資料來源：香港個人資料私隱專員公署

私隱管理系統
最佳行事方式指引(上)

機構在業務運作上會處理不少個人資料，例如客戶及員工的個人資料。隨著公眾及客戶對個人資料私隱保障的期望與日俱增，機構停留在僅符合法律規定層面的態度已不合時宜。

香港個人資料私隱專員自 2014 年起，提倡各機構建立自己的私隱管理系統，由最高管理層（例如董事會）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。這不但可加強客戶的信任，更可從而提升商譽及加強競爭優勢。

事實上，歐洲聯盟於 2018 年 5 月 25 日生效的《通用數據保障條例》（可參閱《香港印刷》127 期）亦已明確納入問責原則，由此可見，機構建立全面私隱管理系統已成為世界的大趨勢。以下將分享由香港個人資料私隱專員公署發出的《私隱管理系統：最佳行事方式指引》，為機構在建立全面私隱管理系統方面提供框架，並輔以具體例子及實用建議以供參考。

實施私隱管理系統的好處

- 減低事故發生（例如個人資料外洩）的風險。
- 有效管理所收集的個人資料。
- 有助遵從《個人資料（私隱）條例》的規定。
- 一旦有事故發生，機構亦有完善的機制處理，將事故造成的損害減至最低。
- 顯示有決心體現良好企業管治，藉此建立客戶及員工的信任。
- 提升商譽、競爭優勢以至潛在商機。

私隱管理系統的組件

要建立全面的私隱管理系統，機構必須培養員工保障個人資料私隱的意識，並制訂處理個人資料的政策及程序予員工遵守，以確保機構處理個人資料的做法符合《個人資料（私隱）條例》（「條例」）的規定。

私隱管理系統包括以下三個組件：

以下將會詳細闡述上述各個組件，並輔以例子作參考之用。請注意，此指引中所提供的建議、例子及文件範本等並非放諸四海皆準的方案，每個機構應視乎其特定的情況（例如規模、業務性質、所處理的個人資料等）建立適合的私隱管理系統。

1. 機構的決心

在機構的管治架構內培養尊重個人資料私隱的文化是首要的組件。機構應設立相應的內部管治架構，確保機構內有關保障個人資料的政策和程序得以落實及執行，以顯示機構以負責任的態度處理個人資料及遵守條例的規定。

1.1 最高管理層的支持

機構要做到「問責」，必需由上而下（即由最高管理層至員工）進行，這樣才能顯示機構保障個人資料私隱的決心及重要性，而尊重個人資料私隱的文化及私隱管理系統才得以建立。

最高管理層應：

- 透過員工會議或通告，向全體員工表達支持建立尊重個人資料私隱的文化及承諾推行私隱管理系統。
- 委任保障資料主任。
- 對系統管控措施及整個私隱管理系統給予認可。
- 分配足夠的資源（包括財政及人手）以推行私隱管理系統。
- 主動參與私隱管理系統的評估及檢討。
- 定期在董事局匯報私隱管理系統的運作情況。

1.2 委任保障資料主任／設立保障資料部門

機構應指派專責人員（即「保障資料主任」）全面監督機構是否有遵從條例的規定及推行私隱管理系統。在大規模的機構應由高級行政人員出任保障資料主任，而在小型機構則可能是由公司擁有人／營運者出任。

保障資料主任通常負責建立、設計及管理私隱管理系統（包括所有程序、培訓、監察／審核、記錄、評估及跟進）。在大規模的機構，由於部門數目較多，所處理的個人資料亦會較多，單靠保障資料主任難以有效推行私隱管理系統，因此，較理想的做法是各個主要部門均設有部門協調主任，支援保障資料主任。無論如何，機構應投入資源，培訓保障資料主任及／或其團隊成為保障個人資料私隱的專才。

在規模較大的機構中，保障資料部門架構及各人員的職責可參考如下：

例子一：保障資料部門架構

角色	出任的人員	
保障資料主任	總經理（行政部）	
個人資料私隱主任	高級經理（行政部）	
部門協調主任	**部門**	**出任的人員**
	行政部	經理
	資訊科技部	高級經理
	機構傳訊部	高級經理
	法律部	高級經理
	市場推廣部	高級經理

