「應對網絡安全威脅及資料外洩事故」講座

2024年3月19日

如何應對資料外洩事故及提升數據安全

郭正熙先生

首席個人資料主任（合規及查詢）

資料外洩事故

甚麼是資料外洩事故?

一般指**資料使用者**持有的個人資料懷疑或已經遭到外洩，令有關資料當事人的個人資料有被**未獲准許的或意外的查閱、處理、刪除、喪失或使用的風險**

例子

- **遺失**載有個人資料的可攜式裝置
- **不當處理**個人資料
- 載有個人資料的資料**系統被非法侵入**或**被未經授權的第三方查閱**
- 第三方以**欺騙手法**從資料使用者取得個人資料
- 在電腦**安裝檔案分享軟件**而導致資料外洩

《私隱條例》的相關規定

保障資料第4(1)原則

資料使用者須**採取所有切實可行的步驟**，確保由資料使用者持有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、喪失或使用所影響

保障資料第4(2)原則

如資料使用者聘用（不論是在香港或香港以外聘用）**資料處理者**，以代該資料使用者處理個人資料，該資料使用者須採取**合約規範方法**或其他方法，以防止轉移予該資料使用者作處理的個人資料被未獲准許或意外地被查閱、處理、刪除、喪失或使用

資料外洩事故可構成違反《私隱條例》 附表1的保障資料第4原則

常見的資料外洩事故種類

1. 網絡攻擊
2. 系統配置錯誤
3. 遺失實體文件或便攜式裝置
4. 不當或錯誤棄置個人資料
5. 經電郵或郵件的無意披露
6. 職員疏忽或行為不當

資料外洩事故應變計劃

載列機構一旦發生資料外洩時會**如何應對的文件**

有助機構快速應對及有效管理事故

資料外洩事故應變計劃應：

① 概述發生事故後**須執行的程序**

② 資料使用者由事故開始到完結就**識別**、**遏止**、**評估**以至**管理**事故所帶來的影響的策略

資料外洩事故應變計劃

計劃涵蓋範疇（非詳盡）

- 描述構成資料外洩事故的要素
- 內部事故通報程序
- 指明專責應變小組成員的角色及責任
- 聯絡名單
- 風險評估工作流程
- 遏止策略
- 通訊計劃
- 調查程序
- 保存紀錄的政策
- 事後檢討機制
- 培訓或演習

如何處理資料外洩事故？

處理資料外洩事故的步驟

1. 立即收集重要資料
2. 遏止事件擴大
3. 評估事件可造成的損害
4. 考慮作出資料外洩通報
5. 記錄事故

指引資料

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

PCPD.org.hk

資料外洩事故的處理及通報指引

引言

良好的資料外洩事故處理作為營商之道

採取良好的資料外洩事故處理政策及措施不但能協助資料使用者減低外洩事故所帶來的損害，還能透過有關資料使用者處理外洩事故以及訂立清晰的後續行動方案，展現其願意承擔責任的精神。另一方面，作出資料外洩通報除了能協助受影響的資料當事人採取適當的應對保護措施，亦有助有關資料使用者減低訴訟風險和維持其商譽及生意關係，而在個別情況下，甚至能保持公眾對有關機構的信心。

本指引旨在協助資料使用者準備及處理資料外洩事故，以防止類似事件再次發生，從而減低對有關資料當事人所帶來的損失和損害，特別是當外洩事故涉及敏感個人資料。

甚麼是個人資料？

資料外洩事故通常涉及個人（例如機構的顧客、服務使用者、僱員及求職者）的個人資料。根據《個人資料（私隱）條例》（香港法例第486章）（《私隱條例》），個人資料指符合以下說明的任何資料[1]—

