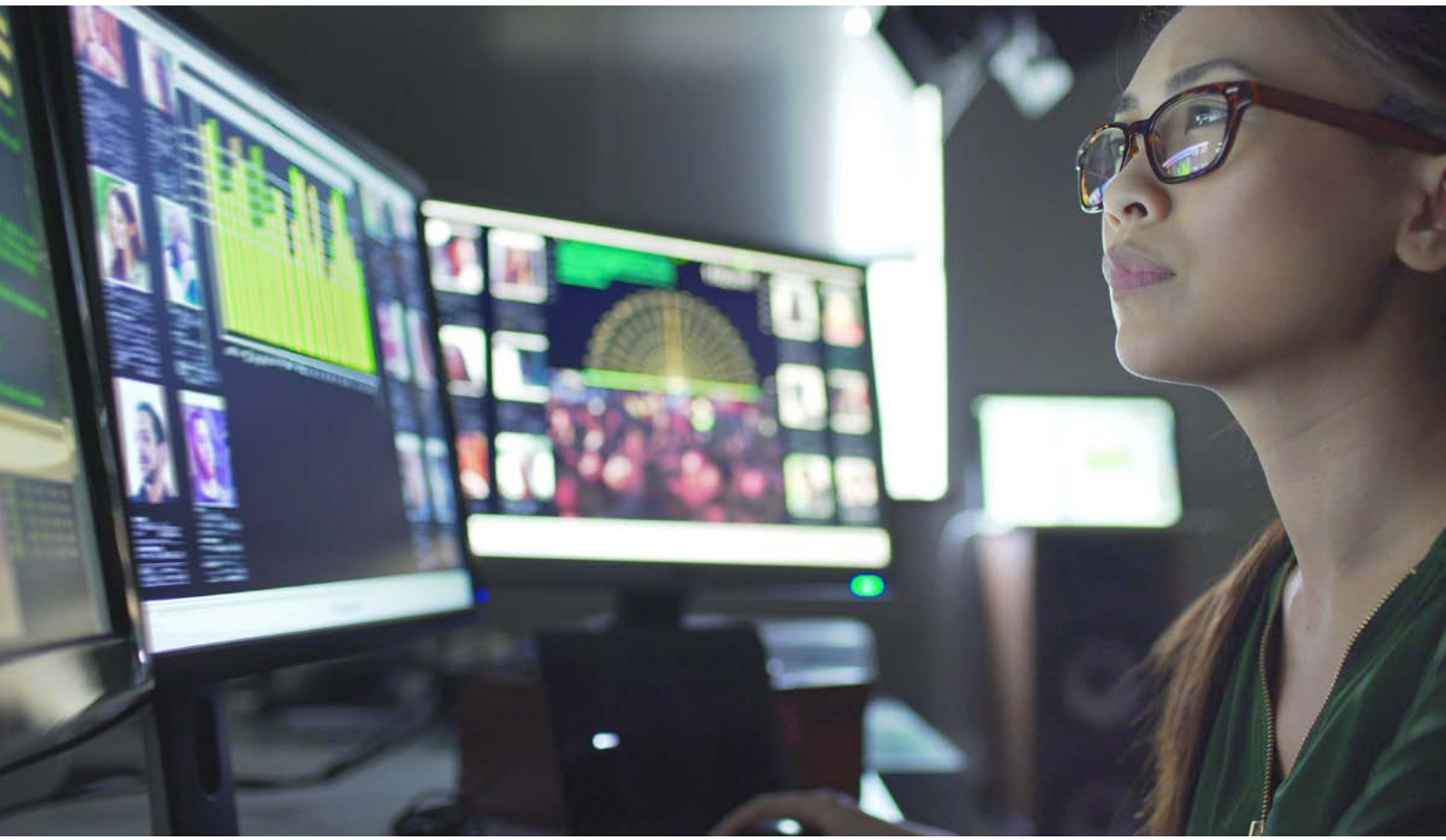
非政府機構
個人資料
私隱指南



pwc 羅兵咸永道

從加強保障個人資料和合規能力，構建非政府機構的誠信力

非政府機構（機構或NGO）致力關注社會需要及服務缺口，為需要幫助的人提供社會服務。因此，機構從身份識別、跟進社會支援需要、監察以及評估等方面，掌握了大量服務使用者的個人資料。隨著社會服務運作數碼化，機構收集及儲存的資料訊息與日俱增，電子媒體的廣泛使用亦增加了機構遵從個人資料私隱合規要求的風險。

