SME Committee of Hong Kong General Chamber of Commerce
香港總商會中小型企業委員會
14.03.2018

Data Privacy Updates for SME
資料私隱保障的最新發展 –
給中小型企業的資訊

Stephen Kai-yi Wong, Barrister
Privacy Commissioner for Personal Data, Hong Kong
黃繼兒大律師
香港個人資料私隱專員

Presentation Outline 大綱

1. Present Situation of SME and their Concerns
   中小企業的現狀及面對的挑戰
2. Cross-border Data Transfer under the Personal Data (Privacy) Ordinance (PDPO) & The European General Data Protection Regulation (GDPR)
   個人資料(私隱)條例下的跨境資料轉移與歐盟的《通用數據保障條例》
3. Recommendations to SME on Cybersecurity Measures
   就網絡保安方面給中小企的建議
4. Privacy Management Programme
   私隱管理系統
5. PCPD's Work to Support SME
   協助中小企

1

Present Situation of SME and their Concerns
中小企業的現狀及面對的挑戰

Ever Changing Business Environment
營商環境不斷改變

Limited Resources
資源有限

Weak Corporate Governance Framework
企業管治架構薄弱

Insufficient Support
支援不足

Insufficient Staff Training
員工培訓不足

Lack of Information Channels
缺乏接收資訊渠道

Present situation of SME and their concerns
中小企業的現狀及面對的挑戰

2

Cross-border Data Transfer under the Personal Data (Privacy) Ordinance (PDPO) & The European General Data Protection Regulation (GDPR)

個人資料(私隱)條例下的跨境資料轉移與歐盟的《通用數據保障條例》

Cross-border Data Transfer
跨境資料轉移

Section 33 of the PDPO prohibits transfer of personal data outside Hong Kong unless under 6 specified circumstances

除非符合條例列明的6種情況，條例第33條禁止轉移個人資料至香港以外地區

Legislative intent:
To ensure personal data transferred outside Hong Kong is afforded with same protection

立法目的:
確保轉移香港以外的個人資料獲得相當於在條例下所提供的保障

Cross-border Data Transfer
跨境資料轉移

Meaning of "Transfer" 「轉移」的定義

Transfer from Hong Kong to a place outside Hong Kong

將個人資料由香港轉移至境外

Transfer between 2 other places where the transfer is controlled by a data user in Hong Kong

在兩個其他司法區之間轉移個人資料，該轉移是由香港的資料使用者所控制

Cross-border Data Transfer 跨境資料轉移

Data user shall not transfer personal data outside Hong Kong unless one of the conditions are met:- 除非符合以下其中一項條件，資料使用者不得將個人資料轉移至香港以外地區:-

s.33(2)(a)

- **Fall within one of the White List jurisdictions (i.e. the law in that place is *"substantially similar to or serves the same purposes as"* the PDPO pursuant to PCPD's assessment)**
  符合白名單列出的其中一個司法管轄區 (該地區實施的有關個人資料保障法律，與條例大致上相似)

s.33(2)(b)

- **Data user's own assessment (that the law in that place is "substantially similar to or serves the same purposes as" the PDPO)**
  資料使用者自行評估該地方有與條例大體上相似或達致與條例的目的相同的目的之法律正在生效

s.33(2)(c)

- **Data subject's written consent to the transfer**
  資料當事人已以書面同意有關轉移

Cross-border Data Transfer 跨境資料轉移

s.33(2)(d)

- Avoidance or mitigation of adverse action against the data subject
  避免針對資料當事人的不利行動或減輕該等行動

s.33(2)(e)

- Exemptions from data protection principle 3 (i.e. use limitation) under Part VIII of the PDPO apply
  條例第8部份下的豁免保障資料第3原則的條款適用

s.33(2)(f)

