私隱管理系統
Privacy Management Programme
最佳行事方式指引
A Best Practice Guide

PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

目 錄

引言

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。

香港個人資料私隱專員（**「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》**[1] 亦已明確納入問責原則[2]，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。

本指引旨在為機構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。

1 私隱專員發出的《歐洲聯盟《通用數據保障條例》2016》小冊子（於 2018 年 5 月 25 日生效），見私隱專員的網站：www.pcpd.org.hk/tc_chi/data_privacy_law/eu/files/eugdpr_c.pdf

2 《通用數據保障條例》第 5、24 及 25 條。

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
- 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
- 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

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：

1. 機構的決心

- **1.1** 最高管理層的支持
- **1.2** 委任保障資料主任 / 設立保障資料部門
- **1.3** 建立匯報機制

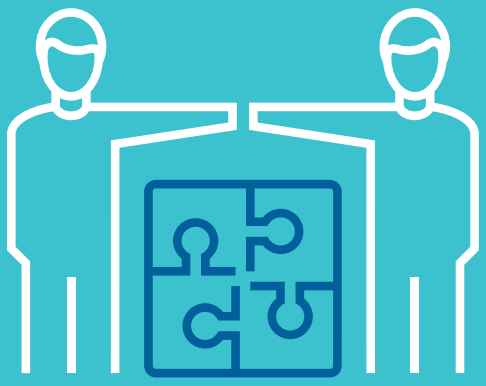
2. 系統管控措施

- **2.1** 個人資料庫存
- **2.2** 處理個人資料的內部政策
- **2.3** 風險評估工具
- **2.4** 培訓及教育推廣
- **2.5** 資料外洩事故的處理
- **2.6** 對資料處理者的管理
- **2.7** 溝通

3. 持續評估及修訂

- **3.1** 制定監督及檢討計劃
- **3.2** 評估及修訂系統管控措施

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，本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，及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[3] / 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。

例子一

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：—

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[4]
	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

3 《通用數據保障條例》第 37 條要求資料控制者（若屬某些類型的機構）須委任保障資料主任。

4 由於行政部的總經理及高級經理已分別出任機構的保障資料主任及個人資料私隱主任，為免角色重疊，行政部的部門協調主任一職由行政部的另一人員出任。

(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，及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

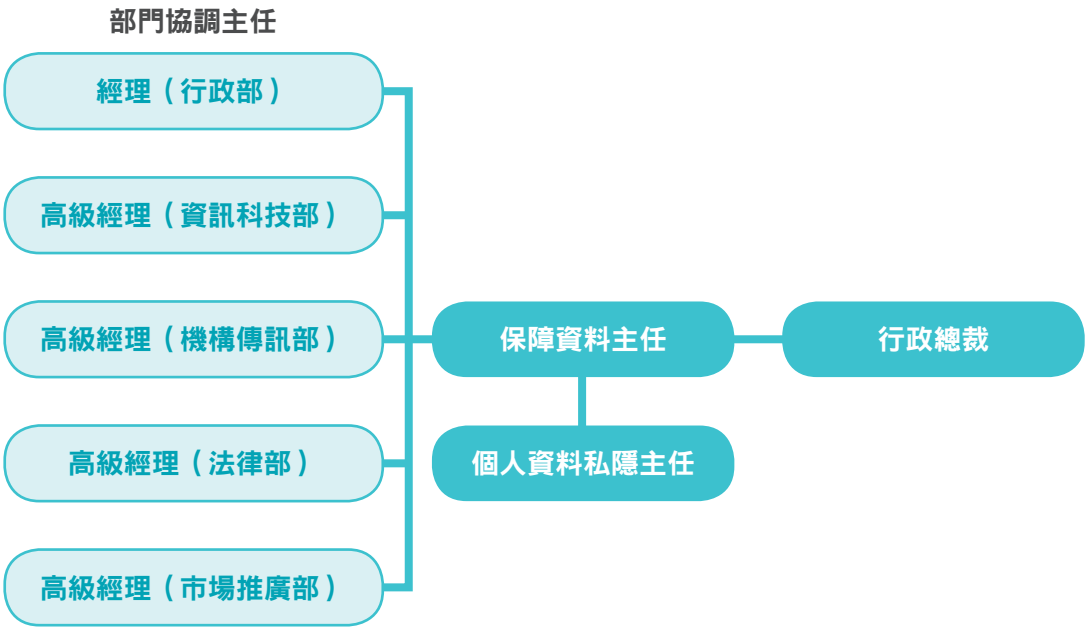
- 管理所屬部門的私隱管理系統，並代表所屬部門與保障資料主任就與系統有關的事宜聯繫
- 每年更新部門的個人資料庫存
- 為所屬部門進行定期的私隱風險評估，並將評估報告交予保障資料主任審視
- 就部門對資料處理者的管理進行檢討，並將檢討結果交予保障資料主任審視
- 確保部門擬備的「收集個人資料聲明」符合條例的規定，並將擬備的「收集個人資料聲明」交予保障資料主任審視
- 協助保障資料主任進行私隱管理系統的持續評估及修訂

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。

例子二

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：—



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[5]

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。

5 《通用數據保障條例》第 24 條要求資料控制者須實施技術性及機構性措施以確保循規。

2.1 個人資料庫存 [6]

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，及負責存檔的人員等。

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。

6 《通用數據保障條例》第 30 條要求資料控制者或處理者，可須保存其資料處理活動的記錄，包括處理的資料種類、使用資料的目的、轉移個人資料至第三國或國際機構 / 企業等，除非符合豁免情況。

例子三

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 7 年	有關會員取消會籍後 1 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路硬碟
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路硬碟
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 7 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路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）[7]，機構可參考以下例子四：—

例子四

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[8]） ▸ 與客戶交易有關的資料保留期[9]
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

7 機構可參閱私隱專員就各種保障資料範疇而發出的指引。

8 私隱專員發出的《人力資源管理實務守則》，見私隱專員的網站：www.pcpd.org.hk/tc_chi/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Chi_AW04_Web.pdf

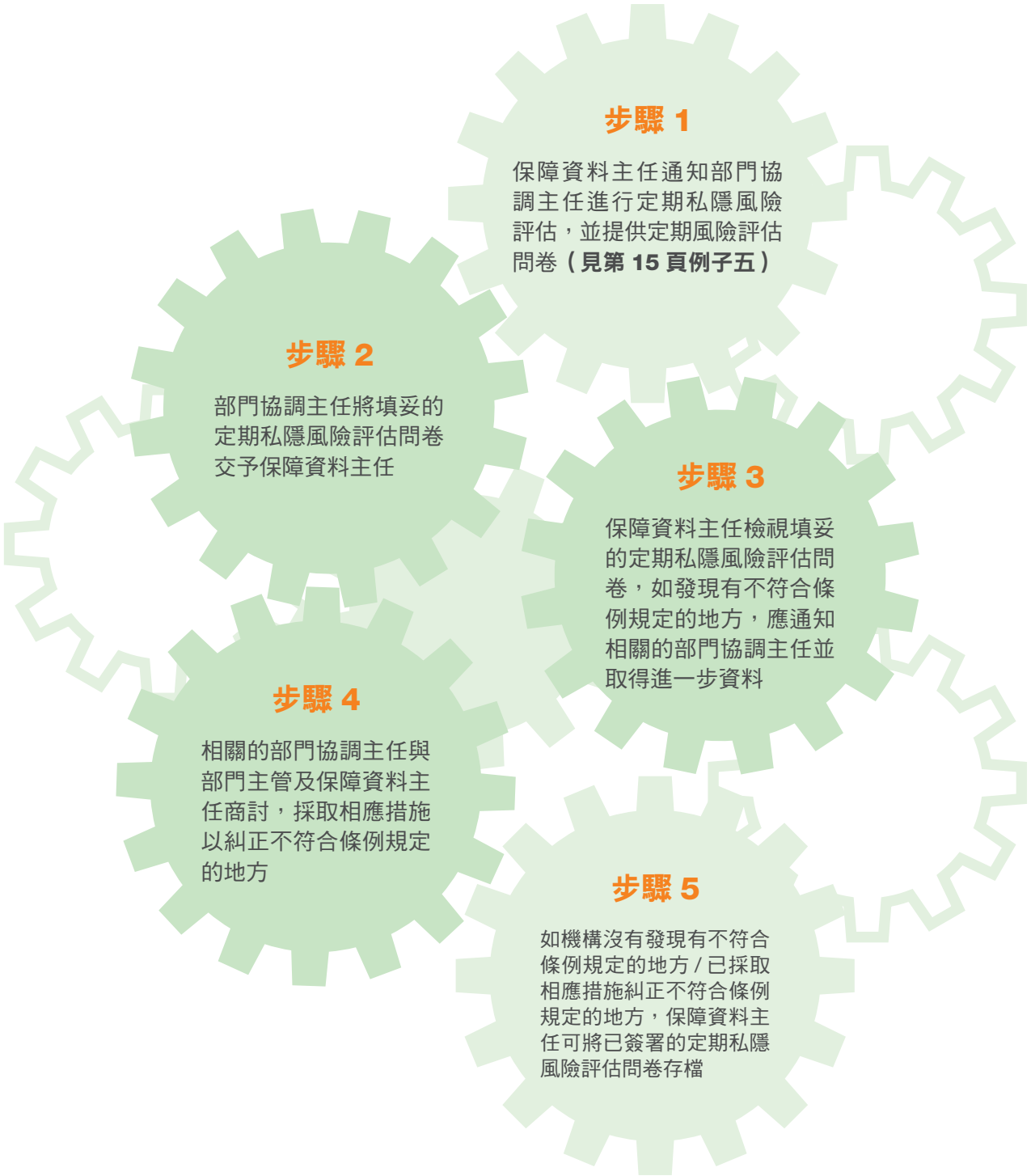
9 根據《稅務條例》第 51C 條，機構應保留交易記錄最少 7 年，詳情請參閱《稅務條例》全文。