作為以服務使用者為本的機構，必須遵守《個人資料（私隱）條例》（第486章）的規定。確保持份者（包括服務使用者、資助者、義工、服務專業人員、員工等）的資料及訊息得到妥善保存。這不僅是合規要求，更是尊重服務使用者和合作夥伴給予機構的信任和信心，實在至為重要。

此《非政府機構個人資料私隱指南》有助提高機構的運作效能，協助它們在提供社會服務時，了解保障個人資料和合規的重要性與影響，並就制訂合規程序和措施提供建議。

目錄

頁碼

《個人資料（私隱）條例》

資料私隱法定機構和條例之目的

香港個人資料私隱專員公署（公署）是一個獨立的法定機構，負責監督《個人資料（私隱）條例》（第486章）（《條例》）的實施。公署的使命是通過對《條例》的推廣、監察及監管，促使各界人士遵從條例，以確保市民的個人資料私隱得到保障。

《條例》旨在保障涉及個人資料的私隱權，即直接或間接與一名在世人士（資料當事人）有關及可確定其個人身份的資料，而此等資訊的儲存形式是可查閱及處理的。任何控制個人資料的收集、持有、處理或使用的人士均須遵守《條例》的規定。

六項保障資料原則簡介

控制個人資料的收集、持有、處理或使用的任何人士（即資料使用者）必須遵守六項保障資料原則，從而保障資料當事人的權利。六項保障資料原則作為《條例》的核心，其規定適用於個人資料使用的整個過程，包括收集、保留、使用、共享、轉移及銷毀。

原則1：收集目的及方式

- 必須以合法公平的方式收集個人資料，且僅用於與資料使用者職能或與活動直接相關之目的。
- 必須告知資料當事人收集之目的以及資料可能會被轉至的第三方。
- 僅收集必需的資料，不得過度。

原則2：準確性及保留期間

- 個人資料務必準確，且保留期限不得超越達致原來目的實際所需。

原則3：資料的使用

- 個人資料必須只用於原先收集之目的或與之直接相關之目的。除非得到資料當事人自願給予的訂明同意，否則個人資料不得用於新目的。

原則4：資料的保安

- 資料使用者必須採取切實可行的步驟，保障個人資料不被未經授權或意外地查閱、處理、刪除、遺失或使用。

原則5：透明度

- 資料使用者必須公佈所持資料類型及用途等相關之政策及常規。

原則6：查閱及改正

- 資料當事人有權查閱自己的個人資料，並對不準確資料作出改正。

依據《條例》定義資料當事人和資料使用者

個人資料	個人資料指符合以下說明的任何資料： 1. 直接或間接與一名在世人士有關； 2. 可直接或間接地查明個人身份；及 3. 以可供查閱及處理方式記錄下來的資料。	例子： • 個人詳情：如姓名、身份證號碼、性別、出生日期和年齡等。 • 聯絡方式：如手機號碼、電郵地址、通訊地址等。 • 其他資料：如婚姻狀況、信用卡號碼、教育背景、病歷、犯罪紀錄等。
資料當事人	資料當事人是指屬於相關個人資料的在世當事人。	例子： • 服務使用者、義工、員工、捐贈者/資助者等。
資料使用者	資料使用者是指獨自控制或聯同其他人共同控制個人資料的收集、持有、處理或使用的人。	例子： • 服務提供者; • 服務提供者聘用的第三方; • 服務合作夥伴。

違反《條例》規定可構成的罪行及補償

如果任何機構違反《條例》，私隱專員可向該機構發出執行通知，指令糾正該違規行為和/或採取起訴行動。違反私隱專員發出的執行通知即屬犯罪，最高可被判罰款港幣5萬元及監禁2年，加上每日罰款港幣1千元。一經再次定罪，最高可被判罰款港幣10萬元及監禁2年，加上每日罰款港幣2千元。

此外, 不當使用個人資料於直接促銷活動也可構成罪行，並將面臨以下處罰：

罰款	監禁	罪行類別
港幣50萬元	3年	• 未獲得資料當事人自願給予的訂明同意，將相關的個人資料用於直接促銷活動。 • 未獲得資料當事人的訂明同意，將個人資料披露給第三方，用於不以盈利為目的之直接促銷活動。 • 未遵守資料當事人提出的「拒絕服務」選擇要求，繼續將其個人資料用於直接促銷活動中。
港幣100萬元	5年	• 未獲得資料當事人的訂明同意，將個人資料披露給第三方，用於以盈利為目的之直接促銷活動。

