從《個人資料（私隱）條例》探索網絡行為的法律責任與合規要求

香港中文大學法學院 - 騰訊研究院網絡法論壇
2025年8月6日

助理個人資料私隱專員（合規、環球事務及研究）
王雅媛女士

大綱

本主旨演講將談及以下範疇

1. 《個人資料（私隱）條例》（《私隱條例》）概覽
2. 打擊「起底」罪行
3. 資料外洩事故
4. 公署在國際及本地層面的工作

定義

個人資料指符合以下說明的任何資料

（《私隱條例》第2(1)條）

直接或間接與一名在世的**個人有關**的

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

該資料的存在形式令予以**查閱及處理**均是**切實可行**的

與誰人有關？

涉及三個類別

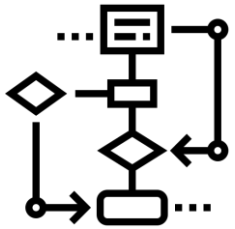
資料當事人

屬該資料的**當事人**的個人

資料使用者

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

資料處理者



指符合以下兩項說明的人

a) **代另一人**處理個人資料；及

b) 並**不**為該人**本身目的**而處理該資料

六項保障資料原則

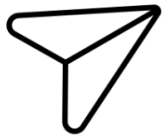
（《私隱條例》附表1）

六項保障資料原則代表**《個人資料（私隱）條例》（《私隱條例》）**的核心規定

涵蓋個人資料由**收集、保存、使用以至銷毀**的整個生命周期

資料使用者**必須遵從**六項保障資料原則

保障資料第1原則
收集個人資料的目的及方式



個人資料是為了**直接與將會使用該資料的資料使用者的職能或活動有關的合法目的**而收集

資料對收集目的而言是**必需及足夠的，但不超乎適度**

收集的方法必須是**合法**和**公平**的

須採取**所有切實可行的步驟，告知**資料當事人他有責任提供該資料抑或是可自願提供個人資料、收集資料的**目的**及該**資料可能移轉予甚麼類別的人**等

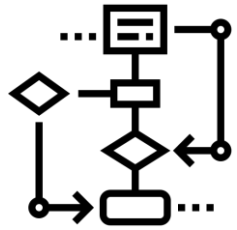
保障資料第2原則
準確性及保留期間

資料使用者

須採取**所有切實可行的步驟**，以確保：

- 個人資料是**準確**的；
- 個人資料的**保存時間不超過**將其保存以貫徹該資料被使用於的目的**所需**的時間

資料處理者

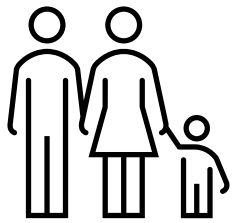


如果聘用**資料處理者**處理個人資料，資料使用者須採取**合約規範或其他方法**，以防止個人資料的保存時間超過處理該資料所需的時間

保障資料第3原則
資料的使用

如無有關的資料當事人的**訂明同意**，個人資料不得用於新目的。

「訂明同意」 指*沒有書面通知撤回的自願給予的明示同意*



資料當事人的有關人士可在某些情況下，代該當事人給予為**新目的**而使用其個人資料所規定的訂明同意。

「新目的」 指*任何原先收集個人資料時擬使用或直接相關的目的以外的*目的。

保障資料第4原則
個人資料的保安

資料使用者須採取**所有切實可行的步驟**，以確保所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

如果聘用**資料處理者**，資料使用者須採取**合約規範或其他方法**，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

保障資料第5原則
透明度

資料使用者須採取所有切實可行的步驟，以確保任何人：

能確定資料使用者在個人資料方面的**政策及實務**

能獲告知資料使用者所持有的**個人資料的種類**

能獲告知資料使用者持有的個人資料是為或將會為甚麼主要**目的**而使用的

保障資料第6原則
資料查閱及改正

資料當事人有權**查閱其個人資料**

如果資料不準確，資料當事人**有權要求改正**

資料使用者須在收到由資料當事人提出的**查閱／改正資料要求後的 40日**內依從該項要求

大綱

接下來會探討.....

