



保障客戶及僱員個人資料講座

提升中小型企業營商優勢

2018.12.17





保障客戶及僱員 個人資料

提升中小型企業 營商優勢

2

PCPD



H K

PCPD.org.hk

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



● 營商環境
不斷改變

● 資源有限

● 企業管治
架構薄弱

● 支援不足

● 員工培訓
不足

● 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



內容

- 第一部: 簡介
- 第二部: 妥善處理客戶個人資料
- 第三部: 產品或服務推廣
- 第四部: 人力資源管理方面事宜
- 第五部: 安裝閉路電視
- 第六部: 外判個人資料的處理
- 第七部: 資料外洩事故的處理
- 第八部: 在香港以內/外營運網上業務或服務
- 第九部: 建立私隱管理系統



第一部：簡介

PCPD



H K



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

《個人資料(私隱)條例》

- 1996年12月20日生效，根據國際認可的保障資料原則制訂
- 立法目的：保障個人資料方面的私隱，便利營商環境
- 2012年條例作出重大修訂，包括訂定條文，以規管在直接促銷中使用個人資料
- 公署致力進行推廣、監察及監管工作，促使各界人士遵從條例的規定，確保市民的個人資料私隱權得到保障



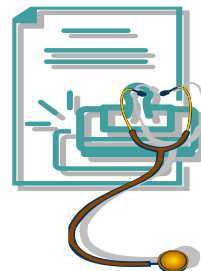
條例內的詞彙定義

「個人資料」須符合以下三項條件：

- (1)直接或間接與一名在世人士有關
- (2)從該等資料直接或間接地確定有關的個人的身分是切實可行的；而
- (3)該等資料的存在形式令予以「查閱」及「處理」均是切實可行的

個人資料的例子

- 包括個人姓名、電話號碼、地址、出生日期、相片、身份證號碼、銀行戶口號碼、信用卡資料等



誰是資料當事人？

- 資料當事人是指屬該個人資料的當事人的在世人士
- 根據條例，已故人士不是資料當事人



誰是資料使用者？

- 資料使用者是獨自或聯同其他人操控個人資料的收集、持有、處理或使用的人士
- 即使個人資料處理程序外判，資料使用者亦須為承辦商的錯失負上法律責任



條例下六項保障資料原則

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，而不超乎適度。

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



資料使用者須確保保存的個人資料準確無誤。資料的保留時間不應超過達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達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.



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



第二部： 妥善處理客戶 個人資料

PCPD



H K



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

(I) 收集客戶的個人資料

可否收集客戶的身份證
號碼作接受服務時核實
身份之用？



《身份證號碼及其他身份代號實務守則》

- 第 2.2.1 段 – 考慮是否有其他較不侵犯私隱的辦法代替收集身份證號碼
- 第 2.3.1 段 – 除非根據法定條文而獲授權，否則不可收取身份證號碼



個人資料(私隱)條例 身份證號碼及 其他身份代號 實務守則

二零一六年四月(第一修訂版)



