

由原則至行動 – 中小企保障個人資料實務手冊

From Principles to Practice –
SME Personal Data Protection Toolkit



PCPD



HK

PCPD.org.hk

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

目錄



序言	03
《私隱條例》的主要釋義	05
《私隱條例》與你的業務	09
中小企十項實務行動	17
實用工具和清單	45
直接促銷與你的業務	63
人力資源管理 — 該做與不該做的事	71
將個人資料移轉至香港以外地方	73
內地民商事務所涉個人信息及網絡安全主要法規簡介	75
《通用數據保障條例》與你	77
建立問責制、加強企業承諾 — 私隱管理系統	78
尊重、互惠和公平 — 數據道德管治	81
私隱公署中小企諮詢服務	83
附錄	84

序言



本港現時共有約34萬¹家中小型企業（中小企），佔全港企業總數逾九成八，聘用的僱員佔私營機構人力市場45%，為約130萬人提供就業機會，對本港的經濟貢獻舉足輕重。

中小企在業務營運過程中經常收集及處理各式各樣客戶及員工的個人資料。在現今「資料猶如一項資產」的世代，公眾及客戶對個人資料私隱保障的期望與日俱增，中小企必須積極主動保障個人資料私隱，依從《個人資料（私隱）條例》（《私隱條例》）的規定和實踐數據道德管治，確保個人資料獲妥善保存及管理，這樣既可贏取客戶的信任，亦能提升其商譽及競爭優勢。

中小企的優勢在於運作靈活，但亦往往礙於資源所限而未能兼顧保障個人資料的措施。故此，我們希望藉著本刊物，提升中小企對保障、尊重個人資料的認知，並提供實用資訊從而系統地協助它們依從《私隱條例》的規定和實踐數據道德，締造一個保障個人資料私隱的工作環境及運作模式，共同攜手構建尊重個人資料私隱的文化。

¹ 資料來源：https://www.tid.gov.hk/tc_chi/smes_industry/smes/smes_content.html

這本《中小企保障個人資料實務手冊》旨在便利中小企制定符合《私隱條例》規定的合規策略，以切合它們業務的實際需要。中小企可視此刊物為企業推行相關合規和管治工作的出發點。本手冊內載有一些實用清單，幫助中小企確定是否已制定必要的政策、控制措施和程序，以依從《私隱條例》的保障資料原則的規定，和符合消費者的期望。

私隱公署另提供一系列實用資源，幫助中小企了解《私隱條例》。這些資源可在私隱公署網站 www.pcpd.org.hk 瀏覽及下載。

黃繼兒大律師

香港個人資料私隱專員

二零二零年六月



《私隱條例》的主要釋義

個人資料

任何資料 1) 與一名在世人士有關，2) 從該資料直接或間接地確定有關的個人的身份是切實可行的；及 3) 該資料的存在形式予以查閱及處理均是切實可行的。

保障資料原則

在《私隱條例》附表 1 列明的原則，包括：個人資料的收集、準確性和保留期間、資料使用、透明度、以及查閱及改正個人資料。

資料當事人

指屬該個人資料的當事人的在世人士

資料使用者

指獨自或聯同其他人或與其他人共同控制該個人資料的收集、持有、處理或使用的人。資料使用者作為主事人，須對其授權的資料處理者的不當行為負上法律責任。

使用個人資料

包括披露或移轉該個人資料

處理個人資料

包括將個人資料修訂、擴增、刪去或重新排列

資料處理者

任何個人或機構 1) 代另一人處理個人資料；2) 並不為該人本身目的而處理該資料。

開始...



開始開



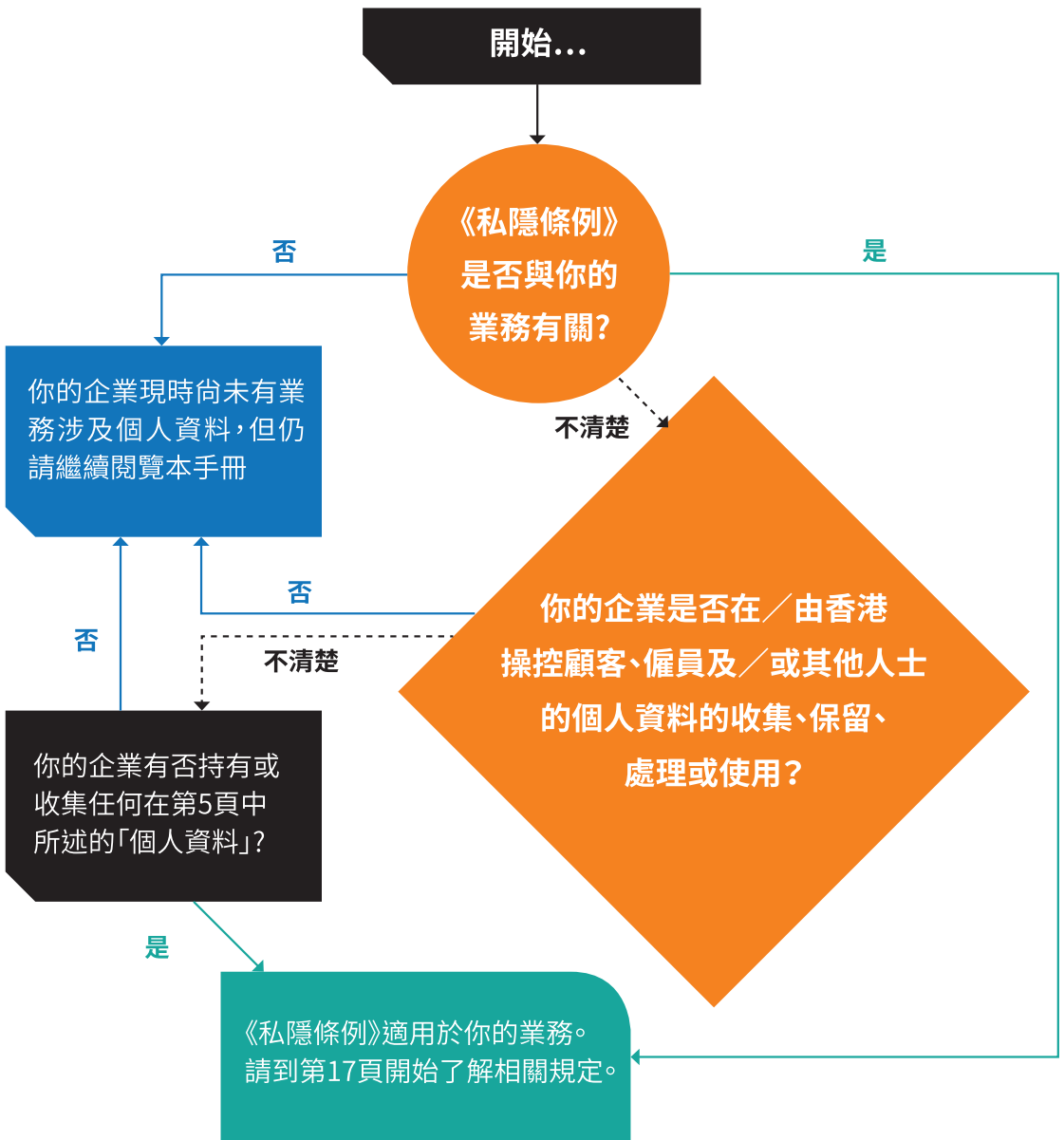
《私隱條例》與你的業務

企業在收集、保留、處理和使用個人資料時依從《私隱條例》，是法律的規定。《私隱條例》亦提供了良好的基礎，讓企業在合規之餘，以更高的數據道德標準處理個人資料。

企業倘能合法和有道德地處理客戶的個人資料，將可贏得客戶以及業務夥伴的信任，最終亦可增加企業的競爭優勢。



個人資料與你業務的關係



中小企十項實務行動



真
十勤
全行
心務
母德

中小企 十項 實務行動

中小企 十項 實務行動

01

認識《私隱條例》

先對《私隱條例》及其保障資料原則作基本認識，以作為你的企業在處理個人資料方面合規的依據。 ▶ 頁 17

02

為何要收集這些個人資料？

在收集個人資料前，確定你收集該等資料的目的，以檢討和確定處理資料程序的私隱風險。 ▶ 頁 22

03

有否清晰地通知個別人士收集其個人資料的目的？

在收集個人資料時或之前，清晰告訴相關人士為何你需要他們的個人資料，及你將如何使用該等資料。 ▶ 頁 23

04

持有個人資料的期限和準確性

確保你的企業持有的個人資料準確無誤，以及保留時間不會超過達致原來目的的实际所需。 ▶ 頁 25

05

如何使用收集所得的個人資料？

檢討資料收集目的，若打算使用於新目的時，須在使用前確保已取得相關人士的訂明同意。 ▶ 頁 27

10

私隱影響評估

使個人資料私隱成為將來業務項目的核心元素。 ▶ 頁 41

09

委聘資料處理者

採用合約或以其他方式以令資料處理者承擔責任。 ▶ 頁 39

08

處理查閱和改正個人資料要求

確保你的企業已訂立程序，回應個別人士提出的相關要求，提供及更新個人資料。 ▶ 頁 34

07

建立資料外洩事故通報程序

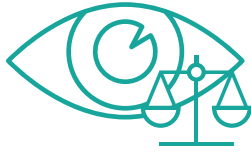
確保你的企業已採取良好行事方式，訂立程序以偵測、匯報和調查資料外洩事故。 ▶ 頁 32

06

檢視資料保安

確保所持有的個人資料的安全，不會未經授權或意外被查閱、處理、刪除、喪失或使用。 ▶ 頁 30

01



認識《私隱條例》

《私隱條例》旨在保障在世人士的個人資料私隱權，屬科技中立和原則性的條例，在科技發展和創新，與保障和尊重個人資料之間取得平衡。

甚麼是「個人資料」？

根據《私隱條例》，個人資料是指任何資料 1) 與一名在世人士有關，2) 從該資料直接或間接地確定有關的個人的身份是切實可行的；及 3) 該資料的存在形式予以查閱及處理均是切實可行的。

一般而言，個人的姓名、年齡、電話號碼、地址、身份證號碼、相片、收入、病歷、受僱紀錄、財務狀況等都是受《私隱條例》保障的個人資料。



六項保障資料原則

任何企業或機構（不論規模和性質）在 / 由香港操控個人資料的收集、持有、處理或使用，都必須遵從《私隱條例》的規定，包括其六項保障資料原則。該六項原則涵蓋了個人資料的整個生命週期。

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。
- 須以切實可行的方法告知資料當事人是否必須提供資料、收集其個人資料的目的、資料可能會被轉移給哪類人士，以及資料當事人要求查閱及改正自己的資料的權利和途徑。
- 收集的資料是有實際需要的，並且不超乎適度。

原則



個人資料的準確性及保留期間

- 資料使用者須採取切實可行的步驟，以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的的實際所需。

原則



個人資料的使用

- 除非得到資料當事人自願給予的明示同意，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。



原則



個人資料的保安

- 資料使用者須採取合理地切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

原則

**公開政策：資訊須在一般情況下可提供**

- 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。



原則

**查閱及更正個人資料**

- 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。

本手冊內其後的章節將更詳盡闡述上述原則的內容。

《私隱條例》的豁免範圍？

《私隱條例》訂明在不同情況下因實際需要，個人資料可獲豁免而不受若干條文所管限，例如：

- 與僱傭事宜及特定程序有關的個人資料，可免受查閱資料原則所管限；
- 若查閱資料原則及使用資料原則的應用於相關的個人資料，相當可能會損及保安、防衛和國際關係；防止或偵查罪行；評估或徵收稅項；新聞活動；健康；法律程序；專業盡職審查；存檔；處理危急情況等（未盡錄），相關資料可獲豁免。



罪行及補償

- 違反保障資料原則並不直接構成刑事罪行，惟私隱專員可發出執行通知，指令有關的資料使用者採取補救措施。
- 不遵守執行通知屬於刑事罪行，一經定罪，最高可被判處罰款港幣五萬元及監禁兩年。
- 若有人認為其個人資料私隱受侵犯而蒙受損失，包括感情傷害，可根據《私隱條例》向相關的資料使用者申索，以彌補損失。
- 《私隱條例》把某些活動刑事化，包括：
 - 錯誤或不當使用個人資料以作直接促銷用途；
 - 不依從查閱個人資料要求；
 - 未獲資料使用者授權而披露取自其持有的個人資料等。

更多資料：
請瀏覽 PCPD.org.hk



02



為何要收集個人資料？

當你計劃向客戶或其他人收集其個人資料時，你應該首先考慮這個問題。

在收集個人資料之前或之時應先確定收集個人資料的原因和目的，這將有助你履行在《私隱條例》下處理個人資料時的有關責任。

- 為甚麼你的企業需要這些個人資料？
- 收集資料的方法是否合法和公平？
- 是否必須收集該等資料，否則你無法提供所需的服務或滿足營運需求？還有其他選擇嗎？
- 將會如何使用該等個人資料？
- 你會否將收集到的個人資料轉移給他人？

此外，在你收集個人資料時：

- 你是否已通知有關人士相關的收集目的？（參見第23頁有關通知個別人士收集其個人資料的目的）

請記錄各項個人資料收集的目的。你可以首先參考第45頁上的個人資料庫存清單，以擬備自己機構的資料清單。

實用貼士

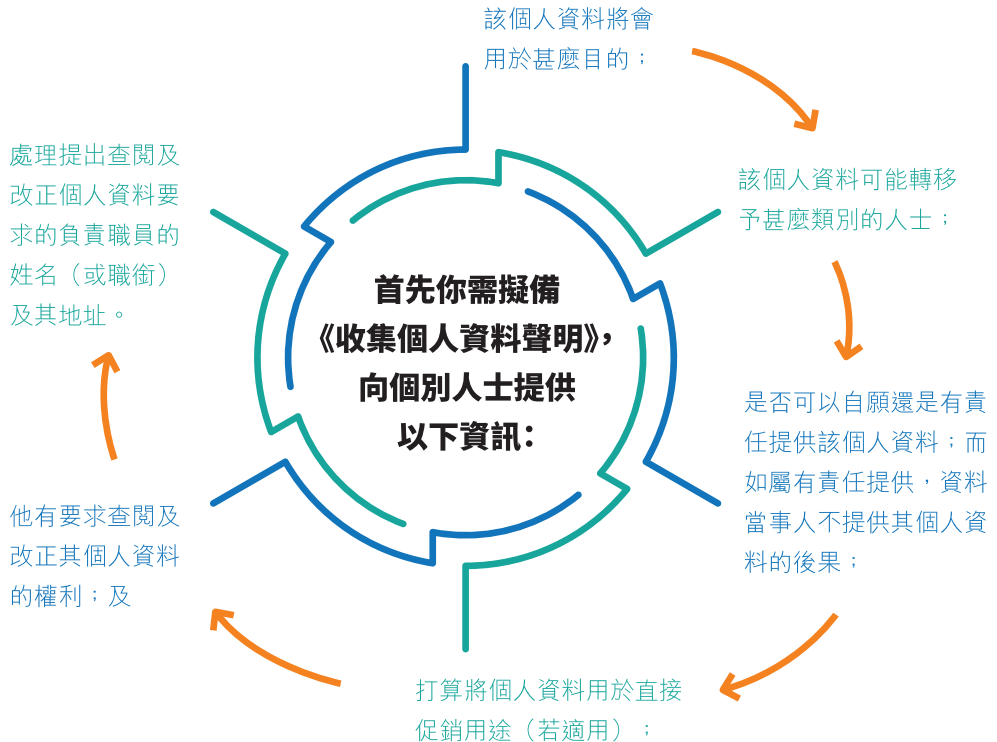
- 當你收集個人資料時，應只收集對該目的而言是必須及足夠的資料，但不要超乎適度。

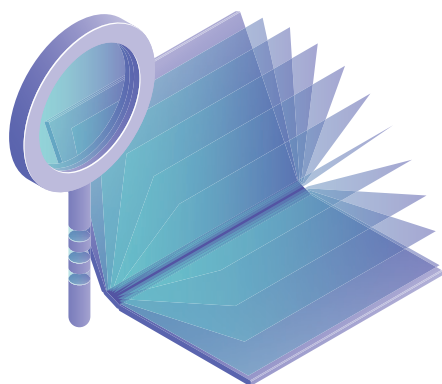
03



有否清晰地通知個別人士收集其個人資料的目的？

在收集個人資料之前或之時，你有沒有明確告知資料當事人為何你需要他們的資料及將會如何使用呢？





你的《收集個人資料聲明》應以易於閱讀及理解的方式展示。每次當收集個人資料時，應提供《收集個人資料聲明》（不論是線上或線下）。

你可以參考第46至47頁的樣本擬備你的《收集個人資料聲明》。

實用貼士—擬備有效的《收集個人資料聲明》

- 內容要具體—《收集個人資料聲明》中所述的目的不應過於含糊及範圍太廣，以便讓個人在知情的情況下作出決定，並清楚訂明資料承轉人類別；
- 簡潔易明—《收集個人資料聲明》的版面及展示方式（包括字體大小、間距、下劃線、標題的使用等）須讓客戶易於閱讀；及
- 使用簡單語言—避免使用艱澀的字眼。

04



持有個人資料的期限和準確性

你應記錄及檢視所持有的個人資料，以確保準確無誤，以及保留時間不會超過達致原來目的的實際所需。

你的企業保留個人資料多久？

《私隱條例》並沒有訂明確實的個人資料保留時限，不過，你應確保個人資料不會保留超過達致原來目的的實際所需，並刪除已不再需要的個人資料。若存在有效的目的（如有法律要求或允許的情況下）則可以保留相關資料。你應採取良好的行事方式，制定個人資料政策（包括檢視時間表和程序），詳細列明你保留的個人資料的安排。



開始你的個人資料庫存檢查!