(a) 直接或間接與一名在世的個人有關的；

(b) 從該資料直接或間接地確定有關的個人的身分是切實可行的；及

(c) 該資料的存在形式令予以查閱及處理均是切實可行的。

甚麼是資料外洩事故？

資料外洩事故一般指資料使用者[2]持有的個人資料懷疑或已經遭到外洩，令有關資料當事人的個人資料有被未獲准許的或意外的查閱、處理、刪除、喪失或使用的風險。

一些資料外洩事故的例子包括：

- 遺失載有個人資料的可攜式裝置，例如手提電腦、USB儲存裝置、可攜式影碟或後備磁帶
- 不當處理個人資料，例如不當地棄置、把電郵發送予非指定的收件人或被未經授權的職員查閱資料系統
- 資料使用者載有個人資料的資料系統被非法侵入或被未經授權的第三方查閱
- 第三方以欺騙手法從資料使用者取得個人資料
- 在電腦安裝檔案分享軟件而導致資料外洩

資料外洩事故可構成違反《私隱條例》附表1的**保障資料第4(1)及(2)原則**。**保障資料第4(1)原則**規定資料使用者須採取所有切實可行的步驟，確保由資料使用者持有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、喪失或使用所影響，尤其須考慮—

1 《私隱條例》第2(1)條。

2 根據《私隱條例》第2(1)條，「資料使用者」，就個人資料而言，指獨自或聯同其他人或與其他人共同控制該資料的收集、持有、處理或使用的人。

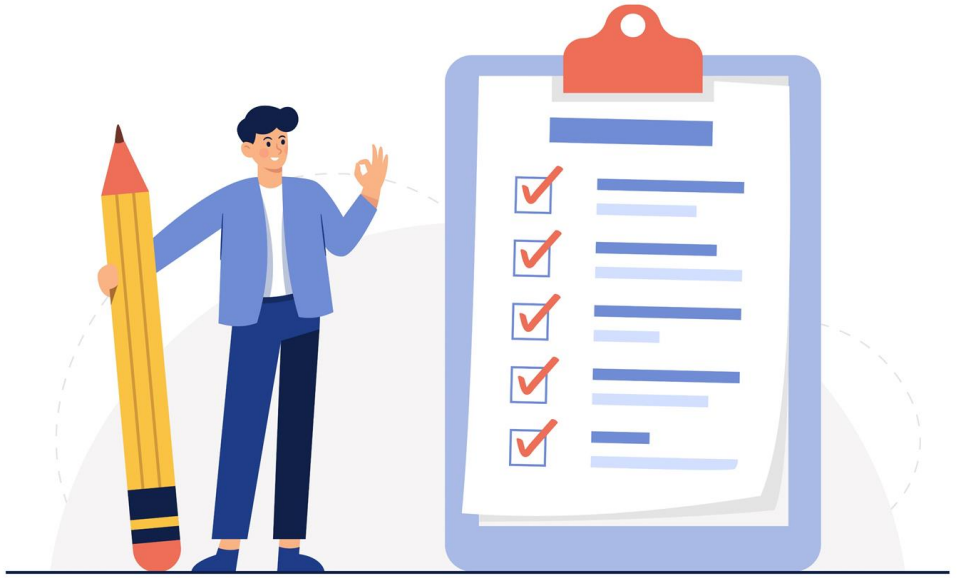
資料外洩事故的處理及通報指引 1 2023年6月

下載《資料外洩事故的處理及通報指引》

步驟 1：立即收集重要資料

收集事故的所有相關資料，以評估對資料當事人的影響及找出適當的緩和措施：—

- 事故於**何時**發生及在**哪裏**發生？
- 事故**如何被發現**及由**誰人發現**？
- 導致事故的**原因**是甚麼？
- 涉及**甚麼種類**的個人資料？
- **有多少個**可能受影響的資料當事人？
- 可能對受影響人士造成甚麼**傷害**？



步驟 2：遏止事件擴大

視乎所涉及個人資料的類別及事故的嚴重性，考慮採取以下的遏止措施：

- **徹底搜尋**載有個人資料的遺失物品
- 要求錯誤接收有關電郵 / 信件 / 傳真的人士**銷毀或交回誤發的文件**
- **關閉或隔離**受損 / 遭破壞的系統 / 伺服器
- **修復**導致事故的**漏洞或錯誤**
- **更改用戶密碼及系統配置**
- **移除**涉嫌造成或引致資料外洩的**用戶的查閱權**
- 如已發生或可能發生身份盜竊或其他犯罪活動，應通知有關執法部門

