香港生產力促進局 SME ONE
歐盟《通用數據保障條例》五月實施
香港企業立即作好準備
24.05.2018

為何《通用數據保障條例》與香港企業/機構有關？

黃繼兒大律師
香港個人資料私隱專員

講座概要

- 就《通用數據保障條例》（GDPR）與香港《個人資料（私隱）條例》（《私隱條例》）作比較
- 為中小企提供建議，讓他們為GDPR的生效作好準備

GDPR

- 將於 **2018年5月25日生效**，取代歐洲議會及理事會第95/45/EC號指令
- 歐盟是香港第二大的貿易夥伴
- 因應GDPR的域外應用，香港企業可能會受到影響

新科技對私隱及道德帶來的影響

私隱及道德的影響

- 資料被暗中收集
- 超出資料使用的預期
- 個人概況彙編會否構成不公平及歧視
- 資料保留
- 資料保安

GDPR的重要訊息

- 可判罰款2千萬歐元或全球年度總營業額的4%
- 資料當事人可重掌控制權
- 問責
- 證明符合法規
- 具透明度
- 域外應用

機構/企業應看GDPR為

- 撥亂反正的機會
- 研發保障私隱及資料的產品
- 與客戶建立具透明度及信任的新關係
- 重置與私隱執法機構的關係

[The Commission Guidance on the direct application of the General Data Protection Regulation, 24 Jan 2018]

公署就GDPR實施的教育工作

GDPR
與《私隱條例》的比較研究

- 目的: 檢視 《私隱條例 》
- 公署在2018年4月3日出版了小冊子

www.pcpd.org.hk//tc_chi/resources_centre/publications/files/eugdpr_c.pdf

www.pcpd.org.hk//english/resources_centre/publications/files/eugdpr_e.pdf

《私隱條例》– GDPR比較研究

主要分別	
1. 域外應用	6. 資料處理者的責任
2. 問責與管治	7. 新增及提升的個人權利
3. 資料外洩事故強制通報	8. 資料保障印章、行為守則及司法管轄區之間的資料轉移
4. 敏感個人資料	9. 懲罰
5. 同意	

個人資料的定義

	歐盟 EU	香港 HK
個人資料 	「個人資料」為： • 任何有關一名已被識別或可被識別的自然人的資訊；而一名可被識別的自然人是指可直接或間接地被識別的。 • 可被明確地識別身份的個人資料的例子延伸至包括位置資料及網上識別符。[第4(1)條]	「個人資料」為指符合以下說明的任何資料： • 直接或間接與一名在世的個人有關的； • 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的；及 • 該資料的存在形式令予以查閱及處理均是切實可行的。[第2(1)條]

GDPR
域外應用

1. 應用

	歐盟 EU	香港 HK
應用 	資料處理者或控制者： • 在歐盟設立公司，或 • 在歐盟以外設立公司，提供貨品或服務，或監察歐盟人士的行為。 [第3條]	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]

域外應用

❑ 在歐盟設立機關

而該機關的活動涉及處理個人資料，不論是否確實在歐盟境內處理資料

(*Weltimmo v. NAIH* (C-230/14))

❑ 向歐盟人士提供貨品或服務或監察他們的行為

無論企業是否向歐盟的一個或多個成員國的個人提供商品或服務（無論付款方式如何）

- 需考慮整體情況

域外應用的例子

- ✓ 為向歐盟人士宣傳、售賣、推廣或銷售貨品或服務而設有銷售辦事處
- ✓ 為以上目的委任銷售代理或代表
- ✓ 一間日本的網上商店在其網站內以英語介紹產品，並以歐元作結算，一日內處理多宗來自歐盟人士的訂單，並寄送產品給他們

[第29條資料保障工作小組的歐盟GDPR：一般資訊文]

GDPR適用於香港的中小企嗎?

適用(如符合域用應用的情況)，除個別情況可獲豁免外

問責與管治

2.問責與管治

	歐盟 EU	香港 HK
問責與管治 	以風險為本；資料控制者須： • 實施技術性及機構性措施以確保循規 [第24條]； • 採取預設貫徹私隱的設計及預設 [第25條]； • 為高風險的處理活動進行資料保障評估 [第35條]；及 • （若屬某些類型的機構）委任保障資料主任 [第37條]。	沒有明確列明問責原則及相關的私隱管理措施。 私隱專員倡議採納私隱管理系統以顯示問責原則。 委任保障資料主任及進行私隱影響評估是為達致問責而建議的良好行事方式。

問責原則

- GDPR第*5(2)*條明確納入問責原則
  - 展示其遵從處理個人資料的原則；
  - 實施適當的技術性及機構性措施以確保循規；及在處理的過程中納入對資料的保障
- 風險為本的方法
- 措施或工具
  - 委任保障資料主任
  - 進行資料保障影響評估
  - 採取貫徹私隱的設計及預設設定
  - 為資料處理活動保存記錄
  - 制定資料處理政策或措施

