調查報告

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

根據香港法例第486章《個人資料（私隱）條例》第 48(2)條
發表的調查報告

選舉事務處

載有選委、選民個人資料的手提電腦遺失事件

報告編號：R17 – 6429

2017 年 6 月 12 日

選舉事務處
載有選委、選民個人資料的手提電腦遺失事件

香港法例第 486 章《個人資料（私隱）條例》（下稱「**條例**」）第 48(2) 條訂明，「[香港個人資料私隱]*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。」

現根據條例第 48(2) 條履行所賦予的權力和責任，發表本調查報告。

黃繼兒
香港個人資料私隱專員
2017 年 6 月 12 日

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
載有選委、選民個人資料的手提電腦遺失事件

<u>摘要</u>

香港個人資料私隱專員（下稱「**私隱專員**」）就選舉事務處（下稱「**處方**」）在2017年行政長官選舉翌日（即2017年3月27日）發現載有約1,200名選舉委員會委員（下稱「**選委**」）及約378萬名地方選區選民（當中包括選委）（下稱「**選民**」）個人資料的兩部手提電腦遺失事件展開調查，並發表本報告。

第一部手提電腦（下稱「**第一部手提電腦**」）只載有選委的姓名，屬公開資料，加上姓名本身不屬敏感的個人資料，私隱專員認為即使遺失第一部手提電腦而令選委的姓名外洩，為選委造成損害的機會不大。而處方就載有個人資料（選委的姓名）的第一部手提電腦所採取的保安措施（包括以密碼保護資料及將有關電腦存放在已上鎖的房間內）尚屬足夠。此外，由於選委可於行政長官選舉中投票，私隱專員認為處方將選委姓名下載於第一部手提電腦以記錄補發載有選委個人資料的名牌的做法可以接受。考慮過所有有關情況後，私隱專員裁定處方沒有因遺失載有選委個人資料的第一部手提電腦而違反香港法例第 486 章《個人資料（私隱）條例》（下稱「**條例**」）保障資料第 4(1)項「資料保安」原則。

第二部手提電腦（下稱「**第二部手提電腦**」）除儲存可供公眾於正式選民登記冊查閱的全體選民姓名、地址外，還載有不作公開查閱兼屬敏感個人資料的選民身份證號碼。私隱專員認為有關第二部手提電腦遺失個案的案情獨特，亦沒有先例可援。雖然所涉及選民的個人資料已經過多重加密儲存，資料外洩風險低，但處方應可避免遺失載有全體選民個人資料的第二部手提電腦，因而引起的關注可以理解。私隱專員認為，處方在檢視及審批使用載有選民的非公開並屬敏感的個人資料的查詢系統一事非常粗疏，蕭規曹隨，只顧依從過往做法，卻沒有適時按情況檢視或更新，從而制訂一套完善的制度。為了提供所聲

稱的服務而備存全體選民的個人資料所帶來的效益與引申的風險亦不合符比例。所採取的保安措施與資料的敏感程度和資料洩漏可能引致的損害，平衡失據。調查結果顯示處方對個人資料私隱保障認知、警覺性和內部溝通不足，應用和實施各項指引的規例欠缺清晰或沒有依從，未能滿足大眾的期望，沒有按實際情況和需要採取所有合理地切實可行的步驟，確保選民的個人資料受保障而不受意外的喪失所影響，因而違反條例下的保障資料第 4(1)原則。私隱專員已根據條例第 50(1)條向處方送達執行通知，以糾正違規事宜及防止事故重演。

背景

1. 香港個人資料私隱專員公署（下稱「**公署**」）在 2017 年行政長官選舉翌日（即 2017 年 3 月 27 日）收到處方的口頭通知，表示處方當日發現在 2017 年行政長官選舉的後備場地亞洲國際博覽館遺失了兩部手提電腦：第一部手提電腦載有約 1,200 名選委的姓名；第二部手提電腦載有約 378 萬名選民（包括選委）的姓名、身份證號碼及地址。處方並於 2017 年 3 月 28 日向公署遞交「資料外洩事故通報表格」。

2. 私隱專員隨即跟進事件，並根據條例第 38(b)條[1]展開調查。

條例的相關規定

3. 條例旨在保障個人資料私隱。總括來說，資料使用者（一般指公、私營機構）有責任依從條例附表 1 的 6 項保障資料原則[2]的規定。

[1] 條例第 38 條訂明：「*由專員進行的調查：凡專員 (a) 收到一項投訴；或 (b) 有合理理由相信有符合以下說明的作為或行為 —(i) 已經或正在(視屬何情況而定)由資料使用者作出或從事的；(ii) 關乎個人資料的；及 (iii) 可能屬違反本條例下的規定的，則 —(i) 如(a)段適用，除第 39 條另有規定外，專員須就有關的資料使用者進行調查，以確定在有關的投訴中指明的作為或行為是否屬違反本條例下的規定；(ii) 如(b)段適用，專員可就有關的資料使用者進行調查，以確定該段所提述的作為或行為是否屬違反本條例下的規定。*」(https://www.elegislation.gov.hk/hk/cap486!zh-Hant-HK@2013-04-25T00:00:00/s38?clpid=153326)。

[2] 6 項保障資料原則為：1) 收集資料原則；2) 資料準確及保留原則； 3) 資料使用原則； 4) 資料保安原則； 5) 公開政策原則； 6) 查閱及更改原則，見條例附表 1 (https://www.elegislation.gov.hk/hk/cap486!zh-Hant-HK@2013-04-25T00:00:00/sch1?clpid=228384)。

