

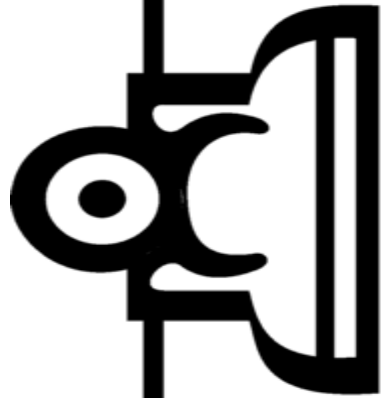
EMBA Forum 2017-18
The Chinese University of Hong Kong
20 November 2017

Privacy and Business Development

保障・尊重個人資料
Protect, Respect Personal Data

Stephen Kai-yi Wong, Barrister
Privacy Commissioner for Personal Data, Hong Kong

Presentation Outline



- **Overview of Hong Kong's Personal Data (Privacy) Ordinance**
- **Privacy and Ethical Implications of New Technologies**
- **EU General Data Protection Regulations and Its Impact in Hong Kong**
- **The Belt and Road Initiative**

An Overview of The Personal Data (Privacy) Ordinance





Legislative Intent

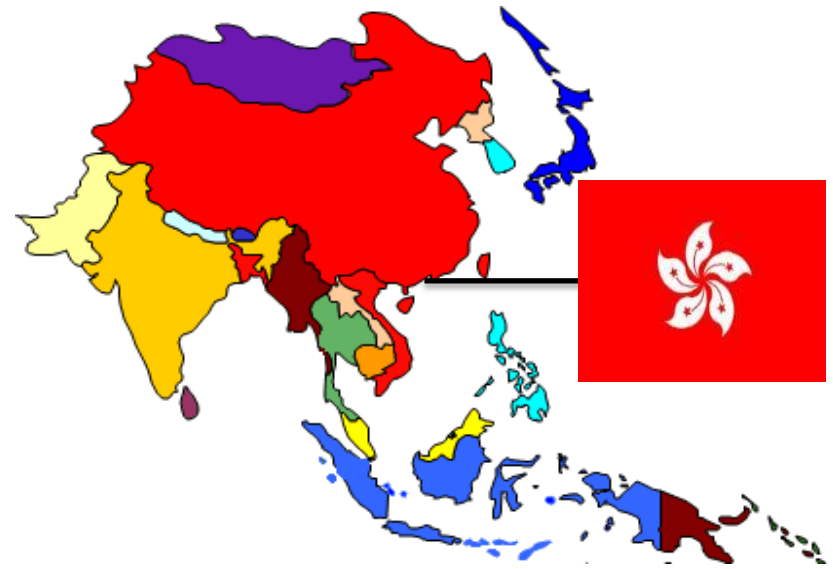


- **Business Perspective** – To facilitate business environment, maintain Hong Kong as a financial and trading hub
- **Human Rights Perspective** – Protect individuals' personal data privacy



Personal Data (Privacy) Ordinance

- enacted in **1995**
- **1st** comprehensive data protection law **in Asia**
- covers the **public** (government) and **private sectors**
- referenced to 1980 OECD Privacy Guidelines and **1995 EC Data Protection Directive**



What is “Personal Data”?



“**Personal data**” (個人資料) means any **data** -

- (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.

“**Data**” (資料) means any representation of information (including an expression of opinion) **in any document**.

Examples of Personal Data in Everyday Life

- a person's name, mobile phone number, address, sex, age, occupation, salary, nationality, photo, identity card number, medical records, etc.



The 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，而不超乎需要。

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



資料使用者須確保其個人資料準確無誤，資料的保留時間不應超過達成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.