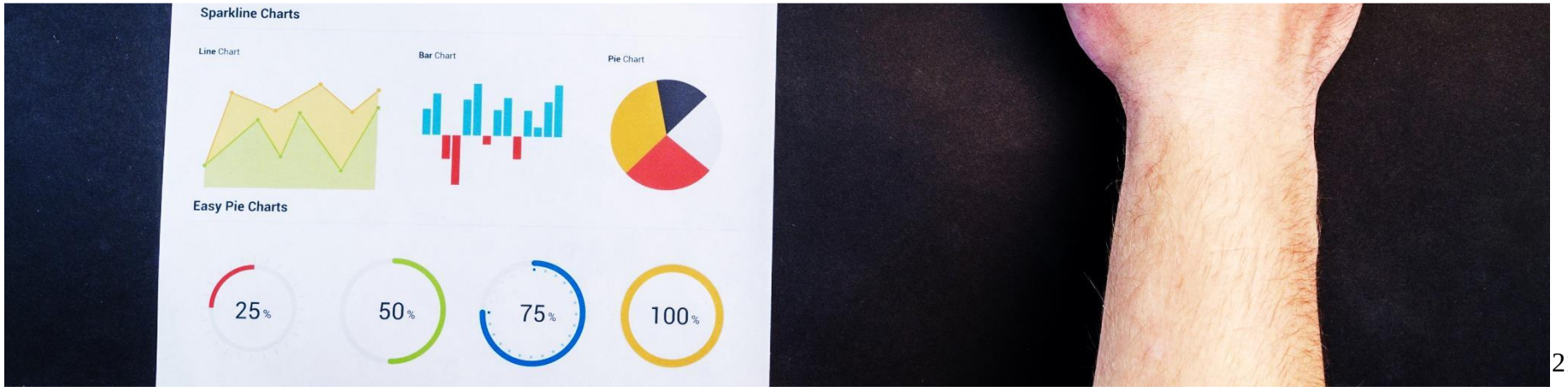
資料保障影響評估

- 協助資料控制者識別及管理資料保障的風險，避免在較後期才發現問題而引致不必要的費用，改善資料保安，及保持信任和聲譽
- 在下述的情況，必須進行資料保障影響評估：

1	以自動化的處理方式，對個人資料訊進行有系統及廣泛的評估，包括個人概況彙編
2	大規模處理敏感個人資料或有關刑事定罪或罪行的資料
3	有系統地對公共範圍作大規模的監察


Morris Charts

資料處理活動的記錄


Sparkline Charts
Line Chart
Bar Chart
Pie Chart
Easy Pie Charts
25%
50%
75%
100%

資料處理活動的記錄

- 記錄須包括:-

i. 企業的名稱及詳細聯絡資料
ii. 處理資料的原因
iii. 資料當事人及個人資料種類的描述
iv. 接收資料機構的類別
v. 轉移個人資料給第三國或國際組織，如適用
vi. 刪除資料的時限，如可能
vii. 在處理時使用安全措施的描述，如可能

資料處理活動的記錄

豁免：

僱用少於250人的機構 / 企業可獲豁免，除非

(i) 其資料處理活動很可能對資料當事人的權利及自由帶來風險;

(ii) 其核心活動涉及處理敏感個人資料、有關刑事定罪及罪行的個人資料或有系統的大規模監察活動;

