The Summit on the Greater Bay Area
Data Interconnection and Secure Development

Regulatory Framework for Personal Data Protection Practices and Cross-border/boundary Data Flow in Hong Kong

05 January 2020 | Hengqing, Zhuhai

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

1

Constitutional protection to privacy in Hong Kong

Hong Kong Bill of Rights Ordinance, Cap 383

Enacted in 1991

Mirror-imaging the provisions of the International Covenant on Civil and Political Rights

Protection against arbitrary or unlawful interference with privacy, family, home or correspondence [Art. 14] (A mirror image of Art. 17 of the ICCPR)

International Covenant on Civil and Political Rights

The Basic Law – Examples of Privacy Rights Protection

Provisions of the International Covenant on Civil and Political Rights, etc. remain in force [Art. 39]

Guarantee freedom and privacy of communication [Art. 30]

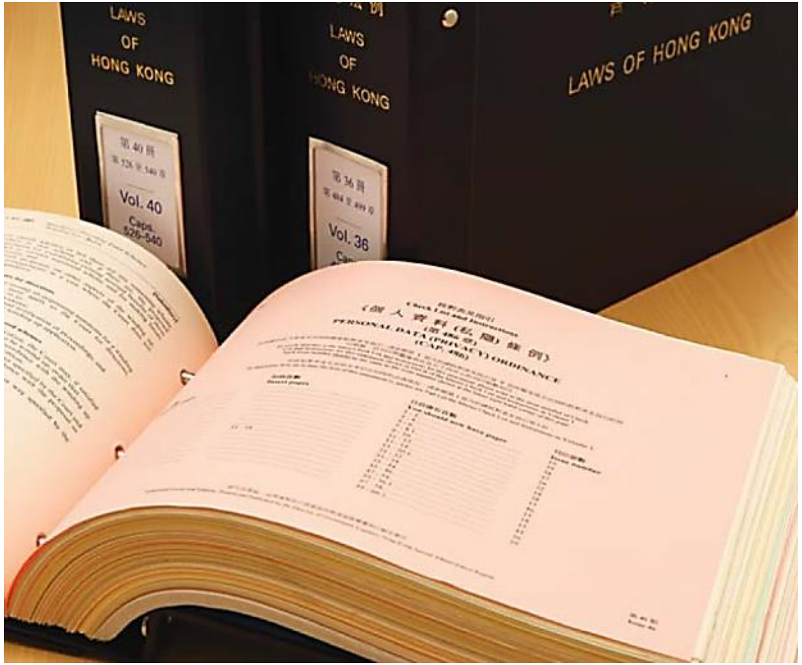
Prohibit arbitrary or unlawful search of, or intrusion into, a resident's home or other premises [Art. 29]

2

Data Protection Regime in Hong Kong

Personal Data (Privacy) Ordinance
Cap 486, Laws of Hong Kong

- Enacted in **1995**
- Protects individuals' privacy in relation **to personal data**
- Created **independent** Privacy Commissioner for Personal Data
- Covers the **public** (including the government) and **private sectors**
- Referenced to **1980 OECD Privacy Guidelines** and **1995 EU Data Protection Directive**



Legislative Background

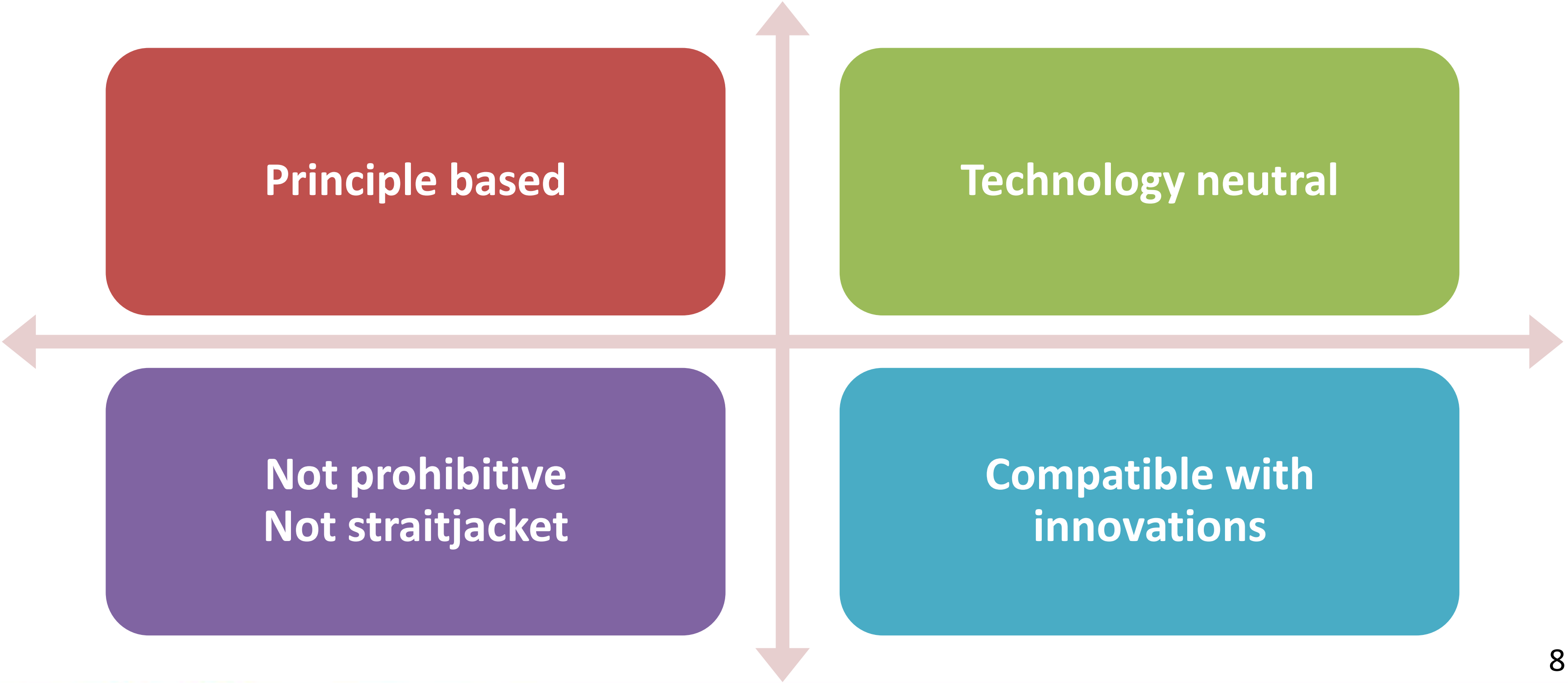
Business Perspective

- Facilitate business environment
- Maintain Hong Kong as a financial and trading hub

