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

選舉事務處

兩宗個人資料外洩事故

報告編號：R22 - 4116
發表日期：2022 年 12 月 29 日

調查報告：選舉事務處
兩宗個人資料外洩事故

香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）第48(2)條訂明，「[個人資料私隱]*專員在完成一項調查後，如認為如此行事是符合公眾利益的，可－*

(a)　發表列明以下事項的報告－

(i)　該項調查的結果；

(ii)　由該項調查引致的、專員認為是適合作出的關乎促進有關資料使用者所屬的某類別的資料使用者遵守本條例條文（尤其是各保障資料原則）的任何建議；及

(iii)　由該項調查引致的、專員認為適合作出的任何其他評論；及

(b)　以他認為合適的方式發表該報告。」

現根據《私隱條例》第 48(2)條履行所賦予的權力，發表本調查報告。

鍾麗玲
個人資料私隱專員
2022 年 12 月 29 日

調查個案（一）：選舉事務處職員錯誤地把載有選民資料的檔案以電郵發送至不明收件人

背景

1. 2022 年 3 月 24 日，選舉事務處（處方）向個人資料私隱專員公署（私隱專員公署）作出資料外洩事故通報，表示一名處方職員於 3 月 23 日錯誤地把載有約 15,000 名選民登記資料的檔案傳送至一個不明電郵地址（事件一），有關檔案載有選民的中英文姓名及住址資料。

2. 處方同日亦就事件一向選舉管理委員會、政制及內地事務局及政府資訊科技總監辦公室作出匯報，並向警方報案。處方於 2022 年 3 月 25 日發布新聞公報[1]向公眾交代事件。

3. 在接獲上述資料外洩事故通報後，個人資料私隱專員（專員）於 2022 年 4 月 6 日根據香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）第 38(b)條[2]就事件一對處方展開調查，以確定處方在事件一中的作為是否涉及違反《私隱條例》的規定。

調查所得的資料

4. 專員在進行調查的過程中，審視及考慮了處方提供與事件一有關的資料，包括處方提供的內部調查報告及處方於 2022 年 9 月 13 日發表的調查報告摘要[3]。專員亦考慮了處方在事件一發生後的跟進及補救工作。

[1] https://www.info.gov.hk/gia/general/202203/25/P2022032500608.htm
[2] 根據《私隱條例》第 38(b)條，當專員有合理理由相信有資料使用者已經或正在作出或從事關乎個人資料的作為或行為，而有關作為或行為可能屬違反《私隱條例》下的規定，專員可就有關的資料使用者進行調查，以確定有關行為或作為是否屬違反《私隱條例》下的規定。
[3] https://www.reo.gov.hk/pdf/incident_report/Summary_Report_data_breach_incident_March2022(Chi).pdf

5. 此外，政府資訊科技總監辦公室、政制及內地事務局和處方的代表因應事件一成立了一個工作小組（該工作小組），於 2022 年 4 月至 6 月期間全面檢視處方在資訊保安方面的工作。政府資訊科技總監辦公室在完成有關檢視後已向處方提供了一份檢視報告（該檢視報告），羅列了提升處方的網絡安全水平及應對網絡風險能力的建議。雖然該檢視報告主要就處方在資訊保安方面的整體情況提供建議，而非查找處方在事件一當中的不足之處，專員在調查過程中亦考慮了該檢視報告的內容。

<u>事件一的背景及經過</u>

6. 根據處方提供的資料，涉案的職員是一名地方選區選民登記組的文書主任（該文書主任），她的其中一項職責是督導其下屬處理有關與其他政府部門進行資料核對的工作。

7. 事件一涉及的資料是由房屋署提供有關已終止公共屋邨單位租約的選民資料。處方在接獲房屋署的資料後，會將由處方備存的選民住址與房屋署提供的地址進行核對。如個別選民的地址相同，處方便有合理理由懷疑該選民的登記住址不再是其唯一或主要住址，遂會根據相關的選舉法例[4]將該選民納入查訊程序。在事件一當中，該文書主任的下屬在完成第一次核對後把有關資料交由該文書主任進行第二次核對。

