

工業貿易署
中小企業支援與諮詢中心

2019年5月27日



保障客戶個人資料 創建營商優勢

PCPD



H K



PCPD.org.hk

est.1996

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：在香港以內/外營運網上業務或服務

第八部：比較《通用數據保障條例》與
《私隱條例》



第一部：簡介

《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：

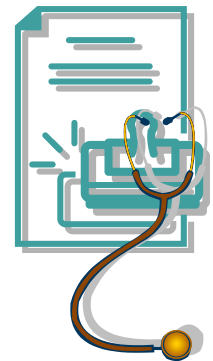
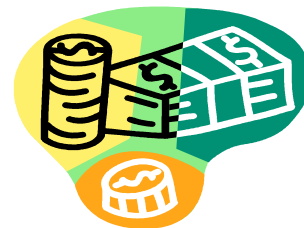
(1)直接或間接與一名在世人士有關

(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持有的個人資料準確無誤，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.

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

PCPD



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



第二部： 妥善處理客戶 個人資料

(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

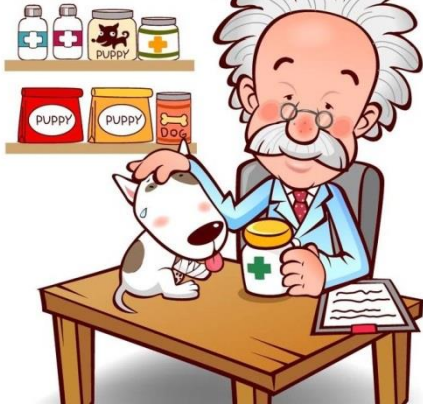


代替方法：要求客戶以會員編號作網上預約，並在接受服務時出示載有其相片及會員編號的會員卡，已可達到上述目的



例子分享

 Veterinary



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
糧的貓主的身分證號碼



- 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



(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？



(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？



《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

(II) 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



(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



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



(IV) 處理查閱及改正個人資料要求

• 條例賦予客戶或僱員有權：-

(a) 要求查閱自己的個人資料；
資料使用者可收取不超乎適度的費用

(b) 要求改正自己的個人資料

資料使用者如何妥善處理改正資料要求

引言

在《個人資料(私隱)條例》(第486章) (「條例」) 下，資料使用者有責任確保其持有的個人資料是準確的。故此，資料使用者在依從資料當事人(或代表該名資料當事人的「有關人士」) 所提出的查閱資料要求¹ 提供其資料的複本後，

評定及處理改正資料要求的四個步驟

資料使用者收到任何改正資料的要求後，可循以下四個步驟評定及處理有關要求：

- 步驟一：評定收到的是否條例釋義下的改正資料要求；
- 步驟二：核實改正資料要求者的身份及所稱的權限；
- 步驟三：評定改正資料要求的內容；及
- 步驟四：決定應依從或拒絕依從有關改正資料要求。

指引資料

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：

- 甚麼是查閱資料要求**
查閱資料要求一般是指一名個人(「查閱資料要求者」) 要求某資料使用者提供他的個人資料複本。
- 依從查閱資料要求**
 - 資料使用者收到查閱資料要求時：
 - 應確查查閱資料要求者的身份；
 - 評估是否正持有相關的個人資料。
 - 資料使用者若持有相關的個人資料，必須在收到查閱資料要求後40個曆日內，按查閱資料要求者的要求提供清楚易辨的個人資料複本。
 - 如資料使用者並無持有所要求的資料，他們須於40日的期限內以書面通知查閱資料要求者沒有其所要求的資料。
- 為依從查閱資料要求而收費**
 - 資料使用者可為依從查閱資料要求而徵收不超乎適度的費用，並應儘快在40日內清楚告知查閱資料要求者將收取多少費用。
 - 被視為超乎適度，或並非與依從查閱資料要求直接有關及必需的收費，如：
 - 收取超出依從查閱資料要求的成本；
 - 由資料使用者某方面引起特殊的情況而令為依從查閱資料要求而預設的成本超出在正常情況下的成本；
 - 資料使用者尋求法律意見或由顧問或職員研究條例的構成而預設的成本；
 - 經常性的行政或辦公室開支費用；
 - 購買的個人資料而執行機械工作所涉及的成本。



資料要求，若：
1. 查閱資料要求者的身份；
2. 便無法依從該要求；
3. 條例或其他法例所禁止。
4. 要求後40日內以書面回覆查閱資料要求者，延遲拒絕依從的理

