視察報告

（根據香港法例第 486 章《個人資料（私隱）條例》第 48(1)條發表）

(1) 中華電力有限公司及
(2) 香港電燈有限公司
的客戶個人資料系統

報告編號： R21 - 3099

發表日期：2021 年 8 月 18 日

(1) 中華電力有限公司及

(2) 香港電燈有限公司

的客戶個人資料系統

香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）第 36 條訂明：

「*在不損害第38條的概括性原則下，專員可對─*

(a) 資料使用者所使用的任何個人資料系統；或

(b) 屬於某資料使用者類別的資料使用者所使用的任何個人資料系統，進行視察，目的在確定資訊以協助專員─

(i) 在─

(A) (a)段適用時，向有關的資料使用者；

(B) (b)段適用時，向有關的資料使用者所屬於的一個類別的資料使用者，

作出建議；及

(ii) 作出關於促進有關的資料使用者或有關的資料使用者所屬於的一個類別的資料使用者（視屬何情況而定）遵守本條例的條文（尤其是各保障資料原則）的建議。」

根據《私隱條例》第 2(1)條，「個人資料系統」是指「*全部或部分由資料使用者用作收集、持有、處理或使用個人資料的任何系統（不論該系統是否自動化的），並包括組成該系統一部分的任何文件及設備。*」

《私隱條例》第 48 條訂明：

「*(1) ... 專員在第36(b)條適用的情況下完成一項視察後，可─*

(a) 發表列明由該項視察引致的、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）的任何建議的報告；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(1)條履行所賦予的權力，發表本視察報告。

鍾麗玲
香港個人資料私隱專員
2021 年 **8** 月 **18** 日

目錄

視察報告

（根據香港法例第 486 章《個人資料（私隱）條例》第 48(1)條發表）

(1) 中華電力有限公司及

(2) 香港電燈有限公司

的客戶個人資料系統

摘要

背景

公用事業公司在管理服務帳戶、處理帳單及客戶查詢的過程中處理大量客戶的個人資料。除了提供可靠優質的服務，公用事業公司亦應把保障個人資料私隱視為其企業管治的一部份，保障客戶個人資料系統免受未經准許的查閱、處理及使用，以符合市民的期望。

香港個人資料私隱專員（專員）認為依據《個人資料（私隱）條例》（第 486 章）（《私隱條例》）第 36 條對公用事業公司進行視察（視察），審視其客戶個人資料系統，符合公眾利益。本視察挑選了中華電力有限公司（中電）及香港電燈有限公司（港燈）作為視察對象。

主要視察結果

良好行事方式

在視察期間，專員欣悉中電及港燈均積極致力保障客戶的個人資料，在下述範疇樹立了良好的榜樣：

(i) 兩間公司皆致力推行以問責為本的個人資料私隱管理系統，將保障個人資料視為其企業管治的一部分，由上而下締造尊重及保障個人資料私隱的文化。

(ii) 兩間公司皆委任了保障資料主任，他們都是負責監察機構遵從《私隱條例》的要求的高級職員，並需依循明確的機制就資料保障事宜向高級管理層匯報。

(iii) 兩間公司的保障資料主任及部門協調主任定期檢視並向員工傳達有關保障資料的政策，並確定培訓需要。

(iv) 兩間公司備有個人資料庫存，清楚知道其持有的客戶個人資料的種類、儲存地點、使用目的及保留期限。兩間公司每年會檢視及更新其個人資料庫存。

(v) 兩間公司均能展示其按員工職能存取客戶個人資料的良好行事方式，並定期檢視存取權限。例如，當一名員工被調往另一職位，該名員工存取客戶個人資料系統的權限會在有關調動生效之前被檢視及更新。

(vi) 兩間公司皆持續提升其資訊保安防護能力，並致力採取符合國際準則的措施保護其客戶個人資料系統免受網絡攻擊或黑客入侵。

(vii) 兩間公司有向員工提供有關保障個人資料私隱的培訓，特別是中電就如何設定及牢記複雜的密碼為員工提供針對性培訓，以避免員工「寫下」複雜的密碼（超過10個字元）。此外，中電在提供予員工的培訓材料中重點指出「起底」活動的嚴重法律後果。