Human Rights Perspective

- Protect individuals' personal data privacy

Characteristics of the Ordinance



Principle based

Technology neutral

Not prohibitive
Not straitjacket

Compatible with innovations

Role of the PCPD

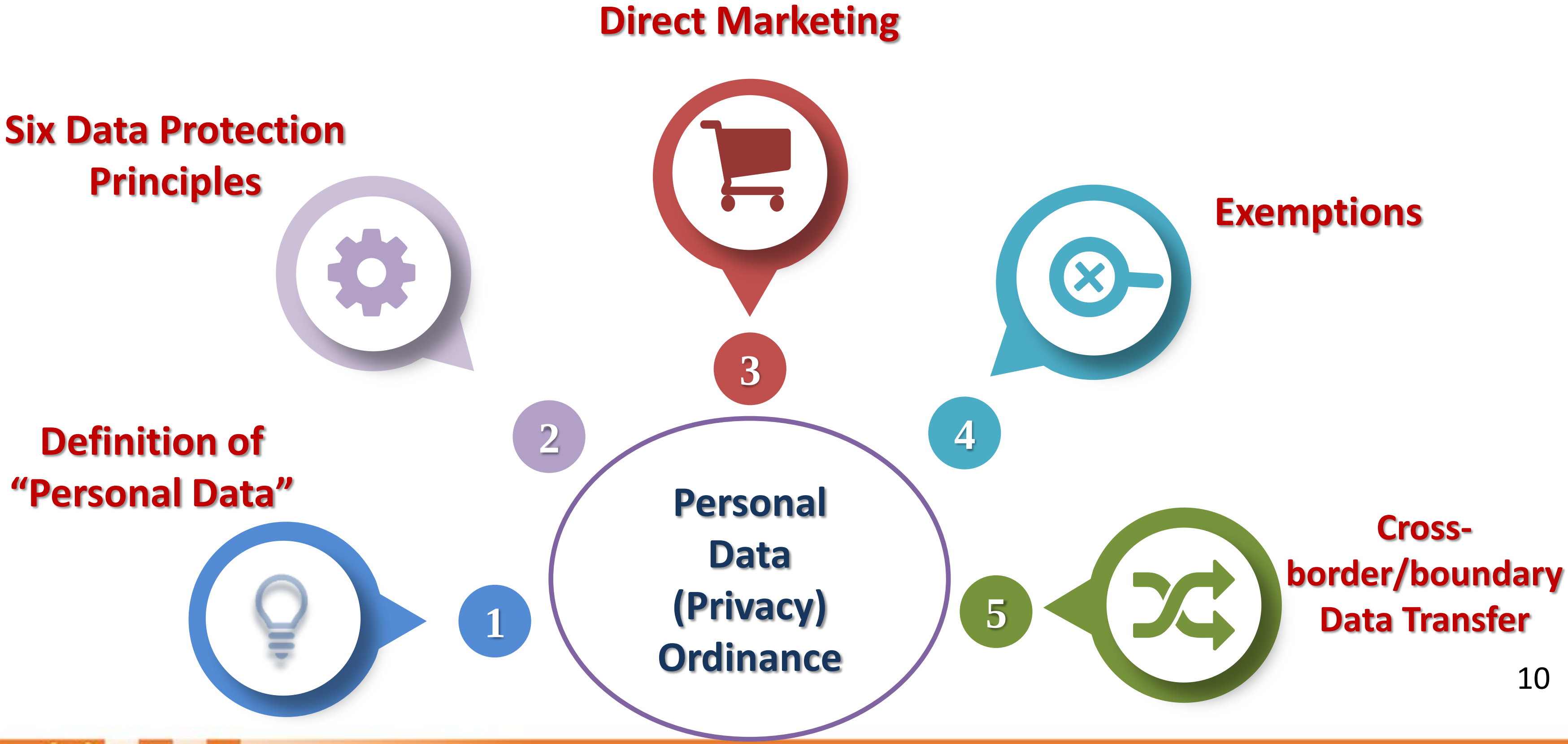
An independent regulatory body

Headed by the Privacy Commissioner (appointed by the Chief Executive of HKSAR)

Performs the functions and exercises the power conferred by the Ordinance, e.g. :

- Education
- Enforcement
- Research
- Advice on legislation
- International liaison

Key Provisions of the Ordinance



Direct Marketing

Six Data Protection Principles

Exemptions

Definition of "Personal Data"

Cross-border/boundary Data Transfer

Personal Data (Privacy) Ordinance

1. 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.*

2. The Six Data Protection Principles of the Ordinance

DPP1:
Collection Purpose & Means

DPP2:
Accuracy & Retention

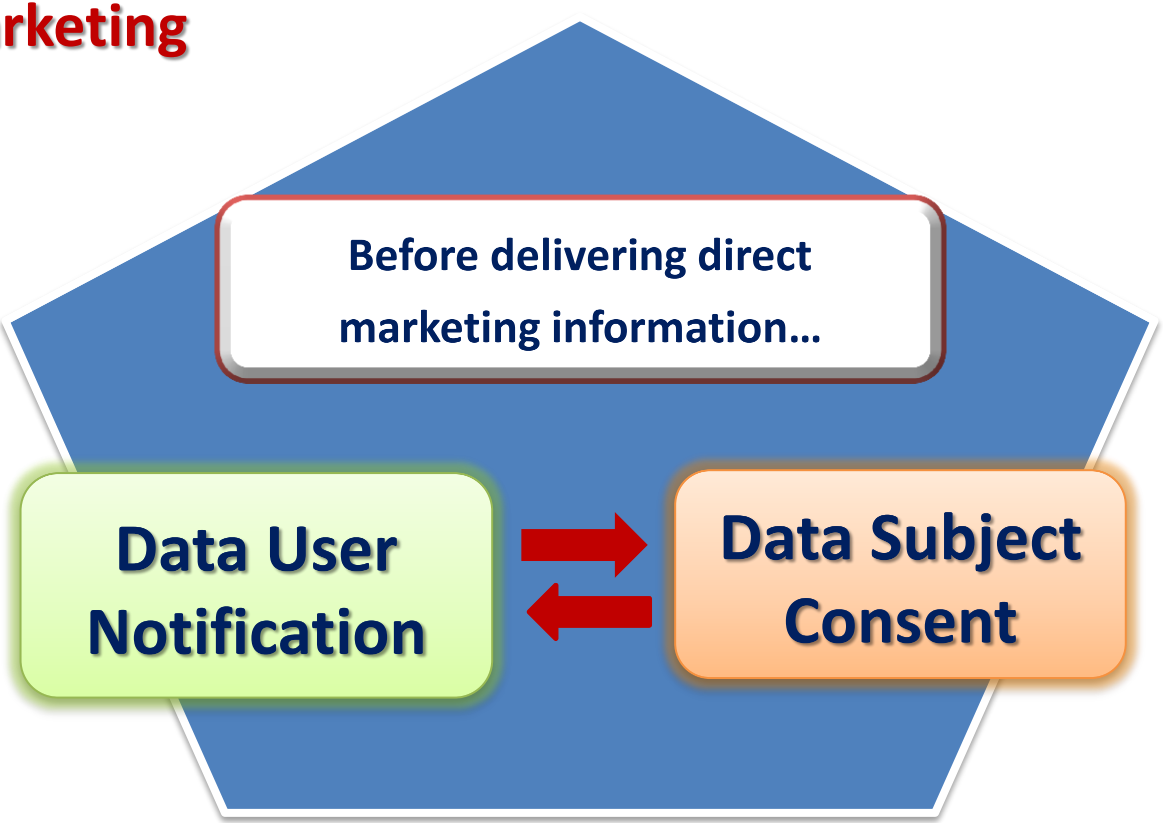
DPP3:
Use

DPP4:
Security

DPP5:
Openness

DPP6:
Data Access & Correction

3. Direct Marketing



Before delivering direct marketing information…

Data User Notification

Data Subject Consent

4. Exemptions under PDPO – Examples (Conditions apply)

Activity	Exempted provision
Domestic Purposes (s.52)	All DPPs
Security of Hong Kong (s.57)	DPP 3, DPP 6
Crimes prevention / detection (s.58)	DPP 3, DPP 6
Health (s.59)	DPP 3, DPP 6
Legal professional privilege (s.60)	DPP 6
Legal proceedings & legal requirements (s.60B)	DPP 3
News (s.61)	DPP 3, DPP 6
Statistics & research (s.62)	DPP 3
Crimes prevention / detection, news activities & public interest (s.64(4)) (statutory defence)	S.64(1)&(2)