不妨利用在第45頁的範本，規劃和檢視你的企業現時所持有和處理的個人資料。

實用貼士

- 需要訂立資料保留程序，並進行定期檢視，以協助釐定相關資料是否仍需保留。
- 定期進行檢視以確定是否仍然需要現時所持有的個人資料。若無需要繼續持有該些資料，便應刪除。
- 訂立最長及最短的個人資料保留時限，當中需考慮其他法律要求或限制。



05



如何使用收集所得的個人資料？

個人資料只可使用、披露或轉移於收集時所述明的目的。因此，在使用收集所得的個人資料時，你需要參考相關的收集目的，並定期進行檢視，並確保資料用於收集資料時述明的目的或直接有關的目的。若用於新目的，之前須獲得個人自願給予的明示同意。

來個快測…

- 當你打算使用收集所得的個人資料時，應先參考相關的收集目的。
- 若打算使用個人資料在任何新的目的時，須取得該名人士的同意方可使用。
- 記錄任何使用個人資料的新目的。



提升行事方式透明度！

制定與個人資料相關的政策和實務，並擬備《私隱政策聲明》，有效地告知你的顧客、僱員和公眾有關企業的資料管理政策和實務。

《私隱政策聲明》應包括：

- **政策聲明**以述明資料使用者在保障個人資料私隱權益方面，為向其提供資料的個人所作出的整體承擔。
(例子：我們承諾遵守《個人資料（私隱）條例》的規定。為履行此承諾，我們會確保屬下職員依從保安及保密方面的最嚴格規定。)
- **實務聲明**以述明資料使用者所持有的個人資料的種類（例如：聯絡資料、財務資料、瀏覽器資料及 IP 地址），及有關資料的使用目的（例如：交付貨物／服務、管理帳戶、便利瀏覽網站）。



擬備有效的 《私隱政策聲明》

- 在未得到負有家長責任的人士的同意前，不應向未成年人士收集個人資料。
- 清楚述明：
 - ▶ 不接受 cookies 的使用者可否瀏覽網站，及因不接受 cookies 而不可使用的功能（如適用）；
 - ▶ 個人資料一般會保留多久；
 - ▶ 如何表達刪除資料要求；
 - ▶ 收集所得的敏感個人資料會如何使用、處理及轉移；
 - ▶ 在未得到資料當事人的明確及自願同意前會不會向其他人士披露個人資料；
 - ▶ 如何確保所收集的個人資料安全及保密；
 - ▶ 甚麼個人資料會被轉移予服務提供者及這些服務提供者會如何保障所收到的個人資料；
 - ▶ 若不會收集或使用個人資料，通過《私隱政策聲明》予以承諾；
 - ▶ 處理個人就資料使用者所持有的個人資料而提出的查閱及改正資料要求的政策；
 - ▶ 企業內負責答覆有關私隱政策及實務查詢的聯絡人詳情（例如辦公地址及電郵地址）
- 應易於理解及閱讀；及
- 如企業的個人資料政策及實務複雜和篇幅較長，應善用標題及以分層方式呈示

定期檢視企業現有的《私隱政策聲明》，以確定是否仍符合《私隱條例》的規定。

實用資料：

《擬備收集個人資料聲明及私隱政策聲明指引》



06



檢視資料保安

企業有責任保障收集所得的個人資料免被遺失或盜取，又或被未經授權查閱、披露或使用。

《私隱條例》沒有訂明企業須採取的資料保安措施。然而，你的企業必須採取所有合理地切實可行的步驟以保障個人資料。考慮因素包括：

- 個人資料的敏感度及保密度
- 資料數量
- 資料形式
- 儲存方式



無論資料屬何種形式，你必須確保所持有的個人資料的安全，包括：

- 實質的措施：如鎖好存放檔案的儲物櫃；
- 電子方式：如設密碼、加密、防火牆；
- 政策管控：如按「有需要知道」原則限制查閱、僱員培訓、與外判商訂立合約；
- 妥善銷毀／刪除個人資料，避免發生資料外洩事故，例如：碎去紙張文本、刪除電子記錄等。

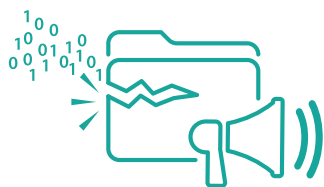


實用貼士－保障企業所持有的個人資料

- 制定和實施企業內部的保安措施，以保障個人資料；
- 使用合適的保安措施以保障不同形式的個人資料；
- 定期檢視相關的保安政策和措施以確保資料是最新的；
- 提供相關的僱員培訓，確保僱員對資料保安的認知；
- 採取合約方式以避免轉移予外判商的個人資料被未經授權而被查閱、處理、刪除、喪失或使用。

若發生個人資料外洩事故，你應怎樣做呢？看看下一項實務行動。

07



建立資料外洩事故通報程序

對企業而言，發生資料外洩事故可以帶來沉重的代價，這對中小企的影響尤甚，其中包括阻礙業務運作、令商譽受損、失去顧客的信任、遭到黑客勒索等。網絡罪行日趨增多，是以企業絕不能忽視個人資料被盜取或喪失的威脅。除了要增強企業的保安措施外，中小企應制定處理資料外洩事故的程序，以減低可能引致的損失。

常見的資料外洩事故包括：

- 遺失庫存的個人資料（如電腦、USB 儲存裝置、文件）
- 不當處理個人資料（如不當棄置、錯誤郵寄或電郵予他人）
- 未經授權查閱客戶或僱員的個人資料
- 載有個人資料的數據庫被外來者未經授權入侵



就從現在開始，制定處理資料外洩事故的政策／程序

採納良好的資料外洩處理政策／程序，可顯示你能以負責和可靠的態度應對事故發生和具備清晰的應變行動計劃。

首先，你可以利用在第48至49頁的資料外洩事故處理清單，制定屬於你的企業的資料外洩事故處理政策／程序。

若發生資料外洩事故，你應如何處理？

切勿慌張！請跟從你所制定的資料外洩處理政策／程序，開始搜集必需的資料，同時考慮盡快採取良好行事方式向受影響人士及監管機構作出通報。

你可利用第51至52頁的資料外洩事故表格，整合資料外洩的資料，並立即採取補救措施，和進行事故後的檢討工作。

雖然現行法例並沒有規定你要就資料外洩事故向私隱專員通報，但盡快作出相關通報屬良好行事方式，以妥善處理有關事故。私隱專員所發出的《資料外洩事故的處理及通報指引》提供相關的實務指引。

如何向私隱專員提交資料外洩事故通報？

- 1) 填妥「資料外洩事故通報表格」
- 2) 透過網上、傳真、親身或郵遞方式向私隱公署提交填妥的表格



實用資料：

《資料外洩事故的處理及通報指引》



08



處理查閱和改正 個人資料要求

在《私隱條例》下，個人有權要求資料使用者向他提供屬於他的個人資料複本，此要求稱為「查閱資料要求」；若他發現其個人資料不準確，可進一步向資料使用者提出資料改正要求。

查閱資料的權利

一般而言，你可以在收集個別人士的個人資料之時或之前，通過《收集個人資料聲明》明確告知其有權要求查閱及改正他的個人資料，以及負責處理該等要求的僱員職銜以及聯絡地址（《收集個人資料聲明》範本可參考第46至47頁）。

查閱資料要求的一些常見例子包括：

- 顧客要求索取他們的服務申請表複本；以及
- 僱員要求索取他們的工作表現評核報告複本。



查閱資料要求表格

查閱資料要求通常是以查閱資料要求表格（OPS003 表格）提出。有時查閱資料要求者未必會採用查閱資料要求表格，而只是在提出要求時表示希望索取他的個人資料。如該要求實質上已包含所需查閱的範圍及詳情，私隱公署極力建議你回覆該項要求。

另外，資料使用者可為依從查閱資料要求而徵收不超乎適度的費用。



查閱資料要求表格

實用貼士

- 查閱資料要求者無權查閱不屬個人資料，亦無權要求查閱不屬於他的個人資料的資料。因此，你須從所要求的資料複本中刪除第三者的個人資料，才向查閱資料要求者提供其個人資料複本。

改正資料的權利

若你已依從查閱資料要求向一名個人提供其資料的複本，該要求者其後認為資料複本有不準確之處，可提出改正該資料的要求。

在《私隱條例》下，企業有責任確保其持有的個人資料準確。若你發現被要求改正的資料是不準確的（即不正確的、有誤導性的、不完全的或過時的），便要在不徵收費用下依從有關要求。



「可被核實的事項」和「意見表達」

當處理改正資料要求時，企業應分辨當中哪些是「可被核實的事項」，哪些是「意見表達」：

- 「可被核實的事項」是指能夠以客觀現實、紀錄或數據為基準評定有關資料是否準確的事項（例如僱員的出勤紀錄、學生成績表上的成績等）。
- 「意見表達」是指不能核實的、或在有關個案的所有情況下予以核實不是切實可行的事實的陳述。若當中涉及專業判斷，在一般情況下，私隱專員不會介入要求專業人士改正其作出的專業判斷的個案。

可被核實的事項

意見表達



實用資料：



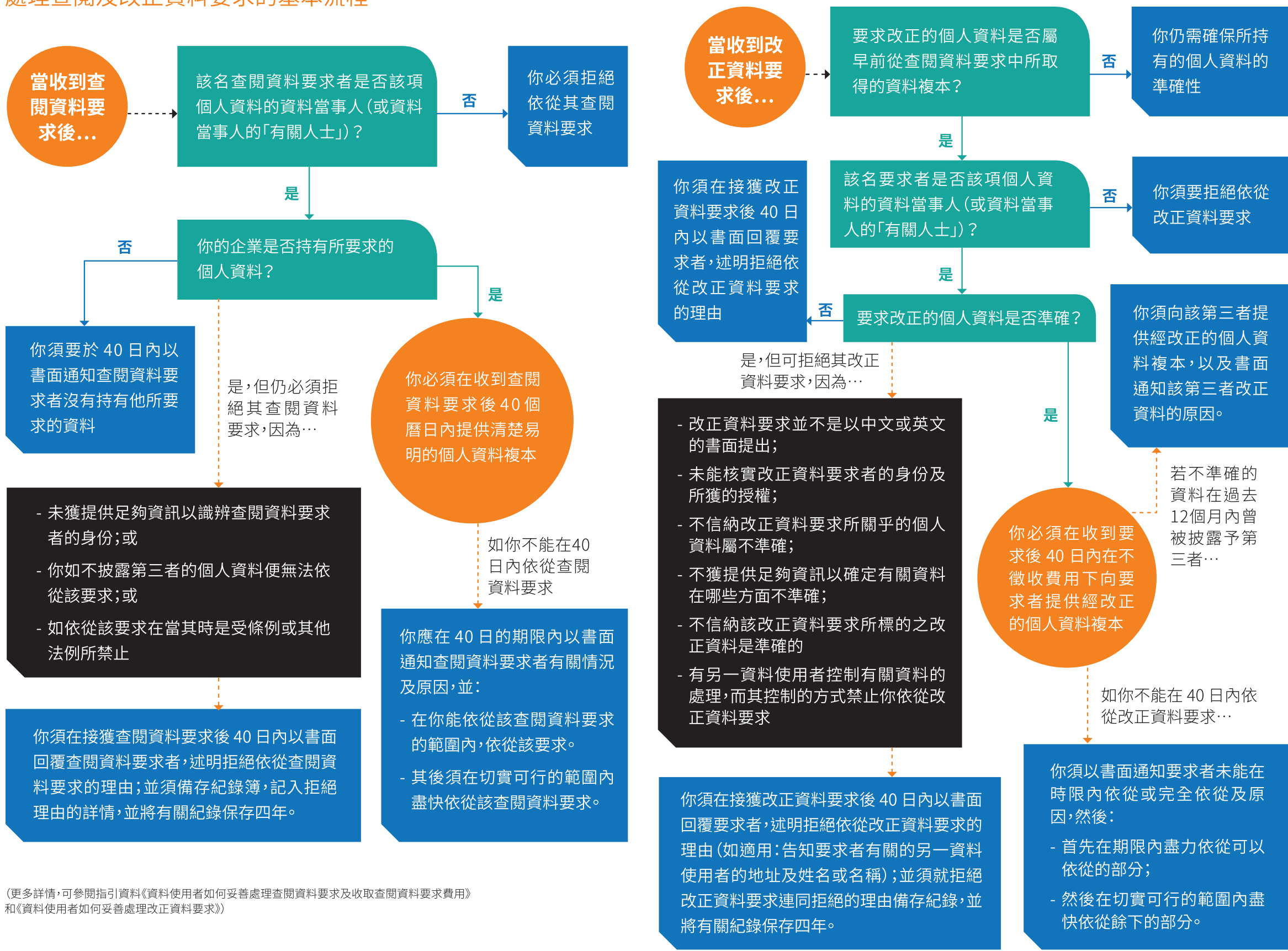
《資料使用者如何妥善處理改正資料要求》



《資料使用者如何妥善處理查閱資料要求及收取查閱資料要求費用》

處理查閱 及 改正資料 要求的 基本流程

處理查閱及改正資料要求的基本流程



(更多詳情, 可參閱指引資料《資料使用者如何妥善處理查閱資料要求及收取查閱資料要求費用》和《資料使用者如何妥善處理改正資料要求》)

09



委聘資料處理者

不少中小企由於人手或資源緊絀，往往會向外尋求專業協助以管理他們的個人資料處理程序，相關的服務包括：

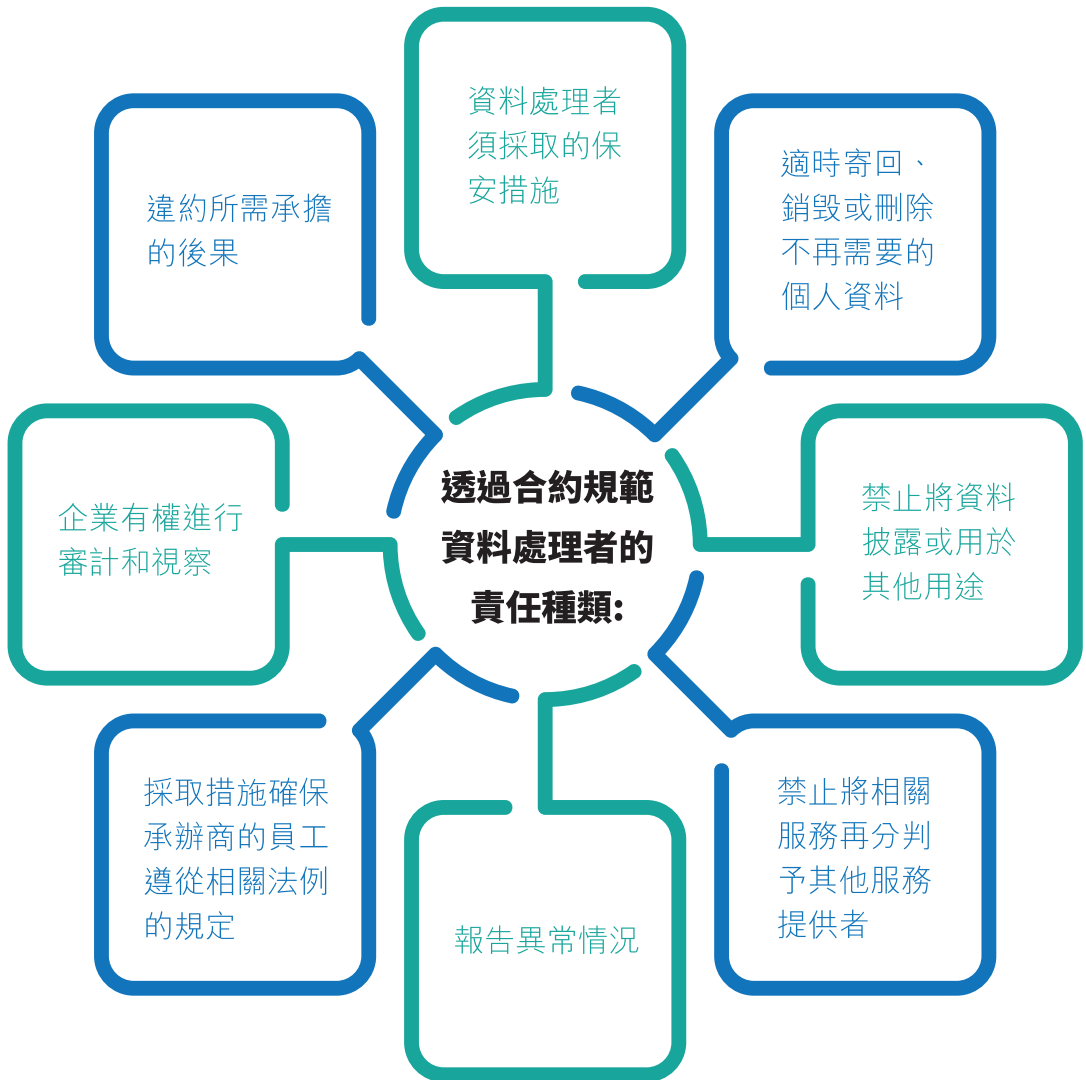
- 網站寄存；
- 伺服器託管；
- 碎紙服務；及
- 活動管理，等等

不過，在《私隱條例》下，若你的企業將處理個人資料工序外判或委託承辦商／服務供應商（作為資料處理者），你作為主事人，仍需為承辦商／服務供應商不當處理個人資料的行為負責。

若你的企業有實質的需要委聘資料處理者，你需要：


- 只向資料處理者提供最低限度的個人資料；
- 採取合約或其他規範方式以保障交託予資料處理者的個人資料；
- 定期進行檢討，以確保已採取足夠和全面的措施管理資料處理者。