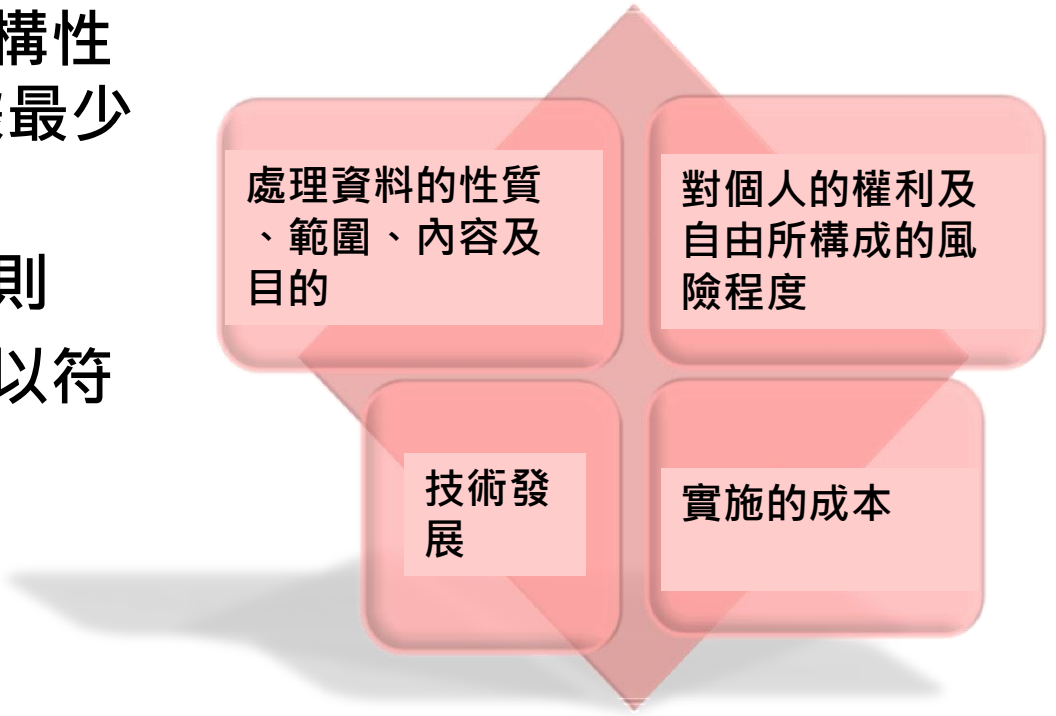
資料處理活動的記錄

- 實用提示

- 設計範本 (採用簡潔精確的語言，並輔以解釋)
- 分類 (內部與外部，種類及日期)
- 資料配對及處理資料的基礎
- 制定有關處理個人資料的政策及實務
- 制定與資訊保安有關的政策及實務
- 具透明度

貫徹私隱的設計及預設

- 實施適當的技術性及機構性措施(例如假名化及數據最少化）
- 以落實執行資料保障原則
- 納入所需的保安措施，以符合GDPR的規定



保障資料主任

保障資料主任

- 資料管治系統中擔當重要角色
- 負責履行問責工具（例如為資料處理活動及政策／措施作記錄、進行資料保障影響評估)
- 歐盟的《保障資料主任指引》
- 不論機構／企業的規模，在下述任何一個情況下均須委任保障資料主任
  - 它是公營機構或團體(輕微豁免)
  - 其核心活動包含處理運作時需要對資料當事人作大規模的定期及系統性監察
  - 其核心活動包含大規模處理敏感個人資料及有關刑事定罪及罪行的資料
- 除上述情況，委任保障資料主任屬於自願性質

保障資料主任

保障資料主任至少須執行下述工作:

- 告知及建議控制者 / 處理者及進行資料處理的僱員有關在GDPR下的責任；
- 監察控制者 / 處理者遵從GDPR及資料保障政策的情況，包括分配職責、提高從事資料處理運作的職員之意識並提供培訓
- 就資料保障影響評估提供建議及作監察
- 與監管機構合作，並擔任聯絡人

保障資料主任

專長

- 根據專業、知識和能力予以委任

聘用

- 可以是內部員工或可外間聘用

支援

- 須向保障資料主任提供足夠的資源以執行其職務

資料外洩事故強制通報

3.資料外洩事故強制通報

	歐盟 EU	香港 HK
通報資料外洩事故 	資料控制者須向監管機構通報資料外洩事故，不可不當地延誤（例外情況適用）。 如事故很可能對資料當事人的權利及利益造成高度風險，資料控制者須通知受影響的資料當事人，除非例外情況適用。 [第33-34條]	沒有強制性規定，但考慮到所有持份者包括資料使用者／控制者／當事人的利益，應通報私隱專員（及資料當事人，如適用）。

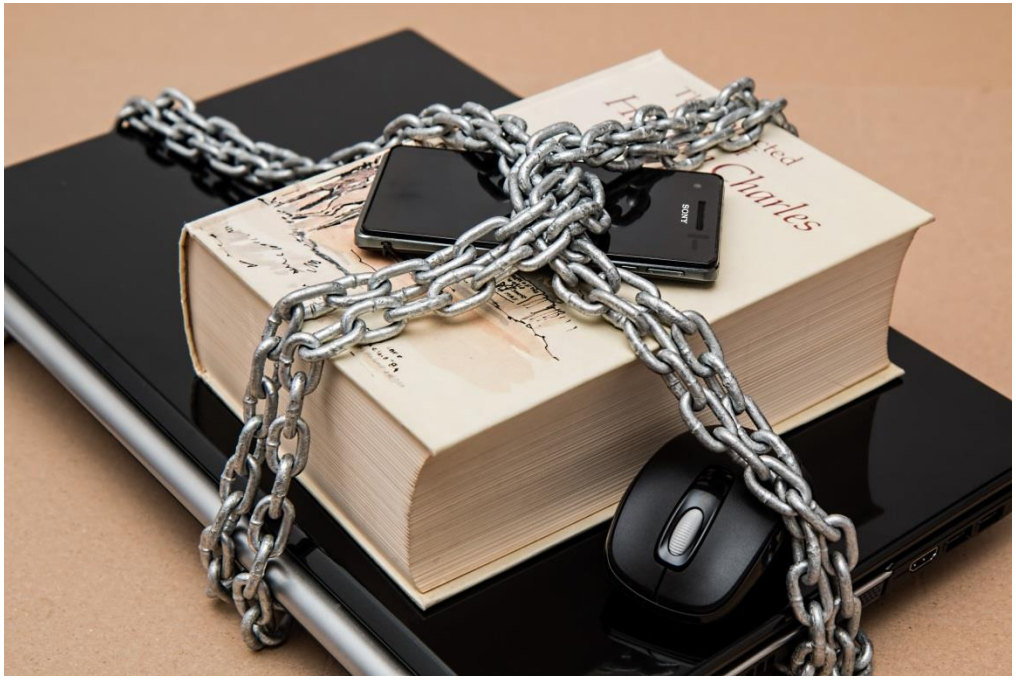
資料外洩事故強制通報

- 事故的性質及可能的後果
- 資料當事人及有關個人資料的類別及大約數目
- 已採取或擬採取的措施，以減低事故造成的不利影響
- 保障資料主任或其他有關人士的聯絡資料

