《保護個人資料 - 實用指引》

BDO

目錄

1 《個人資料（私隱）條例》簡介

《個人資料（私隱）條例》（香港法例第486章）（下稱「條例」）於1996年正式生效。違反條例下的某些條文可構成刑事罪行，一經定罪，最高可處罰款1,000,000港元及監禁5年。

本指引的主要用詞釋義

個人資料	指符合以下所有條件的任何資料： • 與一名在世的個人有關； • 從該等資料可確定有關個人的身分；及 • 該資料的存在形式令予以查閱及處理均是切實可行的（即個人資料必須以某一記錄形式存在，如寫在文件上或儲存在電腦檔案內）。 （例子：文件檔案或電腦檔案所記錄的客戶姓名及地址。）
資料當事人	指屬有關資料之當事人的個人。 （例子：向貴公司提供個人資料的客戶。）
資料使用者	收集、持有、處理或使用有關個人資料的人士或公司
資料處理者	代另一人或公司（資料使用者）處理個人資料，而非為該資料處理者本身目的而處理個人資料的人或公司。 （例子：貴公司委託外判服務供應商進行客戶調查，過程中該服務供應商 收集客戶資料，並將資料及調查結果送交貴公司。）

條例及個人資料私隱專員公署

條例旨在透過規管任何收集、持有或使用個人資料的資料使用者，以及防止及懲罰資料使用者在香港處理個人資料時的濫用或疏忽行為，以保障資料當事人的個人資料。

條例的要點載於其六項「保障資料原則」。有關保障資料原則的詳情載於附錄一，而條例所處若干刑事罪行的例子則載於附錄二。

除了可引致罰款及監禁外，觸犯條例亦可能引起公眾關注，令資料使用者的聲譽嚴重受損。此外，受侵害的資料當事人（例如受影響客戶）可能向有關資料使用者提出民事訴訟，以索取賠償。

個人資料私隱專員公署（下稱「 私隱專員公署」）根據條例成立，是專責保障個人資料私隱的香港監管機構。私隱專員公署監察公、私營機構的資料使用者是否遵守條例的規定，調查公眾就違反條例的投訴，並發布協助資料使用者進一步理解條例規定的實務守則及指引。

有關個人資料私隱的外地法律

除條例外，海外的資料私隱法例亦可能適用於涉及從外國收集及處理個人資料的本地公司 。於2018年5月25日生效的歐洲聯盟（下稱「歐盟」）《通用數據保障條例》正是其中一個顯著例子。如非歐盟公司進行與歐盟成員國境內人士有關的資料處理活動，《通用數據保障條例》可能適用於這些公司。有關《通用數據保障條例》的更多資料，請參閱附錄三。

2

收集、使用及保存個人資料

A. 收集及使用個人資料

閣下須確保按照以下指引原則妥善收集個人資料：

i. 個人資料只可為直接與貴公司業務或活動有關的合法目的而收集。

ii. 所收集的個人資料只可對該目的而言是必需或直接有關，不得收集超過該目的所需的資料。

iii. 不得使用非法或誤導方式收集個人資料。

iv. 於收集個人資料之時或之前，須告知資料當事人以下訊息：

- 該資料將會用於什麼目的；
- 該資料可能轉移予什麼類別的人（包括第三方服務供應商（如適用））；
- 若不提供該資料便會承受的後果（例如，他將無法購買或使用若干產品或服務）；及
- 他可要求查閱及改正由貴公司持有其個人資料的權利（以及如何聯絡貴公司以提出有關要求）。

當從資料當事人（例如客戶或僱員）收集個人資料前，閣下應考慮向他提供一份載有上文第(iv)項中所述全部資料的《收集個人資料聲明》。

個人資料的用途謹限於閣下在收集資料時所告知的目的，除非閣下已獲得有關資料當事人的同意可將有關資料用於新目的。閣下亦應因應有關商業目的，而仔細考慮向資料當事人收集哪些個人資料。例如，如果閣下預期日後以電話或電郵聯絡客戶，就不應收集客戶的郵寄地址。