4. 與本調查直接有關的是條例附表 1 所訂明的保障資料第 4(1)原則：

「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（包括採用不能切實可行地予以查閱或處理的形式的資料）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。」

5. 根據條例第 2(1)條：─

「資料使用者」，就個人資料而言，指獨自或聯同其他人或與其他人共同控制個人資料的收集、持有、處理或使用的人。

「個人資料」指與一名在世人士有關的資料，有關資料是儲存在記錄內，可加以處理或查閱，並且從該資料可直接或間接識辨該名人士的身份。

「切實可行」指合理地切實可行。

公署所獲得的相關資料

6. 根據條例第 38(b)條，私隱專員有合理理由相信處方遺失了載有個人資料的手提電腦的作為有可能屬違反條例的規定，因此進行調查，以確定處方是否違規。為確保公正的執法，私隱專員注意到事實的準確性至為重要。

7. 在處理本個案的過程中，公署曾與處方執行部、選舉部、行政部

和資訊科技管理組代表會面及作出查詢；審視處方提供的文件證據及其他公開資料；要求處方向公署及政府資訊科技總監辦公室代表展示和解釋查閱選民資料的流程及手提電腦內的保安措施；並向電腦保安專家諮詢專業意見。以下為公署所獲得的相關資料。

處方的職能及 2017 年行政長官選舉

8. 處方為選舉管理委員會的行政部門，職能包括協助選舉管理委員會有效執行香港法例第 541 章《選舉管理委員會條例》下的法定職能，並執行選舉管理委員會就地方選區及區議會選區的分界、選民登記及選舉事宜所作出的決定[3]。

9. 為執行與選舉有關的工作，處方收集、持有、處理及使用選民的個人資料，當中包括姓名、身份證號碼、地址、所屬選區和界別、電話號碼、電郵地址、傳真號碼和簽名。

10. 2017 年行政長官選舉於 2017 年 3 月 26 日舉行。中央投票站、中央點票站及傳媒中心的主場地設於灣仔香港會議展覽中心（下稱「**主場地**」），後備場地則設於赤鱲角亞洲國際博覽館（下稱「**後備場地**」）。

11. 處方表示有必要為後備場地作充足準備，包括安排所需的電腦，並在投票日前確保相關電腦系統運作正常。鑑於行政長官選舉的投票時間相對較短，加上後備場地地點遠離主場地，大部份選舉物資均預先安排，以便處方能在最短時間內啟動後備場地並展開投票程序。

報稱遺失事件

12. 根據處方的資料，報稱遺失事件發生的時序如下：—

2017 年 3 月 22 日	處方職員開始於後備場地進行準備工作。所有電腦設備（包括涉事的兩部手提電腦）

[3] 見 http://www.reo.gov.hk/ch/about/ceo_msg.htm。

	被存放於後備場地的 107 號房間(下稱「**該房間**」)。
3 月 23 至 24 日	處方職員曾將該兩部手提電腦攜離該房間，以進行測試；每次測試完成後均由職員關上手提電腦，然後放回該房間。
3 月 24 日	處方職員在完成最後一次測試後關上該兩部手提電腦，將該兩部手提電腦放置於該房間內的一個紙皮箱上，然後離開。
3 月 25 至 26(行政長官選舉日)日	處方職員曾巡視和檢查後備場地，但沒有進入該房間。
3 月 27 日約中午	處方職員在後備場地收拾物資時發現遺失該兩部手提電腦。

13. 處方於 2017 年 3 月 27 日就遺失事件報警，警方已將案件列作盜竊案處理，至今仍在調查中。截至 2017 年 6 月 11 日為止，公署共接獲 92 宗查詢[4]和 1,968 宗投訴[5]，但沒有資料或證據顯示是次遺失事件涉及的個人資料已外洩或遭盜用。

涉及的個人資料

14. 處方表示，第一部手提電腦只載有 1,194 名選委已公開的姓名，儲存在有密碼保護的試算表格式的檔案內；第二部手提電腦則載有 2016 年正式選民登記冊內約 378 萬名選民（當中包括選委）的姓名、地址、身份證號碼、其所屬選區和界別等較登記冊為多的資料，儲存在已加密的選民資料查詢系統（下稱「**該系統**」）內；兩部手提電腦均沒有儲存任何投票記錄和電話號碼。

[4] 查詢者主要表達對處方的不滿、查詢自我保護的方法、更換身份證號碼的可能和公署的調查進度等。

[5] 98%的投訴人向公署反映對個人資料可能洩漏的憂慮，大部份的投訴是使用源於某社交媒體倡議的「一人一信」活動提供的範本提出的，內容完全相同。

為行政長官選舉備存全體選民資料

15. 處方解釋，該系統原本是為受羈押人士投票而設。在過往的立法會及區議會選舉中，指定警署內會設立一個專用投票站並設置該系統。假若有受羈押人士在投票日要求投票，專用投票站的有關職員會透過該系統核實該人士的選民資格。由於受羈押人士可能是任何選區的選民，故該系統儲存了全港選民的資料，以便核對。

16. 在 2007 年、2012 年和 2017 年的三屆行政長官選舉中，該系統亦曾用作核實忘記攜帶選委名牌的選委的資格及解答可能出現的各種關於選民的查詢。如有人對自己是否屬一名合資格的選委有所懷疑，處方會透過該系統即時查核其選民登記資料，向其解釋選民登記詳情，以解答其查詢。

