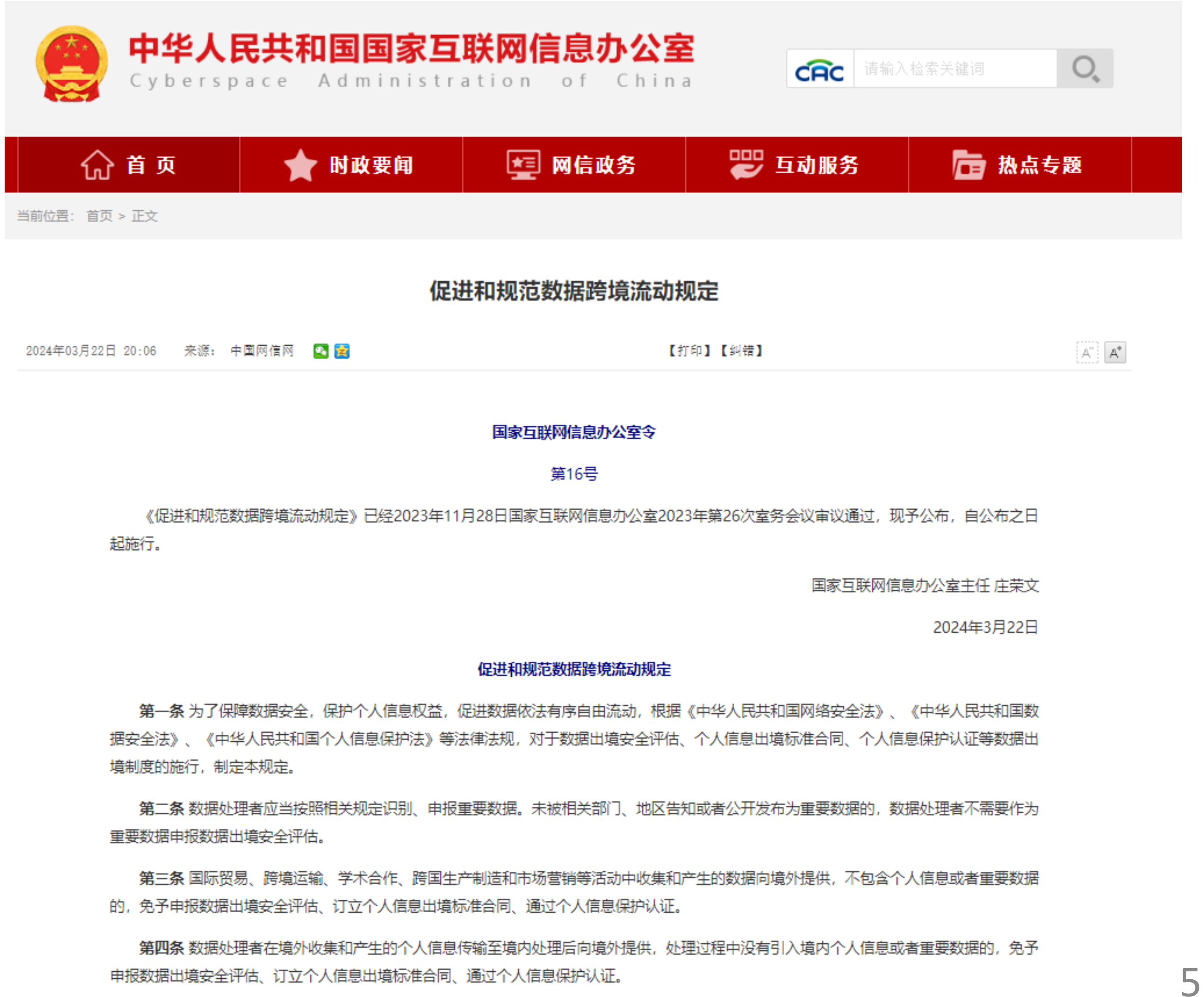
DPP1 of the PDPO stipulates the requirements relating to the purpose and manner of the collection of personal data. If a data user collects personal data directly from a data subject, the data user should take all practicable steps to ensure that the data subject is explicitly informed of the purpose for which the data is to be used and the classes of persons to whom the data may be transferred. Therefore, when a data user conducts cross-boundary data transfers to places outside Hong Kong, it should inform the data subject that his or her personal data will be transferred to data recipients outside Hong Kong and the purpose for which the data is to be used.

[1] According to the GBA SC, personal information processed by personal information processors in the Mainland cities of the GBA shall be determined in accordance with the Personal Information Protection Law of the People's Republic of China; personal information processed by personal information processors in the Hong Kong Special Administrative Region shall be determined in accordance with the definition of "personal data" under the Personal Data (Privacy) Ordinance of the Hong Kong Special Administrative Region.

Guidance on Cross-boundary Data Transfer 1 December 2023

"Regulations on Facilitating and Regulating Cross-Border Data Flow"

- Released by the CAC on 22 March 2024
- Introduces, amongst others, certain exemptions where data processors may be exempted from conducting security assessments, entering into standard contracts, or obtaining personal information protection certification
- Applies to cross-boundary data flows between the Mainland cities in the GBA and Hong Kong



中华人民共和国国家互联网信息办公室
Cyberspace Administration of China

促进和规范数据跨境流动规定

2024年03月22日 20:06 来源： 中国网信网 【打印】【纠错】

国家互联网信息办公室令

第16号

《促进和规范数据跨境流动规定》已经2023年11月28日国家互联网信息办公室2023年第26次室务会议审议通过，现予公布，自公布之日起施行。

国家互联网信息办公室主任 庄荣文

2024年3月22日

促进和规范数据跨境流动规定

第一条 为了保障数据安全，保护个人信息权益，促进数据依法有序自由流动，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规，对于数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度的施行，制定本规定。

第二条 数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

第三条 国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

第四条 数据处理者在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

"Regulations on Facilitating and Regulating Cross-Border Data Flow"

For example, situations where there can be exemptions from conducting security assessments, entering into standard contracts or obtaining personal information protection certifications include:

Article 5	1. the outbound transfer of personal information is **necessary for the execution and performance of a contract** to which the individuals are parties (e.g., for cross-border purchases, cross-border deliveries, cross-border remittances, cross-border payments, cross-border account opening, hotel and air ticket reservations, visa applications, examination services etc.)
	2. the outbound transfer of employees' personal information is **necessary for the implementation of cross-border human resources management** in accordance with applicable labour regulations and legally executed collective contracts
	3. the outbound transfer of personal information is **necessary in emergency circumstances to protect an individual's life, health, and safety of his or her properties**; or
	4. the data processor that is not a critical information infrastructure operator (CIIO) transfers personal information **of less than 100,000 individuals (excluding sensitive personal information) since 1 January of the current year**.

FOLLOW US

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

@ communications@pcpd.org.hk