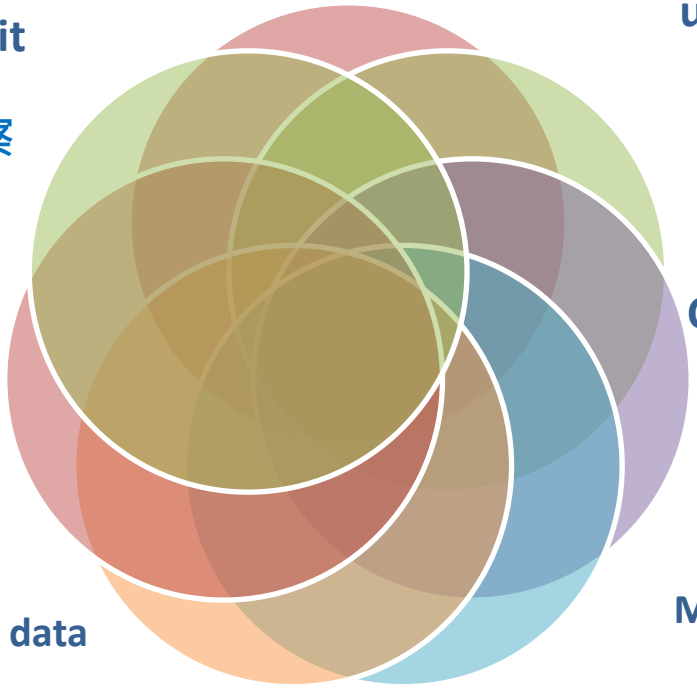
- Data user has taken all reasonable precautions and exercised all due diligence such that personal data transferred will not be handled in a manner that contravenes the PDPO ("Due Diligence Requirement")
  資料使用者已採取所有合理措施及作出所有相應努力確保資料被轉移後的處理不違反條例規定 (「克盡職責的規定」)

Tips for Cross Border Data Transfer
跨境資料轉移的實用提示

Review existing data transfer strategy
檢討資料轉移安排

Control unintended or unnecessary cross-border data flow
控制涉及無意或不必要的跨境資料流動活動

Conduct regular audit and inspection
進行定期審核及視察



Check the White List (when it comes into effect)
檢查白名單 (當正式生效時)

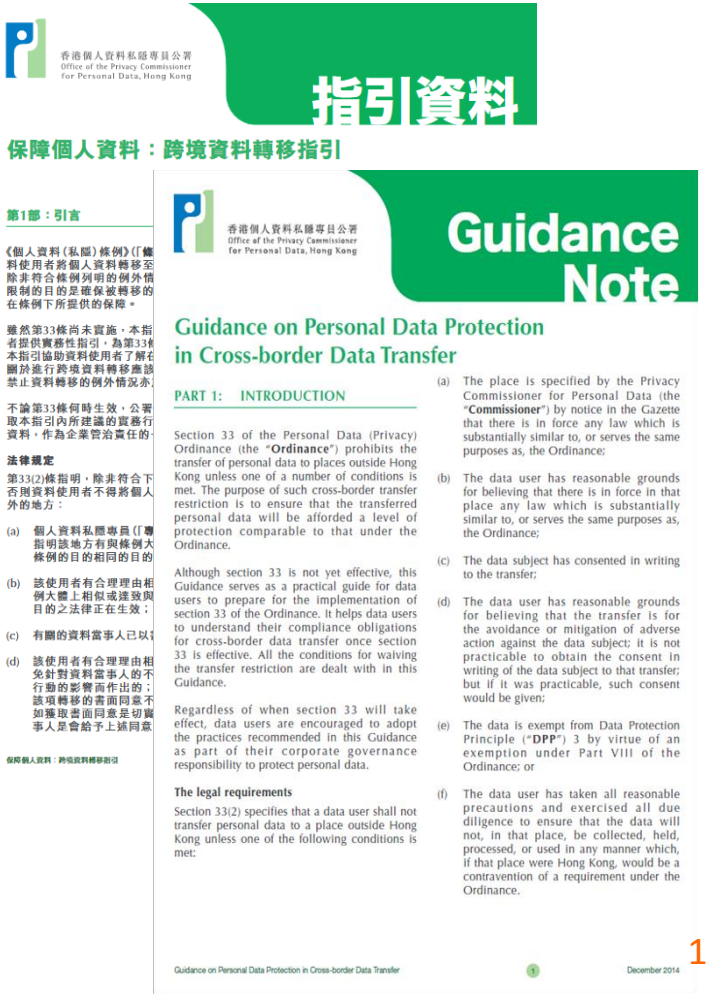
Be transparent
保持透明度

Keep inventory of personal data
備存個人資料庫存

May adopt multiple measures to give more protection
採取更多措施提高保障

Guidance on Personal Data Protection in Cross-border Data Transfer
保障個人資料: 跨境資料轉移指引

- **Although section 33 is not yet effective, the Guidance serves as a practical guide for data users to:**
  雖然第33條尚未實施，有關指引旨在向資料使用者提供實務性指引，以協助他們:
  - **understand compliance obligations;**
    了解應該遵守的義務;
  - **adopt the practices recommended as part of their corporate governance responsibility to protect personal data;**
    採取指引內所建議的實務行事方式以保障個人資料，作為企業管治責任的一部份;
  - **consider adapting and/or including "Recommended Model Clauses" in a data transfer agreement**
    考慮在資料轉移協議內改編/ 採納指引內列出之「建議範本條文」


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

指引資料

保障個人資料：跨境資料轉移指引

第1部：引言

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

Guidance Note

Guidance on Personal Data Protection in Cross-border Data Transfer

PART 1: INTRODUCTION

Section 33 of the Personal Data (Privacy) Ordinance (the "**Ordinance**") prohibits the transfer of personal data to places outside Hong Kong unless one of a number of conditions is met. The purpose of such cross-border transfer restriction is to ensure that the transferred personal data will be afforded a level of protection comparable to that under the Ordinance.