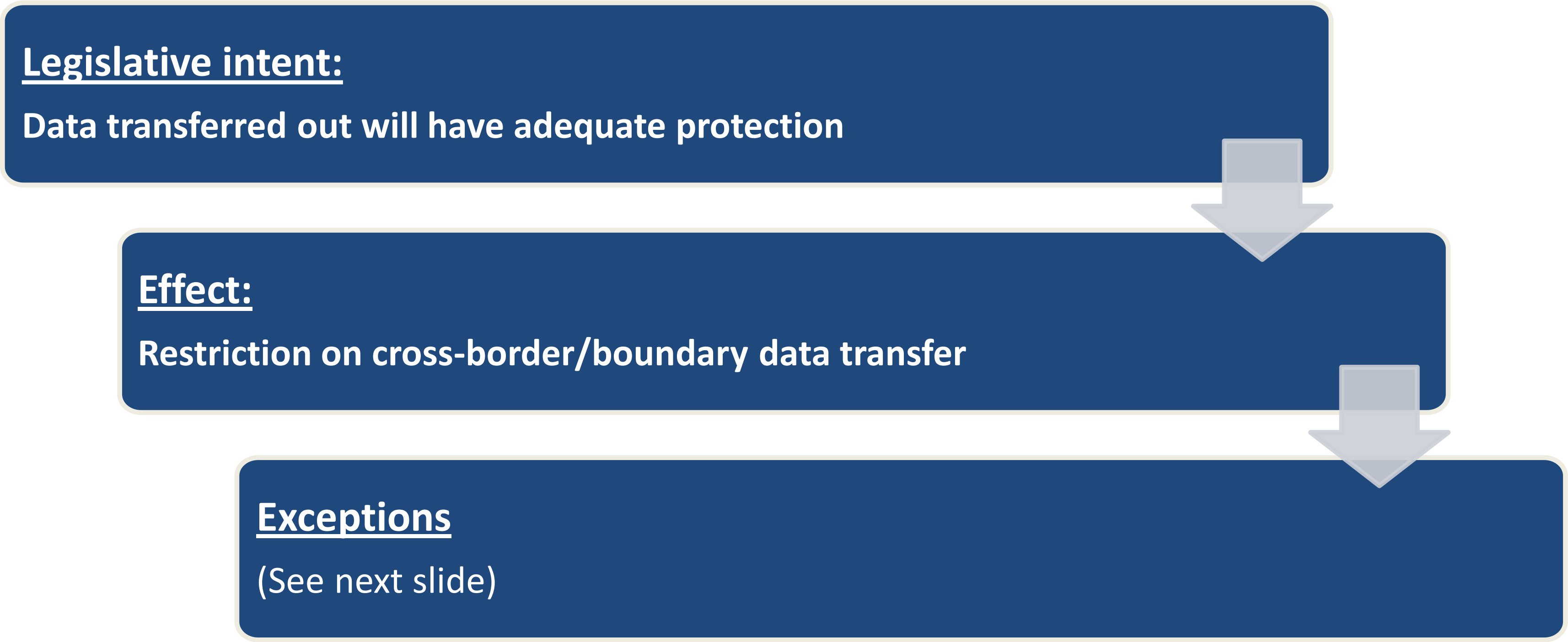
Criminal Offences under PDPO - Examples

Examples of Offence	Max. fine	Max. imprisonment
Direct marketing (Part 6A)	HK$1 million	5 years
Disclosing personal data without data user’s consent for monetary gain or causing psychological harm (s. 64)	HK$1 million	5 years
Non-compliance with enforcement notice (s.50A)	HK$50,000	2 years
Failure to comply with requirements of the Privacy Commissioner (s.50B)	HK$10,000	6 months

3

Current status of cross-border/boundary data transfer in Hong Kong

Cross-border/boundary Data Transfer – PDPO S.33 (Not yet in force)



Legislative intent:

Data transferred out will have adequate protection

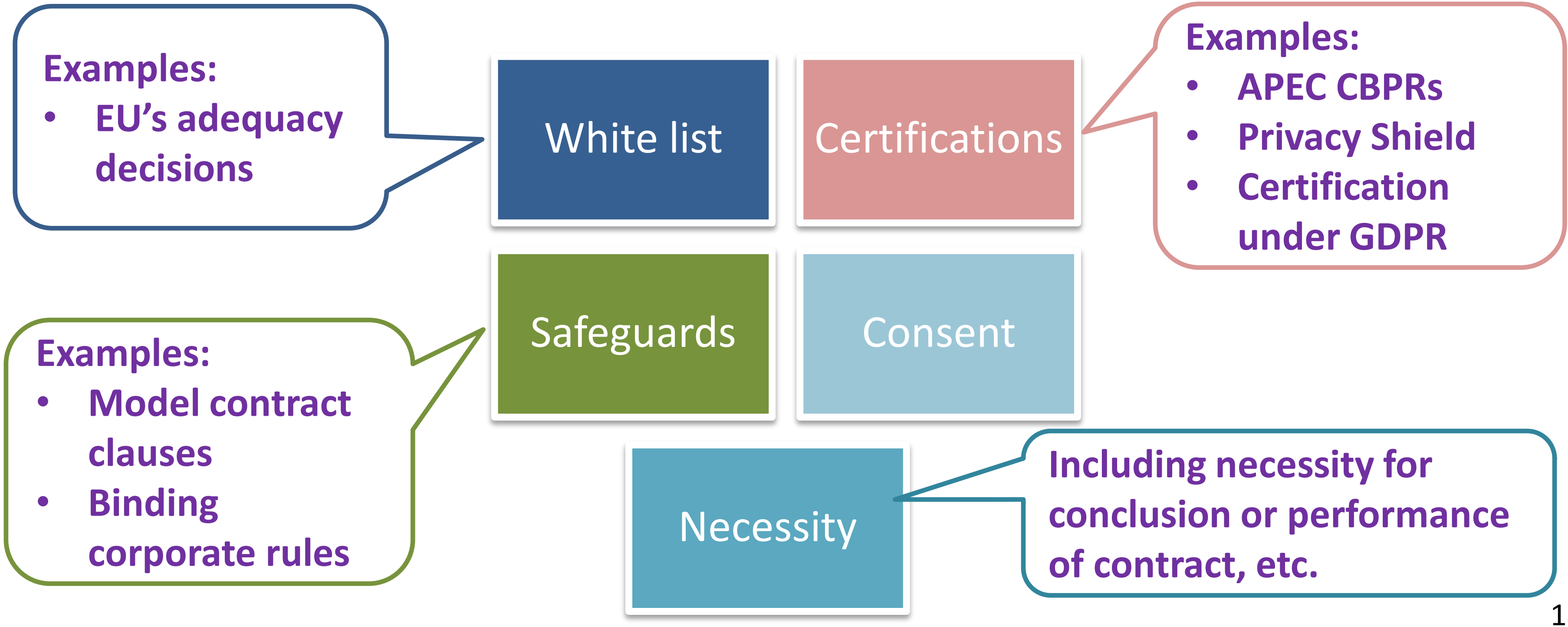
Effect:

Restriction on cross-border/boundary data transfer

Exceptions

(See next slide)

Common models (legal bases) for cross-border / boundary data transfer



White list

Examples:
- EU's adequacy decisions

Certifications

Examples:
- APEC CBPRs
- Privacy Shield
- Certification under GDPR

Safeguards

Examples:
- Model contract clauses
- Binding corporate rules

Consent

Necessity

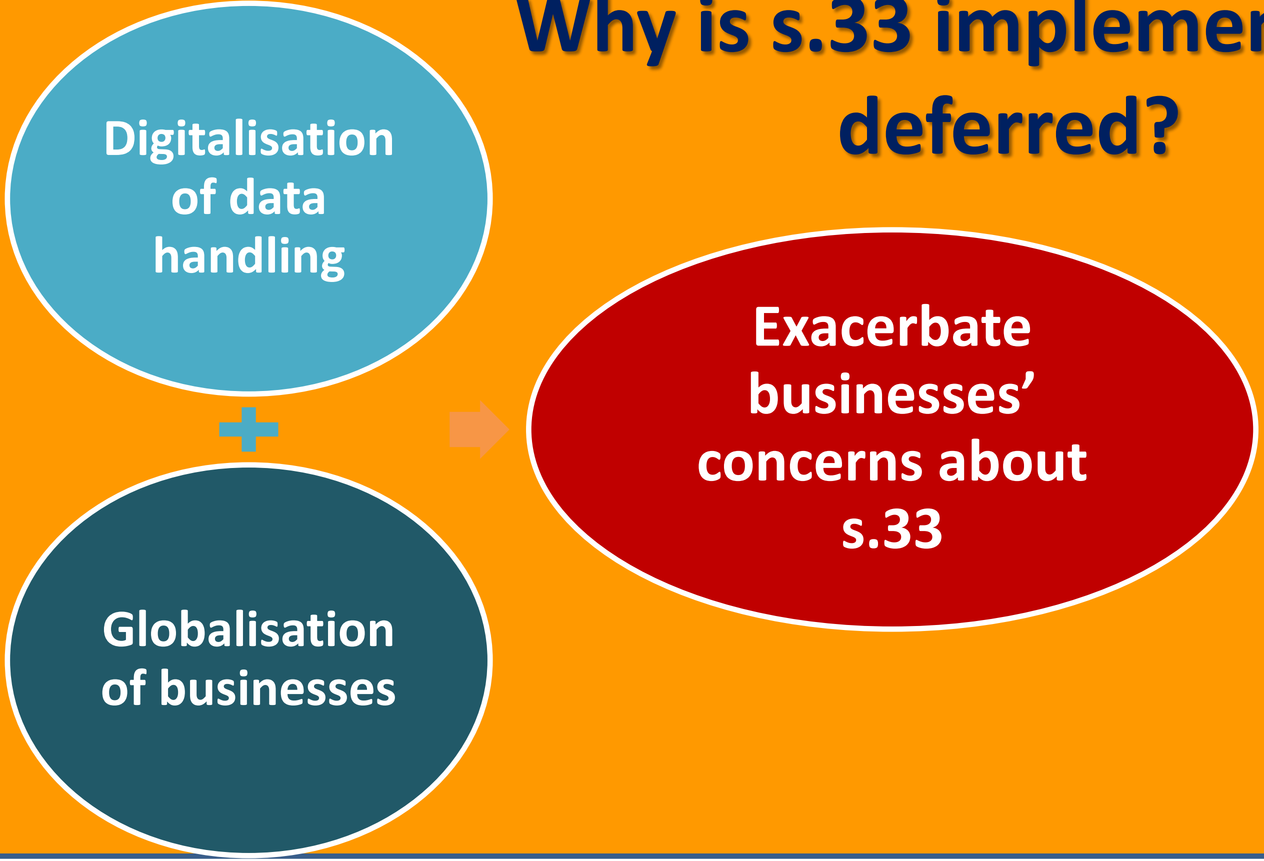
Including necessity for conclusion or performance of contract, etc.