步驟 3：評估事件可造成的損害

資料外洩事故可導致的損害：

- 人身安全受到威脅
- 身份盜竊
- 財務損失
- 受辱或喪失尊嚴、名譽或關係受損
- 失去生意或聘用機會

傷害程度取決於不同情況，例如:

- 外洩個人資料的**種類**、**敏感程度**及**數量**
- 資料外洩的情況
- 傷害的性質
- **身份盜竊**或**詐騙**的可能性
- 遺失的資料**有否備份**
- 外洩資料有否進行足夠的**加密**、**匿名化**或其他保障措施
- 資料外洩**持續的時間**

步驟 4：考慮作出資料外洩通報

資料使用者在決定是否把事故通知受影響資料當事人、私隱專員公署及其他執法部門時，應考慮：

- 事故可能對受影響人士造成的影響
- 影響有多嚴重或重大
- 發生的可能性
- 不作出通知的後果

如資料外洩事故相當可能對受影響資料當事人有構成實質傷害的風險，資料使用者應在知道發生資料外洩後在切實可行的情況下盡快通知私隱專員公署及受影響資料當事人。

步驟 5：記錄事故

- 資料使用者必須**完整地記錄事故**，包括事故的**詳情**、**影響**，**資料使用者所採取的遏止措施和補救行動**
- 機構如須依從其他司法管轄區的法例及規例，亦應留意有關法例及規例下的**強制記錄要求**
- **檢討資料外洩事故，從中汲取教訓，改善其處理個人資料的做法。**