資料外洩事故種類

- **“保密 Confidentiality”**，未經授權或意外洩露或查閱個人資料
- **“可用性 Availability”**，在意外或未經授權的情況下遺失或銷毀個人資料
- **“操守Integrity”**，未經授權或意外更改個人資料

敏感個人資料

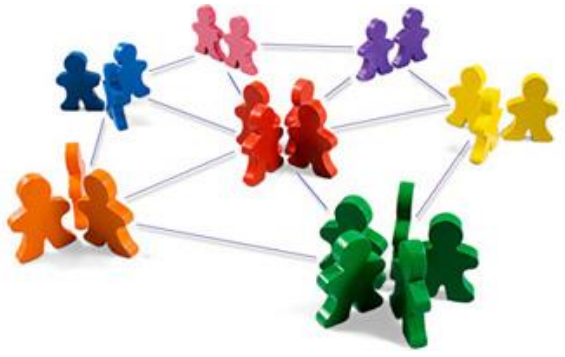


4.敏感個人資料

	歐盟 EU	香港 HK
敏感個人資料 	敏感個人資料的類別被擴大。 只在特定情況下才容許處理敏感個人資料[第9條]	沒有以任何目的區分敏感及非敏感個人資料。

GDPR：敏感個人資料

- 揭示種族或民族本源
- 政治意見
- 宗教或哲學信仰
- 工會會籍
- 健康狀況
- 性生活或
- 性取向的資料，及
- 基因資料或生物辨識資料



（與歐盟指令相比，（間線者）屬新增項目）

更加嚴格的同意

5. 同意

	歐盟 EU	香港 HK
同意 	同意必須是 • 自願給予、具體及知情； • 以聲明或清晰明確的行動不含糊地指明資料當事人的意願， 表示同意處理其個人資料[第4(1)條]；及 • 由16歲（或13歲）以下兒童給予的同意須有家長授權。	同意不是收集個人資料的先決條件，除非個人資料是用於新目的。[保障資料第1及3原則] 在其他情況，若須徵求同意，同意是指自願作出的明示同意。 沒有規定需要家長同意。

同意

❑ 有效同意的例子 [GDPR敘文 32]

- 瀏覽網站的條款及細則時加上剔號
- 為「資訊社會服務」（例如電子商貿企業、提供網上資訊的網上市場、搜尋器提供的互聯網參考服務等）提供技術設定的選擇

❑ 無效同意的例子 [GDPR敘文 32]

- 在空格預設剔號
- 資料當事人保持緘默
- 資料當事人沒有行動

資料處理者的責任

6. 資料處理者的責任

	歐盟 EU	香港 HK
資料處理者 	資料處理者負上額外責任以保存處理記錄、確保處理安全、通報資料外洩事故、委任保障資料主任等。[第30, 32-33, 37條]	資料處理者不是直接受規管。 [第2(12)條] 資料使用者須採取合約或其他方式以確保資料處理者循規。 [保障資料第2(3) 及4(2)原則]

檢視服務合約

- 須委任或揀選在技術性措施及機構性措施方面可提供足夠保證的資料處理者

- 合約要求 [GDPR第28(3)條]
  - 只按控制者的書面指示而處理個人資料；
  - 確保獲授權處理個人資料的人士致力保密或負上適當的法定保密責任
  - 確保所處理的個人資料的安全；
  - 聘用另一處理者時依從指定的條件；
  - 協助控制者回應資料當事人行使GDPR所賦予的權利（例如資料查閱權、修改權等）所作出的要求；
  - 協助控制者遵從資料保安及資料保障影響評估的責任；
  - 在資料處理活動結束後，按控制者的選擇刪除或交還所持有的個人資料， 並刪除現有複本，除非法律規定須儲存有關資料；
  - 向控制者提供能顯示已履行責任所需的資訊，並讓控制者進行審核，包括視察。

資料當事人重掌控制

7. 資料當事人新增及提升的權利

	歐盟 EU	香港 HK
資料當事人新增及提升的權利 	• 就資料處理獲通知的權利 [第13-14條] • 刪除個人資料權（「被遺忘權」）[第17條]	• 對資料使用者／控制者就通知的要求相對未有如此廣泛 • 沒有刪除權，但資料不得保留超過所需的時間 [第26條及保障資料第2(2)原則]