Section 33 of Personal Data Privacy Ordinance (PDPO) [Not yet in force]

- Transfer of personal data outside HK is prohibited except under any one of the following specified circumstances:-

1. Transfer to places specified in "White List" *[s.33(2)(a)]*
2. Adequate data protection regime in the destined jurisdiction *[s.33(2)(b)]*
3. Written consent by data subjects *[s.33(2)(c)]*
4. Transfer for avoidance and mitigation of adverse action against data subjects *[s.33(2)(d)]*
5. Use of personal data is exempted from DPP 3 (use limitation) *[s.33(2)(e)]*
6. Reasonable precautions and due diligence taken by data users (e.g. contract clauses) *[s.33(2)(f)]*

Why is s.33 implementation deferred?



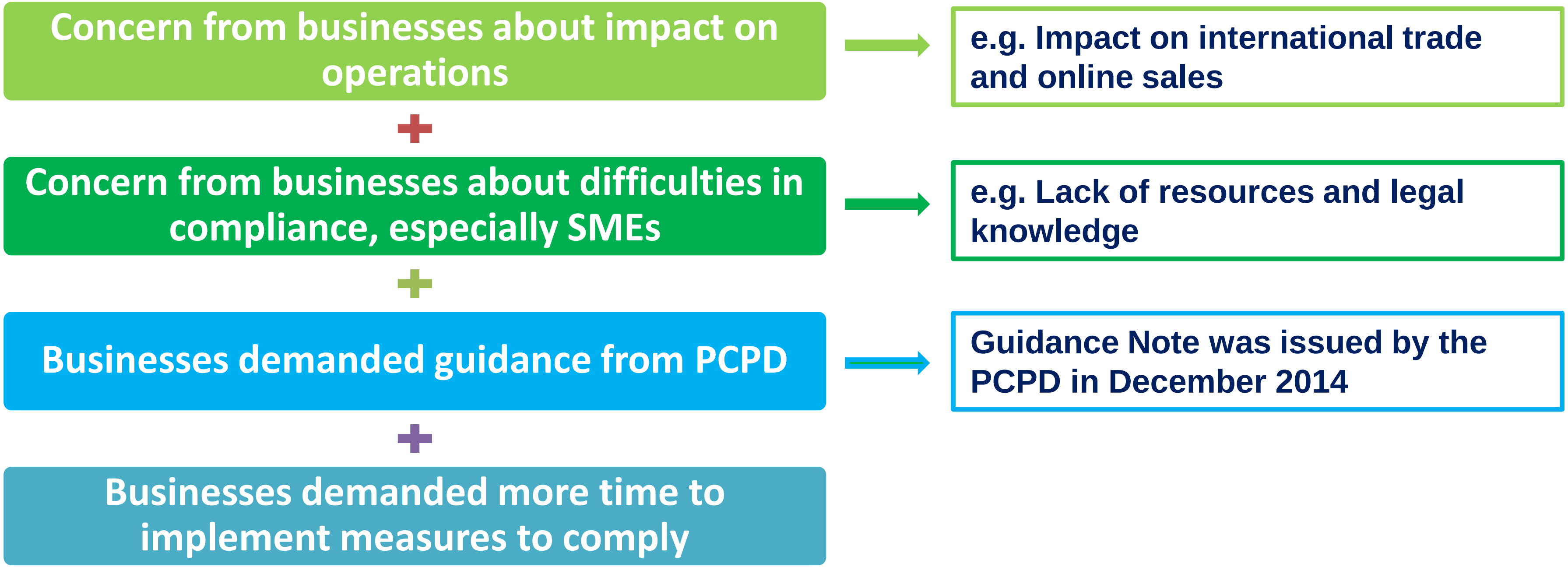
Digitalisation of data handling

+

Globalisation of businesses

Exacerbate businesses' concerns about s.33

Why is s.33 implementation deferred?



Concern from businesses about impact on operations → e.g. Impact on international trade and online sales

+

Concern from businesses about difficulties in compliance, especially SMEs → e.g. Lack of resources and legal knowledge

+

Businesses demanded guidance from PCPD → Guidance Note was issued by the PCPD in December 2014

+

Businesses demanded more time to implement measures to comply

Existing protection under PDPO without s.33 in operation

DPP 3 prohibits transfer of personal data for new purposes without consent

S.65(2) holds data users liable for the acts of their agents, including overseas service providers

DPP 2(3) requires data users to prevent their processors from retaining personal data longer than necessary

DPP 4(2) requires data users to ensure security of personal data transferred to their processors

Existing protection under PDPO without s.33 in operation

Even if s.33 is not in force, for data transferred from other jurisdictions to Hong Kong, parties can impose *contractual restrictions on onward transfer* to places outside Hong Kong.

Recent work by PCPD and HKSAR Government on s.33

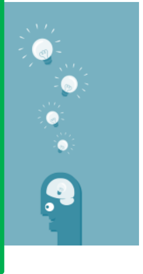
2014 - 2015

To address businesses' demand for guidance, PCPD issued Guidance Note on compliance with requirements of s.33, with a set of model contract clauses recommended

More concerns raised by businesses in response to the Guidance Note

e.g.-

- Unclear about the definition of "personal data" and "transfer"
- Difficult for SMEs to impose contract clauses to services providers?
- What if a "White Listed" region is subsequently delisted?
- Lack of resources to monitor service providers abroad
- Lack of information about the location of cloud servers



Recent work by PCPD and HKSAR Government on s.33

2015-2016

Government commissioned a consultant to conduct a Business Impact Assessment (BIA) Study on implementation of s.33

PCPD rendered comments to the consultant on the interpretation, application and compliance issues of s.33

Recent work by PCPD and HKSAR Government on s.33

2018

Seven issues of concerns raised by Government's consultant in the BIA Study which require further studies

PCPD engaged a consultant to explore how restriction on cross-border data transfer may be implemented in light of these seven issues of concerns

The seven issues of concerns

1. How "transfer" under s.33 and "personal data" are to be defined

2. The mechanism for reviewing and updating the "white list" under s.33

3. Whether the adoption of existing rules and standards in highly regulated industries (e.g., financial industry) would allow a data user to be regarded as having met the requirements of s.33

The seven issues of concerns

4. The ancillary measures or alternatives to facilitate the implementation of s.33

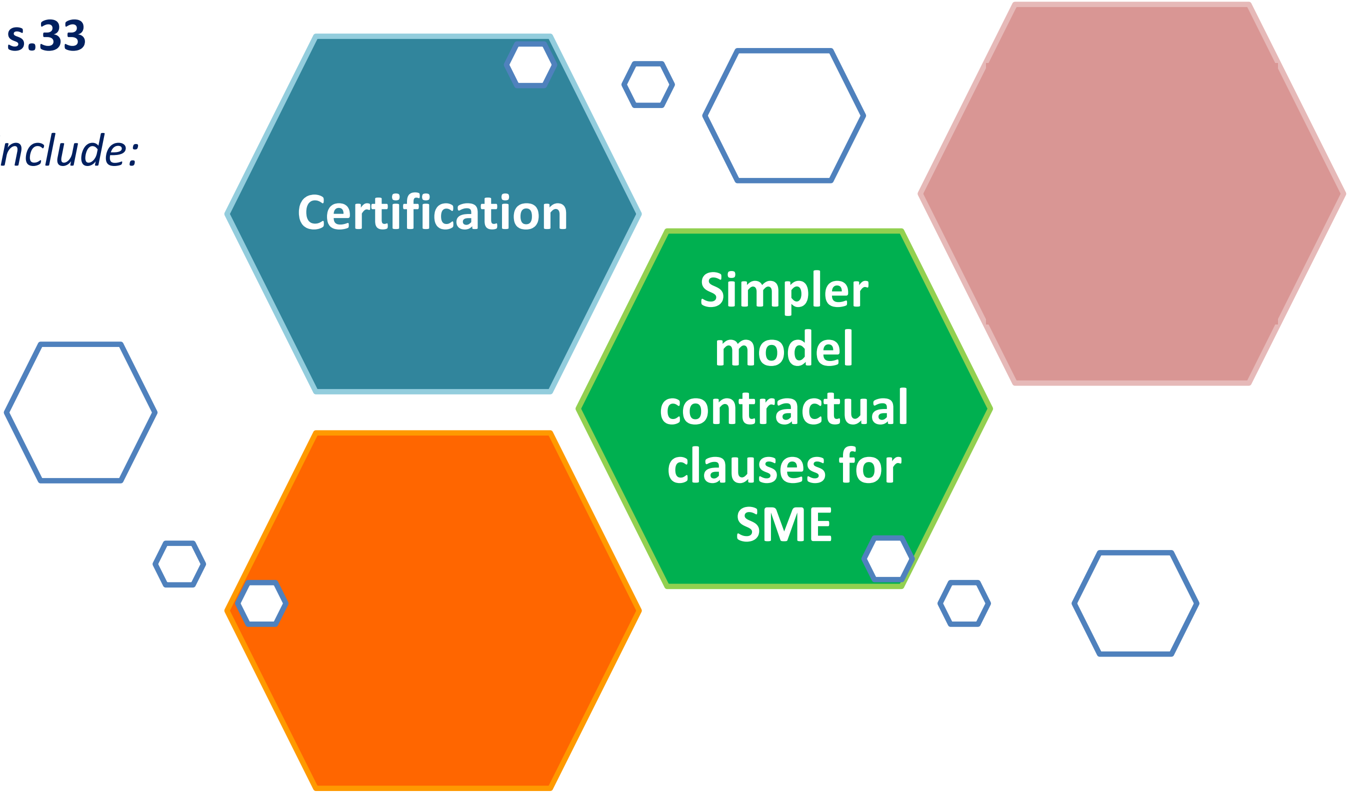
5. Enforcement issues of s.33 and means to tackle them