1. 《個人資料（私隱）條例》（《私隱條例》）概覽
2. **打擊「起底」罪行**
3. 資料外洩事故
4. 公署在國際及本地層面的工作

《2021年個人資料（私隱）（修訂）條例》

於2021年10月8日生效

將「起底」行為訂為

刑事罪行

賦權個人資料私隱專員(私隱專員)進行

刑事調查和**檢控**

賦權私隱專員

強制將「起底」訊息移除

「起底」罪行兩級制

新增條文內容

相關條文	罪行級別	起訴程序	入罪門檻	最高刑罰
第 64(3A) 條 及 第 64(3B) 條	第一級	簡易程序	• 未經資料當事人同意披露個人資料 • 有**意圖**或**罔顧**是否會導致資料當事人或其家人蒙受指明傷害	罰款**10萬元** 監禁**2年**
第 64(3C) 條 及 第 64(3D) 條	第二級	公訴程序	• 未經資料當事人同意披露個人資料 • 有**意圖**或**罔顧**是否會導致資料當事人或家人蒙受指明傷害 • **對資料當事人或其家人構成指明傷害**	罰款**100萬元** 監禁**5年**

兩級制的罪行及處罰機制以**有否對資料當事人或其家人構成指明傷害**區分罪行的嚴重性

「指明傷害」

第64(6) 條

- 對該人的滋擾、騷擾、纏擾、威脅或恐嚇；

- 對該人的身體傷害或心理傷害；

- 導致該人合理地擔心其安全或福祉的傷害；或

- 該人的財產受損

賦予私隱專員刑事調查權及檢控權

專員可以.....

發出書面通知要求任何人提供**相關材料**，或要求任何人**回答相干問題**以協助調查
(第66D條)

申請**手令**以**進入**及**搜查處所**及**檢取**材料以作調查之用，或**查閱電子器材**
(第66G條)

在合理地懷疑某人已干犯涉嫌「起底」的罪行**截停**、**搜查**和**拘捕**任何人
(第66H條)

以專員**本身名義**在裁判法院循**簡易程序檢控**與「起底」行為相關罪行
(第64C條)

- 沒有合理辯解而沒有提供私隱專員就指明調查所需的材料或協助，最高可被罰款20萬元和監禁1年
- 若出於詐騙意圖，在要項上提供虛假或具誤導性的材料或陳述，最高可被罰款100萬元和監禁2年

賦予私隱專員強制移除「起底」訊息的權力

專員可以發出停止披露通知(第66K及66M條)

在甚麼情況下專員可以發出停止披露通知?

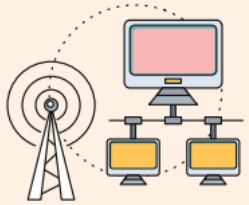
在未經資料當事人同意的情況下透過書面訊息或電子訊息披露該當事人的個人資料（不論是否在香港披露）

披露者**意圖**或**罔顧**該披露會（或相當可能會）導致當事人或其家人蒙受**指明傷害**

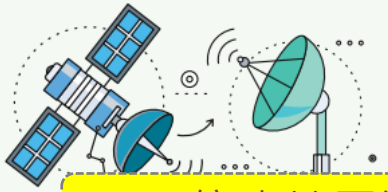
該披露作出時，資料當事人是**屬香港居民或身處香港**

專員可向以下有能力移除有關訊息的人發出停止披露通知:

身處香港的個人



在香港成立或設有業務地點的網絡服務供應商



境外服務提供者
(就電子訊息而言)

停止披露通知具有**域外管轄權**

賦予私隱專員強制移除「起底」訊息的權力

違反停止披露通知屬罪行 (第66O(1)條)

首次定罪	• 罰款5萬元及監禁 2 年 • 如屬持續罪行，則可就該罪行持續期間的每一日，罰款1,000元
其後每次定罪	• 罰款 10萬元及監禁2 年 • 如屬持續罪行，則可就該罪行持續期間的每一日，罰款2,000元

就停止披露通知提出上訴至行政上訴委員會(第66N條)