不妨利用第53頁的資料處理者檢討清單，定期對資料處理者進行檢視！

10



私隱影響評估

在推出新項目、產品或服務前，若涉及收集或使用個人資料，先進行私隱影響評估！

私隱影響評估能協助企業及早發現潛在的私隱風險，以便作出改善，防患於未然。

何時需要進行私隱影響評估？

- 當規管個人資料私隱的法規有重大改動時
- 企業對現行的處理個人資料程序作出重大改動時
- 企業引入新的個人資料種類
- 企業擬委託資料處理者代表處理個人資料時

私隱影響評估的主要成分為何？

私隱影響評估一般包括以下主要成分：

- 資料處理周期分析；
- 私隱風險分析；
- 避免或減低私隱風險；及
- 私隱影響評估報告

你的企業在作出對個人資料私隱有重大影響的計劃時，應考慮尋求獨立的專業意見，另可參考第55至59頁的私隱影響評估問卷。



實用工具和清單



真
工 嘜
用 標
實 和

個人資料庫存清單 (範本)

ABC 公司	
部門	
個人資料類別及資料當事人類別 <i>例子：在職僱員資料、客戶資料、行銷數據庫</i>	
資料類別中包含的個人資料項目 <i>例子：姓名、地址、電話號碼、電郵地址、身份證號碼</i>	
收集個人資料的渠道 / 方式 <i>例子：向個人直接收集；向第三者收集</i>	
收集及使用個人資料的目的 <i>例子：人事安排、行銷、服務提供、研究</i>	
個人資料的保留時間 <i>例子：兩個月？一年？</i>	
儲存資料的地點 <i>例子：人事部的公司網絡磁碟機；網頁供應商的數據伺服器；公司庫存室</i>	
向第三者披露個人資料 (有/ 沒有)	
向第三者披個人資料的原因及該披露是否符合《私隱條例》下的規定	
資料轉移的可能地點	
資料處理者交還或銷毀資料的日期 (如適用)	
採取的保安措施	

由部門協調主任填寫		由保障資料主任審核	
簽署		簽署	
姓名		姓名	
職位		職位	
日期		日期	

樣本一：
訂購產品和
服務

收集個人資料聲明(範本)

ABC 公司 收集個人資料聲明

本公司向你收集的資料會用以處理你的訂單，以及管理你在本公司開設的帳戶。

你必須在訂單上註明(*)的欄目提供所需的個人資料。如你未能提供，我們未必可以處理你的訂單或向你提供我們的產品或服務。

你有權隨時查閱及改正本公司持有關於你的個人資料。如要欲行使上述權利或改正你的個人資料，請透過_____（公司地址）或電郵_____與本公司的保障資料人員聯絡。

樣本二：
招聘員工

收集個人資料聲明（範本）

ABC 公司 收集個人資料聲明

本公司透過本申請表所收集的個人資料，將會用於評估你是否適合擔任所申請的職位，以及在你獲挑選出任該職位時，用作與你商討初步的薪酬、花紅及福利。

申請表中有（*）號的項目是挑選合適入選者所必須考慮的資料。求職者如不提供此等資料，會對申請的處理及結果有所影響。

本公司的政策是為日後的招聘活動保留落選者的個人資料兩年。如本公司的附屬或聯營機構在此期間出現職位空缺，本公司或會將你的申請資料轉交有關機構考慮。

根據《個人資料（私隱）條例》，你有權要求查閱及改正申請表上所填報的個人資料。如你欲行使這項權利，請填妥本公司的《查閱資料要求表格》，並透過郵寄表格至 _____（公司地址）或電郵 _____，交回人力資源部的資料保障主任辦理。

資料外洩事故處理清單 (範本)

以下資料可用作制訂政策的參考:

	是	否
你的公司是否有制定處理資料外洩事故政策	<input type="radio"/>	<input type="radio"/>
• 如否，現時是否適合制訂該政策?	<input type="radio"/>	<input type="radio"/>
你的公司是否有聘用資料處理者，以代替你的公司處理個人資料	<input type="radio"/>	<input type="radio"/>
• 如是，你的公司有否採用合約規範方法或其他方法，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用?	<input type="radio"/>	<input type="radio"/>
○ 如否，現時適合制訂該政策?	<input type="radio"/>	<input type="radio"/>

處理資料外洩事故政策 / 程序的重要元素

1. 收集有關的重要資料

- 指派適當人士 / 小組負責處理資料外洩事故。
指派人士的職稱及職級: _____
- 持有在調查期間需要收集的重要資料的列表：
 - 外洩日期和時間
 - 外洩地點
 - 如何發現外洩事故及由誰人發現
 - 外洩肇因
 - 受影響的資料當時人種類
 - 估計受影響的資料當時人數量
 - 涉及的個人資料種類
- 要求對調查結果進行詳細的調查報告，並向高級管理層和相關單位報告。

2. 聯絡相關人士採取遏止措施

- 備存一份有關向相關人士報告，尋求建議和協助的聯繫清單：
 - 執法部門（例如：警方）
 - 相關規管機構（例如：個人資料私隱專員公署）
 - 互聯網供應商
 - 科技專家
- 建立遏止措施清單:
 - 如資料外洩是系統故障造成，應停止有關系統的操作
 - 更改用戶密碼及系統配置，以控制查閱及使用資料
 - 考慮是否需要尋求技術協助，以修補系統上的漏洞及 / 或阻止黑客入侵
 - 停止或更改涉嫌作出或導致資料外洩的人士的查閱權
 - 如犯罪活動已發生或相當可能發生，應通知有關執法部門
 - 保留資料外洩的證據以協助調查
 - 指示資料處理者立即採取補救措施及將進度告知資料使用者（如適用）

3. 評估事件可造成的損害

- 建立風險評估以判斷資料當事人可能蒙受的傷害程度（參見第50頁的評估範本）

4. 考慮作出資料外洩通報

- 當可辨識資料當事人並能合理地估計實在的傷害風險，可考慮通知資料當事人及相關人士
- 資料外洩通報包含的資料
 - 事件的概況
 - 外洩日期和時間，及持續時間
 - 發現事故的日期及時間
 - 外洩的源頭
 - 表列所涉及的個人資料類別
 - 對外洩事件導致的傷害的風險評估
 - 為防止個人資料進一步洩漏而採取或將會採取的措施
 - 被指派向受影響資料當事人提供進一步資料及協助的聯絡人資料
 - 資料當事人可如何保障自己免受外洩事故不利影響及自己的身份不被盜用或假冒的資料及指引
 - 執法部門、私隱專員及其他有關人士是否獲通知
- 提供有關如何向私隱專員通報資料外洩事故的資料（包括資料外洩事故通報表格）



資料外洩風險評估(範本)

ABC 公司	
分部 / 部門	
資料外洩日期	
資料外洩簡述	
<p>敏感度 (視乎洩露的個人資料的類別) :</p> <p>1 2 3 4 5</p> <p>外洩後果的嚴重程度 (視乎涉及個人資料的數量) :</p> <p>1 2 3 4 5</p> <p>遏止措施的有效程度 (視乎資料外洩情況) :</p> <p>1 2 3 4 5</p> <p>身份被盜用或假冒的可能:</p> <p>1 2 3 4 5</p> <p>外洩資料是否有進行足夠的加密、匿名程度可保障而令其不能查閱 (例如查閱時是否需要用密碼) :</p> <p><input type="radio"/> 是 <input type="radio"/> 否 <input type="radio"/> 不確定</p> <p>資料外洩是否持續? 外洩資料會否進一步曝光?</p> <p><input type="radio"/> 是 <input type="radio"/> 否 <input type="radio"/> 不確定</p> <p>有關事故是否獨立事件?</p> <p><input type="radio"/> 是 <input type="radio"/> 否 <input type="radio"/> 不確定</p> <p>如屬於實物遺失, 相關個人資料有機會被查閱或複印前, 是否已尋回資料?</p> <p><input type="radio"/> 是 <input type="radio"/> 否 <input type="radio"/> 不確定</p> <p>有關事故發生後, 是否已採取緩和 / 補救措施?</p> <p><input type="radio"/> 是 <input type="radio"/> 否</p> <p>你如何估計資料當時人可避免或減低可能蒙受傷害的能力?</p> <p>1 2 3 4 5</p> <p>你如何估計資料當時人對個人資料私隱的合理期望?</p> <p>1 2 3 4 5</p>	
由部門協調主任填寫	
姓名	職位
簽署	日期

資料外洩事故－資料表格(範本)

ABC 公司	
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)
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)
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、香港身份證號碼、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？	<input type="radio"/> 是 <input type="radio"/> 否
(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？	<input type="radio"/> 是 <input type="radio"/> 否
如是，請提供通報日期及通報的內容。	

(III) 已採取 / 將會採取的遏止外洩事故行動	
已採取的遏止外洩事故行動的簡述	
請評估上述行動的成效	
將會採取的遏止外洩事故行動的簡述	
IV) 事件可造成的損害	
請評估事故對資料當事人可能造成的損害 (參見第50頁的資料外洩風險評估範本)	資料當時人可能蒙受的傷害程度 (參見第50頁的評估範本)
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)	
擬定改善措施及實施日期	
檢討上述改善措施成效的日期	

由部門協調主任填寫		由保障資料主任審閱	
簽署		簽署	
姓名		姓名	
職位		職位	
日期		日期	

檢視資料處理者的清單 (樣本範本)

ABC 公司		
甲部：背景資料		
部門		
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：檢視企業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企業有權審核及視察資料處理者如何處理及儲存個人資料？	<input type="radio"/> 是 <input type="radio"/> 否 (請說明)	
(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？	<input type="radio"/> 是 <input type="radio"/> 否 (請說明)	
(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？	<input type="radio"/> 是 <input type="radio"/> 否 (請說明)	
(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？	<input type="radio"/> 是 <input type="radio"/> 否 (請說明)	
(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？	<input type="radio"/> 是 <input type="radio"/> 否 (請說明)	
(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《私隱條例》的規定？	<input type="radio"/> 是 (請列明有關保安措施) <input type="radio"/> 否 (請說明)	

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
(7) 與資料處理者簽訂的合約中有否述明違反合約的後果？	<input type="radio"/> 是 <input type="radio"/> 否 (請說明)	
(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。	<input type="radio"/> 是 (請詳細說明) <input type="radio"/> 否 (請說明)	
(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。	(請詳細說明)	
(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。	<input type="radio"/> 是 (請說明要求) <input type="radio"/> 否 (請說明)	
(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。	<input type="radio"/> 是 (請詳述有關情況及其改善措施) <input type="radio"/> 否 (請說明)	
(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。	<input type="radio"/> 是 (請附上資料外洩事故表格副本) <input type="radio"/> 否 (請說明)	

由部門協調主任填寫		由保障資料主任審閱	
簽署		簽署	
姓名		姓名	
職位		職位	
日期		日期	

私隱影響評估問卷 (樣本範本)

ABC 公司	
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。	<input type="radio"/> 是 — 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 <input type="radio"/> 否 (請說明)
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。	<input type="radio"/> 是 — 請具體說明轉移的目的地及轉移的目的 <input type="radio"/> 否

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
<p>保障資料第 1 原則 — 收集個人資料的目的及方式</p> <p>➤ 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。</p> <p>➤ 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。</p> <p>➤ 收集的資料是必須，但不超乎適度。</p>	<p>是否會告知資料當事人收集其個人資料的目的？</p>	<p><input type="radio"/> 是</p> <p><input type="radio"/> 否（請說明理由）</p>
	<p>是否只收集最少的個人資料（即不會收集超乎適度的資料）？</p> <p>請說明收集敏感個人資料的理由（包括但不限於）：</p> <ul style="list-style-type: none"> • 身份證號碼及其他身份代號（如護照號碼） • 生物特徵資料（如指紋） 	<p><input type="radio"/> 是</p> <p><input type="radio"/> 否（收集敏感個人資料的理由）</p>
	<p>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。</p>	<p><input type="radio"/> 是</p> <p><input type="radio"/> 否（請說明理由）</p>
	<p>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。</p>	<p><input type="radio"/> 是（請述明有關情況）</p> <p><input type="radio"/> 否（請說明理由）</p>
	<p>是否會將資料當事人的個人資料轉移或披露予第三者？</p>	<p><input type="radio"/> 是</p> <p><input type="radio"/> 否</p>
	<p>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。</p>	<p><input type="radio"/> 是</p> <p><input type="radio"/> 否（請說明理由）</p>
		<p><input type="radio"/> 不適用（有關個人資料不會披露予第三者）</p>

<p>保障資料第 2 原則 — 個人資料的準確性及保留期間</p> <p>▶ 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。</p>	<p>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。</p> <p>請詳述個人資料會被保留多久？</p> <p>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。</p>	<p><input type="radio"/> 是（請闡述）</p> <p><input type="radio"/> 否（請說明理由）</p> <p>保留期間： _____</p> <p><input type="radio"/> 是（請詳述有關措施）</p> <p><input type="radio"/> 否（請說明理由）</p>
<p>保障資料第 3 原則 — 個人資料的使用</p> <p>▶ 除非得到資料當事人自願給予的明示同意，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。</p>	<p>個人資料是否只會用於收集個人資料聲明中所述之目的或直接有關的目的？如「否」，請說明理由。</p>	<p><input type="radio"/> 是</p> <p><input type="radio"/> 否（請說明理由）</p>
	<p>若個人資料會用於新目的，有否事先取得資料當事人的自願給予的明示同意？如「否」，請說明理由。</p>	<p><input type="radio"/> 是</p> <p><input type="radio"/> 否（請說明理由）</p> <p><input type="radio"/> 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）</p>
	<p>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。</p>	<p><input type="radio"/> 是（請闡述）</p> <p><input type="radio"/> 否（請說明理由）</p> <p><input type="radio"/> 不適用（有關個人資料不會披露予第三者）</p>
	<p>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。</p>	<p><input type="radio"/> 是</p> <p><input type="radio"/> 否（請說明理由）</p> <p><input type="radio"/> 不適用（有關個人資料不會披露予第三者）</p>

<p>保障資料第 4 原則 — 個人資料的保安</p> <p>► 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。</p>	<p>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。</p>	<p><input type="radio"/> 是（請闡述）</p> <p><input type="radio"/> 否（請說明理由）</p>
	<p>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。</p>	<p><input type="radio"/> 是（請闡述）</p> <p><input type="radio"/> 否（請說明理由）</p> <p><input type="radio"/> 不適用（有關個人資料不會披露予第三者）</p>
	<p>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。</p>	<p><input type="radio"/> 是</p> <p><input type="radio"/> 否（請說明理由）</p> <p><input type="radio"/> 不適用（有關個人資料不會披露予第三者）</p>
<p>保障資料第 5 原則 — 資訊的透明度</p> <p>► 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。</p>	<p>現有的私隱政策是否仍然適用？如「否」，請說明哪部分需要作出更新。</p>	<p><input type="radio"/> 是（請闡述）</p> <p><input type="radio"/> 否（請說明理由）</p>
	<p>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]</p>	<p><input type="radio"/> 是</p> <p><input type="radio"/> 否</p> <p><input type="radio"/> 毋需更新私隱政策</p>

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。

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。	<input type="radio"/> 是 <input type="radio"/> 否（請說明理由）
	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。	<input type="radio"/> 是 <input type="radio"/> 否（請說明理由）

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企業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		由保障資料主任審閱	
簽署		簽署	
姓名		姓名	
職位		職位	
日期		日期	



直接促銷與你的業務



真與
接待
你的
促銷
營業
務

直接促銷與你的業務

甚麼是「直接促銷」?