切勿向客戶或任何其他人士收集香港身份證號碼（或身份證副本），除非閣下將有關資料用於人力資源用途（如招聘或就業）， 需要遵循資料查閱或改正的要求或其他法定要求。

直接促銷

向現有或潛在客戶收集個人資料作直接促銷活動（如寄發推廣信件或電郵）之前，閣下必須遵守以下指引：

i. 告知客戶，貴公司希望使用他們的個人資料進行直接促銷，以及閣下將要推廣的產品、服務或活動類別；

ii. 告知客戶，閣下希望使用的個人資料類別；

iii. 向客戶提供一個回應途徑，讓他可通過該途徑向貴公司傳達書面同意（例如，在登記表中新增欄目，讓新客戶可表示同意貴公司使用他的個人資料作直接促銷）；

iv. 在使用客戶的個人資料作直接促銷前，取得他的書面同意；及

v. 如閣下亦希望提供客戶的個人資料予另一間公司以作直接促銷之用，亦須就此取得他的明確同意。

閣下可將第(i)、(ii)、(iii)及(v)項所述資料載於相關《收集個人資料聲明》、申請表或登記表上。

拒絕接收直接促銷通訊的服務 (即opt-out, 下稱「拒絕服務」)

發送直接促銷通訊及 / 或處理拒絕服務要求的僱員及部門，必須備存並更新「接受服務」(即opt-in) 及「拒絕服務」的客戶名單。兩份名單應集中處理，令需要發送直接促銷資訊的部門可查閱這些名單。

所有直接促銷通訊必須包含一項聲明，告知收件人可選擇拒絕接收貴公司日後的促銷資訊。該聲明亦須闡述拒絕服務的方式。在收到客戶的拒絕服務要求後，處理的僱員必須停止向該客戶發送直接促銷資訊，並迅速更新「接受服務」及「拒絕服務」的客戶名單。

B. 個人資料的準確性、保留及刪除

閣下須採取所有切實可行的步驟，以確保貴公司持有的全部個人資料：

i. 均為準確；

ii. 保存時間不超過為滿足/履行有關用途而需要保留的時間；及

iii. 在有關保存時間屆滿時被妥善刪除。

最佳的行事方式是制訂資料 / 文件的保留政策，規定不同種類的個人資料的最長保留期限，以滿足不同的業務和法律要求。

包含過時或過期個人資料的電子或文件檔案必須妥善刪除或銷毀。如果貴公司已委任外判承辦商處理此程序，承辦商必須受已簽署的服務協議監管，該協議須訂明他們的資料保障責任。

3 資料保安及預防資料外洩措施

A. **私隱管理系統** (Privacy Management Programme)

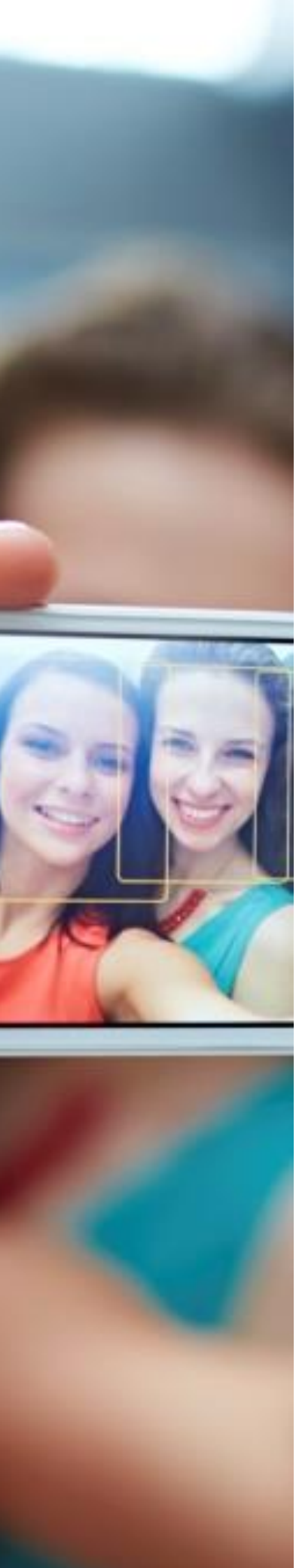
實施私隱管理系統可讓公司全面檢討現有處理個人資料的做法，並根據全公司的業務性質度身制訂有效的資料處理指引及程序。私隱管理系統亦可協助公司各部門中需要處理個人資料的各級僱員遵守條例。