提升就資料處理方面獲通知的權利

- 須以精確、具透明度、容易明白及讀取的方式展示
- 注意：即使資料不是直接從資料當事人收集 **[第14條]**

檢視:

- **收集個人資料聲明**
- **私隱政策及措施**

訂明資訊

- 資料控制者的身份及聯絡資料、保障資料主任（如已委任）的聯絡資料
- 資料處理的目的及基礎（例如處理資料的合法利益）
- 撤回同意的權利（如資料處理是基於同意）及反對有關處理的權利

- 資料接收者的類別
- 保留時期
- 刪除權
- 對個人作出自動化的決策及其背後邏輯
- 向相關資料保障機構投訴的權利

- 提供資料是否屬強制性及不提供的後果
- 司法管轄區之間作出資料轉移的資訊
- 資料來源（如資料非向個人收集）

《擬備收集個人資料聲明及私隱政策聲明指引》

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

擬備收集個人資料聲明及私隱政策聲明指引

引言

本指引旨在為資料使用者在擬備《收集個人資料聲明》及《私隱政策聲明》方面提供參考。《收集個人資料聲明》及《私隱政策聲明》分別是資料使用者依從**《個人資料(私隱)條例》**(「**條例**」)保障資料**第1(3)原則**(「**第1(3)原則**」)及**第5原則**(「**第5原則**」)規定的重要工具。

法律規定

第1(3)原則規定,資料使用者在直接向資料當事人收集個人資料時,須採取所有合理地切實可行的步驟,以確保:

(a) 在收集資料當事人的個人資料之時或之前,以明確或暗喻方式告知資料當事人,他是可以自願或有責任提供該個人資料(如屬有責任,他不提供該個人資料的後果);及

(b) 資料當事人:
(i) 在其個人資料被收集之時或之前,獲明確告知該個人資料將會用於甚麼目的及該個人資料可能轉移予甚麼類別的人;及

(ii) 在個人資料首次被使用之時或之前,獲明確告知他要求查閱及改正該個人資料的權利,及處理向有關資料使用者提出該等要求的個人的姓名(或職

取所有合理地切能確定資料使用務,及獲告知資種類和資料使用會為甚麼主要目

甚麼是個人資料?

根據條例,「**個人資料**」指符合以下說明的任何資料:

(a) 直接或間接與一名在世的個人有關的;
(b) 從該資料直接或間接地確定有關的個人的身份是切實可行的;及
(c) 該資料的存在形式令予以查閱及處理均是切實可行的。

資料使用者經常會特意地收集或查閱各類人士的個人資料,並有意或試圖確定這些人士的身份。在某些情況下,其收集的資料總結起來而可能已經足以識別出個別人士的身份。例如,一間公司追蹤記錄顧客對其產品或服務的消費行為,以便鎖定某類顧客為目標以進行推廣。

甚麼是《收集個人資料聲明》及《私隱政策聲明》?兩者有何分別?

《收集個人資料聲明》(或相等文件)是資料使用者為依從第1(3)原則的通知規定而作出的聲明。雖然條例沒有規定要作出書面通知,但為了提高透明度及避免雙方可能產生誤會,良好的行事方式是以書面向資料當事人提供必要的資訊。

《私隱政策聲明》(或相等文件)一般用以述明資料使用者在處理個人資料方面的私隱政策及實務。儘管條例沒有規定《私隱政策聲明》的形式或展示方式,但良好的行事方式是制訂書面的《私隱政策聲明》,以便有效地傳達資料使用者的資料管理政策及實務。

為依從第1(3)原則,資料使用者在直接向資料當事人收集個人資料之時或之前,應向該資料當事人提供《收集個人資料聲明》。

1 2013年7月

提升刪除的權利（「被遺忘權」）

GDPR的刪除權（亦稱「被遺忘權」）讓個人在指定 情況下有權要求機構／企業刪除其個人資料，包括:

(i) 就收集目的而言，有關個人資料已不再需要;

(ii) 該個人撤回同意;

(iii) 沒有凌駕性的合法利益，或

(iv) 所收集的個人資料是關於接受資訊社會服務的兒童等。

提升刪除的權利（「被遺忘權」）

資料控制者公開披露個人資料(如在互聯網)

通知正處理資料的其他控制者（例如搜尋器）

有關資料當事人所提出關於刪除有關資料的連結或提供複本的要求

提升刪除的權利（「被遺忘權」）

例外情況：

- 為行使表達及資訊自由的權利；
- 為遵從法律責任，或為公眾利益或憑職權而執行的任務；
- 為公眾利益（例如公共健康範疇、管理健康或社會福利系統及服務 等）；
- 為存檔、科學或歷史研究或公眾利益的統計用途；或
- 為確立、行使或維護法律申索

提升反對處理的權利

例子:

透過分析一名人士的上網記錄及購物歷史，預測該人的個人喜好、興趣等。

在GDPR下，個人有權隨時根據下述理由反對處理其個 人資料:

