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（下）

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的層面的態度已不合時宜。機構建立全面私隱管理系統已成為世界的大趨勢，上期《香港印刷》已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》上半部分，今期將刊載指引的下半部分，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。

（承上期）

2. 系統管控措施

2.4 培訓及教育推廣

健全的私隱管理系統有賴機構中的各個員工都知悉其保障個人資料的責任，並付諸實行。因此，機構應針對相關員工的特定需要而提供培訓及教育，並傳達最新資訊。此外，機構應記錄其培訓安排，評估參與度和成效。

例子七：向員工提供有關保障個人資料私隱的培訓及教育推廣活動的建議

範疇	方法／渠道
了解條例的規定	▸ 安排職員參加私隱專員舉辦的專業研習班，或機構的內部培訓 ▸ 在機構的內聯網提供必修的培訓課程單元 ▸ 每月電子通訊或在機構政策的培訓課程中加入相關的單元
了解機構的私隱管理系統	▸ 向新入職員工簡介相關的資訊，並定期（例如每六個月）向所有員工傳閱有關內容
新發出／修訂的個人資料私隱政策及指引	▸ 每當機構發出新的個人資料私隱政策及指引，或就現有的相關政策及指引作出修訂後，應盡快將有關的資訊傳達予所有員工
個案分享	▸ 機構可將被投訴有關不當處理個人資料的個案，或資料外洩的個案，向員工分享，並教導員工條例的相關規定、恰當的做法及如何避免同類事件再次發生
私隱影響評估結果	▸ 機構可將私隱影響評估中所發現的私隱風險及機構所採取的相應措施向員工分享

2.5 資料外洩事故的處理

近年因網絡保安事故而引致個人資料外洩事故的數目有上升趨勢，若機構沒有就資料外洩事故訂立處理的程序及委任專責人員處理，一旦發生資料外洩事故，機構或要付上沉重的代價。

下圖顯示沒有就資料外洩事故訂立處理的程序而可能帶來的問題：

機構在處理資料外洩事故時，可參考以下的步驟：

雖然條例沒有強制規定機構向私隱專員通報資料外洩事故，但近年不少機構在發現資料外洩事故後，都自願依從私隱專員的建議，盡早作出通報以妥善處理有關事故。私隱專員發出的《資料外洩事故的處理及通報指引》在這方面提供了實際的指引。

機構可參考以下的「 資料外洩事故表格 」，當發生資料外洩事故時，有關部門可填寫該表格以整合事故的資料，盡快採取補救行動，並進行事後評估。

例子八：資料外洩事故表格樣本

組別／部門	
組別／部門	
(I) 事故的資料	
(i) 基本資料	
描述事故的情況	
發生事故的日期及時間	
發生事故的地點（例如哪個辦公室、哪個電腦伺服器等）	
發現事故的日期及時間	
如何發現事故（例如在進行恒常的系統檢查時、傳媒報道後知悉等）	
事故的性質（例如資料遺失、資料庫被入侵等）	
事故的起因	
(ii) 事故的影響	
資料當事人的類別（例如員工、客戶、市民等）	
估計涉及的資料當事人數目（請就各項類別的資料當事人說明人數）	
涉及的個人資料類別（例如姓名、出生日期、身份證號碼、地址、電話等）	
載有相關個人資料的媒介（例如實體文件夾、USB 等）	
如相關個人資料是載於電子媒介，資料是否已加密？	
(II) 向監管機構進行資料外洩通報	
是否有將事故向監管機構，例如香港警務處、私隱專員等作出通報？ 如**是**，請提供通報日期及通報的內容。	
(III) 為遏止事故擴大而已採取的行動／將會採取的行動	
簡述為遏止事故擴大而**已採取**的行動	
請評估上述行動的成效	
簡述為遏止事故擴大而**將會採取**的行動	
(IV) 事故可能造成的損害	
請評估事故對資料當事人可能造成的損害	

（續下頁）

(V) 通知受影響的資料當事人	
向受影響的資料當事人作出通知的日期及通知內容	
若不會向受影響的資料當事人作出通知，請述明原因	
(VI) 調查結果	
事故的起因	
(VII) 事後檢討（由保障資料主任填寫）	
建議的改善措施及實施日期	
就上述改善措施進行成效檢討的日期	

