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

經互聯網收集及使用個人資料：給資料使用者的指引

引言

現今，不論是商務企業、非政府組織或公共機構，營運網上業務或服務均十分普遍。這些服務常會涉及收集個人資料。

《**個人資料（私隱）條例**》（下稱「**條例**」）的六項保障資料原則[1]列明資料使用者應如何公平地處理個人資料的資訊。條例下的「資料使用者」，就個人資料而言，指「獨自或聯同其他人或與其他人共同控制該資料的收集、持有、處理或使用的人」。

下述資訊旨在協助資料使用者（在本指引中稱為「機構」）了解經互聯網收集、展示或傳輸個人資料時，應如何依從條例的規定。

保障資料第 1 原則 — 收集目的及方式

收集的個人資料屬足夠但不超乎適度

保障資料第1(1)原則規定機構只可收集對資料的使用目的而言是必需的個人資料，而所收集的資料應屬足夠但不超乎適度。例如，倘沒有在網上購物或要求送遞貨品，收集客戶的信用卡號碼或住址一般會被視為超乎適度及不必要。此外，如所需的只是對方的年齡，或對方已聲明超過某個歲數，則一般不應要求對方提供出生日期。另一個常見的例子是在沒有任何原因下收集顧客的性別資料。

合法及公平收集

保障資料第1(2)原則規定，個人資料須以在有關個案的所有情況下屬合法及公平的方法收集。收集個人資料的目的應以直接公開的方式列明，不要使用取巧或欺騙的手段。例如，透過招聘一些並不存在的職位或以假抽獎來收集個人資料，都不是公平的收集資料方式。向兒童收集個人資料時須特別小心。在收集過程中應採用清晰簡單的語言，並應建議兒童先徵詢家長的意見才提供其個人資料。

- **機構的身份**。機構在互聯網收集個人資料時，有時除了其網址或電郵地址外，並沒有顯示其他聯絡資料，而網址或電郵地址通常不會顯露該機構的真正身份。機構以匿名方式收集個人資料，可能並不符合保障資料第1(2)原則的規定。

  機構除了提供其網址及／或電郵地址外，應清楚披露其名稱、所在地址及聯絡電話及／或傳真號碼，讓資料當事人以可靠的途徑與機構聯絡。機構可將相關資料放於其網頁中的「關於我們」及／或「聯絡我們」一欄。

經互聯網收集個人資料

保障資料第1(3)原則列明資料使用者向個人收集個人資料之時或之前須提供的資訊。機構在其網頁中利用網上表格向個人收集個人資料，或要求他們透過電郵提交其個人資料。機構應就此採取所有合理地切實可行的步驟，確保該些人士已獲告知保障資料第1(3)原則所規定的資訊。

- **在網上提供收集個人資料聲明**。依從**保障資料第1(3)原則**的一個可行方法是在網上向個人提供收集個人資料聲明。收集個人資料聲明應以清楚

[1] www.pcpd.org.hk/chinese/ordinance/ordglance.html

明顯的方式展示（例如放在同一網頁或透過清晰描述的連結取得）、易於閱讀及理解，以及內容必須與印刷版本一致。一般而言，收集個人資料聲明應包括下述資訊：

- 個人屬有責任或可自願提供該資料；如屬有責任提供，不提供該資料的後果；
- 該資料將會用於甚麼目的；
- 該資料可能移轉予甚麼類別的人；及
- 個人要求查閱其個人資料及改正該資料的權利，以及可向其提出該等要求的負責人的姓名（或職銜）及地址。

有關如何擬備收集個人資料聲明，機構可參閱專員發出之《擬備收集個人資料聲明及私隱政策聲明指引》[2]。

- **清楚列明必須或可以自願填寫的項目**。如機構以網上表格及紙張表格收集個人資料，除非有很好的理由，否則所收集的個人資料類型應是相同的；更應清楚列明每個項目是否必須或可以自願填寫，即使用戶沒有填寫自願填寫的項目，亦應獲准繼續進行登記。

