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

Office of the Privacy Commissioner for Personal Data, Hong Kong

20 August 2024

Speaker:
Ms Clemence WONG, Senior Legal Counsel (Acting)

01

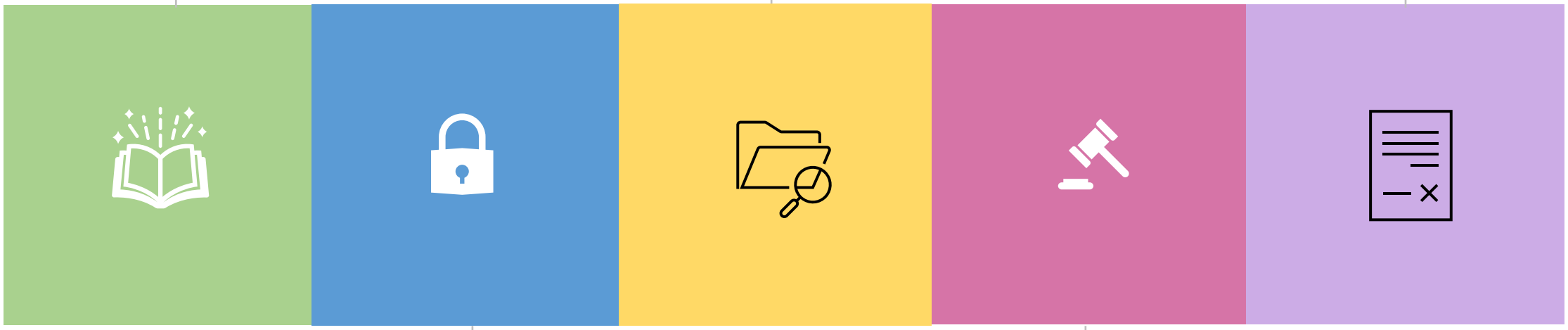
The Personal Data (Privacy) Ordinance (PDPO)

03

Transferring personal data from Hong Kong

05

Cross-boundary flow of personal information within the Greater Bay Area



02

Six Data Protection Principles

04

Cross-border transfer of personal information from the Mainland

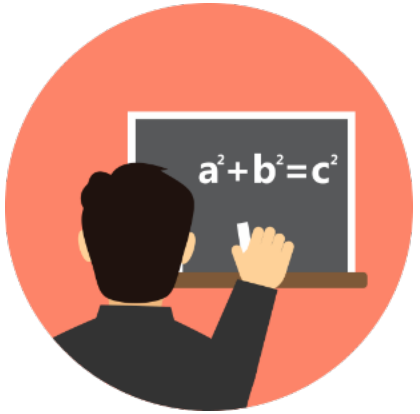
1. The PDPO

Personal Data (Privacy) Ordinance, Cap. 486

- Establishes an independent authority, Privacy Commissioner for Personal Data
- Covers both public (government) and private sectors
- The Data Protection Principles outline how data users should collect, handle and use personal data
- Complemented by other provisions imposing further compliance requirements

Who is the “Data User”?

- A person, who, either alone or jointly or in common with other persons
- Controls the collection, holding, processing or use of the data
- Including government departments, public and private sectors and individuals



Who is the “Data Processor”?

- Processes personal data on behalf of another person
- Does not process the data for any of his own purposes
- Data user is responsible for acts and practices of employees and agents

2. Six Data Protection Principles

Data Protection Principles (DPPs)

- All data users must comply with the six DPPs
- The six DPPs cover every item of personal data in the whole data processing cycle from collection, retention, use to destruction

DPP 1: Purpose & Manner of Collection

- Personal data must be collected in a lawful and fair way, for a lawful purpose directly related to a function/activity of the data user
- Data collected should be necessary but not excessive
- 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