Six Data Protection Principles (DPPs)

- **Core spirits** of the Ordinance
- Cover **the whole data lifecycle** from collection, retention, use, security to destruction

Six Data Protection Principles (DPPs)

DPP1 – Collection

- ✓ Not excessive
- ✓ Lawful and fair
- ✓ Sufficient notice



DPP2 – Accuracy & Retention

- ✓ Ensure accuracy before use
- ✓ Destroy when purpose of collection is accomplished



DPP3 – Use

- ✓ Do not use data for new purposes without data subjects' consent





Six Data Protection Principles (DPPs)

DPP4 – Security



- ✓ All practicable steps shall be taken to prevent data breach

DPP5 – Openness & Transparency



- ✓ Policy and practice should be made readily available to data subjects

DPP6 – Data Access & Correction



- ✓ Allow data subjects to access and correct their personal data

Direct Marketing



New Direct Marketing Regime

- **2012 Ordinance review exercise**
- **new direct marketing regime came into force on 1 April 2013**
- **direct marketing activities under the Ordinance include such activities made to specific persons by mail, fax, email and phone**



Direct Marketing Requirements

Intends to use or provide personal data to others for direct marketing



Provides personal data

<p>Provide “prescribed information” and response channel for data subjects to elect whether to give consent</p> <p>Notification must be easily understandable</p>	<p>Consent should be given explicitly and voluntarily</p> <p>“Consent” includes an indication of “no objection”</p>
---	---

Direct Marketing Requirements

- **data user must comply with the data subject's opt-out request without charge [section 35G]**
- **criminal sanctions** if data user fails to comply with requirements of notification, consent and opt-out requests





Direct Marketing Conviction Cases

Date	Case	Penalty
Sept 2015 (1 st conviction after the 2012 amendment)	<ul style="list-style-type: none">• A telecommunication company ignored customer's opt-out requests.• The company appealed against its conviction at the High Court, and the appeal was dismissed in Jan 2017.	Fined \$30,000
Sept 2015	<ul style="list-style-type: none">• A storage service provider failed to take specified actions and obtain the data subject's consent before direct marketing.	Fined \$10,000
Nov 2015	<ul style="list-style-type: none">• A healthcare services company ignored customer's opt-out requests.	Fined \$10,000



Direct Marketing Conviction Cases

Date	Case	Penalty
Dec 2015	<ul style="list-style-type: none">An individual provided personal data to a third party for direct marketing without taking specified actions and obtaining the data subject's consent.The individual appealed against the conviction at the High Court, and the appeal was dismissed in June 2017.	Fined \$5,000
Apr 2016	<ul style="list-style-type: none">An insurance agent used personal data in direct marketing without taking specified actions and obtaining the data subject's consent.The agent also failed to inform the data subject of his opt-out right when using his personal data in direct marketing for the first time.	Community Service Order of 80 hours for each charge
May 2016	<ul style="list-style-type: none">A telemarketing company used a customer's personal data in direct marketing without taking specified actions and obtaining his consent.The company also ignored opt-out requests.	Fined \$8,000 for each charge

17



Direct Marketing Conviction Cases

Date	Case	Penalty
Nov 2016	<ul style="list-style-type: none">Two financial intermediaries used personal data in direct marketing without taking specified actions and obtaining data subject's consent, total 11 charges, and all convicted.Two senior management of the companies were also charged, but were acquitted due to lack of evidence.	Two companies fined \$165,000 in total (\$15,000 per charge), plus damages to claimants for 25% of profits (\$47,800).
Dec 2016	<ul style="list-style-type: none">A watch company used an individual's personal data in direct marketing without taking specified actions and obtaining his consent.The company also failed to inform the individual of his opt-out right when using his personal data in direct marketing for the first time.	Fined \$8,000 for each charge
Jan 2017	<ul style="list-style-type: none">A bank failed to comply with client's opt-out request.	Fined \$10,000

Direct Marketing 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 Note

New Guidance on Direct Marketing

PART 1: Introduction

Purpose of guidance

1.1 Direct marketing is a common business practice in Hong Kong. It often involves collection and use of personal data by an organization for direct marketing itself and in some cases, the provision of such data by the organization to another person for use in direct marketing. In the process, compliance with the requirements under the Personal Data (Privacy) Ordinance (the "**Ordinance**") is essential. This document is issued by the Privacy Commissioner

takes effect, the Commissioner's "Guidance on the Collection and Use of Personal Data in Direct Marketing" remains fully valid.

What is "direct marketing"?

