

資料保障・利便營商 ——給中小企的綱領提示



“香港的中小企一般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》（下稱：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（下稱：公署）發出《資料保障・利便營商——給中小企的綱領提示》，藉此將為中小企的不同業務功能提供具體例子及實用建議。”

收集客戶的個人資料

中小企在處理客戶的產品訂購和服務預約時，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，否則便屬於超乎適度。以下列出一些中小企特別要注意的情況：

1. 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。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》行事，並考慮是否有其他較不侵犯私隱的辦法取代。



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。
- ✗ 獸醫診所為辨識貓主的身份，以便日後跟進其貓隻的健康狀況，因而收集購買貓糧的貓主的身份證號碼。
- ✓ 收集貓主的姓名及聯絡電話號碼已可達到上述目的。

2. 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

中小企如欲收集客戶的出生日期以提供針對其年齡的產品及服務，收集客戶的年齡或年齡組別（例如40歲至50歲）已足夠，而無需完整的出生日期。至於向客戶提供優惠方面，視乎有關生日折扣的時段及禮物的性質，中小企收集客戶的出生月份或出生月份及日子已足夠。

3. 向客戶提供《收集個人資料聲明》

中小企在收集客戶的個人資料（例如要求客戶填寫會員申請表格）前，應向客戶提供《收集個人資料聲明》，通知客戶所提供的資料用途及可能被轉移至甚麼類別的人士，以及其有權要求查閱及改正該資料。

實用建議：

- 雖然條例沒有規定中小企需以書面形式作出通知，但為了提高透明度及減少誤會，良好的行事方式是以書面形式向客戶提供有關資訊。
- 為確保不會收集超乎適度的個人資料，中小企可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的個人資料，以及哪些與提供其服務或產品無關的個人資料，例如婚姻狀況、教育程度、收入等。機構必須清楚告知客戶收集這些無關的資料的目的，以及提供這些資料全屬自願。

使用客戶的個人資料

中小企收集客戶的個人資料後，只限用於收集時述明或直接相關的目的（例如提供產品或服務）。如欲改變個人資料的用途，必須取得客戶的明確同意。

改變個人資料用途的例子：

- 美容中心將原本為提供美容服務而收集的客戶個人資料，轉售予另一家美容中心圖利。
- 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。

在提供售後服務或處理客戶投訴時，中小企亦須遵守條例的規定，以免過程中不當收集或披露客戶的個人資料。

實用建議：

- 若客戶致電就產品或服務作出一般性的客戶查詢，中小企應考慮毋須收集或核對該客戶身份已可作出回覆。
- 若未能即時回覆客戶的電話查詢，應為處理查詢的目的收集最低限度的個人資料，通常客戶的姓名及聯絡電話號碼／地址已足以達至回覆查詢的目的。
- 中小企應制定處理客戶投訴的程序及內部指引，例如，若投訴人的身份無助處理其投訴，應避免向被投訴一方或其他第三者披露投訴人的身份。

保障客戶個人資料的安全

中小企在處理客戶的個人資料時，須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。特別是在戶外進行推廣活動而涉及收集個人資料時，在運送過程中更應加倍謹慎。

客戶資料欠缺保障的例子：

- ✗ 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。
- ✗ 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。
- ✓ 眼鏡店應停止使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。

營運網上業務或服務

中小企營運網上業務或服務時，例如涉及經互聯網收集、展示或傳輸個人資料，亦須遵從條例的規定。例如進行網上買賣時，應使用較不侵犯私隱的身份認證方法。

較不侵犯私隱的身份認證方法的例子：

- ✗ 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提供一個獨一無二的訂單號碼，並要求顧客憑訂單號碼提貨。

公署特別提醒中小企，互聯網上的保安風險較高，需要特別小心，並須確保已採取足夠的保安措施，以保障個人資料免受未獲授權的查閱，以及定期更新此等措施，以應付不斷轉變的保安風險。

保護網站實用建議：

- 安裝防毒軟件、防火牆和最新的修補程式，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，並注意下文有關外判個人資料的處理事項。

線上無現金交易實用建議：

- 應使用安全的網上付款服務，盡量使用由付款服務供應商提供的應用程式界面／範本。
- 嚴格遵守付款服務供應商所定的執行指引。
- 提醒客戶在網上提交個人資料（特別是信用卡資料）時可能會面對的保安風險。

域外營運

在開拓內地或海外市場時，中小企須注意當地有關個人資料的法規。例如：

- 《中華人民共和國網絡安全法》已於2017年6月1日正式實施，當中包括規定關鍵信息基礎設施運營者在內地收集和產生的個人信息和重要數據須在內地儲存。如因業務需要而確需將有關信息及數據向境外提供，必須先按照政府部門制訂的辦法進行安全評估。
- 歐盟的《通用數據保障條例》(General Data Protection Regulation) 於2018年5月正式生效。屆時，凡向歐盟公民提供產品或服務，或監察歐盟個別人士的香港企業和機構，便可能受到《通用數據保障條例》的相關訂明要求所影響。(另見《香港印刷》第127期)

產品或服務推廣

1. 直接促銷

中小企在將現有或目標客戶的個人資料用於直銷用途之前，須告知客戶他們擬用哪一種類的個人資料、將會進行促銷的貨品或服務類別，並提供回應途徑，讓客戶表明是否同意其個人資料用作直銷用途。若客戶不同意，中小企便不可使用客戶的個人資料作直銷用途。