NOTE

例如歐洲聯盟的《通用數據保障條例》規定資料控制者記錄所有資料外洩事故並保存有關紀錄

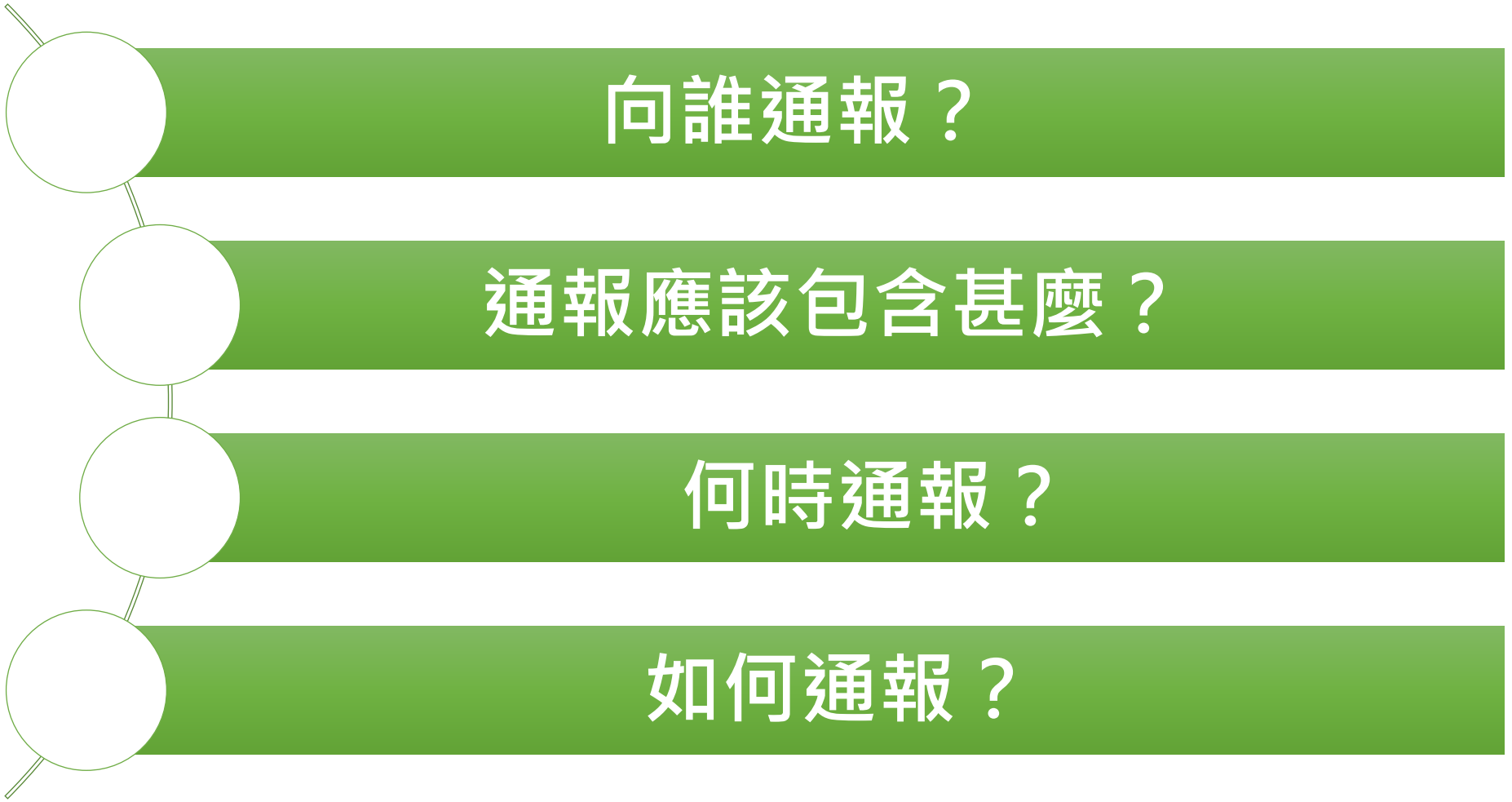
資料外洩通報

資料外洩通報

好處

- ✓ 告知受影響資料當事人**宜主動採取步驟或措施**，以**減低潛在的傷害或損害**
- ✓ 讓相關機構採取適當的**調查**或**跟進行動**
- ✓ 顯示資料使用者決意依從具透明度及負責任的原則，作出妥善的個人資料私隱管理
- ✓ **提高公眾的警覺性**
- ✓ 從私隱專員公署取得適當的意見，以迅速應對事故及改善其處理個人資料的系統及政策，**防止同類事故再次發生**

資料外洩通報



資料外洩通報

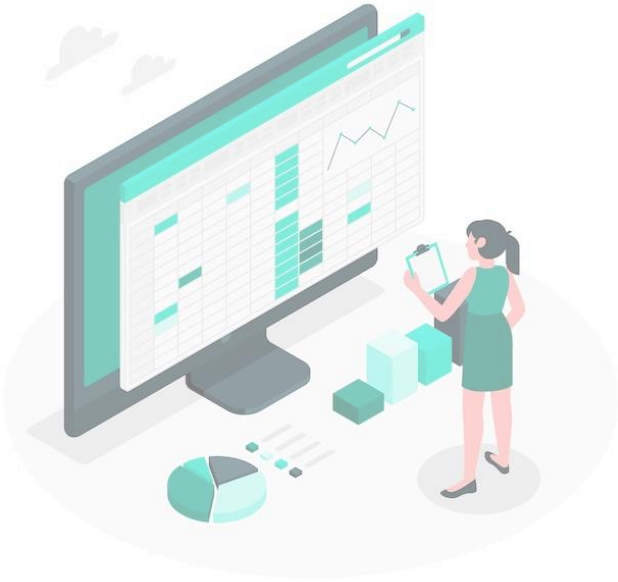
向誰通報?

- **受影響的資料當事人**
- **私隱專員公署**
- 私隱專員公署以外的執法機構
- 其他相關規管機構
- 其他能採取補救行動以保護個人資料私隱和受影響的資料當事人的權益的相關人士（例如：互聯網公司）

資料外洩通報

通報應該包含甚麼？

- 事件的概況
- 外洩的**源頭**、**日期及時間**，及估計或確實的持續時間
- 發現事故的日期及時間
- 所涉及的**個人資料類別**
- 所涉及的**資料當事人**的類別及大約**數目**
- 對事故導致的損害作出的**風險評估**
- 已**採取或將會採取的緩解措施**
- 專責應變小組或負責處理事故的指定職員的**聯絡資料**



資料外洩通報

何時通報?