8. 事件一發生之時正值本地第五波 2019 冠狀病毒病疫情肆虐，處方自 2022 年 1 月 25 日起作出特別在家工作安排，把職員分成不同組別交替在家工作，以減少社交接觸。就此，處方為部份職員提供配置虛擬私人網路的手提電腦以便他們在家工作時登入處方的系統。雖然該文書主任獲安排在某些日子在家工作，但由於該文書主任的工作涉及處理大量個人資料，所以她並未獲發有關的手提電腦，而只可以使用辦公室的電腦處理有關資料核對的工作。

[4]《選舉管理委員會(選民登記)(立法會地方選區) (區議會選區)規例》(第 541A 章)第 7 條。

9. 2022 年 3 月 23 日晚上 7 時 03 分，該文書主任擬把兩個載有選民資料的試算表檔案（該兩個檔案）傳送至其私人電郵帳戶，以方便她翌日在家工作。然而該文書主任卻輸入了錯誤的電郵地址，導致該兩個檔案被傳送至不明收件人。該文書主任留意到她傳送的電郵在十多分鐘後仍未送達她的私人電郵帳戶，才發現出錯，並立刻將情況通知負責進行最後核對的助理選舉事務主任，而該助理選舉事務主任於 2022 年 3 月 24 日早上才通知處方。

10. 處方在該文書主任向警方提供資料後進一步得悉，該文書主任於事發當日另外發送了兩封載有選民資料的電郵至其私人電郵帳戶。該文書主任於下午 5 時 43 分發送的一封電郵涉及約 1,000 名選民的資料（當中載有選民的中英文姓名及不能用作識別個人身份的內部參考編號）。而該文書主任在發現她錯誤地把該兩個檔案傳送至不明收件人後，於晚上 7 時 58 分再次透過電郵把該兩個檔案發送至其私人電郵帳戶，以方便她可於翌日在家工作。

受影響的個人資料

11. 根據《私隱條例》第 2(1)條，「個人資料」是指任何直接或間接與一名在世的個人有關的資料，而有關資料是儲存在紀錄內，可加以處理或查閱，並且從該資料可直接或間接地確定有關的個人的身份。

12. 該兩個檔案載有 15,070 名[5]選民的資料（兩個檔案分別載有 5,264 和 9,806 名選民的資料），包括房屋署就已終止租約的公屋單位所提供的選民姓名及其公屋單位住址，以及處方就該等選民備存的姓名及登記住址。

[5] 撇除 103 名在事件一發生之時已故的選民，受影響的資料當事人的總數為 14,967 人。

該文書主任就事件一的解釋

13. 該文書主任表示，由於處方實施在家工作安排令她在辦公室的工作時間減少，為免耽誤工作進度，她遂於 2022 年 3 月 23 日把一些與工作有關的資料透過其工作電郵帳戶傳送至其私人電郵帳戶，包括該兩個檔案。該文書主任表示未有以密碼保護該兩個檔案。

14. 該文書主任表示她原本打算發送的私人電郵帳戶的電郵地址格式為 xyzxyz0000@gmail.com [6]，但她卻錯誤地輸入一個格式為 xyzabcde11@gmail.com 的電郵地址。這錯誤是源於她擁有另一個格式為 xyzabcde11@hotmail.com 的電郵帳戶 。

15. 該文書主任表示已在處方工作約 26 年，在事發時知道不能把載有選民資料的檔案發送至任何私人電郵帳戶。她承認是一時情急才安排把檔案透過電郵傳送至她的私人電郵帳戶，從而導致是次事件。該文書主任確認已將載有選民資料的檔案（包括該兩個檔案）從她的私人電郵帳戶中刪除。

處方的調查結果

16. 根據處方的內部調查報告，處方表示他們就保障選民的個人資料訂有不同的內部程序及指引。在事件一中，該文書主任沒有遵從部門行政通告編號 7/2017（部門資訊科技保安政策、指引及程序）的附件所載列的指引[7]，當中規定「*僅使用部門的電郵系統以電郵方式傳送保密資料*」及「*不可使用個人電郵帳戶處理公務或傳送保密資料或個人資料*」。處方表示每六個月會向職員傳閱上述通告，而在事件一發生前的上一次傳閱是在 2022 年 3 月 1 日進行。除上述通告外，處方表示該文書主任亦曾觀看有關保障資料的影片 。