- 1.3 The Ordinance does not regulate all types of direct marketing activities. It defines "**direct marketing**" as:
- (a) the offering, or advertising of the availability, of goods, facilities or services;
 - or

Privacy and Ethical Implications of New Technologies



Big Data

- Massive scale of collection, processing, combination and aggregation of unstructured data
- “3 Vs” : Volume, Velocity & Variety



Fintech

- Application of technologies in financial services:
 - crowdfunding
 - e-wallet
 - P2P lending
 - robo-adviser
 - credit scoring



AI

- Machine learning – algorithms which can learn and evolve without the need for human intervention
- Thrive with big data analytics – discover patterns and correlations to make predictions and decisions



Regtech

- Application of technologies in regulatory compliance and monitoring:
 - Detect irregular transactions
 - Anti-money laundering



Privacy and Ethical Implications

- Covert data collection
- Unexpected data use
- Re-identification
- Profiling, unfairness & discrimination
- Unpredictability
- Transparency
- Data security



Privacy-based Solutions



Accountability

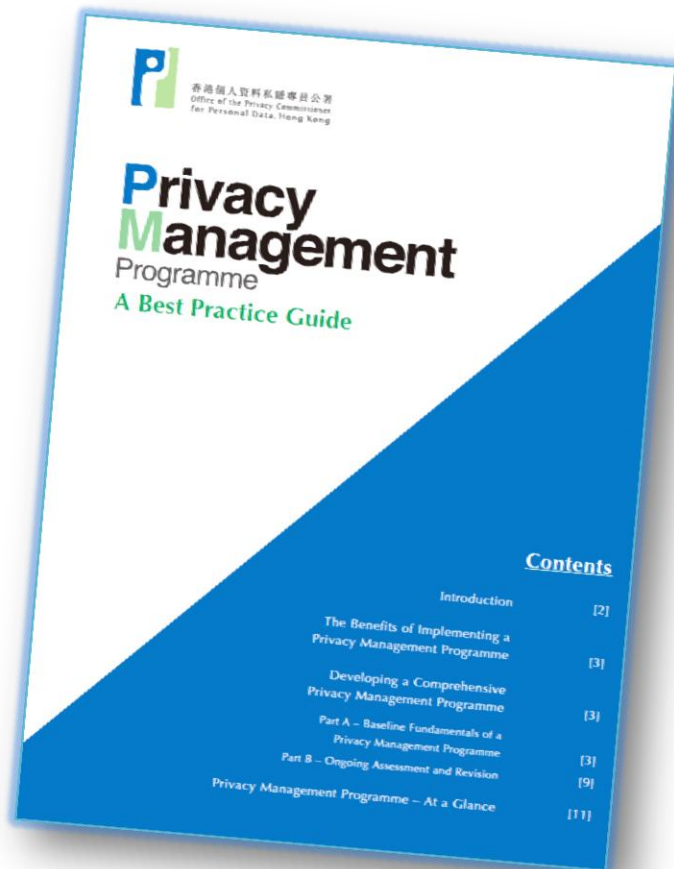


- **“Protect, Respect Personal Data”**
- top management cultivates respect for privacy within organisations
- adopt measures to protect data
- **Privacy Management Programme (PMP)**
- **“Privacy by Design” & “Privacy by Default”**

From Compliance, to Accountability... to



Main Objectives of PMP



- embrace personal data privacy protection as part of the **corporate governance responsibilities**; and
- apply it as a **top-down** business imperative throughout the organisation

https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf

From Compliance to Accountability

Paradigm Shift



Compliance approach

- passive
- reactive
- remedial
- problem-based
- handled by compliance team
- minimum legal requirement
- bottom-up

Accountability Approach

- Active
- Proactive
- Preventative
- Based on customer expectation
- Directed by top management
- Reputation building
- Top-down