17. 處方表示，後備場地共存放了 6 部載有該系統的手提電腦（包括第二部手提電腦）。在要啟動後備場地時，第二部手提電腦將會放置在選委名牌補發櫃檯，另外 5 部則會放置在中央投票站內的特別櫃檯和投票站主任工作檯。此外，處方表示第一部手提電腦中載有選委姓名的檔案是用於記錄因忘記攜帶而要重發選委名牌的個案。

申請和審批程序

18. 處方表示於 2007 年首次在行政長官選舉中使用該系統。然而，處方未能提供任何就該次選舉中有關審批使用該系統的資料，亦未能確認上述的使用是否已獲審批。

19. 就 2017 年行政長官選舉中使用該系統的情況，處方僅提供選舉部 4 中央點票組[6]於 2016 年 10 月 13 日向資訊科技管理組提交的一份「進出主場館管制系統」的「用戶要求」草擬本的電郵。「用戶要求」草擬本當中訂明需參照 2012 年行政長官選舉的安排而設立「進出主場館管制系統」，當中包括用以核實選委身份及安

[6] 選舉部共有四個組別（1 至 4）。選舉部 4 中央點票組協助籌備 2017 年行政長官選舉，工作範圍包括安排主場館的整體保安措施及場地進出管制的事宜。

排補發名牌的程序。然而，處方沒有提供任何資料顯示 2012 或 2017 年的行政長官選舉中使用該系統已獲審批。

20. 除審批使用該系統權限外，公署亦曾要求處方提交有關手提電腦內裝設該系統的審批文件。處方表示，根據處方的《使用電腦及資訊科技相關設備和服務的指引》[7]，部門可授權下載選民資料至手提電腦，但沒有列明相關的章節。就此，處方提供了選舉部 1 投票及點票站組[8]和選舉部 3 中央點票組[9]分別於 2017 年 2 月 19 日和 2017 年 2 月 23 日向資訊科技管理組發出的電郵，當中各自提出須於後備場地設置 5 部和 1 部載有該系統的手提電腦，作為審批證據。

手提電腦的運送和測試記錄

21. 處方表示，資訊科技管理組在根據選舉部 4 中央點票組的「用戶要求」準備相關電腦設備後，記錄了當中所有電腦的品牌、型號、出廠序號、處方存貨編號及為該選舉設置的特定編號等。資訊科技管理組亦編制出一份運送表，以點算及檢查運送到後備場地的電腦設備。

22. 運送到後備場地後的手提電腦由資訊科技管理組進行測試。第二部手提電腦只經過開機測試，但並沒有記錄測試結果。

23. 此外，處方表示，根據供資訊科技管理組填寫的出勤記錄，共有 15 名職員曾於 2017 年 3 月 22 至 24 日和 2017 年 3 月 27 日進入該房間。沒有記錄顯示 2017 年 3 月 25 至 26 日期間有任何處方職員曾進入該房間。

處方的資料保安措施

24. 處方表示在後備場地採取了下述的保安措施：—

[7] 該指引日期為 2008 年 8 月 29 日。

[8] 選舉部 1 投票及點票站組主要負責投票站的相關安排。

[9] 選舉部 3 中央點票組主要負責後備場地的場地支援服務。

技術保安措施

(i) 儲存於第二部手提電腦的選民個人資料已進行加密儲存，採用的加密技術高於政府資訊科技總監辦公室的《資訊科技保安指引》[10]所建議的級別（由於加密技術具高度敏感性，相關詳情不會在此報告中披露；此外，公署要求處方展示與第二部手提電腦保安設置一致的電腦，檢視的結果見第 39 段）；

(ii) 由開啟第二部手提電腦至讀取選民資料，需輸入多重密碼（由於密碼的長度與組合具高度敏感性，相關詳情不會在此報告中披露；公署就處方處理密碼的觀察見第 56 至 57 段）。

(iii) 縱使第二部手提電腦曾有多次不成功登入，所儲存的數據不會被自動刪除。但每次登入失敗後，下一次登錄過程會被延遲，延遲時間從兩秒增加至最多 20 秒；

(iv) 處方曾在 2017 年 4 月 11 日立法會政制事務委員會特別會議上表示共有 5 名職員知悉第二部手提電腦的密碼。其後，處方在 2017 年 4 月 13 日與公署會面時再次確認共有 5 名職員知悉第二部手提電腦的密碼，並表示載有密碼的檔案是以電郵方式傳遞予獲授權的職員。然而，在公署要求提供該電郵副本時，處方卻表示負責的資訊科技管理組職員沒有發出該電郵，只列印了密碼交予另一名資訊科技管理組的職員。處方最終聲稱只有兩名職員知悉密碼；

(v) 在後備場地共有 6 部手提電腦安裝有該系統，該 6 部手提電腦的所有設定（包括密碼）原本都是相同的。處方表示只更改了第二部手提電腦的密碼，而其餘 5 部則保留原有密碼；

(vi) 除上述第(iv)段所指的兩名資訊科技管理組職員外，另有 6 名在投票站工作的職員獲授權知悉其他 5 部手提電腦的

[10] 2016 年 12 月第 8.0 版第 12 段。

密碼。有關密碼是以加密電郵形式傳送予其中一名投票站工作的職員，而該名職員再以未經加密電郵通知其中 4 名職員，並將有關密碼的次序重組後儲存在其手提電話內供餘下一名職員查看；