個人資料生命週期的例子

可能面對的資料私隱風險例子

01

對於資料處理及管理經驗不足

02

個人資料被未經授權的人員查閱

03

保留資料的時間長於實際所需

04

收集過多的個人資料/未獲得訂明同意下收集資料

05

資料保安措施不足

06

未制訂資料外洩處理程序

07

資料私隱意識薄弱

08

對外判供應商/第三方的監管不足

09

未完全刪除不再需要的個人資料

原則1：收集目的及方式

什麼是收集目的及方式原則？

機構在日常運作中會收集大量的個人資料。在開始收集資料之前，請考慮幾個簡單問題：如收集此等資料之目的和理由是什麼？是否必需收集此等資料？資料收集有否超出了必要的範圍？

根據《條例》中的原則1，需要向服務使用者、義工和捐贈者/資助者收集個人資料的機構，必須遵守相關的合規要求。

收集資料時，機構應當考慮以下事項

01

仔細思考並記錄收集、處理個人資料的方式和原因，僅收集特定目的所需資料。

02

收集方式須合法（例如必須在資料當事人知情下進行，不得採取欺騙或脅迫的方式）。

03

了解涉及個人資料的運作流程。

04

向資料當事人提供《收集個人資料聲明》，說明收集的原因。

您可參閱私隱專員發佈的《身份證號碼及其他身份代號實務守則資料使用者指引》資料單張:
https://www.pcpd.org.hk/tc_chi/data_privacy_law/code_of_practices/files/compliance_guide_c.pdf

原則2：準確性及保留期間

什麼是準確性及保留期間原則？

根據《條例》中的原則2，機構收集與持有的個人資料必須為最新的版本，且須準確及完整，以用來達致原本目的。

由於機構通過多種渠道和活動，於不同時間收集個人資料，因此持有的資料可能過期或不準確。另外，由於保留和處理個人資料方面的管治不足，令資料的保留時間可能超過實際所需。

在機構平台（例如網站及流動應用程式）的個人賬號註銷後，相關的個人資料只可保留一段適當的時間。為達到此要求，機構應當建立明確的處理機制，在資料保留期限結束時及時將其刪除。

持有資料時，機構應當考慮以下事項

01 準確性

機構應當確保持有的個人資料準確無誤，並為包括義工、服務使用者、捐贈者或資助者在內的資料當事人，提供更新個人資料的途徑（例如通過電子郵件）。

02 保留

資料保留是指機構在資料收集之後、處置之前能夠保留的時間。機構應根據達致原來目的所需的時間來確定保留期限，並確保及時處置不再需要的所有個人資料。

03 處置

資料處置是指及時刪除不再需要的數碼或實體形式個人資料。機構應制定詳細的程序，規管如何根據處理時間表刪除個人資料，並確保該等資料被完全刪除且無法再被讀取。

原則3：資料的使用

什麼是資料的使用原則？

個人資料僅可用於原先收集之目的或與之直接相關之目的。但如得到資料當事人自願給予的訂明同意下將資料用於新目的，則屬例外。機構很可能將收集到的個人資料用於其他目的，如活動宣傳和籌款。當中須要考慮的問題包括：機構是否應當告知資料當事人？機構將個人資料用於其他目的時，應採取哪些措施來確保符合《條例》之規定並保證其透明度？

使用資料時，機構應當考慮以下事項

01

當個人資料用於新目的時須向資料當事人再次提供《收集個人資料聲明》。

02

個人資料用於直接促銷活動時須獲得訂明同意。

03

容許資料當事人隨時更改其意向，且不需承擔任何費用。

04

建立追索資料當事人同意記錄的機制，並監察執行的情況。

如果機構想將收集到的個人資料用於直接促銷活動，則須獲得相關當事人自願給予的訂明同意。在該等情況下，須向當事人提供另一份或經修訂的《收集個人資料聲明》作說明。有關《收集個人資料聲明》的詳情，請參閱此指南第16頁。