- 可以在停止披露通知送達之後的14日內向行政上訴委員會提出上訴
- 然而，不論是否提出上訴，均須於停止披露通知列明的限期內，遵從通知內的指示

不會影響有關通知的施行

被定罪及判刑的「起底」案件—
牽涉《私隱條例》第64(3A)條的案件

個案背景	• 被告於2021年12月將一個住宅單位租予事主，其後因雙方發生租務糾紛，事主遂於2023年1月遷出單位 • 事主其後發現有人於2022年11月至2023年2月期間，先後四次在**社交媒體平台的群組**中**發布包含事主個人資料的訊息**，並**對事主作出負面的評論**
定罪及判刑	• 被告認罪，被法庭裁定他四項違反《私隱條例》**第64(3A)條**的「起底」罪名成立 • 法庭於2024年12月判處被告**100小時社會服務令**

被定罪及判刑的「起底」案件二

牽涉《私隱條例》第64(3C)條的判刑案件

個案背景	• 被告與事主於2022年3月認識，兩人其後關係轉差，事主封鎖了被告的即時通訊軟件帳戶，與被告斷絕聯絡 • 2022年7月，被告在一個**網上討論區**發布了多條**包含事主個人資料的訊息**，並對事主作出**負面的評論**
定罪及判刑	• 被告認罪，被法庭裁定他一項違反《私隱條例》第64(3C)條的「起底」罪名成立 • 法庭於2024年10月判處被告**監禁四星期，緩刑兩年**

打擊「起底」罪行
2024統計數字一覽

於2024年共處理442宗「起底」個案，相比2023年的756宗大幅減少42%，主要是因為公署持續不斷的執法、宣傳及教育工作及社會氣氛轉趨平和

停止披露通知

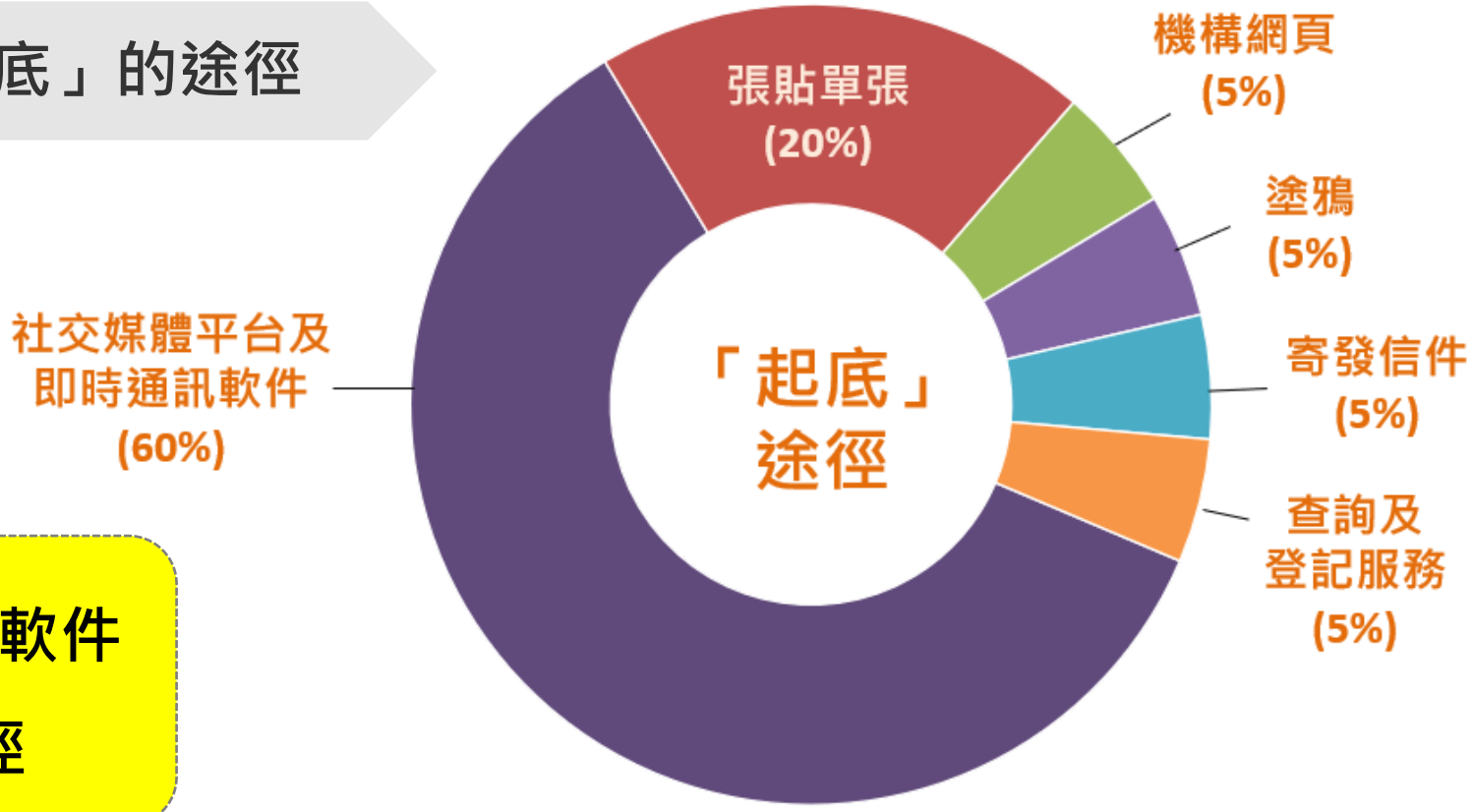
- 合共向20個網上平台發出了194個停止披露通知
- 涉及5,302個「起底」信息
- 遵從率超過96%
- 成功透過發出停止披露通知移除58個用作「起底」的頻道