Although section 33 is not yet effective, this Guidance serves as a practical guide for data users to prepare for the implementation of section 33 of the Ordinance. It helps data users to understand their compliance obligations for cross-border data transfer once section 33 is effective. All the conditions for waiving the transfer restriction are dealt with in this Guidance.

Regardless of when section 33 will take effect, data users are encouraged to adopt the practices recommended in this Guidance as part of their corporate governance responsibility to protect personal data.

The legal requirements

Section 33(2) specifies that a data user shall not transfer personal data to a place outside Hong Kong unless one of the following conditions is met:

(a) The place is specified by the Privacy Commissioner for Personal Data (the "**Commissioner**") by notice in the Gazette that there is in force any law which is substantially similar to, or serves the same purposes as, the Ordinance;

(b) The data user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, the Ordinance;

(c) The data subject has consented in writing to the transfer;

(d) The data user has reasonable grounds for believing that the transfer is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the consent in writing of the data subject to that transfer; but if it was practicable, such consent would be given;

(e) The data is exempt from Data Protection Principle ("**DPP**") 3 by virtue of an exemption under Part VIII of the Ordinance; or

(f) The data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed, or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the Ordinance.

Guidance on Personal Data Protection in Cross-border Data Transfer 1 December 2014

Other Data Protection Principles in relation to Data Transfer
其他與資料轉移有關的保障資料原則

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 -
如資料使用者聘用資料處理者處理個人資料，須透過合約規範或其他方法 -

Principle 原則 2(3)

- to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data
防止轉移予資料處理者處理的個人資料被保存超過所需時間

Principle 原則 4(2)

- to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing
防止轉移予資料處理者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

PDPO – GDPR Comparative Study
《私隱條例》– 《通用數據保障條例》比較研究

Background 背景

- **Keep abreast of overseas** privacy law developments
  使《私隱條例》能緊貼全球私隱法規的發展

- Assess GDPR's **impact on businesses** (in particular multi-national organisations)
  評估《通用數據保障條例》對企業(尤其跨國企業)的影響

- Comparable legal framework facilitates **free flow of information** and commercial activities
  法例框架比較便利資訊自由流通及促進商貿活動

PDPO – GDPR Comparative Study
《私隱條例》– 《通用數據保障條例》比較研究

PCPD identified the following NINE major differences between PDPO and GDPR:
私隱專員公署確立了《私隱條例》與《通用數據保障條例》 的九個主要差異:

1. Extra-Territorial Application 域外效力	**6. Data Processor Obligations** 資料處理者的責任
2. Accountability and Governance 問責及管治	**7. New of Enhanced Rights of Data Subjects/Profiling** 新增或加強資料當事人的權利/個人概況彙編
3. Mandatory Breach Notification 強制資料外洩通報	**8. Certification/Seals and Personal Data Transferred Outside Jurisdictions** 認證及轉移個人資料至管轄區外
4. Sensitive Personal Data 敏感的個人資料	**9. Sanctions** 罰則
5. Consent 同意	

1. Extra-Territorial Application
域外效力

EU GDPR 歐盟的《通用數據保障條例》	HK PDPO 香港的《私隱條例》
Data processors or controllers: 資料處理者或控制者: • with an establishment in the EU, or 於歐盟設立；或 • 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] 於歐盟以外設立，而其產品及服務的受眾目標或其監察行為的目標是歐盟的資料當事人[第 3條]	**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)] 資料使用者指獨自或聯同其他人或與其他人在/從香港共同控制該資料的收集、持有、處理或使用的人 [第2(1)條]

2. Accountability and Governance
問責及管治

EU GDPR
歐盟的《通用數據保障條例》

Risk-based approach to accountability. Data controllers are required to:
風險為本的問責制。 資料控制者須:

- implement technical and organisational measures to ensure compliance [Art 24];主動採取各項技術及措施以確保循規守法 [第24條];
- adopt **data protection by design** and **by default** [Art 25]; 採納**貫徹私隱的設計及預設私隱模式** [第25條];
- conduct **data protection impact assessment** for high-risk processing [Art 35]; and 對高風險的程序進行**資料保障影響評估** [第35條]; 及
- (for certain types of organisations) **designate Data Protection Officers** [Art 37]. (特定種類的機構)委聘資料保障主任 [第37條]

HK PDPO
香港的《私隱條例》

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

  沒有明確說明問責原則和相關的私隱管理工具

- 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.

