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

私 隱 管 理 系 統

Privacy Management Programme

最佳行事方式指引

目錄

引言 [2]

實施私隱管理系統的好處 [2]

建立全面的私隱管理系統 [3]

甲部－私隱管理系統基本原則 [3]

乙部－持續評估及修訂 [7]

私隱管理系統一覽 [8]

私隱管理系統

Privacy Management Programme

最佳行事方式指引

引言

私隱管理系統不是《個人資料(私隱)條例》下的規定。個人資料私隱專員(「**私隱專員**」)提倡機構資料使用者把個人資料私隱保障納入企業管治責任,並在機構中貫徹執行,涵蓋業務常規、操作程序、產品和服務設計、實體建築,以至網絡基礎設施。在策略層面,機構可採用**私隱管理系統**作為框架,輔以恒之有效的檢討及監察程序,建立健全的私隱保障基建,藉以配合機構遵從《個人資料(私隱)條例》(「**條例**」)的規定。**私隱管理系統**亦有助機構推行公開和具透明度的資訊政策和常規,以示機構有決心體現良好企業管治和建立僱員和客戶的信任。

在機構建立**私隱管理系統**,需要慎密的策劃和跨部門、跨職能的考慮。員工應知悉和瞭解適用於其機構的**私隱管理系統**;機構應告知客戶及業務夥伴其**私隱管理系統**中有哪些部分與他們相關,並保證會付諸實行。機構在推出新產品或服務前,往往要制定業務模式及擬備技術和業務常規,過程中應確立和適當地考慮保障私隱方面的責任及風險。機構應設法減低資料外洩的可能;一旦外洩資料的事故發生,應把事故的影響減至最低。

發生失誤是難免的。穩妥的**私隱管理系統**有助機構識辨在保障個人資料方面的缺失,從而鞏固良好的行事方式,展示機構作出應盡的最大努力,甚至提升保障個人資料的水平,而不是僅僅符合法律的最低要求。

這份最佳行事方式指引(「**本指引**」)扼述如何建立私隱專員所提倡的健全**私隱管理系統**,惟指引中的建議並非是所有機構通用的方案。每個機構需要視乎其規模和業務性質而決定如何善用本指引建立各自的**私隱管理系統**。

為免生疑問,公署謹此聲明本指引並不構成根據條例第12條制訂的實務守則,亦非一般具規範作用的資料指引(即就遵從條例特定條文而直接提供建議),如機構選擇不遵從本指引的意見及建議,不會因而直接產生法律責任。另外,本指引用的「應」字,其含意是私隱專員提倡的最佳行事方式,而不是加諸於機構的指令。

本指引甲部概述**私隱管理系統**的基本原則或組件,諸如機構的決心和系統監控等必備元素。

乙部討論如何維繫及持續地改進**私隱管理系統**。機構不應視建立**私隱管理系統**為一勞永逸的工作;系統需要持續的評估及調整,以確保有效及與時並進。機構應定期監察、評估及更新系統的組件,以配合機構內外諸如科技、業務模式、法例及最佳行事方式等各方面的轉變。

實施私隱管理系統的好處

受條例規管的機構都須遵從條例的規定。全面的**私隱管理系統**不單可協助機構有效地循規,而且有助建立和推動尊重私隱的機構文化,這有利機構與客戶、僱員、股東及監管機構建立互信關係。

坐言起行,實施健全的**私隱管理系統**,可贏取持份者(包括客戶)對機構的信任。穩健的**私隱管理系統**亦可提升機構的聲譽,加強競爭優勢。

相反,保障個人資料方面不周,有損機構的信譽。機構若發生個人資料外洩事故,更可能要付上非常沉重的代價(不論在善後及修補聲譽方面而言)。資料外洩對受影響人士而言,代價亦相當大。

不少組織及機構持有大量的個人資料，加上資料的經濟價值日增，公眾對侵犯私隱的事故關注度亦有所提升，機構有必要一方面採取步驟制定及維持**私隱管理系統**，以減低事故發生的風險，另一方面提高處理根本問題的能力，把事故造成的損害減至最低。