- **使用cookies及網上行為追蹤**。如網站需要使用cookies，良好的行事方式是清楚列明甚麼類別的資訊（不論是否涉及個人資料）會被儲存於cookies內。如網站使用第三方cookies，不論是否涉及個人資料，亦應清楚說明此等cookies會收集甚麼類別的資料、該資料會移轉予甚麼人，以及有關目的。

  如網站必須使用cookies，則應清楚列明此為先決條件。如使用cookies並非必須，網站應向使用者提供不接受使用cookies的選擇，並應清楚說明如使用者決定不接受cookies的後果（例如：不接受session cookies可能影響網站的暢順運作）。

  如涉及網上追蹤，資料使用者應遵從《網上行為追蹤》資料單張[3]所載的公平及具透明度的做法。

保障資料第2原則 — 準確性及保留期間

個人資料的準確性

保障資料第2（1）原則規定資料使用者須採取所有合理地切實可行的步驟，確保所收集的個人資料準確。雖然經網頁收集的個人資料的準確性並不是經常可予以核實，但是仍須採取適當及可行的步驟，檢查所收集的個人資料是否準確。例如，為了確保其後的訊息會被送至正確地址，可能需要「雙重確認」（即向所獲提供的電郵地址發出核實電郵訊息，確認有關地址已被正確地輸入）。如網上核實不可行，則可能需要經非網上途徑進行核實。

個人資料的保留期

保障資料第2（2）原則規定，資料使用者須採取所有合理地切實可行的步驟，確保不會將所收集的個人資料保存超過該資料被使用於或會被使用於的目的所需的時間。除了以政策列明所收集的個人資料的保留期外，機構應設立機制確保在保留期之後，一併刪除網上及非網上的有關個人資料[4]。

聘用資料處理者

此外，**保障資料第2（3）原則**規定，如資料使用者聘用（不論是在香港或香港以外聘用）資料處理者，以代該資料使用者處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者的個人資料的保存時間超過處理該資料所需的時間。為協助機構在外判個人資料的處理時遵從保障資料第2（3）原則的規定，專員發出了《外判個人資料的處理予資料處理者》資料單張[5]。

---

2 www.pcpd.org.hk/chinese/files/publications/GN_picspps_c.pdf

3 www.pcpd.org.hk/chinese/publications/files/online_tracking_c.pdf

4 www.pcpd.org.hk/chinese/publications/files/erasure_c.pdf

5 www.pcpd.org.hk/chinese/publications/files/dataprocessors_c.pdf

保障資料第 3 原則 — 個人資料的使用

經互聯網展示個人資料

保障資料第 3 原則規定，除非取得有關的資料當事人或其「有關人士」(如條例下的定義)[6] 的訂明同意(即明確及自願的同意)，否則個人資料不可用於新的目的。經互聯網披露或展示個人資料可構成作個人資料的使用，因此，為依從保障資料第 3 原則的規定，機構應遵守下述各點：

- **收集時說明個人資料會被展示**。如收集的個人資料稍後會經互聯網或其他渠道展示，在收集資料之時或之前，必須向有關個人清楚說明這意圖。例如某機構所提供的網上服務會經互聯網將私人補習導師的資料公開予家長查閱。向準導師收集個人資料時，應向他們聲明這些資料會經互聯網展示。否則，機構如此地展示資料前，必須取得導師的明確許可。

- **展示時應隱去個人資料**。根據條例，匿名資料並不是個人資料，因為從有關資料直接或間接地確定有關個人的身份不是切實可行的。機構應在經互聯網展示個人資料前考慮會否把資料匿名化以達到展示資料的目的。例如，在網頁公布抽獎或比賽得獎者時，應考慮可否展示抽獎券號碼來替代公布得獎者姓名。這樣可以避免第三者利用展示的個人資料作不適當的用途。機構亦要明白只移除資料中的姓名、地址或其他明顯的身份識別代號並不一定可以把資料完全匿名化，因此在每個情況中應確保重新識別身份不是切實可行的。若有必要展示個人資料以達致某目的，所展示的程度亦應只限於達致有關目的需要。

- **限制使用目的**。經互聯網展示個人資料時，應聲明限制資料的進一步或次要使用。例如，電話簿或會員名冊應列明其使用只可限於所述的特定目的。如個人資料不得用於直接促銷用途，應清楚列明。