以下是私隱管理系統中一些重要部分：

i. 委任保障資料主任全面監督公司有關個人資料私隱的所有事宜。

ii. 各部門亦須委任保障資料協調人員，處理所屬部門的日常個人資料私隱事宜，並就匯報資料外洩事故及諮詢複雜的資料私隱問題等事宜，與保障資料主任聯絡。

iii. 審閱個人資料庫存，即檢查並記錄各部門持有的個人資料類別、收集資料的目的、可查閱及使用資料的人、資料的保留方式、保留期間等。

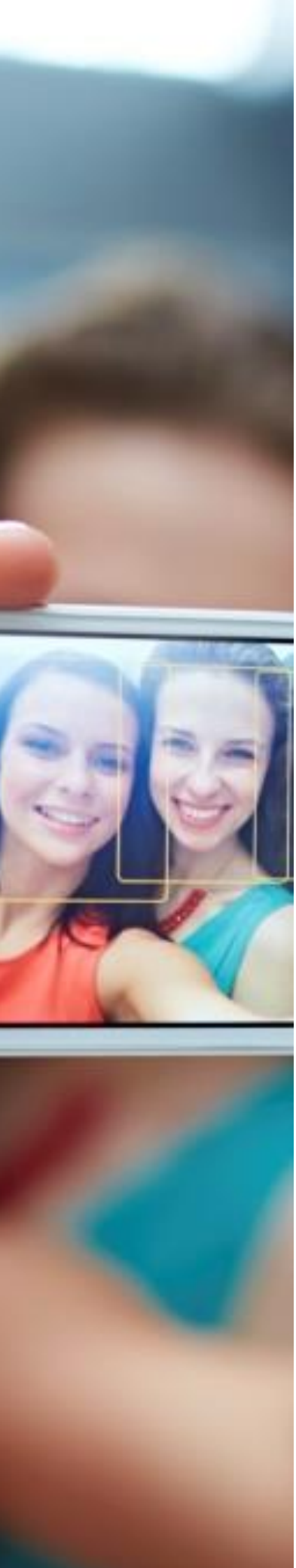


iv. 制訂處理個人資料的政策及程序。閣下可根據貴公司的業務性質，制訂一份全面指引，或就不同範疇（例如，直接促銷及人力資源管理）各自制訂一份政策及程序。這些政策及程序應涵蓋處理資料的所有步驟：收集、使用及披露、保留及棄置、保安措施以及回應查閱資料要求等。

v. 確保循章守法：(a)審視現行各部門的資料處理行事方式，並根據相關資料私隱規例以識別相關漏洞；(b)制訂並實施補救行動；及(c)定期監察及評估補救行動的成效，以識別任何未處理的問題，隨之作出糾正。