《私隱條例》並非規管直接促銷活動。根據《私隱條例》，「直接促銷」指透過直接促銷方法——

- (a) 要約提供貨品、設施或服務，或為該等貨品、設施或服務可予提供而進行廣告宣傳；或
- (b) 為慈善、文化、公益、康體、政治或其他目的索求捐贈或貢獻

你打算將客戶的個人資料用於本身企業的直接促銷（直銷）活動嗎？

若有此打算，那麼你將個人資料用於直銷前，**必須**採取以下措施：

1. 告知客戶你有意使用他的個人資料作直銷，除非得到他的同意，否則不應使用其個人資料；
2. 向客戶提供訂明資訊，述明將使用其個人資料作哪些促銷用途，包括將使用哪類別的個人資料，及將個人資料用於哪類別的促銷目標；
3. 向客戶提供免費回應途徑，讓他可利用作為表達其同意資料被用作直銷用途；及
4. 為協助客戶作出知情的決定，你提供相關的訂明資訊必須簡單易明，如屬書面資訊，則亦須易於閱讀。

此外，如果你是首次將客戶的個人資料用於直銷，則**必須**：

- 告知該客戶他是有權拒絕相關的直銷活動；及
- 在客戶表明拒絕後，停止使用有關個人資料作直銷，亦不能收取該名客戶任何費用。



你只可在收到客戶的同意後，方可將其個人資料用於直銷。

你亦須隨時按客戶的要求，停止在直銷中使用其個人資料，亦不能收取該名客戶任何費用。

另請參閱第65至66頁使用個人資料作直銷清單。

怎樣才算是有效的同意？

「同意」廣義地包括「表示不反對該項使用或提供」。要符合表示不反對的涵意：

- 有關個人必須已**明確地表示**他不反對使用及／或提供其個人資料予另一人作直接促銷；
- 緘默**不構成**同意；
- 如果有關個人以**口頭方式**表示同意，你須在收到該口頭同意起計的**14日內**，向該名人士發出**書面通知**，確認他同意使用哪種個人資料及用於哪種促銷目標。

你打算將客戶的個人資料提供予第三者作直銷用途嗎？

若你亦有此打算，則除了依循前述的措施外，還**必須**：

- **告知**客戶資料以下兩項與該等資料用途有關的資訊：
 - 該個人資料是否用以**圖利**；及
 - 該個人資料擬提供予**甚麼類別的人士**；
- 以**書面方式**通知及回覆客戶；
- 收到客戶的**書面同意**，否則不得將其個人資料提供予第三者。

無論客戶曾否在較早前同意你將其個人資料提供予第三者，他仍可以在任何時候，要求你：

- 停止將其個人資料提供予第三者作直銷用途；及
- 通知獲得該個人資料的第三者，停止在直銷中使用該資料。

當你收到客戶的上述指示後，必須依從，並且不得向其收取任何費用。而你向第三者發出的相關通知必須為書面通知。該第三者收到你的通知後，必須按照該通知，停止在直銷中使用相關的個人資料。

實用資料：



《直接促銷新指引》

與直接促銷相關的清單和樣本 使用個人資料作直接促銷清單



- 在收集客戶的個人資料之時或之前，告知他你的企業擬使用其個人資料作直銷之用

- 通知內容包含：**

- 你擬在直接促銷中使用他的個人資料；
 - 除非你收到他對擬進行的使用的同意，否則不得如此使用該資料；
 - 擬使用的個人資料的種類；
 - 該資料擬就甚麼類別的促銷標的而使用；及
 - 提供一個回應途徑，讓他可在無需向你繳費的情況下，通過該途徑傳達他對上述的擬進行的使用的同意
- 上述資訊須以易於理解和閱讀的方式呈示



- 已取得客戶的同意將其個人資料用於直銷：

- 以書面同意方式（可參考第 67 至 68 頁的範本）
- 以口頭同意方式
 - 在收到該口頭同意後 14 日內須向他發出書面確認，當中應包含下述資訊：
 - 收到該項同意的日期
 - 有關許可種類個人資料
 - 有關許可類別促銷標的
 - 你的聯絡資料（以便他可以就該確認表示異議）
- 確認客戶的聯絡方式（例如發送短訊的電話號碼、發送文字訊息的通訊或電郵地址），以便發送書面確認
- 保存客戶給予同意的記錄（不論書面形式或錄音）及發出書面確認的記錄



在首次使用客戶的個人資料作直銷時，告知他有權要求你的企業停止這樣使用他的個人資料：

- 以電郵進行促銷
 - 指出這項拒絕服務的權利，並向他提供你的電子連結地址，讓他行使這項權利
- 以郵遞或傳真進行促銷
 - 提供一個可加上「✓」號的空格，並附上回郵地址，以便客戶行使其拒絕服務的權利
- 以電話進行促銷
 - 清楚向客戶表示：「如果你不希望再收到我們的促銷電話，請告訴我，我們不會再致電給你」（或類似語句），讓他知道有權拒絕服務
- 以短訊進行促銷
 - 提供收取拒絕服務要求的電話熱線或請客戶向該電話號碼以短訊回覆



依從客戶的拒絕服務要求：

備存一份「拒絕服務名單」—所有已表示不希望再收到任何直銷活動的客戶的名單：

- 以網上電腦網絡保存名單：
 - 個別促銷職員在每次接獲新的拒絕服務要求時會將有關要求即時加進名單內
- 如不是利用電腦網絡發放名單：
 - 定期將最新的名單分派促銷職員，每星期不少於一次
- 若由你不同的分行保存名單：
 - 每一間分行應備存本身的拒絕服務名單
 - 總公司向所有分行收集拒絕服務的資料統籌更新一份綜合的拒絕服務名單
 - 總公司持續地把已更新的資料通知分行
- 制定機構內部查閱及更新拒絕服務名單的正規程序，讓職員有所依從

保留拒絕服務名單及同意記錄：

- 評估是否需要刪除已提出拒絕服務要求的客戶的所有或部分個人資料，並相應地刪除不必要的個人資料
- 定期檢討所持有的個人資料，查看是否有需要保留及定期進行所需的資料刪除工作

樣本
1通知客戶有關使用其個人資料作直接促銷並
取得其選擇性同意

1. 我們擬使用你的個人資料作直接促銷；
2. 除非我們已取得你的同意，否則我們並不可以如此使用你的個人資料；
3. 我們將會使用下述所指個人資料促銷我們的服務：
 - 你的姓名
 - 你的住址
 - 你的流動電話號碼
 - 你的住宅電話號碼
 - 你的電郵地址

請在空格加上「✓」號以表示你同意。

4. 你的個人資料會用於促銷我們下述的服務：
 - 流動電話
 - 互聯網網絡

請在空格加上「✓」號以表示你同意。

客戶簽署

姓名：XXXXXX

日期：

樣本
2

一般性不反對的例子

我們擬使用你的姓名、電話號碼及地址以促銷信用卡及保險產品／服務，但我們在未得到你的同意之前不能如此使用你的個人資料。

請在本文最後部份表示你同意如此使用你的個人資料。如你不同意，請在以下空格加上「✓」號，然後簽署。

本人（姓名如下）反對使用個人資料於擬作出的直接促銷。

客戶簽署

姓名：XXXXXX

日期：



其他資料



料
料
資
資
他
他
其
其

人力資源管理— 該做與不該做的事

企業需要使用個人資料以進行人力資源管理，期間必須遵守《私隱條例》。作為僱主，你有責任保障求職者、你的現職及前僱員的個人資料。



以下是一些重點留意事項：

	應做的事項	不應做的事項
招聘	<ul style="list-style-type: none"> ▶ 招聘廣告須載有聲明，告知求職者收集個人資料的目的，並提供企業的聯絡資料。 ▶ 如與職位所須具備的條件直接相關，你可收集入選求職者在相關健康狀況方面的個人資料。 ▶ 僱主可保留落選者的資料不超過兩年，由求職者落選的日期起計。 	<ul style="list-style-type: none"> ▶ 你或你所聘用的職業介紹所不應在沒有提供可識別其身份的招聘廣告中，直接要求求職者提供個人資料。 ▶ 在招聘過程中不應收集求職者的身份證副本，直至求職者已接受聘任。

	應做的事項	不應做的事項
現職僱員	<ul style="list-style-type: none"> ▶ 在僱員收集個人資料前，向其提供收集個人資料聲明。 ▶ 若為履行僱傭目的或法律規定，可向僱員及其家屬收集額外的個人資料。 ▶ 在工作表現評估及晉升策劃等過程中收集的僱員資料只應使用於與該等程序直接相關的目的。 	<ul style="list-style-type: none"> ▶ 不應在取得僱員的同意前，向第三者披露僱員的僱傭資料，除非披露該等資料的目的與僱傭直接相關，或是法律規定必須披露該等資料。 ▶ 向第三者轉移或披露僱傭資料時，不應披露超越該第三者所需的資料。
前僱員	<ul style="list-style-type: none"> ▶ 一般而言，保留前僱員的個人資料不應超過七年，由前僱員停止受僱的日期起計。但僱主如有具體理由須保留該資料一段較長時間，或僱主在履行合約上或法律的責任方面需要該資料，則可保留該資料一段較長時間。 ▶ 在僱員離職後，只保留為滿足有關需要而必須保留的前僱員資料。 	<ul style="list-style-type: none"> ▶ 不可在前僱員的離職公開聲明中，披露前僱員的身份證號碼。 ▶ 在取得前僱員的同意前，不應向第三者提供前僱員的工作表現評介，除非你能確認要求提供評介的第三者已取得有關前僱員的同意。

實用資料：



《人力資源管理實務守則》



《身份證號碼及其他身份代號實務守則》



《僱主及人力資源管理者指引》



《人力資源管理：常問問題》



將個人資料移轉至香港以外地方



隨著科技進步，加上機構的業務模式和行事方式改變，個人資料的轉移已變成數據化。跨境/地域數據流動持續不斷，而且規模越來越大。機構（包括中小企）不停地提升效率、方便用戶及引進新產品，當中對全球數據流動有一定的影響。有些機構透過雲端運算技術把數據分散存放在不同的司法管轄區，有些則把處理資料的工序外判給世界各地的承辦商。國際間在人力資源、金融財務、電子商貿、公共安全和醫療研究方面的電子資料轉移，已是當今全球經濟不可分割的部分。

有見及此，規管跨境/地域數據流動比以前更加刻不容緩。世界各經濟體都紛紛採取機制，加強保障跨境數據流動方面的個人資料私隱。

《私隱條例》第33條規定，除在特定情況下，禁止將個人資料轉移到香港以外地方。儘管第33條自制定以來尚未生效，但《私隱條例》的現有規定已經為跨境資料轉移提供保障，以確保在目前的監管體制下，對向香港以外的跨境資料轉移提供相同的保障水平。資料使用者必須：

- i) 發出通知以明確告知資料當事人資料承轉人的類別（包括在香港以外的承轉人）（保障資料第1（3）原則）；
- ii) 在更改已收集的個人資料用途時，獲得資料當事人的訂明同意（保障資料第3原則）；
- iii) 採用合約或其他方式，防止任何轉移到資料處理者的個人資料（無論是在香港之內或之外）未經授權或意外地被查閱、處理、刪除、喪失或使用（保障資料第4（2）原則）；
及
- iv) 採用合約或其他方式，防止任何轉移到資料處理者的個人資料（無論是在香港之內或之外）的保留期間超過所需（保障資料第2（3）原則）。

為保障個人資料私隱而不阻礙商業發展及經濟增長，私隱公署在2014年發出《保障個人資料：跨境資料轉移指引》，為有需要因商業運作而在香港以外地區轉移個人資料的機構提供實用指引。該指引協助機構為第33條的實施作好準備，加強跨境資料轉移的私隱保障，也讓機構更清楚他們在第33條下須承擔的法律責任。私隱公署特別擬備了一份建議範本條文，協助機構制定與海外資料接收者訂立的跨境資料轉移協議。即使第33條仍未生效，私隱公署亦鼓勵機構採取指引中的建議，以履行其企業管治的責任。

實用資料：



《保障個人資料：
跨境資料轉移指引》



《內地民商事務所涉 個人信息及網絡安全 主要法規簡介》



現時內地網絡市場龐大，企業要從中獲得最大效益，不可忽視內地網絡監管政策及相關法規限制。

目前中國內地針對個人信息保護方面的規管分散於多部法律、行政法規、部門規章和指引等規範性文件中，有關監管框架也在不斷擴張。此外，中國內地亦開始著重將隱私權及個人信息權視為獨立的人格權，並賦予民事保障。隨著各種法規的出台，社會大眾的隱私和個人信息受到更廣泛及更大程度的保障。然而，由於中國內地關乎個人信息保護的法規眾多，期待到這個新興市場擴展業務的企業須面對符規方面的挑戰。

為此，私隱公署出版了《內地民商事務所涉個人信息及網絡安全主要法規簡介》（《簡介》），介紹內地針對個人信息保護方面的相關法規，旨在成為商界在拓展內地市場的錦囊，幫助他們了解內地相關法規，從而更順暢地走入大灣區拓展網絡市場，擴大商業效益。

《簡介》除了整合和介紹目前相關的內地法規及案例，亦列出並比較香港與內地的私隱法例，例如內地《網絡安全法》指出在中國境內運營中收集和產生的個人信息和重要數據應當在境內存儲。此外，《數據安全管理辦法》（徵求意見稿）亦規定收集個人敏感信息須向网信部門備案並委任數據安全責任人。

請瀏覽私隱公署網頁下載《簡介》。



《通用數據保障條例》與你

《通用數據保障條例》是甚麼？

《通用數據保障條例》於 2018 年 5 月 25 日生效，取代了歐盟指令中訂明的資料保障規例；該指令在九十年代中訂立香港《個人資料（私隱）條例》時曾被參考。《通用數據保障條例》強調資料控制者需具透明度、安全性和問責原則。

《通用數據保障條例》是否適用於你的企業？

《通用數據保障條例》亦適用於歐盟以外的企業，包括向身處歐盟人士提供貨品或服務或監察其行為的企業。

基於這域外應用，符合上述範圍的香港企業可能希望了解更多有關《通用數據保障條例》的資訊。

想進一步了解《通用數據保障條例》？

為了提高香港企業認識《通用數據保障條例》對它們可能帶來的影響，私隱公署刊發了**歐洲聯盟《通用數據保障條例》2016（於 2018 年 5 月 25 日生效）**小冊子，具體說明這法例的主要特點以及與香港《個人資料（私隱）條例》的差異。

有關《通用數據保障條例》的最新更新及相關的教育材料和活動，可到 PCPD.org.hk 瀏覽有關專頁：



建立問責制、加強企業承諾 — 私隱管理系統

在規模較小的企業中推行私隱管理系統，可行嗎？

除達至最低合規水平外，更進一步是建立你的私隱管理系統 — 企業應將個人資料保障納入企業管治責任，成為業務中不可或缺的一環。這不但可加強客戶對你的信任，更可從而提升商譽及競爭優勢。



私隱管理系統包括以下三個組件：



實施私隱管理系統的好處

- 有效管理所收集的個人資料；
- 有助遵從《私隱條例》的規定；
- 減低事故發生的風險（例如個人資料外洩）；
- 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；及
- 一旦有事故發生，確保企業亦有完善的機制處理，將事故造成的損害減至最低。

開始建立你的私隱管理系統！

請參閱私隱公署製作的《私隱管理系統 — 最佳行事方式指引》，參考具體例子及實用建議，以制定框架建立全面的私隱管理系統。



尊重、互惠和公平 — 數據道德管治

在數據推動的經濟下，中小企（包括科技初創企業）越來越多視顧客的個人資料作為經營及推展其業務的資產而使用有關資料。資訊通訊科技的急速發展，特別是高階數據處理活動（包括大數據分析和人工智能），在帶來商機的同時，亦為私隱和數據保障帶來了挑戰。



無可置疑，個人資料是屬於資料當事人的。從個人資料獲取利益的中小企應摒棄在營運時只達致最低監管要求的想法。相反，他們應恪守更高的道德標準，在符合相關法例和監管要求的同時，亦符合持份者的期望。因此，數據道德可填補法例要求和持份者期望兩者之間的落差。

為了保障顧客個人資料私隱及增強顧客信心，中小企在處理個人資料時，應遵從數據道德的三大核心價值：

尊重

- 機構應顧及與數據相關及 / 或因使用數據而受影響的人士的期望
- 任何人士可隨時提出查詢和取得有關闡釋資料，若有需要，他們可就高階數據處理活動對其影響提出覆檢

互惠

- 如高階數據處理活動對個別人士有潛在影響，該等活動所帶來的好處和潛在風險，須予以界定、識別及評估
- 採取措施以減低所有識別的風險，平衡各方的利益

公平

- 應定期審查在決策時使用的數據運算法、模式和數據集的準確性和相關性，以減少錯誤、不確定情況及歧視

數據道德影響評估

中小企決定從事高階數據處理活動前，可藉解答以下問題，進行數據道德影響評估，以了解其數據道德責任，並找出數據處理活動對持份者權益的影響。

活動目的

- 此數據活動的業務需求 / 目的為何？
- 誰人對此數據活動擁有最終決策權？誰人須為各階段的數據活動負責？
- 如何確保充份履行適用於數據收集、分析、使用和轉移的法律及其他責任？

充份了解數據、其使用和涉及的各方

- 數據是否可識別個別人士身份？是否有可能從匿名數據重組識別個別人士身份？
- 有關數據（例如種族、族裔、性傾向、生理或心理健康狀況）或預期使用的目的是否敏感？
- 就該數據活動的目的而言，數據是否足夠準確？

對各方，特別是個人的影響

- 對個人、群體及社會有哪些益處？會帶來甚麼風險？
- 會實施哪些技術和程序保護措施（例如加密和將數據去除身份識別），以預防和減低風險？

利益及已減低的風險之間是否已取得適當平衡，並足以支持進行數據處理活動

- 是否已恰當地顧及個人的利益、權利和期望？
- 數據活動產生的風險與利益是否合符比例？是否已在切實可行範圍內盡量減低有關風險？

實用資料：



《中小企的數據倫理道德》

私隱專員發表了道德問責框架，該框架透過兩個評估模式列舉指導性問題，以協助企業完成評估工作。

實用資料：

有關中國香港的道德問責框架的報告
[只有英文版]



數據管理問責、數據影響評估和監督模式
[只有英文版]



私隱公署中小企諮詢服務

我們全方位支援你!

為加強與中小企的溝通與合作，私隱公署推出專為中小企而設的諮詢熱線和電郵，以便私隱公署就有關保障個人資料事宜向他們提供意見。

中小企的專屬諮詢熱線號碼為 2110 1155，在私隱公署的辦公時間內接聽（星期一至五上午 8 時 45 分至下午 12 時 45 分及下午 1 時 50 分至下午 5 時 40 分，公眾假期除外）。中小型企業亦可透過電郵至 sme@pcpd.org.hk 向私隱公署提出你的查詢，每個查詢均由私隱公署專責團隊回覆。



☎ 2110 1155

✉ sme@pcpd.org.hk

附錄

6 保障資料原則

Data Protection Principles

PCPD.org.hk

1

收集目的及方式 Collection Purpose & Means



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。

須以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給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/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.

2

準確性、儲存及保留 Accuracy & Retention



資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達成原來目的的实际所需。

Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used.

3

使用 Use



個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

Personal data is used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject.

4

保安措施 Security



資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5

透明度 Openness



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。

A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

6

查閱及更正 Data Access & Correction



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。

A data subject must be given access to his personal data and to make corrections where the data is inaccurate.

立即參加!