<u>改善範疇</u>

儘管中電及港燈採取了上述的良好行事方式，視察人員留意到兩間公司在監察員工讀取客戶的個人資料方面有可改善的地方。

雖然兩間公司的客戶個人資料系統設有機制，檢查日誌記錄中是否出現任何異常情況，但視察人員發現兩間公司的系統只可以追查員工名稱、登入時間和為時多久，以及員工所進行的活動（即用戶輸入或更改資料），但卻沒有功能記錄搜尋活動。在這情況下，兩間公司均難以偵測個別員工在異常的情況下，讀取客戶的個人資料，例如：因好奇或為其他目的而進行姓名搜尋，或查閱客戶的聯絡資料。

總結

視察結果顯示，中電及港燈致力實施個人資料私隱管理系統，以及採取了良好的行事常規，而兩間公司的客戶個人資料系統的保安措施符合國際準則，令人滿意。專員認為兩間公司在保障客戶個人資料方面，符合《私隱條例》中附表1保障資料第4原則有關個人資料的保安的要求。

建議

專員希望透過本視察，向日常須處理大量客戶個人資料的公用事業公司及機構作出下述建議：

(i) **未雨綢繆：**科技急速發展對個人資料私隱帶來前所未有與不可忽視的風險。現時，很多機構已投放大量資源在先進的網絡保安科技上，以保護其網絡及資料庫並抵禦外來威脅。機構應留意客戶的個人資料有可能落入心懷不軌的內部成員手上以用作「起底」或其他非法行為的風險。

(ii) **設立個人資料私隱管理系統：**機構應建立一套遵從《私隱條例》規定的制度，循規地使用個人資料。個人資料私隱管理系統有助機構符規，迅速應對任何資料外洩事故，以及贏得客戶及其他持份者的信任。

(iii) **委任保障資料主任：**被指派負責監察遵從《私隱條例》的保障資料主任應依循明確的機制向高級管理層匯報。保障資料主任其中一項職責是把員工提出的保障資料事宜和涉及客戶個人資料事故的經驗及教訓納入機構的培訓材料中。

(iv) **建立個人資料庫存：**機構應建立及備存涵蓋整個機構的個人資料庫存，以確保所有相關員工了解他們正在處理甚麼個人資料，以及保障個人資料的程序。

(v) **制定系統保安政策及程序:** 機構應制定符合國際準則的系統保安政策，定期進行保安風險評估，並監察有關保安措施的成效，繼而採取改善措施以保護客戶個人資料系統免受網絡攻擊或黑客入侵。

(vi) **按員工職能存取客戶資料：**機構應只容許有需要檢視客戶資料來履行特定職責的員工存取客戶資料。例如技術人員，不論其職級，便沒有需要存取客戶的聯絡資料。細分的存取控制能有效地避免個人資料被濫用。由於有些舊系統未必支援細分的存取控制，機構在更新舊系統或開發新系統以管理客戶的個人資料時，應考慮加入有關存取控制的功能。

(vii) **預防及監察措施同樣重要：**全面的審核日誌可記錄使用者的數碼足跡。要有效地監察任何可疑的行為，機構應具備追查員工存取資料的系統，包括他們搜尋及更改記錄的情況。一旦偵測到可疑的行為，應考慮立即通知警方及個人資料私隱專員公署。

(viii) **保護電子與紙本記錄：**機構應同時就電子與紙本記錄制定保留政策及行事方式，並建立機制以定期監察載有個人資料的文件是否按預定的時限內銷毀。此外，桌面清理政策可減低載有客戶個人資料的文件被內部人員未經准許查閱的風險，亦可減低這些文件被誤置或遺失的風險。

(ix) **提升員工意識的措施：**全面的保障資料培訓計劃有助機構內建立尊重及保障客戶個人資料的文化。為避免機構的資料庫成為「起底」活動的來源，機構應提醒其員工，未經准許存取客戶的個人資料或會構成《私隱條例》或其他法例下的刑事罪行。機構可把法庭對「起底」個案的裁決納入培訓材料中，以提醒員工「起底」可帶來的嚴重法律後果。