(vii) 密碼（包括第一部手提電腦、第二部手提電腦及其餘 5 部手提電腦的密碼）並沒有以任何方式張貼或展示在手提電腦或存放在該房間的物品上；

(viii) 職員在每次測試完畢後均會關上手提電腦，第一部手提電腦及第二部手提電腦在遺失時是處於關機狀態；

實體保安措施

(ix) 處方在與後備場地的管理公司（亞洲國際博覽館）簽訂的許可使用時段內（即 2017 年 3 月 22 至 28 日）額外安排了 34 名保安主任、152 名保安主管及 275 名保安員於後備場地內的各處巡視及駐守，當中包括安排了保安人員在該房間外的走廊位置輪班駐守；

(x) 處方在後備場地的不同位置額外加裝了 29 台閉路電視鏡頭（包括在該房間正門外的走廊）；

(xi) 該房間原是一間儲物室。在 2017 年行政長官選舉期間，該房間是處方伺服器室及資訊科技管理組辦公室，房間正門被標記為 ITMU Office。該房間共有 3 個出入口，處方持有的電子咭片鎖匙只能開啟其中兩個出入口的門鎖，該兩個出入口使用電腦鎖，在所有時間均自動鎖上。處方在 2017 年 3 月 22 至 24 日將其中一個出入口從內上鎖，職員均須利用電子咭片鎖匙從另一出入口進出該房間。處方表示，該房間的其餘一個出入口由亞洲國際博覽館長期鎖上；

(xii) 處方持有該房間的兩張電子咭片鎖匙，由資訊科技管理組兩名選舉助理保管，他倆並不知悉安裝有該系統的手提電

腦（包括第二部手提電腦）密碼。每次有處方職員需進入該房間時，均會由上述的其中一名選舉助理陪同進入。如該兩名選舉助理需離開該房間，其他獲授權進入該房間並逗留在該房間的資訊科技管理組職員會按照授權進入該房間的列表，讓其他授權人士[11]進入該房間；

(xiii) 處方職員在每天工作開始前和完畢後，必須經後備場地的控制中心分別啟動和關閉該房間的相應電子咭片鎖匙。處方表示在 2017 年 3 月 24 日工作完畢後，處方職員已指示控制中心停用該房間的電子咭片鎖匙，即是說，除非控制中心再次啟動電子咭片鎖匙，否則電子咭片鎖匙無法開啟門鎖；及

(xiv) 處方表示，在辦公時間內，當有訪客要進入該房間時，該房間內的資訊科技管理組職員會查詢訪客到訪的目的，並決定是否讓訪客進入該房間。只有提出合理的到訪目的的訪客才會被准許進入該房間，如：安裝室內電話、檢查機房設備等。該房間內的資訊科技管理組職員亦會全程陪同訪客，防止訪客接近存放電腦設備的範圍或在未經許可下，對該房間內部進行拍攝。

25. 處方表示曾與亞洲國際博覽館於 2017 年 2 月 1 日和 2017 年 3 月 8 日的後備場地工作會議中商討場地保安安排；處方亦曾就後備場地的保安人員部署計劃及閉路電視安裝位置諮詢警方的意見，並於 2017 年 3 月 8 日的後備場地工作會議中向警方解釋有關安排。

處方的私隱管理

政策及指引

26. 處方表示，所有職員均須遵守處方發出的兩份有關保障私隱的通

[11]處方共有 38 名資訊科技管理組的職員獲授權進出該房間，他們的主要職責是安裝及測試電腦系統和管理場地電腦物資等。

告[12]，當中訂明職員須遵從條例的規定和列出處方的個人資料政策及實務指引。其中一份通告述明身份證號碼屬敏感的個人資料，列明須採取所有切實可行的步驟，使敏感的個人資料只限在「有需要知道」和「有需要使用」的原則下被查閱和處理，以及確保敏感的個人資料受保障而不受未獲准許的或意外的查閱、披露、處理、刪除、或其他使用所影響。該兩份通告每 6 個月傳閱一次。

27. 此外，處方向公署提供了一份由負責處理選民登記的執行部制訂的《執行部處理選民個人資料指引和資料保障措施》的行政通告[13]。該行政通告供執行部的職員遵循，並在資料安全方面列明*「輸出個人資料須獲相關組別授權」*和*「為免資料洩漏，除非絕對有必要，使用者不得使用手提電子裝置儲存個人資料」*。然而，處方其後向公署表示此行政通告不適用於負責 2017 年行政長官選舉的選舉部。

28. 處方表示，他們依從香港特別行政區政府規例中的《保安規例》[14]、政府資訊科技總監辦公室的《基準資訊科技保安政策》[15]和《資訊科技保安指引》[16]的相關條款來處理手提電腦內的資料。此外，處方制訂有《使用電腦及資訊科技相關設備和服務的指引》[17]，就如何正確使用處方的電腦及其他資訊科技設備和服務提供指引。

職員操守及培訓

29. 處方資訊科技管理組的所有合約職員以及獲授權查閱手提電腦內

[12]兩份通告分別是"Departmental Staff Circular Memorandum No. 1/2016 – Compliance with the Personal Data (Privacy) Ordinance"（日期為 2016 年 4 月 7 日，並於 2017 年 4 月更新）和 "REO Administrative Circular No. 3/2006 – Administrative Procedures for Dealing with Data Holding/Access/Correction Requests on Employment-Related Personal Data"（日期為 2006 年 7 月 6 日，並於 2017 年 4 月更新）。