[6] 在此所述的所有電郵地址格式並非真實電郵地址。
[7] DOs and DON'Ts

17. 處方於內部調查報告總結地指出，該文書主任在事件一中涉及疏忽處理個人資料，並違反部門有關資訊科技保安的指引。處方認為由於事件涉及大量的選民資料，事件屬嚴重的資料外洩事故，該文書主任須就事件負上個人責任。處方表示正根據公務員紀律處分機制跟進該文書主任的不當行為。

<u>處方的跟進工作及改善措施</u>

18. 在知悉事件一發生後，處方於 2022 年 3 月 24 日立刻向有關的不明收件人發電郵要求立刻及永久刪除該兩個檔案，並要求該收件人聯絡處方作出跟進。處方亦於同日向私隱專員公署、選舉管理委員會、政制及內地事務局及政府資訊科技總監辦公室匯報事件，並向警方報案。處方在 2022 年 3 月 25 日發出新聞公報[8]公布事件，並於 2022 年 3 月 31 日以書面通知受是次事件影響的選民。

19. 警方及後成功聯絡有關的不明收件人，確認該名人士並沒有開啟上述載有選民資料檔案的電郵，亦已經將該電郵刪除。

20. 為加強資料保安並防止類似事件再次發生，處方自 2022 年 4 月起向相關組別的職員實施資訊保安技術限制措施。除非有真正的運作需要，否則助理選舉事務主任以下職級的職員無法透過部門的電郵系統傳送電郵至私人電郵帳戶，而他們的電腦亦不可瀏覽本港常用的互聯網電郵服務供應商的網站。

21. 政府資訊科技總監辦公室在該工作小組完成全面檢視處方在資訊保安方面的工作後已向處方提供該檢視報告，在資訊保安管理、資訊保安的意識及培訓、系統保安及資訊科技設施的額外保障方面提供了具體建議。處方已承諾會就實施該工作小組的建議訂立優次，並申請所需撥款和人手。

[8] 見註 1。

調查結果及違例事項

處方作為資料使用者

22. 處方的其中主要職能包括處理選民登記及管理香港的選舉事宜。在執行這些職能時，處方會收集、持有、處理及使用選民的個人資料。因此，處方屬《私隱條例》第 2(1)條釋義下的資料使用者[9]，須遵從《私隱條例》的規定行事，包括《私隱條例》附表一所列明的六項保障資料原則。

保障資料第 4(1)原則

23. 《私隱條例》附表一保障資料第 4(1)原則訂明，資料使用者須採取所有切實可行的步驟，以確保由資料使用者持有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，尤其須考慮 ─

(a) 該資料的種類及如該等事情發生便能做成的損害；
(b) 儲存該資料的地點；
(c) 儲存該資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；
(d) 為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及
(e) 為確保在保安良好的情況下傳送該資料而採取的措施。

24. 經考慮與事件一有關的事實及在調查過程中所獲得的證據，專員認為以下原因導致事件一發生：—

[9] 根據《私隱條例》第 2(1)條，就個人資料而言，資料使用者指「*獨自或聯同其他人或與其他人共同控制該資料的收集、持有、處理或使用的人*」。

(1) 職員沒有遵從部門有關資訊科技保安的指引

25. 該文書主任沒有遵從部門行政通告編號 7/2017（部門資訊科技保安政策、指引及程序）的附件所載列的指引，即「*僅使用部門的電郵系統以電郵方式傳送保密資料*」及「*不可使用個人電郵帳戶處理公務或傳送保密資料或個人資料*」，於事發當日先後三次安排把載有選民資料的檔案發送至其私人電郵帳戶，包括其中一次把該兩個檔案錯誤地傳送至一名不明收件人，導致是次資料外洩事故。

26. 此外，該文書主任在發現有關電郵已被誤發至不明收件人後，仍然以方便她翌日在家工作為由，在未詳加考慮的情況下再次把該兩個檔案發送至其私人電郵帳戶，此舉完全漠視處方訂定的指引。

(2) 職員資料保障意識不足

27. 該文書主任不僅沒有遵從部門的相關指引，更嚴重缺乏保障資料的意識：

(i) 該文書主任在沒有充分考慮所涉及的安全風險的情況下，疏忽地將載有大量個人資料的電郵發送到處方電郵系統以外的電郵地址，並且未有以任何形式（例如將檔案加密或設置密碼）保護有關檔案；