1. 為公眾利益而執行的任務或行使賦予資料控制者的職權；
2. 資料控制者或第三方追尋的合法利益；
3. 直接促銷目的；或
4. 科學或歷史研究目的或統計目的。

提升反對處理的權利

例外情況:

- 資料控制者在收到反對根據上述 (1) & (2): 必須停止處理相關個人資料（包括個人概況彙編），除非它能展 示有力的合法理據，足以凌駕該人的利益、權利及自由，又或是為確 立、行使或維護法律申索，以此維持處理個人資料（包括個人概況彙編）
- (3):純粹為直接促銷目的而處理個人資料，沒有例外情況可適用。
- (4): 可依據其特別的情況而提出反對，除非有關處理是為公眾利益而進行的任務所必需的。

新增權利：資料可攜權

- 這項新增權利可讓個人從一名資料控制者取得其個人資料的複本（須為 具結構性、常用及機器可讀的格式），然後傳送予另一名資料控制者， 條件是：

  (a) 資料處理是按該個人的同意或履行合約作為法律基礎；及

  (b) 資料處理是以自動化方式進行


認證、印章

8. 認證、印章、行為守則及司法管轄區之間的資料轉移

	歐盟 EU	香港 HK
認證、印章及行為守則 	設有明確認可機制以證明資料控制者及處理者合規。[第42條]	沒有正式的認證或私隱印章機制以證明合規。私隱專員在諮詢後可核准實務守則。 [第12條]
司法管轄區之間的資料轉移 	述明認證及依從核准的行為守則作為其中一項資料轉移的法律基礎。[第46條]	認證制度及依從實務守則未有明確定為法律基礎。

懲罰

9. 懲罰

	歐盟 EU	香港 HK
懲罰	資料保障機構獲授權可判處資料控制者及處理者行政罰款。[第58條] 視乎違規的性質，罰款可達二千萬歐元或全球年度總營業額的4%。[第83條]	私隱專員沒有獲賦權施加行政罰款或刑罰。 私隱專員可向資料使用者送達執行通知，在完成司法程序後違法者可能被判罰。 [第50條]

9. 懲罰

- 違反下述規定者可判以最高一千萬歐元，或上一個財政年度的全球年度總營業額的*2%* (以較高者為準）的行政罰款（非詳盡無遺）

(a) 就處理兒童的個人資料取得家長的同意；
(b) 如無必要識別資料當事人，以匿名方式處理個人資料；
(c) 作出資料外洩事故通報；
(d) 進行資料保障影響評估；及
(e) 委任保障資料主任。

- 違反下述規定者可判以最高二千萬歐元，或上一個財政年度的全球年度總營業額的4*%* (以較高者為準）的行政罰款（非詳盡無遺）

(a) 遵從資料處理的基本原則，例如合法及公平地處理或以同意作為基礎而進行處理；
(b) 遵從資料當事人的權利，例如通知權、查閱個人資料權、修訂個人資料權、刪除權（被遺忘權）、反對處理的權利、反對自動化決策（包括個人概況彙編）的權利；及
(c) 依據合法機制把個人資料轉移至第三國的接收者或國際機構。

給企業的實用提示

就資料政策週期進行全面評估

評估與資料處理者訂立的合約

評估資料國際轉移的路徑

評估整體管治權(包括技術性及機構性措施)

典型合規項目 - 可能實施的要求

保存處理活動記錄		更新與僱員有關的文件		更新與顧客有關的文件
更新與醫療/反禁/操守文件	更新網站/應用程式的範本		檢視設立保障資料主任的需要及其擔當的角色	制定資料保障政策及與職系(如人事, IT)有關的指引
制定處理資料外洩事故政策		問責/貫徹私隱的設計工具		資料保障影響評估工具
制定資料保留政策	訂立聘用外判商的程序及處理協議		制定資料轉移及共享指引	就問責制和持續維持提供建議

更多資訊

- 留意GDPR第88條
- 私隱專員發出的歐洲聯盟《通用數據保障條例》小冊子
- 官方網站了解詳情及相關指引 (http://ec.europa.eu/justice/data-protection/index_en.htm)(http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360)
- 網上圖鑑 (http://ec.europa.eu/justice/smedataprotect/index_en.htm)