保障資料主任的職責

i. 建立及實施系統管控措施，包括：
- 保存機構的個人資料庫存、指示及監督各部門每年更新個人資料庫存。
- 指示各部門進行定期的私隱風險評估，並就各部門所遞交的私隱風險評估報告作出監督、檢討及提供意見。
- 就進行私隱影響評估作出監督、檢討及提供意見。
- 向員工提供培訓及教育，提高員工保障個人資料私隱的意識，並定期傳閱機構的個人資料私隱政策、指引及其他與個人資料私隱有關的資訊，以及在作出修訂後通知員工。
- 協調及監督私隱外洩事故的處理，並對調查事故方面提供意見。
- 就部門對資料處理者的管理提供意見，並進行檢討。
- 就相關部門擬備「收集個人資料聲明」進行監督、檢討及提供意見。

ii. 檢討私隱管理系統的成效，當中包括擬備監督及檢討計劃，並因應檢討的結果修訂及更新私隱管理系統和系統管控措施。

iii. 定期向最高管理層匯報機構的循規情況、所遇到的問題、接獲與個人資料私隱有關的投訴等。

個人資料私隱主任的職責

- 協助保障資料主任實施私隱管理系統。
- 處理與個人資料私隱有關的投訴及查詢。
- 處理查閱及改正個人資料要求。

部門協調主任的職責

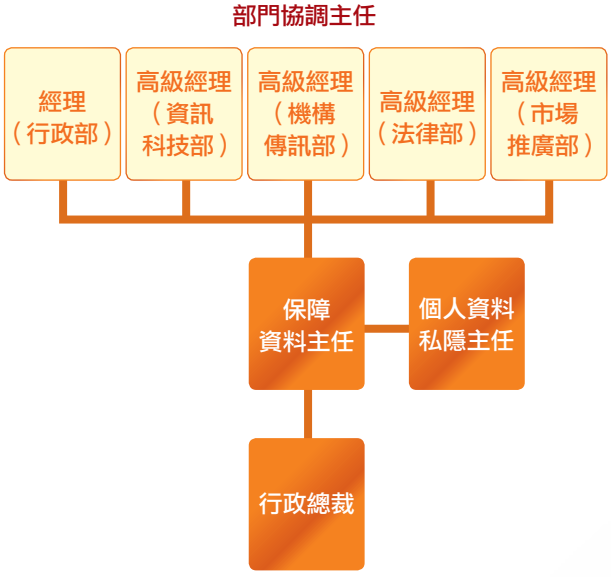
- 管理所屬部門的私隱管理系統，並代表所屬部門與保障資料主任就與系統有關的事宜聯繫。
- 每年更新部門的個人資料庫存。
- 為所屬部門進行定期的私隱風險評估，並將評估報告交予保障資料主任審視。
- 就部門對資料處理者的管理進行檢討，並將檢討結果交予保障資料主任審視。
- 確保部門擬備的「收集個人資料聲明」符合條例的規定，並將擬備的「收集個人資料聲明」交予保障資料主任審視。
- 協助保障資料主任進行私隱管理系統的持續評估及修訂。

1.3 建立匯報機制

機構應建立內部匯報機制，清楚訂明負責執行及管理私隱管理系統的人（例如部門協調主任及保障資料主任），報告機構整體的循規情況、所遇到的問題、接獲與個人資料私隱有關的投訴或可能發生私隱外洩事故時的匯報架構及程序。最高管理層在掌握這些資訊後可進一步向董事局匯報。

就上述例子一的情況，機構就私隱管理系統的匯報架構可參考如下：

例子二：私隱管理系統的匯報架構



在某些時候，例如因保安措施失效而導致資料外洩事故的發生，或接獲投訴時，機構應考慮把事故提升至更高的層面處理。在回應事故的過程中，專責人員和解決問題所需的人士都應參與其中。對大型機構而言，這可能牽涉來自資訊科技、法律及機構傳訊範疇的代表。機構應清楚訂明如何及何時把事件升級，並向員工清楚解釋。此外，機構應記錄所有匯報程序。

2. 系統管控措施

系統管控措施是指一些協助機構建立私隱管理系統的措施。透過這些管控措施，機構可確保其處理個人資料的做法符合條例的規定。

2.1 個人資料庫存

不同的機構收集個人資料的方法、所收集得的個人資料的類別、儲存資料的地點及保留期間、如何使用有關個人資料及所採取的資料保安措施不盡相同。機構應清楚了解他們收集及處理個人資料的情況，並記錄在個人資料庫存內，因為這有助機構：