- **在知悉事故後，不論內部調查的進度如何，在切實可行的情況下盡快作出通報**
- 如未能提供事故的詳情，最好盡量提供所有已掌握的資訊

NOTE

- **由於其他司法管轄區可能有指定的通報時限，如資料使用者須向海外的規管機構作出通報，有需要時應尋求專業意見，確保根據相關規定在法定時限內作出通報**

資料外洩通報

如何通報？

通知資料當事人

- 透過電話、書面、電郵或親身向資料當事人作出通報
- 如直接的資料外洩通報不切實可行，可發出公告、報章廣告，或於網站或社交媒體平台發出帖文

通知私隱專員公署

- 經私隱專員公署**網頁**、傳真、親身或郵寄方式遞交「**資料外洩事故通報表格**」
- **不接受口頭通報**

NOTE

不論資料使用者有否作出通報，公署可就資料外洩事故展開調查。

資料外洩事故通報表格

資料外洩事故一般指資料使用者持有的個人資料外洩，令此等資料承受未獲准許的或意外的查閱、處理、刪除、遺失或使用的風險。視乎個案的情況而定，資料外洩事故可構成違反《個人資料（私隱）條例》（《私隱條例》）的保障資料第 4 原則。

雖然《私隱條例》沒有規定資料使用者必須就資料外洩事故作出通報，但個人資料私隱專員公署（私隱公署）建議資料使用者在資料外洩發生後盡快向私隱公署、受影響資料當事人及相關機構作出通報。

資料使用者可使用此通報表格向私隱公署通報資料外洩事故，需時大約 10-15 分鐘。你可參考私隱公署的「處理資料外洩事故的實務建議」（見附錄）以獲取更多資訊。

收集個人資料聲明

請注意，你可自願向私隱公署提供你的個人資料。你提供的所有個人資料只會用於與是次資料外洩事故通報及個人資料私隱專員行使規管權力及職能直接有關的用途。

你有權要求查閱及改正私隱公署所持有你的個人資料。查閱或改正該等資料，可用書面向保障資料主任提出，地址為香港灣仔皇后大道東 248 號大新金融中心 12 樓。

你所提供的個人資料可能轉移給私隱公署因處理本個案而接觸的人士或機構，包括獲授權收取有關資料以作出執法或起訴行動的人士或機構。

❑ 本人明白上述內容，並代表資料使用者提交資料外洩事故通報。*

*必須填寫　*請圈出適用者

資料使用者的基本資料

資料使用者機構：❑ 私營機構　❑ 公營機構

公司／機構名稱*：

香港辦事處的聯絡地址：

聯絡人資料

作出此通報的人士的姓名*：

職位：　電郵地址*：

國家編號（非香港電話號碼）：

聯絡電話號碼*：

你是否你所屬公司／機構的資料保障主任？* 是／否

1

公署的「資料外洩事故通報表格」

汲取教訓：防止資料外洩事故再次發生

資料使用者應從事故汲取教訓、檢討處理個人資料的方式，以找出問題根源，並制訂清晰的政策，以防止類似事故再次發生

資料保安建議措施

《資訊及通訊科技的保安措施指引》

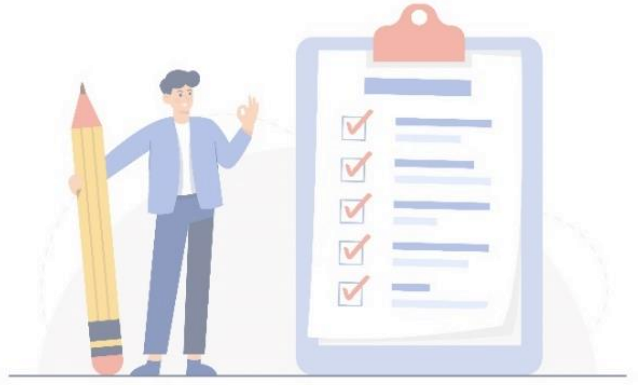
1. 資料管治和機構性措施
2. 風險評估
3. 技術上及操作上的保安措施
4. 資料處理者的管理
5. 資料保安事故發生後的補救措施
6. 監察、評估及改善
7. 其他考慮