建立全面的私隱管理系統

甲部－私隱管理系統的基本原則

機構應如何確保其處理個人資料的做法恰當？如何判辨做法的錯對？如何向機構內部、客戶、公眾及私隱專員證明有能力遵從及已經遵從條例的規定？

公署建議機構指派專責人員訂立、推行及維持機構的個人資料保障措施和常規。制定政策及程序，以及培訓僱員都是必要的。如機構把個人資料交由承辦商（資料處理者）處理，須以合約規範方法（或其他方法）確保有關資料受保障的程度等同由該機構提供的。機構應設立制度去回應個人就其個人資料而提出的查閱及改正資料要求，以及處理僱員及客戶有關個人資料私隱受侵犯的投訴。

本部分概述**私隱管理系統**的必要組件。

1 機構的決心

培養尊重私隱文化的內部管治架構是首要的組件。

機構應建立及實施系統監控，以確保遵從條例附表1的保障資料原則。機構需要設立相應的管治架構，或最低限度引入可依循的程序及確保這些程序得以落實，方可有效地和以負責任的態度遵從法律規定。另外，機構需要培養尊重私隱的文化。

(a) 最高管理層的支持

成功推行**私隱管理系統**，有賴最高管理層的支持，這亦是推動尊重私隱文化的關鍵因素。

機構最高管理層要以問責的態度以示保障私隱的決心，**私隱管理系統**才有機會成功，尊重私隱的文化才可得以建立。

最高管理層應坐言起行，支持推行**私隱管理系統**。因應機構的架構，他們應該：

- 委任保障資料主任；
- 對系統的監控給予認許；及
- 適時地向董事局匯報系統運行的情況。

(b) 保障資料主任／保障資料部門

委任或指派專責人員管理**私隱管理系統**。

機構應指派專責人員全面監督機構遵從條例的規定，這人員在大企業可能是高級行政人員，在小型機構則可能是公司擁有人／營運者（統稱「**保障資料主任**」）。保障資料主任的職務不一定是全職的。在規模較大的機構，保障資料主任可能需要其他的專責人員支援。此外，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），機構內其他人員也可能會參與處理個人資料的工作。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。

保障資料主任在保障個人資料方面身兼多個角色，一般包括：

- 建立及實施系統監控；
- 協調機構內相關部門或職能的合適人士；
- 負責對系統監控進行持續評估及修訂；
- 代表機構回應私隱專員的查詢，及配合其視察或調查；及
- 在機構內提倡個人資料保障。

上述最後一個角色的重要性不下於其他角色。機構要權衡不同方面對工作的要求，而個人資料保障只是其中一項議題。個人資料保障不應止於法律上的循規，還涵蓋改善流程、客戶關係管理及機構聲譽等。機構各層面都應該肯定**私隱管理系統**的重要性，把這系統融入每個涉及使用個人資料的主要職能，包括產品開發、客戶服務或營銷活動。

(c) 匯報

建立匯報機制，並在系統監控中反映。

機構應建立內部匯報機制，以確保有關職員認識其機構的**私隱管理系統**，以及系統運作有否達致預期效果。大機構的最高管理層在聽取這些資訊後可繼而向董事局匯報。所有匯報機制應反映在機構的系統監控中。

機構應制定某種形式的內部審核及保證程序，以監察其保障個人資料政策的遵守情況。小型機構的監察內容可以包括客戶及僱員對系統的意見；對大型機構來說，可以是第三者的核證。如機構面對公署根據條例作出的查詢、視察或調查，這些報告或有助證明該機構已遵從條例的規定。

不過，單單設有匯報機制是不足夠的。在某些時候，例如保安失效而外洩資料，或接獲投訴，機構應考慮把涉及個人資料的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。為確保相關人士依從既定流程，機構在啟動應變機制時可能需要監察所需步驟的依從情況。一些機構更會對個人資料外洩事故的識別、升級機制及回應行動進行測試。

有效的匯報機制：

- 清楚訂明匯報程序（報告機構整體的循規活動），及在接獲投訴或可能發生資料外洩事故時員工的匯報程序；
- 對內部匯報程序進行測試及報告成效；及
- 記錄所有匯報程序。