DPP 2 – Accuracy and Duration of Retention

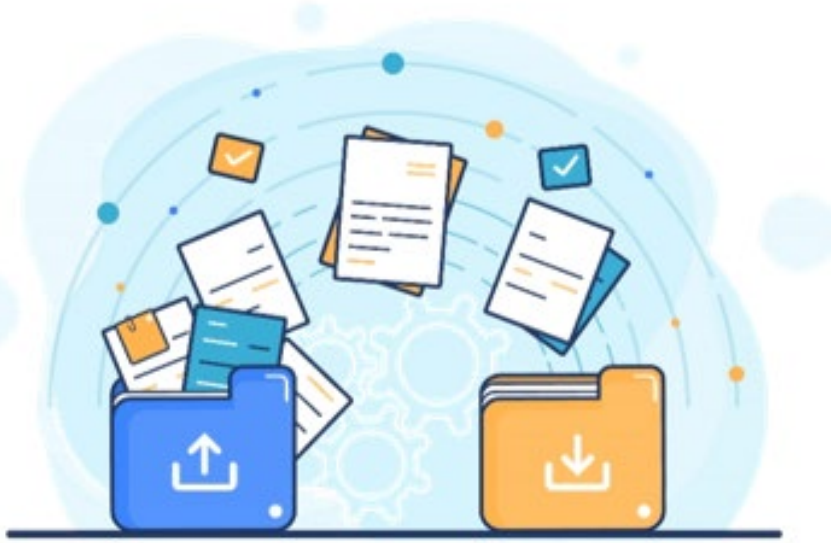
- Data users shall take all practicable steps to ensure the accuracy of personal data held by them

- All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose

- If a data user engages a data processor to process personal data on the data user's behalf, 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 processing of the data

DPP 3: Use of Personal Data

- Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose



New purpose:
any purpose other than the purpose for which they were to be used at the time of collection or directly related purposes

DPP 4: Security of Personal Data

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

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

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 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

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)

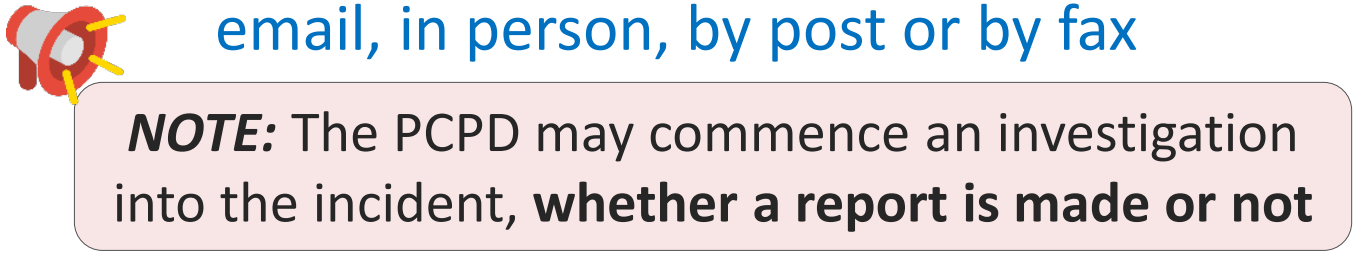
- Description of what makes a data breach
- Internal incident notification procedure
- Contact details of response team members
- Risk assessment workflow
- Containment strategy
- Communication plan
- Investigation procedure
- Record keeping policy
- Post-incident review mechanism
- Training or drill plan

Data Breach Notifications

Give data breach notification to PCPD?

- NOT a statutory requirement
- But a **recommended practice**
- How?
  - Submit the **online** "Data Breach Notification Form" available on PCPD's webpage
  - Submit the paper version of the "Data Breach Notification Form" to PCPD by email, in person, by post or by fax

NOTE: The PCPD may commence an investigation into the incident, **whether a report is made or not**



Data Breach Notification

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

While it is not a statutory requirement on data users to inform the PCPD about a data breach incident concerning the personal data held by them, data users are nevertheless advised to do so as a recommended practice for proper handling of such incident. You may make reference to our "Guidance on Data Breach Handling and Data Breach Notifications" before submitting a data breach notification.

