俊思管理有限公司資料外洩事故的調查結果

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）已就俊思管理有限公司（俊思）通報的一宗資料外洩事故完成調查。

調查源於俊思於 2024 年 5 月 31 日向私隱專員公署通報資料外洩事故，表示俊思於 2024 年 5 月 15 日收到黑客的勒索訊息，聲稱竊取其資料並威脅出售相關資料（外洩事件）。

調查發現，黑客於 2024 年 5 月 4 日入侵一個俊思於 2024 年 4 月 24 日在防火牆設立的臨時用戶帳戶（相關帳戶），相關帳戶是為供應商作系統緊急遠端支援的用途所設立，而黑客利用相關帳戶取得進入俊思網絡的訪問權限。在取得訪問權限後，黑客在俊思的網絡進行橫向移動，並利用一個應用程式伺服器上已終止支援的操作系統的保安漏洞，進一步入侵網域控制器及其他載有個人資料的伺服器。調查顯示，外洩事件導致約 68GB 的資料從俊思的網絡外洩。外洩事件導致俊思共四台伺服器及五個系統帳戶被入侵。

俊思是一間品牌管理及分銷公司，為國際時裝及美容品牌提供服務，並為其旗下的合作品牌管理會員計劃。外洩事件牽涉俊思營運的兩個會員計劃：ICARD 會員計劃及 Brooks Brothers 會員計劃。外洩事件合共影響 127,268 名人士的個人資料，包括 100,185 名 ICARD 會員、27,069 名 Brooks Brothers 會員、14 名俊思現職僱員及前僱員等。涉及的個人資料包括會員的姓名、電郵地址、電話號碼、出生月份、性別及國籍，以及僱員的護照副本等。

俊思在外洩事件發生後已通知所有受影響的資料當事人，並為受影響的資料當事人提供支援，包括進行暗網監控及設立特定電郵地址以處理相關查詢。俊思亦採取一系列的補救措施以提升系統安全，包括刪除相關被入侵的帳戶、更換已終止支援的應用程式伺服器，以及安裝端點偵測及回應方案以進行即時偵測及分析。

調查結果

私隱專員公署就外洩事件共進行了六次查訊，並審視了俊思提供的資料，包括俊思委聘的網絡安全專家提供的調查報告，以及俊思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）鍾麗玲認為俊思的以下缺失是導致外洩事件發生的主因（詳見附件一）：—

1. 未有在修復系統故障後適時刪除臨時帳戶；
2. 使用已被終止支援的操作系統；
3. 資訊系統欠缺有效的偵測措施；及
4. 對資訊系統進行的保安風險評估及審計不足。

私隱專員的決定

基於俊思是一間具規模的國際時裝及美容品牌管理及分銷公司，而公司持有及處理大量客戶及僱員的個人資料，私隱專員鍾麗玲認為持份者（尤其是客戶）對俊思為其資訊系統實施高水平的資料保安措施抱有合理期望。然而，調查發現外洩事件是由於人為疏忽及欠缺足夠的保安措施保障資訊系統所引致。私隱專員認為，假如俊思於事發前及時刪除相關帳戶及停止使用已終止支援的操作系統，是次資料外洩事件是相當有機會可以避免的。

基於上述原因，私隱專員裁定俊思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《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。

私隱專員已向俊思送達執行通知，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。

鍾麗玲

個人資料私隱專員

2025 年 3 月 31 日

附件一

俊思管理有限公司資料外洩事故
導致資料外洩事故的缺失

1. **未有在修復系統故障後適時刪除臨時帳戶**：雖然俊思知悉長期維持供遠端存取的帳戶存在被未獲授權的第三方入侵俊思網絡的風險，但由於員工疏忽，俊思未有在修復系統故障後適時刪除相關帳戶，最終導致黑客在設立相關帳戶的 10 天後利用相關帳戶入侵俊思的網絡。此外，俊思缺乏創建和管理此類臨時帳戶的標準程序，令刪除臨時帳戶與否完全依賴個別員工的做法；

2. **使用已被終止支援的操作系統**：儘管俊思知悉相關應用程式伺服器的操作系統自 2020 年 12 月起不再獲安全更新，然而基於資源考慮，俊思原定在 2024 年底前才更換相關應用程式伺服器，換言之，相關伺服器暴露在風險中超過三年。這導致黑客得以利用相關伺服器中的保安漏洞入侵俊思的網絡，造成個人資料外洩；

3. **資訊系統欠缺有效的偵測措施**：俊思只在有需要時才檢查防火牆日誌，以致在收到黑客的勒索訊息前無法偵測到約 68GB 的資料從其網絡外洩；及

4. **對資訊系統進行的保安風險評估及審計不足**：俊思沒有對載有個人資料的系統的保安狀況進行全面的評估及審計。這導致俊思未能識別保安漏洞及實施必要的改善措施，以保護載有個人資料的系統免受網絡攻擊。