2.3 風險評估工具 [10]

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 [11] 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：



10 《通用數據保障條例》第 35 條要求資料控制者須為高風險的資料處理活動進行資料保障影響評估。

11 在大規模的機構，由於涉及部門較多，故可每年選取個別部門進行定期風險評估。規模較小的機構，則可以每年對所有部門進行定期風險評估。

例子五

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		

續下頁

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 _____

2.3.2 私隱影響評估

機構在推出新項目、產品或服務前進行私隱影響評估，能協助機構及早發現潛在的私隱風險，並作出改善，以防患於未然。

何時需要進行私隱影響評估？

- 當規管個人資料的法規有重大改動時
- 機構對現行個人資料程序作出重大改動時
- 機構引入新的處理個人資料程序時
- 機構擬委託資料處理者代為處理個人資料時

機構應：

- 訂立內部政策，述明於何時進行私隱影響評估、評估的實際程序、誰人負責進行評估及檢視評估的結果
- 參考私隱專員發出的《私隱影響評估》資料單張 [12]
- 為增加透明度及顯示機構有保障個人資料私隱的決心，可將已進行的私隱影響評估內容上載於機構的網頁

例子六

以下是私隱影響評估問卷的樣本，供參考之用。

例子六 — 私隱影響評估問卷樣本

甲部：擬進行的改動 / 計劃之背景資料	
計劃名稱	
組別 / 部門	
負責同事（姓名及職位）	
預計實行時間	
描述收集有關個人資料的目的及處理流程	
擬收集的個人資料種類（如：姓名、出生日期、身份證號碼、地址、電話號碼等）	
預計涉及的資料當事人數目	
是否涉及資料處理者？如「是」，是否已採取合約規範方式或其他方法以確保資料處理者已對有關個人資料採取相應的保安措施，並請詳細描述相關措施。如「否」，請詳述理由。	( ) 是 ( ) 否
是否涉及跨境個人資料轉移？如「是」，請具體說明轉移的目的地及轉移的目的。	( ) 是 ( ) 否

續下頁

12 見私隱專員的網站：www.pcpd.org.hk//tc_chi/resources_centre/publications/files/InfoLeaflet_PIA_CHI_web.pdf

乙部：私隱風險分析		
範圍	私隱影響評估問題	組別 / 部門的回應
保障資料第 1 原則 — 收集個人資料的目的及方式 ▸ 資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。 ▸ 須採取所有切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移予甚麼類別的人。 ▸ 收集的資料是必須，但不超乎適度。	是否會告知資料當事人收集其個人資料的目的？如「否」，請說明理由。	( ) 是 ( ) 否
	是否只收集最少的個人資料（即不會收集超乎適度的資料）？ 請說明收集敏感個人資料的理由（包括但不限於）： ▸ 身份證號碼及其他身份代號（如護照號碼）[13] ▸ 生物特徵資料（如指紋）[14]	( ) 是 ( ) 否。收集敏感個人資料的理由： _____ _____ _____
	是否會在收集資料當事人的個人資料之前或之時，告知他他有責任提供個人資料抑或是可自願提供有關資料？如「否」，請說明理由。	( ) 是 ( ) 否，_____
	如資料當事人有責任提供有關個人資料，是否會告知他如不提供有關資料便會承受的後果？如「是」，請述明有關情況。如「否」，請說明理由。	( ) 是，_____ ( ) 否，_____ ( ) 不適用（資料當事人可自願提供有關個人資料）
	是否會將資料當事人的個人資料轉移或披露予第三者？	( ) 是 ( ) 否
	若有關個人資料會轉移予第三者或資料處理者，是否會告知資料當事人其個人資料會被轉移予甚麼類別的人？如「否」，請說明理由。	( ) 是 ( ) 否，_____ ( ) 不適用（有關個人資料不會披露予第三者）
保障資料第 2 原則 — 個人資料的準確性及保留期間 ▸ 資料使用者須採取所有切實可行的步驟，以確保持有的個人資料準確無誤，而資料的保存時間不應超過達致原來收集目的所需的時間。	是否有相關措施以確保所持有的個人資料準確性？如「是」，請詳述有關措施。如「否」，請說明理由。 請詳述個人資料會被保留多久？ 是否有相關措施以確保所持有的個人資料保存時間不超過該資料被使用的目的？如「是」，請詳述有關措施。如「否」，請說明理由。	( ) 是，_____ ( ) 否，_____ 保留期間：_____ ( ) 是，_____ ( ) 否，_____

續下頁

13 私隱專員發出的《身份證號碼及其他身份代號實務守則》，見私隱專員的網站：www.pcpd.org.hk/tc_chi/data_privacy_law/code_of_practices/files/picode_tc.pdf

14 私隱專員發出的《收集及使用生物辨識資料指引》，見私隱專員的網站：www.pcpd.org.hk//tc_chi/resources_centre/publications/files/GN_biometric_c.pdf

乙部：私隱風險分析		
範圍	私隱影響評估問題	組別 / 部門的回應
保障資料第 3 原則 — 個人資料的使用 ▸ 除非得到資料當事人自願和明確的同意，否則個人資料只限用於收集時述明的目的或直接相關的目的。	個人資料是否只會用於收集個人資料聲明中所述之目的？如「否」，請說明理由。	( ) 是 ( ) 否，_____
	若個人資料會用於新目的，有否事先取得資料當事人的明確同意？如「否」，請說明理由。	( ) 是 ( ) 否，_____ ( ) 不適用（個人資料不會被用於當初收集目的以外的其他目的。）
	若個人資料會披露予第三者，有否提醒該第三者個人資料只可作甚麼用途及其責任？如「是」，請詳述有關情況。如「否」，請說明理由。	( ) 是，_____ ( ) 否，_____ ( ) 不適用（個人資料不會披露予第三者。）
	如個人資料會披露予第三者，所披露的資料是否只屬必須但不超乎適度？如「否」，請說明理由。	( ) 是 ( ) 否，_____ ( ) 不適用（個人資料不會被披露予第三者。）
保障資料第 4 原則 — 個人資料的保安 ▸ 資料使用者須採取所有切實可行的步驟，保障個人資料不受未獲准許的或意外的查閱、處理、刪除、喪失或使用。	是否有任何保安措施以確保個人資料受到保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響？如「是」，請詳述有關措施。如「否」，請說明理由。	( ) 是，_____ ( ) 否，_____
	如有委託資料處理者處理個人資料，是否有以合約規範方法或其他方法保障委託資料處理者所處理的個人資料？如「是」，請詳述有關方法。如「否」，請說明理由。	( ) 是，_____ ( ) 否，_____ ( ) 不適用（沒有委託資料處理者處理個人資料。）
	如有委託資料處理者處理個人資料，是否只披露必須但不超乎適度的個人資料予資料處理者。如「否」，請說明理由。	( ) 是 ( ) 否，_____ ( ) 不適用（沒有委託資料處理者處理個人資料。）

續下頁

乙部：私隱風險分析		
範圍	私隱影響評估問題	組別 / 部門的回應
保障資料第 5 原則 — 資訊的透明度 ▸ 資料使用者須採取切實可行的步驟來公開其處理個人資料的政策和行事方式，並交代其持有的個人資料類別和用途。	現有的私隱政策是否仍然適用？如「否」，請述明哪部分需要作出更新。	( ) 是 ( ) 否，_____
	若有需要更新現有的私隱政策，是否有通知保障資料主任，及是否會在推行新的改動 / 計劃前將更新的私隱政策上載於網頁？如「否」，請說明理由。[見備註]	( ) 是 ( ) 否，_____ ( ) 不適用（毋需更新私隱政策。）
保障資料第 6 原則 — 查閱及改正資料 ▸ 資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。	是否會告知資料當事人有權查閱及改正個人資料？如「否」，請說明理由。	( ) 是 ( ) 否，_____
	是否會告知資料當事人有關負責處理查閱及改正資料要求的人員的職銜及地址？如「否」，請說明理由。	( ) 是 ( ) 否，_____
丙部：潛在風險及解決方法		
[就各項所發現的風險，請描述有關解決方法。因應乙部的分析結果，負責的人員應就每項保障資料原則評估潛在的風險，特別是回應為「否」的項目。請在下述「所發現的潛在風險」的欄目說明有關風險及相應的解決方法。如有關的風險並沒有方法可以解決，負責的人員應諮詢組別 / 部門主管及保障資料主任，以評估所帶來的影響及機構是否可承受有關風險。]		
所發現的潛在風險		
解決方法		

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 _____

備註：

若有需要更新私隱政策，負責的人員應通知保障資料主任以便他作出更新，及上載更新的版本至網頁。負責的人員有責任確保相關的內容已被更新，及在推行該改動 / 計劃前更新的版本已被上載至網頁。