[13] 該通告於 2014 年 8 月 29 日制訂。

[14] 2016 年 12 月更新版本。

[15] 2016 年 12 月的第 6.0 版。

[16] 2016 年 12 月第 8.0 版。

[17] 該指引日期為 2008 年 8 月 29 日。

選民資料的職員均須在入職時簽署不披露協議及入職聲明，內容有列明須遵守條例和香港法例第 521 章《官方機密條例》，以確保他們具有良好操守、審慎態度和相應能力。

30. 處方在 2017 年 3 月 15 日舉行的選舉工作人員一般簡介會中，為負責選委進場認證工作的職員提供了一份簡介，當中列明該系統是用於查核選委的身份，並示範了使用該系統的步驟。

31. 此外，處方向公署提供了 2016 年立法會換屆選舉的工作手冊及選舉委員會界別分組一般選舉的培訓資料中有關保障個人資料的摘錄。當中列明，如投票站主任於佈置日攜帶手提電腦往投票站作測試之用，他們於測試完畢後必須看管及保存手提電腦，而手提電腦不可留在投票站至投票日。

處方的跟進措施

32. 處方在發現遺失手提電腦的當天（即 2017 年 3 月 27 日）發出新聞公報公佈事件，政制及內地事務局和選舉管理委員會亦分別於 2017 年 3 月 27 及 28 日發出新聞公報，責成處方配合警方調查電腦遺失事件。處方其後於 2017 年 3 月 28 及 30 日和 2017 年 4 月 6 日發出新聞公報以回應傳媒查詢、澄清事件和致歉。

33. 處方期後於 2017 年 3 月 30 日起分批向約 55 萬名已提供電郵地址的選民發出電郵澄清事件，並於 2017 年 3 月 31 日起分批把信件郵寄予其餘選民，以提高資料當事人的警覺性和減低因事件可能引致的潛在損害。

34. 此外，處方亦已就事件致函各政府部門及不同界別的機構，包括金融、保險、電訊、零售、地產代理、資訊科技界別等行業，呼籲有關機構作出適當措施，以保障機構及資料當事人的利益。

35. 處方已於 2017 年 3 月 29 日刪除其餘 5 部載有該系統的手提電腦內的選民資料。

36. 總選舉事務主任於 2017 年 4 月 3 日出席立法會財務委員會特別會議，回應議員就事件的提問；並於 2017 年 4 月 11 日出席立法

會政制事務委員會特別會議解釋事件及相關跟進措施。

處方的初步檢視結果

37. 處方已初步檢視事件，並在提交予2017年4月11日立法會政制事務委員會特別會議的文件[18]中列出初步的檢視結果及擬議改善措施，內容簡述如下：—

(i) 基於不同的選民基礎，為立法會、區議會等選舉中受羈押人士而設的系統並不適宜應用在行政長官選舉中。在未來的行政長官選舉中，相關系統只會儲存有關選委的資料；

(ii) 有關提前將手提電腦存放在後備場地的做法，實有改善空間；在有需要啟用後備場地時才把電腦運送往後備場地是較為穩妥的做法；

(iii) 選舉場地，包括後備場地的詳細保安安排應由主管級職員審批，而主管級職員亦應向前線員工提供充足指示，以確保各項保安安排穩妥；及

(iv) 處方會連同相關部門代表全面檢討處方在收集、使用、處理和儲存選民資料的安排、系統要求和整體保安程序等，並會全面落實公署提出的任何改善措施及建議。

檢視電腦設置

38. 2017年4月13日，處方應公署要求使用一部與第二部手提電腦設置相同的手提電腦示範查閱選民資料的流程及相關技術保安措施，以評估所採用的電腦保安技術。考慮到披露技術詳情（例如加密軟件品牌、密碼組合、查閱資料步驟等）所帶來的風險，公署只邀請了政府資訊科技總監辦公室的專家出席該次示範，即時向處方提問和向公署提供專業意見。

[18] 整份文件可於下列網址下載：
http://www.legco.gov.hk/yr16-17/chinese/panels/ca/papers/ca20170411cb2-1167-1-c.pdf。

39. 考慮到政府內部保安和公眾利益，私隱專員將檢視電腦設置所得的結果、政府資訊科技總監辦公室的意見，以及處方在事後提供的補充資料中可公開的部份概述如下：－

(i) 手提電腦使用者需進入多個程式後才能透過該系統查閱選民資料，選民資料已獲多層加密保護；

(ii) 最穩固的其中一層保護表面上已達行業標準，即符合強加密要求，如要解拆的話，就需要以「暴力攻擊」[19]破解密碼。若以一般的商用電腦去破解這一層的加密算式，應該需要用上過百年的時間；

(iii) 由於在多次因輸入錯誤密碼而不能成功登入後，保護層會延長可再次登入的時間，即使以超級電腦快速攻擊密碼，但保護層則會以慢速來回應，故此破解密碼時間會被延長。究竟要猜估密碼多少次才成功則視乎超級電腦有多幸運；

(iv) 查閱選民資料並沒有採用雙重認證方式，即是說查閱者只需輸入數組正確的密碼而毋須使用另一種工具如電子證書、電子保安顯示器或手提電話便可開啟該系統，從而查閱資料；

(v) 進入該系統後並不會同時間顯示多於一名選民的資料。查閱者需先輸入一名選民的有效身份證號碼，該系統才會顯示該名選民的資料；及

(vi) 身份證號碼在儲存於該系統前已加密，其他的個人資料則以純文字儲存。

有關條例和調查結果

40. 根據保障資料第 4(1)原則，處方（資料使用者）須採取所有合理

[19] 根據政府資訊科技總監辦公室製作及管理的「資訊安全網」，「暴力攻擊」是指嘗試所有可能性以破解加密或認證系統的技術 (https://www.infosec.gov.hk/tc_chi/glossary/glossary_b.html)。

