
投入選舉 共創未來
Join the Election Together We Create the Future
2025 立法會換屆選舉
Legislative Council General Election
12月7日
7 DEC
齊投票！
投票箱
Ballot Box
投票箱
Ballot Box
投票箱
Ballot Box
elections.gov.hk
2891 1001

私隱專員公署+生產力局 中小企數據安全培訓系列

# 「中小企如何應對資料外洩事故」研討會

2025年11月12日（星期三）| 下午3:00至4:15

**譚嘉榮先生**
私隱專員公署
署理高級個人資料主任
（資訊科技）

**陳仲文工程師**
生產力局
網絡安全及數碼轉型部
總經理

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

hkpc 生產力局

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

# 「中小企如何應對資料外洩事故」研討會

譚嘉榮
署理高級個人資料主任（資訊科技）

2025年11月12日

# 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
- 載有個人資料的資訊**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

## 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

***保障資料第4(1)原則***

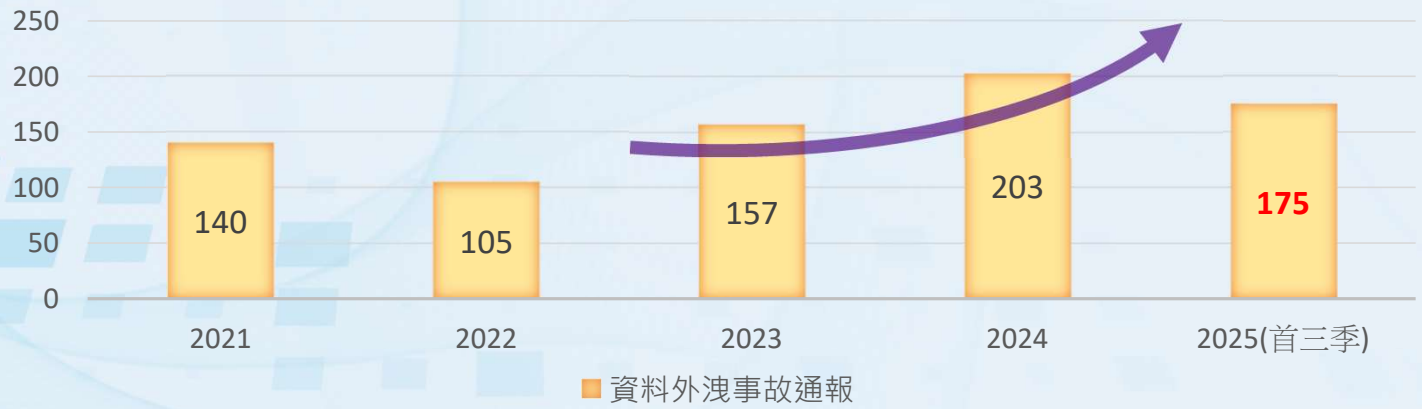
資料使用者須**採取所有切實可行的步驟**，確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響

***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處理者作處理的個人資料被未獲准許或意外地查閱、處理、刪除、喪失或使用

# 公署接獲的資料外洩事故通報

- 私隱專員公署於2025年首三季共接獲175宗資料外洩事故通報




- 在2024年接獲的資料外洩事故通報中，61宗涉及黑客入侵，佔整體資料外洩事故通報的30%
- 在2025年首三季接獲的資料外洩事故通報中，61宗涉及黑客入侵，佔整體資料外洩事故通報的35%

# 個案分享(一)

# 事件背景

零售商A向會員寄發優惠訊息電郵時意外披露其他會員的電郵地址

- 事件源於一間零售商向會員寄發優惠訊息電郵時，將**全體會員的電郵地址錯誤填寫在「收件人」欄目**，引致收件人看到其他逾千名會員的電郵地址

- 事件肇因是一名職員發出電郵時，錯誤將所有會員的電郵地址填寫在「收件人」一欄

# 糾正錯誤

- 事件發生後，該公司向所有涉事會員發出道歉信，要求客戶注意錯發的電郵並刪除涉事電郵
- 經私隱專員公署介入後，該公司已就電郵發送作出糾正措施，每當員工發送電郵至兩個或以上公司以外人士的電郵地址時，系統會自動以密件副本（即b.c.c.）功能發送電郵，讓除收件人自己以外的其他電郵地址均被隱藏
- 該公司亦發出通告提醒所有員工正確使用發送電郵的密件副本（即b.c.c.）功能