  私隱專員提倡**私隱管理系統**以體現問 責原則。保障資料主任的任命和私隱影響評估的實施是實現問責的良好行事方式。

3. Mandatory Breach Notification
強制資料外洩通報

EU GDPR 歐盟的《通用數據保障條例》	HK PDPO 香港的《私隱條例》
• Data controllers are required to notify the authority about a data breach without undue delay (exceptions apply). 資料控制者須及時向監管當局通報資料外洩事故(除例外情況適用) • Data controllers are required to notify affected data subjects unless exempted. [Arts 33-34] 除非獲得豁免，資料控制者須通知受影響的資料當事人 [第33-34條]	• No mandatory requirement. Voluntary breach notification. 沒有強制要求，自願作出資料外洩通報

4. Sensitive Personal Data
敏感的個人資料

EU GDPR 歐盟的《通用數據保障條例》	HK PDPO 香港的《私隱條例》
• Expand the category of sensitive personal data. 擴大敏感個人資料的類別 • Processing of sensitive personal data is allowed only under specific circumstances. [Art 9] 在特定的情況下才能處理敏感的個人資料 [第9條]	• No distinction between sensitive and non-sensitive personal data. 沒有明確區分感敏及非敏感的個人資料

5. Consent 同意

EU GDPR
歐盟的《通用數據保障條例》

- One of the 6 lawful bases for processing
  六項合法處理資料方式之一

- Consent must be 同意必須是
  - ✓ **freely given, specific and informed**; and 自願提供、具體及知情的情況下毫無疑問地給予;並
  - ✓ **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)]
    明確反映資料當事人的意願, 透過聲明或明確的行動取得當事人在處理其個人資料方面的同意 [第4(1)條]

HK PDPO
香港的《私隱條例》

- 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]
  在收集個人資料上沒有規定必須先取得資料當事人的同意，除非個人資料使用於新目的。[保障資料第1及3原則)

6. Data Processor Obligations
資料處理者的責任

EU GDPR 歐盟的《通用數據保障條例》	HK PDPO 香港的《私隱條例》
• 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] 附加額外責任予資料處理者，例如保留處理個人資料的紀錄、確保處理個人資料的保安、通報資料外洩事故、委任保障資料主任等 [第30,32-33, 37條]	• Data processors **are not directly regulated**. 資料處理者並非直接受規管 • Data users are required to **adopt contractual or other means** to ensure data processors comply with **data retention and security requirements**. [DPPs 2&4] 資料使用者必須以合約規範方法或其他方法以確保資料處理者遵守資料保留及保安方面的規定[保障資料第2及第4原則]

7. New or Enhanced Rights of Data Subjects / Profiling
新增或加強資料當事人的權利/個人概況彙編

EU GDPR 歐盟的《通用數據保障條例》	HK PDPO 香港的《私隱條例》
• Right to **erasure of personal data** (also known as "right to be forgotten") [Art 17] 賦予**刪除個人資料**的權利(亦稱為「被遺忘權」)[第17條]	• No general right to erasure, but shall not retain personal data for longer than necessary [S.26 & DPP 2(2)] 沒有賦予刪除個人資料的權利，但保留個人資料的期限不得超過實際目的所須 [第26條及保障資料第2(2)原則)
• Right to **data portability** [Art 20] 個人資料可攜性方面的權利 [第20條]	• No right to data portability 沒有個人資料可攜性方面的權利
• Right to object to processing (including profiling) [Art 21] 反對處理其個人資料的權利(包括個人概況彙編) [第21條]	• 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 [s. 30-31] 沒有反對處理其個人資料的權利 (包括個人概況彙編)，但可**拒絕直接促銷活動**[第35G及35L條] 及包含規管資料核對程序的條文 [第30-31條]
• **"Profiling"** is defined as any form of automated processing involving personal data to evaluate certain personal aspects of a natural person [Art 4(4)] 「個人概況彙編」是指以任何自動化方式處理個人資料，藉以推算某人士的個人資訊 [第4(4)條]	
• Expanded notice requirement for the new or enhanced rights 擴大通知責任以加強資料當事人的權利	

8. Certification / Seals and Personal Data Transferred Outside Jurisdictions
認證及轉移個人資料至管轄區外

EU GDPR 歐盟的《通用數據保障條例》	HK PDPO 香港的《私隱條例》
• Explicitly recognises privacy seals and establishes certification mechanism for demonstrating compliance by data controllers and processors. [Art 42] 提供私隱認證及建立認可機制，證明資料控制者及處理者有循規守法[第42條]	• No such certification or privacy seals mechanism for demonstrating compliance. 沒有私隱認可或認證機制證明資料控制者及處理者有循規守法
• Certification as one of the legal bases for cross-border data transfer. 認證機制是跨境轉移資料的法律基礎之一	