第 I 部 – 序言

背景

1. 公用事業公司在管理服務帳戶、處理帳單及客戶查詢的過程中處理大量客戶的個人資料。除了提供可靠優質的服務，公用事業公司亦應把保障個人資料私隱視為其企業管治的一部份，保障客戶個人資料系統免受未經准許的查閱、處理及使用，以符合市民的期望。

2. 科技急速的發展及紙本記錄的電子化，令資料處理更有效率。不過，廣泛使用電腦資料庫或資料系統或令如何儲存及保障客戶個人資料的問題更為複雜 。

3. 與此同時，由於2019冠狀病毒病大流行，自2020年初公私營機構不時實施在家工作安排。因此，機構可能需要給予員工遙距連接公司網絡的權限。在這情況再加上公眾對「起底」活動[1]（機構的數據庫可成為「起底」者取得個人資料的來源[2]）的關注，顯示提升客戶個人資料系統的存取控制已成為日常須處理大量客戶個人資料的機構的迫切任務。

4. 香港個人資料私隱專員（專員）的權力由《個人資料（私隱）條例》（第486 章）（《私隱條例》）賦予。根據 《私隱條例》第8(1) 條，專員須就遵守《私隱條例》條文作出監察及監管，並促進對《私隱條例》

[1] 「起底」涉及從不同來源收集目標人物或其家屬的個人資料，然後在未經相關資料當事人同意的情況下，在互聯網、社交平台或其他公開平台披露那些個人資料。

[2] 在一宗於 2020 年 11 月被判刑的「起底」案件中，被告利用在電訊公司工作之便，從公司電腦取得一名警務人員家屬的個人資料，然後向某社交平台的群組披露有關資料以供「起底」，因而令受害人蒙受心理傷害。

的認識及理解以及遵守。《私隱條例》第 36 條賦權專員對資料使用者或屬於某資料使用者類別的資料使用者所使用的任何個人資料系統進行視察。

5. 專員認為依據《私隱條例》第 36 條對公用事業公司進行視察（視察），審視其客戶個人資料系統，符合公眾利益。本視察挑選了中華電力有限公司（中電）及香港電燈有限公司（港燈）作為視察對象。

視察範圍

6. 在進行視察前，專員先分別致函中電及港燈表達進行視察的意向。兩間公司均回覆表示支持和合作，並向專員提供其客戶個人資料系統的相關資訊。各方同意本視察會聚焦兩間公司在控制存取客戶個人資料系統方面的保安措施。

7. 兩間公司所使用的客戶個人資料系統具有下述共通點和目的：

(i) 根據供應地址備存客戶帳戶使用及帳單資料；

(ii) 備存住宅帳戶持有人或商業帳戶聯絡人的個人資料（姓名、供應地址、通訊地址、電話號碼和電郵地址等）；

(iii) 系統的終端用戶（兩間公司的指定員工）可以透過系統檢視及輸入資料；

(iv) 透過互聯網或熱線支援互動式客戶服務，例如提供網上平台讓客戶結束帳戶、轉移帳戶及為新地址開立新帳戶；及

(v) 為管理層提供有用和適時的資訊，以作策劃及決策。

8. 有關個人資料的保安，《私隱條例》附表1的保障資料第4原則規定資料使用者須採取所有切實可行的步驟，以確保其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。

9. 除了資料保安及存取控制（保障資料第4原則），其他保障資料原則，尤其是保障資料第1原則（收集資料）及保障資料第2(2)原則（保留資料）亦與保障客戶的個人資料相關。六項保障資料原則載列於**附錄A**，以便參考。

10. 《私隱條例》在設計上屬於原則性及科技中立的法例。保障資料第4原則並沒有清單列明資料使用者須採取資料保安及存取控制程序的具體規定。一般來說，專員認為資料保安及存取控制程序的嚴格程度應與個人資料私隱的風險相稱。在考慮到兩間公司處理客戶個人資料的數量和性質，專員訂明對兩間公司的政策及行事方式的主要評估範疇如下：

個人資料私隱的風險	**評估範疇**
<u>企業的固有私隱風險</u> • 如收集的個人資料對提供客戶服務而言不是必需，一旦發生資料外洩事故，對客戶的影響會較大。	(1) 資料管治架構 (2) 個人資料庫存 (3) 保留資料政策及行事方式