vi. 設立資料外洩事故的匯報機制。此機制應涵蓋向高級人員匯報資料外洩事故及通知受影響資料當事人的程序（詳情見第4節）。

（參考資料：私隱專員公署發出的Privacy Management Programme Manual (for Private Sector) – 只有英文版）



B. **私隱影響評估** (Privacy Impact Assessment)

在推出新活動或項目（當中涉及收集及使用個人資料）之前，或現有活動或項目的資料處理程序出現重大變化，進行私隱影響評估能協助貴公司盡量減低私隱風險。

總括而言，私隱影響評估包括：

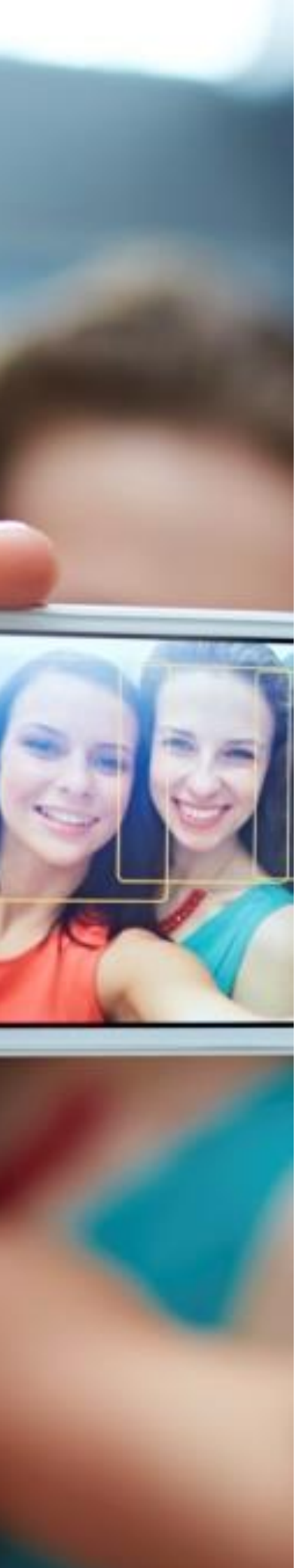
i. 資料處理週期分析；

ii. 私隱風險分析；

iii. 避免或減低私隱風險；及

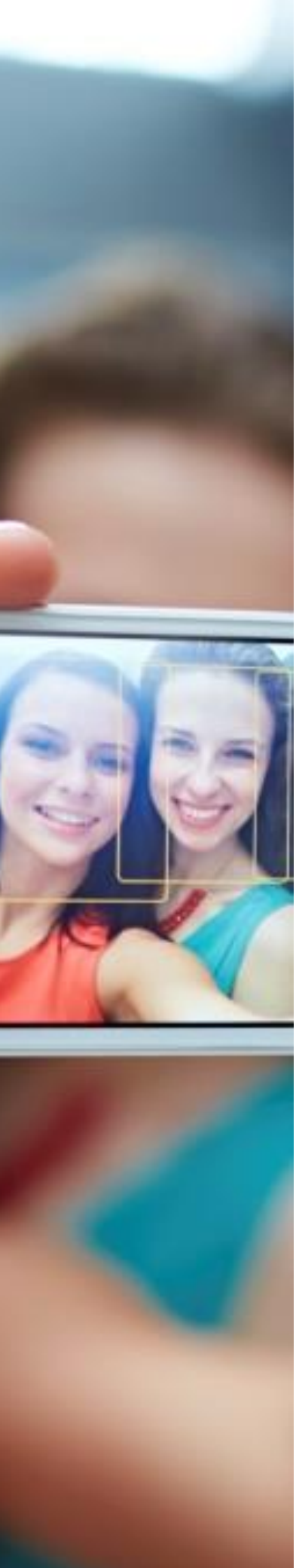
iv. 報告及持續監察。

（參考資料：私隱專員公署有關私隱影響評估的資料單張）



C. 資料保安及預防資料外洩措施的其他例子

i.	對資料查閱權制訂明確指引，以規管在不同情況下查閱及使用個人資料。查閱權的一般原則是，只限「有需要知道」該等資料的人士查閱。
ii.	對資訊科技系統、電腦伺服器及電子資料檔案採取保安措施。相關例子如下： • 如果閣下在網上收集客戶的個人資料及付款詳情，則須採取切實可行的步驟，確保客戶的裝置與貴公司伺服器之間的資料傳輸是安全的，例如使用Secure Sockets Layer (SSL安全憑證）。儲存在伺服器中的敏感資料（如香港身份證、銀行賬戶及信用卡號碼）應進行掩蔽處理。 • 讓僱員設定登入名稱及密碼，以保障貴公司提供的所有桌上或筆記電腦。如果電腦在無人使用下超過5至10分鐘，電腦應自動登出。 • 記錄僱員登入已儲存客戶或僱員個人資料的電腦系統的情況。
iii.	對文件及檔案採取保安措施。相關例子如下： • 不要將載有個人資料的文件放在無人看管的地方，應放在上鎖的櫃子內。 • 確保僱員在放工時清理辦公枱。 • 利用碎紙機銷毀載有個人資料的過時文件。閣下亦可考慮聘用聲譽良好的服務供應商銷毀大量的過時文件。
iv.	假如閣下需要以電郵寄出包含個人資料的檔案，須確保檔案已加密處理。分開以不同電郵寄出檔案與開啟檔案的密碼。此外，於點擊「寄出」或「回覆」前，閣下必須檢查收件人的電郵地址，以避免將機密資料發送至其他不相關的人士。



v.	規範僱員使用社交媒體平台。僱員切勿在社交媒體上披露公司敏感資訊及其他僱員的個人資料（其個人資料除外）。建議僱員加強對社交媒體賬戶的私隱設定（例如，僅限指定人士查閱其賬戶）。
vi.	切勿使用便攜式資料儲存裝置（如USB記憶體）儲存個人資料。如果閣下必須為履行職務而使用這類裝置，請遵守以下要求： • 僱員只能使用公司提供的裝置，並且必須妥善記錄借用日期及時間。 • 裝置中所有資料檔案必須加密。 • 避免將裝置帶離辦公室。
vii.	為僱員提供培訓，讓他們了解貴公司採取的所有預防資料外洩措施；以及定期向僱員發出相關措施的通訊，以提醒他們對這方面的意識。