2 系統監控

系統監控是**私隱管理系統**的另一組件，以確保機構依據管治架構的方針行事。本部分簡述**私隱管理系統**的監控，設立這些監控有助保障資料主任在機構中建立適當的**私隱管理系統**，監控措施亦可反映機構遵從條例規定的情況。

(a) 個人資料庫存

機構的**私隱管理系統**不論已否發展成熟，或只是新引入的，它均可以經仔細檢視其持有的個人資料及現行的資料處理方法而從中獲益。

機構應知道它持有甚麼種類的個人資料（例如僱員的個人資料、客戶的個人資料等）、如何使用有關個人資料，以及是否真正需要有關資料。了解及記錄所收集的個人資料類別和資料的存放處是重要的（例如有否已轉移任何資料處理者），因為這關乎機構應向資料當事人徵求何種方式的同意，應如何保護有關資料，以及令機構更容易配合個人行使查閱及改正資料的權利。具問責性及有效的**私隱管理系統**，每個組件都需要先作這項評估。

機構應清楚知道：

- 它持有甚麼種類的個人資料，資料存放在何處（在機構內，或由資料處理者持有）；並作記錄；及
- 它為何收集、使用或披露個人資料，並記錄有關原因。

(b) 政策

機構應就履行條例下的責任而制定內部政策，並予以記錄。機構應向員工傳達相關政策，並定期提醒他們這些政策及通知他們最新的修訂內容。

機構可因應遵行條例下六項保障資料原則而制定內部政策，這些政策應予以記錄，內容亦應與法律規定相符。

機構應制定的主要政策如下：

- 個人資料的收集；
- 個人資料的準確性及保留時間；
- 個人資料的使用，包括徵求同意的規定；
- 個人資料的保安；
- 機構的個人資料政策及常規的透明度；及
- 個人資料的查閱及改正。

機構亦應適當地把個人資料保障的循規要求納入機構的其他政策中，例如，合約管理政策、採購政策、人力資源政策及有關披露個人資料予監管機構、執法機關及其他政府部門的政策。

機構可參閱私隱專員就各種保障資料的範疇而發出的指引。

(c) 風險評估工具

個人資料的私隱風險可隨時間而改變。為確保機構的政策及常規持續地遵從條例的規定，定期的風險評估是任何**私隱管理系統**不可或缺的部分，尤其是當規管個人資料的法規有重大改動，或資料使用者對現行個人資料程序作出重大改動，或引入新的個人資料程序，都應該事先進行評估。

機構所提供的服務有時會牽涉收集、使用或披露個人資料，但機構卻未有從私隱角度作全面審視。妥善利用風險評估工具有助預防問題發生。機構在推出某項目、產品或服務前，事先細心推敲其目的，並進行評估以減低對個人資料私隱造成的影響，至為重要。在問題發生後才去補救，所付出的代價可能相當高昂。

總括而言，機構在推行任何新措施前，若與現行做法大相逕庭，而又涉及個人資料，或進行任何新方式收集、使用或披露個人資料，都應該進行上述評估。機構應訂立程序（可包括私隱影響評估），以識別及減低資料外洩及保安的風險。保障資料主任在這方面應擔當諮詢或顧問的角色。公署發出《私隱影響評估》[1]資料單張，就這方面提供建議。

(d) 培訓及教育推廣

健全的**私隱管理系統**有賴機構中的相關成員（即處理個人資料的人士）都知悉其保障個人資料的責任，並付諸實行。針對相關員工的特定需要而提供培訓及教育，以傳達最新資訊，是有效推行**私隱管理系統**的關鍵。

為求**私隱管理系統**有效推行，相關員工應知悉保障個人資料的一般規定，並熟悉機構的政策及常規，以遵從條例的規定。直接處理個人資料的員工可能因應其職責所需要接受額外的培訓。培訓及教育要與時並進，和配合實際所需。機構可派員參加公署舉辦的專業研習班，或安排機構內部培訓。

員工有保障個人資料的意識，自然可以為機構更積極地保護個人資料。機構可能有非常周全的政策及系統監控，但如果僱員不依從，**私隱管理系統**便形同虛設。機構應經常提醒相關員工依從機構的政策及系統監控，並強調保障資料是其職責不可或缺的部分。