如果中小企擬轉移個人資料予第三者作直銷，則必須以書面告知客戶有關資訊，並須取得客戶的書面同意。此外，中小企在收到客戶有關停止使用其個人資料作直接促銷的要求後，須在不收費的情況下依從該項要求。違反上述規定屬刑事罪行。

中小企應備存一份所有客戶已表示不希望再收到任何直接促銷訊息的名單，並採取有系統的方式依從客戶的上述要求（例如定期更新該名單，並把更新名單分發給相關員工）。

2. 從公共領域取得的個人資料

中小企透過公共登記冊、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，必須留意這些個人資料同樣受條例的保障。使用取自公共領域的個人資料前，必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。

不當使用從公共領域取得的個人資料的例子：

- ✗ 財務公司從公共領域取得一名人士的破產紀錄，從而根據當中的住址資料向該人士發信推介「破產洗底」服務。
- ✗ 使用從政府電話簿取得的個人資料作直接促銷。

3. 使用社交網站及手機應用程式作推廣

在透過社交網絡及手機應用程式向現有或目標客戶進行營銷及提供服務時，中小企必須遵循保障資料原則的規定處理客戶資料。

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。
- 如中小企開發的手機應用程式會收集用家的個人資料（例如姓名、電郵地址等）或讀取其手機內的資料（例如用家身處的位置、手機識別碼等），應透過《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。

招聘人手

如中小企在招聘廣告中要求求職者遞交個人資料，必須述明自己的身份及有關資料的擬使用目的。中小企在收集、保留、使用及保障求職者及僱員個人資料方面，與處理客戶的個人資料一樣，都必須依從條例的規定。

不當收集個人資料作招聘用途的例子：

- ✗ 公司在招聘廣告中向求職者收取個人資料，卻沒有提及公司的名字，只提供其電郵地址及電話號碼。事實上，公司的電郵地址、電話號碼或傳真號碼，一般不足以証明僱主的身份，或會構成不公平收集求職者的個人資料。
- ✗ 餐廳招聘侍應生時，要求求職者提供出生日期、賬戶號碼、婚姻狀況、配偶姓名及身份證號碼，以及緊急事故聯絡人的姓名及電話號碼。然而，該餐廳並無需要在雙方正式建立僱傭關係之前，收集上述個人資料以作甄選。

使用閉路電視作保安用途

若中小企以保安理由於店鋪安裝具錄影功能的閉路電視，無可避免地會攝錄到途經人士的影像，故中小企應評估閉路電視系統的設計及使用情况是否適當、必需及相稱（例如安裝的位置不會超出為達至保安目的的範圍），並採取切實可行的措施，以告知途人有關閉路電視的監察。

實用建議：

- 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，以收提醒之效。
- 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。
- 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（如向警方報案作證據）。

收集僱員的個人資料作監察

中小企若選擇借助科技以監察僱員，首先應按其業務需要衡量是否適合進行僱員監察，並採取私隱侵犯程度較低的可行方法。此外，中小企應公開其所採納的僱員監察政策，並實行保障私隱的行事方式，妥善管理從僱員監察活動收集的個人資料。



其中一種近年常見被用作僱員監察的科技為指紋辨識。雖然其價格日趨大眾化，但僱主不應只為節省成本，而強制收集僱員的指紋資料。

**不適合地使用指紋辨識系統
收集僱員的指紋資料的例子：**

- ✗ 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（例如電腦打咭系統）。
- ✗ 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。
- ✓ 事實上一般的門鎖、密碼鎖及鍵鎖亦能達至防止盜竊的效果，而又不涉及收集和保存個人資料。如作為追查失竊事件用途，安裝閉路電視鏡頭是更有效的保安方法。

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，因此必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的個人資料的保存期超過處理該資料所需的時間，或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。此外，中小企亦可透過合約限制資料處理者不得為受託目的以外的其他目的使用或披露有關個人資料。

機構須為外判公司的行為負責的例子：

- ✗ 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姓氏、電話號碼及地址的送貨單棄置於客戶的單位樓層的升降機大堂。
- ✓ 該傢俬公司須為該名供應商職員不妥善地處理送貨單以致客戶個人資料外洩負責。該傢俬公司事後就處理載有客戶個人資料的文件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。

機構須為外判公司的行為負責的例子：

- ✗ 僱傭公司聘請外判維修員維修電腦，該維修員在備份資料時，一時疏忽將載有客戶資料的文件夾上載到外判商的伺服器，而伺服器出現保安漏洞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維修員不妥善地處理電腦檔案以致客戶個人資料外洩負責。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。

處理查閱及改正 個人資料要求

條例賦予客戶或僱員查閱及改正資料的權利。中小企作為資料使用者，須依從客戶或僱員根據條例作出的查閱資料要求及改正資料要求。條例規定於收到有關要求後 40 天內依從。縱使並未持有所要求的資料，仍需在相同的時限內以書面通知提出查閱資料要求者，並述明原因。中小企收到上述要求，如不懂處理，應盡快尋求法律意見或參考公署發出的指引，以免違反條例的規定。

結語

公眾及客戶對個人資料私隱保障的期望與日俱增，因此中小企應採取積極的態度和措施保障個人資料私隱，增強他們的信任。若能達至上述目標，中小企的商譽、競爭優勢以至潛在商機均可隨之提升。■

如欲了解更多資訊，敬請聯絡：

香港個人資料私隱專員公署

網頁：PCPD.org.hk

熱線：+852 2827 2827

傳真：+852 2877 7026

電郵：enquiry@pcpd.org.hk