調查及拘捕數字

- 就118宗個案展開刑事調查
- 將40宗案件轉介予警方繼續跟進
- 合共拘捕20人

打擊「起底」罪行
2024統計數字一覽

2024年被捕人士將事主「起底」的途徑



社交媒體平台及即時通訊軟件是「起底」的主要途徑

執法行動的總結

自《2021年個人資料（私隱）（修訂）條例》生效至2024年底統計數字一覽

自《2021年個人資料（私隱）（修訂）條例》於2021年10月8日生效至2024年底，公署共處理3,326宗「起底」個案（包括主動經網上巡查發現的「起底」個案及接獲與「起底」相關的投訴）

停止披露通知

- 合共向53個平台發出2,072個停止披露通知，涉及33,687個「起底」信息
- 遵從率超過96%
- 成功透過發出停止披露通知移除250個用作「起底」的頻道

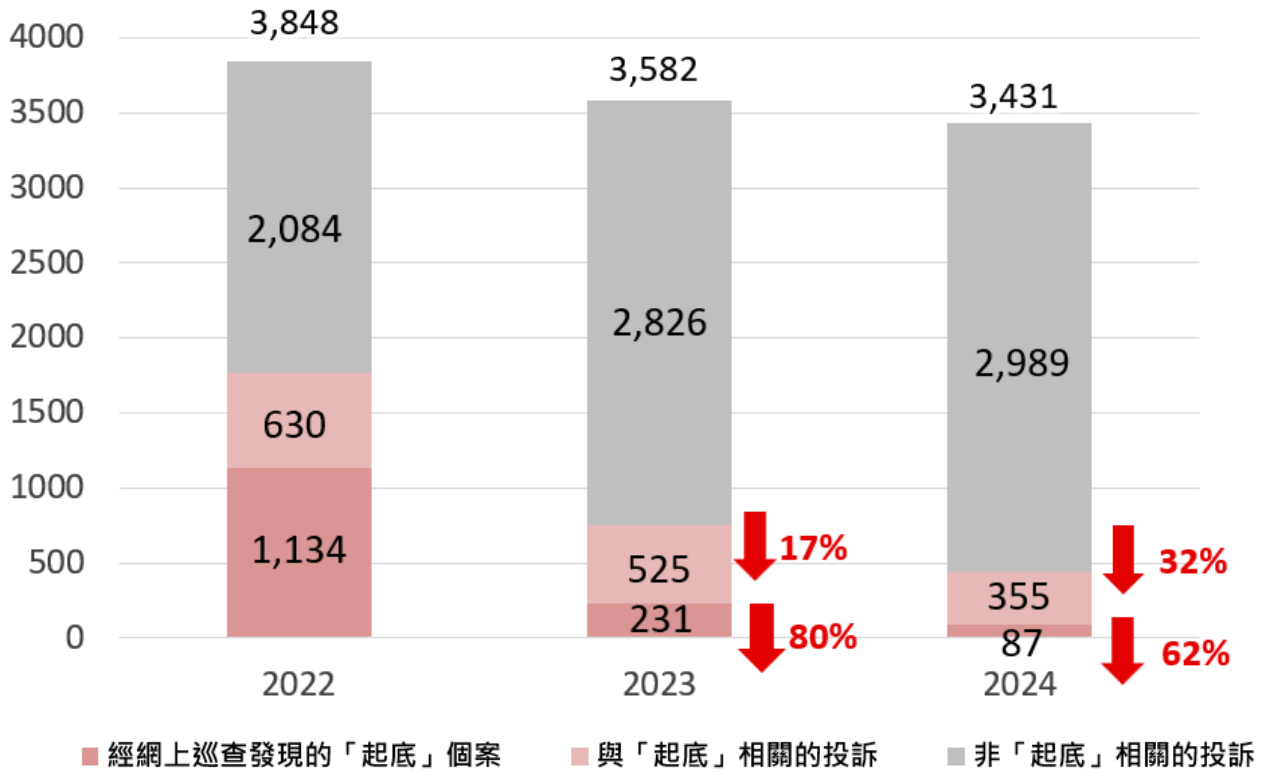
調查及拘捕數字

- 就372宗個案展開刑事調查
- 合共將103宗案件轉介予警方繼續跟進
- 合共拘捕63人

執法行動的總結

自《2021年個人資料（私隱）（修訂）條例》生效至2024年底統計數字一覽

「起底」個案及投訴數字節節下降