Data Users are encouraged to use the online data breach notification form to notify the PCPD of any data breach incidents. Please click here to access the online data breach notification form.

In addition to the online form, data users can still download the paper version of the data breach notification form for completion. Please click here to download the paper version of the data breach notification form. After completing the form, please submit it and other relevant documents concerning the data breach (if any) which you wish to provide by the following channels: -

- **By Post / In Person**

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

  Opening hours of Reception Counter:
  Monday to Friday: 8:45 a.m. to 12:45 p.m. & 1:50 p.m. to 5:40 p.m.

- **By Fax**
  Fax number: 2877 7026

- **By Email**
  Email address: dbn@pcpd.org.hk

The PCPD does not accept oral notification.

PCPD H K

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

數據安全專題網頁
Data Security Webpage

DPP 5: Information to be Generally Available

Transparency

Data users have to provide:

(a) policies and practices in relation to personal data;

(b) the kind of personal data held;

(c) the main purposes for which personal data are used

DPP 6: Data Access & Correction

A data subject shall be entitled to：

i. request access to his/her personal data; data users may charge a fee for complying with the data access request

ii. request correction of his/her personal data

If the data user holds the relevant personal data, it should supply a copy of the requested data within 40 calendar days after receiving the data access request

AAB 37/2009:

- Fee: "**directly related to and necessary**" for complying with a DAR
- ≠ "reasonable"
- **Flat-rate fees**: acceptable so long as it is **lower** than direct and necessary costs
- Evidential burden on data user to show the fee charged is non-excessive

3. Transferring personal data from Hong Kong

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

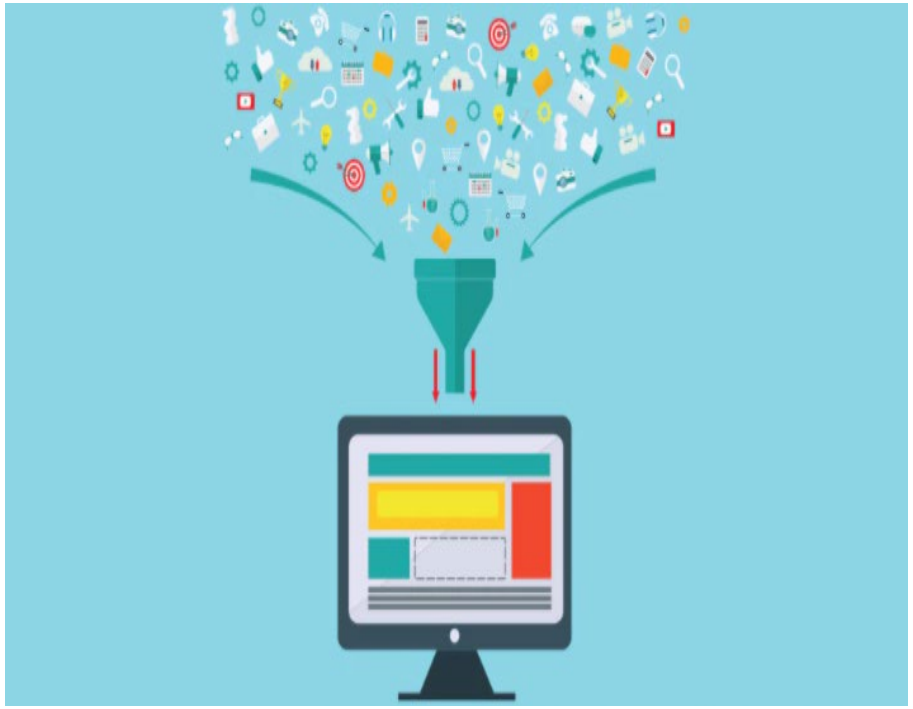
DPP1 (Purpose and Manner of Collection of Personal Data)

- 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))