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

給中小企的建議及協助

Privacy Management Programme

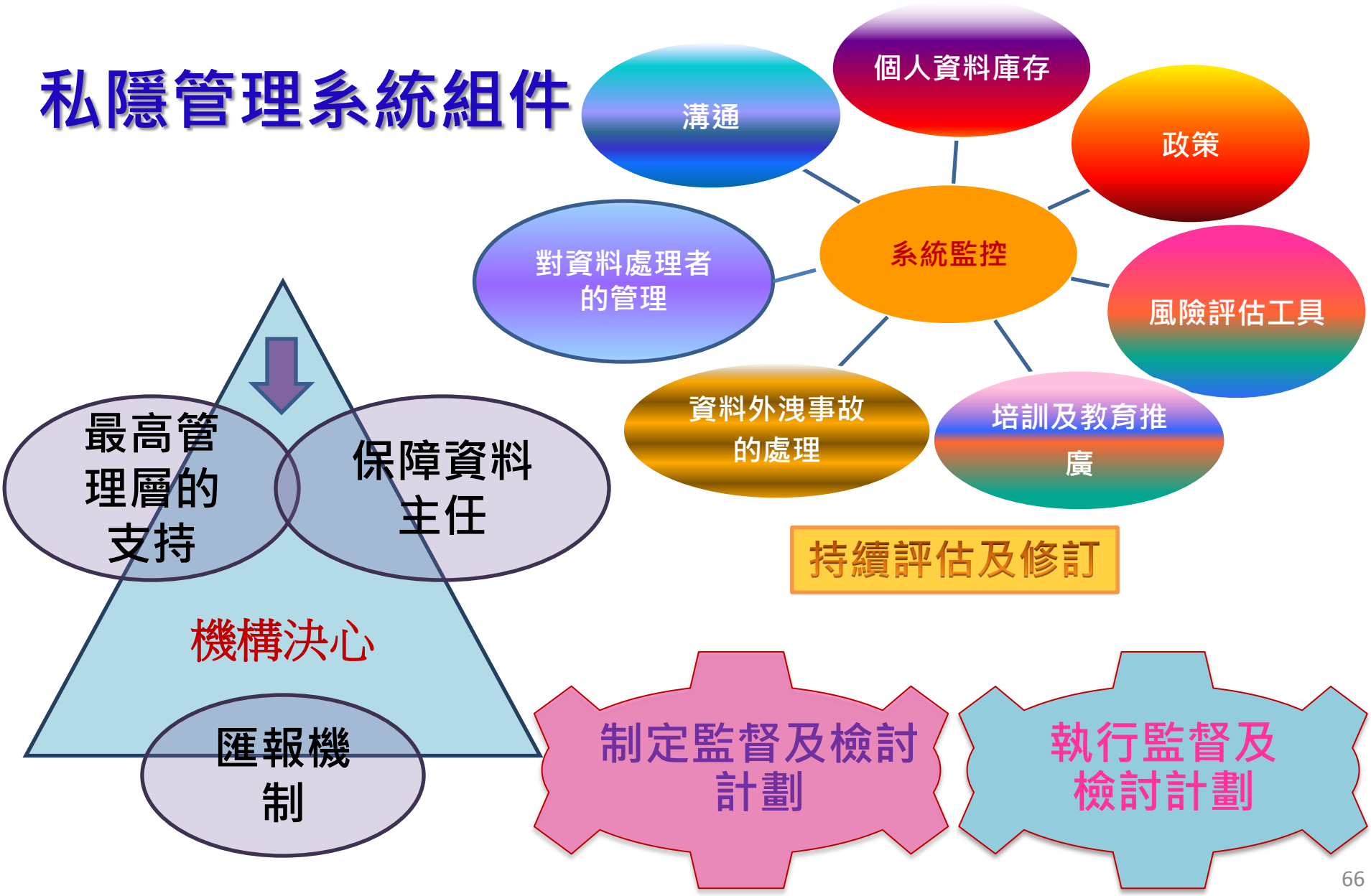
From Compliance to *Accountability*

甚麼是私隱管理系統

模式轉變

符規方式	問責方式
• 被動	主動
• 消極	積極
• 補救	預防
• 以解決問題為本	以符合客戶期望為本
• 由合規部門處理	由最高管理層指派
• 符合法律的最低要求	建立商譽
• 由下而上	由上而下