6. The criteria or yardsticks for deciding whether a data user has "*taken all reasonable precautions and exercised all due diligence*" under s.33

7. Suggestions on the forms of support or guidance from the PCPD to help businesses understand and comply with the requirements of s.33

PCPD will formulate measures to facilitate implementation of s.33

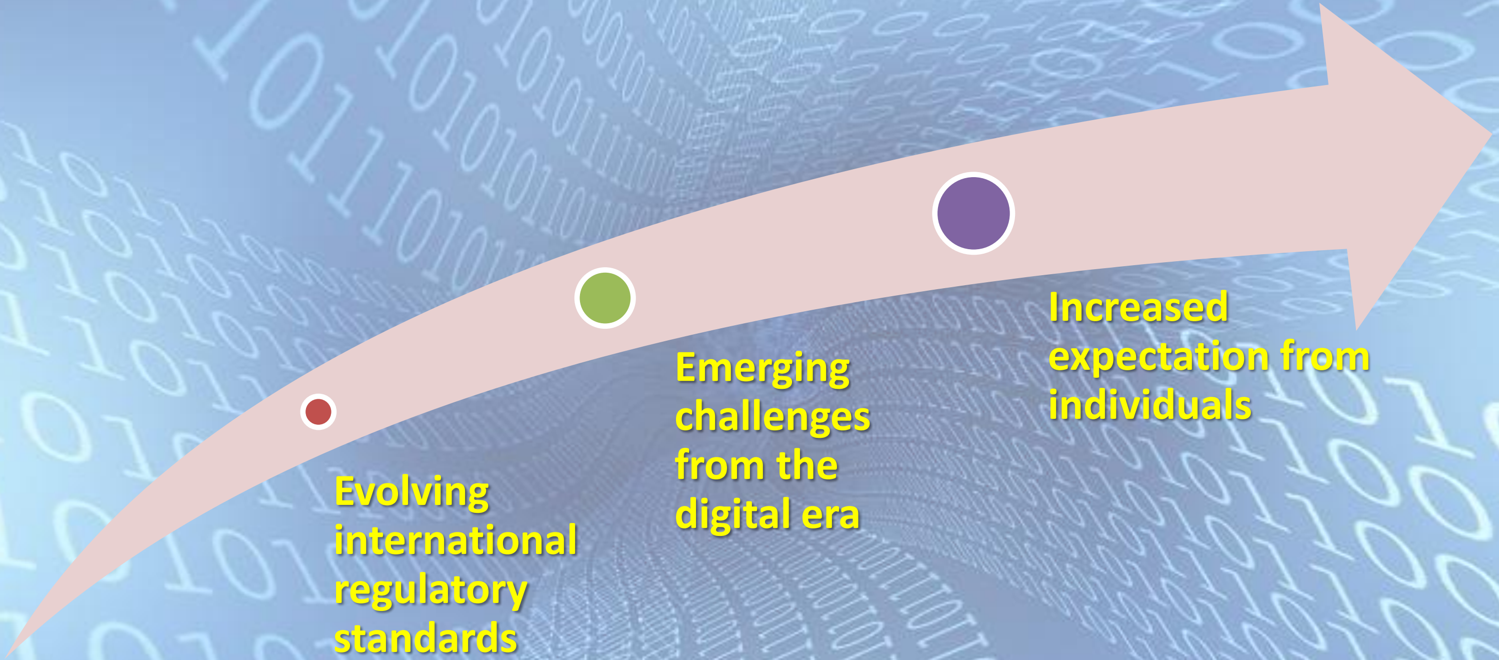
Possible measures include:



4

Paradigm shift in personal data protection practice and possible reforms of the PDPO

Why do we need changes?



Evolving international regulatory standards

Emerging challenges from the digital era

Increased expectation from individuals

From Compliance

To Accountability

To Data Ethics

私隱管理系統
Privacy Management Programme

No legal requirement

Information Accountability Foundation

Ethical Accountability Framework for Hong Kong, China

A Report prepared for the Office of the Priva
Commissioner for Personal Data

Analysis and Model Assessment Framewor

Spirit

Institutionalise organisational and technical measures to ensure and demonstrate compliance

Rationale

Organisations are in the best position to identify, assess and address the privacy risks of their activities

Objectives

- Privacy by design and by default
- Good data governance and stewardship from cradle to grave

Possible amendments to PDPO :

(1) Expand the definition of ‘personal data’ under PDPO:

Personal data may include:

- Information practicable to ***ascertain an identity*** (direct/indirect); and
- Information ***relating to an identifiable*** person

Definitions of "personal data"

PDPO	Overseas (e.g. AU, CA, EU)
Criteria: - Practicable to ascertain identity	Criteria: - Relating to or about an identifiable individual
Meaning: - Knowing who a person is	Meaning: - Able to single out a person, not necessarily knowing who the person is
Result: - Narrower scope of personal data and less protection to privacy	Result: - Wider scope of personal data and stronger protection to privacy

Possible amendments to PDPO (cont.)

(2) Additional regulation on the retention of personal data

- Disclose personal data **retention policy**
- Stipulation of **maximum retention period**

Possible amendments to PDPO (cont.)

(3) Regulate data processors directly

Data processors' obligations on:

- **retention period** of personal data
- **security** of personal data
- **notification to data users** of data breaches without undue delay
- Data processors with a Hong Kong link or a presence in Hong Kong will be covered

Possible amendments to PDPO (cont.)

(4) Mandatory Breach Notification

- Notify both the **PCPD** and the **impacted individuals**
- High threshold for breach notification – e.g. “***real risk of significant harm***” to individuals
- Set **time limit** – e.g. 5 days for notifying PCPD; ‘as soon as practicable’ for notifying individuals
- Allow for investigation period for ‘suspected breach’ before notification

Possible amendments to PDPO (cont.)

