Adastria Asia Co., Limited
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 Adastria Asia Co., Limited（Adastria）通報的一宗資料外洩事故完成調查。

調查源於 Adastria 於 2024 年 11 月 18 日向私隱專員公署通報資料外洩事故，表示其客戶關係管理平台及電子商務平台（統稱受影響平台）遭受未獲授權的第三方入侵，導致 Adastria 客戶的個人資料被竊取（外洩事件）。

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。在外洩事件當中，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。

Adastria 的總公司是一間日本的跨國企業，在多個亞洲國家經營服裝零售。Adastria 在外洩事件發生時透過其網上平台「dot st HK」管理旗下品牌（包括 GLOBAL WORK, “niko and …”, LOWRYS FARM, Heather, JEANASiS, studio CLIP, repipi armario, LEPSIM, PAGEBOY）在香港的銷售。外洩事件合共影響 59,205 名客戶的個人資料，涉及的個人資料包括客戶的姓名、電話號碼及訂單資料（包括交易參考編號、訂單日期、會員號碼、送貨方式、送貨／取貨日期、送貨地址、產品名稱與描述，以及價格資料）。

在調查過程中，Adastria 發現受影響的個人資料於外洩事件發生約兩個月後在「暗網」公開，並可供下載。

Adastria 在外洩事件發生後已通知所有受影響的客戶。Adastria 亦就外洩事件中發現的缺失採取一系列的補救措施，包括啟用受影響平台的保安功能，例如密碼措施、多重認證功能及限制 IP 位址連接功能，以及安裝端點偵測及回應方案以進行偵測及攔截資訊系統中的任何惡意活動。

調查結果

私隱專員公署就外洩事件共進行了五次查訊，並審視了 Adastria 提供的資料，包括 Adastria 委聘的第三方顧問提供的兩份調查報告，以及 Adastria 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 Adastria 的以下缺失是導致外洩事件發生的主因（詳見附件一）：—

1. 薄弱的密碼管理；
2. 未有為存取帳戶啟用多重認證功能；
3. 缺乏保障個人資料的意識；及
4. 未有對受影響平台進行適當的保安檢視。

私隱專員的決定

基於 Adastria 是一個知名的跨國時裝品牌集團，亦持有大量客戶的個人資料，私隱專員對 Adastria 的資料保安意識不足及欠缺適當措施以保障所持有的個人資料，表示遺憾。私隱專員認為，假如 Adastria 於事發前採取合適及足夠的機構性及技術性措施，是次資料外洩事故是相當有機會可以避免的。

基於上述原因，私隱專員裁定 Adastria 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 Adastria 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

Adastria Asia Co., Limited 資料外洩事故
導致資料外洩事故的缺失

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、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，Adastria 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 Adastria 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 Adastria 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；及

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 Adastria 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。