4

資料外洩事故的處理方式

條例並無為「資料外洩事故」一詞設立定義 。資料外洩事故一般指個人資料受到意外的或未經准許的查閱、處理、刪除、喪失、使用或披露的事件。大部分資料外洩事故都是由於資料保安措施不足所致，因此，資料使用者如引起資料外洩事故，便可能已違反條例中保障資料第4原則有關資料保安的規定。

下列是一些資料外洩事故的例子：

- 遺失儲存客戶或僱員個人資料的便攜式儲存裝置，例如手機或USB記憶體。
- 儲存客戶資料庫的電腦伺服器在互聯網上遭不明人士入侵。
- 不當地棄置載有僱員身份證、僱員評核表等資料的個人檔案。

如果發生資料外洩事故，引起資料外洩的員工、負責部門的保障資料協調人員及保障資料主任等有關人士，應合力作出以下程序：

收集有關資料並將事故上報 → 決定應採取的緩解措施 → 通知受影響的資料當事人 → 採取補救行動 → 監察進展

A. **收集有關資料並將事故上報**

i. 外洩資料或發現資料外洩事故的僱員，須立即盡可能收集有關事故的資料以回應以下問題，並隨之向其直屬上司報告。

- 事故於何時及何地發生？例如，哪一個客戶資料庫遭入侵？
- 涉及什麼種類的個人資料？例如，姓名、電話號碼或電郵地址？
- 受影響的資料當事人類別？例如，XXX計劃的客戶/成員或XXX部門的員工？
- 受影響的資料當事人數目？
- 是否牽涉資料處理者？
- 資料外洩事故的肇因是什麼？該事故如何被發現？

（備註：若負責僱員無法收集上述信息，其直屬上司須提供協助。）

ii. 負責僱員及／或其直屬上司須向有關部門的保障資料協調人員報告事故的詳細資料，然後再由協調人員向部門主管及保障資料主任作出有關報告。

ii. 保障資料主任應評估事故的嚴重性（例如事故可能造成的傷害），以決定是否須向高級管理層報告。

在決定是否向高級管理層報告事故時，保障資料主任可能要考慮的因素包括：受影響的客戶數目、潛在的財務損失、對公司聲譽的預計受損程度以及任何相關刑事責任。

B. 決定應採取的緩解措施

根據資料外洩事故的情況，公司應立即採取臨時措施，以減輕損失及限制資料外洩事故的影響範圍。以下是一些例子：

- 如事故是電腦系統故障造成或系統遭黑客入侵，應暫時停止有關系統的操作，並徵詢資訊科技專家以修補有關漏洞。
- 如事故與外判服務供應商或資料處理者有關，應敦促該資料處理者立即採取補救措施。如有必要，與該資料處理者合作，共同解決問題。
- 如事故牽涉犯罪活動（例如，僱員盜竊客戶資料再將資料出售），保障資料主任應考慮徵詢法律意見，並通知有關執法部門。

C. **通知受影響的資料當事人（及私隱專員公署（如必要））**

條例並無強制資料使用者在資料外洩事故發生後，必須通知受影響的資料當事人。然而，通知有關當事人是良好的行事方式，因為受影響的當事人可對有關事故作出警惕，並採取必要的預防措施，以避免損失擴大。通知的內容可包括以下事項：

- 事故的概況（例如，事發地點及時間、外洩的個人資料類別、事故的肇因）。
- 已（或將）採取的補救行動。
- 貴公司可為受影響的資料當事人提供的協助或建議。

若保障資料主任認為資料外洩事故嚴重，亦應通知私隱專員公署。私隱專員公署備有「資料外洩事故通報表格」，可於公署的網站下載。

資料使用者亦可能須向其他相關執法部門及規管機構（例如，警方或香港金融管理局）作出通知。由於某類資料外洩事故或須強制向特定的監管機構作出通報，資料使用者應就此徵詢法律意見。