(ii) 該文書主任在發出有關電郵前明顯地未有仔細核對收件人的電郵地址（即該文書主任的私人電郵地址）；及

(iii) 該文書主任發現有關電郵已被誤發至不明收件人後，並沒有停止傳送相關資料，卻竟再次安排發送同一封載有該兩個檔案的電郵至她的私人電郵帳戶，以方便其在家工作。

28. 處方在調查過程中向專員確認事發前曾向該文書主任提供有關保障資料的通告，而該文書主任亦曾觀看有關保障資料的影片。明顯

地，這些培訓措施並不足以提升該名於處方任職了 26 年的職員的資料保障意識至應有的水平。

29. 專員注意到政府資訊科技總監辦公室在該檢視報告中向處方提供了兩項就資訊保安的教育及培訓方面的建議，包括建立資訊安全意識和培訓工作小組，以制定有關建立資訊安全意識的計劃，及擴大資訊安全意識活動的種類和傳遞渠道，以推廣資訊安全文化。由此看來，處方在資訊保安的教育及培訓方面實有不足之處。

(3) 處方的資訊保安措施不足

30. 處方在事發前並未設置適當的保安技術限制，以禁止職級為助理選舉事務選舉主任以下的職員（包括該文書主任）使用其工作電郵帳戶發送電郵到私人電郵帳戶。處方僅在事後設置上述的保安技術措施作為補救行動。此外，處方亦未採用任何保安措施，例如設置資料外洩防護工具，以偵測及攔截任何載有個人資料的電郵及附件被傳送出處方電郵系統。

31. 明顯地，因應處方持有和日常處理超過百萬名選民的個人資料，若處方當初能根據職員的職能及責任訂立對外發送電郵的權限，並採取適當保安措施以偵測及攔截任何載有個人資料的電郵及附件被傳送到處方電郵系統以外，則應可避免是次事件發生。

結論：違反保障資料第 4(1)原則

32. 在考慮本個案所有證據後，**專員認為事件一主要涉及人為錯誤。資料外洩事故源於個別職員的疏忽和缺乏資料保障意識，以致違反處方有關資訊科技保安的指引。有關職員在沒有充分考慮所涉及的安全風險及未有仔細核對收件人的電郵地址的情況下，單純地為方便在家工作而將載有大量個人資料的電郵發送到處方電郵系統以外的錯誤電郵地址。**

33. 另一方面，專員認為處方持有及處理大量選民的個人資料，理應採取更嚴格的資訊保安措施，以確保其系統能充分應對職員的疏忽或不恰當行為。然而，處方在事發前並未設置適當的資訊保安措施，令職員可隨意將載有個人資料的檔案透過處方的電郵系統發送到處方電郵系統以外的私人電郵地址，亦是事件一發生的肇因。

34. 綜合以上情況，專員認為處方在事件一當中沒有採取所有切實可行的步驟以確保相關的選民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，因而違反了保障資料第**4(1)**原則有關個人資料保安的規定。

調查個案（二）：處方錯誤地將一名選舉委員會委員送交的回條夾附在測試電郵內

背景

35. 2022 年 4 月 28 日，處方向私隱專員公署作出另一個資料外洩事故通報，表示處方職員於同日將附有一名選舉委員會委員（選委）及其助理個人資料的回條（該回條）錯誤地夾附在發送予 38 名選委及 26 名選委助理的測試電郵內（事件二）。該回條載有該名選委及其助理的姓名、電郵地址、電話號碼，以及該名選委的簽署。

36. 處方亦於同日就事件二向選舉管理委員會、政制及內地事務局及政府資訊科技總監辦公室作出匯報。

37. 在接獲上述資料外洩事故通報後，專員於 2022 年 5 月 6 日根據《私隱條例》第 38(b)條就事件二對處方展開調查，以確定處方在事件二中的作為是否涉及違反《私隱條例》的規定。

調查所得的資料

38. 專員在進行調查的過程中，審視及考慮了處方提供與事件二有關的資料，包括處方提供的內部調查報告，及處方於 2022 年 9 月 13 日發表的調查報告摘要[10]。專員亦考慮了處方在事件二發生後的跟進及補救工作。

事件二的背景及經過

39. 2022 年行政長官選舉（該選舉）的投票日於 2022 年 5 月 8 日舉行。為準備該選舉，處方於 2022 年 3 月 25 日向選委發出一封郵件，向他們提供與該選舉有關的資料，並邀請選委於 2022 年 4 月 6 日前填交回條以提供選委及其助理的電郵地址及流動電話號碼，以便處方及