下載《資訊及通訊科技的保安措施指引》

資訊及通訊科技的資料保安建議措施

1) 資料管治和機構性措施

- 資料使用者應制訂明確針對**資料管治**和**資料保安**的**內部政策**和**程序**
- 資料使用者應**委任合適的領導人物**負責個人資料保安（如首席資料官、首席私隱官等）、提供適當的人手配置及制訂指引
- 工作人員應在入職時及往後**定期接受足夠培訓**



NOTE

資料使用者應根據當時情況（如行業內的新標準、資料保安新威脅等），定期和及時地覆檢與修訂政策及程序，並機構可考慮將「演習」納入資料保安培訓（例如模擬的網絡騙案），以提高員工的警覺程度。

資訊及通訊科技的資料保安建議措施

NOTE

風險評估的結果應定期向高級管理層匯報，而發現的保安風險亦應及時處理。

2) 風險評估

資料使用者應:

- 在啟用新系統和新應用程式前，以及在啟用後**定期進行資料保安風險評估**
- 就控制的個人資料**備存清單**，並評估有關資料的性質，以及它們被洩露的潛在損害
- 在收集敏感資料前作慎重考慮，確保**只收集必要的資料並提供更穩妥的保障**（例如以加密的形式儲存在獨立安全的資料庫中）

資訊及通訊科技的資料保安建議措施

3) 技術上及操作上的保安措施

- 保護電腦網絡
- 資料庫管理
- 存取管控
- 電郵及檔案傳送
- 防火牆和反惡意軟件
- 保護網絡應用程式
- 加密
- 資料備份、銷毀及匿名化

資訊及通訊科技的資料保安建議措施

4) 資料處理者的管理

NOTE

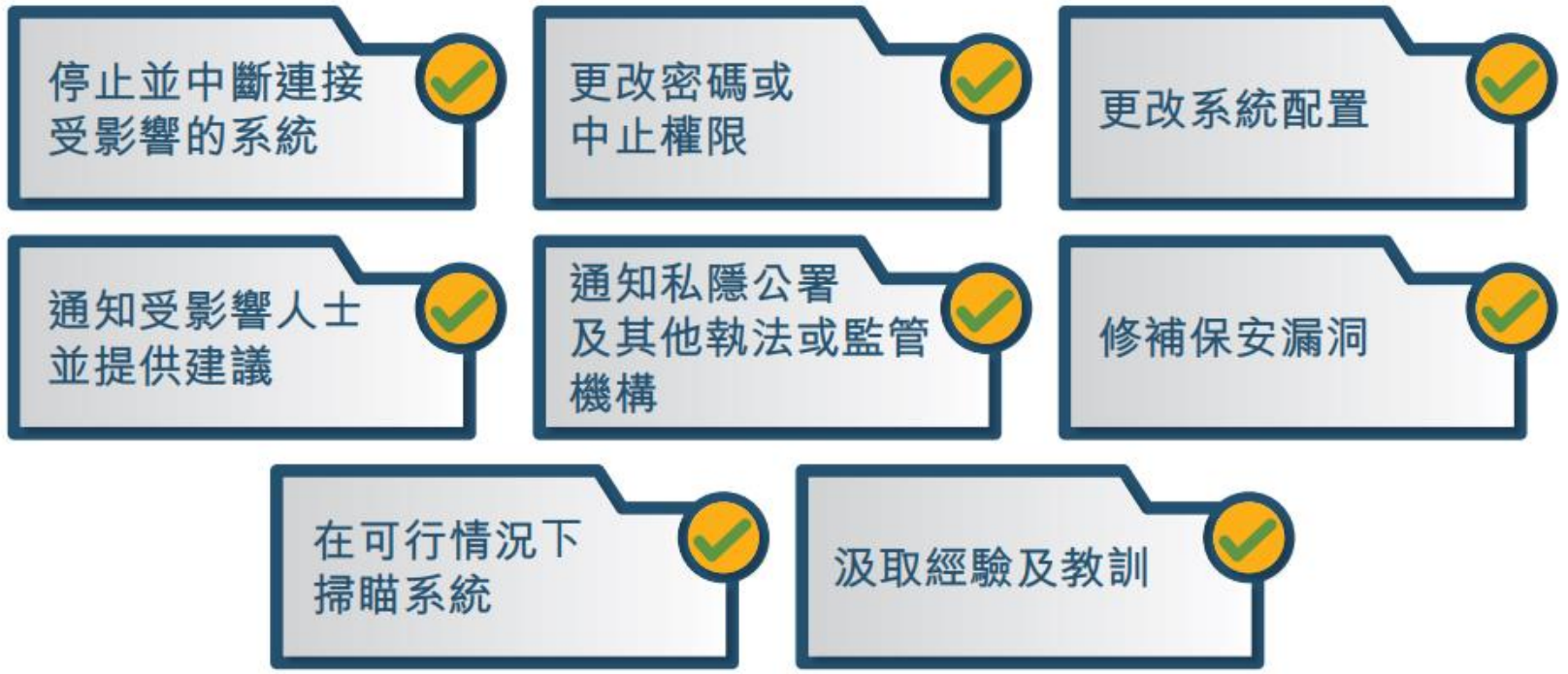
根據《私隱條例》第65(2)條，資料使用者有可能需對其代理人（包括資料處理者）的有關行為負責