D. 採取補救行動

除程序B所述的臨時措施外，亦可能須採取進一步補救行動。所需補救行動將視乎事故的具體情況而定，在採取進一步行動之前，閣下應考慮以下各項：

i. 資料外洩事故是否屬個別事件，還是屬於系統性或持續的問題？例如，即使有關僱員已遵守日常的行事方式或內部指引，事故依然發生？如出現系統性或持續問題，負責部門必須檢討現行指引，並作出必要修改。貴公司亦可能需要修復現有（或引進嶄新）設備或資訊科技基礎設施，以解決相關問題。

ii. 事故是否涉及遺失大量客戶的個人資料，可能會引起社會關注？如是，處理事故的負責人可能需要與行政或企業傳訊部人員合作，預備一些標準的問題和答案，以便僱員能夠回應受影響客戶以及傳媒之查詢。例如，已遺失個人資料的種類、受影響客戶的大概數目、已採取的即時／臨時補救行動，以及正在向受影響客戶提供的協助及建議。

iii. 事故是否涉及遺失載有個人資料的文件或流動裝置？

- 如果文件或裝置遺留在辦公室外而無人看管，負責僱員其後又取回該文件或裝置，閣下應首先檢查有關個人資料會否被其他人查閱或複製。
- 如果文件或裝置遺留在辦公室外一段時間而無人看管，而其他人有可能查閱或複製有關資料，閣下亦需要考慮聯絡受影響的資料當事人，以提醒他們有關事件。

在採取進一步的補救行動前，務請尋求相關人士的專業意見，如資訊科技、法律、人力資源及公關專業人士等。

E. **監察程序B、C及D的進展並記錄相關事故的全部詳細資料**

負責人員（如有關部門的保障資料協調人員）應將資料外洩事故的主要資料記錄在中央檔案內，例如：

- 事故的基本資料（如程序A所載）。
- 已採取的補救及額外預防措施。
- 自事故發生以來，已進行的檢討工作（例如，針對貴公司及客戶所造成的傷害）。
- 對日常工作流程或業務營運的任何變動，以避免同類事件再次發生。
- 如果事故是外判資料處理者或服務供應商的過失，則負責部門是否已檢討日後為同類工作委聘資料處理者的程序及準則，以及貴公司會否終止該資料處理者的合約。

5 對外判資料處理者的合約管理

如閣下須外聘服務供應商（資料處理者）代貴公司處理個人資料，我們建議閣下採取合約規範方法，以防止資料處理者未經准許或意外地查閱、處理、刪除、遺失或使用有關個人資料。我們亦建議閣下採取相同方法，以防止任何轉移予資料處理者的個人資料被保存超出處理所需的時間。

以下是一些可加於與資料處理者簽訂的服務合約的資料保安規定例子：

- 資料處理者須採取的保安措施以保障有關個人資料，並規定資料處理者須遵守條例中的保障資料原則。
- 適時交還、銷毀或刪除不再需要用於貴公司所委託用途的個人資料。
- 資料處理者不得將有關個人資料用於有關服務合約規定以外的用途（包括在未得貴公司的同意下向第三方披露有關個人資料）。
- 除非資料處理者已取得貴公司的事先同意，否則不得將所委託的服務外判。
- 立即向貴公司報告任何資料外洩事故，並採取適當的補救行動。
- 資料處理者必須制訂保障個人資料的政策及程序，並向員工提供相關培訓。
- 資料處理者須就違反任何保障資料的責任向貴公司作出賠償。

附錄一

條例的六項保障資料原則

六項保障資料原則載於條例之附表1，概述如下：

第1 原則- 收集個人資料的目的及方式

個人資料必須為合法目的而收集。收集的目的必須直接與資料使用者的職能或活動有關。就該目的而言，資料屬足夠但不超乎適度。

凡從某人就特定目的收集個人資料，而該人是資料當事人，他須獲告知以下資料：

- 該資料將會用於甚麼目的；
- 該資料可能移轉予甚麼類別的人；
- 資料當事人有責任提供該資料抑或是可自願提供該資料；
- 資料當事人若不提供該資料便會承受的後果；及
- 資料當事人要求查閱其資料及要求改正資料的權利。