個人資料私隱的風險	評估範疇
• 如機構沒有備存最新的個人資料庫存，便不能有效地監察及掌握載有客戶個人資料的記錄的保留期限。	
<u>內部威脅</u> • 不恰當的客戶個人資料存取權限會增加員工濫用資料作出售、網絡欺凌或「起底」的機會。 • 員工意外遺失載有客戶個人資料的文件或便攜式裝置。	(4) 客戶個人資料系統的存取控制 (5) 追查存取情況的監察機制 (6) 在家工作安排 (7) 員工培訓及提升私隱意識計劃
<u>外部威脅</u> • 網絡攻擊或黑客入侵	(8) 實體及系統保安措施 (9) 資料保安系統的第三方審核

第 II 部 – 視察方法

11. 為了視察中電及港燈的客戶個人資料系統及員工如何有效地遵從有關公司的資料保安政策和行事方式，專員審閱了兩間公司的所有相關政策、手冊、指引、僱員行為守則及培訓資料。

12. 此外，專員根據《私隱條例》行使進入處所的權力，進行實地視察，作出實際評估。2021年3月份，視察人員[3] 在各方同意下七次到訪兩間公司，實地視察了11個部門，包括總辦事處、分公司、數據中心及電話服務中心。

13. 視察人員的實地視察工作包括：

(i) 與負責管理客戶個人資料系統的人員面談；

(ii) 到訪兩間公司的不同部門，了解客戶個人資料系統的實際運作及相關的存取控制機制；

(iii) 邀請兩間公司超過 100 名員工（挑選準則是基於他們有權存取客戶個人資料系統）填寫一份問卷，內容是關於他們在工作上保障客戶個人資料的意識和態度[4]。該問卷的複本載於**附錄 B**。

[3] 視察人員包括一位首席個人資料主任、兩位高級個人資料主任及四位個人資料主任組成。

[4] 由於視察時爆發2019冠狀病毒病的關係，問卷是以電子形式填寫，以保持良好的社交距離。

14. 本視察報告（報告）擬協助兩間公司找出可以改善之處。另一方面，視察結果可以展示兩間公司如何致力保障客戶的個人資料，它們或可在資料保障政策及行事方式方面為其他資料使用者樹立良好的榜樣。專員認為毋須評論哪間公司在指定的範疇表現較佳或遜色。

第 III 部 – 視察結果

15. 本報告是根據中電及港燈所提供的資訊及視察人員於實地視察留意到的事宜而作出的。遵從《私隱條例》的規定是兩間公司的法律責任。本報告的視察結果及建議不會影響或損害專員根據《私隱條例》行使任何權力或履行任何職能。

(1) 資料管治架構

16. 有鑒於客戶及持份者對公司負責任地使用個人資料的期望越來越高，為了取得客戶的信任及提升企業的聲譽和競爭優勢，專員一直倡議機構建立自己的個人資料私隱管理系統及委任保障資料主任，從而設立一個既能負責任地使用個人資料並符合《私隱條例》規定的系統[5]。因此，香港董事學會出版的《獨立非執行董事指南》在提及推動「環境、社會及管治」的多項因素時，亦納入個人資料私隱管理系統，鼓勵機構實施這系統。

17. 視察人員知悉兩間公司的最高管理層視個人資料私隱的處理為重要及優先的事宜，並承諾在僱員間培養尊重及保障個人資料私隱的文化。兩間公司的保障資料政策及程序清晰界定客戶的個人資料屬於「機密」，必須極為謹慎地儲存、使用及棄置。

18. 個人資料私隱管理系統的其中一環是委任保障資料主任／設立保障資料部門全面監督機構是否有遵從《私隱條例》的規定及推行個人資料私隱

[5] 有關如何制定及推行全面的個人資料私隱管理系統的例子及實用指引，請參閱《私隱管理系統最佳行事方式指引》：https://www.pcpd.org.hk//chinese/resources_centre/publications/files/PMP_guide_c.pdf

管理系統。兩間公司的保障資料主任是高級行政人員，就建立、設計及管理個人資料私隱管理系統（包括收集、持有、處理及使用個人資料的所有相關程序、培訓、監察或審核、記錄、評估及跟進）直接向最高管理層匯報。