詳細資料請參閱本指引內容。

第1頁

1

2018年3月



見改
求
詳
以

編
制
部
別

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帶本。
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。填妥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繳費通知是不足夠的。在依從要求時，你應刪除或不披露除資料當事人外，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 條有合法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述明理由(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

(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



提交個人資料

- | | |
|--|---|
| <ul style="list-style-type: none">▪ 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 | <ul style="list-style-type: none">▪ 必須自願和清晰作出▪ 不反對也屬同意 |
|--|---|

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

「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，協助機構熟習新條文及循規措施。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

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

Office of PCPD
Guidance Note
JO: 38896M0
1P*110113
B1

直接促銷指引

第1部：導言

指引目的

1.1 直接促銷在香港是常見的商业活動，一般是指機構收集及使用市民的個人資料以向資料當事人促銷產品或服務，某些機構會將收集所得的個人資料交給他人作直接促銷之用。在上述直銷活動中的資料使用者必須遵從《個人資料(私隱)條例》(下稱「**條例**」)的規定。個人資料私隱專員(下稱「**專員**」)發出本指引，向資料使用者提供實務性指引，以遵從條例下新增的第VIA部(有關直接促銷的新規定)，並協助資料使用者全面了解其責任和推廣良好行事方式。資料使用者亦應參考其他不抵觸條例規定而關乎直接促銷的法例、規例、指引及實務守則。

1.2 本指引將於條例第VIA部實施日期起同日生效(下稱「**生效日期**」)，並取替專員於2012年11月發出的《收集及使用個人資料作直接促銷指引》。為免生疑問，在條例第VIA部生效日前，專員的《收集及使用個人資料作直接促銷指引》仍繼續有效。

甚麼是「直接促銷」?

1.3 條例並非規管所有類型的直接促銷活動。根據條例，「**直接促銷**」指透過**直接促銷方法**—

(a) 要約提供貨品、設施或服務，或為該等貨品、設施或服務可予提供而進行廣告宣傳；或

(b) 為慈善、文化、公益、康體、政治或其他目的索求捐贈或貢獻*。

另外，「**直接促銷方法**」指—

(a) 藉郵件、圖文傳真、電子郵件或其他形式的傳訊，向指名特定人士送交資訊或貨品；或

(b) 以特定人士為致電對象的電話通話。

1.4 因此，條例下的「**直接促銷**」並不包括非應邀的商业電子訊息及撥打隨機抽出電話號碼的人對人電話通話³。

直接促銷的例子：

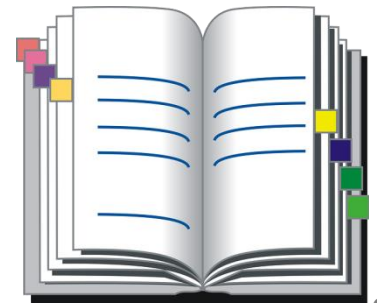
- ✓ 發送至具名人士的流動電話號碼的促銷短訊屬於直接促銷。
- ✓ 電訊服務供應商以電話聯絡現有客戶要約提供升級服務屬於直接促銷。
- ✗ 直銷郵件送交某地址或某地址的「住戶」不屬於直接促銷，因為不是向指名特定人士送交。
- ✗ 推銷員叩門向潛在顧客推銷其產品不屬於直接促銷。
- ✗ 客戶服務經理向客戶當面介紹產品/服務並不屬於直接促銷(但是其後使用這客戶的個人資料向他送達推廣資料，則屬直接促銷)。
- ✗ 向某不明人士的電話號碼發出的促銷電話不屬於直接促銷。

1
2013年1月

1. 個人資料(私隱)(修訂)條例其中新加入的部分。該部將於政府當局公布的日期生效。
2. 《非應邀電子訊息條例》(香港法律第593章)。

(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**



36

(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

(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



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?