[1] www.pcpd.org.hk/chinese/publications/files/PIAleaflet_c.pdf

機構可利用不同的方法提供保障個人資料的培訓及教育，例如在公司的內聯網提供必修的培訓課程單元、舉行小組會議、一對一培訓，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。機構應記錄其培訓安排，評估參與度和成效。

有效的個人資料保障培訓及教育推廣活動應：

- 為新入職員工的簡介內容中提供相關的資訊，並其後定期再提示；
- 覆蓋機構制定的政策及程序；
- 配合機構的需要，以適合及有效的方式提供；及
- 如有緊急需要，應盡快把必要的訊息傳達予相關員工。

(e) 資料外洩事故的處理

從多方面看，一旦發生個人資料外洩事故，機構要賠上很大的代價，更可能因而失去客戶的信任。

機構應確立程序及委派專責人員或指定團隊負責處理個人資料外洩事故，並明確界定對內及向外通報事故的責任。

雖然條例沒有強制規定機構向私隱專員通報重大的資料外洩事故，但私隱專員鼓勵機構在處理資料外洩事故時採納通報程序。

機構在處理個人資料外洩事故時，應考慮事故的情況，決定應否盡快通知下述人士：

- 受影響的資料當事人；
- 執法部門；
- 私隱專員；
- 相關監管機構；及
- 其他可採取補救行動，保障受影響資料當事人的個人資料私隱及利益的人士，例如互聯網搜尋公司可提供協助，從搜尋引擎移除相關的快取連結。

公署發出的《資料外洩事故的處理及通報指引》[2]在這方面提供了實際的指引。

(f) 對資料處理者的管理

交由資料處理者處理個人資料的安排是另一個需要考慮的重要範疇。機構是否有採用合約規範或其他方法保障個人資料？

機構委以資料處理者的責任包括以下幾類：

- 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使用及披露；
- (絕對或有限制地)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；及
- 承擔違反合約的後果。

機構可參考公署發出的《外判個人資料的處理予資料處理者》[3]資料單張。

(g) 溝通

採取所有切實可行的步驟，確保員工及客戶知悉其個人資料政策及常規。

傳達的訊息應清晰及易於理解，而非純粹覆述條例內容。一般而言，溝通應：

- 提供足夠的資訊，讓公眾知道機構收集、使用及披露個人資料的目的，以及保留資料多久；
- 包括向公眾介紹，如有需要提出問題或關注時可聯絡的機構專責職員；及
- 讓公眾容易獲取相關資訊。

機構應讓公眾知悉他們可以查閱機構持有關於他們的個人資料，及如何提出改正資料的要求或查詢機構遵從條例規定的情況。

[2] www.pcpd.org.hk/chinese/publications/files/DataBreachHandling_c.pdf

乙部－持續評估及修訂

甲部說明了構成**私隱管理系統**的組件。本指引乙部概述確保維持**私隱管理系統**持續有效、循規及具問責性的基本工作。為妥善保障個人資料及符合法律規定，機構應不停監察、評估及修訂其框架，以確保該系統切合實際需要和恒之有效。

1 制定監督及檢討計劃

制定監督及檢討計劃，有助機構持續推行其**私隱管理系統**及保持系統切合最新情況。

保障資料主任或部門應定期制定監督及檢討計劃，當中列明監察及評估**私隱管理系統**成效的方法和時間，以實踐機構的決心（如甲部1所列）。機構可因應其循規及監控的基礎設施，把這計劃納入機構整體的監督及檢討體系之中。該計劃應訂立評估表現的準則、檢討政策及其他系統監控的時間表。

2 評估及修訂系統監控

機構應監察系統監控的成效，定期審核及在有需要時予以修訂。

監察是應該持之以恆，並可回應以下一些基本問題：

- 有甚麼新的威脅及風險？
- 系統監控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，所涉及的個人資料收集、使用或披露有所增加？
- 是否需要提供培訓？如需要的話，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。

對於重大或高風險的流程，機構應定期地進行內部或對外的審核，以評估其**私隱管理系統**是否有效地運行。其次保障資料部門亦可定期進行評估，以確保主要的流程得以遵行。對於較小型的機構或非正規的定期檢討，機構應制定清單。無論如何，機構應採取適合的評估方法，制定實務措施，確保員工或承辦商依從機構的政策及系統監控。