例子分享



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

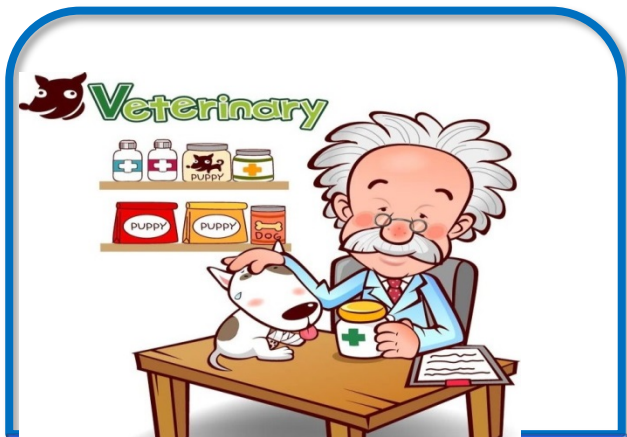


代替方法：要求客戶以會員編號作網上預約，並在接受服務時出示載有其相片及會員編號的會員卡，已可達到上述目的



15

例子分享



獸醫診所為識辨貓主的身份，以便日後跟進其貓隻的健康狀況而收集購買貓糧的貓主的身份證號碼



- name



代替方法：收集貓主的姓名及聯絡電話號碼已可達到上述目的



16

(I) 收集客戶的個人資料

可否收集客戶的出生日期
以提供針對其年齡的服務
及生日優惠？



17

(I) 收集客戶的個人資料



收集客戶的年齡或年齡組別
(例如40-50歲)



收集客戶的出生月份或出生月份
及日子

(I) 收集客戶的個人資料

根據私隱條例，在收集客戶資料前須向客戶提供甚麼資訊？



19

《收集個人資料聲明》

向客戶收集個人資料時，須告知他們以下各項資訊：

- (a) 收集資料的目的；
- (b) 資料可能會轉移給甚麼類別的人；
- (c) 資料當事人是否有責任抑或是可自願提供資料；
- (d) 如資料當事人有責任提供該資料，他拒絕提供資料所需承受的後果；及
- (e) 他有權要求查閱及要求改正自己的個人資料及提供處理有關要求的人士的職銜及地址。

實用建議



以書面向客戶提供《收集個人資料聲明》，並以易於閱讀的方式設計 (包括字體大小和行距，並適當地運用亮點)



清晰地顯示《收集個人資料聲明》，例如將它分開印刷為一份獨立通告或將它作為申請表格的一部分



使用易於理解的語言，例如選用簡單的字詞



於申請表格上列明哪些項目是為提供其服務或產品而必須收集及屬自願提供

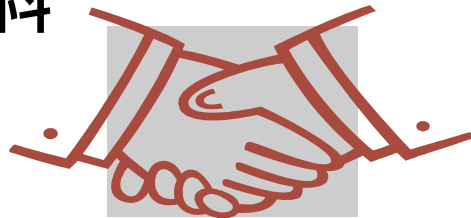


收集目的聲明及資料承讓人類別不應過於含糊及範圍太廣

21

(III) 使用客戶的個人資料

- 如無客戶的明確同意，其個人資料只限用於收集時述明或直接相關的目的。
- 在提供售後服務或處理客戶投訴時，避免在過程中不當收集或披露客戶的個人資料



例子分享



美容中心將原本為提供美容服務而收集的客戶個人資料轉售予另一間美容中心圖利



PROMOTION

喜帖印刷公司擅自將客戶自行設計並載有其個人資料的喜帖展示於門市的樣版架上，以收宣傳之效



23

(III) 保障客戶個人資料的安全

- 根據資料的敏感度及其他實際情況，採取合適的保安措施保障個人資料，以防意外遺失或被未獲授權人士查閱



例子分享



診所遺失病人的病歷檔案，但無法確定最後接觸該病歷檔案的人是誰及遺失的原因



診所應派員於每天休診後檢查當日曾經取出的病歷檔案是否已放回原處，以及規定職員在非應診的情況下取出病歷檔案須作出記錄



25

例子分享



眼鏡店因為登記表格用罄而要求客戶將其資料寫在廢紙上，該客戶其後發現廢紙背面載有另一名客戶的個人資料



POLICY

眼鏡店應停止用載有個人資料的廢紙，並制訂使用環保紙的政策供僱員依循



26

PCPD.org.hk

指引資料

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

資料使用者如何妥善處理改正資料要求



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

查詢：香港個人資料私隱專員公署
Enquiry: Personal Data Commissioner

PCPD.org.hk

指引資料

定及處理改資料要求的步驟

如使用者收到任何改資料的要求後，可採取四個步驟如下處理有關要求：

- 一、評定收到的資料提供條款的改資料要求。
- 二、核實改資料要求的身份及所附的證據。
- 三、評定改資料要求的內容，及決定決定依從或拒絕從有改資料要求。
- 四、評定收到的是否應提供條款的改資料要求。