保障資料第 4 原則 — 個人資料的保安

儲存及傳輸個人資料的保安

保障資料第 4(1) 原則規定，資料使用者須採取所有合理地切實可行的步驟，實施保安措施，其程度應與資料外洩可能造成的傷害的嚴重性相稱。互聯網上的保安一般較為薄弱，需要特別小心，以確保在儲存及傳輸個人資料方面的保安措施足夠。

- **由上而下及「保障私隱 全面貫徹」(Privacy by Design)**的方式。機構需要採用由上而下的方式以全面保障個人資料。在制定適當的保障從而制定政策、指引、程序及措施前，首先須考慮可接受的風險程度。機構應採取「保障私隱 全面貫徹」的取向，以確保個人資料的保障在任何系統的可行性階段已成為不可或缺的部分，而不是後加的。

- **風險評估**。並不是所有儲存於互聯網或以互聯網傳送的個人資料都需要相同程度的保障。保障程度的高低應視乎所涉及的個人資料的敏感程度及數量。因此機構應對儲存於互聯網或以互聯網傳送的各類個人資料，定期進行風險評估，從而制定政策、指引、程序及措施，和作出定期檢討，以保障個人資料的機密性及完整性，並確保相關人士存取這些個人資料的問責性及可追溯其行動，例如閱讀／寫入／修改資料。

- **制定處理個人資料的政策**。條例**第 65(1) 條**規定僱主須對僱員在受僱用中所作出的行為負上法律責任，除非僱主能提供證據，證明他已採取切實可行的步驟，防止僱員違反條例的規定。因此機構應制定處理個人資料的政策、程序及指引，並定期提醒職員遵守。根據條例**第 65(2) 條**，機構聘用代理處理個人資料亦有類同責任。因此，機構在選擇服務供應商時，應評估或審視該服務供應商在保障個人資料私隱方面所實施的系統，包括是否有足夠的保安措施及程序。

[6] 例如，如資料當事人是未成年人，機構可從其父母取得訂明同意。請參閱條例第 2(1) 條下「有關人士」的定義。

- **考慮使用科技保安措施**。如機構主理的應用程式或持有的資料庫容許網上查閱個人資料，應實施足夠的措施，保障個人資料免受未獲授權的查閱，及定期更新此等措施，以應付不斷轉變的保安風險。此等措施的例子如下：

  - 把傳送中的個人資料加密以防止未獲授權的截取或查閱。
  - 如個人資料是儲存於互聯網，應以存取控制措施、加密及／或其他適當措施，防止未獲授權的查閱或更改。
  - 應以措施管控密碼的複雜性、重試及重設，以加強密碼的功能。
  - 應以適當配置的防火牆以保護載有個人資料的伺服器。在合適的情況下凡載有或收取個人資料的伺服器或資料庫應以「三層架構」保護，阻止互聯網的用戶直接查閱個人資料。
  - 制定正式的保安修補程式管理程序，以確保及時安裝軟件供應商所發布的保安修補程式。應定期掃描可經互聯網進出的伺服器，檢查是否有漏洞；如發現漏洞，應採取適當的補救行動。
  - 不要使用可容易被猜度的方法(例如在網址加上順序變數)，來查閱個人資料。此舉可避免未經授權的第三者猜度出網址而從而查閱個人資料。
  - 不要儲存或要求用戶上載沒有妥善保護(如存取權控制及／或加密)但載有個人資料的檔案至網絡伺服器，不論時間有多短。現代的搜尋器威力強大，最隱蔽的網址所儲存的檔案亦可以被搜尋到。
  - 機構可考慮安裝防止流失資料的系統，以掃描網上通訊是否包含未經授權作披露的個人資料。
  - 如單一的伺服器具有多項伺服器功能或應用程式，應測試個人資料的跨應用存取權，以防各應用程式之間出現未獲授權的個人資料的查閱。
  - 可能的話，應考慮使用私隱提升技術，以保障個人資料私隱。私隱提升技術是減低資料外洩風險的技術措施。常見的技術包括加密或雜湊功能以保障資料的機密性，使用機械人排除協定，以防止搜索引擎為網站進行索引，使用需人手輸入的驗證碼以防止整個數據庫被自動下載。