Transparency



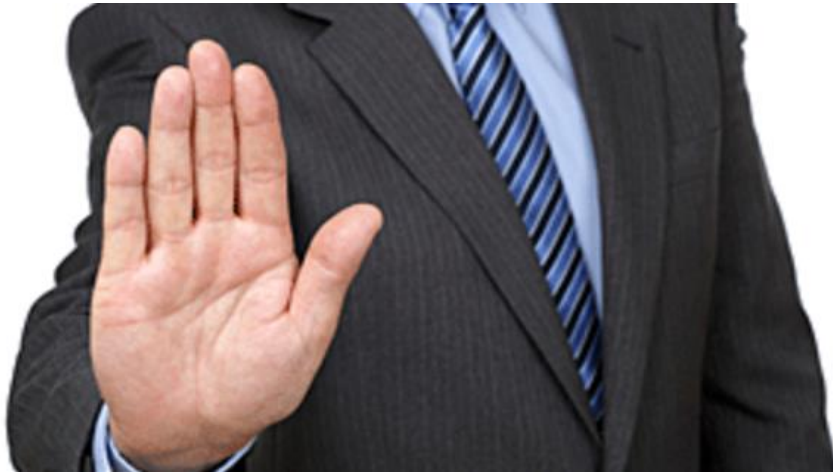
- **Two “Ts” – Transparency and Trust**
- **transparency builds up trust**

Transparency



- explain **what data** is collected and **purposes** of use
- explain **logic** and **rationale** behind decision

Meaningful Choices



Meaningful Choices and Control

- allow individuals to **object** to profiling
- allow individuals to **object** to decisions which may significantly affect them



and Its Impact on Hong Kong

EU General Data Protection Regulation (GDPR)

- Enacted in May 2016
- To be effective on **25 May 2018**
- Will replace **1995 EU Data Protection Directive (95/46/EC)**
- Harmonise data protection laws across Europe





PDPO – GDPR Comparative Study

PCPD identified the following 9 major differences between PDPO and GDPR:

9 Major Differences	
1. Extra-Territorial Application	6. Data Processor Obligations
2. Accountability and Governance	7. New or Enhanced Rights of Data Subjects/Profiling
3. Mandatory Breach Notification	8. Certification/Seals and Personal Data Transferred Outside Jurisdictions
4. Sensitive Personal Data	9. Sanctions
5. Consent	

1. Extra-Territorial Application

EU GDPR

Data processors or controllers:

- with an establishment in the EU, or
- **established outside the EU**, that offer goods or services to individuals in the EU, or monitor the behaviour of individuals in the EU. [Art 3]

HK PDPO

Data users who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the personal data **in or from Hong Kong**. [S.2(1)]



2. Accountability and Governance



EU GDPR

Risk-based approach to accountability.

Data controllers are required to:

- implement technical and organisational measures to ensure compliance [Art 24];
- adopt **data protection by design and by default** [Art 25];
- conduct **data protection impact assessment** for high-risk processing [Art 35]; and
- (for certain types of organisations) **designate Data Protection Officers** [Art 37].

HK PDPO

The accountability principle and the related privacy management tools are not explicitly stated.

The Privacy Commissioner advocates the **Privacy Management Programme** which manifests the accountability principle. The appointment of data protection officers and the conduct of privacy impact assessment are recommended good practices for achieving accountability.

3. Mandatory Breach Notification



EU GDPR

- Data controllers are required to **notify the authority** about a data breach without undue delay (**exceptions** apply).
- Data controllers are required to **notify affected data subjects unless exempted**.
[Arts 33-34]

HK PDPO

- No mandatory requirement.
Voluntary breach notification.

4. Sensitive Personal Data

EU GDPR

- Expand the category of sensitive personal data.
- Processing of sensitive personal data is allowed only under specific circumstances. [Art 9]

HK PDPO

- No distinction between sensitive and non-sensitive personal data.