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 _____

2.6 對資料處理者的管理

機構將處理個人資料的工作外判予代理人的情況日益普遍。機構須知道，根據條例的規定，若資料處理者不當處理個人資料（例如沒有採取足夠的保安措施以致資料外洩），作為主事人的機構須對資料處理者的有關作為負責。因此，機構在考慮委託資料處理者代為處理個人資料時，應考慮以下事項：

機構是否有實際需要委託資料處理者處理個人資料？

是

- 只將最少的個人資料交予資料處理者
- 採取合約規範或其他方法保障委託予資料處理者處理的個人資料
- 每年檢視對資料處理者的管理是否足夠及全面

機構委以資料處理者的責任應包括：

資料處理者須採取的保安措施	適時交還、銷毀或刪除不再需要的個人資料	禁止將個人資料作其他用途及披露	禁止資料處理者將服務分判給其他服務供應商
報告不尋常的徵兆	採取措施確保合約員工履行已同意的責任	接受機構的審核及視察	承擔違反合約的後果

有關外判個人資料的處理予資料處理者需要注意的事項，請參考私隱專員發出的《外判個人資料的處理予資料處理者》資料單張。

值得注意的是，《通用數據保障條例》除了要求資料控制者的資料處理活動（包括委託資料處理者代為處理個人資料）符合《通用數據保障條例》的要求外，亦對資料處理者施加直接的責任。換句話說，資料處理者是直接受條例所規管，違反條例相關要求可被判罰。

如機構有委託資料處理者（不論境內或境外）代為處理個人資料，應每年檢視對資料處理者的管理是否足夠及全面。機構可制定檢視資料處理者的清單，在上述年檢時使用。

以下是機構在檢視其對資料處理者的管理時使用的清單樣本，供參考之用。

例子九：機構檢查其對資料處理者的管理清單樣本

甲部：背景資料	
部門名稱	
資料處理者名稱	
委託資料處理者的目的	
簡述涉及的個人資料	
委託資料處理者的日期	

乙部：檢視機構對資料處理者的管理		
問題	**是／否（如「否」，請說明理由及理據）**	**備註**
(1) 與資料處理者簽訂的合約中有否述明機構有權審核及視察資料處理者如何處理及儲存個人資料？		
(2) 與資料處理者簽訂的合約中有否規定資料處理者必須即時報告任何不尋常徵兆、保安違規或遺失個人資料等情況？		
(3) 與資料處理者簽訂的合約中有否規定除了受託進行的目的之外，資料處理者不得為其他目的而使用或披露有關個人資料？		
(4) 與資料處理者簽訂的合約中有否涵蓋有關資料處理者可否將受託提供的服務分判？		
(5) 與資料處理者簽訂的合約中有否規定資料處理者須適時交還、銷毀或刪除有關資料？		
(6) 與資料處理者簽訂的合約中有否列明資料處理者所須採取的保安措施，以保障受託的個人資料及遵從條例的規定（請列明有關保安措施）？		
(7) 與資料處理者簽訂的合約中有否述明違反合約的後果？		

（續下頁）

問題	是／否（如「否」，請說明理由及理據）	備註
(8) 部門是否認為資料處理者有履行合約中有關保障個人資料的責任？如「是」，請詳細說明。		
(9) 如對上述（8）的答案為「否」，請詳述部門就此所作出的跟進行動。		
(10) 部門在過去36個月內有否審核及視察（包括突擊檢查）資料處理者處理及儲存個人資料的情況？ 如「有」，請述明： 10.1 進行審核及視察的日期； 10.2 有否發現任何不尋常的情況； 10.3 有否採取任何跟進行動。 如「否」，請說明理由。		
(11) 如部門在本年度有對資料處理者進行審核及視察，部門是否有發現任何不尋常的情況？ 如「有」，請詳述有關情況及資料處理者對此採取哪些改善措施。		
(12) 是否曾發生由資料處理者引起的資料外洩事故？ 如「是」，請詳述有關情況，並附上資料外洩事故表格副本。		