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

以下是一些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：—

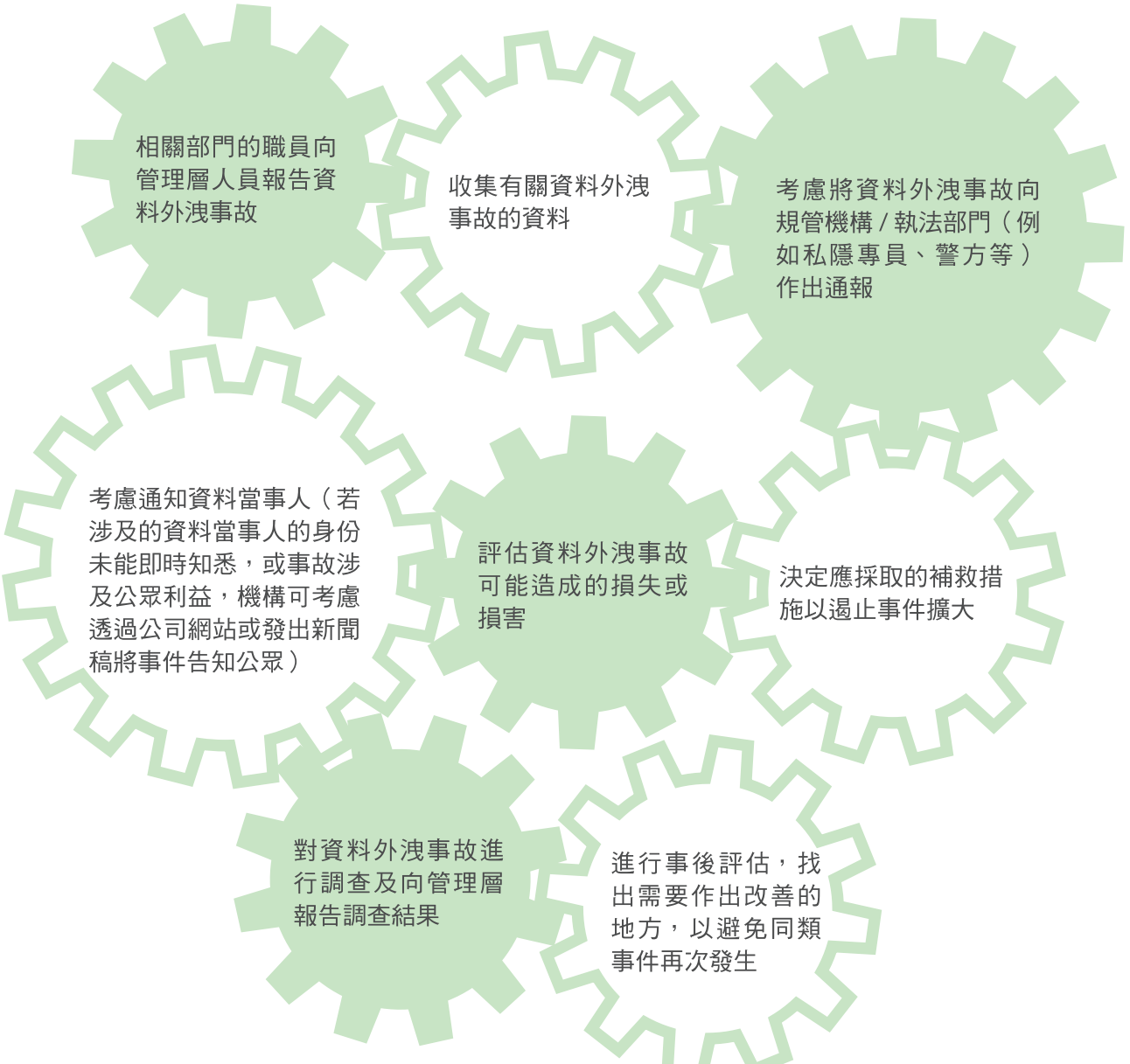
範疇	方法 / 渠道
了解條例的規定	▸ 安排職員參加私隱專員舉辦的專業研習班，或機構的內部培訓 ▸ 在機構的內聯網提供必修的培訓課程單元 ▸ 每月電子通訊或在機構政策的培訓課程中加入相關的單元
了解機構的私隱管理系統	▸ 向新入職員工簡介相關的資訊，並定期（例如每 6 個月）向所有員工傳閱有關內容
新發出 / 修訂的個人資料私隱政策及指引	▸ 每當機構發出新的個人資料私隱政策及指引，或就現有的相關政策及指引作出修訂後，應盡快將有關的資訊傳達予所有員工
個案分享	▸ 機構可將被投訴有關不當處理個人資料的個案，或資料外洩的個案，向員工分享，並教導員工條例的相關規定、恰當的做法及如何避免同類事件再次發生
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 [15]

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，可參考以下的行動：



15 《通用數據保障條例》第 33 及 34 條要求資料控制者須向監管機構通報資料外洩事故，不可不當地延誤（如情況許可，應在得悉事件後不多於 72 小時內通報）。

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》[16] 在這方面提供了實際的指引。

例子八

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（例如在進行恆常的系統檢查時、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？	

續下頁

16 見私隱專員的網站：www.pcpd.org.hk//tc_chi/resources_centre/publications/files/DataBreachHandling2015_c.pdf

(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	
(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日益普遍。機構須知道根據條例的規定[17]，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[18]
- 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[19]。

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。

17 條例第 65(2) 條。
18 保障資料第 2(3) 原則及第 4(2) 原則。
19 見私隱專員的網站：www.pcpd.org.hk//tc_chi/resources_centre/publications/files/dataprocessors_c.pdf

例子九

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。

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」，請解釋原因及理據）	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 _____

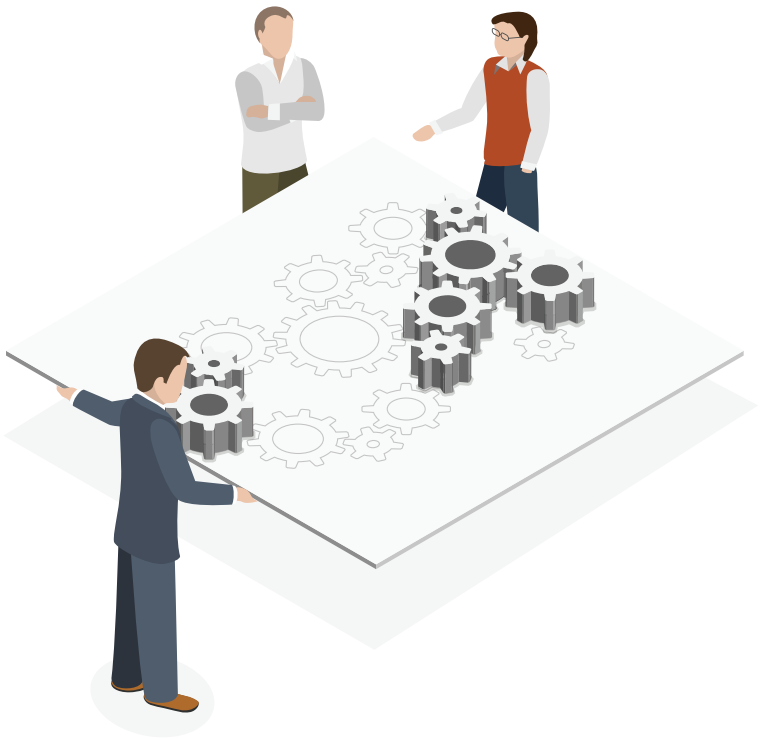
日期 _____

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》[20]。



20 見私隱專員的網站：www.pcpd.org.hk//tc_chi/resources_centre/publications/files/GN_picspps_c.pdf

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，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

例子十

以下是監督及檢討計劃的例子，供參考之用。

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

例子十一

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，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。

CONTENTS

Introduction

Organisations handle vast amount of personal data, e.g. personal data of customers and employees, in the course of business operation. With the rising public expectations for privacy protection, organisations should go further than merely treating personal data protection as a compliance issue.

The Privacy Commissioner for Personal Data, Hong Kong (**the Privacy Commissioner**) has advocated since 2014 that organisations should develop their own Privacy Management Programme (**PMP**). Organisations should embrace personal data protection as part of their corporate governance responsibilities and apply them as a business imperative throughout the organisation, starting from the boardroom. This can, not only build trust with clients, but also enhance their reputation as well as competitiveness.

In fact, the European Union's General Data Protection Regulation (**GDPR**)[1], which came into force on 25 May 2018, expressly incorporates an accountability principle[2]. Apparently, the adoption of the accountability approach in handling personal data through implementation of PMP becomes a global trend for organisations.

This Best Practice Guide aims at providing organisations with a framework for constructing a comprehensive PMP with concrete examples and practical guidance for reference.

1 See the Booklet: European Union General Data Protection Regulation 2016 (Effective 25 May 2018) issued by the Privacy Commissioner, available at www.pcpd.org.hk/english/data_privacy_law/eu/files/eugdpr_e.pdf

2 Articles 5, 24 and 25 of the GDPR.

The Benefits of Implementing a PMP

- Minimise the risk of incidents (e.g. data breach)
- Manage the personal data collected effectively
- Ensure compliance with the Personal Data (Privacy) Ordinance
- Demonstrate the organisations' commitment to good corporate governance and building trust with employees and customers
- Enhance corporate reputation, competitive advantage and potential business opportunities
- Effective handling of privacy breaches to minimise the damage arising from breaches

Components of a PMP

To develop a comprehensive PMP, organisations should foster staff awareness of data privacy protection, and devise policies and procedures in relation to personal data handling for staff to follow so as to ensure that the organisations' practice of personal data handling is consistent with the Personal Data (Privacy) Ordinance **(the Ordinance)**.

A PMP consists of the following three components:

1. Organisational Commitment

- **1.1** Buy-in from the Top
- **1.2** Appointment of Data Protection Officer/ Establishment of Data Protection Office
- **1.3** Establishment of Reporting Mechanisms

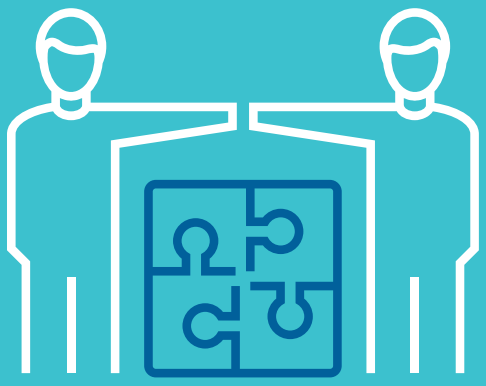
2. Programme Controls

- **2.1** Personal Data Inventory
- **2.2** Internal Policies on Personal Data Handling
- **2.3** Risk Assessment Tools
- **2.4** Training, Education and Promotion
- **2.5** Handling of Data Breach Incident
- **2.6** Data Processor Management
- **2.7** Communication

3. Ongoing Assessment and Revision

- **3.1** Development of an Oversight and Review Plan
- **3.2** Assessment and Revision of Programme Controls

The above components will be expounded with examples below. Please note that the recommendations, examples and sample documents provided in this Best Practice Guide are not one-size-fits-all solutions. One organisation's PMP may vary to another, depending on the organisation's specific circumstances (e.g. size, nature of business and the personal data it handles).