保障資料主任聯會

(會籍申請)

成為會員，你可以：

- 透過經驗分享和出席私隱公署舉辦的培訓活動，增加對資料私隱合規的認識和促進企業合規實踐
- 報讀私隱公署專業研習班，報名費享有八折優惠
- 透過私隱公署出版的電子通訊接收資料私隱的最新發展資訊

成為保障資料主任聯會會員後，私隱公署會把貴公司名稱刊登在私隱公署網頁內「保障資料主任聯會會員列表」

年費：港幣 \$150 (只限中小企會員)

查詢：d poc@pcpd.org.hk



https://www.pcpd.org.hk/misc/dpoc/files/appform_19_20_new_member_sme.pdf

Content



Foreword	89
Key PDPO Definitions	91
What Does the PDPO Mean for Your Business?	95
Ten Practical Steps for SMEs	103
Useful Tools and Checklists	131
Direct Marketing and Your Business	149
Do's and Don'ts - Human Resource Management	157
Transfer of Personal Data Outside Hong Kong	159
Introduction to the Regulations in the Mainland of China Concerning Personal Information and Cybersecurity Involved in Civil and Commercial Affairs	161
GDPR and You	163
Create Accountability, Strengthen Commitment - Privacy Management Programme	164
Respectful, Beneficial and Fair - Ethical Data Governance	167
PCPD Enquiry Services for SMEs	169
Appendix	170

Foreword



Currently there are about 340,000¹ small and medium enterprises (SMEs) in Hong Kong. They account for over 98% of local enterprises and employ 45 % of workforce of the private sector, providing about 1.3 million job opportunities. The SME sector makes enormous contributions to Hong Kong's economy.

SMEs often collect and handle various kinds of personal data of customers and employees in their business operations. Personal data is regarded as an asset nowadays. There are ever-increasing expectations among customers and members of the public with regard to protection of their personal data. In order to win customers' trust, enhance corporate reputation and competitive advantage, SMEs must diligently safeguard personal data privacy, comply with the requirements of the Personal Data (Privacy) Ordinance (PDPO) and practise ethical data governance to ensure that personal data are held and managed properly.

While SMEs are flexible in operations, it is sometimes a challenge for them to attach sufficient importance to protection of personal data with their limited resources. Therefore, we hope this publication can raise the awareness of SMEs in protecting and respecting personal data, and provide a structured toolkit assisting them in complying with the provisions of the PDPO and practise data ethics so as to create a workplace and an operating model that uphold the culture of respecting personal data privacy.

¹ Source: https://www.tid.gov.hk/english/smes_industry/smes/smes_content.html

Entitled “SME Personal Data Protection Toolkit”, this publication is designed to facilitate SMEs in developing a compliance strategy that best suits their needs in relation to the requirements of the PDPO. This Toolkit is intended to be a starting point for SMEs in terms of their compliance and governance efforts. It includes checklists that will help determine whether the necessary policies, control measures and procedures are in place to comply with the Data Protection Principles in the PDPO and meet the expectations of consumers.

The PCPD has provided a range of resources to assist SMEs in understanding the PDPO. These resources are available on our website at www.pcpd.org.hk for viewing and download.

Stephen Kai-yi WONG

Barrister
Privacy Commissioner for Personal Data, Hong Kong
June, 2020



Key PDPO Definitions

Personal Data

Any data 1) relating to a living person, 2) can be used to identify that person, and 3) in a form in which access to or processing of the data is practicable.

Data Protection Principles (DPPs)

Principles set out in Schedule 1 to the PDPO, on personal data collection, accuracy and retention, data use, data security, openness, as well as data access and correction.

Data Subject

A living individual who is the subject of the personal data concerned.

Data User

A person or organisation who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the personal data in or from Hong Kong. The Data User is liable as the principal for the wrongful act of its authorised data processor.

Use

Includes disclosure or transfer of personal data.

Processing

Includes amending, augmenting, deleting or rearranging the personal data.

Data Processor

A person or organisation who 1) processes personal data on behalf of another person; and b) does not process the personal data for any of the person's own purposes.



To Start with...



**To start
with...**

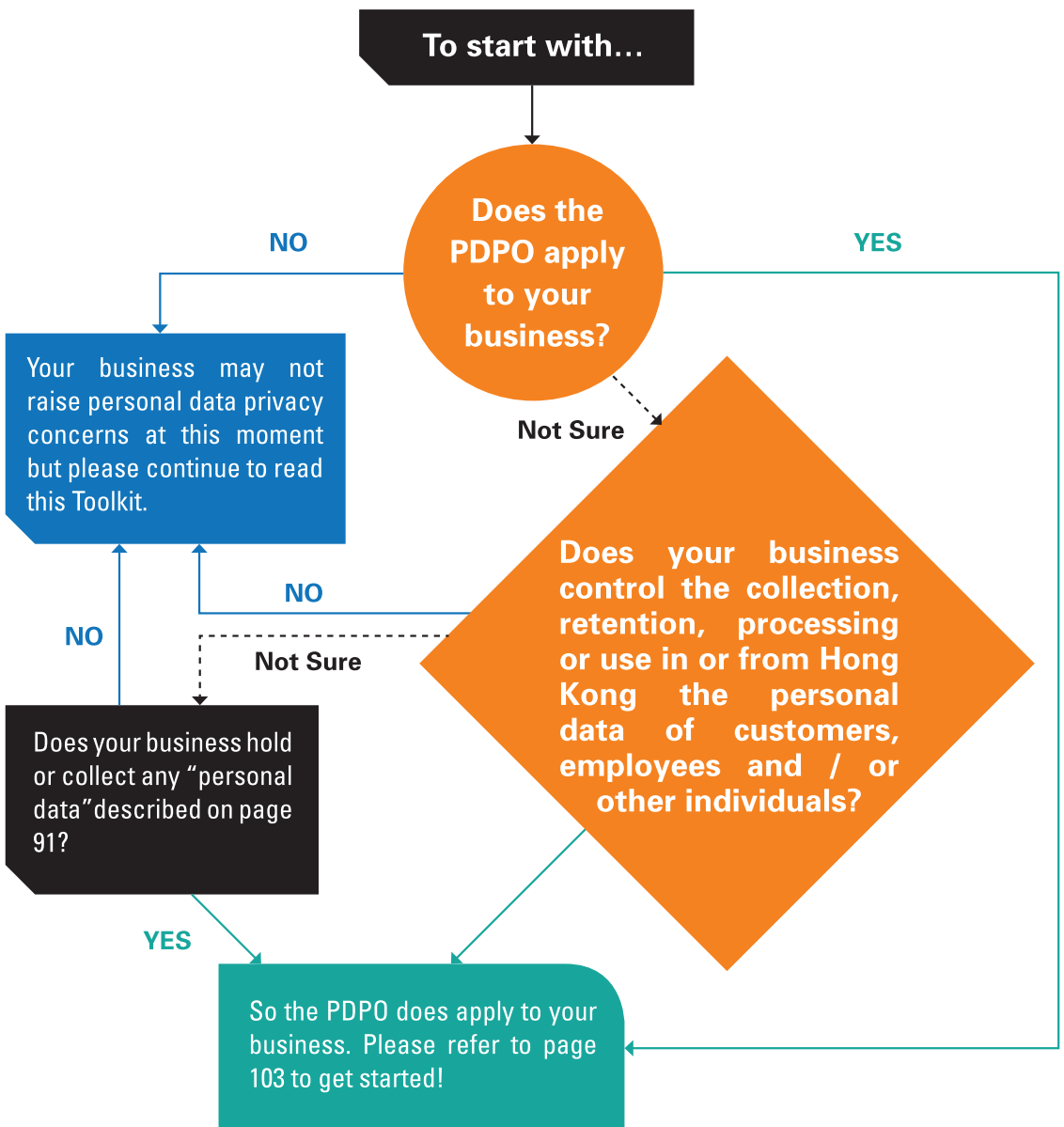
What Does the PDPO Mean for Your Business?

It is a legal requirement to comply with the provisions of the PDPO in respect of collecting, retaining, processing and using personal data. The PDPO also provides a good foundation for businesses to achieve above and beyond legal compliance in handling data in an ethical manner.

Businesses that handle customers' personal data lawfully and ethically will win trust from customers as well as business partners, which can ultimately add a competitive edge to the businesses.



Personal Data and Your Business



Ten Practical Steps for SMEs



Ten Practical Steps for SMEs

Ten Practical Steps for SMEs



01

Getting to Know the PDPO

Get started with understanding the basics of the PDPO and its DPPs in order to know the legal basis you rely on to justify your handling of personal data. > [page 103](#)

02

Why Do You Collect Those Personal Data?

Before collecting personal data, identify your reason for doing so in order to review and identify risk areas of data handling processes. > [page 108](#)

03

Have You Clearly Notified People of the Collection Purpose?

Clearly tell the individuals why you need their personal data and how you will use it on or before the point you collect it from them. > [page 109](#)

04

Accuracy and Duration of Retention of Personal Data You are Holding

Ensure the personal data you hold is accurate and kept no longer than is needed for the purpose for which it was collected. > [page 111](#)

05

How Do You Use the Personal Data?

Review the data collection purposes, and ensure that explicit consent has been obtained before using it for new purposes. > [page 113](#)

10

Privacy Impact Assessments

Make personal data privacy at the heart of all future projects. > [page 127](#)

09

Engaging a Data Processor

Adopt contractual or other means to impose obligations on data processors under the contract. > [page 125](#)

08

Handling Personal Data Access and Correction Requests

Make sure you have processes in place that allow you to provide and update personal data in response to individuals making the requests. > [page 120](#)

07

Develop a Process for Data Breach Notification

Make sure you have the procedures in place to detect, report and investigate a data breach as a good practice. > [page 118](#)

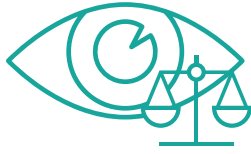
06

Data Security Checking

Ensure that personal data is held securely and against unauthorised or accidental access, processing, erasure, loss or use. > [page 116](#)

Ten Practical Steps for SMEs:

01



Getting to Know the PDPO

The objective of the PDPO is to protect the privacy rights in relation to personal data of living individuals. It is technology-neutral and principle-based, allowing the Privacy Commissioner to strike a balance between embracing technology development and innovation, and protecting and respecting personal data of individuals.

What is “Personal Data”?

Under the PDPO, personal data includes any data 1) relating to a living person, 2) that can be used to identify that person, and 3) in a form in which access to or processing of the data is practicable.

In general, examples of personal data protected by the PDPO include: names, ages, phone numbers, addresses, identity card numbers, photos, income, medical records, employment records, financial records, etc.



Six Data Protection Principles (DPPs)

Any organisation (regardless of the size and nature) that controls the collection, holding, processing or use of the personal data in or from Hong Kong should comply with the requirements under the PDPO, including the six DPPs which represent the core of the PDPO covering the life cycle of a piece of personal data:

DPP



Data Collection Principle: Purpose and Manner

- Personal data must be collected in a lawful and fair way, for a purpose directly related to a function / activity of the data user.
- Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred.
- Data collected should be necessary but not excessive.




DPP



Accuracy & Retention Principle

- Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used.

DPP




Data Use Principle

- Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.



DPP



Data Security Principle

- A data user needs to take reasonably practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

DPP



Openness Principle: information to be generally available

- A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.



DPP



Data Access & Correction Principle

- A data subject must be given access to his/her personal data and allowed to make corrections if it is inaccurate.

These principles are further described in detail in the following sections of this Toolkit.

What is not covered by the PDPO?

The PDPO provides exemptions for practical needs and in various circumstances. Some examples include:

- Exemptions from access requirement for certain employment-related personal data and relevant process; and
- Exemptions from access and use limitation requirements for data which are likely to prejudice security, defence and international relations; crime prevention or detection; assessment or collection of any tax or duty; news activities; health; legal proceeding; due diligence exercise; archiving; handling life-threatening emergency situation, etc. (non-exhaustive).



Offences and Compensation

- Non-compliance with the DPPs does not constitute a criminal offence directly. The Privacy Commissioner may serve an Enforcement Notice to direct the data user to remedy the contravention.
- Contravention of an Enforcement Notice is an offence which could result in a maximum fine of HK\$50,000 and imprisonment for two years.
- An individual who suffers damage, including injured feelings, by reason of a contravention of the PDPO in relation to his personal data privacy may seek compensation from the data user concerned.
- The PDPO also criminalises:
 - misuse or inappropriate use of personal data in direct marketing activities;
 - non-compliance with Data Access Request;
 - unauthorised disclosure of personal data obtained without data user's consent, etc.

MORE INFORMATION:
Visit PCPD.org.hk



02



Why Do You Collect Those Personal Data?

This should be the first question that comes up to your mind when you plan to collect personal data from your clients or other individuals!



Identify the reasons and purposes for collecting personal information before or at the time of collection. This will help you fulfill your obligation for processing personal data under the PDPO.

- Why is the data needed for your business?
- Are the means of collection lawful and fair?
- Is it a must to collect the data or else you are not able to provide the service required or fulfill the operation needs? Are there any alternatives?
- How will the data be used?
- Will you transfer personal data collected to others?

And, at the time you collect the personal data:

- Have you notified the individual of and obtained consent (orally or in writing) for these purposes? (See page 109 about the notification of the collection purpose)

Remember to document the collection purposes. You may start by using the Personal Data Inventory Checklist on page 131 to develop your own data inventory list.

USEFUL TIPS

- *You should only collect the data as necessary and adequate but not excessive for the purpose.*

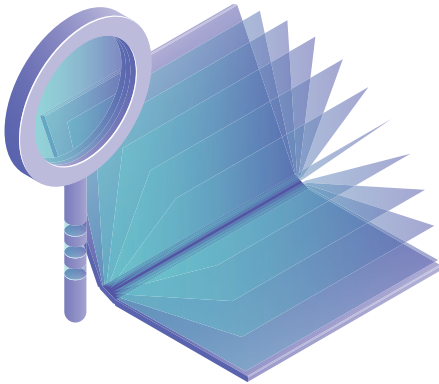
03



Have You Clearly Notified People of the Collection Purpose?

Before and at the time you collect individuals' personal data, have you clearly informed them why you need it and how you will use it?





Your PICS must be easy to read and understand, and given to individuals whenever you collect their personal data, both online and offline.

You can refer to the sample templates of PICS on page 132-133 to build your own ones.

USEFUL TIPS FOR BUILDING AN EFFECTIVE PICS

- *Be specific - the purposes stated in the PICS should not be too vague and too wide in scope so that the individuals can make an informed decision. The class of transferees should also be clearly defined.*
- *Be user-friendly - the layout and presentation (including the font size, spacing, underling, use of headings, etc.) of the PICS should be easy to read by customers with normal eyesight;*
- *Use simple language – and avoid using difficult terms.*

04



Accuracy and Duration of Retention of Personal Data You are Holding

Ensure that you document and review your personal data holdings to ensure the data is accurate and kept no longer than is needed for the purpose for which it was collected.

How long can your organisation hold the personal data?

The PDPO does not stipulate a fixed period of retention of personal data. However, you have to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose for which the data is or is to be used, and erase it when it is no longer required. You may retain the data if there is subsisting purpose (e.g. as required by or permitted under the laws). You should have a personal data retention policy (with review schedule and procedures), as a good practice, that specifies in detail the retention arrangements for personal data you hold.



Start your data inventory check!

Make use of the template on page 131 to map out and review the personal data that your organisation is currently holding and processing.

USEFUL TIPS

- *Have a data retention schedule and conduct regular reviews of personal data to help determine whether data is still required.*
- *Conduct regular review to help identify if specific personal data is still required. Erase the personal data that is no longer required.*
- *Set maximum and minimum retention periods for personal data, taking into account any legal requirements or restrictions.*



05



How Do You Use the Personal Data?

Use, disclose or transfer personal information only for the purposes for which it was collected. Therefore, you always need to refer to the related collection purposes at the time of using the personal data collected. Ensure explicit consent has been obtained before using for new purposes.

TAKE A QUICK CHECK

- At the time of using the personal data collected, always refer to the related collection purposes;
- If there are any new purposes of using the personal data, obtain the individuals' consent before using it;
- Record any new purpose for the use of personal data.



Be Transparent!

Develop policies and practices in relation to personal data, and develop a Privacy Policy Statement (PPS) in order to effectively communicate your data management policies and practices to your customers, staff members and members of the public.

The content of PPS includes:

- A statement of policy to express your overall commitment in protecting the privacy interests of the individuals. (*Example: We are committed to protecting the privacy, confidentiality and security of the personal information we hold by complying with the requirements of the Personal Data (Privacy) Ordinance with respect to the management of personal information.*)
- A statement of practices that includes the kinds of personal data (e.g. contact details, financial details, browser details and IP addresses) held by you and the purposes for which you use the data (e.g. delivery of goods / services, account management, facilitation of website access).



CHECKLIST FOR BUILDING AN EFFECTIVE PPS

- **Do not collect personal data from minors without prior consent from a person with parental responsibility for the individual.**
- **State clearly:**
 - ▶ **whether the website allows access by individuals who do not accept cookies, and what loss of functionality may result from not accepting cookies;**
 - ▶ **how long the personal data will be retained;**
 - ▶ **how to make a deletion request;**
 - ▶ **how sensitive personal data will be used, processed, handled and transferred;**
 - ▶ **whether personal data would or would not be disclosed to other parties with the data subject's express and voluntary consent;**
 - ▶ **how they ensure the security and confidentiality of the personal data collected;**
 - ▶ **what personal data will be transferred to service providers and how the service providers will ensure protection of the personal data collected;**
 - ▶ **if you do not collect or use personal data obtained from or about individuals, you should make this practice known through a PPS to assure the public of your commitments;**
 - ▶ **your policy on handling individuals' requests to access and to correct individuals' personal data held;**
 - ▶ **the contact details (e.g. office and email addresses) of the officer in your organisation who will answer enquiries;**
- **Should be easily understandable and readable; and**
- **Use proper heading and adopt a layered approach in presentation in case the privacy policies and practices is complex and lengthy.**

Regularly review all current PPS to identify any gaps on compliance with the PDPO.