5. Consent

EU GDPR

- One of the 6 lawful bases for processing
- Consent must be
 - ✓ **freely given, specific and informed**; and
 - ✓ **an unambiguous indication of a data subject's wishes, by statement or by clear affirmative action, which signifies agreement to the processing of his personal data.** [Art 4(1)]

HK PDPO

Consent is not a pre-requisite for the collection of personal data, unless the personal data is used for a new purpose. [DPPs 1&3]



6. Data Processor Obligations

EU GDPR

- Data processors are imposed with additional obligations, such as: **maintaining records of processing, ensuring security of processing, reporting data breaches, designating Data Protection Officers, etc.**
[Arts 30, 32-33, 37]

HK PDPO

- Data processors are **not directly regulated.**
- Data users are required to **adopt contractual or other means to ensure data processors comply with data retention and security requirements.** [DPPs 2&4]



39

7. New or Enhanced Rights of Data Subjects / Profiling

EU GDPR

- Right to **erasure of personal data** (also known as “right to be forgotten”) [Art 17]
- Right to **data portability** [Art 20]
- **Right to object to processing** (including profiling) [Art 21]
- **“Profiling”** is defined as any form of automated processing involving personal data to evaluate certain personal aspects of a natural person [Art 4(4)]
- Expanded notice requirement for the new or enhanced rights

HK PDPO

- No general right to erasure, but shall not retain personal data for longer than necessary [S.26 & DPP 2(2)]
- No right to data portability
- No general right to object to processing (including profiling), but may **opt out from direct marketing activities** [Ss.35G &35L] and contains provisions regulating data matching procedure [Ss. 30-31]

8. Certification / Seals and Personal Data Transferred Outside Jurisdictions

EU GDPR

- Explicitly recognises privacy seals and establishes **certification mechanism** for demonstrating compliance by data controllers and processors. [Art 42]
- Certification as **one of the legal bases for cross-border data transfer.**

HK PDPO

- No such certification or privacy seals mechanism for demonstrating compliance.



9. Sanctions



EU GDPR

- Data protection authorities can impose **administrative fines** on data controllers and processors. [Art 58]
- Depending on the nature of the breach, the fine could be up to **€20million** or **4%** of the total worldwide annual turnover. [Art 83]

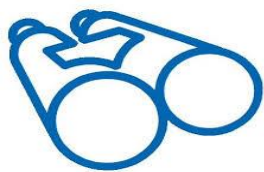
HK PDPO

- The Privacy Commissioner is not empowered to impose administrative fines or penalties.
- The Privacy Commissioner may serve **enforcement notices** on data users.



PDPO – GDPR Comparative Study





Observations – Notice & Consent

- **Balance** with genuine needs for processing data
- Over reliance on consent may **impede** business activities
- PDPO is principle-based and **technology neutral**
- Suggest stick to DPP1 & DPP3:
 - **DPP1** – notice; lawful purpose directly related to a function or activity
 - **DPP3** – use for new purpose not allowed without prescribed consent



Observations – Accountability

- **Suggest formalising accountability principle (including mandatory DPO regime) under PDPO because it can:**
 - give effect to principle-based PDPO by promoting responsible use of data by data users
 - facilitate compliance
 - allow for more flexibility to tackle the challenges brought by ICT, AI, Big Data, etc.
- **To mitigate adverse effect on businesses, risk-based approach to accountability can be considered**
- **PCPD is open-minded as to formalising PIA as it is already a part of PMP**



Observations – Sanctions

- Allow PCPD to impose administrative fines would **deter non-compliance** and bring PDPO in line with overseas data protection laws (e.g. Singapore, UK)
- **Some regulators in Hong Kong are also vested with power** to order pecuniary penalty, e.g. Monetary Authority, Securities and Futures Commission
- **Appropriate check & balance mechanism** may allay concerns of over-concentration of powers:
 - i. stipulating criteria for imposing fines
 - ii. prescribing fine limit
 - iii. allowing appeal channel against fine imposed



Observations – Extra-Territorial Application

- Given rapid ICT developments, data collection and processing nowadays is borderless. **Currently, PCPD will resort to cross-border enforcement where appropriate**
- Adopting extra-territoriality to PDPO requires consideration of **complicated legal issues**, practicality of enforcement and consistency with international comity
- PCPD has reservation on making same change to PDPO
- It is **still an open question to be clarified by legal precedent** as to whether PDPO has extra-territorial effect

Way Forward

- **Publication of Guidance**
- **Trainings for data users**
- **Information exchange and experience sharing on issues and challenges relating to compliance with GDPR**
- **Strengthen international cooperation**





The Belt and Road Initiative

BELT AND ROAD INITIATIVE 「一帶一路」倡議



Source: HKTDC

Hong Kong's Unique Advantages

“**Hong Kong**...has many **unique advantages**...for instance, free and open economy, efficient business environment, advanced professional services sector, well-established infrastructure and facilities, internationally recognised legal system, **free flow of information** and large supply of quality professionals...”