正如前文所述，本指引文件並不是放諸四海皆準的方案。每個機構需要決定如何建立其**私隱管理系統**，考慮的因素包括機構的規模、業務性質及所處理的個人資料有多少和敏感程度。

機構應以專注、持續及徹底的方式，評估其系統監控（如甲部所述）。

根據評估結果，保障資料主任應考慮是否需要更新及修訂系統監控，這項責任十分重要。機構如要改動系統監控，應即時通知員工，或為員工提供適當的培訓以溫故知新。

簡而言之，資料保障主任應採取以下的措施：

- **監察及更新個人資料庫存**
  定期確保資料不過時，辨識及評估新收集的個人資料，及其使用及披露方式。
- **檢討及修訂政策**
  因應資料外洩事故或投訴，遵從新指引和相關行業的最佳行事方式，以及外在環境因素，適時地作出評估和審核。
- **私隱影響評估及保安風險評估**
  這些評估必需要不斷更新，緊隨私隱和保安風險改變或機構的新業務而作出相應的評估和措施。
- **檢討及更新培訓教育的內容**
  要與時並進，持續評估，若有系統監控更新時，應適時地傳達給相關的人員。
- **檢討及訂立資料外洩事故的應變管理機制**
  實施最佳的行事方式和採納建議，並在事後檢討中汲取教訓。
- **檢討並適時地作出微調**
  與資料處理者簽訂的合約內容要定期檢討相關的要求。
- **更新及澄清，並適時地溝通**
  機構應向僱員和客戶解釋其個人資料政策。

[3] www.pcpd.org.hk/chinese/publications/files/dataprocessors_c.pdf

私隱管理系統一覽

甲部、基本原則

機構的決心

最高管理層的支持	保障資料主任／部門	匯報
• **私隱管理系統的**成功關鍵，有賴最高管理層的支持，方可有效地推動尊重私隱的文化。	• 有專責人員擔任相關職能，在適當情況下參與機構的決策過程。 • 清晰界定機構內監察循規的角色和責任，並傳達給所有相關人員。 • 負責建立及實施系統監控，持續作出評估及修訂。 • 確保業務中每個涉及使用個人資料的主要部門，均有相應的資料保障政策和程序。	• 建立匯報機制，並在系統監控中反映匯報機制的運作。

系統監控
設立以下監控機制：

個人資料庫存	政策	風險評估工具
• 機構有能力識別其監管或控制的個人資料 • 機構有能力識別其收集、使用及披露個人資料的原因	涵蓋： • 個人資料的收集 • 個人資料的準確性及保留時間 • 個人資料的使用，包括徵求同意方面的規定 • 個人資料的保安 • 機構的個人資料政策及常規的透明度 • 個人資料的查閱及改正	培訓及教育推廣 資料外洩事故的處理 對資料處理者的管理 溝通

乙部、持續評估及修訂

監督及檢討計劃

- 制訂監督及檢討計劃

  保障資料主任／部門應定期制訂監督及檢討計劃，訂出監察及評估系統監控成效的方法。

按需要評估及修訂系統監控

- 更新個人資料庫存
- 修訂政策
- 不斷更新風險評估工具
- 更新培訓及教育的內容
- 訂立資料外洩事故應變機制
- 調整對資料處理者的管理
- 改善溝通

私隱管理系統
Privacy Management Programme

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

www.pcpd.org.hk/pmp

鳴謝

本指引乃參照加拿大私隱專員公署、加拿大阿爾伯達及卑詩省資訊及私隱專員公署於2012年4月出版的指引"Getting Accountability Right with a Privacy Management Program"撰寫(www.oipc.bc.ca/guidance-documents/1435)，公署謹此向有關作者致謝。

免責聲明

本指引所載的資料只作一般參考用途，並非為《個人資料(私隱)條例》的應用提供詳盡指引。有關法例的詳細及明確內容，請直接參閱條例的條文。私隱專員並沒有就上述資料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。上述建議不會影響私隱專員在條例下獲賦予的職能及權力。

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 : enquiry@pcpd.org.hk