(5) PCPD’s Powers

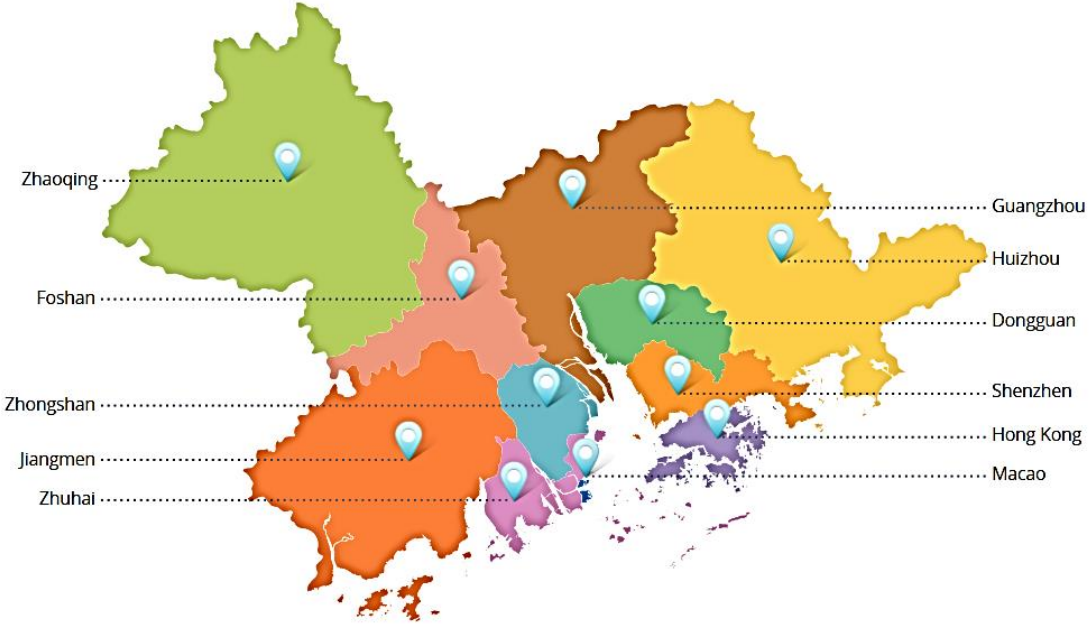
Confer additional powers on the PCPD to:

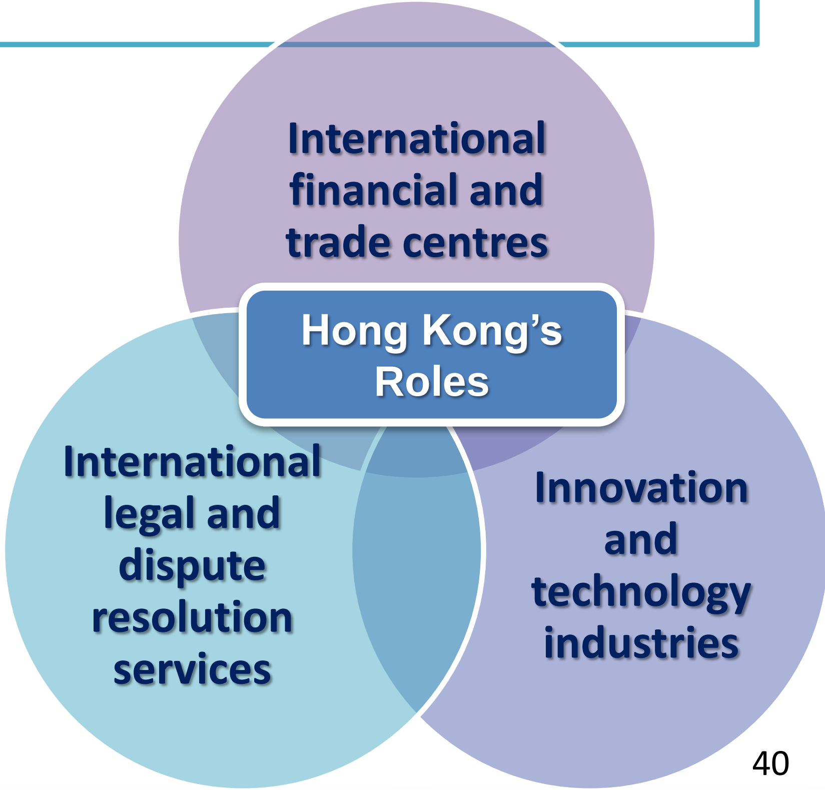
- Conduct **criminal investigations/prosecutions**
- Impose **administrative fines**
- Make **prohibitive orders by way of interim enforcement notices binding on any relevant parties**

5

Data in the Greater Bay Area: Unique and irreplaceable attributes of Hong Kong

Outline Development Plan for the Guangdong-Hong Kong-Macao Greater Bay Area 《粵港澳大灣區發展規劃綱要》





Hong Kong's Roles

International financial and trade centres

International legal and dispute resolution services

Innovation and technology industries

Data & GBA

Outline Development Plan for the Guangdong-Hong Kong-Macao Greater Bay Area 《粤港澳大灣區發展規劃綱要》

Data-related, regional collaborations

Facilitate cross-boundary and regional flow of people, goods, capital and information

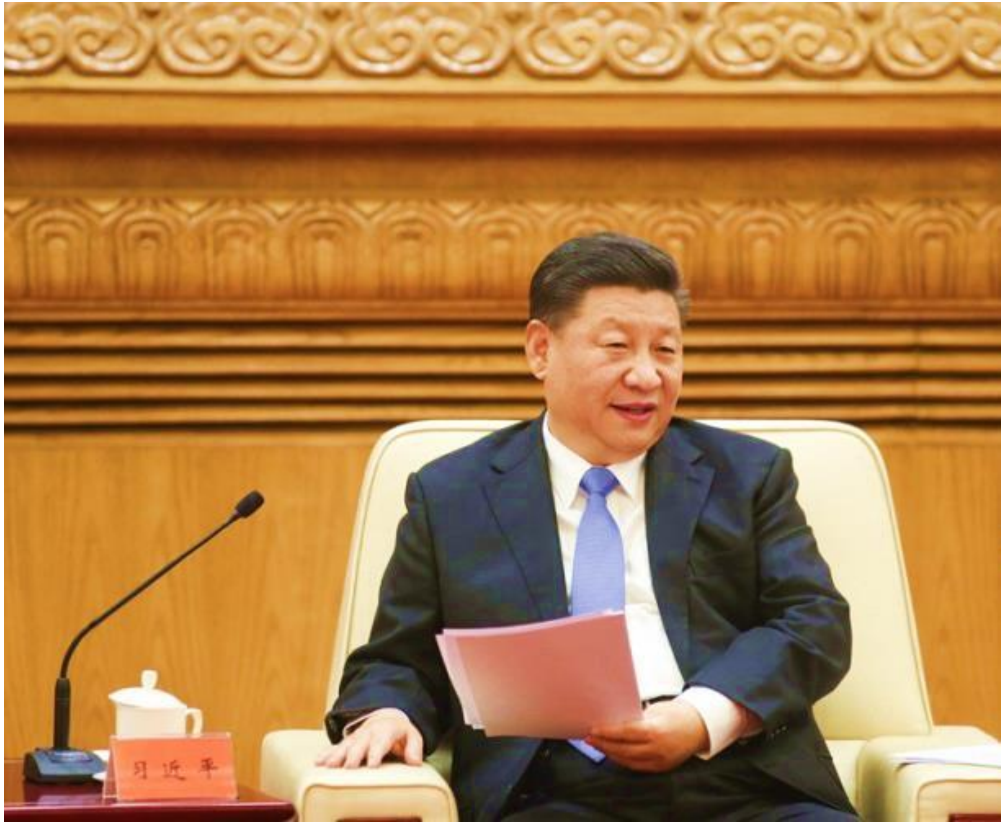
Jointly develop a Greater Bay Area big data centre

Formulate plan to enhance management on cross-boundary use of medical data and bio-samples

Explore the establishment of common standards, open up data ports, develop interconnected public application platforms

> “*Hong Kong…has many unique attributes…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,
Chairman of the Standing Committee of the National People’s Congress
of the PRC, Keynote Speech, Belt and Road Summit,
18 May 2016



> ***"In the country's reform and opening in the new era, Hong Kong and Macao still possess special, unique and irreplaceable attributes."***

Xi Jinping, President of China

Speech at the meeting with Hong Kong delegation
in the Celebration of the 40th Anniversary
of the Reform and Opening Up of the Country
12 November 2018

Think tank: Hong Kong can become a global data hub for the Greater Bay Area

Global businesses that rely on big data are in need of a "neutral" hub to help bridge divergences in the digital systems of China… Hong Kong is an obvious location.

[Hong Kong] already has in place stringent data privacy laws and legal protections that mainland and international firms can trust.