# 個案分享(二)

# 事件背景

珠寶公司B向私隱專員公署通報資料外洩事故，表示其資訊系統出現異常，並收到黑客的訊息指儲存於其系統內的資料已被盜取。經檢查後，珠寶公司B確認儲存於資料庫伺服器的資料已被黑客盜取及刪除（外洩事件）。

涉及的個人資料包括該公司客戶及員工的姓名、香港身份證號碼、電話號碼等

# 調查結果

- 黑客透過**暴力攻擊**取得一個具系統管理員權限的帳戶（相關帳戶）的**帳戶憑證**
- 黑客利用相關帳戶取得進入珠寶公司B的資訊系統的訪問權限後，在資訊系統**進行橫向移動**，包括於一台用於內部系統開發及編程的桌上電腦**注入木馬程式**，繼而獲取能**操控資料庫伺服器的原始程式碼**，並成功盜取及刪除儲存在內的個人資料

# 調查結果

| | |
|---|---|
| 1. 未有適時刪除離職員工帳戶 | 相關帳戶在事發時不僅閒置超過13年，且未有啟用多重認證及帳戶鎖定功能，黑客最終利用相關帳戶入侵珠寶公司B資訊系統並盜取及刪除儲存於資料庫伺服器的個人資料 |
| 2. 資訊系統欠缺有效的保安及偵測措施 | 珠寶公司B配置的防火牆及防毒軟件屬已過時的版本，未能有效抵禦是次的黑客攻擊，而他們亦沒有設定能有效實時或定期監察資訊系統活動的其他防禦措施 |
| 3. 伺服器的作業系統已過時 | 受外洩事件影響的資料庫伺服器的作業系統並非最新版本，供應商已終止支援相關作業系統達四年之久<br><br>珠寶公司B在外洩事件前既未有適時更新資料庫伺服器的作業系統，亦未有採取任何額外的防護措施 |
| 4. 欠缺資訊保安政策及指引 | 珠寶公司B未有在系統保安、帳戶管理、密碼要求、活動偵測及系統更新方面制訂書面政策或指引供員工依循，亦未備有資料保安事故的應變計劃和通報機制 |
| 5. 未有對資訊系統進行保安評估及審計 | 珠寶公司B在外洩事件發生前未曾對資訊系統進行任何形式的保安評估及審計，以識別潛在的資訊保安風險 |

# 個案分享(三)

# 事件背景

- 零售公司C向私隱專員公署通報資料外洩事故，表示其資訊系統平台遭受未獲授權的第三方入侵，導致該公司客戶的個人資料被竊取
- 調查發現，受影響平台由第三方供應商（該平台供應商）提供，以軟件即服務（Software-as-a-Service）方式運作
- 黑客利用一名現職員工的管理員帳戶的帳戶憑證，從一個不明的海外 IP 位址連接至受影響平台，繼而下載儲存於當中的訂單資料
- 涉及的個人資料包括客戶的姓名、電話號碼、及訂單資料

# 調查結果

| | |
|---|---|
| 1. 薄弱的密碼管理 | 受影響平台中所有用戶的密碼都只是六位數字的簡單組合，且在零售公司C外洩事件發生前兩年未曾更改。儘管該平台供應商提供多項可套用於受影響平台的密碼管理措施，包括密碼的最短長度及複雜程度，及密碼自動過期的設定，以及帳戶在多次登入失敗後自動鎖定的功能。然而，零售公司C未有啟用這些可供使用的密碼管理措施 |
| 2. 未有為存取帳戶啟用多重認證功能 | 儘管該平台供應商已於受影響平台提供多重認證功能，惟零售公司C未有在外洩事件發生時為其任何用戶帳戶啟用相關功能，包括遭入侵的管理員帳戶 |
| 3. 缺乏保障個人資料的意識 | 該平台供應商為受影響平台提供一系列的保安措施，包括密碼管理措施、多重認證功能、監察登入及限制IP位址連接的功能，但零售公司C在外洩事件發生時沒有啟用上述任何一項可供使用的保安措施 |
| 4. 未有對受影響平台進行適當的保安檢視 | 雖然該平台供應商會定期為受影響平台進行針對其基礎架構的保安檢視，但零售公司C在外洩事件發生前未有從服務使用者的角度對受影響平台進行任何保安檢視 |