19. 兩間公司亦委任部門協調主任，支援保障資料主任。在這方面，兩間公司建立了內部匯報機制，處理有關個人資料私隱及可能發生資料外洩事故時的職員查詢。除了定期匯報，部門協調主任和保障資料主任亦會一起整合不同營業單位所遇到的問題，找出值得關注的地方，作為員工培訓材料中的經驗教訓和實用提示。

(2) 個人資料庫存

20. 記錄個人資料的處理是個人資料私隱管理系統的主要組件。全面及最新的個人資料庫存有助機構不時檢視收集了甚麼個人資料、收集資料的目的及應如何保護資料。

21. 視察人員得悉兩間公司備有個人資料庫存，當中的資訊包括所收集的個人資料的類別 （姓名、供應地址、通訊地址、電話號碼和電郵地址等）、儲存資料的地點、保留期限，以及如何處理個人資料。兩間公司均每年會檢視個人資料庫存，以確保所收集的個人資料符合收集最少資料的原則，屬必須但不超乎適度。

(3) 保留資料政策及行事方式

22. 兩間公司就客戶的個人資料制定了正式的保留政策，以確保個人資料的保存時間不超過將其保存以貫徹該資料被使用於的目的所需的時間[6]。

23. 保留政策包含下述要素：

(i) 指定員工負責銷毀不再需要的個人資料；

(ii) 根據個人資料的類別考慮保留資料的期限；

(iii) 訂明棄置方法及保安措施；

(iv) 備存銷毀記錄；

(v) 涵蓋電子及紙本記錄。

24. 不過，在實地視察期間，視察人員在港燈發現部分於2018年從客戶收集得的服務申請表仍儲存在文件櫃中，但根據紙本服務申請表的保留期限，這些表格應在收集後兩年內銷毀。據港燈其後表示，由於部分服務申請表在視察期間仍在跟進中，故未有銷毀。

25. 專員建議港燈將完成跟進及仍在跟進中的客戶申請表分開儲存，並確保紙本服務申請表在完成跟進後按預定的時間銷毀。

[6] 保障資料第 2(2)原則的規定

(4) 客戶個人資料系統的存取控制

26. 兩間公司均就客戶個人資料系統的存取控制採取了下述良好的行事方式：

(i) **按職能存取：**按「有需要知道」的原則授予員工的存取權限與員工的職級、職能及責任相符。例如客戶服務中心的熱線員工獲准查閱客戶的帳單資料，以處理客戶的查詢，但人力資源部的員工則不能如此查閱。

(ii) **更新及刪除存取權限的程序：**在授予個別員工任何存取權限之前，必須取得書面批准。在進行任何員工調職之前，須檢視及更新存取權限，以確保員工不會得到不必要的存取權限。在中電，「特許存取」只在短期內有效，並在預定期限屆滿後，系統會自動刪除有關權限。

(iii) **密碼管理：**兩間公司的員工獲分配獨一無二的用戶名稱及密碼。兩間公司皆制定了政策禁止員工共用密碼及要求他們須定期更改密碼。密碼必須符合最少數位及複雜程度的要求。如多次登入系統錯誤，用戶帳戶會被鎖定。

為避免員工「寫下」複雜的密碼（超過10個字元），中電就如何設定及牢記複雜的密碼為員工提供針對性的培訓。在實地視察期間，視察人員並沒有發現電腦螢幕或電腦貼有顯示密碼的便利貼或紙張。

(5) 追查存取情況的監察機制

27. 視察人員知悉兩間公司就其客戶個人資料系統，備存了員工活動的日誌記錄。它們的系統設有機制，檢查日誌記錄中是否出現任何異常情況。如出現異常狀況（例如個別員工於非辦公時間下載大量個人資料），便會通知相關的主管級職員。兩間公司會保留日誌記錄，作定期審計調查之用。

28. 不過，視察人員發現兩間公司的系統只可以追查員工名稱、登入時間和為時多久，以及員工所進行的活動（即用戶輸入或更改資料），但卻沒有功能記錄搜尋活動。在這情況下，兩間公司難以偵測個別員工在異常的情況下，讀取客戶的個人資料，例如：因好奇或為其他目的而進行姓名搜尋，或查閱客戶的聯絡資料。