9. Sanction 罰則

EU GDPR 歐盟的《通用數據保障條例》	HK PDPO 香港的《私隱條例》
• Data protection authorities can impose **administrative fines** on data controllers and processors. [Art 58] 容許資料保障機構向資料控制者及處理者徵收**行政罰款** [第58條]	• The Privacy Commissioner is not empowered to impose administrative fines or penalties. 私隱專員沒被賦予權力徵收行政罰款或懲罰
• Depending on the nature of the breach, the fine could be up to **€20million** or **4%** of the total worldwide annual turnover. [Art 83] 視乎資料外洩的性質，罰款可達**2000萬歐羅**或該機構全球總年度收入的**4%** [第83條]	• The Privacy Commissioner may serve **enforcement notices** on data users. 私隱專員可向資料使用者發出**執行通知**

3

Recommendations to SME on Cybersecurity Measures
就網絡保安方面給中小企的建議

Recent Cybersecurity Incidents
近期的網絡保安事故

source: https://goo.gl/oY6ArS

source: https://goo.gl/9sSQHN

source: https://goo.gl/1ZVttD

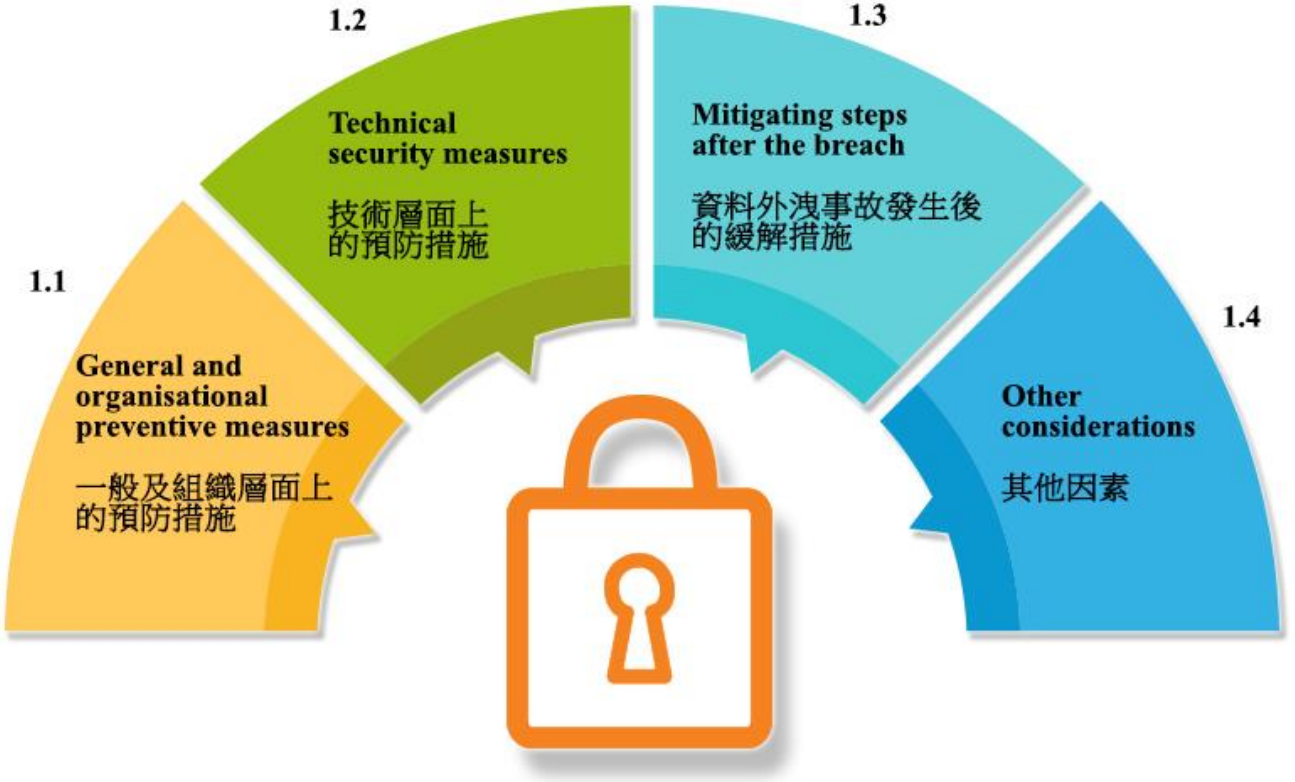
Cybersecurity-related Data Protection Principles
與網絡保安有關的保障資料原則