公署的打擊「起底」工作並無影響市民的言論自由

亦無影響網上平台在港的合法營運

公署會繼續果斷執法，打擊「起底」罪行，確保市民的個人資料私隱獲得充分保障

大綱

接下來會談及.....

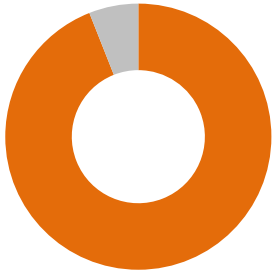
1. 《個人資料（私隱）條例》（《私隱條例》）概覽
2. 打擊「起底」罪行
3. **資料外洩事故**
4. 公署在國際及本地層面的工作

環球網絡安全形勢

網絡攻擊情況不容忽視

針對機構的網絡攻擊

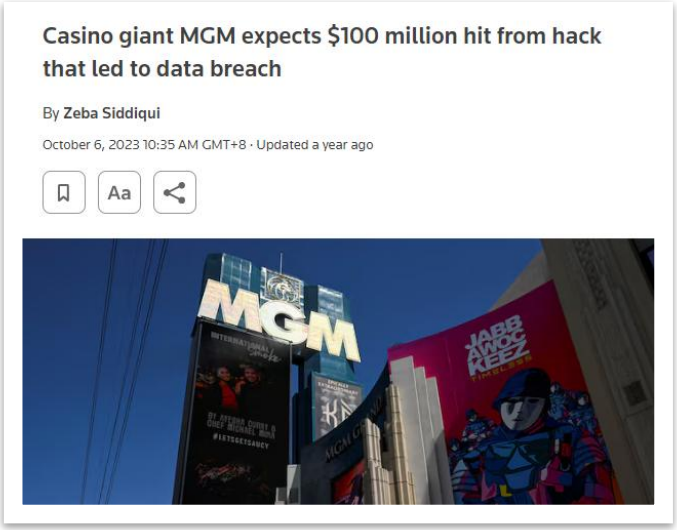
有國際調查顯示**94%**
機構曾遭遇網絡攻擊



57% 資訊科技專業人員因擔心其機構遭受網路攻擊而無法入睡

Source: Sophos

環球網絡安全形勢
資料外洩事故


Casino giant MGM expects $100 million hit from hack that led to data breach

By Zeba Siddiqui

October 6, 2023 10:35 AM GMT+8 · Updated a year ago

Aa

美國電訊商AT&T (2024)