1 Organisational Commitment

An internal governance structure to foster a personal data privacy respectful culture is the key component of a PMP. Organisations should have a governance structure to ensure the policies and procedures on personal data protection are being followed. This also reflects that organisations handle personal data in a responsible manner and in compliance with the Ordinance.

1.1 Buy-in from the Top

To be accountable, a top-down approach must be adopted by the organisations to demonstrate their commitment to personal data privacy protection so that a PMP and a privacy respectful culture will more likely be established.

Top management should:

- convey to all staff of their support to cultivate a personal data privacy respectful culture and commitment to the implementation of PMP through staff meetings or internal circulars
- appoint the Data Protection Officer
- endorse the programme controls and the whole PMP
- allocate adequate resources (including finance and manpower) to implement PMP
- actively participate in the assessment and review of PMP
- report to the Board on the programme regularly

1.2 Appointment of Data Protection Officer[3]/Establishment of Data Protection Office

Organisations should appoint a designated officer (i.e. Data Protection Officer) to oversee the organisations' compliance with the Ordinance and implementation of PMP. For a major corporation, the Data Protection Officer should be a senior executive, whereas for a very small organisation, this should be the owner/operator.

The Data Protection Officer is usually the one responsible for structuring, designing and managing the PMP, including all procedures, training, monitoring/auditing, documenting, evaluating, and follow-up. In large organisations, it is recommended to set up a departmental coordinator to support the Data Protection Officer. Resources should be channeled to train and develop the Data Protection Officer and/or his/her team as a professional in personal data privacy protection.

Example 1

In large organisations, the structure of the Data Protection Office and duties of its officers are listed below for reference:

Structure of Data Protection Office

Role	Staff who took up the role	
Data Protection Officer	General Manager (Administration Department)	
Personal Data Privacy Officer	Senior Manager (Administration Department)	
Departmental Coordinator	**Department**	**Staff who took up the role**
	Administration	Manager[4]
	Information Technology	Senior Manager
	Corporate Communications	Senior Manager
	Legal	Senior Manager
	Marketing	Senior Manager

3 Article 37 of the GDPR requires data controllers (for the applicable types of organisations/businesses) to designate a Data Protection Officer.

4 As the General Manager and Senior Manager of the Administration Department have taken up the roles of Data Protection Officer and Personal Data Privacy Officer respectively, the Departmental Coordinator of Administration Department is taken up by another staff member to avoid role overlap.

Duties of Data Protection Officer

(i) Establishing and implementing the PMP programme controls, in particular –

- keeping a record of the organisation's personal data inventory; initiating and monitoring the annual personal data inventory review exercise
- initiating the commencement of periodic risk assessment to all departments and monitoring, reviewing and providing advice on the completed risk assessment report
- monitoring, reviewing and providing advice on conducting privacy impact assessment
- carrying out training and education and promoting staff awareness on privacy protection by circulating updates on data privacy policies, guidelines and other privacy-related information
- coordinating and monitoring the handling of data breach incidents; providing advice to departments on conducting investigations
- providing advice to and conducting review on departments' data processor management
- monitoring, reviewing and providing advice on the preparation of Personal Information Collection Statement

(ii) Reviewing the effectiveness of the PMP, including preparing an oversight and review plan for the PMP, and revising the programme controls where necessary

(iii) Reporting to the top management periodically on the organisation's compliance issues, problems encountered and complaints received in relation to personal data privacy

Duties of Personal Data Privacy Officer

- Assisting the Data Protection Officer to implement the PMP
- Handling personal data privacy complaints and enquiries
- Handling data access and correction requests made to the organisation

Duties of Departmental Coordinator

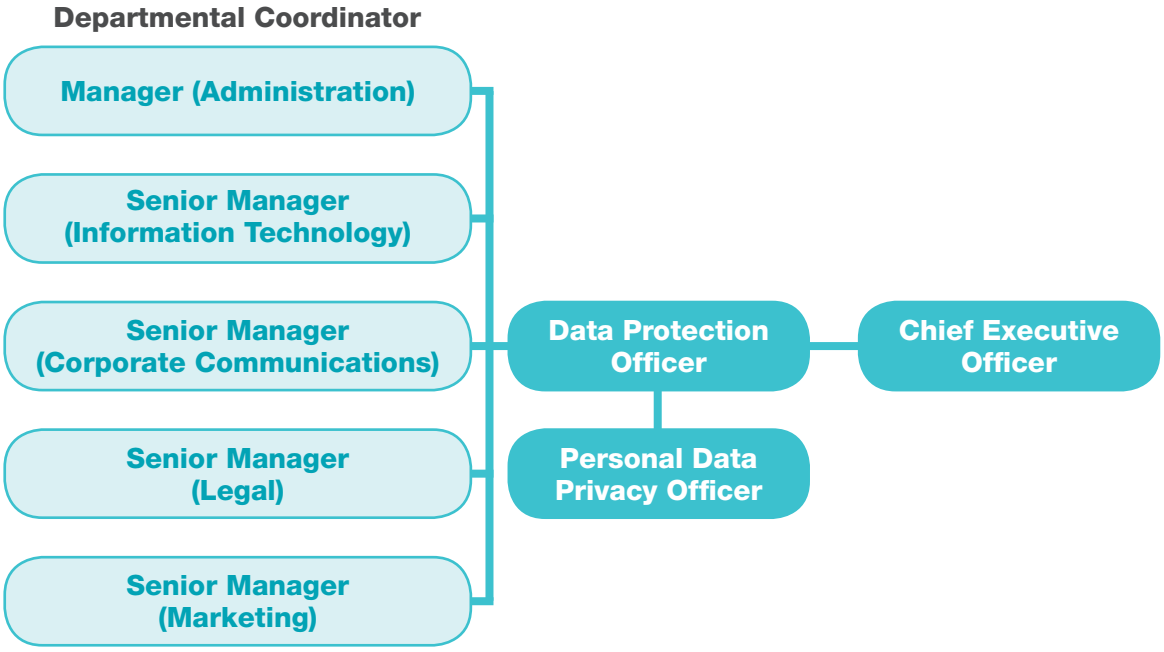
- Managing the PMP of his/her department, and representing the department to communicate with the Data Protection Officer for matters relating to PMP
- Updating personal data inventory of his/her department annually
- Carrying out periodic risk assessments within his/her department and submitting the assessment report to the Data Protection Officer for review
- Conducting data processors management review for his/her department and submitting the review report to the Data Protection Officer for review
- Ensuring the Personal Information Collection Statement prepared by his/her department is consistent with the requirements under the Ordinance, and submitting the Personal Information Collection Statement to the Data Protection Officer for review before it is presented to an individual for collecting his/her personal data
- Assisting the Data Protection Officer in carrying out the Ongoing Assessment and Revision of PMP

1.3 Establishment of Reporting Mechanisms

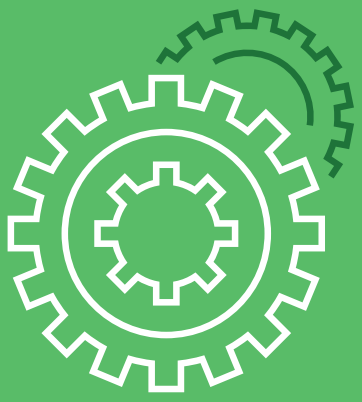
The organisation should establish internal reporting mechanisms and clearly state the reporting structure and procedures for reporting organisation's overall compliance situation, the problems encountered, the personal data privacy complaints received, and possible data breaches. The top management can further report this information to the Board of directors.

Example 2

The PMP reporting structure of the organisation in Example 1 above is listed below for reference:



There will be times when escalation of personal data issues should be considered, for example, when there is a security breach or in case of complaints. Escalation means involving people of relevant responsibility and ensuring that the needed persons in the organisation are included in the resolution of the issue. In large organisations, this could include, for example, representatives from technical, legal and corporate communications streams. How and when to escalate should be clearly defined and explained to employees. Moreover, organisations should document all of their reporting procedures.



2 Programme Controls[5]

Programme controls are measures that assist organisations to develop a PMP. Developing these controls can ensure that the organisation is compliant with the Ordinance.

5 Article 24 of the GDPR requires data controllers to implement technical and organisational measures to ensure compliance.

2.1 Personal Data Inventory[6]

The means of collecting personal data, the kinds of personal data collected, the locations for data storage, the duration of retention, the ways of using the personal data, and the data security measures adopted may vary from one organisation to another. Organisations should be clear about what kinds of personal data it holds and how the personal data is being processed, and document the information in the personal data inventory. A personal data inventory can assist an organisation to:

- understand the type of consent that the organisation needs to obtain from data subjects
- determine how the data is protected (e.g. the more sensitive the data is, the higher level of security is required)
- comply with data access and correction requests
- In case of a personal data leakage incident happened due to hacking of an organisation's database, the organisation can easily find out the kinds of personal data contained in the database, whether the personal data is encrypted, etc. from the personal data inventory so as to assess the impact of the incident and take corresponding remedial measures

Organisations should update their personal data inventory annually to ensure that all the personal data they hold is well recorded in the personal data inventory. In this connection, the procedures for updating personal data inventory, the time for updating, the persons-in-charge, the processes of updating and reviewing, and the persons responsible for filing the inventory should be established.

The Privacy Commissioner suggests that departments of an organisation to update their respective personal data inventory. The reason is that each department understands what kinds of personal data are held by the department. The Departmental Coordinators then submit the updated personal data inventory for the Data Protection Officer's review and filing.

6 Article 30 of the GDPR requires data controllers/data processor to keep record of their processing activities, including the types of data processed, the purposes for which the data is used, the transfer of personal data to a third country or an international organisation/business etc. unless in exempted situations specified in the GDPR.