74

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





第五部： 安裝閉路電視

私隱條例有否禁止
安裝閉路電視？



東周刊 vs 香港個人資料私隱專員公署



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

49



第六部： 外判個人資料 的處理

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



例子分享



傢俬公司委託其供應商運送傢俬，但供應商的職員事後把一張載有客戶的個人資料的送貨單棄置於客戶的單位樓層的升降機大堂



該傢俬公司須為該客戶個人資料外洩負責。該傢俬公司事後向其所有供應商發出指引，並要求後者將有關指引下達至前線職員



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





第七部： 在香港以內/外 營運網上業務或服務

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



為中小企編制之指引資料

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

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：

- 收集客戶的個人資料
- 使用客戶的個人資料
- 保障客戶個人資料的安全
- 營運網上業務或服務
- 域外營運
- 產品或服務推廣
- 招聘人手
- 使用閉路電視作保安用途
- 收集僱員的個人資料作監察
- 外判個人資料的處理
- 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。

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/misc/sme_kit。
號碼及其他身份代號實務守則》，第2.1至2.3節。

顯示 1 2017年12月



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

Guidance Note

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 SME:

- Collecting customers' personal data
- Use of customers' personal data
- Safeguarding customers' personal data
- Operating online businesses or services
- Operating business outside Hong Kong
- Marketing of products or services
- Recruitment
- Installing CCTV for security purpose
- Collecting employees' personal data for monitoring
- Outsourcing the processing of personal data
- 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.

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.
the *Code of Practice on the Identity Card Number and Other Personal Identifiers*

ing Principles for Small and Medium Enterprises 1 December 2017



為中小企編制之指引資料



資料單張

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

中小企的數據倫理道德

序言

在數據推動的經濟下，中小企（包括科技初創企業）越來越多視顧客的個人資料作為經營及推展其業務的資產而使用有關資料。資訊通訊科技的急速發展，特別是高階數據處理活動（包括大數據分析和人工智能），在帶來商機的同时，亦為私隱和數據保障帶來了挑戰。

無可置疑，個人資料是屬於資料當事人的。從個人資料獲取利益的中小企應摒棄在營運時只達致最低監管要求的想法。相反，他們應恪守更高的道德標準，在符合相關法例和監管要求的同時，亦符合持份者的期望。因此，數據倫理道德可填補法例要求和持份者期望兩者之間的落差。

事實上，有道德的使用個人資料極有利於業務發展。**尊重、互惠和公平**地使用顧客的個人資料，可提升商譽及增強持份者的信心。本單張旨在協助中小企了解如何實踐數據倫理道德。如中小企有制定評估程序，確保個人資料的處理符合數據倫理道德，顧客將對其數據保障更有信心。因此，顧客的信任日增，並將成為中小企的競爭優勢。在將來智慧社會提供服務和產品的個人化及移動化的趨勢之下，掌握及實踐數據倫理道德，會令企業更有競爭優勢。

數據倫理道德的三大核心價值

香港個人資料私隱專員公署（公署）鼓勵中小企按照數據倫理道德的三大核心價值—**尊重、互惠和公平**來處理個人資料。

尊重¹

- 中小企應對進行高階數據處理活動負責
- 中小企應考慮及與數據相關的人士及/或因使用數據而受影響的人士的期望
- 中小企應將所有數據持份者納入考慮當中
- 針對個別人士所作出的決定及其決策過程須屬合理，並能作出清晰交代
- 任何人士可隨時提出查詢和取得有關闡釋資料，若有需要，他們可就高階數據處理活動對其影響提出覆檢




互惠²

- 如高階數據處理活動對個別人士有潛在影響，該等活動所帶來的好處和潛在風險，須予以界定、識別及評估
- 採取措施以減低所有識別的風險，及平衡各方的利益，不能亦不應一面倒只考慮企業自身的利益



1 尊重價值符合《個人資料（私隱）條例》（香港法例第486章）附表1的保障資料第1
2 互惠價值符合保障資料第4原則訂明的減低風險概念。

中小企的數據倫理道德 1



Information Leaflet

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

Data Ethics for Small and Medium Enterprises

Preamble

In a data-driven economy, small and medium enterprises ("SMEs"), including tech start-ups, increasingly use personal data of customers as an asset in operating and advancing their businesses. The rapid development in information and communications technology, particularly advanced data processing activities (including big data analytics and artificial intelligence), present business opportunities but at the same time challenges privacy and data protection.

It is not in dispute that personal data belongs to the data subjects. SMEs that derive benefits from personal data should ditch the mindset of conducting their operations to merely meet the minimum regulatory requirements only. They should instead be held to a higher ethical standard that meets stakeholders' expectations alongside the requirements of laws and regulations. Data ethics can therefore bridge the gap between legal requirements and stakeholders' expectations.