Victor Fung, Chairman of The 2022 Foundation

Source: The Standard (29 March 2019)
http://www.thestandard.com.hk/breaking-news.php?id=125179&sid=4

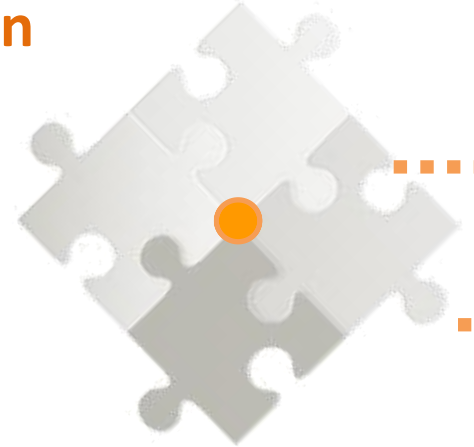
> *"Hong Kong has unique functions in the Greater Bay Area. … Support Hong Kong to become an international innovation centre. … Hong Kong should apply its advantage in professional services in the development of the Greater Bay Area."*
>
> **Han Zheng**
>
> Vice Premier of the State Council; March 2019

第十三届全国人民代表大会第二次会议
香港特别行政区代表团全体会议
新华网
WWW.NEWS.CN

Source: xinhuanet.com; March 2019

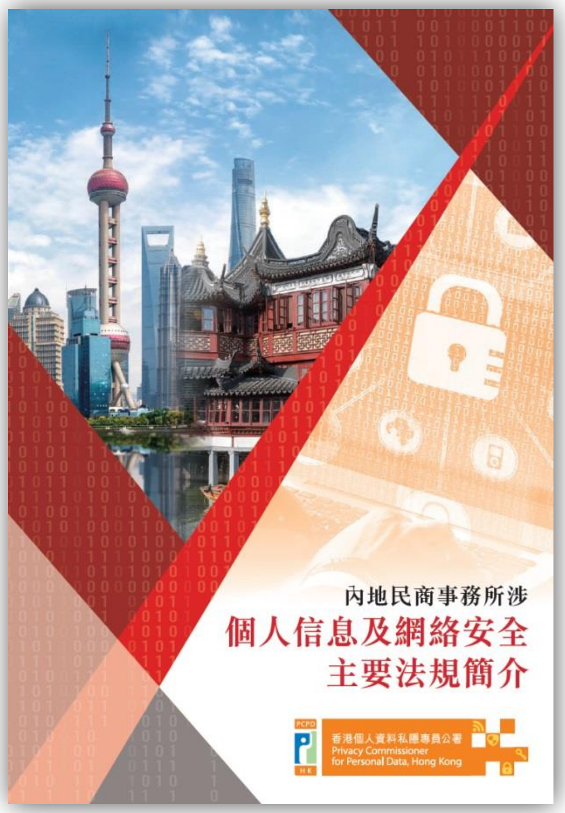
Unique & Irreplaceable Attributes of Hong Kong

Free Flow of Information



Only Region in China with English as One of the Official Languages

Personal Data (Privacy) Protection Framework



內地民商事務所涉
個人信息及網絡安全
主要法規簡介

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

PCPD publication on mainland personal information regulation
《內地民商事務所涉個人信息及網絡安全主要法規簡介》

Objectives

- Provide an overview of related regulations
- Serve as a handy kit to help the business sector operating in GBA
- Promote cross-boundary data flow and development of data economy

Comparison between PDPO and Data Protection Laws in the mainland of China

	《個人資料(私隱)條例》	內地相關法規
立法目的	在個人資料方面保障個人的私隱。	視乎不同法規而定。 例如《網絡安全法》的主要目的為保障網絡、國家及社會安全，維護公民、法人和其他組織的合法權益，促進經濟社會信息化健康發展。《數據安全管理辦法》（徵求意見稿）的目的包括保障個人信息和重要數據安全。
規管對象	資料使用者，即就個人資料而言，獨自或聯同其他人或與其他人共同控制該資料的收集、持有、處理或使用的人。	視乎不同法規而定。 例如《網絡安全法》、《數據安全管理辦法》（徵求意見稿）和《兒童個人信息網絡保護規定》規管網絡運營者，《電子商務法》規管電子商務經營者，《消費者權益保護法》規管向消費者提供商品和服務的經營者。
個人資料 /個人信息的定義	個人資料是指（1）直接或間接與一名在世的個人有關的任何資料，（2）而從該資料直接或間接地確定有關的個人的身分是切實可行，以及（3）該資料的存在形式必須是令查閱及處理均是切實可行的。	按《網絡安全法》，個人信息是指以電子或者其他方式記錄的能夠單獨或者與其他信息結合識別自然人個人身份的各種信息。 按最高人民法院及最高人民檢察院聯合公布的解釋，以及《個人信息安全規範》（徵求意見稿），個人信息還包括可反映特定自然人活動情況的各種信息。
個人敏感信息	《條例》沒有專屬定義。 然而，《條例》附表1的保障資料第4原則的某些規定，可應用於保障個人敏感信息。該原則規定，資料使用者在個人資料保安方面，除了其他事宜外，尤其須考慮資料的種類，及因未獲准許的或意外的查閱、處理、刪除、喪失或使用而做成的損害。	按《個人信息安全規範》（徵求意見稿），個人敏感信息是指一旦洩露、非法提供或濫用可能危害人身和財產安全，極易導致個人名譽、身心健康受到損害或歧視性待遇等的個人信息，具體例子包括身份證件號碼、個人生物識別信息、銀行帳號、通信記錄和內容、財產信息、徵信信息、行蹤軌跡、住宿信息、健康生理信息、交易信息以及14歲以下兒童的個人信息等。 《數據安全管理辦法》（徵求意見稿）要求收集敏感個人信息的網絡運營者向所在地的網信部門備案，並須明確數據安全責任人。

	《個人資料 (私隱) 條例》	內地相關法規
收集	《條例》附表1的保障資料第1原則規定，資料使用者須以合法和公平的方式收集他人的個人資料，收集目的須為合法目的並須是必需或直接與資料使用者的職能或活動有關，所收集的資料必須不超乎適度。	《網絡安全法》規定，收集、使用個人信息，應當遵循合法、正當、必要的原則，必須取得被收集者的同意。不得收集與提供的服務無關的個人信息。 《數據安全管理辦法》（徵求意見稿）規定在收集個人信息時須向個人提供收集及使用個人信息的規則，並禁止以改善服務品質、提升用戶體驗、定向推送信息、研發新產品等為由，以預設授權、功能捆綁等形式強迫、誤導個人同意其收集個人信息。 如收集的屬個人敏感信息，《數據安全管理辦法》（徵求意見稿）規定須向所在地的網信部門備案，而《個人信息安全規範》（徵求意見稿）則建議要取得個人的「明示同意」。 《兒童個人信息網絡保護規定》要求收集和使用兒童個人信息前，須告知兒童的監護人，並取得監護人的同意。
使用及披露	《條例》附表1的保障資料第3原則規定，資料使用者使用（包括披露）個人資料的目的必須屬收集時的目的或直接有關的目的，否則須先取得資料當事人的同意。	《網絡安全法》規定，收集、使用個人信息，應當遵循合法、正當、必要的原則，必須取得被收集者的同意。 《數據安全管理辦法》（徵求意見稿）規定使用個人信息時，不得違反向個人說明了的收集、使用規則。如因業務需要，確需擴大個人信息使用範圍，須徵得個人同意。若要向第三方披露個人信息，須先評估安全風險，並取得個人同意。 《兒童個人信息網絡保護規定》要求收集和使用兒童個人信息前，須告知兒童的監護人，並取得監護人的同意。
透明度	《條例》附表1的保障資料第1原則規定，資料使用者須採取所有切實可行的步驟，以確保在收集個人資料之時或之前，資料當事人獲告知收集其個人資料的目的、資料可能會被轉移給哪類人士、資料當事人是否有責任提供資料，及不提供資料的後果。 《條例》附表1的保障資料第5原則規定，資料使用者須採取所有切實可行的步驟，以確保任何人能確定資料使用者在個人資料方面的政策及實務，並能獲告知資料使用者所持有的個人資料的種類及使用之主要目的。	《網絡安全法》及《數據安全管理辦法》（徵求意見稿）規定要公開收集、使用規則，明示收集、使用信息的目的、方式和範圍等。 《兒童個人信息網絡保護規定》要求設置專門的兒童個人信息保護規則和用戶協議，有關規則和協議應當簡潔、易懂。

	《個人資料 (私隱) 條例》	內地相關法規
保安	《條例》附表1的保障資料第4原則規定 – • 資料使用者須採取所有切實可行的步驟，以確保由其持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響。 • 如聘用資料處理者代為處理個人資料，資料使用者須採取合約規範方法或其他方法，以防止轉移予資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用。	《網絡安全法》規定要採取技術措施和其他必要措施，確保其收集的個人信息安全，防止信息洩露、毀損、丟失。 《數據安全管理辦法》（徵求意見稿）要求網絡運營者參照國家相關標準，建立數據安全管理制度，制定數據安全計劃，實施數據安全技術防護（例如數據分類、備份、加密等）以保障數據安全。
保存期限	《條例》附表1的保障資料第2(2)原則規定，資料使用者須採取所有切實可行的步驟，以確保個人資料的保存時間不超過為貫徹使用該資料之目的而所需的時間。 《條例》第26條規定，資料使用者須採取所有切實可行步驟，刪除不再需要的個人資料。	按《數據安全管理辦法》（徵求意見稿），個人信息保存期不應超出收集使用規則中的保存期限。 《電子商務法》規定在用戶註銷帳戶後立即刪除有關用戶的信息。
準確性	《條例》附表1的保障資料第2(1)原則規定– • 資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤。 • 若有合理理由相信個人資料不準確時，資料使用者須確保該資料不會被使用或會被刪除。 • 若知悉向第三者披露的個人資料在要項上不準確時，資料使用者須確保第三者獲告知，及獲提供所需詳情以令第三者能更正。	《個人信息安全規範》（徵求意見稿）在「確保安全原則」下建議要採取措施保護個人信息的完整性和可用性。
問責制	《條例》沒有相關規定。 私隱專員鼓勵資料使用者實行「私隱管理系統」以實踐問責制。	《網絡安全法》規定網絡運營者應當對其收集的個人信息嚴格保密，並建立健全的信息保護制度。 《數據安全管理辦法》（徵求意見稿）明確要求開展數據安全風險評估，制定網絡安全事件應急預案，並組織數據安全教育、培訓。 《兒童個人信息網絡保護規定》要求有指定專人負責兒童個人信息保護。 《個人信息安全規範》（徵求意見稿）建議任命專職的個人信息保護負責人和設立個人信息保護工作機構，負責個人信息安全工作。

