機電工程署個人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）已就機電工程署（機電署）通報的一宗資料外洩事故完成調查。

調查源於機電署於 2024 年 5 月 1 日向私隱專員公署通報資料外洩事故，表示懷疑由其持有的市民個人資料外洩，當中涉及在 2022 年「限制與檢測宣告」行動（「強檢行動」）中受檢測人士的個人資料（「外洩事件」）。

機電署在 2022 年 3 至 7 月期間共執行了 14 次強檢行動，對分別處於 14 座大廈內的居民／訪客進行 2019 冠狀病毒病檢測（見附錄一）。為收集強檢行動中受檢測市民的資料，機電署向承辦商採購並使用雲端平台 ArcGIS Online 附設的電子表格平台（「該電子表格平台」）製作了 14 張電子表格作記錄，而相關的電子表格及資料會被儲存在 ArcGIS Online 雲端平台數據儲存庫中。

機電署於 2022 年底知悉強檢行動告一段落後，隨即通知有關承辦商於 2023 年 2 月底合約屆滿後不再就該電子表格平台的服務續約。根據機電署，機電署認為在合約屆滿後，該電子表格平台的帳戶便會失效，而有關資料亦會被承辦商自動刪除。直至 2024 年 4 月 30 日，經私隱專員公署通知機電署，機電署才得知強檢行動中受檢測市民的個人資料可在毋須輸入帳戶及密碼的情況下在 ArcGIS Online 雲端平台的相關網址被瀏覽，遂立即要求承辦商同日從該電子表格平台中移除涉事的個人資料，令公眾不能再瀏覽有關資料，並於翌日向私隱專員公署通報。

受外洩事件影響的受檢測人士數目超過 17,000 人，所涉及的個人資料包括姓名、地址、香港身份證號碼、電話號碼、年齡、性別、有否接種新冠疫苗、是否核酸檢測陽性及確診日期等。

根據機電署所提供的資料，外洩事件發生後，機電署致力從事件中汲取教訓，採取了一系列的措施及行動，包括強化私隱管理、全面檢視處理個人資料的工作及指引、加強員工培訓及承辦商監管，以及優化部門電腦支援系統，以建立更穩健的私隱保安框架及保障個人資料企業文化。

調查結果

私隱專員公署就外洩事件向機電署進行了五次查訊，亦兩度去信要求承辦商就外洩事件提供相關資料。私隱專員公署感謝機電署及承辦商配合調查，並提供所要求的資訊及文件。**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）認為機電署的以下缺失是導致外洩事件發生的主因：—**

1. 沒有就強檢行動所收集的個人資料保存期限制訂書面政策，為資料的存廢提供明確依據。縱使機電署或未能於強檢行動展開之前或期間訂立個人資料的保存期限或訂定相關的資料保存政策，但機電署由始至終僅依靠於 2022 年底已通知承辦商不再續約，作為實際上已為資料設定保存期限的根據，卻一直沒有透過書面政策訂定上述資料的保存期限。有關的書面政策可為資料的存廢提供明確依據，有其重要作用。

特別在本個案中，所涉的資料屬敏感的個人資料，當中不但有市民的姓名、年齡、性別、詳細地址、電話號碼，還包含其香港身份證號碼及核酸檢測資料，而受影響的市民超過 17,000 人，故此機電署更應對有關資料的處理提高警覺、格外小心；

2. 未有清楚向承辦商提出刪除相關資料的要求，即使機電署於 2022 年底知悉強檢行動告一段落，但於通知承辦商不再續約的過程中，並無明確向承辦商提出刪除涉事的個人資料的要求。事實上，機電署在 2024 年 4 月 30 日得知外洩事件後，才要求承辦商於同日從該電子表格平台中移除涉事的個人資料，而相關資料在當晚已被移除，令公眾不能再瀏覽有關資料。由此可見，機電署只需向承辦商提出要求，有關資料便可被移除。

私隱專員認為，署方在通知承辦商不再續約時，向承辦商提出刪除涉事資料的要求，屬有效且切實可行保障個人資料的步驟，惟機電署未有採取此行動；

3. 沒有自行主動刪除涉事的個人資料，特別是在 2022 年 12 月底通知承辦商不再續約，直至 2023 年 2 月底合約屆滿期間，雖然機電署仍有權限登入該電子表格平台管理當中的個人資料，但機電署只是等待與承辦商的相關合約結束，並無主動採取行動自行查核及刪除平台上的個人資料，以避免不必要地或過長地保存個人資料，此屬一明顯缺失；及

4. **沒有適當跟進承辦商刪除資料**，機電署只假定承辦商在相關合約結束後會自行採取行動，卻從沒有督促、查核或提醒承辦商刪除該電子表格平台上的個人資料，亦從沒有了解或監察承辦商有關行動的進度或成效。機電署作為資料使用者，決不能只是被動地等待承辦商採取行動，或因信賴承辦商而不去查核其實際的工作情況，此屬另一明顯缺失。

私隱專員的決定

面對嚴峻的疫情，私隱專員鍾麗玲理解參與檢疫工作的部門需要迅速部署並執行行動。由於時間緊迫，機電署在籌劃及展開強檢行動時或許未及考慮日後刪除個人資料的政策及安排。然而，由始至終，機電署一直沒有就相關個人資料保存期限制訂政策，亦未有清楚向承辦商提出刪除資料的要求，機電署在完成強檢行動後，也沒有主動採取相應的行動刪除或跟進及查核承辦商刪除個人資料的工作，令相關的個人資料被不必要地暴露於資料外洩的風險中，做法明顯未能符合《個人資料（私隱）條例》（《私隱條例》）的要求，亦虧負了公眾的合理期望，情況令人遺憾。因此，私隱專員裁定機電署：—

(i) 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該資料實際所需的時間，因此違反了《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；及

(ii) 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。

私隱專員已向機電署送達執行通知，指示其採取措施糾正違規事項，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

2024 年 12 月 9 日

附錄一

涉事 14 座大廈強檢行動的相關日期、樓宇名稱及人數資料

行動日期	地點	涉及人數
3-4 / 3 / 2022	德朗邨 德瑩樓	1,506
6-7 / 3 / 2022	啟晴邨 欣晴樓	1,451
9-10 / 3 / 2022	友愛邨 愛明樓	1,608
14-15 / 3 / 2022	富昌邨 富良樓	210
17-18 / 3 / 2022	湖景邨 湖暉樓	1,330
19-20 / 3 / 2022	蝴蝶邨 蝶影樓	1,348
21-22 / 3 / 2022	安達邨 善達樓	1,966
23-24 / 3 / 2022	東頭(二)邨 偉東樓	285
25-26 / 3 / 2022	廣福邨 廣惠樓	1,010
30/3 - 1/4/2022	博康邨 博逸樓	1,823
12-13 / 4 / 2022	祥華邨 祥豐樓	939
3-4 / 5 / 2022	明德邨 明道樓	1,582
30-31 / 5 / 2022	元洲邨 元盛樓	469
4-5 / 7 / 2022	鳳德邨 黛鳳樓	1,798
	合計	**17,325**