光雅珠寶貿易有限公司及愛飾管理有限公司
資料外洩事故的調查報告

根據香港法例第 486 章《個人資料（私隱）條例》第 48（2）條發表

背景

個人資料私隱專員公署（私隱專員公署）已就光雅珠寶貿易有限公司（光雅）及愛飾管理有限公司（愛飾）通報的一宗資料外洩事故完成調查。

調查源於光雅及愛飾於 2024 年 11 月 11 日向私隱專員公署通報資料外洩事故，表示其共用的資訊系統出現異常，並收到黑客的訊息指儲存於光雅及愛飾資訊系統內的資料已被盜取。經檢查後，光雅及愛飾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）。

光雅是愛飾的母公司，從事珠寶製造及批發，而愛飾則從事珠寶零售，經營「My Jewelry 愛飾珠寶」品牌。光雅及愛飾共同管理及使用受外洩事件影響的資訊系統，包括當中的伺服器、應用程式及資料庫。

調查發現，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光雅及愛飾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。

根據光雅及愛飾提供的資料，受外洩事件影響的資料當事人約 79,400 名，包括光雅的公司客戶、現職及離職員工，以及愛飾的店舖客戶、現職及離職員工的個人資料，涉及的個人資料包括員工姓名、香港身份證號碼、出生日期、電話號碼、地址及入職日期，以及客戶的姓名、香港身份證號碼（首四位數字或英文字母）、出生年份及月份、電話號碼、電郵地址及會員編號。

光雅及愛飾在外洩事件發生後已採取改善措施提升資訊系統的保安，包括重設所有用戶的登入密碼、更新伺服器作業系統，防毒軟件及防火牆，以及配置「擴展偵測與回應」工具以對資訊系統進行持續的監察等。此外，光雅及愛飾亦在發生外洩事件後通知所有受影響的資料當事人。

調查結果

私隱專員公署就外洩事件共進行了七次查訊，並審視了光雅及愛飾提供的資料，以及光雅及愛飾就外洩事件的跟進及補救工作。經考慮外洩事件的情況及調查所獲得的資料，個人資料私隱專員（私隱專員）鍾麗玲認為光雅及愛飾的以下缺失是導致外洩事件發生的主因（詳見附件一）：—

1. 未有適時刪除離職員工帳戶；
2. 資訊系統欠缺有效的保安及偵測措施；
3. 伺服器的作業系統已過時；
4. 欠缺資訊保安政策及指引；及
5. 未有對資訊系統進行保安評估及審計。

私隱專員的決定

私隱專員認為光雅及愛飾在外洩事件發生時未有採取足夠及有效的保安措施，以保護其所持有的個人資料。私隱專員對於光雅及愛飾未有意識到資訊系統存在的保安風險，以致未有適時刪除離職員工帳戶、未能採取有效的保安及偵測措施、使用過時的伺服器的作業系統、並無制訂資訊保安政策及指引，及未有對資訊系統進行保安評估及審計，最終導致是次資料外洩事故發生，表示非常遺憾。

基於上述原因，私隱專員裁定光雅及愛飾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，因而違反了《個人資料（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。

私隱專員已向光雅及愛飾送達執行通知，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。

建議

私隱專員希望藉此報告，建議機構應採取合適的機構性及技術性措施以保障載有個人資料的資訊系統，加強數據安全：

- 制訂明確針對資訊系統安全的內部政策和程序，並貫徹執行相關政策和程序；
- 實施有效措施以預防、偵測及應對網絡攻擊，包括定期進行漏洞掃瞄、以及適時修補保安漏洞；
- 停止使用已被終止支援的軟件，以及適時更新軟件；
- 加強資訊系統的密碼管理，並採用多重認證功能；
- 定期為資訊系統進行全面的保安風險評估及審計；
- 對第三方供應商提供的服務平台設置合適的保安功能，並進行定期的保安檢視；
- 制訂資料外洩事故應變計劃；及
- 為員工提供適當培訓，提高員工的數據安全意識。

鍾麗玲
個人資料私隱專員
2025 年 8 月 21 日

附件一

光雅珠寶貿易有限公司及愛飾管理有限公司資料外洩事故
導致資料外洩事故的缺失

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光雅及愛飾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**：光雅及愛飾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，而它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。光雅及愛飾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**：光雅及愛飾未有在系統保安、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；及

5. **未有對資訊系統進行保安評估及審計**：光雅及愛飾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。