Principle 4 – Security of personal data
第4原則 – 個人資料的保安

Data users shall take all practicable steps to safeguard personal data against unauthorised or accidental access, processing, erasure, loss or use

資料使用者須採取切實可行的步驟確保個人資料的保安，免受未獲授權或意外的查閱、處理、刪除、喪失或其他使用

What is “all practicable steps”?
何謂「切實可行的步驟」？



DPP4 & Data Security

保障資料第4原則及資料保安

What is "all practicable steps"?
何謂「切實可行的步驟」？

Embrace personal data privacy protection as part of the corporate governance responsibilities, covering business practices, operational processes, policies and training

在企業管治方面貫徹執行個人資料私隱保障，涵蓋業務常規、操作程序、政策、培訓等

Comprehensive and on-going review and monitoring process; build a robust privacy infrastructure

有整全的檢討及監察程序，建立健全的私隱保障基建

General and organisational preventive measures

一般及組織層面上的預防措施

Open and transparent information privacy policies and practices

公開和具透明度的資訊私隱政策和常規

Has top management commitment, a top-down business imperative throughout the organisation

由管理層開始，從上而下推

What is "all practicable steps"?
何謂「切實可行的步驟」？

Technical security measures 技術層面上的預防措施

Hardware security, e.g. information system, network infrastructure, etc
硬件方面的保安工作，如資訊系統、網絡基礎設施等

Policies and procedures for regular review of security systems
保安系統的定期審視政策和程序

Security measures and steps for system login, data transmission and storage, and adoption of international standards and technology, e.g. hashing, encryption, etc
在進入系統、資料傳送和保存方面的保安措施和步驟，以及採用國際間接受的準則和技術，如轉為亂碼 (hashed)、加密等

What is “all practicable steps”?
何謂「切實可行的步驟」？

What is "all practicable steps"?
何謂「切實可行的步驟」？

Other considerations
其他因素

- The nature, size and resources of the data user
  資料使用者的規模、性質及資源
- The likelihood of adverse consequences for affected individuals
  受影響人士可能遭受的不利後果
- The complexity of its operations of the data user and its business model
  資料使用者的業務或經營模式的複雜性
- The amount and sensitivity of personal data held
  個人資料的數量及敏感度