- 黑客竊取了該企業儲存於雲端的資料，包括約1.1億人的電話號碼和通話記錄

Source: TechCrunch (2024)

PCPD HK

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

新聞稿　敬希發布

多個社交媒體及網上平台全球性資料外洩
私隱專員公署提醒平台用戶提高警惕

多個社交媒體及網上平台全球性資料外洩 (2024)

- 有網絡安全資訊網站的研究人員指出，多個網上平台發生全球性的資料外洩事故，涉及260億項個人資料

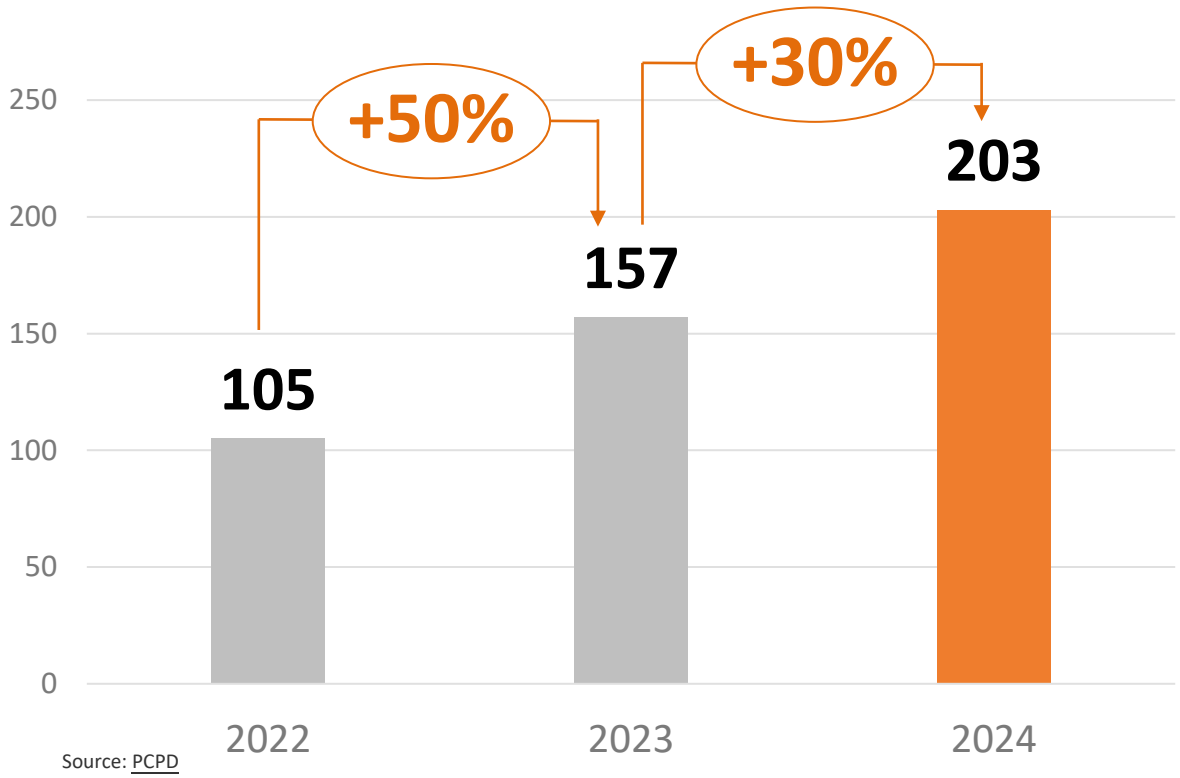
Source: PCPD (2024)

香港資料外洩事故

本地資料外洩宗數持續上升；黑客入侵佔最多

本地資料外洩宗數持續上升

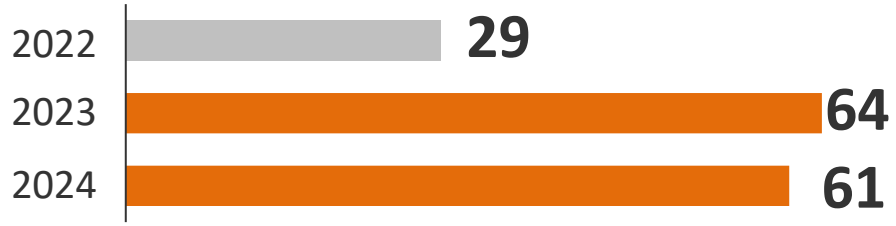
私隱專員公署接獲的資料外洩事故通報



Source: PCPD

涉及黑客入侵的資料外洩事故

私隱專員公署接獲涉及黑客入侵的資料外洩事故通報



- 2024年，私隱專員公署接獲**203宗資料外洩事故通報**，較2023年的**157宗**增加**近三成**
- 在2024年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%**，佔比屬所有類別中最高