地切實可行的步驟，以確保所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[20]或使用所影響。當中尤其須考慮的情況包括*「該資料的種類及如該等事情*（如保安事故）*發生便能做成的損害」*。即是說，資料使用者採取的保安措施須與所涉及資料的敏感度及如發生保安事故可造成的損害相稱。「損害」不限於對資料當事人（選民）個人資料私隱的損害，而是包括所有因侵犯其個人資料私隱而引致的損害。

41. 保障資料第 4 原則並不是要求處方對其持有的個人資料的保安提供絕對保證。單因遺失儲存裝置而喪失個人資料並不代表處方已違反保障資料第 4 原則；反過來說，即使沒有直接證據證明個人資料已落入第三者手中，私隱專員仍須考慮處方在事件中所採取的保安措施方可決定處方有否違反保障資料第 4 原則的規定。

42. 由於公署的調查對象是處方而非個別職員，而處方已向公署提供有關保障個人資料的內部政策及守則，處方的任何跟進行動不會影響私隱專員對本個案的決定。

(A) 第一部手提電腦

43. 第一部手提電腦只載有選委的姓名，而有關資料已刊登在可供公眾查閱的選舉委員會正式委員登記冊內，公眾亦可在網上[21]閱覽，屬公開資料，加上姓名本身不屬敏感的個人資料，私隱專員認為即使遺失第一部手提電腦而令選委的姓名外洩，為選委造成損害

[20] 「喪失」一詞是由《2012 年個人資料(私隱)(修訂)條例》所引入的，明確要求資料使用者須採取相應的保安措施以防喪失個人資料。

[21] 選委姓名可於以下網址閱覽：

(1)「2016 年選舉委員會界別分組選舉」網址 (http://www.elections.gov.hk/ecss2016/chi/results.html?1496970116050) 查閱由界別分組選舉產生的選委的姓名；

(2) 2016 年 12 月 12 日的政府新聞公告 (http://www.info.gov.hk/gia/general/201612/12/P2016120900455.htm)查閱由宗教界界別分組提名產生的選委的姓名；及

(3)「 中國人大網」(http://www.npc.gov.cn/npc/gadbzl/xgdbzl_11/node_8514.htm)及立法會網址 (http://www.legco.gov.hk/general/chinese/members/memberslist/precedence/sixthlegislativecouncil_2016_2020.pdf)查閱當然委員（香港地區全國人民代表大會代表及立法會議員）的選委的姓名。

的機會不大。而處方就第一部手提電腦存有的個人資料（選委的姓名）所採取的保安措施（包括以密碼保護資料及將有關電腦存放在已上鎖的該房間內）尚屬足夠。

44. 此外，由於選委可於行政長官選舉中投票，私隱專員認為處方將選委姓名下載於第一部手提電腦以記錄補發名牌的做法可以接受。

45. 考慮過所有有關情況後，私隱專員裁定處方沒有因遺失載有選委個人資料的第一部手提電腦而違反條例保障資料第 4(1)項（資料保安）原則。

(B) 第二部手提電腦

46. 第二部手提電腦除儲存可供公眾於正式選民登記冊查閱的全體選民姓名、地址外，還載有不作公開查閱兼屬敏感個人資料的選民身份證號碼，不法之徒取得有關資料可能為選民帶來嚴重損害，包括盜用選民的身份進行詐騙等。故此，私隱專員在調查遺失第二部手提電腦時需重點考慮：(i)在行政長官選舉中使用的手提電腦儲存全體選民資料的需要；(ii)處方就個人資料保安的管理、政策和實務；和(iii)處方所採用的技術及實體保安措施。

(i) 在行政長官選舉中使用的手提電腦儲存全體選民資料的需要

47. 該系統載有約 378 萬名選民的個人資料，包括敏感的身份證號碼。私隱專員認為，處方在審批是否應該使用該系統，以至裝設該系統至較易遺失的手提電腦必須十分謹慎及具警覺性，以符合大眾期望。處方必須評估下載是否有必要，否則不可視為已採取所有合理地切實可行的步驟保護選民的個人資料。如無充分理由，處方便應避免下載選民資料，以減低資料外洩的風險。

48. 公署注意到該系統早於 2007 年行政長官選舉中已被應用，因而要求處方提供下載全體選民資料至手提電腦的審批權限、評估下載是否有必要的證據以及審批所根據的指引，但處方未能提供任何審批使用該系統的資料和依據，甚至未能向公署確認有關應用

已獲審批，私隱專員對此感到驚訝。

49. 同樣地，在籌辦 2017 年行政長官選舉方面，處方只能提供一份「進出主場館管制系統」的「用戶要求」草擬本電郵而未有任何其他審批記錄。然而，上述的草擬本看來沒有列明需要使用該系統，只表示需參照上一屆的行政長官選舉的安排，但其後在安排電腦設備時資訊科技管理組則按指示提供載有該系統的手提電腦。從選舉部有關組別向資訊科技管理組要求在主場地和後備場地設置電腦設備的電郵中，可見有 21 名職員得悉會使用載有該系統的手提電腦，當中包括屬主管級別的高級選舉事務主任。

50. 處方曾指出下載是根據《使用電腦及資訊科技相關設備和服務的指引》而獲授權。公署在審閱該指引後，認為相關指引可能包括*「未經有關組別主管事先批准，不得把敏感資料帶離辦公室」*、*「未經有關組別主管事先批准，不得把電腦器材、裝置或附件帶離辦公室」*或*「...提取特定資料的要求，應由二級行政主任/選舉事務助理或以上職級的人員經組別主管向 ITMU（資訊科技管理組）主管提交，並述明理據」*，但沒有提及在何種情況下可批准下載全體選民資料至手提電腦。