原則4：資料的保安

什麼是資料保安原則？

近年來，資料外洩的事故越來越多，原因之一是對資料保安的監管不足。《條例》中的原則4要求機構保護個人資料，包括提供給第三方資料處理者進行處理的個人資料。

以下是個人資料儲存媒體的例子

01 可攜式儲存設備

02 電子檔案，包括儲存備份

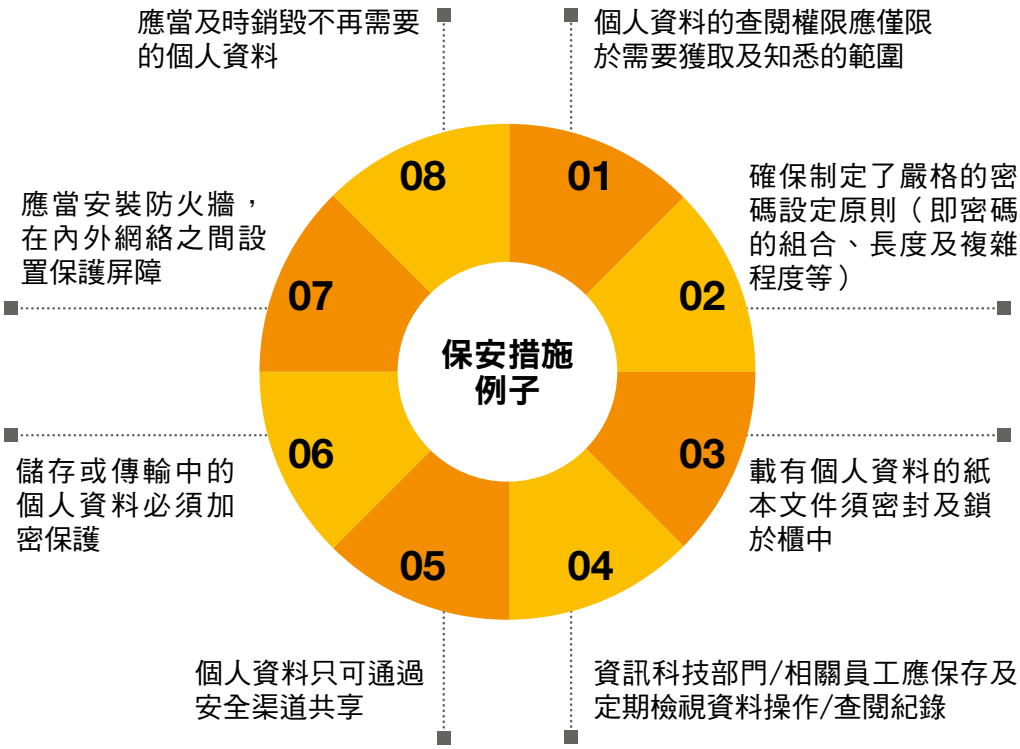
03 文件打印本

04 雲端運算平台

05 流動應用程式

06 網站伺服器

儲存、處理和輸送個人資料時，機構應考慮哪些保安措施？



網上行為追蹤

機構在其網站上設置可收集網站使用者個人資料的在線追踪功能（例如通過使用cookies）時，應遵循與個人資料收集、持有及使用相關的六項保障資料原則。

通過承辦商（例如提供網站瀏覽分析服務的公司）進行網上行為追踪時，資料使用者也應確保直接促銷活動的嚴謹管理以及對個人資料的恰當保護。

當使用cookies收集網上行為的資訊時，建議機構採取以下措施：

1. 為cookies設定合理的有效期限;
2. 必要時加密cookies內容；及
3. 除非機構能為網站用戶提供解除或拒絕此等cookies的選擇，否則不要採用閃存、殭屍、超級cookies等技術, 因為這些cookies會忽略瀏覽器是否接受cookies設定。

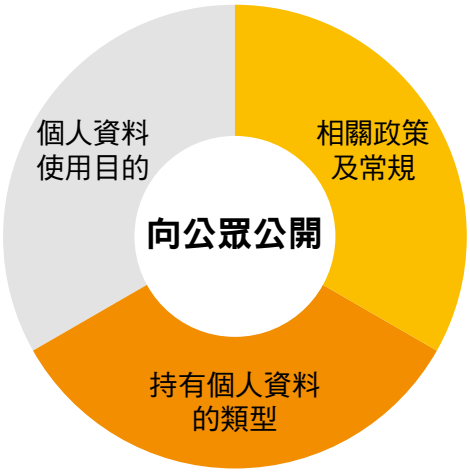
您可參閱私隱專員發佈的《網上行為追蹤》資料單張：
https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/online_tracking_c.pdf

原則5：透明度

什麼是透明度原則？

在數碼時代，保護個人資料對機構而言至關重要，而就資料當事人來說，對資料使用者保持警惕亦同樣重要。《條例》中的原則5規定機構必須採取一切切實可行的步驟，將處理個人資料相關的政策與程序公之於眾。