法律責任
保障資料第4原則

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**，以確保所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未獲准許或意外地被查閱、處理、刪除、喪失或使用。

個案分享

非牟利組織A遭勒索軟件攻擊

背景

2024年7月，非牟利組織A向私隱專員公署作出資料外洩事故通報，表示組織**遭受勒索軟件攻擊，其資訊系統因而受到影響**

細節

- 黑客透過**暴力攻擊**及利用**防火牆的嚴重漏洞**，執行遠端指令，以取得保密插口層虛擬私有網絡（SSL VPN）主控台的存取權限，繼而控制一個**資訊科技測試人員帳戶**
- 黑客識別出組織網絡中**存有漏洞的伺服器**，並取得管理員權限。黑客隨後進行**橫向移動**，入侵組織的伺服器、工作電腦及手提電腦

影響

330GB 超過330GB的數據從非牟利組織A的資訊系統中被竊取

550,000名人士

可能受事件影響的資料當事人約550,000名，包括捐款者、活動參加者、義工、項目夥伴、項目參與者、項目顧問、現職及離職僱員、求職者及管治成員

涉及的個人資料包括姓名、配偶姓名、香港身份證號碼／副本、護照號碼／副本、出生日期、電話號碼、電郵地址、地址、信用卡號碼及銀行帳戶號碼

調查結果

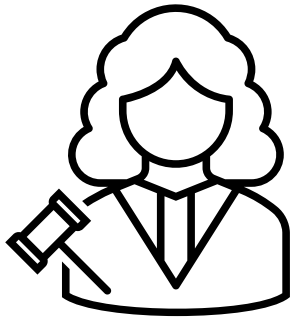
七項缺失

私隱專員考慮過事件的情況及調查所獲得的資料，認為該組織A的以下缺失是導致事件發生的主因:

- 過時的防火牆存在嚴重漏洞
- 對資訊系統進行的保安評估不足
- 未有啟用多重認證功能
- 資訊保安政策有欠具體
- 沒有對伺服器進行關鍵保安修補
- 過長地保存個人資料
- 資訊系統欠缺有效的偵測措施

非牟利組織A遭勒索軟件攻擊

私隱專員裁定.....



違反保障資料第 4(1)原則

- 該組織沒有採取所有切實可行的步驟以確保涉事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**
- 違反了《私隱條例》的**保障資料第4(1)原則**有關個人資料保安的規定

違反保障資料第 2(2)原則

- 沒有採取所有切實可行的步驟，以確保個人資料的**保存時間不超過使用相關資料實際所需的時間**
- 違反了《私隱條例》的**保障資料第2(2)原則**有關個人資料保存期限的規定

私隱專員已向該組織**送達執行通知**
指示其採取措施以糾正違規事項，以及防止類似違規情況再次發生

大綱

最後為大家介紹.....

1. 《個人資料（私隱）條例》（《私隱條例》）概覽
2. 打擊「起底」罪行
3. 資料外洩事故
4. 公署在國際及本地層面的工作

就數據擷取發表環球聯合聲明

聯同十多個私隱或資料保障機構發表兩份聯合聲明

Joint statement on data scraping and the protection of privacy

August 24, 2023

Key takeaways

- Personal information that is publicly accessible is still subject to data protection and privacy laws in most jurisdictions.
- Social media companies and the operators of websites that host publicly accessible personal data have obligations under data protection and privacy laws to protect personal information on their platforms from unlawful data scraping.
- Mass data scraping incidents that harvest personal information can constitute reportable data br
- Individuals can als scraping, and socia with their services