私隱管理系統組件

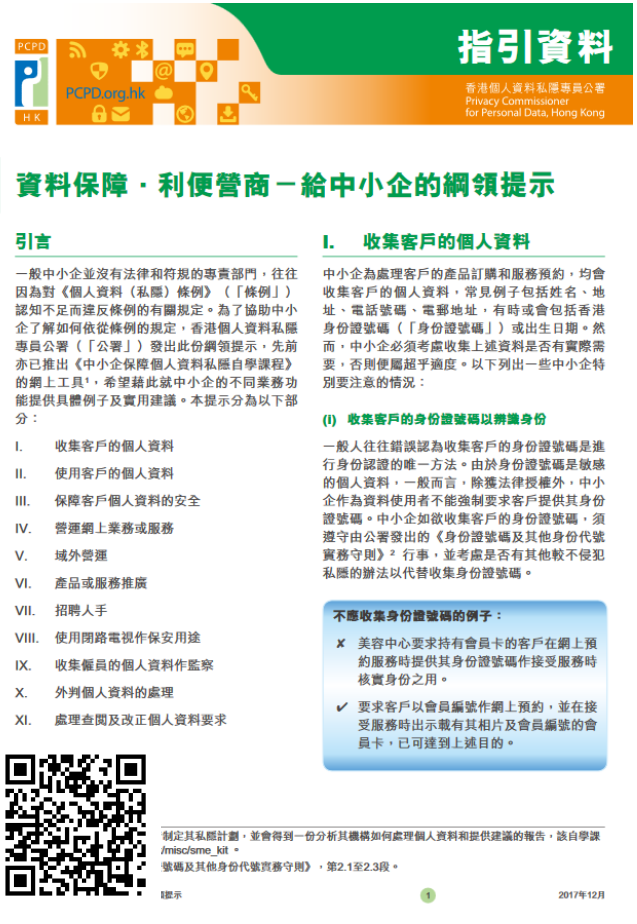

個人資料庫存
溝通
政策
系統監控
對資料處理者的管理
風險評估工具
資料外洩事故的處理
培訓及教育推廣
持續評估及修訂
最高管理層的支持
保障資料主任
機構決心
匯報機制
制定監督及檢討計劃
執行監督及檢討計劃

參與私隱管理系統

承諾機構

- ✓ 76個政府政策局及部門
- ✓ 25間保險公司
- ✓ 9間電訊公司
- ✓ 5間其他行業機構

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－給中小企的網領提示

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」）發出此份網領提示，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。

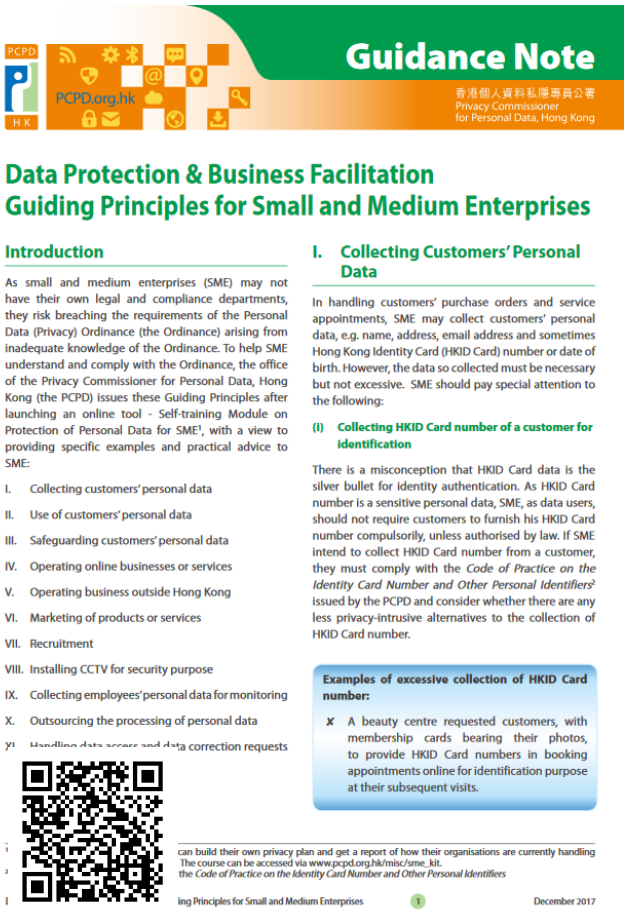
不應收集身份證號碼的例子：

✗ 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] 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，該自學課程可在www.pcpd.org.hk/misc/sme_kit。

[2] 《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

As small and medium enterprises (SME) may not have their own legal and compliance departments, they risk breaching the requirements of the Personal Data (Privacy) Ordinance (the Ordinance) arising from inadequate knowledge of the Ordinance. To help SME understand and comply with the Ordinance, the office of the Privacy Commissioner for Personal Data, Hong Kong (the PCPD) issues these Guiding Principles after launching an online tool - Self-training Module on Protection of Personal Data for SME[1], with a view to providing specific examples and practical advice to SME:

I. Collecting customers' personal data
II. Use of customers' personal data
III. Safeguarding customers' personal data
IV. Operating online businesses or services
V. Operating business outside Hong Kong
VI. Marketing of products or services
VII. Recruitment
VIII. Installing CCTV for security purpose
IX. Collecting employees' personal data for monitoring
X. Outsourcing the processing of personal data
XI. Handling data access 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.

[1] can build their own privacy plan and get a report of how their organisations are currently handling The course can be accessed via www.pcpd.org.hk/misc/sme_kit.

[2] the *Code of Practice on the Identity Card Number and Other Personal Identifiers*

中小企保障私隱活動

- 為中小企編製遵守條例規定資料套
- 加強網上「中小企保障個人資料私隱自學課程」的內容
- 舉辦培訓課程

中小企保障私隱運動
Privacy Campaign for SME

中小企專用諮詢
Dedicated Enquiry Services for SME

2110 1155
sme@pcpd.org.hk

PCPD
HK

PCPD.org.hk

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

重要事項

講座的資訊和建議只作一般參考用途，並非為法例的應用提供詳盡指引。機構 / 企業應按其所需徵詢具體的法 律意見，並對其私隱政策、措施及程序作出適當修訂。


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

PCPD
HK

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

PCPD.org.hk