香港樂施會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）已就香港樂施會（樂施會）通報的一宗資料外洩事故完成調查。

調查源於樂施會於 2024 年 7 月 13 日向私隱專員公署通報資料外洩事故，表示樂施會遭受勒索軟件攻擊，其資訊系統因而受到影響（外洩事件）。

調查發現，黑客透過暴力攻擊及利用樂施會防火牆的嚴重漏洞，執行遠端程式碼及指令，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（IT）測試人員帳戶。黑客從外部網絡透過SSL VPN連接到樂施會的資訊系統後，識別出樂施會網絡中存有漏洞的伺服器，並取得樂施會的活動目錄（Active Directory）的管理員權限。黑客隨後進行橫向移動，入侵樂施會的伺服器、工作電腦及手提電腦。

黑客於 2024 年 7 月 10 日在樂施會的資訊系統放置勒索軟件「DarkHack」，導致儲存在系統內的檔案及資料被加密及竊取。外洩事件導致樂施會共 37 台伺服器及 24 台工作電腦／手提電腦被入侵，當中包括 (i) 檔案伺服器；(ii) 捐款者資料庫及其用於數據遷移的暫存伺服器；(iii) 樂施會毅行者網站資料庫；(iv) 人力資源系統；及(v) Active Directory 伺服器。

調查發現有超過 330 GB 的數據從樂施會的資訊系統中被竊取，可能受外洩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（詳見附件一）。

樂施會已就外洩事件通知受影響人士，並在外洩事件發生後實施各項機構性及技術性的改善措施以加強整體系統安全，從而更好地保障個人資料私隱。這些措施包括實施外部顧問就資訊安全措施所提供的建議，而樂施會亦承諾更新其資訊科技政策，以建立全面的漏洞管理計劃，包括進行定期漏洞掃描及滲透測試。

調查結果

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）鍾麗玲認為樂施會的以下缺失是導致外洩事件發生的主因（詳見附件二）：—

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

私隱專員的決定

私隱專員鍾麗玲認為樂施會是一間具規模的機構，恆常地持有並處理大量不同人士的個人資料。因此，持份者及公眾會合理地期望樂施會投入足夠資源確保其資訊系統的安全及符合數據安全的標準。然而，調查顯示樂施會於事發前未有採取足夠及有效的措施以保障其資訊系統的安全，亦未有制訂有效的機制適時地銷毀超過保存期限的個人資料，以致發生大規模的資料外洩事故，情況令人遺憾。

基於上述原因，私隱專員裁定樂施會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》（《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。

此外，私隱專員認為樂施會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，因而違反了《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。

私隱專員已向樂施會送達執行通知，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 1 月 23 日

附件一

樂施會資料外洩事故

樂施會的資料外洩事件中受影響的資料當事人類別，及涉及個人資料的種類如下表所示：—

	資料當事人的類別	估計可能涉及人數[1]	可能涉及的個人資料種類
(i)	捐款者	521,130	姓名、香港身份證號碼、出生日期、電話號碼、電郵地址、地址、信用卡號碼、銀行帳戶號碼
(ii)	活動參加者	87,831	姓名、香港身份證號碼、出生日期、電話號碼、電郵地址、地址
(iii)	義工	7,928	姓名、電話號碼、電郵地址、地址
(iv)	項目夥伴	472	姓名、電話號碼、電郵地址、地址、銀行帳戶號碼
(v)	項目參與者	6,665	姓名、電話號碼、電郵地址、地址
(vi)	項目顧問	78	姓名、香港身份證號碼、電話號碼、地址、銀行帳戶號碼
(vii)	現職及離職僱員	471	姓名、配偶姓名、香港身份證號碼／副本、出生日期、電話號碼、電郵地址、地址
(viii)	求職者	746	姓名、電話號碼、電郵地址、地址
(ix)	管治成員	103	姓名、香港身份證號碼／副本、護照號碼／副本、電話號碼、電郵地址、地址

[1] 樂施會表示，從資料庫去除重複的數字後，樂施會估計可能涉及人數總共約為 550,000。

附件二

樂施會資料外洩事故
導致資料外洩事故的缺失

1. **過時的防火牆存在嚴重漏洞**：自 2023 年 6 月以來，樂施會未曾對涉事防火牆進行任何修補或更新。儘管涉事防火牆存在的兩項嚴重漏洞的修補程式已分別於 2023 年 6 月及 2024 年 2 月發布，樂施會在外洩事件發生時仍未為防火牆安裝最新的修補程式。因此，黑客成功利用這些漏洞執行遠端程式碼及指令，控制了用於連接至 SSL VPN 的 IT 測試人員帳戶，並最終獲得了樂施會網絡的存取權限並放置勒索軟件；

2. **未有啟用多重認證功能**：儘管樂施會於外洩事件發生前正在為 SSL VPN 實施雙重認證，但這項關鍵的保安措施於外洩事件發生前尚未完成。考慮到樂施會的資訊系統中載有大量個人資料，私隱專員對於樂施會延遲實施多重認證表示失望；

3. **沒有對伺服器進行關鍵保安修補**：導致黑客利用存在於樂施會資訊系統的四台名稱伺服器（Name Server）的嚴重漏洞，獲取有關伺服器的存取權限，並提升其權限以安裝惡意軟件、加密檔案及從受影響的裝置竊取資料；

4. **資訊系統欠缺有效的偵測措施**：儘管在黑客成功入侵樂施會的資訊系統前，樂施會曾多次偵測到黑客的活動，包括異常的登入嘗試，但樂施會卻沒有採取任何行動。樂施會解釋，由於缺乏通知相關團隊或人員的機制，因此未能察覺到這些可疑活動。另一方面，黑客在成功進入樂施會的資訊系統後，入侵了用於偵測樂施會網絡內惡意活動的端點保安服務，使其無法有效偵測及防止是次勒索軟件攻擊，而樂施會亦缺乏定期監察及檢視資料庫或伺服器日誌的措施以偵測可疑活動；

5. **對資訊系統進行的保安評估不足**：樂施會於外洩事件發生前的兩年內對其網站進行了兩次漏洞評估，惟評估範圍並無涵蓋存有嚴重漏洞的防火牆及名稱伺服器。此外，樂施會在 2024 年 2 月至 3 月期間進行的資訊科技保安評估範圍並不包括對樂施會的資訊科技保安環境進行漏洞掃描或滲透測試，因此亦未能識別與外洩事件有關的保安漏洞；

6. **資訊保安政策有欠具體**：樂施會的「資訊科技用戶手冊」欠缺確保數據安全的重要細節，包括有關修補程式管理的規定及程序、漏洞管理、保安評估及日誌監察，這些都是導致外洩事件發生的原因。雖然該手冊涵蓋一些與資訊保安措施及原則相關的指引，惟內容屬廣泛的原則，並沒有提供具體執行這些原則的指引；及

7. **過長地保存個人資料**：樂施會意外地保存部分個人資料超過實際所需的時間，包括樂施會在七年前舉辦的活動約 4,000 項參加者的個人資料（包括姓名、地址、電話號碼及／或電郵地址）；在 2021 至 2024 年間樂施會項目 600 項落選者的個人資料（包括姓名、出生日期、電話號碼及電郵地址）；50 項與顧問的香港身份證號碼及履歷有關的個人資料，這些顧問的個人資料在完成向樂施會提供顧問服務超過七年仍被保存；及 35 份前管治委員會成員的香港身份證或護照副本。