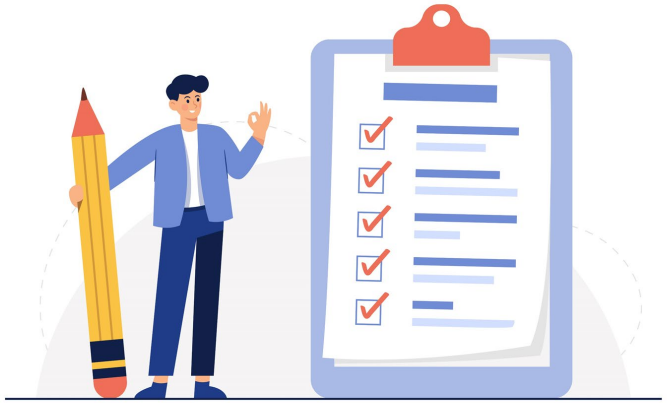
4. Cross-border transfer of personal information from the Mainland

Personal Information Protection Law: Cross-border Transfer of Personal Information

Personal Information Protection Law ("PIPL") – Article 38

1) Passing the **security assessment** organized by the national cyberspace department in accordance with Article 40 of the PIPL;
2) obtaining **personal information protection certification** from the relevant specialized institution according to the provisions issued by the national cyberspace department;
3) concluding a contract stipulating both parties' rights and obligations with the overseas recipient in accordance with the **standard contract** formulated by the national cyberspace department;
4) meeting other conditions set forth by laws and administrative regulations and by the national cyberspace department

Personal Information Protection Law: Cross-border Transfer of Personal Information



Other Necessary Conditions set out in the PIPL

- Notification (Article 39)
- Separate consent (Article 39)
- Personal information protection impact assessment (Article 55(4))
- Ensuring that the personal information processing activities of the overseas recipient meet the personal information protection standards set forth in the PIPL (Article 38)

5. Cross-boundary flow of personal information within the Greater Bay Area

Aligning with the Relevant Laws and Regulations of the Mainland

- The Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong) ("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

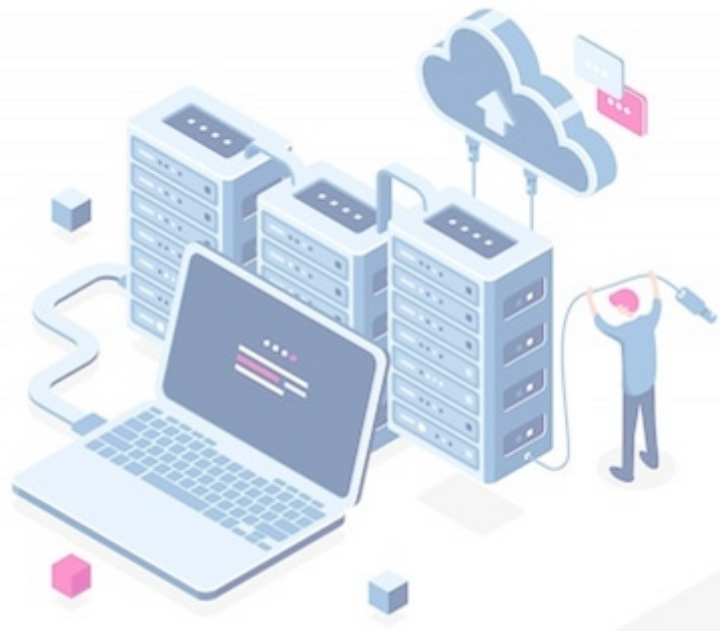
- The personal information processor shall conduct a personal information protection impact assessment on the intended transfer
- The parties shall adhere to the filing procedures of the GBA SC
- Restrictions of further transfer of personal information out of the GBA are imposed upon the recipient