4 Privacy Management Programme
私隱管理系統

Privacy Management Programme

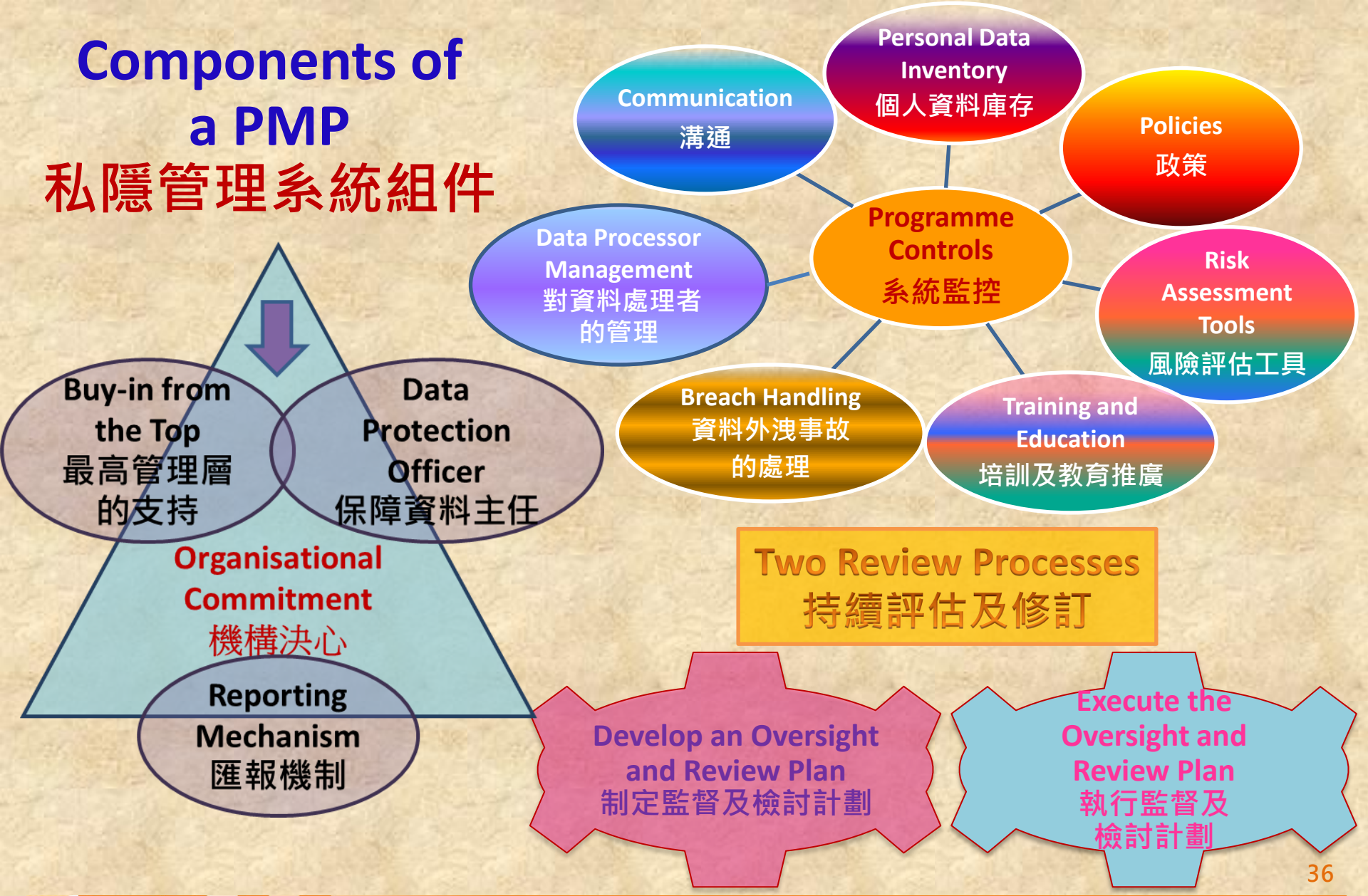
From Compliance to *Accountability*

What is PMP? 甚麼是私隱管理系統

Paradigm Shift 模式轉變

Compliance Approach 符規方式	Accountability Approach 問責方式
• passive 被動	active 主動
• reactive 消極	proactive 積極
• remedial 補救	preventive 預防
• problem-based 以解決問題為本	based on customer expectation 以符合客戶期望為本
• handled by compliance team 由合規部門處理	directed by top-management 由最高管理層指派
• minimum legal requirement 符合法律的最低要求	reputation building 建立商譽
• bottom-up 由下而上	top-down 由上而下

Components of a PMP
私隱管理系統組件



Participation in the PMP 參與私隱管理系統

Pledging Organisations 承諾機構

- ✓ All 76 bureaux and departments of Hong Kong Government 政府政策局及部門
- ✓ 25 Insurance companies 保險公司
- ✓ 9 Telecommunication companies 電訊公司
- ✓ 5 Organisations from other sectors 其他行業機構

Government Consultancy Project on Implementation of PMP

政府就實施私隱管理系統的顧問項目

Consultant engaged to facilitate bureaux/departments to implement PMP

聘請外間顧問協助政府決策局及部門實施私隱管理系統

Advice provided by the PCPD

公署建議

PMP Manual

(To be completed this year)

私隱管理系統手冊

(今年內完成)

PMP Training

培訓

PCPD's Future Plan 公署未來工作

5

PCPD's Work to Support SME

協助中小企

Guidance Note for SME
為中小企編制之指引資料

指引資料

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

PCPD.org.hk

資料保障・利便營商－給中小企的綱領提示

引言

一般中小企並沒有法律和符規的專責部門，往往因為對《個人資料（私隱）條例》（「條例」）認知不足而違反條例的有關規定。為了協助中小企了解如何依從條例的規定，香港個人資料私隱專員公署（「公署」）發出此份綱領提示，先前亦已推出《中小企保障個人資料私隱自學課程》的網上工具[1]，希望藉此就中小企的不同業務功能提供具體例子及實用建議。本提示分為以下部分：

I. 收集客戶的個人資料
II. 使用客戶的個人資料
III. 保障客戶個人資料的安全
IV. 營運網上業務或服務
V. 域外營運
VI. 產品或服務推廣
VII. 招聘人手
VIII. 使用閉路電視作保安用途
IX. 收集僱員的個人資料作監察
X. 外判個人資料的處理
XI. 處理查閱及改正個人資料要求

I. 收集客戶的個人資料

中小企為處理客戶的產品訂購和服務預約，均會收集客戶的個人資料，常見例子包括姓名、地址、電話號碼、電郵地址，有時或會包括香港身份證號碼（「身份證號碼」）或出生日期。然而，中小企必須考慮收集上述資料是否有實際需要，否則便屬超乎適度。以下列出一些中小企特別要注意的情況：