資料使用者如何妥善處理查閱資料要求及收取查閱資料要求費用

摘要

本指引主要涵蓋以下四個範疇：

- 一 查閱查閱資料要求
 - 查閱資料要求一是指由一名人士（「查閱資料要求者」）要求某資料使用者提供他的個人資料權利。
- 二 對查閱資料要求
 - 資料使用者收到查閱資料要求時：
 - 應清楚查閱資料要求者的身份；
 - 對查閱資料要求者有合理的個人資料；
 - 資料使用者應告知有關的個人資料，必須在收到查閱資料要求後40個日內，以書面查閱資料要求的申請清楚陳述明白的個人資料提供。
 - 如資料使用者並無持有該資料，他們須於40日的期限內以書面通知查閱資料要求者沒有該資料的資料。
- 三 對拒絕查閱資料要求而收費
 - 資料使用者可為收取查閱資料要求而收取不超過規定的費用，並應於40日內清楚告知查閱資料要求者應收取多少費用。
 - 被視為合理程度，或足以收回查閱資料要求直接有關及必需的收費，如：
 - 收取超出規定查閱資料要求的成本；
 - 由於資料使用者方面特別特殊的情況而令為提供查閱資料要求而排除的成本超出正常情況下的成本；
 - 資料使用者要求法律意見或成立裁決或購買資料研究的費用而排除的成本；
 - 提供資料的行政或合規性費用。
 - 資料使用者不得拒絕或延誤有關的個人資料而執行機械性工作的成本。
- 四 拒絕提供查閱資料要求
 - 資料使用者必須通知拒絕查閱資料要求，並：
 - 應清楚告知與資料以與查閱資料要求者的身份；
 - 不披露最近查閱的個人資料和申請或拒絕情況；
 - 拒絕提供資料時及時及理由或此後如何處理。
 - 資料使用者不得在提供查閱資料要求後40日內以書面拒絕查閱資料要求者，並應拒絕提供的原因，並應於規定期限內存檔。

詳細資料請參閱本指引內容。

如使用者收到任何改資料的要求後，可採取四個步驟如下處理有關要求：

- 一、評定收到的資料提供條款的改資料要求。
- 二、核實改資料要求的身份及所附的證據。
- 三、評定改資料要求的內容，及決定決定依從或拒絕從有改資料要求。
- 四、評定收到的是否應提供條款的改資料要求。

例下的改資料要求是為查閱資料使用者已提供查閱資料要求一是指由一名人士（「查閱資料要求者」）要求某資料使用者提供他的個人資料權利。資料使用者認為資料根本有不便披露之處，而拒絕提供該資料的要求。