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 _____

2.7 溝通

機構應採取所有切實可行的步驟，以清晰及易於理解的文字告知員工及客戶有關機構的個人資料政策及實務，包括：

- 透過收集個人資料聲明及私隱政策聲明，讓員工及公眾知道機構收集、使用及披露個人資料的目的，以及保留資料多久
- 告知公眾如有需要提出問題或關注時可聯絡的機構專責職員
- 告知公眾如何向機構提出查閱／改正個人資料要求
- 讓公眾容易獲取相關資訊（例如機構可將其個人資料私隱政策及實務上載於機構的網站，及將有關資訊的列印本放於機構的辦事處供公眾取閱）

機構可參考私隱專員發出的《擬備收集個人資料聲明及私隱政策聲明指引》。

3. 持續評估及修訂

私隱管理系統並非一次性的措施，而是要透過不斷的監察及評估系統內的措施、政策和程序，並在有需要時作出修訂，以確保系統行之有效。

保障資料主任應每年制定監督及檢討計劃，以及評估和修訂系統管控措施。

3.1 制定監督及檢討計劃

保障資料主任應擬備監督及檢討計劃，當中須：

(i) 涵蓋所有系統管控措施的施行
(ii) 涵蓋所有與個人資料私隱有關的政策及程序
(iii) 述明於何時、如何及由哪些人士進行評估，並釐定評估準則
(iv) 定期進行評估（至少每年進行一次）
(v) 監督及檢討計劃應由最高管理層認可

以下是監督及檢討計劃的例子，供參考之用。

例子十：監督及檢討計劃

月份	監督及檢討活動
擬備監督及檢討計劃	
1至4	▸ 更新個人資料庫存 ▸ 檢視機構對資料處理者的管理 ▸ 進行定期風險評估 ▸ 更新培訓內容及培訓計劃
5至7	評估各項系統管控措施的成效，並作出相關修訂
8至10	檢視及修訂私隱管理系統操作手冊，及其他與個人資料私隱有關的政策和指引
11	向員工傳閱私隱管理系統操作手冊及其他與個人資料私隱有關的政策和指引
12	檢視監督及檢討計劃的執行，並擬備來年的監督及檢討計劃

保障資料主任可參考以下私隱管理系統成效檢討文件，以記錄已完成監督及檢討計劃中的事項，並交予最高管理層。

例子十一：私隱管理系統成效檢討文件樣本

活動	完成／未完成	上次完成檢討／更新的日期	所發現的問題及建議的跟進措施
(1) 更新個人資料庫存			
(2) 檢視機構對資料處理者的管理			
(3) 定期風險評估			
(4) 更新培訓內容及培訓計劃			
(5) 檢視及修訂私隱管理系統操作手冊，及其他與個人資料私隱有關的政策和指引			
(6) 向員工傳閱私隱管理系統操作手冊及其他與個人資料私隱有關的政策和指引			
(7) 檢視處理資料外洩事故的機制			

3.2 評估及修訂系統管控措施

機構應監察系統管控措施的成效，定期審核及在有需要時予以修訂。在決定系統管控措施是否有需要作出修訂前，機構可考慮以下因素：

- 有甚麼新的威脅及風險？
- 系統管控措施是否可以應付新的威脅和顧及最近的投訴或審核結果，或私隱專員發出的指引？
- 機構有沒有提供新的服務使個人資料收集、使用或披露有所增加？
- 是否需要提供培訓？如「是」的話，有沒有推行？是否有效？政策及程序是否獲得依從？系統是否切合最新情況？

如在監察過程中發現問題，有關人員應記錄及處理有關問題，並向最高管理層匯報關鍵事項。此外，機構如要改動系統管控措施，應即時通知員工，並為員工提供適當培訓以溫故知新。

結語

若機構僅視個人資料和私隱保障為遵從法例最低要求的事宜，而忽視或沒有充分回應客戶對私隱保障的期望，這樣是不足夠的。機構應用遠大的目光，以及以客戶為本的理念處理私隱保障。要達至此目標，就必需有機構最高管理層的支持，以建立和維持私隱管理系統，確保機構所有措施、項目和服務在設計階段已納入私隱保障的考慮；並在機構貫徹執行個人資料的保障。這種積極進取的態度，定能為機構、員工和客戶帶來三贏的局面。■

如參閱以下聯絡資料，以取得更多有關香港個人資料私隱專員公署的資訊。

香港個人資料私隱專員公署

查詢熱線：+852 2827 2827
傳傳傳真：+852 2877 7026
電傳傳郵：enquiry@pcpd.org.hk
網傳傳址：www.pcpd.org.hk/