- 了解應向資料當事人徵求何種方式的同意。
- 決定如何保護有關資料（例如資料的敏感度愈高，所需要的保安程度亦愈高）。
- 依從查閱及改正資料要求。
- 若機構的資料庫遭黑客入侵以致個人資料外洩，機構便可透過翻查個人資料庫存知悉該資料庫載有哪些個人資料、涉及的個人資料是否有加密等，以便機構就事故作出評估及採取相應的補救措施。

機構應每年更新其個人資料庫存，確保已將持有的所有個人資料記錄在個人資料庫存中。就此，機構應訂立更新個人資料庫存的程序，述明何時進行有關更新、負責的人員、更新及檢視的流程、負責存檔的人員等。

私隱專員建議機構每年要求各部門更新其個人資料庫存，理由是部門較為清楚本身持有的個人資料的情況。部門協調主任將已更新的個人資料庫存交予保障資料主任審閱及存檔。

以下是個人資料庫存的樣本，供參考之用。

例子三：個人資料庫存樣本

部門	行政部	市場推廣部
紀錄的種類	人事檔案	會員檔案
所載有的個人資料	僱員的個人資料： - 姓名 - 身份證副本 - 聯絡資料（包括地址、手提電話號碼及電郵地址）	會員的個人資料： - 姓名 - 聯絡資料（包括地址、手提電話號碼及電郵地址）
收集資料的方法／途徑	僱員資料表格	會員申請表
收集及使用資料的目的	處理與僱傭有關的事宜	處理與向會員提供產品服務有關的事宜
資料的保留期間	有關員工離職日期起計七年	有關會員取消會籍後一年
資料的儲存地點	實體檔案： 人事檔案室內的文件櫃	實體檔案： 市場推廣部的文件櫃 電子檔案： 市場推廣部的電腦網絡硬碟
是否會披露予第三者（包括資料處理者）及該第三者的名稱和相關資料（是／否）	否	資料會交予服務承辦商進行電話推廣
資料可能會被轉移至何處（例如雲端的位置）	不適用	服務承辦商的電腦網絡硬碟
有關資料披露的目的及是否符合《個人資料（私隱）條例》的規定	不適用	進行電話推廣（已取得資料當事人的同意可進行直接促銷）
資料處理者退回或銷毀有關資料的日期（如適用）	不適用	服務承辦商會在合約期屆滿後七日內銷毀有關資料
所採用的保安措施	文件櫃已上鎖，只有人力資源部總經理及人事主任才持有該文件櫃的鑰匙	市場推廣部的文件櫃已上鎖，只有市場推廣部的職員才持有該文件櫃的鑰匙 市場推廣部的電腦網絡硬碟只有市場推廣部的職員才獲授權查閱

2.2 處理個人資料的內部政策

機構應制定內部政策，以確保機構在處理個人資料方面的做法符合條例的規定，並定期向員工傳達相關政策。如政策內容有所更新，應立即通知員工。

一般來說，機構處理個人資料的內部政策，應涵蓋處理個人資料的整個生命週期（即條例附表一的六項保障資料原則），機構可參考下表：

例子四：處理個人資料的內部政策

保障資料第 1 原則	個人資料的收集，包括： • 處理透過熱線電話作出查詢 • 電話錄音 • 使用閉路電視進行監察 • 收集身份證號碼及副本
保障資料第 2 原則	個人資料的準確性及保留期間 • 與僱傭有關的個人資料保留期（例如落選的求職者的個人資料不得保留超過兩年、前僱員的個人資料不得保留超過七年） • 與客戶交易有關的資料保留期
保障資料第 3 原則	個人資料的使用，包括： • 徵求同意的規定 • 處理監管機構、執法機關及政府部門要求索取個人資料
保障資料第 4 原則	個人資料的保安，包括： • 載有個人資料的實體文件保安 • 資訊科技方面的保安（例如使用載有個人資料的「自攜裝置」時應採取的保安措施） • 指示外判的服務承辦商在處理個人資料時需採取的保安措施
保障資料第 5 原則	私隱政策聲明的透明度
保障資料第 6 原則	處理查閱及改正個人資料要求的步驟
條例第 35A 條	• 在使用個人資料進行直接促銷前需採取的行動 • 處理「拒收直銷訊息要求」的步驟