真的改資料要求者給予他查閱資料使用者應考慮改其個人資料提供他的個人資料權利，以及資料。



QR Code

資料使用者可要求查閱資料要求及收取查閱資料要求

10-16888



個人資料(私隱)條例

查閱資料要求表格

致查閱資料要求者的重要通告

1. 請在填寫本表格前，細閱本表格的內容及註釋。如本表格載有《個人資料(私隱)條例》(下稱「本條例」)的有關規定的摘要，該摘要只作參考之用。關於法例的詳細及明確內容，請參閱本條例的條文。
2. 本表格是個人資料私隱專員(下稱「專員」)根據本條例第 67(1)條所指明的，其生效日期為 2012 年 10 月 1 日。如你不採用本表格來提出查閱資料要求(下稱「你的要求」)，資料使用者可拒絕依從你的要求(見本條例第 20(3)(e)條)。
3. 請以中文或英文填寫本表格。如你的要求不是以中文或英文作出，資料使用者可拒絕依從你的要求(見本條例第 20(3)(a)條)。
4. 查閱資料要求必須由你作為資料當事人或由本條例第 2 條或 17A 條所指的「有關人士」(請參閱本表格第 III 部)提出。
5. 你沒權查閱不屬於你的個人資料或不屬個人資料的資料(見本條例第 18(1)條)。資料使用者只須向你提供你的個人資料的複本，而不是載有你的個人資料的文件的複本。在大多數情況下，資料使用者或選擇提供有關文件的複本。如你所要求的個人資料是以錄音形式記錄，資料使用者可提供該段載有你的個人資料的錄音複本。
6. 你必須在本表格內清楚及詳細地指明你所要求的個人資料。如你未能向資料使用者提供他為找出你所要求查閱的個人資料而合理地要求的資訊，資料使用者可拒絕依從你的要求(見本條例第 20(3)(b)條)。如你為使資料使用者依從你的要求而在本表格內提供虛假或有誤導性的資訊，可構成犯罪(見本條例第 18(5)條)。
7. 請勿把本表格送交專員。填寫的表格應直接送交資料使用者，以作出你的要求。
8. 資料使用者可要求你提供身分證明，例如香港身分證，及向你收取依從查閱資料要求的費用(見本條例第 20(1)(a) 及 28(2)條)。
9. 資料使用者在本條例第 20 條指定的情況下可拒絕依從你的要求。

致資料使用者的重要通告

1. 你必須根據本條例第 19(1) 條的規定，在收到查閱資料要求後的 40 日內，依從該項要求。依從查閱資料要求是指：(a)如你持有所要求的資料，以書面告知查閱資料要求者你持有該資料及提供一份該資料的複本，或(b)如你並無持有所要求的資料，以書面告知查閱資料要求者你並無持有該資料(除了香港警務處可以口頭告知查閱資料要求者它並無持有他的任何刑事犯罪紀錄)，僅是向查閱資料要求者發出收取所要求的資料的通知或向要求者發出應費通知是不足夠的。在依從要求時，你應刪除或不披露資料當事人外，其他人士的姓名或可識別該些人士的身分的資料。
2. 如你不能於 40 日內依從該項查閱資料要求，你必須在 40 日的期限內以書面通知該查閱資料要求者有關情況及原因，並在你能依從該項查閱資料要求的範圍(如有的話)內，依從該項查閱資料要求。你其後必須在切實可行的範圍內盡快依從或盡快完全依從(視屬何情況而定)該項查閱資料要求。(見本條例第 19(2)條)
3. 如你依據本條例第 20 條有合理理由拒絕依從該項要求，你必須於上述 40 日期間內，以書面通知該查閱資料要求者你拒絕依從該項查閱資料要求及說明理由(見本條例第 21(1)條)。
4. 不根據本條例規定依從查閱資料要求即屬犯罪。資料使用者一經定罪，可處第 3 級罰款(現時為 10,000 港元)(見本條例第 64A(1)條)。
5. 你可就依從查閱資料要求收取費用，但本條例第 28(3)條訂明：「為依從查閱資料要求而徵收的費用不得超乎適度」。就資料使用者收取查閱資料要求費用方面，本條例未有對「超乎適度」一詞下定義。根據行政上訴案件第 37/2009 號的判決所訂立的原則，資料使用者只可收取與依從查閱資料要求「直接有關及必需」的費用。
6. 在以下情況，你須拒絕依從查閱資料要求——
 - (a) 你不獲提供你合理地要求——
 - (i) 以令你信納提出要求者的身分的資訊；
 - (ii) (如提出要求者看來是就另一名個人而屬有關人士)以令你——
 - (A) 信納該另一名個人的身分；及
 - (B) 信納提出要求者確是就該另一名個人而屬有關人士，的資訊；
 - (b) (在符合本條例第 20(2)條的規定下)你不能在不披露一名個人屬其資料當事人的個人資料的情況下依從該項要求；但如你信納該另一名個人已同意向該提出要求者披露該等資料，則屬例外；或
 - (c) (在其他情況下)在當其時，依從該項要求根據本條例或任何其他條例是被禁止的。(見本條例第 20(1)條)