為了就資料處理與資料當事人進行有效溝通及避免產生疑問，機構有必要提供書面形式的個人資料政策和程序，並撰寫《私隱政策聲明》，陳述如何處理個人資料。



什麼是《私隱政策聲明》？

《私隱政策聲明》是關於資料使用者（例如NGO）的私隱政策及常規的概括陳述，內容涉及所處理的個人資料。《私隱政策聲明》應通過網站或小冊子等形式提供，以方便大眾查閱。

《私隱政策聲明》有任何修訂，機構均應主動告知資料當事人。

機構對制訂《私隱政策聲明》的關鍵考慮

1. 保護個人資料私隱的承諾是什麼
2. 所持有的個人資料種類及如何使用該等資料
3. 是否收集未成年人的個人資料或在當事人不知情的情況下（例如使用cookies）收集資料
4. 個人資料將被保留多久
5. 如何處理個人資料及會否將資料披露予第三方
6. 如何保障個人資料安全及是否會通過服務供應商對個人資料進行處理
7. 制定了哪些保安措施來保障所收集的個人資料
8. 誰人負責資料查閱及改正要求與聯絡方式

您可參閱私隱專員發佈的《擬備收集個人資料聲明及私隱政策聲明指引》：
https://www.pcpd.org.hk/chinese/publications/files/GN_picspps_c.pdf

原則6：查閱及改正

什麼是資料查閱及改正原則？

收集了資料當事人的個人資料後，機構有責任確保有關的資料準確無誤。因此，機構有必要建立可供資料當事人查閱自己個人資料的機制，以便驗證資料的準確性並在必要時作出更正。《條例》中的原則6為機構提供了在處理資料當事人查閱要求方面的指引。

機構應在收集個人資料時通過《收集個人資料聲明》，明確告知資料當事人享有查閱及改正個人資料的權利。根據《條例》，除非有正當理由拒絕要求（例如無法證實要求者的身份），否則機構必須在40日（曆日）內按照該要求行事。