29. 為有效偵測任何可疑的行為，專員建議兩間公司考慮更新相關系統，以追查員工的完整數碼足跡，包括他們在系統中進行的搜尋活動。當偵測到可疑的行為時，應考慮立即通知警方及個人資料私隱專員公署。

(6) 在家工作安排

30. 自2020 年初爆發2019冠狀病毒病以來，本地機構不時採取在家工作的政策，令個人資料較以往有更大機會遭外洩。2020年11月，專員發出三份有關在家工作安排下的個人資料保障指引，分別向機構（給機構的指引載於**附錄C**）、僱員及使用視像會議軟件的用戶提供實用建議，以提升資料保安及保障個人資料。

31. 視察人員知悉兩間公司制定了遙距工作的政策，涵蓋下述事宜：

(i) 遙距連接機構網絡的技術管控措施（例如採用多重認證）；及

(ii) 授權進行遙距工作的程序。

32. 專員建議兩間公司在日後考慮實際業務情況而檢討其在家工作的政策時，可參考以上第30段所提及的三份指引。兩間公司應向員工提供下述的實用提示：

(i) 避免在公共地方工作，以防止意外地向第三者披露個人資料或限閱資料；

(ii) 如機構已向員工提供電子裝置，員工應只使用機構的電子裝置工作；

(iii) 提升 Wi-Fi 連接及電子通訊的保安（例如把電郵和附件加密）；

(iv) 如需要把紙本文件帶離辦公室，要確保妥善處理個人資料。

(7) <u>員工培訓及提升私隱意識計劃</u>

33. 視察人員注意到兩間公司為員工提供以下一連串關於保障資料的培訓：

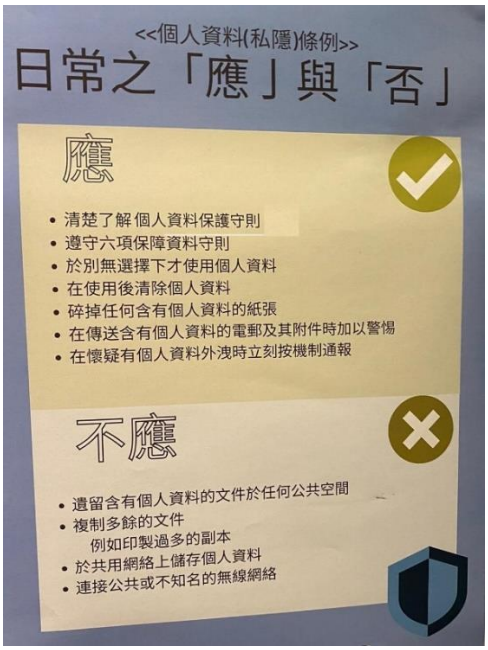
(i) 新入職的員工必須接受培訓，才獲准登入客戶個人資料系統；

(ii) 定期的研討會或工作坊作為複修訓練；

(iii) 網上學習及影片；及

(iv) 在辦公室張貼海報，提升員工對保障資料的意識和認識。

34. 以下是視察期間發現的海報：

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
</table>

35. 視察人員知悉中電除了介紹《私隱條例》及保障資料原則之外，亦在培訓材料中重點指出「起底」活動的嚴重法律後果。

36. 為避免機構的資料庫成為「起底」活動的來源，專員建議兩間公司應提醒其員工，未經准許存取客戶的個人資料或會構成《私隱條例》或其他法例下的刑事罪行。機構可把法庭對「起底」個案的裁決納入培訓材料中，以提醒員工「起底」的嚴重法律後果。

(8) 實體及系統保安措施

實體保安

37. 視察人員知悉兩間公司制定了實體保安措施，以防有人未經准許進入工作間，從而減低未經准許存取客戶個人資料的風險。這些措施包括：

(i) 訪客必須登記，並由員工陪同；

(ii) 智能卡門禁系統；

(iii) 訪客必須佩戴訪客名牌，以資識別；及

(iv) 桌面清理政策。

38. 桌面清理政策可減低載有客戶個人資料的文件被內部人員未經准許或意外地查閱的風險，亦可減低文件被誤置或遺失個人資料的風險。在實地視察期間，視察人員注意到載有客戶個人資料的實體檔案是存放在上鎖的受限區域內。