第三部： 產品或服務推廣

PCPD



H K



PCPD.org.hk

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

(i) 直接促銷

- 條例中的直銷活動包括向特定人士以郵遞、圖文傳真、電子郵件及電話進行的直銷活動
- 現行條例規定凡資料使用者在首次使用個人資料於直銷活動，須提供一個「拒收直銷訊息」的選擇予當事人
- 如當事人表示拒絕再接收有關的直銷資料，資料使用者須在不收費的情況下照辦

直接促銷新規管機制

於2013年4月1日生效

擬用客戶個人
資料作直銷用
途或轉交另他
人作直銷用途

資料使用者

通知

資料當事人

同意

提交個人資料

- 提供「訂明資訊」及回應途徑，讓資料當事人選擇同意或表示「不反對」個人資料被用作直銷
- 通知必須清楚易明

- 必須自願和清晰作出
- 不反對也屬同意

31

直接促銷新規管機制

於2013年4月1日生效

訂明資訊：

擬用客戶個人資料作直銷用途	擬轉交客戶個人資料給他人作直銷用途
1) 擬在直接促銷中使用該資料當事人的個人資料	1) 資料使用者擬將資料當事人的個人資料提供予另一人，以供該人在直接促銷中使用
2) 除非收到資料當事人的同意，否則不得如此使用該資料	2) 須收到資料當事人提供的書面同意，否則不得如此提供該資料
3) 擬使用的個人資料的種類	3) 該資料是擬為得益而提供的
4) 該資料擬就甚麼類別的促銷標的而使用	4) 擬提供的個人資料的種類
5) 提供一個回應途徑	5) 該資料擬提供予甚麼類別的人士
	6) 該資料擬就甚麼類別的促銷標的而使用
	7) 提供一個回應途徑

32

「同意」包括表示「不反對」

一般性不反對的例子：

「我們擬使用你的姓名、電話號碼及地址以促銷信用卡及保險產品／服務，但我們在未得到你的同意之前不能如此使用你的個人資料。」

請在本文最後部份表示你同意如此使用你的個人資料。如你不同意，請在以下空格加上「✓」號，然後簽署。

☐ 本人(姓名如下)反對使用個人資料於擬作出的直接促銷。」

客戶簽署

姓名：xxx

日期：年/月/日

交回已簽名的服務申請表格，但沒有剔選方格以表示
反對資料被用作直銷 = 同意

33

直接促銷新規管機制：嚴懲違例者

	最高罰款	監禁最高年期
未依例行事	50萬元	3 年
賣資料予他人直銷用途，而未有依例行事	100萬元	5年

協助資料使用者的指引

- 出版《直接促銷新指引》為進行直銷的資料使用者提供指引
- 專業研習班，協助機構熟悉新條文及循規措施。歡迎個人資料保障主任、負責合規事務的專業人士、律師和市場推廣從業員參加



(ii) 從公共領域取得的個人資料

- 透過公共登記冊、公共搜尋器等公共領域查閱及取得他人的個人資料以尋找目標客戶時，須留意：
 - 該等資料存放於公共領域的**原來使用目的**；
 - 使用的**限制**(如有)；及
 - 資料當事人在個人資料私隱方面的**合理期望**

(iii) 使用社交網站及手機應用程式作推廣 實用建議



透過社交網絡舉辦抽獎活動或問答遊戲，不應要求網民以留言形式公開提供個人資料



透過《私隱政策聲明》清楚列明會向用家讀取、使用、傳輸及分享甚麼資料，並提供足夠資訊來說服用家該程式為何需要讀取相關的個人資料



第四部： 人力資源管理 方面事宜

PCPD



H K



PCPD.org.hk

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

(i) 招聘人手

- **不應**向求職者收集超乎招聘所需的個人資料
- 在求職者接受聘任之前，**不應**收集其身份證副本
- 述明僱主身份及有關資料的擬使用目的
 - 提供《收集個人資料聲明》
- 保留落選求職者的個人資料不多於2年
- 在使用求職者的個人資料前存有疑慮，應取得他們的口頭或書面同意
- 妥善保障資料的安全
- 依從求職者作出的查閱及改正資料要求