有關管理資料處理者的更多資訊，可參閱私隱公署的《外判個人資料的處理予資料處理者》資料單張

資訊及通訊科技的資料保安建議措施

5) 資料保安事故發生後的補救措施

資料使用者在資料保安事故發生時可採取的補救措施:



NOTE

資料使用者亦應從資料保安事故中汲取經驗及教訓，覆檢和加強其整體資料治理和資料保安措施。

有關如何處理資料外洩的詳細指引，可參閱私隱公署發出的《資料外洩事故的處理及通報指引》

資訊及通訊科技的資料保安建議措施

NOTE

如發現違反政策的行為或保安措施成效不彰，應採取改善行動

6) 監察、評估及改善

資料使用者可委派獨立的專責小組（如內部或外部審計隊），並負責:

- 定期**監察**資料保安政策的**遵從情況**
- 定期**評估**資料保安措施的**成效**

資訊及通訊科技的資料保安建議措施

7) 其他考慮 — 雲端服務及自攜裝置

雲端服務

- 檢視雲端的現有保安功能及評估雲端服務供應商的能力
- 設立穩固的查閱管控和認證程序

自攜裝置

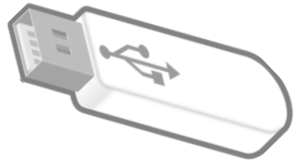
- 控制對儲存在自攜裝置設備內的個人資料的存取
- 使用並非自攜裝置設備內建的加密方法及安裝適合的軟件

便攜式儲存裝置

如有必要使用便攜式儲存裝置，應：

- 制訂政策
- 使用端點保安軟件
- 保存便攜式儲存裝置的清單使用
- 使用後妥善地刪除便攜式儲存裝置的資料

有關使用便攜式儲存裝置的詳細指引，請參閱私隱公署發出的《使用便攜式儲存裝置指引》



數據安全快測

- 讓企業及機構就**其資訊及通訊科技系統的資料保安措施**是否足夠進行快捷方便的**自我評估**
- 共有**12條**問題，需時大概**15分鐘**
- 當提交答案後，系統會發出一份報告，提供有關機構的**資料保安風險水平概覽**以及**具體的建議**以供參考和跟進

立即進行
「數據安全快測」

Thank you!

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

☎ 2827 2827

2877 7026

www.pcpd.org.hk

@ communications@pcpd.org.hk

香港灣仔皇后大道東248號大新金融中心13樓1303室