# 有關個人資料保安的建議

- 上述兩宗資料外洩事件都涉及持有大量客戶個人資料的零售業機構，而其中一宗更有證據明確顯示客戶資料外洩後在「暗網」公開，可見資料外洩個案與個人資料被販賣圖利，以及個人資料被騙徒使用於形形色色的詐騙活動不無關係

- 面對與日俱增的網絡安全威脅，機構應視其所持有的個人資料為重要資產，投放足夠資源於網絡保安及數據安全，從而保障所持有的個人資料，以符合《私隱條例》的規定及資料當事人的合理期望

# 資訊及通訊科技的資料保安建議措施

## 資料保安建議措施 *七大建議措施一覽*

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


下載指引

下載小冊子

# 資料外洩事故處理


下載指引

下載小冊子

# 資料外洩事故處理

## 「事故發生前」－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
- 計劃主要涵蓋範疇包括：外洩事故的**定義**、**通報**程序、應變小組的**角色及責任**、**風險評估**工作流程、**遏止**策略、**調查**程序、**紀錄**政策、事後**檢討**機制、**培訓或演習**計劃等

# 資料外洩事故處理

步驟1
立即收集
重要資料

步驟2
遏止事
件擴大

步驟3
評估事件
可造成的
損害

步驟4
考慮作出
資料外洩
通報

步驟5
記錄事故

# 資料外洩事故處理

## 「事故發生後」－處理資料外洩事故5大步驟

### 步驟 1 ：立即收集重要資料

資料使用者必須**迅速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，包括：

- 事故於**何時及哪裏**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**？

NOTE

**最先發現事故的職員應考慮是否依從資料外洩事故應變計劃所訂的程序向專責應變小組／高級管理層／保障資料主任通報事故**

# 資料外洩事故處理

## 步驟 2：遏止事件擴大

機構可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分盜竊或其他犯罪活動，應**通知有關執法部門**

# 資料外洩事故處理

## 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包括：**

- 人身安全受到威脅
- 身分盜竊
- 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

***因資料外洩而可能蒙受的傷害程度取決於：***

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
- **身分盜竊**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**

# 資料外洩事故處理

## 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**

NOTE

**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**

# 資料外洩事故處理

## 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**

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**

# 資料外洩事故通報

## 如何通報?

### 通知資料當事人

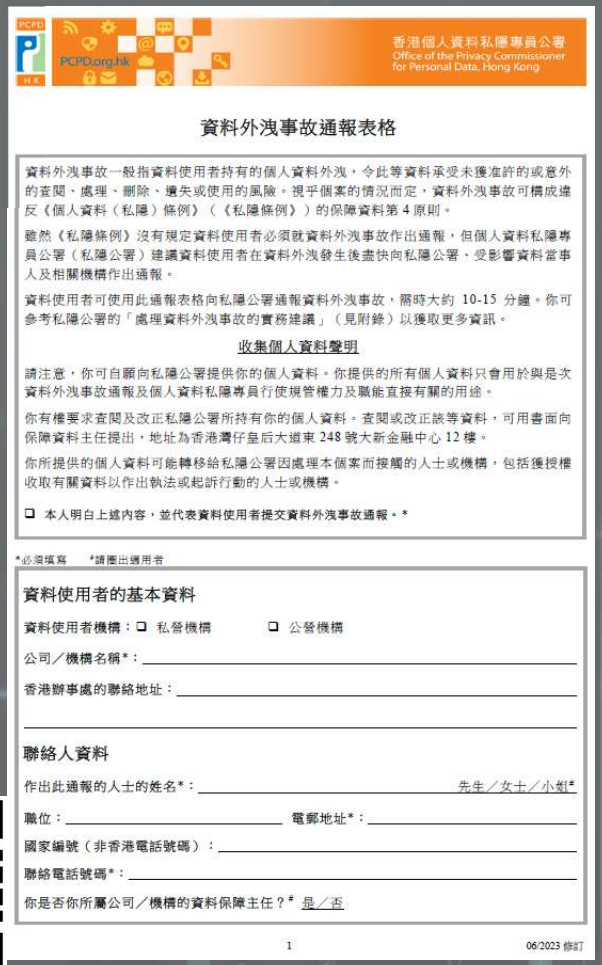
- 透過電話、書面、電郵或親身向資料當事人作出通報
- 如在有關情況下直接的資料外洩通報並不切實可行，可發出公告、報章廣告，或於網站或社交媒體平台發出帖文