個人資料(私隱)條例 人力資源管理 實務守則

二零一六年四月(第一修訂版)



39

不公平收集個人資料例子 – 匿名廣告

公司助理

- 中五或以上程度
- 熟悉公司秘書職務

請將履歷寄往郵政信箱第100號

- 要求求職者提供個人資料
- 沒有提供僱主身分

公司助理

- 中五或以上程度
- 熟悉公司秘書職務

有興趣人士可致電 2808-2808 與
人力資源部主任陳安琪小姐聯絡

- 沒有要求求職者提供個人資料
- 提供聯絡人姓名，以便求職者
 - 詢問僱主身分
 - 詢問目的聲明方面的資料

(ii) 收集僱員的個人資料作監察

- 科技進步有助僱主更方便及更有效益地監察僱員
- 考慮因素:
 - 1) 監察是否**必需**?
 - 2) 有沒有其他**較不侵犯私隱**的選擇?
 - 3) 有否與受影響人士進行有效**溝通**?
 - 4) 有否定期進行**審核及檢討**?

常見監察方法

- 收集電話及互聯網使用記錄
- 電子郵件監察
- 閉路電視



僱主可否使用指紋辨識系統
監察僱員出勤紀錄？



例子分享



甜品專門店為考勤目的
收集僱員的指紋資料



僱主應提供除收集指
紋資料以外其他較不
侵犯私隱的替代方法
供僱員選擇 (如電腦打
咭系統)



例子分享



高級時裝公司為防盜目的，要求進出陳列室的僱員提供指紋資料



一般的門鎖、密碼鎖及鏈鎖已能達至防止盜竊的效果。如為追查失竊事件用途，則安裝閉路電視鏡頭看來是更有效的保安方法



44



第五部： 安裝閉路電視

PCPD



H K



PCPD.org.hk

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

私隱條例有否禁止
安裝閉路電視？



PCPD



H K



PCPD.org.hk

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

東周刊 vs 香港個人資料私隱專員公署



47

收集個人資料的要素

➤ 資料使用者 -

- 藉此匯集一名已辨識其身份的人士；或
- 設法或欲辨識該名個人的身份
- 視該名人士的身份為重要的資訊

使用拍攝裝置的建議



應在受閉路電視監察範圍內及入口處放置明顯的告示，並說明監察的特定目的



在沒有充分的理據下，不應採用隱藏式的閉路電視進行監察影像及錄影



定期以不可逆轉及安全方式刪除閉路電視片段，除非有關片段需用作特定用途



影像及錄影只可用於在收集資料時所述明的用途或與其直接有關的用途



為防止影像及錄影遭未獲授權的查閱，必須採取保安措施



確保相關職員獲悉及依從所訂立的政策及指引，並定期進行循規審查及覆核



第六部： 外判個人資料的處理

PCPD



H K



PCPD.org.hk

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

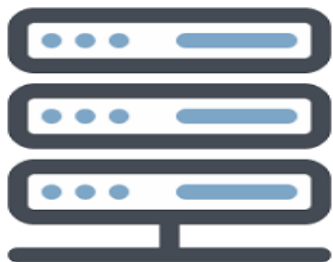
外判個人資料的處理

- 中小企須為所聘用的資料處理者的行為負責
(條例第65條)
- 必須採取合約規範方法或其他方法，限制轉移予資料處理者的個人資料：
 - 保存期超過處理該資料所需的時間；
 - 受到未獲准許或意外地被查閱、處理、刪除、喪失或使用所影響；及
 - 不得為受託目的以外的其他目的使用或披露