USEFUL INFORMATION:

Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement



06



Data Security Checking

You are responsible for protecting personal data collected from loss or theft, as well as for safeguarding the data from unauthorised access, disclosure or use.

The PDPO does not specify any data security measures that organisations have to adopt. Instead, you have to take all reasonably practicable steps to safeguard personal data. Factors that need to be considered include:

- Sensitivity / confidentiality of the data
- Data volume
- Format of the data
- Type of storage

Regardless of the data format, you have to ensure that personal data is held securely. This can include:

- Physical measures: e.g. locking filing cabinets, restricting access to filing areas in office
- Electronic means: e.g. passwords, encryption, firewall
- Policy control: e.g. limited access on a “need-to-know” basis, staff training, entering contract with vendors
- Destroy / erase personal data in a way that prevents a privacy breach, e.g. shredding paper files, deleting electronic records, etc.

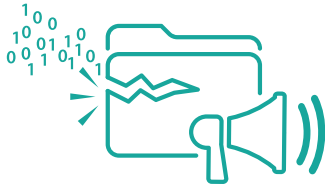


USEFUL TIPS FOR PROTECTING PERSONAL DATA YOU HOLD

- ***Develop and implement in-house security policy to safeguard the personal data;***
- ***Use appropriate security measures to protect personal data in different formats;***
- ***Regularly review security policies and measures to ensure they are up-to-date;***
- ***Ensure staff awareness by providing related training;***
- ***Adopt contractual means to prevent unauthorised access, processing, erasure, loss or use of the data entrusted to vendors.***

What do you need to do if a data breach occurs? Please see the next step.

07

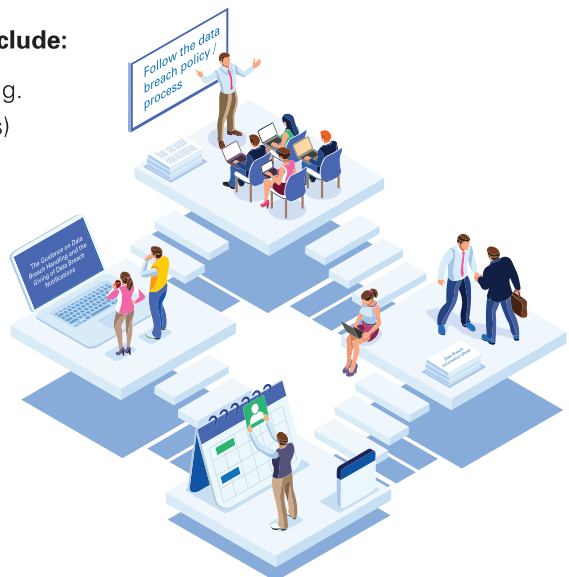


Develop a Process for Data Breach Notification

The cost of data breaches can be devastating to businesses, especially to SMEs. The impact could range from disruption to business operations, loss of business reputation and customers' trust, being held ransom by hackers, etc. Amid the growing rise of cybercrime, the threat of data being lost or stolen cannot be underestimated. Apart from improving your security stance, SMEs should also develop procedures in relation to the handling of data breach incidents so as to eliminate the loss and damage that may be caused.

Common examples of data breaches include:

- Loss of personal data kept in storage (e.g. computers, USB flash drives, paper files)
- Improper handling of personal data (e.g. improper disposal, post or email sent to wrong recipients)
- Unauthorised access to personal data of customers or staff members
- Database containing personal data being hacked by outsiders without authorisation



Be Proactive! Develop a data breach handling policy / procedure

A good data breach handling policy / procedure adopted shows your responsible and accountable attitude in tackling the breach and putting in place a clear action plan to be followed in the incident.

To get started, you can make use of the Data Breach Handling Checklist on pages 134-135 to develop your own data breach handling policy / procedure.

What to do when it happens to you?

Don't panic! Follow the data breach policy / procedure that you have developed and start gathering essential information. Consider informing affected parties and the regulatory authority soonest you can as a good practice.

You may make use of the "Data Breach Information Sheet" on pages 137 - 138 to consolidate the information relating to the breach, take remedial actions promptly and conduct post-incident review.

While it is not a statutory requirement for you to inform the Privacy Commissioner of a data breach incident, 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* issued by the Privacy Commissioner provides practical guidance in this regard.



HOW TO SUBMIT A DATA BREACH NOTIFICATION TO THE PRIVACY COMMISSIONER?

- 1) **Complete a Data Breach Notification Form**
- 2) **Submit the completed form to the PCPD online, by fax, in person or by post**



USEFUL INFORMATION:

Guidance on Data Breach Handling and the Giving of Breach Notifications



08



Handling Personal Data Access and Correction Requests

Under the PDPO, individuals have the right to ask you for a copy of their own personal data you hold about them. This is called the data access request (DAR). It ties in with a further right under the PDPO for an individual to make a correction request to a data user if his personal data was found to be inaccurate.

Right to Request Access

In general, you can inform an individual of his rights to request access to, and correction of, his personal data, as well as the name of job title, and the address of the person to whom any such request may be made, in the "Personal Information Collection Statement (PICS)" which is provided to the individual on or before collection of his personal data. (An example of PICS can be found on page 132-133)

Common examples of DARs include:

- requests by consumers for copies of their service application forms; and
- requests by employees for copies of their performance appraisal reports.



Data Access Request Form

A DAR is usually made on the Data Access Request Form (Form OPS003). Sometimes, a requestor may not use the DAR Form to make the DAR but will simply say in his request that he wishes to obtain his personal data. If the request sets out the scope and details of the requested personal data, you are strongly advised to respond to the request.

A data user may impose a fee for complying with a DAR which should not be excessive.



[Download Data Access Request Form](#)

USEFUL TIPS

- ***A requester is not entitled under a DAR to access data which is not personal data or personal data not belonging to him. Therefore, you should erase any personal data relating to a third party from the copy of the requested data.***

Right to Correction

If an individual has obtained a copy of his personal data held by you by way of a DAR, he can then make a data correction request (DCR).

Under the PDPO, organisations are required to ensure that the personal data they hold is accurate. If you discover that the data being requested for correction is inaccurate (i.e. incorrect, misleading, incomplete or obsolete), you should accede to the DCR without a fee.

“Verifiable matters” and “expression of opinion”

When handling a DCR, organisations should distinguish between the “verifiable matters” and the unverifiable “expression of opinion”:

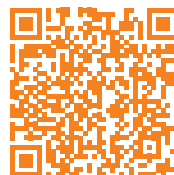
- “Verifiable matters” refer to facts that can be proved with objective reality, record and data for ascertaining their accuracies (e.g. attendance record, school grants etc.).
- “Expression of opinion” includes an assertion of fact which is unverifiable; or in all the circumstances of the case, is not practicable to verify. When it involves a professional judgment, the Privacy Commissioner usually would not intervene any correction request.



USEFUL GUIDANCE NOTES ISSUED BY
THE PRIVACY COMMISSIONER:



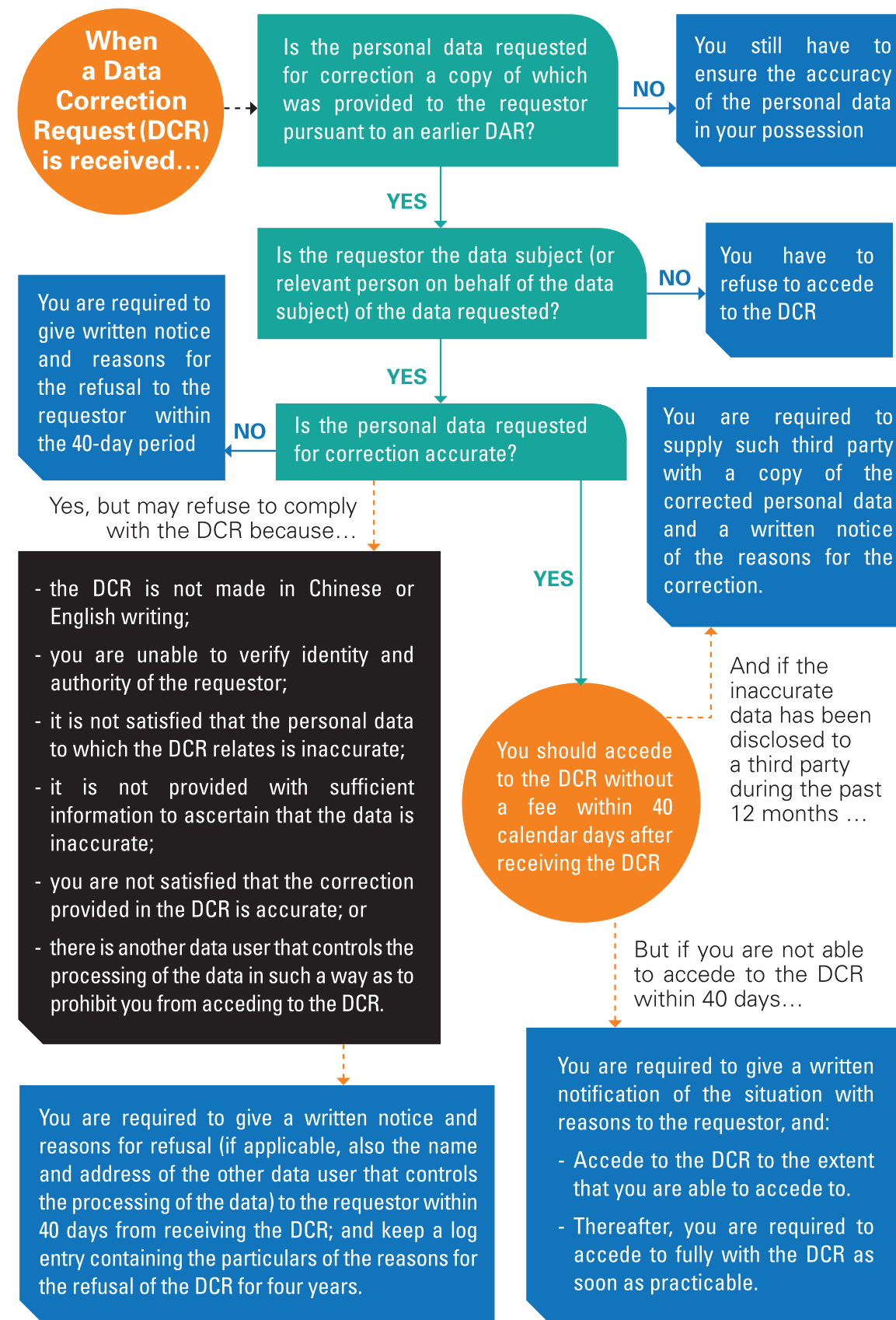
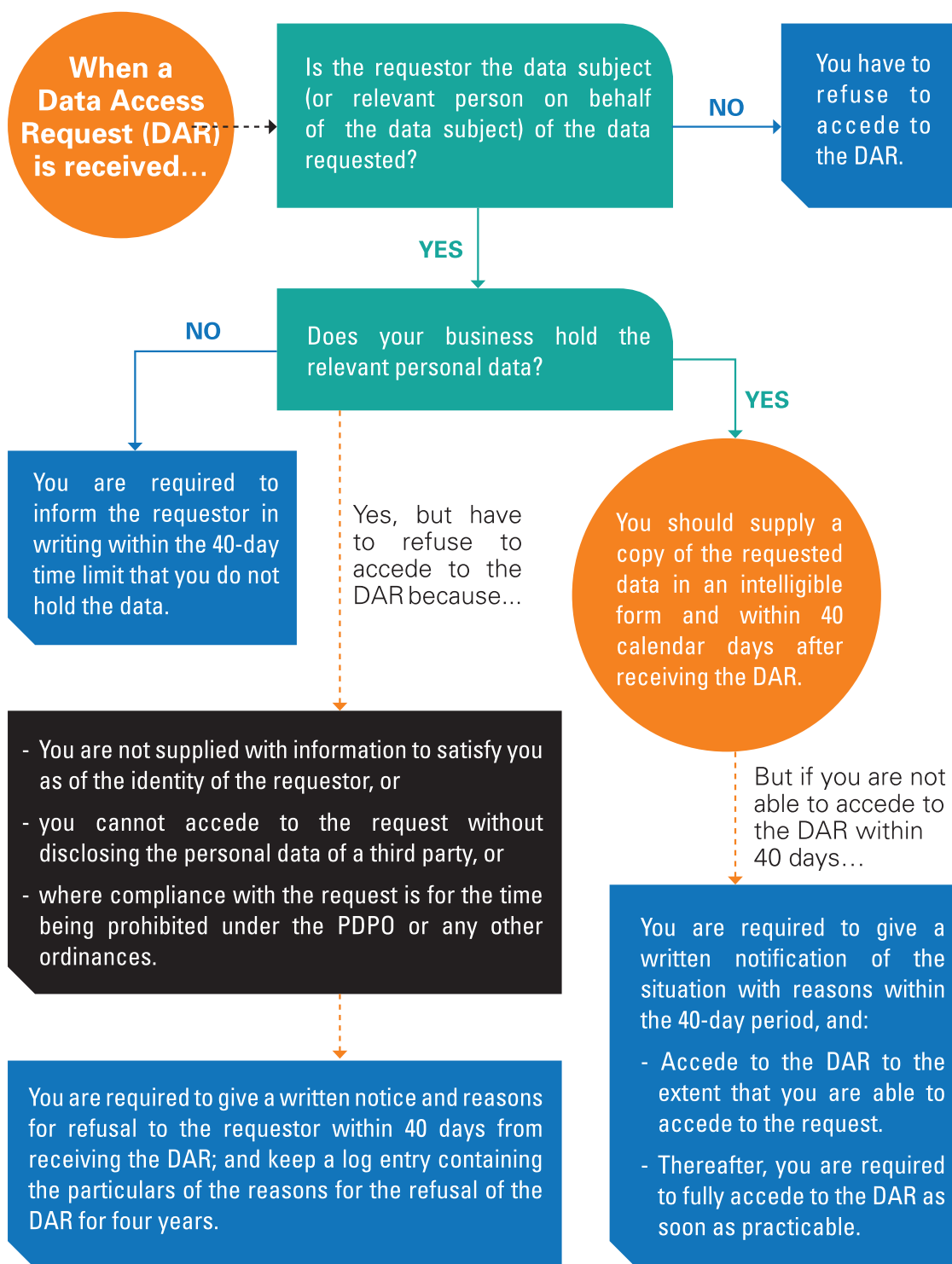
**Proper Handling
of Data Access
Request and
Charging of Data
Access Request Fee
by Data Users**



**Proper Handling
of Data Correction
Request by Data
Users**

Basic Workflow of Data Access and Correction Request Handling

Basic Workflow of Data Access and Correction Request Handling



(For details, please refer to Guidance Notes "Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users" and "Proper Handling of Data Correction Request by Data Users")

09



Engaging a Data Processor

With limited manpower and resources, many SMEs may seek external expertise to manage their personal data processing work. These services may include:

- Web hosting;
- Server hosting;
- Paper shredding;
- Event management. etc.

However, under the PDPO, if your organisation outsources or entrusts personal data processing work to agents / service providers (as data processor), you are responsible for the improper handling of personal data by your agents / service providers.

If your enterprise has actual need to engage a data processor, you should:

- pass only the minimum personal data to the data processor;
- adopt contractual or other means to protect personal data entrusted to the data processor;
and
- conduct annual review to ensure that the management of data processor is adequate and comprehensive.





Conduct review on a regular basis by completing the Data Processor Review Checklist on page 139 now!

10



Privacy Impact Assessments

Always conduct a Privacy Impact Assessment (PIA) before launching a new project, product or services!

It allows organisations to identify potential privacy risks before they arise, and come up with a way to mitigate them.

When to conduct a PIA?

- When there is a material change to the regulatory requirements relating to personal data privacy;
- When there is a material change to the organisation's existing personal data handling process;
- When introducing a new kind of personal data in your organisation;
- When your organisation intends to engage data processors to handle personal data on your behalf.

What are the key components of a PIA?

A PIA generally includes the following key components:

- Data processing cycle analysis;
- Privacy risks analysis;
- Avoiding or mitigating privacy risks; and
- PIA reporting.

It is recommended to consider seeking external professional advice especially when the data user is in a project which may have a significant privacy impact on personal data. You can also refer to page 141-145 for a sample of PIA Questionnaire.



Useful Tools and Checklists



Useful Tools and Checklists

Personal Data Inventory Check (Sample Template)

Company ABC	
Division / Department	
Categories of personal data and data subjects <i>e.g. current employees' data; customers' data; marketing database</i>	
Elements / items of personal data contained in each data category <i>e.g. name, address, telephone number, email address, HKID card no.</i>	
Source / means of collection of the personal data <i>e.g. collected directly from individuals; collected from third parties</i>	
Purpose of collection and use of personal data <i>e.g. HR matters, marketing, providing services, research</i>	
Retention period of personal data <i>e.g. two months? one year?</i>	
Location of data storage <i>e.g. company network drive of Personnel Department; website vendor's data server; inventory room in office</i>	
Disclosure of personal data to any third parties (Yes / No)	
Purpose of disclosing the personal data and whether the disclosure complies with the PDPO	
The location where the data may be transferred to	
Date of return or destruction by the data processor (if applicable)	
Security measures adopted	

Completed by Departmental Coordinator		Reviewed by Data Protection Officer	
Signature		Signature	
Name		Name	
Post		Post	
Date		Date	

Sample A
Purchase of
Products and
Services

Personal Information Collection Statement (Sample)

Company ABC Personal Information Collection Statement

The information collected from you will be used for the purpose of processing your purchase orders and managing our account with us.

Please note that it is mandatory for you to provide personal data marked with (*) on the purchase order form. In the event that you do not provide such personal data, we may not be able to process your purchase order and provide you with our products or services.