[10] https://www.reo.gov.hk/pdf/incident_report/Summary_Report_data_breach_incident_April2022(Chi).pdf

其他有關部門就該選舉可在投票日或在有需要的情況下以短訊或電郵方式就最新的選舉安排或緊急應變措施作出即時通知。

40. 處方其後於 2022 年 4 月 22 日再向選委發出郵件，提醒他們若在投票日出現緊急或突發情況（例如需要更改投票日期或時間、實施投票或點票應變措施），處方將會向選委提供的流動電話號碼及／或電郵地址發出短訊及／或電郵，以通知選委最新選舉安排或緊急應變措施。處方並計劃於 2022 年 4 月 27 日發送測試短訊及／或電郵給已提供流動電話號碼及／或電郵地址的選委及／或其助理，以確保他們能接收相關資訊。

41. 測試短訊及／或電郵的發送由一名選舉事務主任（該選舉事務主任）負責，並由四名行政助理協助。處方在收到選委及其助理提供的回條後，會以人手將回條上涉及約 1,800 名選委及其助理的資料，包括選委的地址、電郵地址及流動電話號碼，及選委助理的姓名、電郵地址及流動電話號碼輸入至一份電腦資料總表（該資料總表），並由該選舉事務主任及四名行政助理加以核對。

42. 處方其後安排了一名高級項目主任（該高級項目主任）負責監督是次發送測試電郵（及短訊）的工作。由於該高級項目主任於 2022 年 4 月 27 日（即處方計劃發送測試電郵的日期）作出多次核對後仍發現該資料總表存在不準確的資料，遂指示職員分批次核對電郵地址及發送測試電郵。另一方面，由於多數回條是以電郵方式提交，考慮到列印回條需時及會造成浪費，因此有關職員直接以電子版回條進行核對。

43. 測試電郵由兩名行政助理草擬，經過以下的核對步驟，才能從行政助理的電腦發出：

	負責職員	所需的核對步驟
第一次檢查	行政助理	在輸入該批次的收件人的電郵地址至測試電郵擬稿「副本密送」欄後，核對所輸入的電郵地址是否與選委及／或其助理提交的回條 上提供的電郵地址相同
第二次檢查	該選舉事務主任	檢查測試電郵擬稿的內容，並覆核於測試電郵擬稿所輸入的電郵地址是否與選委及／或其助理提交的回條上提供的電郵地址相同
第三次檢查	該高級項目主任	再次核對測試電郵擬稿的內容，以及於測試電郵擬稿輸入的電郵地址是否與選委及／或其助理提交的回條上提供的電郵地址相同

44. 為方便核對，負責發送測試電郵的行政助理會把電腦螢幕分為左右兩邊視窗，左邊顯示測試電郵擬稿，而右邊則顯示電子版回條。行政助理使用鍵盤的上下箭頭鍵選擇相應的回條（以預覽視窗方式顯示），逐一核對已輸入至測試電郵擬稿「副本密送」欄內的電郵地址。其後該選舉事務主任及該高級項目主任會於行政助理的電腦分別進行第二及第三次檢查。只有在該高級項目主任以電子版回條覆核有關電郵地址及確定測試電郵內容無誤後，行政助理才會按下「傳送」鍵發送有關電郵。

45. 處方於 2022 年 4 月 28 日凌晨 1 時 37 分開始分批次發送測試電郵。為加快程序，該高級項目主任指示自第四批次起省略第二次檢查，以安排該選舉事務主任協助草擬測試電郵。

46. 直至 2022 年 4 月 28 日早上 6 時 02 分，處方共發送 13 批次的測試電郵予 848 名選委及其助理。同時，該選舉事務主任在覆核已發出的測試電郵時，發現一個於上午 4 時 42 分發送予 38 名選委及 26 名選委助理的電郵，錯誤夾附了該回條。隨後，負責職員改以紙本版回條覆核有關電郵地址及確定測試電郵，並於 2022 年 4 月 29 日完成餘下 18 批次測試電郵的發送。