51

例子分享



僱傭公司聘請外判維修員維修電腦，該維修員因疏忽將載有客戶資料的文件夾上載到伺服器，令公眾可於互聯網搜尋及取覽客戶資料



該僱傭公司須為該外判商的資料外洩事故負責。他們應透過合約規範方法防止轉移予外判商的個人資料受未獲准許或意外的查閱



52



第七部： 資料外洩事故的處理

資料外洩事故的處理及通報

資料外洩事故例子：

- 遺失儲存的個人資料：如USB記憶體、手提電腦等
- 不當處理個人資料：如把資料錯誤地發給他人
- 載有個人資料的資料庫被黑客入侵

資料外洩事故的處理



立即收集資料

立即收集有關資料外洩事故的重要資料，包括：

- 事故於何時及何地發生？
- 事故如何被發現及由誰人發現？
- 事故的肇因是甚麼？
- 涉及甚麼種類的個人資料及範圍有多大？
- 受影響的資料當事人有多少？

資料外洩事故的處理



遏止措施可包括：

- 如資料外洩是系統故障造成，應停止有關系統的操作
- 更改用戶密碼及系統配置，以控制查閱及使用資料
- 考慮是否需要尋求技術協助，以修補系統上的漏洞及 / 或阻止黑客入侵
- 停止或更改涉嫌作出或導致資料外洩的人士的查閱權
- 如犯罪活動已發生或相當可能發生，應通知有關執法部門
- 保留資料外洩的證據以協助調查
- 指示資料處理者立即採取補救措施及將進度告知資料使用者(如適用)

資料外洩事故的處理



評估損害

評估資料外洩事故可造成的損害，如：

- 人身安全受到威脅
- 身份盜竊
- 財務損失
- 受辱或喪失尊嚴、名譽或關係受損
- 失去生意或聘用機會

資料外洩事故的處理



考慮作出通報

在資料外洩事故中，如可以合理地估計實在的傷害風險，資料使用者應考慮：

- 通知資料當事人及相關人士
- 不作出資料外洩通知的後果



第八部： 在香港以內/外 營運網上業務或服務

PCPD



H K



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

經互聯網收集、展示或傳輸個人資料

進行網上買賣時，應使用較不侵犯私隱的身份認證方法：



網上商店要求顧客訂貨時提供其身份證號碼，供職員在顧客提貨時核對身份之用



商店可在顧客訂貨時向他提供一個獨一無二的訂單號碼，要求顧客憑訂單號碼提貨

保護你的網站實用建議



安裝防毒軟件、防火牆和最新的修補程式，以避免網絡系統、伺服器及應用程式受病毒及惡意程式碼入侵



當執行數據傳送、處理或儲存時，要將敏感的數據加密



定期以不可逆轉及安全方式銷毀經網站收集的個人資料



如聘用外判公司管理網站，應選擇信譽良好的公司

開拓內地或海外市場



《中華人民共和國網絡安全法》

➤ 於2017年6月1日正式實施



《通用數據保障條例》

(General Data Protection Regulation)