In fact, ethical use of personal data makes good business sense. **Respectful, beneficial and fair** use of customers' personal data can improve business reputation and enhance stakeholders' confidence. This leaflet aims to help SMEs understand the means to implement data ethics. When SMEs develop an assessment process to ensure that personal data is processed ethically, individuals will have greater confidence in their data being protected. In turn, customers' trust will grow and become a competitive edge of the SMEs. Under the trend of service and

Three Core Values of Data Ethics

SMEs are encouraged to handle personal data pursuant to three core values, namely being **Respectful, Beneficial and Fair**.

Respectful¹

- SMEs should be accountable for conducting advanced data processing activities
- SMEs should consider the expectations of the individuals to whom the data relate and/or impacted by the data use
- SMEs should consider all parties that have interests in the data
- Decisions made about an individual and the relevant decision-making process should be explainable and reasonable
- Individuals should be able to make inquiries, obtain explanation and appeal against decisions on the advanced data processing activities that impact them



1 The Respectful value is consistent with Data Protection Principles (DPPs) 1, 3, 5 and 6 in Schedule 1 of the Ordinance (Chapter 486 of the Laws of Hong Kong).

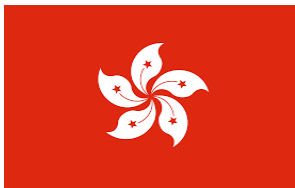
Data Ethics for Small and Medium Enterprises 1



《通用數據保障條例》－《私隱條例》 比較研究

背景

- 使《私隱條例》能緊貼全球私隱法規的發展
- 評估《通用數據保障條例》對企業(尤其跨國企業)的影響
- 法例框架比較便利資訊自由流通及促進商貿活動



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

PCPD





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



《通用數據保障條例》 – 《私隱條例》 比較研究

歐盟的《通用數據保障條例》及香港的《個人資料(私隱)條例》的主要分別:

	歐盟	香港
<p>應用</p> 	<p>資料處理者或控制者：</p> <ul style="list-style-type: none">• 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]	<p>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]</p>
<p>個人資料</p> 	<p>「個人資料」為：</p> <ul style="list-style-type: none">• 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]	<p>「個人資料」為指符合以下說明的任何資料：</p> <ul style="list-style-type: none">• 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]





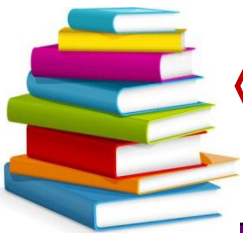
《通用數據保障條例》 – 《私隱條例》 比較研究

	歐盟	香港
<p>問責與管治</p> 	<p>以風險為本；資料控制者須：</p> <ul style="list-style-type: none"> • 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]。 	<p>沒有明確列明問責原則及相關的私隱管理措施。</p> <p>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。</p>
<p>敏感個人資料</p> 	<p>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]</p>	<p>沒有以任何目的區分敏感及非敏感個人資料。</p>
<p>同意</p> 	<p>同意必須是</p> <ul style="list-style-type: none"> • 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。 	<p>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。</p> <p>沒有規定需要家長同意。</p>





《通用數據保障條例》 – 《私隱條例》 比較研究

	歐盟	香港
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]





《通用數據保障條例》 – 《私隱條例》 比較研究

	歐盟	香港
<p>資料當事人新增及提升的權利</p> 	<ul style="list-style-type: none"> • 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] • 限制處理及資料可攜權 [第18及20條] • 反對處理 (包括個人概況彙編) 的權利 [第21條] 	<ul style="list-style-type: none"> • 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] • 就資料處理沒有限制及沒有資料可攜權, 但需遵從查閱資料及改正資料的權利 [保障資料第6原則, 第5部] • 沒有反對處理資料的權利 (包括個人概況彙編), 但可拒絕直銷活動 [第35G及35L條], 而《條例》中亦有條文規管資料核對程序 [第30-31條]
<p>認證、印章及行為守則</p> 	<p>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]</p>	<p>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]</p>

65



《通用數據保障條例》 – 《私隱條例》 比較研究

	歐盟	香港
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確定為法律基礎。
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]

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



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

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
新舊刊物

「關注私隱運動2018」－保障私隱 坐言起行
啟動中小企保障私隱運動－凝致智慧 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 機構

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

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》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

PCPD



PCPD.org.hk

est. 1996

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