資料使用者可向有關資料當事人提供一份《收集個人資料聲明》，以涵蓋上述須告知資料當事人的資料。

第2 原則- 個人資料的準確性及保留期間

資料使用者須採取所有切實可行的步驟，以確保所持有的資料是準確及最新的。保留資料的時間不應超過為達到收集資料的目的所需的時間。

如果資料使用者聘用資料處理者（例如外判服務供應商）代為處理個人資料，則應採取合約規範方法或其他方法，確保其聘用的資料處理者不會將資料保留超過所需的時間。

第3 原則- 個人資料的使用

除非有關資料當事人已給予資料使用者訂明同意，否則個人資料不得用於收集資料時所述目的以外的其他目的（或直接有關的目的）。訂明同意指資料當事人自願給予的明確同意。

附錄一（續）

第4 原則- 個人資料的保安

資料使用者必須採取妥善的保安措施，以確保他們所收集的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除或使用。如資料使用者聘用資料處理者（例如外判服務供應商）代為處理個人資料，則應採取合約規範方法或其他方法，確保其聘用的資料處理者亦會遵守上述資料保安規定。

第5 原則- 資訊須在一般情況下可提供

資料使用者處理個人資料的政策及實務必須具透明性。他們可制訂及發出私隱政策聲明，當中可概括列出所收集個人資料的種類、收集目的、準確性、保存期限、所採取的保安措施，以及資料當事人提出查閱資料及改正資料要求的途徑。

第6 原則- 查閱個人資料

資料當事人有權查詢資料使用者是否持有其任何個人資料，並要求索取該等個人資料的副本。如資料當事人發現所載資料不準確，他可進一步要求資料使用者改正資料紀錄。

資料使用者須於40日法定期限內依從查閱及改正資料要求。如果資料使用者拒絕有關要求，亦須於40日內回覆，說明拒絕的理由。

違反保障資料原則

如資料使用者違反保障資料原則，私隱專員公署可能會發出執行通知，強制資料使用者採取相關補救行動 。未有遵從私隱專員公署發出的執行通知即屬犯罪。

查閱及改正資料要求亦受條例第17A至25條規管。資料使用者如不依從查閱 / 改正資料要求，亦可能招致刑事責任。

有關上述罪行的資料，請參閱附錄二。

附錄二

關乎違反條例的若干主要罪行

未有遵從執行通知

未有遵從私隱專員公署發出的執行通知即屬犯罪，一經定罪，最高可處罰款50,000港元及監禁2年；如罪行在定罪後持續，可處每日罰款1,000港元。一經再次定罪，最高可處罰款100,000港元及監禁2年；如罪行在定罪後持續，可處每日罰款2,000港元（見條例第50A條）。

拒絕依從查閱及改正資料要求

如未能於40日的法定期限內依從查閱或改正資料要求，最高可處罰款10,000港元（見條例第64A條）。

使用個人資料作直接促銷

違反有關向資料當事人發出通知、獲取資料當事人同意及遵從拒絕服務的規定， 最高可處罰款500,000港元及監禁3年（見條例第35C、35E、35F及35G條）。

披露未經資料使用者同意而取得的個人資料

任何人在以下情況下，即屬觸犯條例第64條的罪行。

i. 披露未經資料使用者同意而取自該資料使用者的某資料當事人的任何個人資料，而該項披露是出於以下意圖：獲取得益（不論是為自己或他人受惠而獲取），或導致該資料當事人蒙受損失（註）； 或

ii. 披露未經資料使用者同意而取自該資料使用者的某資料當事人的任何個人資料，而該項披露（不論其意圖如何）導致該資料當事人蒙受心理傷害。

（註：不僅為金錢上的「得益」或「損失」，亦包括其他財產 / 資產的得益或損失。）

關於第(i)項的例子是，有僱員盜竊僱主的客戶個人資料，並將這些資料出售給另一人以獲取報酬；關於第(ii)項的例子是，有僱員從公司的資料庫中竊取同事的個人資料，然後公開這些資料以進行報復。上述罪行的最高刑罰是罰款1,000,000港元及監禁5年。

附錄三

歐洲聯盟《通用數據保障條例》簡介

《通用數據保障條例》（於2018年5月生效）具有域外應用效力，這表示即使貴公司並非在歐盟成員國成立，但在若干前提下，貴公司亦可能需要遵從《通用數據保障條例》的規定。