Introduction

1. Data scraping generally authorities are seeing in and other websites that
2. The capacity of data scr personal information fr information being scrap
3. In most jurisdictions, pe "of a public nature" on t and companies that scr they comply with these operators of other webs websites) also have data sites. These obligations publicly accessible or n

◀ 2023年8月

▼ 2024年10月

Concluding joint statement on data scraping and the protection of privacy

Informed by engagement with industry on the initial Joint Statement on Data Scraping and the Protection of Privacy (August 2023)

October 2024

Key takeaways

Initial Statement

This Concluding Statement builds on the Joint statement on data scraping and the protection of privacy (the Initial Statement), published August 24, 2023, which highlighted the following key messages:

- Personal information that is publicly accessible is subject to data protection and privacy laws in most jurisdictions.
- Social media companies (SMCs) and the operators of websites that host publicly accessible personal data have an obligation to protect publicly accessible personal data on their platforms from data scraping that violates data protection and privacy laws ("unlawful scraping").
- Mass data scraping incidents that harvest personal information can constitute reportable data breaches in many jurisdictions.
- Individuals can also take steps to protect their personal information from data scraping, and social media companies have a role to play in enabling users to engage with their services in a privacy protective manner.

甚麼是數據擷取?

- 從互聯網以自動化程序收集資料（包括個人資料）

為何要關注數據擷取的問題？

數據擷取可引起重大私隱問題

- 針對性網絡攻擊
- 身分盜竊
- 濫發直接促銷或垃圾郵件

聯合聲明的對象?

- 社交媒體平台和其他載有公開個人資料的網站

就數據擷取發表環球聯合聲明

聯同十多個私隱或資料保障機構發表兩份聯合聲明

私隱法規與數據擷取

聯署機構指出：

- 在大多數司法管轄區中，公開的個人資料仍受資料保障及私隱法保護
- 社交媒體平台及其他載有可供公眾查閱個人資料的網站有責任保護個人資料免遭非法數據擷取

2023年聯合聲明的重點建議

平台和網站應在技術及程序層面實施多重控制措施

- 指派團隊及／或特定人員來識別和實施控制措施
- 採取步驟審查自動擷取程式並採取行動停止相關活動
- 持續監控安全風險和威脅

2024年聯合聲明的進一步建議

- 機構應考慮使用AI技術加強防禦非法數據擷取
- 若數據擷取是在獲准許的情況下進行，機構應確保相關行為合法及符合合約條款
- 當機構准許第三方合法從所營運的平台收集公開的個人資料時，機構應考慮提供應用程式介面，以控制存取資料，以及偵測和減輕未獲授權的數據擷取

資訊及通訊科技的保安措施指引

加強資料保安的良好行事方式

背景

近年資料外洩事故的數量呈上升趨勢

資料使用者應加強保安措施，防範資訊系統受到惡意的攻擊

穩健的資料保安系統是良好資料管治的核心元素之一

7項建議資料保安措施

提升機構數據安全

資料管治和機構性措施

風險評估

技術上及操作上的保安措施

資料處理者的管理

資料保安事故發生後的補救措施

監察、評估及改善

其他考慮

資料保安建議措施

資料管治和機構性措施：政策及程序

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，並涵蓋：

NOTE

資料使用者應根據當時情況（如業內新標準、資料保安新威脅等），定期和及時地覆檢與修訂政策及程序。

資料保安建議措施

技術上及操作上的保安措施

資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：

資料外洩事故應變計劃

未雨綢繆 減低事故影響

內容

載列機構一旦發生資料外洩時會如何應對的文件

資料外洩事故應變計劃應：

- 概述發生事故後須執行的程序
- 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

目的

協助機構快速應對及有效管理事故

資料外洩事故應變計劃

計劃應涵蓋的範疇

- 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
- 專責應變小組各成員的聯絡詳情
- 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
- 培訓或演習計劃

處理資料外洩事故

處理資料外洩事故的五個步驟

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

PCPD
HK

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

聯絡我們

查詢 2827 2827　傳真 2877 7026

網址 www.pcpd.org.hk

電郵 communications@pcpd.org.hk

地址 香港皇后大道東248號大新金融中心13樓1303室

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

追蹤我們最新資訊