2.3 風險評估工具

個人資料的私隱風險可隨時間而改變。為確保機構的私隱政策及實務持續地遵從條例的規定，進行定期私隱風險評估及私隱影響評估是任何私隱管理系統不可或缺的一環。

2.3.1 定期私隱風險評估

機構每年應選取不同部門／所有部門進行定期私隱風險評估，以確保機構的私隱政策及實務符合條例的規定。機構可參考以下進行定期風險評估的步驟：

步驟 1
保障資料主任通知部門協調主任進行定期私隱風險評估，並提供定期風險評估問卷（見下頁例子五）。

步驟 2
部門協調主任將填妥的定期私隱風險評估問卷交予保障資料主任。

步驟 3
保障資料主任檢視填妥的定期私隱風險評估問卷，如發現有不符合條例規定的地方，應通知相關的部門協調主任並取得進一步資料。

步驟 4
相關的部門協調主任與部門主管及保障資料主任商討，採取相應措施以糾正不符合條例規定的地方。

步驟 5
如機構沒有發現有不符合條例規定的地方／已採取相應措施糾正不符合條例規定的地方，保障資料主任可將已簽署的定期私隱風險評估問卷存檔。

以下是定期私隱風險評估問卷的樣本，供參考之用。

例子五：定期私隱風險評估問卷的樣本

問題	是／否	數目	需採取的進一步行動
甲．涉及個人資料的新計劃或現有計劃的改動			
1. 在過去36個月內，所屬部門是否有涉及個人資料的新計劃或現有計劃的改動，當中包括個人資料的收集、使用和處理（例如新的處理個人資料程序、推行新系統等），並請說明有關計劃的數目？ 如「是」，請繼續回答下述問題（2）至（4）。 如「否」，請繼續回答下述乙部的問題。	（ ）是 （ ）否		
2. 是否有就上述新計劃或現有計劃的改動中所涉及的個人資料更新個人資料庫存？	（ ）是 （ ）否		如「否」，請立即更新個人資料庫存並交予保障資料主任。
3. 是否有就上述新計劃或現有計劃的改動進行私隱影響評估並交予保障資料主任？此外，請說明已進行私隱影響評估的計劃名稱。	（ ）是 （ ）否		如經審慎考慮後認為毋需進行私隱影響評估，請確保已妥善記錄有關的理據。
4. 如已進行私隱影響評估，該評估的內容及結果是否仍然適用（舉例來說，如出現新轉變或新的方法以解決有關私隱風險，便可能需要更新私隱影響評估詳情）？	（ ）是 （ ）否		如「否」，請更新私隱影響評估的文件，並交予保障資料主任。
乙．資料外洩事故			
5. 在過去36個月內，所屬部門是否曾發生資料外洩事故？ 如「是」，請繼續回答下述問題（6）至（7）。 如「否」，請繼續回答下述丙部的問題。	（ ）是 （ ）否		
6. 是否有就每宗資料外洩事故填寫「資料外洩事故表格」並交予保障資料主任？	（ ）是 （ ）否		如「否」，請填寫「資料外洩事故表格」並交予保障資料主任。
7. 該宗／該些資料外洩事故是否已受控制？	（ ）是 （ ）否		

問題	是／否	數目	需採取的進一步行動
丙．所收到的投訴			
8. 在過去36個月內，所屬部門是否曾被投訴不當處理個人資料？ 如「是」，請繼續回答下述問題（9）。 如「否」，請繼續回答下述丁部的問題。	（ ）是 （ ）否		
9. 是否已將上述投訴個案向保障資料主任匯報？請說明有關投訴個案的編號。	（ ）是 （ ）否		如「否」，請立即將有關投訴個案向保障資料主任匯報。
丁．新聘用的資料處理者			
10. 在過去36個月內，所屬部門是否曾聘用資料處理者代為處理個人資料？ 如「是」，請繼續回答下述問題（11）。 如「否」，請繼續回答下述問題（12）。	（ ）是 （ ）否		
11. 是否有檢視部門對資料處理者的管理，並填寫「資料處理者檢視清單」並交予保障資料主任？	（ ）是 （ ）否		如「否」，請填寫「資料處理者檢視清單」並交予保障資料主任。
戊．個人資料的保留期間			
12. 所屬部門是否已銷毀／刪除所有保留期間已屆滿的個人資料？	（ ）是 （ ）否		如「否」，請立即安排銷毀／刪除所有保留期間已屆滿的個人資料。

由部門協調主任填寫

簽署 _____

姓名 _____

職位 _____

日期 _____

由保障資料主任審閱

簽署 _____

姓名 _____

職位 _____

日期 _____

下期《香港印刷》將刊登其他有關風險評估、資料外洩事故的處理等內容，敬請留意。

UPM Finesse Classic Matt, 80 gsm