處理資料當事人查閱及/或改正要求時，機構應當考慮以下事項

01

確定處理資料當事人查閱及改正要求的政策與程序，確保機構可在法定要求時間內作出答覆。

02

向資料當事人提供《收集個人資料聲明》，就享有的個人資料查閱權及改正權與其進行溝通。

03

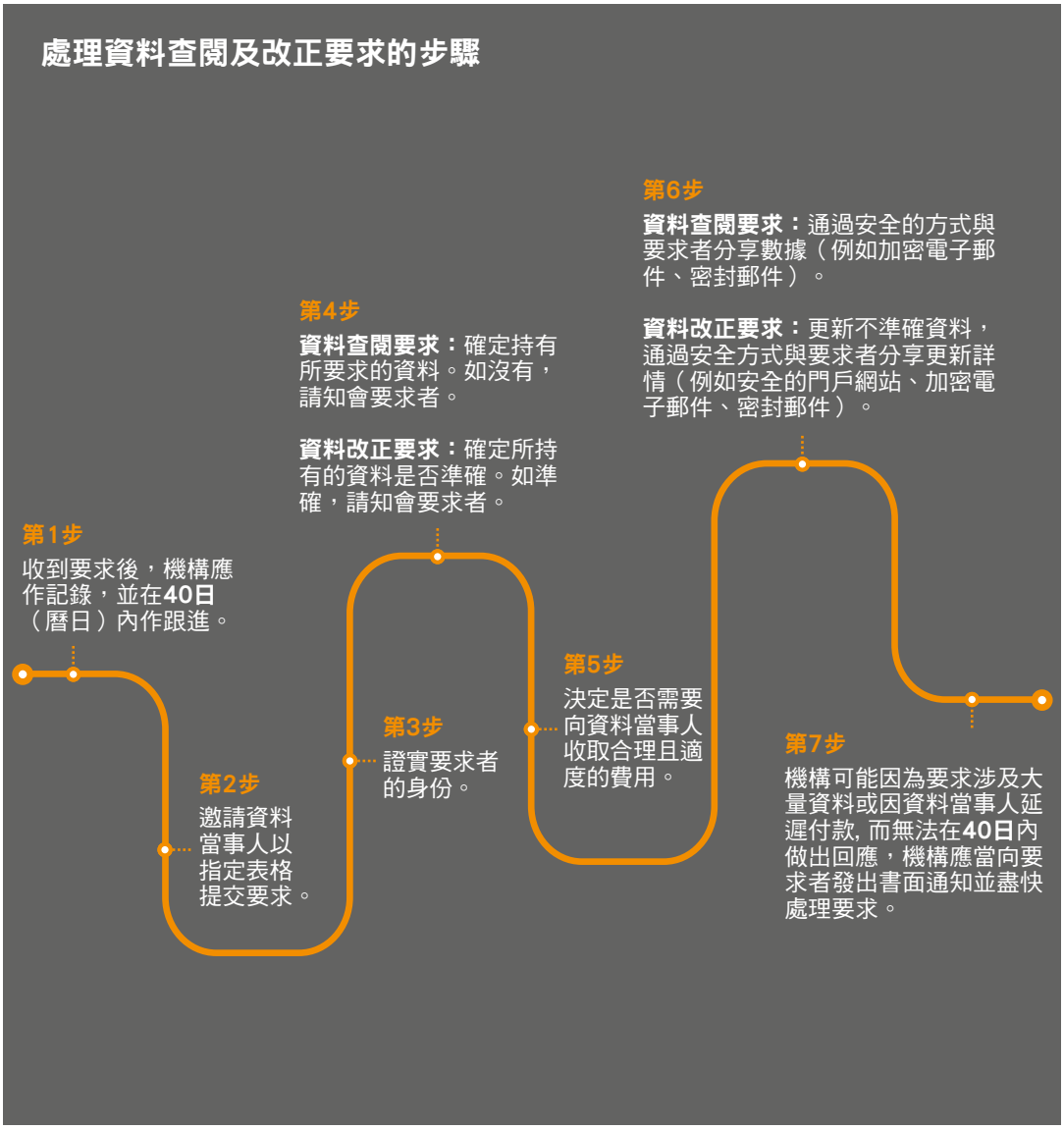
委派專人負責處理所有的資料查閱及改正要求，並將聯絡方式載於《收集個人資料聲明》中。所有的要求均應正式記錄在案。

04

就拒絕查閱及/或改正資料要求連同拒絕的理由備存紀錄，並將紀錄保存四年。

資料查閱及改正管理指引

為了遵守資料查閱及改正原則，機構應當制定詳細的指引，列明處理資料當事人查閱及/或改正要求的步驟。以下例子僅供參考：



資料私隱管理架構

建立資料私隱管治架構

隨著市民對個人資料私隱保障的意識和期望提高，機構必須在合規以外，對個人資料採取更嚴格的保障措施。完善的內部管治架構對培養資料私隱文化，以及確保落實保障個人資料的政策和程序非常重要。通過界定處理資料私隱的角色和責任，機構可將保障個人資料作為日常運作職責的一部分，並在機構內實施相關措施。這有利於建立與工作夥伴及服務使用者的信任，並增強社會各界與機構合作的信心。

建立資料私隱管治架構的好處

典型資料私隱管治結構中的關鍵角色和責任

機構領導人應以身作則，在其機構內培養資料私隱文化，來展示他們致力於保障個人資料私隱的承諾。以下是資料私隱管治架構一些關鍵角色和職責，以供參考：

董事會/高級管理層

董事會/高級管理層的角色和職責例子包括：

- 發展與培養健全的資料私隱和保障文化
- 制訂整體的資料私隱願景和策略
- 監督關鍵的資料私隱和保障風險
- 監督及確保制訂私隱政策和程序

保障資料辦公室/保障資料主任

建議按機構規模大小，委任指定人員擔任保障資料主任或成立保障資料小組。保障資料主任的角色和職責例子包括：

- 保存機構完整和準確的個人資料庫存
- 根據法規改變更新與私隱相關的政策
- 對所有部門的個人資料定期進行風險評估
- 處理對機構提出的資料查閱及改正要求，以及私隱相關的投訴和查詢
- 進行培訓和分發教材，以提高員工的私隱保障意識