You have the right to request access to and correction of information held by us about you. If you wish to access or correct your personal data, please contact our data protection officer at _____ (company address) or _____ (email).



Sample B
For Job
Application

Personal Information Collection Statement (Sample)

Company ABC Personal Information Collection Statement

The personal data collected in this job application form will be used by us to assess your suitability to assume the job duties of the position for which you have applied and to determine preliminary remuneration, bonus payment, and benefits package to be discussed with you subject to selection for the position.

Personal data marked with (*) on the application form are regarded as mandatory for selection purposes. Failure to provide these data may influence the processing and outcome of your application.

It is our policy to retain the personal data of unsuccessful applicants for future recruitment purposes for a period of two years. When there are vacancies in our subsidiary or associate companies during that period, we may transfer your application to them for consideration of employment.

Under the Personal Data (Privacy) Ordinance, you have a right to request access to, and to request correction of, your personal data in relation to your application. If you wish to exercise these rights, please complete our "Data Access Request Form" and forward it to our Data Protection Officer in the Human Resources Department at _____ (company address) or _____ (email).

Data Breach Handling Checklist (Sample Template)

The following information can be used to structure your policies:

	Yes	No
Does your company have a data breach handling policy?	<input type="radio"/>	<input type="radio"/>
• If no, is it opportune time to develop one?	<input type="radio"/>	<input type="radio"/>
Does your company engage a data processor to process personal data on your company's behalf?	<input type="radio"/>	<input type="radio"/>
• If yes, have you adopted contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing?	<input type="radio"/>	<input type="radio"/>
• If no, is it opportune time to adopt one?	<input type="radio"/>	<input type="radio"/>

Key elements of a data breach handling policy / process

1. Gather essential information

- Assign a staff member / team at an appropriate level to assume overall responsibility in handling data breach incidents.
Title and rank of the designated officer: _____
- Have a list of essential information that needs to be gathered during the investigation:
 - Date and time of the breach
 - Location of the breach
 - How the breach was detected and by whom
 - Cause of the breach
 - Types of data subject affected
 - Estimated number of data subjects affected
 - Types of personal data involved
- Required to produce a detailed investigation report on the findings and report to senior management and relevant units.

2. Contact interested parties and adopt containment measures

- Maintain a contact list of interested parties for reporting, advice and assistance:
 - Law enforcement agencies (e.g. police)
 - Relevant regulators (e.g. PCPD)
 - Internet service providers
 - IT experts
- Establish a list of containment measures:
 - Stop the system if the data breach is caused by a system failure
 - Change the users' passwords and system configurations to control access and use
 - Consider whether technical assistance is needed to remedy the system loopholes and / or stop the hacking
 - Cease or change the access rights of individuals suspected to have committed or contributed to the data breach
 - Notify the relevant law enforcement agencies if criminal activities are or likely to be committed
 - Keep the evidence of the data breach to facilitate investigation
 - Direct the data processor to take immediate remedial measures and request it to notify the data user of the progress, if applicable

3. Assess the risk of harm

- Establish a risk assessment to determine the extent of harm that may be suffered by the data subjects (*refer to page 136 for an assessment template*)

4. Consider giving data breach notification

- When data subjects can be identified, consider notifying the data subjects and the relevant parties when actual risk of harm is reasonably foreseeable in a data breach
- Information to be included in a data breach notification
 - General description of what occurred
 - Date and time of the breach, its duration
 - Date and time the breach was discovered
 - Source of the breach
 - List of the types of personal data involved
 - Assessment of the risk of damage
 - Description of the measures already taken or to be taken to future breaches
 - Contact information of the designated person for affected data subjects to obtain more information and assistance
 - Information and advice on actions the data subjects can take to protect themselves from the adverse effects of the breach and against identity theft or fraud
 - Whether law enforcement agencies, the Privacy Commissioner and other parties have been notified
- Provide information on how to inform Privacy Commissioner about a data breach incident (including PCPD's Data Breach Notification Form)



Data Breach Risk Assessment (Sample Template)

Company ABC	
Branch / Department	
Date of the breach	
Brief description of the breach	
<p>Level of sensitivity (depends on the kind of personal data being leaked):</p> <p>1 2 3 4 5</p> <p>Seriousness of consequences (depends on the amount of personal data involved):</p> <p>1 2 3 4 5</p> <p>Effectiveness of data containment (depends on the circumstance of the breach):</p> <p>1 2 3 4 5</p> <p>Likelihood of identity theft or fraud:</p> <p>1 2 3 4 5</p> <p>Whether the leaked data is adequately encrypted, anonymised or otherwise rendered inaccessible (e.g. passwords are needed for access)</p> <p><input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Not sure</p> <p>Is the data breach ongoing? Will there be further exposure of the leaked data?</p> <p><input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Not sure</p> <p>Is the breach an isolated incident?</p> <p><input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Not sure</p> <p>If there is a physical loss, has the personal data been retrieved before it has the opportunity to be accessed or copied?</p> <p><input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Not sure</p> <p>Any mitigation / remedial measures have been taken after the breach occurs?</p> <p><input type="radio"/> Yes <input type="radio"/> No</p> <p>How will you estimate the ability of the data subjects involved to avoid or mitigate possible harm?</p> <p>1 2 3 4 5</p> <p>How will you estimate the reasonable expectation of personal data privacy of the data subjects?</p> <p>1 2 3 4 5</p>	

Completed by Departmental Coordinator			
Name		Post	
Signature		Date	

Data Breach Information Sheet (Sample Template)

Company ABC	
Branch / Department	
(I) INFORMATION OF THE BREACH	
(i) General information of the breach	
Description of the breach	
Location of the breach	<i>(e.g. which office, which computer server, etc.)</i>
Date and time of discovering the breach	
How the breach was discovered	<i>(e.g. discovered during routine system checking, known after reported by media, etc.)</i>
Nature of the breach	<i>(e.g. loss of data, database is hacked, etc.)</i>
Cause of the breach	
(ii) Impact of the breach	
Types of data subjects affected	<i>(e.g. staff, customers, public, etc.)</i>
Estimated number of data subjects affected	<i>(Please state the respective number for each type of data subjects)</i>
Types of personal data affected	<i>(e.g. name, date of birth, Hong Kong Identity Card number, address, telephone number, etc.)</i>
Medium holding the affected personal data	<i>(e.g. physical folders, USB, etc.)</i>
If the personal data is held in electronic medium, is the data encrypted?	<input type="radio"/> Yes <input type="radio"/> No
(II) DATA BREACH NOTIFICATION TO REGULATORY BODIES	
Are regulatory bodies such as the Hong Kong Police Force or the PCPD notified of the data breach?	<input type="radio"/> Yes <input type="radio"/> No
If yes, please provide the date and details of each notification given	

(III) ACTIONS TAKEN/TO BE TAKEN TO CONTAIN THE BREACH	
Brief description of actions taken to contain the breach	
Please evaluate the effectiveness of the above-mentioned 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 (refer to the "Data Breach Risk Assessment" template on page 136)	
(V) DATA BREACH NOTIFICATIONS TO DATA SUBJECTS AFFECTED	
Dates and details of the data breach notifications issued to data subjects affected by the breach	
(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 dates	
Date to review the effectiveness of the above-mentioned improvement measures	

Completed by Departmental Coordinator		Reviewed by Data Protection Officer	
Signature		Signature	
Name		Name	
Post		Post	
Date		Date	

Data Processor Review Checklist (Sample Template)

Company ABC		
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
Q1) Do the contractual terms cover the organisation's right to audit and inspect how the data processor handles and stores personal data?	<input type="radio"/> Yes <input type="radio"/> No (please explain)	
Q2) 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?	<input type="radio"/> Yes <input type="radio"/> No (please explain)	
Q3) 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?	<input type="radio"/> Yes <input type="radio"/> No (please explain)	
Q4) Do the contractual terms cover the limitation on sub-contracting the service that it is engaged to provide?	<input type="radio"/> Yes <input type="radio"/> No (please explain)	
Q5) Do the contractual terms cover the timely return, destruction or deletion of personal data by the data processor?	<input type="radio"/> Yes <input type="radio"/> No (please explain)	
Q6) 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 PDPO?	<input type="radio"/> Yes (please specify the security measures) <input type="radio"/> No (please explain)	

Part B: Review of the organisation's management of data processors		
Questions	YES / NO (if NO, please explain the reasons and justifications)	Remarks
Q7) Do the contractual terms cover the consequences for breach of the contract?	<input type="radio"/> Yes <input type="radio"/> No (please explain)	
Q8) Is the Branch/Department satisfied that the data processor had followed the contractual obligations in respect of personal data protection? If YES, please elaborate.	<input type="radio"/> Yes (please elaborate) <input type="radio"/> No (please explain)	
Q9) If the answer to Q8) above is NO, please specify the actions taken by the Branch/ Department?	(please specify)	
Q10) Has the Branch/Department performed any audit and inspection on the data processor in the past 36 months (including spot-checks)? 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.	<input type="radio"/> Yes (please state as request) <input type="radio"/> No (please explain)	
Q11) 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.	<input type="radio"/> Yes (please state the details and the improvement measures) <input type="radio"/> No (please explain)	
Q12) Has there been any data breach incidents caused by the data processor? If YES, please provide the corresponding Data Breach Information Sheet as attachment.	<input type="radio"/> Yes (please provide the corresponding Data Breach Information Sheet) <input type="radio"/> No (please explain)	

Completed by Departmental Coordinator		Reviewed by Data Protection Officer	
Signature		Signature	
Name		Name	
Post		Post	
Date		Date	

PIA Questionnaire (Sample Template)

Company ABC	
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 collecting the personal data 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 / have taken appropriate data security measures? If NO, please elaborate on the justification.	<input type="radio"/> Yes - contractual or other means have been adopted to ensure that the data processor(s) has/have taken appropriate data security measures <input type="radio"/> No (please explain)
Will there be any cross-border or cross-boundary transfer of personal data? If YES, please specify the destination(s) and the purpose(s) of such cross-border transfer.	<input type="radio"/> Yes - please specify the destination(s) and the purpose(s) <input type="radio"/> No

Part B: Privacy Risk Analysis		
Area	PIA Questionnaire	Answers by Branch / Division
<p>Data Protection Principle (DPP) 1 - Purpose and manner of collection of personal data</p> <p>▶ 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.</p> <p>▶ 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.</p> <p>▶ Data collected should be necessary but not excessive.</p>	<p>Will the data subjects be informed of the purpose of collecting their personal justifications?</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No (please explain):</p>
	<p>Will the collection of personal data be on a minimum level (i.e. no excessive personal data is collected)?</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No (please justify)</p>
	<p>Please provide justifications on the collection of sensitive personal data below (including but not limited to):</p> <ul style="list-style-type: none"> • Hong Kong Identity Card number and other personal identifier (e.g. passport number) • Biometric data (e.g. fingerprints) 	
	<p>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 justify.</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No (please justify)</p>
	<p>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 justify.</p>	<p><input type="radio"/> Yes (please elaborate)</p> <p><input type="radio"/> No (please justify)</p>
	<p>Will the personal data collected be transferred or disclosed to any third party?</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>
	<p>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.</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No (please provide the reason)</p> <p><input type="radio"/> Not applicable (personal data collected will not be transferred or disclosed to any third party)</p>

<p>DPP 2 - Accuracy and duration of retention of personal data</p> <p>➤ 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.</p>	<p>Will there be any measures in place to ensure accuracy of the personal data held? If YES, please elaborate. If NO, please justify.</p> <p>What will be the retention period of the personal data? Please specify.</p> <p>Will there be any measures in place to ensure that personal data is not kept longer than is necessary to fulfil the purpose of using the data? If YES, what are the measures? If NO, please justify.</p>	<p><input type="radio"/> Yes (please elaborate)</p> <p><input type="radio"/> No (please justify)</p> <p>Retention period: _____</p> <p><input type="radio"/> Yes (what are the measures)</p> <p><input type="radio"/> No (please justify)</p>
<p>DPP 3 - Use of personal data</p> <p>➤ 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.</p>	<p>Will personal data be used only for the original purpose stated in the Personal Information Collection Statement? If NO, what are the reasons?</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No (please specify the reasons)</p>
	<p>Where the personal data will be used for a new purpose, has explicit consent been obtained from the data subjects? If NO, please justify.</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No (please justify)</p> <p><input type="radio"/> Not applicable (personal data will not be used for purposes other than the original purposes for which it is collected)</p>
	<p>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.</p>	<p><input type="radio"/> Yes (please elaborate)</p> <p><input type="radio"/> No (please justify)</p> <p><input type="radio"/> Not applicable (personal data collected will not be disclosed to a third party)</p>
<p>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.</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No (please justify)</p> <p><input type="radio"/> Not applicable (personal data collected will not be disclosed to a third party)</p>	

<p>DPP 4 - Security of personal data</p> <p>▶ Data user needs to take all practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.</p>	<p>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.</p>	<p><input type="radio"/> Yes (please elaborate)</p> <p><input type="radio"/> No (please justify)</p>
	<p>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.</p>	<p><input type="radio"/> Yes (please elaborate)</p> <p><input type="radio"/> No (please justify)</p> <p><input type="radio"/> Not applicable (third party data processor will not be engaged)</p>
	<p>Where data processor(s) will be engaged, is the personal data disclosed to data processor only necessary but not excessive? If NO, please justify.</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No (please justify)</p> <p><input type="radio"/> Not applicable (third party data processor will not be engaged)</p>
<p>DPP 5 - Openness of information</p> <p>▶ 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.</p>	<p>Is the existing Privacy Policy still applicable? If NO, please specify what update is needed.</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No (please specify)</p>
	<p>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 onto the website before the implementation of the change / launch of the project? If NO, please explain. ^[Note]</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p> <p><input type="radio"/> No update is required</p>

Note:

If there is a need to update the Privacy Policy, the subject 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 subject 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.

<p>DPP 6 - Access to and correction of personal data</p> <p>➤ 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.</p>	<p>Will the data subjects be informed of their right to access and correct their personal data? If NO, please justify.</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No (please justify)</p>
	<p>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.</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No (please justify)</p>

Part C: Potential Risks and Mitigation Action

[For any privacy risks identified, please describe the means to address the risks. Based on the results of Part B, the subject 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 subject officer should consult the Branch/Department Head and the Data Protection Officer to assess the impact and whether the organisation could bear such risks.]

Potential risks identified	
Mitigation measures	

Completed by Departmental Coordinator		Reviewed by Data Protection Officer	
Signature		Signature	
Name		Name	
Post		Post	
Date		Date	

Direct Marketing and Your Business



Direct Marketing and Your Business

Direct Marketing and Your Business

What is Direct Marketing?

The PDPO does not prohibit direct marketing activities. According to the PDPO, direct marketing means:

- (a) the offering, or advertising of the availability, of goods, facilities or services; or
 - (b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes,
- through direct marketing means.

Do you intend to use personal data of your customers for your own direct marketing purposes?

If so, **before** using personal data in direct marketing, you **MUST**:

1. Inform the customers of your intention to use their personal data for direct marketing, and you may not so use the data unless you have the customers' consent;
2. Provide the customers with information on the intended use of the data, including the kinds of personal data to be used and the classes of marketing subjects in relation to which the data is to be used;
3. Provide the customers with a free-of-charge channel through which they may communicate their consent to the intended use; and
4. Present the information to the customers in a manner that is easily understandable and, if in written form, easily readable, in order to help the customers make an informed choice.

And, if you are using the customers' personal data in direct marketing **for the first time**, you **MUST**:

- Notify the customers of their opt-out right, and
- Stop using the personal data in direct marketing if the customers opt out, without charge to them.



Remember, you can use the personal data in direct marketing **ONLY AFTER** you have received the customers' consent to the intended use of their personal data.

You must also comply with the customers' request at **any time** to stop using their personal data in direct marketing without charge to them.

Please refer to page 151-152 for a checklist.

What is a valid consent?

It includes an indication of no objection to the use or provision of the personal data. To qualify:

- The individual concerned must have **explicitly indicated** that he did not object to the use and/or provision of his personal data to another for use in direct marketing.
- Silence does **NOT** constitute consent.
- If the individual gives his consent **orally**, you must confirm **in writing** to him **within 14 days** from receiving his consent the permitted kind of personal data and class of marketing subjects.

Do you intend to provide personal data to third parties for use in direct marketing?

If so, in addition to follow the previous outlined procedure, you **MUST**:

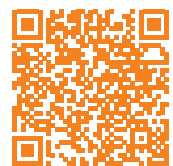
- **inform** the customers of two other kinds of information in relation to the intended use:
 1. whether the data is to be provided for gain; and
 2. the classes of persons to whom the data is to be provided;
- Notify and respond to the customers **in writing**; and
- Obtain **written consent** from the data subject. Otherwise the data cannot be provided to a third party.

Customers may at any time and irrespective of whether they have previously given consent to the provision of their personal data to a third party require you —

- to stop providing their personal data to a third party for use by that party in direct marketing; and
- to notify any third party to whom the data has been so provided to stop using the data in direct marketing.

Once you have received these instructions, you must, without charge to the data subjects, comply with them. The notification made by you to the third party must be in writing. Any third party who receives such a notification from you must stop using the personal data in direct marketing in accordance with the notification.

USEFUL
INFORMATION:



New Guidance on
Direct Marketing

Direct Marketing Related Checklist and Examples

Use of Personal Data in Direct Marketing Checklist



Inform the customer that you have the intention to use his personal data for direct marketing purpose on or before the data is collected:

- Include the following information in the notice to the customer:
 - You intend to use his personal data for direct marketing;
 - You may not so use the data unless you have received his consent to the intended use;
 - The kind of personal data to be used;
 - The classes of marketing subjects in relation to which the data is to be used; and
 - The response channel through which the customer may, without charge by you, communicate his consent to the intended use.
- The information above in the notice is presented in a manner that is easily understandable and easily readable.