51. 從處方所提供的事實資料，私隱專員認為，處方在檢視及審批使用載有選民的非公開並屬敏感的個人資料的該系統一事非常粗疏，蕭規曹隨，只顧依從過往做法，卻沒有適時按情況檢視或更新，從而制訂一套完善的制度。

52. 此外，就為何處方在只有 1,194 名選委有資格投票的行政長官選舉中備存全體選民的個人資料，處方向公署解釋稱該些資料是用作核實選委的資格和解答可能出現的各種關於選民的查詢。私隱專員認為雖然這些目的一般而言可視為合理兼合法，但在行政長官選舉動用全體選民的個人資料，並不符合比例，平衡失據。

53. 既然處方設有選民資料網上查閱系統，如遇查詢，可利用該網上系統查閱資料或提供有關網址供選民參考，而無需使用儲存於手提電腦的資料。

(ii) 個人資料保安的管理、政策和實務

54. 處方的兩份關於保障私隱的通告[22]，當中只提醒職員須遵從條例的規定和簡略列出處方的個人資料政策及實務。然而，處方卻沒有就行政長官選舉中使用手提電腦以儲存選民的個人資料及須採用何種保障措施列明清晰的政策或內部指引。

(iii) 技術及實體保安措施

55. 處方強調資料已進行加密儲存，設有多重加密，極難破解。私隱專員知悉該加密標準為美國國家標準技術研究所認可並為美國政府機關所採用[23]。根據處方的回覆及所作的電腦示範，私隱專員認為處方已使用合理標準的方式來加密選民資料以及相關的程式及系統。

56. 公署留意到處方沒有依從處方的《使用電腦及資訊科技相關設備和服務的指引》及政府資訊科技總監辦公室的《資訊科技保安指引》有關密碼的要求[24]。雖則如此，資料顯示處方所採用的密碼並非簡單易破的密碼。系統設置需要查閱者先輸入正確密碼，再輸入某名選民的有效身份證號碼，才會顯示該名選民的姓名、地址及其所屬選區和界別。即是說，不獲授權的人士需先猜中密碼，再猜中某名選民的有效身份證號碼，才可查閱當中只屬於該名選民的資料。如密碼輸入錯誤，該系統則會延長可再次登入的時間。私隱專員接納處方所採用的加密技術和系統設置使非授權者要查閱所有選民資料將甚為艱難及耗時。

57. 雖有上述的技術保安措施，處方對登入手提電腦密碼的處理卻減弱了其效用。私隱專員認為共用密碼令處方無法確定何人曾查閱資料；再加上以未經加密的電郵方式傳遞密碼亦會增加密碼外洩的風險。私隱專員認為安排每位職員使用獨立的密碼、提供指引要求職員以穩妥的方法告知密碼是切實可行但處方未有採取相

[22] 即註腳 12 所指的兩份通告。

[23] 美國國家標準技術研究所 SP 800-131A 修訂 1 可於下列網址下載：http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf。

[24] 2016 年 12 月第 8.0 版第 11.4(c)段。

關措施。

58. 在實體保安措施方面，私隱專員知悉處方已採用了若干實體保安措施，包括將該房間上鎖、安排保安人員在該房間外的走廊位置輪班駐守、在該房間的正門外的走廊加裝閉路電視鏡頭；亦曾就實體保安措施徵詢警方的意見。

59. 然而，該房間的出入口並不在閉路電視攝錄範圍之內、處方沒有記錄出入該房間的人士的資料、而遺失的兩部手提電腦是被放置在紙皮箱上而非如在主場地般存放在上鎖的鋼櫃內。私隱專員因而認為處方在制訂實體保安措施時，未有充分考慮該房間會儲存重要和敏感的個人資料而加強該房間的保安。

60. 處方在初步檢視後承認在有需要啟用後備場地時才把電腦運送往後備場地較為穩妥，以及場地的詳細保安安排應由主管級職員審批，而主管級職員亦應向前線員工提供充足指示，以確保各項保安安排穩妥。此外，有意見指出在上鎖的房間內應再設有上鎖的儲物櫃以存放手提電腦、房間應設 24 小時保安、記錄每名出入該房間的人士、手提電腦應設遙控刪除檔案程式等更嚴謹的保安措施。私隱專員歡迎處方的改善措施及任何加強保護個人資料的建議。

61. 有關遺失第二部手提電腦一事，調查顯示處方(i)沒有充分檢視和評估在行政長官選舉中應否繼續使用和備存於便攜式儲存裝置（如手提電腦）內全體選民資料的必要和私隱風險；(ii) 沒有列明便攜式儲存裝置（包括手提電腦）儲存選民個人資料的清晰政策及內部指引；(iii)沒有向所有職員提供在行政長官選舉中保障選民資料的詳細指引；(iv)容許職員共用啟動該系統的密碼和粗疏處理密碼；以及(v)後備場地的實體保安安排有欠周詳。

62. 考慮過所有有關事實、情況和專家意見後，私隱專員認為有關第二部手提電腦遺失個案的案情獨特，亦沒有先例可援。雖然所涉及選民的個人資料已經過多重加密儲存，資料外洩風險低，但處方應可避免遺失載有全體選民個人資料的第二部手提電腦，因而引起的關注可以理解。處方為了提供所聲稱的服務而備存全體選