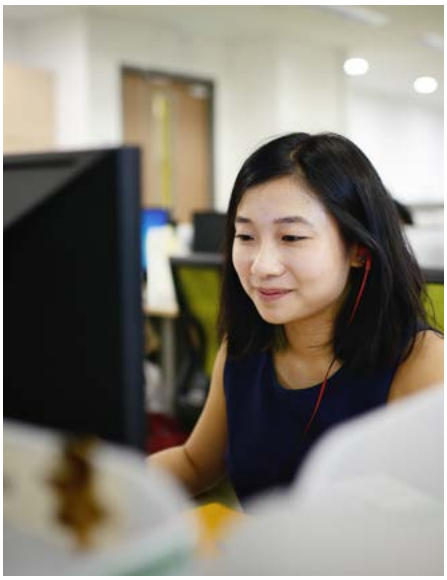
個人資料庫存

什麼是個人資料庫存？

個人資料庫存是指個人資料訊息的紀錄，包括但不限於所收集的個人資料類型、收集個人資料的方式、儲存資料的位置、保留資料的期限、使用個人資料的方式及採取的資料保安措施。

機構建立個人資料庫存的首要目標，是瞭解收集的個人資料類型，以及如何處理該等個人資料。

定期檢查和更新個人資料庫存（至少每年進行一次），可讓機構瞭解所持有最新、最準確的個人資料。



維護個人資料庫存的好處

- 資料庫存可準確提供資料位置和收集的資料元素，有助資料當事人查閱及/或改正對資料。
- 瞭解機構從資料當事人收集的個人資料之類型和數量。
- 確定要採取的保安措施級別（例如保安管控措施的嚴格程度應與個人資料的敏感程度相應）
- 如果發生資料外洩，可以通過查找個人資料的類型和數量以及時評估影響。

您可參閱私隱專員發佈的《私穩管理系統：最佳行事方式指引》第12頁有關個人資料庫存的範本：
https://www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf

私隱影響評估

什麼是私隱影響評估？

私隱影響評估是系統的風險評估工具，在推行需要收集個人資料的項目或計畫時可納入決策過程。

何時須進行私隱影響評估？

- 新的程序或修改現有的程序可能會為個人帶來高度風險時
- 直接促銷活動中收集大量/敏感的個人資料時
- 推出新計畫或項目需要收集/使用大量個人資料時
- 當規管個人資料的法例有具體改動時
- 準備委任資料處理者代為處理個人資料時
- 更改資訊科技系統基礎設施時

私隱影響評估為何不可缺少?

私隱影響評估可以在項目實施之前，識別和檢測任何與項目相關的私隱問題，為機構提供「預警」。機構應進行評估，以有效管理項目可能涉及的私隱風險：

- 由機構或由機構任命的代理人處理、儲存或分析個人資料；
- 使用可能侵犯公眾私隱的科技（例如在工作場所安裝閉路電視）；
- 機構常規的重大修改或增加個人資料的收集、處理或共享的數量和範圍。

私隱影響評估的目的

- 解決私隱問題
- 有助決策
- 保證資料來源的可靠性
- 以經濟有效的方式降低私隱風險
- 設定基準

您可參閱私隱專員發佈的《私穩管理系統：最佳行事方式指引》第15頁有關私隱影響評估的範本：
https://www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf

《收集個人資料聲明》

什麼是《收集個人資料聲明》？

《收集個人資料聲明》（《聲明》）是指資料使用者（例如NGO）在收集個人資料時或之前，向資料當事人提供的聲明。該《聲明》是一項重要工具，旨在遵守《條例》中資料收集原則下的通知要求。為避免機構與資料當事人之間產生誤解，機構應以書面形式提供《聲明》所需的公開資料。

《聲明》中包含的關鍵元素

01

目的：所收集到的個人資料之用途，如義工招募、籌款等。

02

提供個人資料是強制的還是自願的：如資料當事人有義務提供個人資料，機構應解釋不提供資料的後果。

03

潛在承轉人：機構可能會向其他人士或機構轉移及共享從資料當事人取得的個人資料，如社會福利署和服務合作夥伴等。

04

直接促銷：如機構使用個人資料作直接促銷，必須事先取得資料當事人的訂明同意。如讓個人在《聲明》中做相應勾選，以表明他們是否允許機構將其個人資料用於直接促銷。

05

查閱及改正個人資料權利：告知資料當事人擁有查閱及改正其個人資料的權利。

06

查閱及改正要求的聯絡方式：處理資料查閱及改正要求的負責人之姓名（及/或職銜）和聯絡方式。

撰寫《聲明》的良好做法

清楚陳述目標

讓資料當事人明確收集和使用其個人資料之目的。

採用淺白易明的語言和表達方式

建議《聲明》在長度、複雜程度、字體及無障礙程度方面，以易讀易明的方式呈現。

保安措施聲明

建議《聲明》中包含有關機構為保障個人資料而採取的保安措施。

鏈接到《私隱政策聲明》

可就機構的《私隱政策聲明》內容提供網頁鏈接，提醒資料當事人注意。

您可參閱私隱專員發佈的《擬備收集個人資料聲明及私隱政策聲明指引》：
https://www.pcpd.org.hk/chinese/publications/files/GN_picspps_c.pdf