### 通知私隱專員公署

- 使用私隱專員公署的「**資料外洩事故通報表格**」
- 經私隱專員公署網頁、傳真、親身或郵寄方式遞交

NOTE

**私隱專員公署並不接受口頭通報。**



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

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*：　先生／女士／小姐#

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　06/2023 修訂

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

# 數據安全熱線
# Data Security Hotline
# 2110 1155

## 數據安全快測
## Data Security Scanner
https://www.pcpd.org.hk/Toolkit/tc/


## 數據安全專題網頁
## Data Security Webpage
https://www.pcpd.org.hk/tc_chi/data_security/index.html

PCPD.org.hk

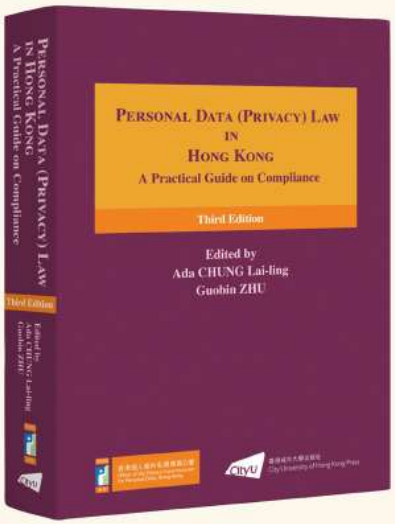
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

# Personal Data (Privacy) Law in Hong Kong

## A Practical Guide on Compliance (Third Edition)

**Ms Ada CHUNG Lai-ling**
Privacy Commissioner for Personal Data, Hong Kong

**Professor ZHU Guobin**
Professor ZHU Guobin
City University of Hong Kong




## Highlights:

- Provisions of the PDPO on combatting doxxing
- Cross-border transfers of personal data from Hong Kong
- The Mainland's personal information protection regime
- Recent decisions by the Administrative Appeals Board and the Court
- PCPD's investigation reports and materials
- Comparison table on the personal data protection laws of Hong Kong, the Mainland and the European Union

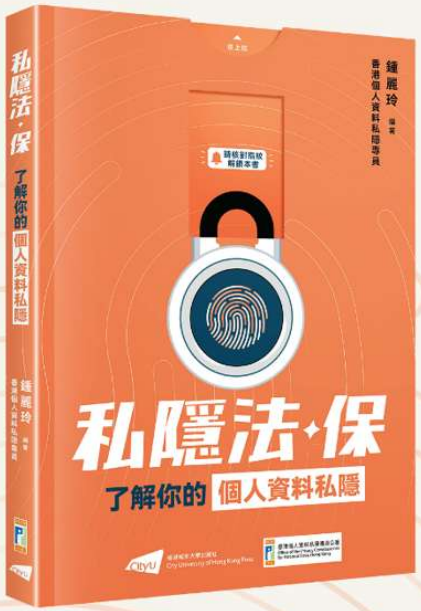
Buy Now

# 《私隱法．保 — 了解你的個人資料私隱》

**鍾麗玲女士**
個人資料私隱專員 編著

## 重點：

- 保障個人資料原則
- 打擊「起底」
- 私隱保障趨勢
  - ♦ 人工智能
  - ♦ 聊天機械人
- 保護私隱精明貼士




**立即購買**


投入選舉 共創未來
Join the Election Together We Create the Future
2025 立法會換屆選舉
Legislative Council General Election
12月7日
7 DEC
齊投票！
投票箱
Ballot Box
投票箱
Ballot Box
投票箱
Ballot Box
elections.gov.hk
2891 1001

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

# 謝謝！Thank you!