民的個人資料所帶來的效益與引申的風險亦不合符比例[25]。所採取的保安措施與資料的敏感程度和資料洩漏可能引致的損害，平衡失據。調查結果顯示處方對個人資料私隱保障認知、警覺性，應用和實施各項指引的規例欠缺清晰或沒有依從，內部溝通亦不足。根據調查獲得的所有資料，私隱專員認為處方沒有按實際情況和需要採取所有合理地切實可行的步驟，確保選民的個人資料受保障而不受意外的喪失所影響，因而違反條例下的保障資料第4(1) 項（資料保安）原則。

執行通知

63. 根據條例第 50(1)條，私隱專員在完成此調查後，如認為有關的資料使用者正在或已經違反條例的規定，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。

64. 基於公署調查發現處方在處理第二部手提電腦所涉及的個人資料一事違反有關規定，私隱專員決定根據條例第 50(1)條向處方送達執行通知，以糾正違規事宜及防止事故重演。私隱專員指令處方：—

(i) 禁止為行政長官選舉活動下載或使用地方選區選民的個人資料（姓名及地址除外）以作查詢之用並就此項指令定期向有關員工發出通告；

(ii) 制訂有關選舉活動中就處理個人資料的內部指引，包括：
   (a) 技術保安措施（資訊系統加密及密碼管理）；
   (b) 實體保安措施；
   (c) 使用手提電腦或其他便攜式儲存裝置的行政措施；及

(iii) 實施有效的措施，確保職員遵從這些指引。

[25] 參看 *Attorney General of Hong Kong v Lee Kwong-Kut* [1993] AC 951, (Privy Council); *HKSAR v LAM Hon Kwok Popy*, CACC 528/2004, 21 July 2006: *Hysan Development Co. Ltd. and Others v Town Planning Board* FACV 21/ 2015, 26 September 2016 (Court of Final Appeal)案中有關"合符比例"原則的闡釋。

建議

65. 另外，私隱專員根據本個案的情況就有關個人資料的議題作出以下 11 項建議：－

確保在有關選舉中只採用「需要」的個人資料

(i) 處方在處理所有選舉活動時，尤其涉及便攜式儲存裝置如手提電腦應採用「需要知道」和「需要使用」的原則，只備存必需要查閱或使用的個人資料。處方亦應採用「最小權限」的存取原則，只有獲授權處理核對身份工作的職員可存取或查閱有關的個人資料以降低個人資料外洩的風險；

嚴格審批及監察所有載有選民個人資料的系統的下載或複製

(ii) 處方應嚴格評估每次下載或複製選民個人資料的必要性，並訂立審批程序及準則；

(iii) 處方應監察載有選民個人資料的系統有否被未獲授權的下載或複製。系統及有關的伺服器應記錄所有活動日誌，每當系統使用者查閱、使用、下載、編輯及/或刪除資料後，處方可追蹤有關記錄；

(iv) 處方亦應在載有選民個人資料的系統及伺服器設定監察及警報系統，每當出現不尋常的活動時（例如：大量下載或刪除個人資料），可適時匯報有關情況，並進行追溯檢討；

使用便攜式儲存裝置儲存選民個人資料時採取有效的技術保安措施

(v) 由於將個人資料儲存於手提電腦或其他便攜式儲存裝置內會構成甚大的資訊保安風險，如非必要，不應將個人資料儲存在手提電腦或其他便攜式儲存裝置內；

(vi) 如確有必要將選民的個人資料儲存於手提電腦或其他便攜式儲存裝置，處方應因應資料的數量及敏感度考慮採取更

多有效的技術保安措施，例如採用雙重認證方式來查閱資料、在多次嘗試登入失敗後裝置會自動上鎖或資料會自動刪除、安裝追蹤遺失軟件等；

制訂、有系統地檢視及更新個人資料保安政策

(vii) 除依從政府及政府資訊科技總監辦公室的相關政策外，處方應因應其職能及活動制訂、有系統地檢視及更新現有的個人資料保安政策及指引（包括網上(on-line)及非網上(off-line)），確保有關處理選民個人資料的資訊是最新的；

(viii) 有效地將個人資料保安政策、程序及實務指引傳遞予所有職員，確保他們得悉及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；

(ix) 檢討及制訂一個定期和有系統的循規審核系統，以確保個人資料保安政策、程序及實務指引獲得遵從；

進行私隱影響評估

(x) 在展開任何涉及建立、收集、使用或儲存大量選民資料或涉及特別敏感資料的新工作或項目之前，處方應進行私隱影響評估[26]。處方應實行足夠的保安措施，以應付有關項目所帶來的私隱風險，評估過程及步驟應清楚地記錄存檔；及

推行私隱管理系統

(xi) 政府（包括所有決策局及部門）已於 2014 年承諾推行私隱管理系統[27]，將個人資料私隱管理納入管治責任的一環。私隱專員建議處方應汲取教訓，由上而下切實推行私隱管

[26] 公署的《私隱影響評估》資料單張可於下列網址下載：https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/InfoLeaflet_PIA_CHI_web.pdf。

[27] 公署的《私隱管理系統最佳行事方式指引》可於下列網址下載：https://www.pcpd.org.hk/pmp/files/PMP_guide_c.pdf。

理系統，重新檢視及更新系統監控（包括個人資料庫存、政策、風險評估工具、培訓及教育推廣，及資料外洩事故的處理等項目），全面提升職員尊重和保護選民個人資料私隱的意識，以符合條例的規定。

香港個人資料私隱專員公署
2017 年 6 月 12 日