Example 3

Below is a sample of personal data inventory for reference.

Example 3 — Sample of Personal Data Inventory

Department	Administration	Marketing
Category of record	Personnel records	Membership records
Items of personal data contained in the record	Employees' personal data: - Name - HKID copy - Contact information (including address, mobile number and email address)	Members' personal data: - Name - Contact information (including address, mobile number and email address)
Means of collection of the data	Employee Information Form	Membership Application Form
Purpose of collection and use of the data	Handle employment-related matters	Handle matters related to provision of products and services to members
Retention period of the data	7 years after the employee has left the service	1 year after cancellation of membership by the member
Location for data storage	Physical: Filing cabinets in Personnel Record Room	Physical: Filing cabinets in Marketing Department Electronic: Network drive of Marketing Department
Disclosure of data to any third parties including data processors and the names and relevant details of third parties (Yes/No)	No	Data will be transferred to service provider for telemarketing
Possible location of transfer (e.g. cloud server location)	N/A	Network drive of service provider
Purpose of disclosing the data and whether the disclosure complies with the Ordinance	N/A	Carry out telemarketing (consent has been obtained from data subjects)
Date of return or destruction by the data processor (if applicable)	N/A	Service provider will destroy the data within 7 days after expiry of contract
Security measures adopted	Filing cabinets are locked and the key is kept by Head of Personnel Department and Personnel Officer	Filing cabinets are locked and the key is kept by staff of Marketing Department. Marketing Department's network drive can only be accessed by staff of Marketing Department.

2.2 Internal Policies on Personal Data Handling

Organisations should develop internal policies to ensure that their handling of personal data complies with the Ordinance. These policies should be made available to employees who should be reminded of these policies periodically and any updates immediately.

In general, the internal policies on personal data handling should cover the entire life-cycle of personal data handling (i.e. the six Data Protection Principles **(DPPs)** in Schedule 1 of the Ordinance)[7]. Organisations may make reference to Example 4 below:

Example 4

DPP1	Collection of personal data, including ▸ Handling of hotline enquiries ▸ Telephone recording ▸ CCTV monitoring ▸ Collection of Identity Card number and copy
DPP2	Accuracy and retention of personal data ▸ Retention period of personal data related to employment (e.g. unsuccessful job applicants' personal data shall not be retained for a period longer than two years and former employees' personal data not more than seven years[8]) ▸ Retention period of data related to transactions with customers[9]
DPP3	Use of personal data, including ▸ The requirements for consent ▸ Handling of requests from regulatory bodies, enforcement authorities and government departments for obtaining personal data
DPP4	Security of personal data, including ▸ Security of physical documents containing personal data ▸ IT security (e.g. security measures for using portable devices containing personal data) ▸ Directing outsourced service provider to adopt necessary security measures when handling personal data
DPP5	Transparency of organisations' personal data policies and practices
DPP6	Steps for handling data access and data correction requests
Section 35A of the Ordinance	▸ Actions to be taken before using personal data in direct marketing ▸ Steps for handling opt-out requests

7 Please refer to the guidance notes issued by the Privacy Commissioner on various subjects of data protection.

8 See *Code of Practice on Human Resource Management* issued by the Privacy Commissioner, available at www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf

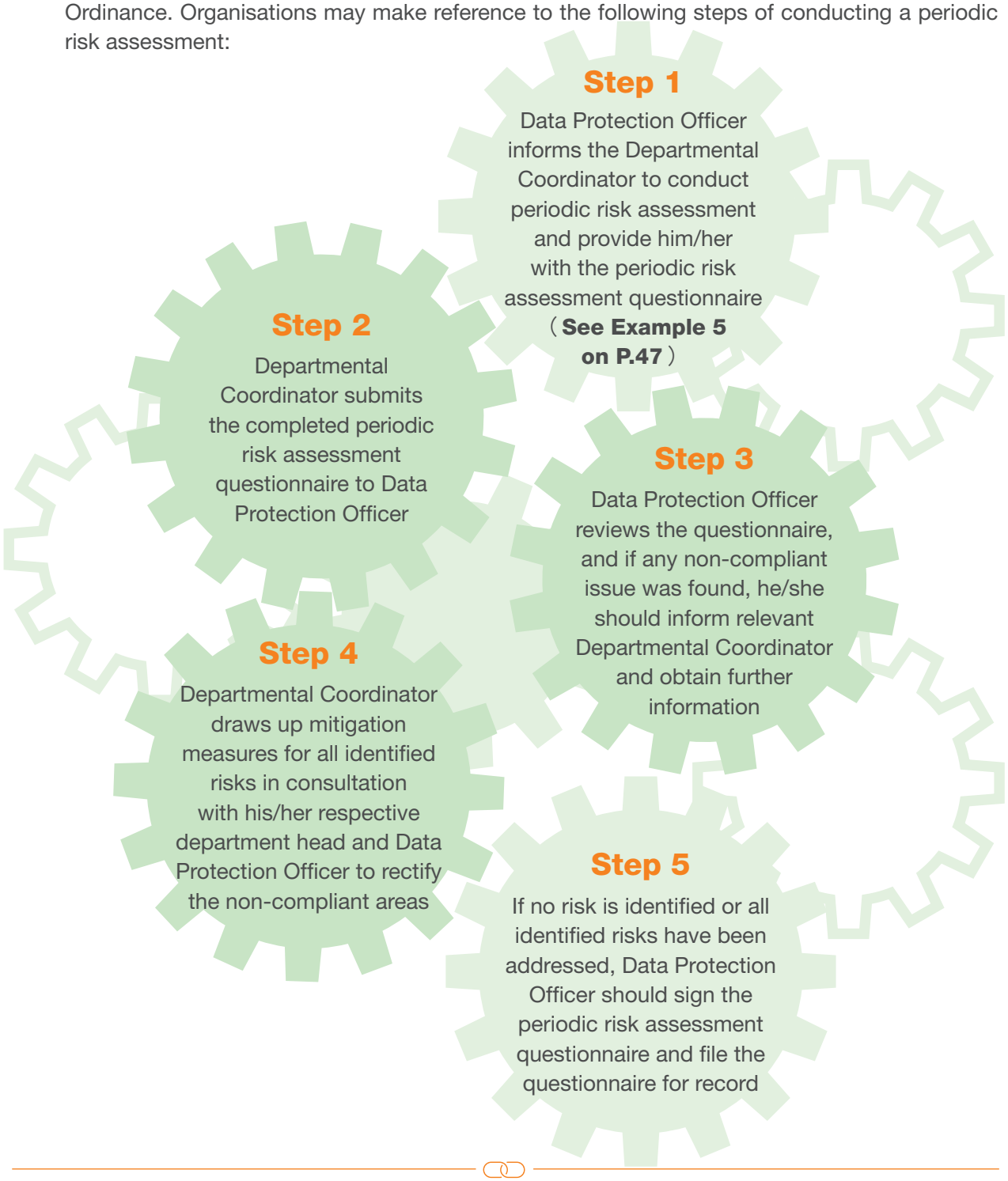
9 Under section 51C of the Inland Revenue Ordinance, business records should be kept for a period of not less than 7 years. For details, please refer to the Inland Revenue Ordinance.

2.3 Risk Assessment Tools[10]

Personal data risks evolve over time. Conducting periodic risk assessments and privacy impact assessment is an important part of any PMP to ensure that the privacy policies and practices of organisations are and remain compliant with the Ordinance.

2.3.1 Periodic Risk Assessment

Every year, organisations should invite selected/all departments[11] to participate in the periodic risk assessments to ensure that their privacy policies and practices comply with the Ordinance. Organisations may make reference to the following steps of conducting a periodic risk assessment:



10 Article 35 of the GDPR requires data controllers to conduct data protection impact assessment for high-risk processing.

11 Large organisations, which have various departments, may select a particular department for conducting periodic risk assessments. Small organisations may invite all departments to conduct periodic risk assessments.

Example 5

Below is a sample of periodic risk assessment questionnaire for reference.

Example 5 — Sample of Periodic Risk Assessment Questionnaire

Questions	Yes/No	Number	Further actions required
A. New initiatives/projects developed or changes to existing activities involving personal data			
1. Have any new initiatives/projects or changes to existing activities involving personal data been launched or developed in your department in the past 36 months, which involve the collection, use and processing of personal data (e.g. new personal data handling processes, launching of new systems, etc.) Please state the number of new initiative(s)/ project(s) launched. If the answer is "Yes", please proceed to Q(2)-Q(4) below. If the answer is "No", please proceed to B.	( ) Yes ( ) No		
2. Has all personal data involved in the new initiative(s)/project(s) or changes to existing activities been updated in the personal data inventory?	( ) Yes ( ) No		If no, please update the personal data inventory immediately and submit the updates to the Data Protection Officer.
3. Has privacy impact assessment (PIA) been conducted for the new initiative(s)/ project(s) or changes to existing activities and submitted to the Data Protection Officer for review? Please also state the name(s) of the PIA(s) conducted.	( ) Yes ( ) No		If due consideration was given before and there was no need to conduct a PIA, please make sure the relevant justification is properly documented.
4. If a PIA has been conducted, are the content and result of the PIA still applicable? (i.e. Are there any new changes, new privacy risks and means to address those risks, which require updates on the PIA?)	( ) Yes ( ) No		If no, please update the relevant documents and submit them to the Data Protection Officer.
B. Data breach incidents			
5. Has any data breach incident occurred in the past 36 months in your department? If the answer is "Yes", please proceed to Q(6)-Q(7) below. If the answer is "No", please proceed to C.	( ) Yes ( ) No		
6. For each of the incidents, has a Data Breach Information Sheet been prepared and submitted to the Data Protection Officer?	( ) Yes ( ) No		If no, please complete the Data Breach Information Sheet(s) and submit it to the Data Protection Officer.
7. Has the data breach(es) been contained?	( ) Yes ( ) No		

To be continued

Questions	Yes/No	Number	Further actions required
C. Complaints received			
8. Are there any complaints about your department's handling of personal data in the past 36 months? If the answer is "Yes", please proceed to Q(9) below. If the answer is "No", please proceed to D.	( ) Yes ( ) No		
9. Were all relevant complaints reported to the Data Protection Officer? Please state the reference number of the complaints received.	( ) Yes ( ) No		If no, please report the complaints to the Data Protection Officer immediately.
D. New data processor			
10. Has your department engaged any new data processor(s) to handle personal data in the past 36 months? If the answer is "Yes", please proceed to Q(11) below. If the answer is "No", please proceed to Q(12) below.	( ) Yes ( ) No		
11. Has the Data Processor Review Checklist been completed and submitted to the Data Protection Officer?	( ) Yes ( ) No		If no, please complete the Data Processor Review Checklist and submit it to the Data Protection Officer.
E. Data Retention Period			
12. Has data disposal exercise been performed for all time-expired records within your department?	( ) Yes ( ) No		If no, please arrange for data disposal.