➤ 於2018年5月25日正式實施

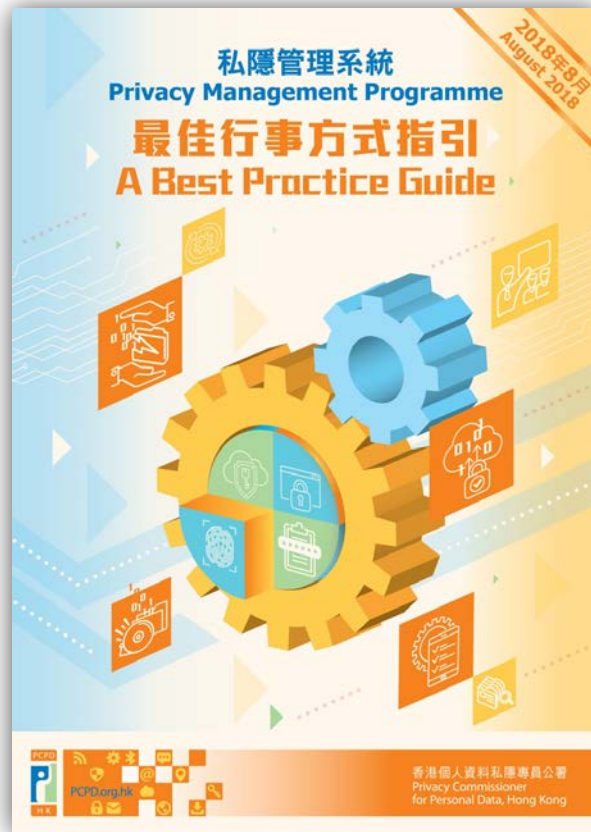


第九部： 建立私隱管理系統

私隱管理系統

(Privacy Management Programme)

私隱專員提倡各機構建立自己的**私隱管理系統**，由最高管理層做起，將個人資料保障視為其**企業管治責任**，並將之納入處理業務中不可或缺的一環，**由上而下**貫徹地在機構中執行有關保障個人資料的政策



為中小企編制之指引資料



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規定的專責部門，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」）推出此套綱領提示，先將已推出《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理
- X. 外判個人資料的處理
- XI. 處理查詢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，有時還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。由於身份證號碼是極敏感的個人資料，一般而言，除法律規定外，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辨識號碼的辦法》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/mis/ucme.htm。

² 請參閱公署發出的《身份證號碼及其他身份辨識號碼守則》，第2.1及2.3段。



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 SME¹, with a view to providing specific examples and practical advice to SMEs.

- 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 to 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 Identifiers² 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 Upon completion of the course, SME can build their own privacy plan and get a report of how their organisations are currently handling personal data with recommendations. The course can be accessed via www.pcpd.org.hk/mis/ucme.htm.

² Please refer to paragraphs 2.1 to 2.3 of the Code of Practice on the Identity Card Number and Other Personal Identifiers.

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



H K



PCPD.org.hk

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

關於公署 | 私隱條例 | 資訊及活動 | **查及執法** | 投訴 | 法律協助 | 教育及培訓 | 資源中心 | 查詢






專員的決定

法庭裁決

行政上訴委員會的裁決

個案簡述

資料外洩事故通報

就私隱事宜提交的文件

諮詢

資源中心 | 查詢

刊物

多媒體

行業資源

按題目分類的資源

常見問題

銷售刊物

關鍵字搜尋

RSS

A A A

Eng

更多

主組就許智峯議員事件會面

「保障私隱 坐言起行」

啟動中小企保障私隱運動 凝聚智慧 創建優勢

私隱專員公署獲僱員再培訓局嘉許為「人才企業」

聘任副個人資料私隱專員及助理個人資料私隱專員

私隱專員就許智峯議員公開查詢的回應

關於立法會綜合大樓內監察及記錄個別議員的行蹤以及政府人員手提電話被取事件

私隱專員回應有關香港寬頻一宗懷疑客戶資料庫遭入侵事件

個人

網上私隱有法保

明智使用電腦及互聯網

精明使用社交網

身分證號碼與你的私隱

機構

歐盟《通用數據保障條例》

開發流動應用程式

專業研習班

網上課程

歐洲聯盟
《通用數據保障條例》
2016 (於2018年5月25日生效)

《歐洲聯盟《通用數據保障條例》
2016》小冊子

香港個人資料私隱專員公署



- ❑ 查詢熱線 - 2827 2827
- ❑ 傳真 - 2877 7026
- ❑ 網址 - www.pcpd.org.hk
- ❑ 電郵 - enquiry@pcpd.org.hk

❑ 地址 - 香港灣仔皇后大道東248號陽光中心13樓1303室