	《個人資料(私隱)條例》	內地相關法規
外洩通報	《條例》沒有相關規定。 私隱專員鼓勵資料使用者發現個人資料外洩時通報受影響人士及相關規管 / 執法機構。	《網絡安全法》、《電子商務法》、《兒童個人信息網絡保護規定》、《數據安全管理辦法》（徵求意見稿）及《個人信息出境安全評估辦法》（徵求意見稿）均規定在發生或者可能發生個人信息洩露或其他信息安全事故時，應當立即向有關主管部門報告，甚或通知受影響的個人。 《網絡安全威脅信息發布管理辦法》（徵求意見稿）規定，任何企業、組織或個人在發布網絡安全威脅信息前，應事先向相關網信部門及公安機關報告。
跨境數據轉移	《條例》第33條規管 (1) 在香港收集、持有、處理或使用的個人資料，或(2) 主要業務地點在香港的資料使用者，控制收集、持有、處理或使用的個人資料。 該條規定，除非符合《條例》下的指明條件（例如得到資料當事人的書面同意，或資料使用者已採取所有合理的預防措施及已作出所有應作出的努力，以對個人資料提供足夠的保護），否則受規管的個人資料不得轉移離開香港。但相關規定尚未實施。	《網絡安全法》規定「關鍵信息基礎設施的運營者」須將個人信息及重要數據儲存在中國內地。如要出境，須進行安全評估。 《個人信息出境安全評估辦法》（徵求意見稿）將《網絡安全法》下的個人信息出境限制擴展至所有網絡運營者，並要求將安全評估向省級網信部門申報及取得其批准後方可將個人信息傳送到境外。
個性化及自動決策	《條例》沒有就個性化及自動決策，特定給予相關定義及作出相關規定。 然而，《條例》第30至32條規管「核對程序」，而有關程序可能會應用於個性化的操作。 「核對程序」指符合以下全部四項準則的程序： (1) 有關程序將兩套為不同目的而收集的個人資料加以核對； (2) 每一項比較涉及十個或以上資料當事人； (3) 比較並非以人手方法進行； (4) 核對資料的結果可即時或在將來用來對有關資料當事人採取不利行動。 除非獲資料當事人或私隱專員同意，資料使用者不得進行「核對程序」。	《電子商務法》規定如果電子商務經營者向個人提供個性化的商品或服務的搜尋結果，須容許個人關閉此個性化推薦的功能。 《數據安全管理辦法》（徵求意見稿）規定如網絡運營者向個人推送個性化的新聞信息、商業廣告等，應當以明顯方式標明「定推」字樣，並提供停止接收定向推送信息的選項。 《個人信息安全規範》（徵求意見稿）建議在進行會對個人信息主體權益造成顯著影響的自動決策前，須開展個人信息安全影響評估，並且向個人信息主體提供針對自動決策結果的申訴管道。
查閱及更正權	《條例》第18及22條，及附表1的保障資料第6原則訂明，資料當事人有權向資料使用者要求查閱個人資料，及要求改正不準確的個人資料。	《網絡安全法》規定個人有權要求網絡運營者更正錯誤的個人信息。 《數據安全管理辦法》（徵求意見稿）規定網絡運營者要遵從個人查閱及更正個人信息的要求。 《電子商務法》規定電子支付服務提供者須向使用者免費提供最近三年的交易記錄。

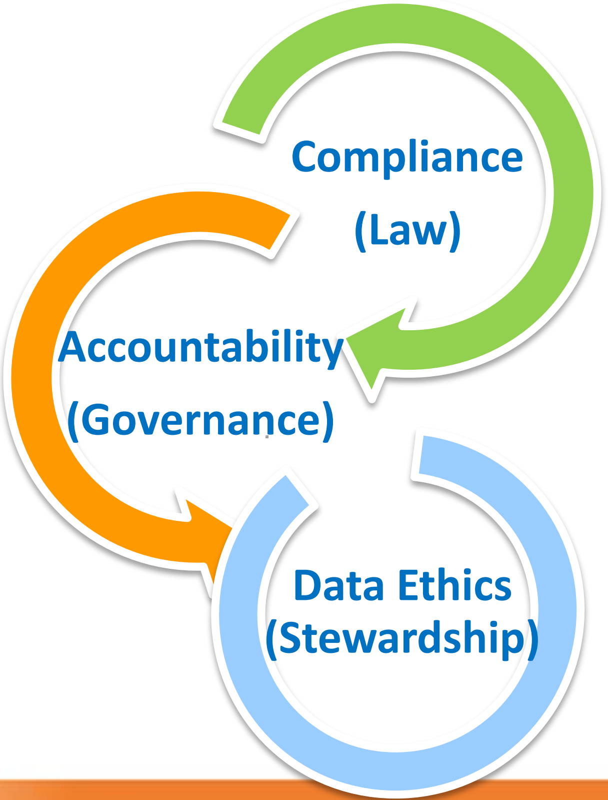
	《個人資料(私隱)條例》	內地相關法規
刪除權	資料當事人沒有明確的權利要求刪除其個人資料。 然而，《條例》第26條及附表1的保障資料第2(2)原則規定，資料使用者須採取所有切實可行步驟，刪除不再需要的個人資料。	按《網絡安全法》，如網絡運營者違規收集或使用個人信息，個人有權要求網路運營者將信息刪除。 《數據安全管理辦法》（徵求意見稿）亦規定網絡運營者要在合理的代價和時間內遵從個人刪除個人信息的要求。
執法機構	私隱專員	沒有單一、指定的執法機構。視乎行業和案件性質，執法機構可以為網信辦、公安部、工信部或其他主管部門。
罰則	專員可向違反《條例》要求的資料使用者發出執行通知。不遵守執行通知是刑事罪行，違者如屬首次定罪，最高可判罰款五萬元及監禁兩年；如屬再次定罪，最高可判罰款十萬元及監禁兩年。 違反《條例》的某些規定亦構成刑事罪行，違者可判罰款甚至監禁。例如（1）為得益而沒有依從資料當事人的要求，停止將該當事人的個人資料提供予其他人在直接促銷中使用，或（2）披露未經資料使用者同意而獲取的個人資料並導致有關資料當事人蒙受心理傷害，最高可判罰款100萬元及監禁五年。	視乎不同法規而定。 例如違反《網絡安全法》的規定可被責令改正，並根據情節嚴重程度而處以警告、沒收違法所得（如有）、處以罰款（最高為違法所得的十倍或100萬元）、對直接負責的主管人員和其他直接責任人員處以最高10萬元罰款，甚或責令暫停相關業務、停業整頓、關閉網站、吊銷相關業務許可證或營業執照。如構成犯罪的， 依法追究刑事責任。
民事索償	根據《條例》第66條，資料當事人因資料使用者違反《條例》而蒙受損害（包括感情傷害），有權向該資料使用者申索補償。 根據《條例》第66B條，專員可就申索補償的法律程序，向有關資料當事人給予協助，當中包括（1）提供意見、（2）安排律師或大律師提供意見或協助及（3）安排其他人代表該資料當事人行事。	根據《民法總則》，侵犯公民的隱私權或個人信息須要承擔民事責任，當中包括停止侵害、賠償損失、消除影響、恢復名譽及賠禮道歉。

PCPD's Roles – Enforcer + Educator + Facilitator

Fair Enforcement

Engaging

Incentivising



Privacy-friendly Culture

Thank you

Stephen Kai-yi WONG, Barrister

Privacy Commissioner for Personal Data,
Hong Kong, China