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

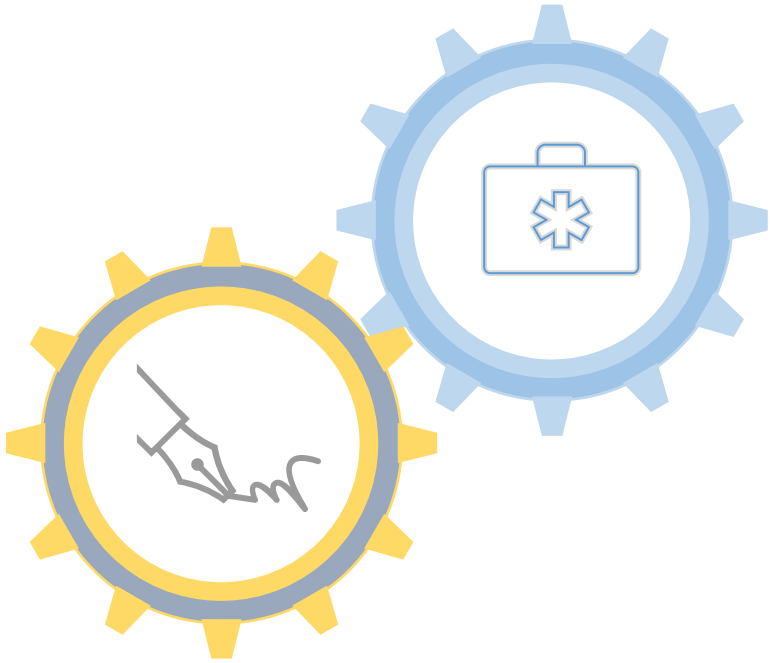


(2) Inform the personal information subjects (including data subjects) of the requisite information, such as name and contact information of the recipient, purposes and means of processing, etc.

(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



(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 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

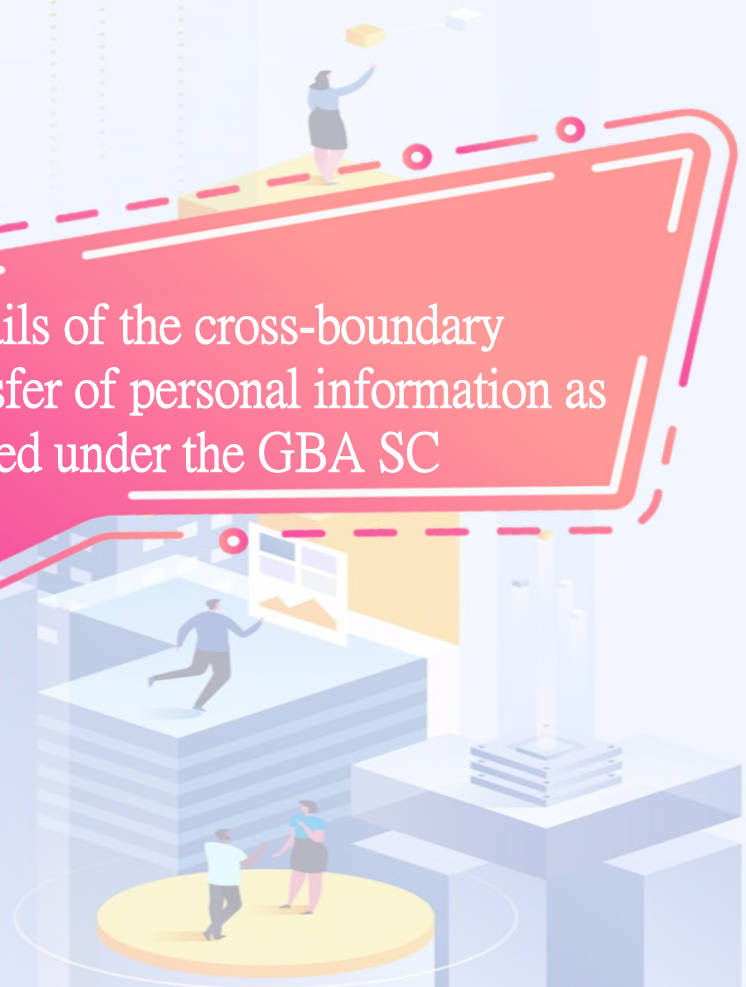
Article 3

(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)