受影響的個人資料

47. 事件二涉及一名選委及其助理的姓名、電郵地址、電話號碼，及該名選委的簽署。

處方的調查結果

48. 處方於調查報告表示，根據草擬及核對測試電郵的工作流程，相信有職員在工作過程中，不小心把該回條錯誤夾附在一封測試電郵內，以致發生事件二。處方表示未能確認意外發生的實質過程，但認為以下兩個情況為可能發生的原因：—

(1) 行政助理在草擬測試電郵期間，有意圖或不小心地夾附該回條至測試電郵內；或
(2) 該高級項目主任在進行覆檢的過程中，有意圖或不小心地夾附該回條至測試電郵內。

49. 處方認為以人手輸入選委送交的回條上的資料，過程中容易出現錯誤，而職員核對電郵地址的方式導致電子版回條有可能被意外地夾附至測試電郵內。此外，職員在發出測試電郵前，並未再三確認該電郵有否夾附其他不適當的附件。

處方的跟進工作及改善措施

50. 在發現事件二後，處方立即改以紙本回條核對餘下批次測試電郵的電郵地址，以避免不小心把電子版的回條錯誤夾附在測試電郵內。

51. 處方於 2022 年 4 月 28 日通知收到該回條的選委及／或其助理，要求他們立即及永久性刪除該回條，並就是次事件致電通知該名受影響的選委及其助理並致歉。

52. 為進一步加強資料安全並防止類似事件再次發生，處方承諾不時檢視處理個人資料的工作流程及作出合適改善措施，並避免採用容易導致不適當地處理個人資料的工作程序。同時，處方亦承諾探討利用資訊科技以收集選委個人資料及發送大量電郵的可行性，以避免出現人為錯誤。

調查結果及違例事項

處方屬事件二的資料使用者

53. 與事件一的情況相同，處方在事件二屬《私隱條例》第 2(1)條釋義下的資料使用者，須遵從《私隱條例》的規定行事，包括《私隱條例》附表一所列明的六項保障資料原則。

保障資料第 4(1)原則

54. 如上文所述，根據《私隱條例》附表一保障資料第 4(1)原則，資料使用者須採取所有切實可行的步驟，以確保由資料使用者持有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。

55. 經考慮與事件二有關的事實及在調查過程中所獲得的證據，專員認為以下原因導致事件二發生：—

(1) 職員疏忽及資料保障的意識不足

56. 處方於調查報告表示，相信有職員在工作過程中，不小心把該回條錯誤夾附在一封測試電郵內，以致發生事件二。處方並認為以下兩個情況為可能發生的原因；行政助理在草擬測試電郵期間，有意圖或不小心地夾附該回條至測試電郵內；或該高級項目主任在進行覆檢的過程中，有意圖或不小心地夾附該回條至測試電郵內。明顯地，如果有關職員在編制該資料總表和檢查核對測試電郵擬稿時更加謹慎，本應可以避免事件二的發生。事實上，錯誤地附有該回條的測試電郵擬稿在發出前理應已經過兩層檢查，相關職員在兩層的檢查時理應可以發現錯誤。事件二的發生清楚反映了涉事職員欠缺保障個人資料的意識及確保個人資料準確的警覺性。

(2) 處方的工作流程明顯存有不足

57. 根據處方的工作流程，與事件二有關的回條所載的選委及其助理的個人資料是由人手輸入至該資料總表，而沒有任何較有系統的核對安排。該高級項目主任在發出測試電郵的預定日期當天（即 2022 年 4 月 27 日）才首次收到該資料總表，卻發現當中的資料並不準確。

58. 由於未能確保該資料總表的準確性，導致處方須在非正常的工作時間對測試電郵擬稿中的電子郵件地址進行最後一刻的核對（專員留意到附有該回條的電郵於 2022 年 4 月 28 日凌晨 4:42 發送）。這項超時的工作明顯地引致相關人員的工作疲勞從而增加人為錯誤的風險。若然處方早於 2022 年 4 月 27 日之前對該資料總表進行適當的核對並確保其準確性，則不需使用電子版回條以進行最後一刻的核對工作，而事件二應該不會發生。

59. 在核對測試電郵擬稿的工作模式方面，為方便核對，行政助理的電腦螢幕分為左右兩邊視窗，左邊顯示測試電郵擬稿，右邊則顯示電子版回條。行政助理使用鍵盤的上下箭頭鍵選擇相應的回條（透過預覽視窗方式顯示），逐一核對已輸入至測試電郵擬稿「副本密送」欄內的電郵地址。上述的核對方式顯然是導致職員意外地將該回條拖曳到涉事的測試電郵的主要原因。這項安排看來是為工作方便而臨時採用的，顯示出處方未有將私隱保障納入相關的工作流程，亦未有充分評估有關安排對個人資料私隱的影響。