資料外洩事故應變

甚麼是資料外洩？

個人資料外洩是指涉嫌違反機構規定的個人資料保安，令該等資料面臨未經授權或意外的查閱、處理、刪除、遺失或使用的風險。以下是資料外洩的例子：

01 遺失帶有個人資料的打印文件

02 通過電子郵件意外傳輸個人資料

03 未經授權查閱個人資料系統

從多方面來說，個人資料外洩代價高昂。機構應考慮制定處理外洩事故的程序，並在可行情況下，指定資料外洩回應小組承擔相關的角色和職責。該小組可由保障資料主任（如已在機構內任命）以及相關部門/團隊的資料私隱代表（們）領導。小組成員應包括來自保障資料辦公室、傳訊及公共關係部門、資訊科技部門、法律及秘書部門以及人力資源等各部門的代表。

資料外洩的遏制措施

一旦發現資料外洩，機構應立即決定採取相應措施遏制洩漏，將影響範圍減至最低程度，並儘快採取補救方案。機構可考慮以下遏制相應措施：

- 因系統故障導致的資料外洩，應停止有關系統的運作
- 更改用戶密碼和系統配置以控制查閱和使用
- 確定是否需要技術援助來修復系統漏洞和/或阻止黑客入侵
- 停止或更改涉嫌造成或促成資料外洩的個人的查閱權限
- 保留資料外洩證據以方便調查。如有需要，建立圖像備份作調查之用
- 若涉犯罪活動則通知有關當局（即私隱專員）和/或報警處理
- 在不影響當前運作下，對系統中敏感及關鍵資料作出保護，如將資料移至其他媒介
- 指示資料處理者採取即時補救措施

您可參閱私隱專員發佈的《資料外洩事故的處理及通報指引》資料：
https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/DataBreachHandling2015_c.pdf

直接促銷和「拒絕服務」選擇

直接促銷

直接促銷的活動是關於(1)提供或宣傳商品、設施或服務、或(2)為慈善、文化、公益、康體、政治或其他目的尋求捐贈或貢獻。

直接促銷包括通過郵件、傳真、電子郵件、電話或其他通訊方式向特定的人群(按姓名傳訊給特定人士)發送資訊或商品。

根據資料的使用原則,機構如欲將個人資料用於直接促銷活動,則須在《收集個人資料聲明》內列明,並應在首次為其他指定用途收集此類資料時取得資料當事人的訂明同意。

是否屬於直接促銷活動?

直接促銷例子

- 發送到指定個人手機號碼的直接促銷短信
- 機構通過電話或電子郵件聯絡現有服務使用者推廣近期的活動

非直接促銷例子

- 對不明身份的某一電話號碼使用者進行電話推銷,以推廣機構提供的服務
- 郵寄到某一地址而沒有指定收件人的郵件
- 不推廣其他服務的活動詳情通知

「拒絕服務」選擇

「拒絕服務」選擇指不論資料當事人是否事先給予同意,可隨時要求機構停止在直接促銷活動中使用其個人資料。

機構收到資料當事人的通知後,必須停止使用該個人資料及不收取任何費用。當機構收到資料當事人的「拒收直接促銷訊息要求」後,可能需要評估是否要刪除已經表明拒收意向的個人資料,然後相應地作刪除。

《收集個人資料聲明》中的《拒收直接促銷訊息聲明》例子

您可隨時行使「拒絕服務」權來撤回我們將你的資料用於直接促銷的同意。此後,我們會停止將您的資料用於直接促銷活動。

如您有撤銷意願,請聯絡我們的保障資料主任 (姓名及聯絡方式) 。

您可參閱私隱專員發佈的《直接促銷新指引》資料:
https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/GN_DM_c.pdf

如對此指南內容有任何疑問，請聯絡:

賀琪偉
風險及控制服務主管合夥人
羅兵咸永道中國內地及香港
jennifer.cw.ho@hk.pwc.com

鍾嘉鈺
合夥人
羅兵咸永道香港
kristine.ky.chung@hk.pwc.com

顧裕華
高級經理
羅兵咸永道香港
shirley.y.gu@hk.pwc.com