Guidance Note

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

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

Digital Policy Office's web page on **Facilitating Cross-boundary Data Flow within the Greater Bay Area**: https://www.digitalpolicy.gov.hk/en/our_work/digital_infrastructure/mainland/cross-boundary_data_flow/

“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

首页 | 时政要闻 | 网信政务 | 互动服务 | 热点专题

当前位置： 首页 > 正文

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。

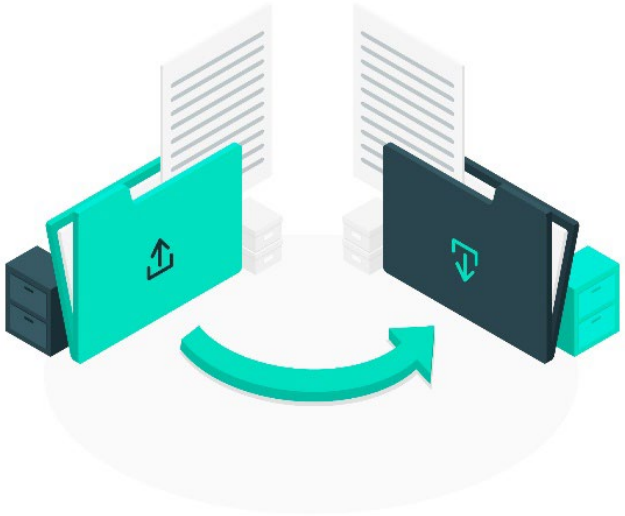
第三条 国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

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 3	where the data to be transferred out of the Mainland is collected and generated from **international trade, cross-border transportation, academic collaboration, cross-border manufacturing activities, and marketing or sales activities**, which does not contain any personal information or important data
Article 4	where the personal information **collected and originated by a data processor outside Mainland is transferred to the Mainland for domestic processing before being provided abroad**, the process of which does not involve any personal information or important data within the Mainland



"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**

“Regulations on Facilitating and Regulating Cross-Border Data Flow”

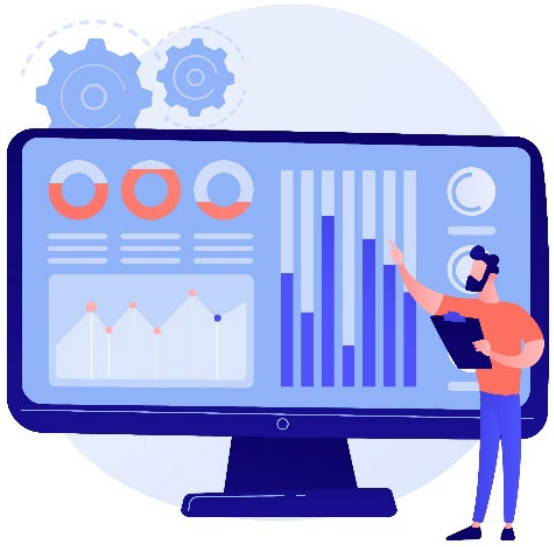
Security assessments shall be filed with the CAC through provincial cyberspace authorities where one of the following requirements is met:

Article 7	**Critical information infrastructure operators (“CIIOs”)** are to transfer personal information or important data outside Mainland
	Non-CIIOs are to transfer **important data**, or personal information of **over 1,000,000 individuals (not containing any sensitive personal information)**, or **sensitive personal information of over 10,000 individuals** since 1 January of the current year outside Mainland

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

Data processors that are not CIIOs are required to enter into standard contracts or obtain personal information protection certifications under the following circumstances:

Article 8	When personal information of the following threshold (to be counted from 1 January of the current year) is to be transferred out of the Mainland: • **personal information of over 100,000 individuals but less than 1,000,000 individuals** (not containing any sensitive personal information); or • **sensitive personal information of less than 10,000 individuals**



Follow us to receive PCPD's latest updates!

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

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