Have received the customer's consent to the intended use:

- In writing (See examples on page 153-154)
- Orally
 - A written confirmation has sent to the customer no later than 14 days after the oral consent is obtained with the following information:
 - The date of receipt of the consent
 - The permitted kind of personal data
 - The permitted class of marketing subjects
 - Your contact information (to facilitate the customer to dispute the confirmation)
 - Obtain the customer's contact means (e.g. telephone number, correspondence or email address) to which the written confirmation is to be sent.
- Have kept a record of the consent of the customer and a record of the written confirmation sent.





Have notified the customer of his right to request you to cease to use the data in direct marketing when using his personal data FOR THE FIRST TIME:

- By email
 - Have highlighted the opt-out right of the customer in the email with a hyperlink to the address of your organisation for the customer to exercise such right.
- By mail or fax
 - Have provided a "tick" box and return address to facilitate the customer to exercise his opt-out right.
- By telephone
 - Have informed the customer of his right by making clear to the called party that "if you do not wish to receive further marketing calls from us, let us know and we will not call again" (or words to the same effect).
- By SMS
 - Have provided a telephone hotline to receive opt-out requests.



Comply with a customer's opt-out request:

Maintain an "Opt-Out List" – a list of all customers who have indicated that they do not wish to receive further marketing approaches:

- Via an online computer network:
 - Individual marketing staff will input new opt-out requests as and when they are received.
 - The opt-out list is distributed other than by a computer network:
 - Notify marketing staff members of the updates at a frequency of no less than once per week.
 - Via your branch offices:
 - Each branch office has to maintain its own Opt-Out List of customers.
 - The head office has to coordinate the updating of a consolidated Opt-Out List by collecting the opt-out information supplied by all branch offices.
 - The head office has to inform its branch offices of the updated position on a continuous basis.
 - Have developed standing procedures for its staff members to follow in regard to accessing and updating the Opt-Out List and complying with the data subjects' opt-out requirements.
- Retention of Opt-Out List and record of consent:**
- Make an assessment of the necessity of deleting all or some of the personal data of those customers who have indicated their opt-out requirements, and erase unnecessary personal data accordingly.
 - Review regularly the personal data held to see if it is still necessary to retain the same and perform data erasure as required at regular intervals.

**Example
1**

Notification to Customers of the Use of Personal Data in Direct Marketing and Obtaining Their Consent Selectively

1. We intend to use your personal data for direct marketing;
2. We may not so use your personal data unless we have received your consent;
3. We shall use the following personal data for marketing our services -
 - your name
 - your residential address
 - your mobile phone number
 - your residential phone number
 - your email address

Please tick the box(es) provided to indicate your consent for the above item(s).

4. Your personal data will be used for marketing our services as follows:-
 - mobile phone
 - internet network

Please tick the box(es) provided to indicate your consent for the above item(s).

Signature of the customer

Name: XXXXXX

Date:

Example
2

Indicating No Objection Generally

We intend to use your name, telephone number and address for direct marketing credit card and insurance products / services but we cannot so use your personal data without your consent.

Please sign at the end of this statement to indicate your agreement to such use. Should you find such use of your personal data not acceptable, please indicate your objection before signing by ticking the box below.

- The customer named objects to the proposed use of [his / her] personal data in direct marketing.*

Signature of the customer

Name: XXXXXX

Date:



Other Useful Information



**Other
Useful
Information**

Do's and Don'ts - Human Resource Management

Organisations who handle personal data in performing human resource management functions and activities need to observe the requirements of the PDPO. As employer, you are liable to protect the personal data of job applicants, your current and former employees.



Below is a quick glance of the do's and don'ts:

	Do's	Don'ts
Recruitment	<ul style="list-style-type: none"> ➤ Job advertisements should include a statement informing potential applicants about the data collection purposes and contact information of your organisation ➤ May collect personal data of pre-employment medical examination that is directly related to the job requirements ➤ May retain personal data of unsuccessful applicants for not more than two years from the date of rejecting applicants 	<ul style="list-style-type: none"> ➤ Should not solicit personal data via job advertisements without providing identification of either your organisation or the employment agency on its behalf ➤ Should not collect Hong Kong Identity Card copies from job applicants during the recruitment process until the candidates have accepted the job offers

	Do's	Don'ts
Current Employment	<ul style="list-style-type: none"> ▶ Provide a PICS to the employees before collecting personal data from them ▶ May collect additional personal data from employees and their family members for employment purposes and fulfilling lawful requirements ▶ Personal data of an employee (compiled during performance appraisal or staff compensation) should only be used for purposes directly related to the collection purposes 	<ul style="list-style-type: none"> ▶ Should not disclose employment-related personal data of employees to third parties without obtaining the employees' consent unless the disclosure is for the purpose directly related to employment or other lawful requirements ▶ Should not transfer or disclose employment-related personal data in excess of that is necessary for the purpose of use by the third party
Former Employment	<ul style="list-style-type: none"> ▶ Generally, personal data may be retained for a period up to seven years from the date the former employee ceases employment. The data may be retained for a longer period if there is a subsisting reason that obligates the employer to do so, or the data is necessary for the employer to fulfil contractual or legal obligations. ▶ Only relevant personal data of former employees is retained to satisfy the retention requirements 	<ul style="list-style-type: none"> ▶ Do not disclose former employees' identity card numbers in any public announcement notice related to them ▶ Do not provide job references of former employees to the third parties without first obtaining the employees' consent

USEFUL INFORMATION:



Code of Practice on Human Resource Management



Code of Practice on the Identity Card Number and Other Personal Identifiers



Compliance Guide for Employers and Human Resource Management Practitioners



Human Resource Management: Some Common Questions



Transfer of Personal Data Outside Hong Kong



Advances in technology, along with changes in organisations' business models and practices, have turned personal data transfers into personal data flows. Data is moving across borders/boundaries, continuously and in greater scales. Organisations, including SMEs, are enhancing their efficiency, improving user convenience and introducing new products by practices which have implications for global data flows. They vary from storing data in different jurisdictions via the 'cloud' to outsourcing activities to contractors around the world. Electronic international data transfers in areas such as human resources, financial services, education, e-commerce, public safety, and health research are now an integral part of the global economy.

Against this background, the issue of regulating cross-border/boundary data flows is becoming more acute than ever before. Economies worldwide are adopting a range of mechanisms to protect the personal data privacy of individuals in the context of cross-border data flows.

Section 33 of the PDPO prohibits the transfer of personal data to places outside Hong Kong except in specified circumstances. Although section 33 has not been brought into operation since its enactment, the existing provisions of the PDPO have already provided safeguards for cross-border / boundary data transfer to ensure that the personal data transferred outside Hong Kong would be afforded with the same level of protection under the current regulatory regime. In this connection, data users are required to:-

- i) give notice to explicitly inform data subjects of the classes of persons to whom the data may be transferred (Data Protection Principle 1(3));
- ii) obtain the prescribed consent of data subjects for change of use of the personal data collected (Data Protection Principle 3);
- iii) adopt contractual or other means to prevent any personal data transferred to the data processors, whether within or outside Hong Kong, from unauthorised or accidental access, processing, erasure, loss or use of the data being transferred for processing (Data Protection Principle 4(2)); and
- iv) adopt contractual or other means to prevent any personal data transferred to the data processors, whether within or outside Hong Kong, from being kept longer than is necessary for processing of the data (Data Protection Principle 2(3)).

To protect personal data privacy without hindering business development and economic growth, the PCPD published the “Guidance on Personal Data Protection in Cross-border Data Transfer” in 2014 to provide practical guidance to organisations which need to transfer personal data outside Hong Kong during their business operations. The Guidance assists organisations to prepare for the eventual implementation of section 33 and enhance privacy protection for cross-border data transfer. It helps organisations understand their compliance obligations under section 33. In particular, the PCPD has prepared a set of recommended model clauses to assist organisations in developing their cross-border data transfer agreement with the overseas data recipients. Organisations are encouraged to adopt the practices recommended in the Guidance as part of their corporate governance responsibility even before section 33 takes effect.

USEFUL INFORMATION:



**Guidance Note on
Personal Data Protection
in Cross-border Data
Transfer**



Introduction to the Regulations in the Mainland of China Concerning Personal Information and Cybersecurity Involved in Civil and Commercial Affairs



To take full advantage of the vast online market in the mainland of China, enterprises should not ignore its network supervision policies and related regulatory restriction.

At present, the regulations concerning the protection of personal information in the mainland of China are covered by an assortment of normative instruments, such as laws, administrative regulations, departmental rules and guidelines, and the relevant regulatory framework is ever-expanding. In addition, the mainland of China is moving towards treating the right to privacy and personal information as an independent moral right with the introduction of civil protection. With the promulgation of various regulations, the privacy and personal information of the general public are protected in a greater and more extensive extent. However, owing to the multiplicity of regulations on the protection of personal information in the mainland of China, enterprises looking for business ventures in this emerging market are encountering compliance challenges.

In light of this, the PCPD published a Chinese booklet entitled “Introduction to the Regulations in the Mainland of China Concerning Personal Information and Cybersecurity Involved in Civil and Commercial Affairs” (the Booklet), which provides an overview of related regulations regarding personal data protection in the mainland of China. The Booklet attempts to serve as a handy kit to help the business sector better understand the relevant regulatory regime, so that they could expand their online business smoothly in the Greater Bay Area and maximise business benefits.

The Booklet consolidates and introduces current relevant regulations and cases in the mainland of China, and also sets out and compares the privacy laws of Hong Kong and the mainland of China. For instance, China’s Cybersecurity Law requires that personal information and important data collected and generated by operators within the mainland of China should be stored locally. The Administrative Measures for Data Security (Consultation Draft) stipulates that network operators should register with the cyberspace administration and appoint a person responsible for data security, if the network operators intend to collect sensitive personal information.

Visit the website of the PCPD to download the Booklet.



GDPR and You

What is the GDPR?

The General Data Protection Regulation (GDPR), which came into effect on 25 May 2018, replaces the data protection framework under the EU Data Protection Directive based on which the PDPO modelled upon back in mid-1990s. It emphasises transparency, security and accountability by data controllers.

Does the GDPR apply to your business?

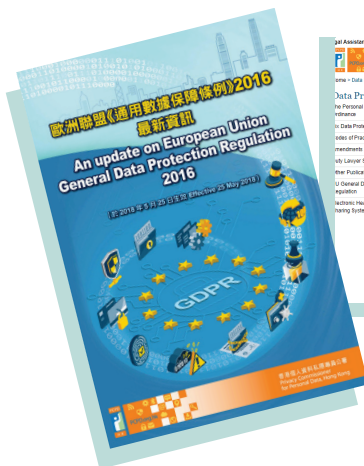
The GDPR also applies to organisations outside the EU that offer goods or services to or monitor the behavior of individuals in the EU.

With this extra-territorial effect, businesses in Hong Kong fitting in with the above scope may wish to know more about GDPR.

Want to learn more about the GDPR?

To raise the awareness amongst businesses in Hong Kong of the possible impact of the GDPR, a Booklet **“European Union General Data Protection Regulation 2016 (Effective 25 May 2018)”** was published, featuring the major characteristics of the new law and the areas of differences with Hong Kong’s PDPO.

A dedicated web page with the latest updates on GDPR and the related educational materials and activities is also available on PCPD.org.hk:



Create Accountability, Strengthen Commitment – Privacy Management Programme

Is it practicable to adopt a PMP in your small business?

One step further is to develop your own Privacy Management Programme (PMP). Organisations should embrace personal data protection as part of your corporate governance responsibilities and apply them as a business imperative throughout the organisation. This can, not only build trust with clients, but also enhance your reputation as well as competitiveness.



Three components of PMP



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

Benefits of implementing a PMP

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

Start constructing you own PMP!

Refer to our Privacy Management Programme: A Best Practice Guide to get a framework for constructing a comprehensive PMP, with the help of concrete examples and practical guidance.



Respectful, Beneficial and Fair - Ethical Data Governance



In a data-driven economy, SMEs including tech start-ups, increasingly use personal data of customers as an asset in operating and advancing their businesses. The rapid development in information and communications technology, particularly advanced data processing activities (including big data analytics and artificial intelligence), present business opportunities but at the same time challenges privacy and data protection.

It is not in dispute that personal data belongs to the data subjects. SMEs that derive benefits from personal data should ditch the mindset of conducting their operations to merely meet the minimum regulatory requirements only. They should instead be held to a higher ethical standard that meets stakeholders' expectations alongside the requirements of laws and regulations. Data ethics can therefore bridge the gap between legal requirements and stakeholders' expectations.

To protect customers' personal data privacy and enhance their confidence, SMEs should handle personal data pursuant to three core values:

Respectful

- Enterprises should consider the expectations of the individuals to whom the data relate and/or impacted by the data use
- Individuals should be able to make inquiries, obtain explanations and appeal against decisions on the advanced data processing activities that impact them

Beneficial

- To define, identify and assess the benefits and potential risks of the advanced data processing activities which have potential impact on individuals
- To implement measures to mitigate all the identified risks and balance the interests of different parties

Fair

- To review the accuracy and relevance of algorithms, models and datasets used in decision-making regularly to reduce error, uncertainty, bias or discrimination

Ethical Data Impact Assessment

SMEs can conduct Ethical Data Impact Assessment before deciding to pursue an advanced data processing activity by answering the following questions to understand their ethical responsibilities for data protection and find out the impact of their data driven activities on their stakeholders' rights and interests.

Purpose of the activity

- What is the business need/objective for this data activity?
- Who needs to be involved in making decision regarding the data activity? Who has ultimate decision-making authority for the data activity?
- How will the laws applied to the collection, analysis, use and transfer of data, and other obligations be managed and satisfied?

A full understanding of the data, its use and parties involved

- Is the data personally identifiable? Is data reidentification possible from anonymised data?
- Is the data (e.g. race, ethnic origin, sexual orientation, physical or mental health) or its anticipated use sensitive?
- Is the data accurate enough for the purpose of the data activity?

Impact on parties, in particular individuals

- What are the benefits and the risks to the individual, groups of individuals and society?
- What kinds of technical and procedural safeguards (e.g. encryption and deidentification of data) will be implemented to prevent and mitigate risks?

Whether an appropriate balance of benefits and mitigated risks supports the data-processing activity

- Have the interests, rights and expectations of individuals been duly considered?
- Are the risks arising from the data activity proportionate to the benefits? Have the risks been mitigated to the greatest extent practicable?

USEFUL INFORMATION:



**Data Ethics for
Small and Medium
Enterprises**

The Privacy Commissioner published an Ethical Accountability Framework with setting out guiding questions of two assessment models to help organisations complete the assessment tasks.

USEFUL INFORMATION: **Report on "Ethical
Accountability
Framework for
Hong Kong, China"**



**Data Stewardship
Accountability,
Data Impact
Assessments and
Oversight Models**



PCPD Enquiry Services for SMEs

We Offer All-round Support for You!

To strengthen communication and cooperation with SMEs, we operate a dedicated hotline and an email service providing advice on data protection.

The SME Hotline is 2110 1155, operating during the PCPD office hours (Monday to Friday from 8:45 am to 12:45 pm and 1:50 pm to 5:40 pm, except public holidays). SMEs can also make email enquiries to sme@pcpd.org.hk. SME-related enquiries are handled by a special team.



Appendix

6 保障資料原則

Data Protection Principles

PCPD.org.hk

1

收集目的及方式 Collection Purpose & Means



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。

須以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給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/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.

2

準確性、儲存及保留 Accuracy & Retention



資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的的实际所需。

Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used.

3

使用 Use



個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

Personal data is used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject.

4

保安措施 Security



資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5

透明度 Openness



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。

A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

6

查閱及更正 Data Access & Correction



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。

A data subject must be given access to his personal data and to make corrections where the data is inaccurate.



**JOIN
TODAY!**

Data Protection Officers' Club

(Membership Application)

By becoming a DPOC member, you will:

- **advance your knowledge and practice of data privacy compliance through experience sharing and training;**
- **enjoy 20% discount on the registration fee for PCPD's Professional Workshops;**
- **receive updates on the latest development in data privacy via regular e-newsletter**

As a DPOC member, your organisation's name will be published on DPOC membership list at the PCPD's website, demonstrating your commitment on personal data protection to your existing and potential customers as well as your stakeholders.

Membership fee: HK\$150 per year (for SME members only)
Enquiries: dpoc@pcpd.org.hk



https://www.pcpd.org.hk/misc/dpoc/files/appform_19_20_new_member_sme.pdf

The page contains a large rectangular area designed for writing. It features a solid teal top border and a solid teal bottom border. The interior of this area is filled with horizontal dotted lines, providing a guide for text alignment. The dotted lines are evenly spaced and extend across the width of the page. There are small teal circles at the top-left and bottom-right corners of the writing area, where the solid lines meet the dotted lines.



私隱公署網頁
PCPD website
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:	傳真: Fax:	電郵: Email:
(852) 2827 2827	(852) 2877 7026	enquiry@pcpd.org.hk

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

中小型企業查詢熱線: SME Hotline:	中小型企業電郵: SME Email:
(852) 2110 1155	sme@pcpd.org.hk



本刊物使用署名4.0國際 (CC BY 4.0) 的授權條款，只要你註明原創者為香港個人資料私隱專員，便可自由分享或修改本刊物。詳情請瀏覽 creativecommons.org/licenses/by/4.0/deed.zh。

This publication is licensed under Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this publication, as long as you attribute the work to the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.

免責聲明

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，亦不構成法律或其他專業意見。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。

Disclaimer

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 and do not constitute legal or other professional advice. 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.

2020年6月初版
First published in June 2020



下載本刊物
Download this
publication