60. 事實上，該高級項目主任在某個階段為加快程序省略第二次檢查，以安排該選舉事務主任協助草擬測試電郵。這大大削弱了原先三層檢查機制的有效性，亦是導致事件二的因素之一。

(3) 相關工作欠缺書面程序

61. 處方沒有就發送測試電郵的機制，包括上文第 43 至 44 段的核對步驟制定任何書面程序，而僅依賴職員之間就所涉及的工作流程進行的溝通。 在沒有書面程序以明確訂明在發送測試電郵之前所須的檢查步驟的情況下，人為偏差及未有依循所需步驟的風險自然增加，從而削弱相關的保障個人資料措施。

結論：違反保障資料第 4(1)原則

62. 在考慮本個案所有證據後，**專員認為事件二主要是由人為錯誤所引起。事件二是由於相關職員的疏忽及缺乏資料保障的意識，以及處方相關工作流程的不足所導致。在事件二當中，不準確的資料總表明顯地導致了工作流程的突然改變，以致職員須在午夜之後對測試電郵擬稿中的電郵地址與電子版回條進行最後一刻的核對。專員認為如果處方備有恰當的工作流程，以確保該資料總表能適時及準確地備妥，有關職員則毋須在時間緊迫下進行最後一刻的人手核對，**

亦毋須利用不穩妥的方式進行核對；同時，如果相關職員在核對的過程中更為謹慎，應可避免事件二的發生。

63. 另一方面，處方沒有就發送測試電郵的機制，包括核對步驟制定任何書面程序，從而增加了人為偏差及未有依循所需步驟的風險。專員理解處方職員進行最後一刻的核對時所面對的壓力，但書面程序的欠缺無可避免地增加了人為錯誤的風險，尤其是考慮到當職員須長時間工作，以及為了加快整個工作流程而省略了第二次檢查，以致削弱了原先三層檢查機制的有效性。

64. 鑑於上述情況，專員認為處方沒有採取所有切實可行的步驟確保所持有的選委及其助理的個人資料受到保障，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，因而違反了保障資料第 **4(1)**原則有關個人資料保安的規定。

執法行動

65. 根據《私隱條例》第 50(1)條，如專員在完成一項調查後，認為有關的資料使用者正在或已經違反《私隱條例》的規定，專員可向該資料使用者送達書面通知，指示該資料使用者糾正該項違反，以及（如適當的話）防止該項違反再發生。

事件一

66. 專員認為在事件一當中處方違反了《私隱條例》附表一的保障資料第 4(1) 原則，因此已根據《私隱條例》第 50(1)條所賦予的權力向處方送達執行通知，指示處方採取以下步驟以糾正，以及防止有關違規情況再發生：

(1) 採取技術性保安措施，以限制未獲授權的職員使用任何處方配置的電郵系統傳送載有個人資料的郵件或檔案至非處方的電郵帳戶；

(2) 加強有關資訊保安及個人資料保障的培訓，包括：

(i) 每年為全體職員舉辦最少兩次有關資訊保安及個人資料保障的講座／研討會／工作坊；

(ii) 為所有新入職職員提供有關資訊保安及個人資料保障的講座／研討會／工作坊，並設立考核機制以確保職員明白有關課程的內容；及

(iii) 設立機制，讓職員每年重溫有關資訊保安及個人資料保障培訓的材料；

(3) 妥善記錄上述(2)的培訓進度，並每年檢視及評估有關培訓的參與度及有效程度，以確保相關培訓的有效性，並涵蓋最新

的資訊；及

(4) 由執行通知的日期起計兩個月內向專員提供文件，證明已實施上述第 (1)至(3)項指示。

事件二

67. 專員認為在事件二當中處方違反了《私隱條例》附表一的保障資料第 4(1) 原則，因此已根據《私隱條例》第 50(1)條所賦予的權力向處方送達執行通知，指示處方採取以下步驟以糾正，以及防止有關違規情況再發生：