Completed by
(Departmental Coordinator)

Signature _____
Name _____
Post _____
Date _____

Reviewed by
(Data Protection Officer)

Signature _____
Name _____
Post _____
Date _____

*2.3.2 Privacy Impact Assessment **(PIA)***

Conducting a PIA before launching a new project, product or service can help the organisation discover the potential privacy risks in the early stage so as to make necessary improvements.

When to conduct a PIA?

- There is a material change to the regulatory requirements relating to personal data
- There is a material change to the organisation's existing personal data process
- Introducing a new personal data handling process in the organisation
- The organisation intends to engage data processors to handle personal data on its behalf

Organisations should:

- devise internal policies stating when to conduct a PIA, the procedures of conducting a PIA, and the persons responsible for conducting a PIA and reviewing the result
- make reference to the *Information Leaflet on Privacy Impact Assessment*[12] issued by the Privacy Commissioner
- upload the content of the PIA on the organisation's website to enhance transparency and demonstrate its commitment to protect personal data privacy

Example 6

Below is a sample of PIA questionnaire for reference.

Example 6 — Sample of PIA Questionnaire

Part A: Background information of the proposed change/project	
Project name	
Branch/Department	
Responsible officer (name & post)	
Expected date of implementation	
Description of the purpose of the personal data collection and the flow of handling personal data	
Types of personal data to be collected (e.g. name, date of birth, Identity Card number, address, telephone number, etc.)	
Estimated number of data subjects from whom data is collected	
Will any data processor(s) be involved? If "yes", have contractual or other means been adopted to ensure that the data processor(s) has taken appropriate data security measures? If "no", please elaborate on the justification.	( ) Yes ( ) No
Will there be any cross-border transfer of personal data? If "yes", please specify the destination(s) and the purpose(s) of such cross-border transfer.	( ) Yes ( ) No

To be continued

12 See the Privacy Commissioner's website: www.pcpd.org.hk//english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

Part B: Privacy risks analysis		
Area	PIA Question	Answers by Branch/Division
Data Protection Principle (DPP) 1 — Purpose and manner of collection of personal data ▸ Personal data must be collected in a lawful and fair way, for a purpose directly related to a function or an activity of the data user. ▸ All practicable steps shall be taken to notify the data subjects of the purpose of data collection and the classes of persons to whom the data may be transferred. ▸ Data collected should be necessary but not excessive.	Will the data subjects be informed of the purpose of collecting their personal data? If "no", please provide justifications.	( ) Yes ( ) No, _____
	Will the collection of personal data be on a minimum level (i.e. no excessive personal data is collected)? Please provide justifications on the collection of sensitive personal data below (including but not limited to): ▸ Hong Kong Identity Card number and other personal identifier (e.g. passport number) [13] ▸ Biometric data (e.g. fingerprints) [14]	( ) Yes ( ) No Justification on the collection of sensitive personal data: _____ _____
	Will the data subjects be informed, on or before the collection of the personal data, of whether the supply of the personal data is voluntary or obligatory? If "no", please provide justifications.	( ) Yes ( ) No, _____
	Where it is obligatory for data subjects to supply the personal data, will the data subjects be informed of the consequence of not providing the personal data? If "yes", please elaborate. If "no", please provide justifications.	( ) Yes, _____ ( ) No, _____ ( ) Not applicable (it is completely voluntary for the data subjects to supply their personal data.)
	Will the personal data collected be transferred or disclosed to any third party?	( ) Yes ( ) No
	If the personal data is to be transferred to any third party or data processor, will the data subjects be informed of the classes of persons to whom their personal data may be transferred? If "no", please provide the reason.	( ) Yes ( ) No, _____ ( ) Not applicable (personal data collected will not be transferred or disclosed to any third party.)

To be continued

13 The Code of Practice on the Identity Card Number and Other Personal Identifiers issued by the Privacy Commissioner can be found at www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/picode_en.pdf

14 The Guidance on Collection and Use of Biometric Data issued by the Privacy Commissioner can be found at www.pcpd.org.hk//english/resources_centre/publications/files/GN_biometric_e.pdf

Part B: Privacy risks analysis		
Area	PIA Question	Answers by Branch/Division
DPP 2 — Accuracy and duration of retention of personal data ▸ All practicable steps shall be taken to ensure personal data is accurate and is not kept longer than necessary to fulfil the purpose for which it was originally collected.	Will there be any measures in place to ensure accuracy of the personal data held? If "yes", please elaborate. If "no", please justify. What will be the retention period of the personal data? Please specify. Will there be any measures in place to ensure that personal data is not kept longer than necessary to fulfil the purpose of using the data? If yes, what are the measures? If no, please justify.	( ) Yes, _____ ( ) No, _____ Retention period: _____ ( ) Yes ( ) No, _____
DPP 3 — Use of personal data ▸ Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless the data user obtains from the data subject voluntary and explicit consent to use the data for a new purpose.	Will personal data be used only for the original purpose stated in the Personal Information Collection Statement? If "no", what are the reasons.	( ) Yes ( ) No, _____
	Where the personal data will be used for a new purpose, has explicit consent been obtained from the data subjects? If "no", please justify.	( ) Yes ( ) No, _____ ( ) Not applicable (personal data will not be used for purposes other than the original purposes for which it is collected.)
	Where personal data will be disclosed to a third party, will the third party be reminded of the use of the data and its responsibilities? If "yes", please elaborate. If no, please justify.	( ) Yes ( ) No, _____ ( ) Not applicable (personal data collected will not be disclosed to a third party.)
	Where personal data will be disclosed to a third party, is the personal data disclosed to third party only necessary but not excessive? If "no", please justify.	( ) Yes ( ) No, _____ ( ) Not applicable (personal data of data subjects will not be disclosed to a third party.)

To be continued

Part B: Privacy risks analysis		
Area	PIA Question	Answers by Branch/Division
DPP 4 — Security of personal data ▸ Data user needs to take all practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.	Will there be any safeguarding measures to prevent unauthorised or accidental access, processing, erasure, loss or use of personal data? If "yes", please elaborate. If "no", please justify.	( ) Yes: _____ ( ) No, _____
	Where data processor(s) will be engaged, will there be any contractual or other means to secure the personal data? If "yes", please elaborate. If "no", please state the reason.	( ) Yes, _____ ( ) No, _____ ( ) Not applicable (third party data processor will not be engaged.)
	Where data processor(s) will be engaged, is the personal data disclosed to data processor only necessary but not excessive? If "no", please justify.	( ) Yes ( ) No, _____ ( ) Not applicable (third party data processor will not be engaged.)
DPP 5 — Openness of information ▸ Data user must take all practicable steps to make known to the public its personal data policies and practices, types of personal data it holds and the main purposes for which it uses the data.	Is the existing Privacy Policy still applicable? If "no", please specify what update is needed.	( ) Yes ( ) No: _____ _____
	Where there is a need to update the Privacy Policy, has the Data Protection Officer been informed and will the updated Privacy Policy be uploaded to the website before the implementation of the change/ the launch of the project? If "no", please explain. **[Note]**	( ) Yes ( ) No, _____ ( ) No update is required
DPP 6 — Access to and correction of personal data ▸ Data subject has the right to request access to his/ her own personal data, and request the correction of the personal data if it is inaccurate.	Will the data subjects be informed of their right to access and correct their personal data? If "no", please justify.	( ) Yes ( ) No, _____
	Will the data subjects be informed of the post title and the address of the officer who is responsible for handling data access and correction requests? If "no", please justify.	( ) Yes ( ) No, _____

To be continued

Note:

If there is a need to update the Privacy Policy, the responsible officer should inform the Data Protection Officer so that the Data Protection Officer can make necessary amendments to the Privacy Policy and upload the updated version onto the organisation's website. It is the responsible officer's responsibility to ensure that necessary amendments are made and the revised version is published before the implementation of the proposed change or project.

Part C: Potential risks and mitigation actions	
[For any privacy risks identified, please describe the means to address the risks. *Based on the results of Part B, the responsible officer should assess the potential risks identified in relation to each of the DPPs, especially those areas with "No" as answers. These risk areas should be highlighted in the table below with the respective mitigating measures identified. For those risk areas where no mitigating measures could be identified, the responsible officer should consult the Branch/Department Head and the Data Protection Officer to assess the impact and whether the organisation could bear such risk.]*	
Potential risks identified	
Mitigation measures	

Completed by
(Departmental Coordinator)

Signature _____
Name _____
Post _____
Date _____

Reviewed by
(Data Protection Officer)

Signature _____
Name _____
Post _____
Date _____

2.4 Training, Education and Promotion

A sound PMP requires all members of an organisation to be aware of, and be ready to act on personal data protection obligations. Hence, the organisation should provide employees with up-to-date training and education tailored to specific needs. The organisation should also document its training processes and measure participation and effectiveness.