- **提供私隱警告訊息**。機構應向資料當事人提供安全傳送個人資料的方式。如有關個人選擇以沒有加密的方式傳輸其個人資料，在傳送之前，應給予該人適當的風險警告。

- **避免使用已知的個人資料作認證用途**。建議機構不應使用第三者較易取得的個人資料，例如出生日期、身份證號碼或電話號碼，作為認證用途(例如用作初始密碼或確認碼)。

- **在工作地方推廣關注私隱的文化**。機構應令每名僱員認識尊重資料私隱權的重要性，這既是道德責任，亦是法律規定。所有處理個人資料的人員應在了解條例的規定及循規措施方面獲得足夠的培訓。

- **資料外洩事故的處理**。資料在互聯網上外洩可以很迅速及廣泛，不當處理會對機構的聲譽造成無法挽回的損害。因此，機構應設立具透明度的資料外洩事故處理系統[7]，清楚列明應依從的行動計劃，以遏制事故及減低對資料當事人可能造成的損失及損害。

聘用資料處理者

保障資料第4(2)原則規定，如資料使用者聘用(不論是在香港或香港以外聘用)資料處理者，以代該資料使用者處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者作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。

有關制定資料處理合約條款的詳細指引，請參閱專員發出的《外判個人資料的處理予資料處理者》資料單張[8]。

---

[7] 請參閱專員發出的《資料外洩事故的處理及通報指引》www.pcpd.org.hk/chinese/publications/files/DataBreachHandling_c.pdf

[8] 請參閱註 5

保障資料第 5 原則 — 政策及措施的透明度

公開機構的個人資料私隱政策

保障資料第5原則規定機構的個人資料私隱政策及措施須公開。擁有網站的機構應擬備私隱政策聲明，讓網絡用戶查閱或下載。

- **私隱政策聲明應易於查閱**。可行的方法是以連結頁載列私隱政策聲明，從主頁或收集個人資料的頁面（例如會員登記頁或客戶協議頁）連結。該連結應清楚標示，例如以「私隱政策」為名或具類似字眼的按鈕或圖示。

- **清楚列明私隱政策**。私隱政策聲明應把機構所持有的個人資料種類及個人資料的主要使用目的告知用戶。此外，該聲明可載有其他有關個人資料私隱的資訊，例如機構以cookies（如有）追蹤訪客、機構的直接促銷政策，以及個人資料的保安和保留政策。

有關如何擬備個人資料私隱政策，機構可參閱專員發出之《擬備收集個人資料聲明及私隱政策聲明指引》[9]。

保障資料第 6 原則 — 查閱個人資料

根據**保障資料第6原則**，個人有權查閱及改正機構所持有他們的個人資料。不論機構是在網上或其他途徑收集或持有個人資料，在處理方面並無分別。載有關於依從查閱資料要求[10]及改正資料要求[11]的進一步資料，可從公署網站參閱。

直接促銷活動

機構如果利用個人資料作直接促銷，則必須遵守條例**第VI A部**對直接促銷活動的規定。

機構可參閱專員發出之《直接促銷新指引》[12]。

資料使用者應留意不論其使用的個人資料是從網上或直接從個人取得，及不論其促銷活動是否在網上或以慣常方式推行，凡是進行直接促銷，條例**第VI A部**有關直接促銷活動的條文都會適用。

機構以電子訊息進行直接促銷活動時亦須遵守由通訊事務管理局辦公室執行的《非應邀電子訊息條例》(第593章)[13]。

香港個人資料私隱專員公署
查詢熱線：(852) 2827 2827
傳真：(852) 2877 7026
地址：香港灣仔皇后大道東248號12樓
網址：www.pcpd.org.hk
電郵：enquriy@pcpd.org.hk

初版印於二零一一年十二月
二零一四年四月

9 請參閱註 2

10 請參閱www.pcpd.org.hk/chinese/publications/files/DAR_c.pdf

11 www.pcpd.org.hk/chinese/publications/files/dcr_c.pdf

12 www.pcpd.org.hk/chinese/files/publications/GN_DM_c.pdf

13 詳情請參閱www.ofca.gov.hk/tc/industry_focus/uemo/index.html