(1) 檢視並改善收集選委個人資料及發送大量附有個人資料的電郵的工作流程；

(2) 根據上述(1)的檢視結果，制訂／修訂相關的書面操作程序／指引，當中須包括向選委及有關人士發出測試電郵（如處方日後仍會發出測試電郵）的具體程序；及

(3) 加強有關資訊保安及資料保障的培訓，包括：

(i) 每年為全體職員舉辦最少兩次有關資訊保安及個人資料保障的講座／研討會／工作坊；

(ii) 為所有新入職職員提供有關資訊保安及個人資料保障的講座／研討會／工作坊，並設立考核機制以確保職員明白有關課程的內容；及

(iii) 設立機制，讓職員每年重溫有關資訊保安及個人資料保障培訓的材料；

(4) 妥善記錄上述(3)的培訓進度，並每年檢視及評估有關培訓的參與度及有效程度，以確保相關培訓的有效性，並涵蓋最新

的資訊；及

(5) 由執行通知的日期起計兩個月內向專員提供文件，證明已實施上述第 (1)至(4)項指示。

68. 根據《私隱條例》第 50A 條，資料使用者違反執行通知，即屬犯罪，一經首次定罪，最高可被判處第五級罰款（即港幣 50,000 元）及監禁兩年。

69. 誠上所述，專員認為兩宗資料外洩事故都涉及人為疏忽。專員留意到，處方表示正根據公務員紀律處分機制跟進有關職員的不當行為。由於這次的調查範圍是處方在有關事件中有否根據《私隱條例》附表一的保障資料第 4(1) 原則對所持有的個人資料採取足夠的保安措施，處方就有關事件對個別職員所採取的紀律處分行動並非本報告的涵蓋範圍。

70. 雖然處方在資訊保安及個人資料保障的培訓，以及資訊保安措施方面有待改善，專員樂見處方在兩宗資料外洩事故發生後及時作出資料外洩事故通報，配合私隱專員公署的調查，並致力從事件中汲取教訓。專員留意到，處方已加強保安措施及檢視相關的處理個人資料的工作流程，以加強個人資料私隱的保障。

建議

71. 《私隱條例》第 48(2)條訂明，專員在完成一項調查後，如認為如此行事是符合公眾利益的，可發表報告列明該項調查的結果及由該項調查引致的、專員認為適合作出的任何建議或其他評論。專員除了根據《私隱條例》第 50(1)條就有關的兩宗資料外洩事故向處方送達執行通知外，亦希望藉此報告，向持有大量個人資料的機構作出下述建議。

貫徹落實個人資料私隱管理系統

72. 資料使用者，尤其是持有大量個人資料的機構，應推行個人資料私隱管理系統，將個人資料私隱管理納入數據管治的一環。個人資料私隱管理系統有助機構管理由收集至銷毀個人資料的整個生命週期，令機構可迅速應對任何資料外洩事故，並確保遵從《私隱條例》的規定。

就非常規的工作安排進行私隱風險評估並制訂具針對性的指引

73. 資料使用者應就非常規的工作安排（例如在家工作，或涉及處理大量個人資料的工序）進行私隱風險評估，以評估有關安排對資料保安及個人資料私隱方面構成的風險。機構應按照風險評估的結果，審視現有政策及工作流程，作出適當的修訂，或考慮制訂具針對性的指引，以供職員依循。

建立有效的教育及培訓計劃

74. 資料使用者，特別是持有大量個人資料的機構，應讓職員了解尊重及保護個人資料私隱以及遵守《私隱條例》規定的重要性。就此，機構應建立合適的教育及培訓計劃，以有效並持續地將個人資料保安政策、程序及實務指引傳遞予所有職員，確保他們得悉並了解有

關的政策內容及要求，並提供清晰的途徑，讓他們能快捷地搜尋相關資訊。此外，機構亦應採取措施定期檢視有關計劃的成效。

使用資訊保安措施以減少人為錯誤的風險

75. 處理大量個人資料的機構應考慮廣泛地使用科技以減少人為錯誤的風險。在日常處理個人資料方面，機構可考慮使用自動化的方式或配置合適的系統以收集、處理及比對個人資料，以增加資料的準確性；而在個人資料保安方面，機構應配置合適的保安技術措施，以有效地保障機構持有的個人資料，並監控職員使用資訊設備（包括電郵系統）的情況，從而避免資料外洩事故。

－完－