《通用數據保障條例》第3(2)條規定：

如果由並非在歐盟成立的資料控制者或處理者處理在歐盟內的資料當事人的個人資料，而有關處理活動關乎以下各項，《通用數據保障條例》則適用：

(a) 向該等在歐盟內的資料當事人提供貨品或服務（不論資料當事人是否需付款）；或

(b) 監察他們的行為（只要該等資料當事人的行為在歐盟內進行）。

換言之，如一間公司並非在歐盟成立，但它 (i)收集身處歐盟成員國的資料當事人的個人資料；及(ii)提供以歐盟市場為目標的貨品或服務，或者監察資料當事人在歐盟成員國內進行的行為，該公司仍可能受《通用數據保障條例》所規管。

《通用數據保障條例》的若干主要規定

閣下務請注意，以下為對《通用數據保障條例》所規管公司的若干主要規定，但並無詳盡羅列。如需了解更多，請徵詢法律意見。

- 問責：資料使用者須實施技術性及內部管控措施以確保循規（例如，制訂妥善的保障資料政策、為高風險項目進行資料保障影響評估）

- 通報資料外洩事故：當發生資料外洩事故後，資料使用者須於得悉事件後72小時內，向相關資料保障監管機構通報該事故，惟豁免條文適用者除外。對於會構成高風險的事故，資料使用者亦須通知受影響的資料當事人。

附錄三（續）

《通用數據保障條例》的若干主要規定（續）

- 敏感個人資料：根據《通用數據保障條例》，有關類別包括種族、政治意見、宗教信仰、工會會籍、生物辨識資料及健康資料等個人資料。根據規定，敏感個人資料只可在特定情況下處理（例如，資料當事人已明確同意貴公司就特定目的處理他們的資料；為了就業及社會保障目的，有關處理屬必需的；或為了公眾健康方面的公眾利益，有關處理屬必需的）。

- 事先同意：資料使用者在收集資料當事人的個人資料時，需要事先取得資料當事人的同意，除非有關資料將用於某些規定目的（例如，為履行法律責任或為履行合約而需要處理資料）。

- 被遺忘權：資料當事人在指定情況下有權要求資料使用者刪除其個人資料，例如，就當初收集資料的目的而言，有關個人資料已不再需要，或有關個人資料被資料使用者不合法地處理。

- 懲罰：相關資料保障監管機構可對資料使用者處以行政罰款（即最高2,000萬歐元，或有關違規公司之全球年度營業額的4%，以較高者為準）。

需要個人資料私隱諮詢服務?
立信德豪樂意為您提供協助

管理服務
- 個人權限管理
- 私隱措施設計及管理
- 私隱管控能力成熟程度評估
- 私隱風險監管
- 資料保護專員（Data Protection Officer）服務支援

評估
- 個人資料私隱措施的整備情況評估
- 個人資料私隱措施的審計/盡職調查
- 年度私隱措施評估
- 資料處理流程核實及圖像化
- 資料保護鑒證/認證

實施與補救措施
- 個人資料私隱策略和實施
- 私隱項目管理
- 製定私隱政策聲明，及內部私隱政策和程序指引文件
- 實施管控措施
- 涉及第三方資料處理者的監管補救措施
- 制定有關減少資料蒐集、資料保留、刪除和分類的策略和流程

技術支援
- 設計和審查規劃中和現有的私隱處理措施架構
- 進行私隱影響評估
- 資料當事人的權利管理
- 個人資料私隱管理工具的選擇、設計和採用
- 資料掩蔽和資料加密工具
- 安全評估：漏洞掃描，滲透測試，道德駭客和社交工程

其他支援
- 提供有關處理資料當事人要求和資料洩露的建議
- 提供與第三方的合同安排建議
- 協助建立有關國際資料傳輸的政策和登記冊

聯繫我們

如有任何疑問、意見或建議，請與我們聯繫。如欲了解有關BDO風險諮詢服務的更多資訊，請瀏覽：

www.bdo.com.hk/en-gb/services/advisory/risk-advisory

鄭文漢
香港立信德豪董事兼風險諮詢服務總監
rickycheng@bdo.com.hk

彭兆楷
香港立信德豪董事
peterpang@bdo.com.hk

www.bdo.com.hk

BDO Limited 香港立信德豪 BDO Limited 香港立信德豪