Example 7

Below are examples of personal data privacy protection training and education activities provided to employees:

Area	Means / Channels
The requirements of the Ordinance	▸ Send employees to participate in the Privacy Commissioner's professional workshops, or arrange in-house training ▸ Provide essential training modules on the organisation's intranet ▸ Insert relevant modules in the organisation's monthly e-newsletters or training course on organisation policies
The organisation's PMP	▸ Explain relevant information to new employees in the organisation's induction programme, and circulate the information to all employees periodically (e.g. every six months)
New/revised personal data privacy policies and guidelines	▸ Circulate the information to all employees as soon as practical whenever the organisation issues new personal data privacy policies and guidelines, or makes amendments to current policies and guidelines
Case sharing	▸ Share with employees the complaint cases in relation to improper handling of personal data or data breaches, and educate them about the requirements of the Ordinance, proper way to handle the matters and how to prevent the recurrence of similar incidents
Results of Privacy Impact Assessments	▸ Share with employees the privacy risks identified in Privacy Impact Assessments and the mitigation measures taken

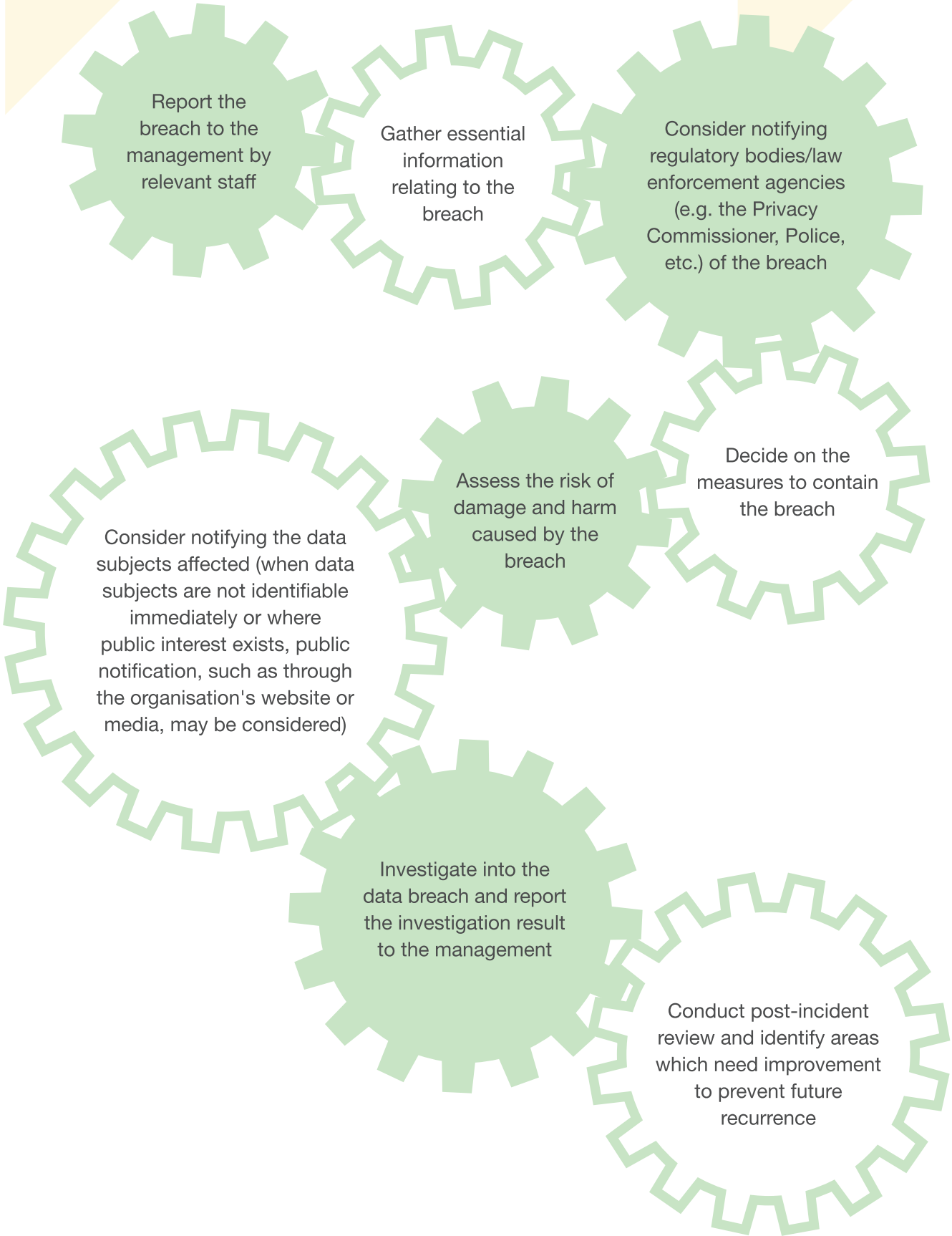
2.5 Handling of Data Breach Incident[15]

The numerous leakages of customers' data due to cybersecurity incidents have been widely reported in recent years. Personal data breaches are expensive on many fronts. As such, organisations should develop procedures in relation to the handling of breach incidents and appoint designated officer(s) to handle breach incidents.

Possible consequences that may occur without procedures in relation to the handling of breach incidents are listed below:

15 Articles 33 and 34 of the GDPR require data controllers to notify the authority of a data breach without undue delay (and where feasible, no later than 72 hours after becoming aware of it).

Organisations may make reference to the following actions to be taken when handling data breaches:



While it is not a statutory requirement for data users to inform the Privacy Commissioner of a data breach incident, the Privacy Commissioner is pleased to see that more and more organisations are willing to follow the Privacy Commissioner's recommendations to notify him of a data breach incident voluntarily. It is a good practice to report the incident to the Privacy Commissioner the soonest in order to handle the incident properly. The Guidance on *Data Breach Handling and the Giving of Data Breach Notifications*[16] issued by the Privacy Commissioner provides practical guidance in this regard.

Example 8

When there is a data breach, the subject department of the organisation may fill in the Data Breach Information Sheet as below to consolidate the information relating to the breach, take remedial actions promptly and conduct post-incident review.

Example 8 — Sample of Data Breach Information Sheet

BRANCH / DEAPRTMENT	
Branch/Department	
(I) INFORMATION OF THE BREACH	
(i) General information of the breach	
Description of the breach	
Date and time of the breach	
Location of the breach (e.g. which office, which computer server, etc.)	
Date and time of discovering the breach	
How the breach is discovered (e.g. discovered during routine system checking, known after reported by media, etc.)	
Nature of the breach (e.g. loss of data, database is hacked, etc.)	
Cause of the breach	
(ii) Impact of the breach	
Types of data subjects affected (e.g. staff, customers, public, etc.)	
Estimated number of data subjects affected (Please state the respective number for each type of data subjects)	
Types of personal data affected (e.g. name, date of birth, Hong Kong Identity Card number, address, telephone number, etc.)	
Medium holding the affected personal data (e.g. physical folders, USB, etc.)	
If the personal data is held in electronic medium, is the data encrypted?	

To be continued

16 See the Privacy Commissioner's website: www.pcpd.org.hk//english/resources_centre/publications/files/DataBreachHandling2015_e.pdf

(II) DATA BREACH NOTIFICATION TO REGULATORY BODIES	
Are other regulatory bodies such as the Hong Kong Police Force or the office of the Privacy Commissioner for Personal Data, Hong Kong being notified of the data breach? If **yes**, please provide the date and details of each notification given.	
(III) ACTIONS TAKEN/WILL BE TAKEN TO CONTAIN THE BREACH	
Brief description of actions **taken** to contain the breach	
Please evaluate the effectiveness of the abovementioned actions taken	
Brief description of actions that **will be taken** to contain the breach	
(IV) RISK OF HARM	
Please assess the potential harm to data subjects caused by the data breach and the extent of it	
(V) DATA BREACH NOTIFICATIONS TO DATA SUBJECTS AFFECTED	
Dates and details of the data breach notifications issued to data subjects affected by the breach	
If no data breach notification is issued/will be issued, please state the consideration	
(VI) INVESTIGATION RESULTS	
Cause(s) of the breach	
(VII) POST-INCIDENT REVIEW (To be completed by the Data Protection Officer)	
Recommended improvement measures and the respective implementation date	
Date to review the effectiveness of the abovementioned improvement measures	

Completed by
(Departmental Coordinator)

Signature _____
Name _____
Post _____
Date _____

Reviewed by
(Data Protection Officer)

Signature _____
Name _____
Post _____
Date _____

2.6 Data Processor Management

Outsourcing and entrusting personal data processing work by organisations to their agents is increasingly common. However, organisations should note that they, being the principal, are responsible for the improper handling of personal data (e.g. failed to take security measures resulting to leakage of personal data entrusted to it) by their agents pursuant to the Ordinance[17]. Hence, organisations should take into account the following areas when considering engaging data processors to process personal data on their behalf:

Does the organisation have actual need to engage a data processor?

Yes

- Pass only the minimum personal data to the data processor
- Adopt contractual or other means to protect the personal data entrusted to the data processor[18]
- Conduct annual review to ensure that the management of data processor is adequate and comprehensive

The types of obligations to be imposed on data processor include:

- Security measures to be taken by the data processor
- Timely return, destruction or deletion of the personal data no longer required
- Prohibition against other use and disclosure
- Prohibition against sub-contracting to other service providers
- Reporting of irregularity
- Measures to ensure contract staff's compliance with the agreed obligations
- Organisation's right to audit and inspect
- Consequences for breach of the contract

Organisations are advised to take note of the *Information Leaflet on Outsourcing the Processing of Personal Data to Data Processor*[19] issued by the Privacy Commissioner.

It is worth noting that while data controllers are required to comply with the requirements of the GDPR for their data processing activities (including the processing of personal data by the entrusted data processor), the GDPR also imposes direct obligations on data processors. In other words, data processors are regulated directly under the GDPR, and they are liable to be penalised for breach of their obligations.