(I) 收集客戶的身份證號碼以辨識身份

一般人往往錯誤認為收集客戶的身份證號碼是進行身份認證的唯一方法。由於身份證號碼是敏感的個人資料，一般而言，除獲法律授權外，中小企作為資料使用者不能強制要求客戶提供其身份證號碼。中小企如欲收集客戶的身份證號碼，須遵守由公署發出的《身份證號碼及其他身份代號實務守則》[2] 行事，並考慮是否有其他較不侵犯私隱的辦法以代替收集身份證號碼。

不應收集身份證號碼的例子：

✘ 美容中心要求持有會員卡的客戶在網上預約服務時提供其身份證號碼作接受服務時核實身份之用。

✔ 要求客戶以會員編號作網上預約，並在接受服務時出示載有其相片及會員編號的會員卡，已可達到上述目的。

1 完成課程後，中小企可自行制定其私隱計劃，並會得到一份分析其機構如何處理個人資料和提供建議的報告，該自學課程網址為 www.pcpd.org.hk/misc/sme_kit。

2 請參閱公署發出的《身份證號碼及其他身份代號實務守則》，第2.1至2.3段。

Guidance Note

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

PCPD.org.hk

Data Protection & Business Facilitation Guiding Principles for Small and Medium Enterprises

Introduction

s small and medium enterprises (SME) may not ve their own legal and compliance departments, y risk breaching the requirements of the Personal (Privacy) Ordinance (the Ordinance) arising from equate knowledge of the Ordinance. To help SME stand and comply with the Ordinance, the office Privacy Commissioner for Personal Data, Hong he PCPD) issues these Guiding Principles after g an online tool - Self-training Module on n of Personal Data for SME[1], with a view to specific examples and practical advice to

ing customers' personal data
istomers' personal data
ing customers' personal data
online businesses or services
isiness outside Hong Kong
roducts or services

or security purpose
ees' personal data for monitoring
ocessing of personal data
and data correction requests

I. Collecting Customers' Personal Data

In handling customers' purchase orders and service appointments, SME may collect customers' personal data, e.g. name, address, email address and sometimes Hong Kong Identity Card (HKID Card) number or date of birth. However, the data so collected must be necessary but not excessive. SME should pay special attention to the following:

(I) Collecting HKID Card number of a customer for identification

There is a misconception that HKID Card data is the silver bullet for identity authentication. As HKID Card number is a sensitive personal data, SME, as data users, should not require customers to furnish his HKID Card number compulsorily, unless authorised by law. If SME intend to collect HKID Card number from a customer, they must comply with the *Code of Practice on the Identity Card Number and Other Personal Identifiers*[2] issued by the PCPD and consider whether there are any less privacy-intrusive alternatives to the collection of HKID Card number.

Examples of excessive collection of HKID Card number:

✘ A beauty centre requested customers, with membership cards bearing their photos, to provide HKID Card numbers in booking appointments online for identification purpose at their subsequent visits.

ME can build their own privacy plan and get a report of how their organisations are currently handling ns. The course can be accessed via www.pcpd.org.hk/misc/sme_kit.
of the *Code of Practice on the Identity Card Number and Other Personal Identifiers*

ing Principles for Small and Medium Enterprises 1 December 2017

Privacy Campaign for SME
中小企保障私隱活動

- To publish a privacy toolkit for SME on the compliance with the PDPO
  為中小企編製遵守條例規定資料套

- To revamp online "Self-training Module on Protection of Personal Data for SME"
  加強網上「中小企保障個人資料私隱自學課程」的內容
- To organise training programme
  舉辦培訓課程

Service & Information Exclusively for SME
為中小企而設的服務及資訊

- **Answer SME's enquiries on personal data privacy**
  為中小企解答與個人資料私隱有關的查詢

  - **a dedicated email account ; and**
    增設專用的電郵帳戶;及
  - **a dedicated hotline**
    專人接聽的諮詢熱線

Privacy Awards Presentation
私隱奧斯卡

- **Encourage SME to enhance personal data protection**
  鼓勵中小企加強保障個人資料私隱

- **Commend organsations which have made effort in personal data protection or actively implemented Privacy Management Programme**
  嘉許着力於個人資料保障或積極推行私隱管理計劃的企業

- **Enhance reputation**
  提升商譽


ngiyabonga
danke
謝謝
teşekkür ederim
спасибо
dank je
thank you
gracias
tapadh leat
mochchakkeram
bedankt
hvala
mauruuru
dziękuję
go raibh maith agat
obrigado
sagolun
sukriya
kop khun krap
arigatō
takk
dakujem
grazie
мерси
terima kasih
감사합니다
merci
ευχαριστώ