*Mr Zhang Dejiang,
Member of the Standing Committee of
the Political Bureau of the Communist Party
of China Central Committee;
Chairman of the Standing Committee of the
National People's Congress of the People's
Republic of China
Keynote Speech,
Belt and Road Summit, 18 May 2016*



51

Hong Kong's Unique Advantages

“With the combined advantages of ‘one country’ and ‘two systems,’ **Hong Kong** can serve as a ‘**super-connector**’ (超級聯繫人) between the Mainland of China and the rest of the world. In areas such as finance, investment, professional services, trade, logistics, culture, creativity, innovation and technology, Hong Kong’s unique ‘super connector’ role can bring together the strengths of Belt and Road economies.”

*The Hon C Y Leung, GBM, GBS, JP
Former Chief Executive, Hong Kong SAR
Opening Remarks
Belt and Road Summit, 18 May 2016*



52

Hong Kong – Asia's Leading Data Hub

- **2016 Cloud Readiness Index Overall Ranking # 1:**
 - International Connectivity #1
 - **Data Centre Safety #1**
 - Privacy #1
 - Broadband Quality #2
 - Power Grid, Green Policy & Sustainability #2



53

Support of Hong Kong Government

Hong Kong Government fully supports developing Hong Kong into Asia's Leading Data Hub:

“Data centres are an essential infrastructure to support pillar sectors like financial services, trading and logistics as well as other economic sectors. Data centres also provide the catalyst for the development of new content and applications, as well as cloud computing services... the Government fully supports the development of data centres in Hong Kong as the backbone to our economic growth...”

Source : Hong Kong Office of the Government Chief Information Officer

Hong Kong Government Policy

- Set up a **Data Centre Facilitation Unit** and a thematic information portal, to provide coordinated services to interested developers and investors on matters related to setting up of data centres in Hong Kong
- Step up **promotion** to position Hong Kong as a **prime location for data centres** in the Asia Pacific region;
- Promote the incentive measures that **optimise the use of industrial buildings** for the benefit of developing data centres; and
- **Identify sites** for development of **high-tier data centres** and appropriate land disposal arrangements.

Source : Hong Kong Office of the Government Chief Information Officer

55

Hong Kong – Reputable Legal System

- The **Rule of Law**
- **Common Law** Jurisdiction
- Strong Commercial and Property Law
- **Independence of the Judiciary**
- Arbitration and Mediation



Hong Kong – Leading Business Centre

- International Trade
- Intellectual Property
- International Arbitration
- **Professional Knowledge**
- Diverse Cultures
- **International Vision**



Hong Kong's comprehensive data protection regime

- **Personal Data (Privacy) Ordinance:** A comprehensive data protection law in line with international standards
- **Office of the Privacy Commissioner for Personal Data:** independent, fair and reliable enforcement agency trusted by local citizens and overseas enforcement agencies



Contact Us



Copyright



This PowerPoint is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this PowerPoint, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.

- Hotline 2827 2827
- Fax 2877 7026
- Website www.pcpd.org.hk
- E-mail enquiry@pcpd.org.hk
- Address 12/F, Sunlight Tower,
248 Queen's Road East,
Wanchai, HK

спасибо
 danke 謝謝
 ngiyabonga
 teşekkür ederim
 tapadh leat
 dank je
 gracias
 mochchakkeram
 bedankt
 hvala
 maururu
 thank you
 go raibh maith agat
 dziekuje
 unjofes
 sukriya
 kop khun krap
 arigato
 takk
 dakujem
 merci
 merси
 obrigado
 sagolun
 sukriya
 terima kasih
 감사합니다
 ευχαριστώ
 grazie