If organisations engage data processors (whether within or outside Hong Kong) to process personal data on their behalf, the organisations should review whether their management of data processor is adequate and comprehensive on an annual basis. Organisations can devise a Data Processor Review Checklist for conducting the annual review.

17 Section 65(2) of the Ordinance.
18 DPP 2(3) and DPP 4(2).
19 See the Privacy Commissioner's website: www.pcpd.org.hk//english/resources_centre/publications/files/dataprocessors_e.pdf

Example 9

Below is a sample of Data Processor Review Checklist for reference.

Part A: Background information	
Branch/Department	
Name of data processor	
Purpose of engaging the data processor	
Brief description of personal data involved	
Date of engagement with the data processor	

Part B: Review of the organisation's management of data processors		
Questions	Yes/No (If no, please explain the reasons and justifications)	Remarks
(1) Do the contractual terms cover the organisation's right to audit and inspect how the data processor handles and stores personal data?		
(2) Do the contractual terms cover the data processor's obligation to report immediately to the organisation for any signs of abnormalities, security breaches or loss of personal data?		
(3) Do the contractual terms cover the prohibition against any use or disclosure of the personal data by the data processor for a purpose other than the purpose for which the personal data is entrusted to it by the organisation?		
(4) Do the contractual terms cover the limitation on sub-contracting the service that it is engaged to provide?		
(5) Do the contractual terms cover the timely return, destruction or deletion of personal data by the data processor?		
(6) Do the contractual terms cover the data processor's obligations to adopt security measures to protect the personal data entrusted to it and to comply with the Ordinance (please specify the security measures)?		
(7) Do the contractual terms cover the consequences for breach of the contract?		

To be continued

Questions	Yes/No (If no, please explain the reasons and justifications)	Remarks
(8) Is the Branch/Department satisfied that the data processor had followed the contractual obligations in respect of personal data protection? If "Yes", please elaborate.		
(9) If the answer to Q(8) above is "No", please specify the actions taken by the Branch/ Department?		
(10) Has the Branch/Division performed any audit and inspection on the data processor in the past 36 months (including surprise visit)? If the answer is "Yes", please state: 10.1 the date of the audit and inspection; 10.2 any irregularities identified; and 10.3 any remedial actions taken. If the answer is "No", please explain why an audit/inspection is not performed.		
(11) If audit and inspection were performed on the data processor this year, has the Branch/ Department identified any irregularities? If "Yes", please state the details and the improvement measures taken by the data processor.		
(12) Has there been any data breach incidents caused by the data processor? If "Yes", please provide the corresponding Data Breach Information Sheet as attachment.		

Completed by
(Departmental Coordinator)

Signature _____
Name _____
Post _____
Date _____

Reviewed by
(Data Protection Officer)

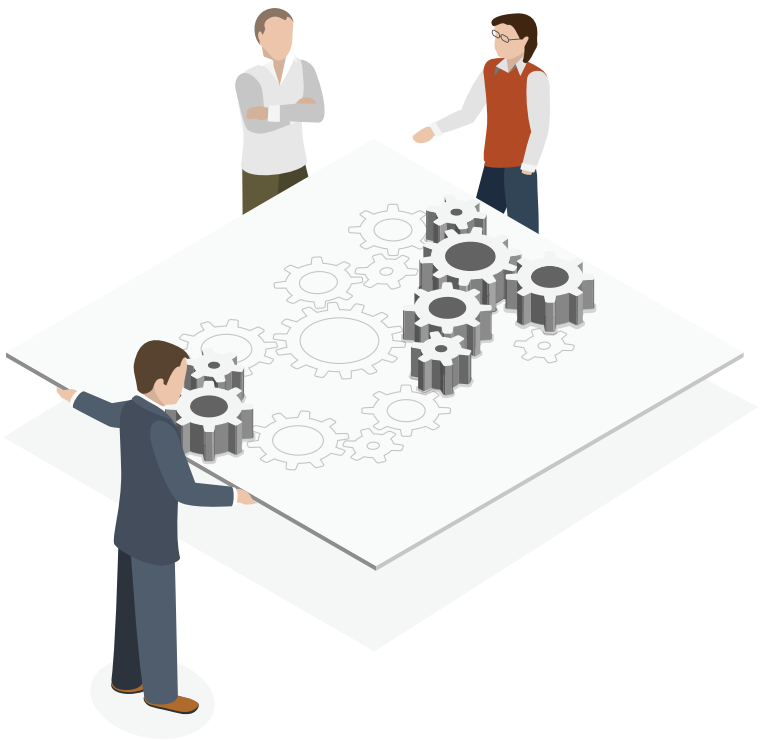
Signature _____
Name _____
Post _____
Date _____

2.7 Communication

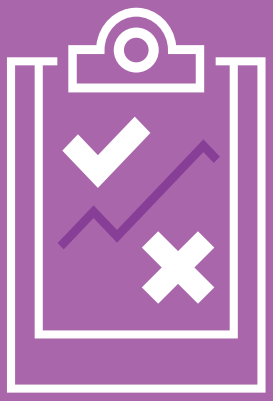
Organisations should take all practical steps to inform employees and customers of their personal data policies and practices which is clear and easily understandable, including:

- inform employees and the public of the purposes of collecting, using and disclosing personal data and the duration of retention through the Personal Information Collection Statement and the Privacy Policy Statement
- inform the public of the information on who to contact with questions or concerns
- inform the public of how to make data access/correction requests to the organisations
- the above information should be made easily available to individuals (e.g. uploading the personal data privacy policies and practices to the organisation's website, printed copies are available for collection in the office of the organisation)

Organisations may make reference to the *Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement*[20] issued by the Privacy Commissioner.



20 See the Privacy Commissioner's website: www.pcpd.org.hk//english/resources_centre/publications/files/GN_picspps_e.pdf



3 Ongoing Assessment and Revision

PMP is an ongoing process which needs continuous monitoring and assessment of the measures, policies and procedures of the programme, and making necessary amendments to ensure its effectiveness. Data Protection Officer should develop an oversight and review plan, and assess and revise programme controls annually.

3.1 Development of an Oversight and Review Plan

Data Protection Officer should prepare an oversight and review plan, which must:

(i) cover the implementation of all programme controls

(ii) cover all policies and procedures related to personal data privacy

(iii) state when and how to conduct the assessment by whom, and set the assessment criteria

(iv) include periodic assessment (at least once a year)

(v) be endorsed by the top management

Example 10

The following sample of an oversight and review plan is provided for reference.

Month	Oversight and review activities
Prepare the oversight and review plan	
Jan - Apr	▸ Update personal data inventory ▸ Review the organisation's data processor management ▸ Conduct periodic risk assessment ▸ Update training content and training plan
May - Jul	Assess the effectiveness of all PMP programme controls, and make corresponding amendments
Aug - Oct	Review and revise the PMP manual as well as other personal data privacy policies and guidelines
Nov	Circulate the PMP manual as well as other policies and guidelines related to personal data privacy to employees
Dec	Review the execution of the oversight and review plan, and prepare the plan for the next year

Example 11

In order to document the annual review on the effectiveness of the PMP, the Data Protection Officer may complete the following review table and confirm that the actions set out under the oversight and review plan have been carried out appropriately, and submit it to the top management.

Example 11 — Sample of PMP Review Document

Action		Completed/ Not completed	Date of last review/ update	Difficulties observed and proposed mitigation measures
(1)	Update personal data inventory			
(2)	Review of data processor management			
(3)	Periodic risk assessments			
(4)	Update training content and training plan			
(5)	Review and revise the PMP manual, and other personal data privacy policies and guidelines			
(6)	Circulate the PMP manual and other personal data privacy policies and guidelines to employees			
(7)	Review the data breach handling mechanism			

3.2 Assessment and Revision of Programme Controls

The effectiveness of programme controls should be monitored, periodically audited, and where necessary, revised. Organisations may consider the following factors before determining whether the programme controls should be revised:

- What are the latest threats and risks?
- Are the programme controls addressing new threats and reflecting the latest complaint or audit findings, or guidance of the Privacy Commissioner?
- Are new services being offered that involve increased collection, use or disclosure of personal data?
- Is training necessary and if yes, is it taking place, is it effective, are policies and procedures being followed, and is the programme up to date?

If problems are found during the monitoring process, concerns should be documented and addressed by the appropriate officers. Critical issues should be brought to the attention of top management. Moreover, changes should be communicated to employees either as they are made or in "refresher" education and training modules, as appropriate.

Conclusion

Privacy and data protection cannot be managed effectively if they are merely treated as a compliance issue — doing the least possible to comply with the legal requirements, but with little or no regard to customers' privacy expectations. Instead, organisations should consider the subject from a broad business perspective, bringing the concept of customer centricity into the business equation. To this end, top management's commitment is required to build and maintain a PMP which ensures that privacy is built by design into all initiatives, programmes or services, and data protection is practised throughout the organisation. This proactive approach should lead to a win-win-win outcome for the organisations and their staff as well as customers.

PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

查詢熱線 Enquiry Hotline : **(852) 2827 2827**
傳真 Fax : **(852) 2877 7026**
地址 Address : **香港灣仔皇后大道東248號陽光中心13樓 1303室**
Room 1303, 13/F, Sunlight Tower,
248 Queen's Road East, Wanchai, Hong Kong.
電郵 Email : **enquiry@pcpd.org.hk**

下載本刊物
Download
this publication

免責聲明 Disclaimer

本刊物所載的資訊和建議只作一般參考用途，並非為法例的應用提供詳盡指引。私隱專員並沒有就本刊物內所載的資訊和建議的準確性或個別目的或使用的適用性作出明示或隱含保證。相關資訊和建議不會影響私隱專員在《個人資料（私隱）條例》下獲賦予的職能及權力。

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.

二零一四年二月初版
二零一八年八月（第一修訂版）
二零一九年三月（第二修訂版）

First published in February 2014
August 2018 (First Revision)
March 2019 (Second Revision)