39. 視察人員知悉中電會定期巡查工作間，查看載有客戶個人資料的文件是否無人看管。如有員工被發現沒有遵從桌面清理政策，該員工會收到提醒他／她立即改善情況的警告標貼。

40. 專員建議兩間公司應繼續實行桌面清理政策，並進行定期巡查，以確保員工遵守政策。

<u>系統保安</u>

41. 視察人員欣悉中電及港燈皆持續提升其資訊保安防護能力，制訂資訊科技保安政策時均有參考國際準則ISO/IEC 27002作業規範的框架，涵蓋系統防護、存取控制、實體保安等技術層面。所涉及的技術措施包括防火牆、資料遺失防護系統及端點監控等。基於保安技術保密性，細節不在此報告詳述。

(9) 資料保安系統的第三方審核

42. 視察人員知悉中電及港燈均在內部指派一個部門，定期審核不同營運單位，並作出保障個人資料的建議。

43. 此外，中電聘請了外部顧問檢視其資訊科技保安和資料保安，而港燈則聘請了外部顧問評估其資訊科技系統。兩間公司已就有關審核採取了糾正措施。

總結

44. 視察結果顯示，中電及港燈致力實施個人資料私隱管理系統，以及採取了良好的行事常規，而兩間公司的客戶個人資料系統的保安措施符合國際準則，令人滿意。專員認為兩間公司在保障客戶個人資料方面，符合《私隱條例》中附表1保障資料第4原則有關個人資料的保安的要求。

第 IV 部 – 建議

45. 專員希望透過本視察，向日常須處理大量客戶個人資料的公用事業公司及機構作出下述建議：

(i) **未雨綢繆：**科技急速發展對個人資料私隱帶來前所未有與不可忽視的風險。現時，很多機構已投放大量資源在先進的網絡保安科技上，以保護其網絡及資料庫並抵禦外來威脅。機構應留意客戶的個人資料有可能落入心懷不軌的內部成員手上以用作「起底」或其他非法行為的風險。

(ii) **設立個人資料私隱管理系統：**機構應建立一套遵從《私隱條例》規定的制度，循規地使用個人資料。個人資料私隱管理系統有助機構符規，迅速應對任何資料外洩事故，以及贏得客戶及其他持份者的信任。

(iii) **委任保障資料主任：**被指派負責監察遵從《私隱條例》的保障資料主任應依循明確的機制向高級管理層匯報。保障資料主任其中一項職責是把員工提出的保障資料事宜和涉及客戶個人資料事故的經驗及教訓納入機構的培訓材料中。

(iv) **建立個人資料庫存：**機構應建立及備存涵蓋整個機構的個人資料庫存，以確保所有相關員工了解他們正在處理甚麼個人資料，以及保障個人資料的程序。

(v) **制定系統保安政策及程序:** 機構應制定符合國際準則的系統保安政策，定期進行保安風險評估，並監察有關保安措施的成效，繼而採取改善措施以保護客戶個人資料系統免受網絡攻擊或黑客入侵。

(vi) **按員工職能存取客戶資料**：機構應只容許有需要檢視客戶資料來履行特定職責的員工存取客戶資料。例如技術人員，不論其職級，便沒有需要存取客戶的聯絡資料。細分的存取控制能有效地避免個人資料被濫用。由於有些舊系統未必支援細分的存取控制，機構在更新舊系統或開發新系統以管理客戶的個人資料時，應考慮加入有關存取控制的功能。

(vii) **預防及監察措施同樣重要**：全面的審核日誌可記錄使用者的數碼足跡。要有效地監察任何可疑的行為，機構應具備追查員工存取資料的系統，包括他們搜尋及更改記錄的情況。一旦偵測到可疑的行為，應考慮立即通知警方及個人資料私隱專員公署。

(viii) **保護電子與紙本記錄**：機構應同時就電子與紙本記錄制定保留政策及行事方式，並建立機制以定期監察載有個人資料的文件是否按預定的時限內銷毀。此外，桌面清理政策可減低載有客戶個人資料的文件被內部人員未經准許查閱的風險，亦可減低這些文件被誤置或遺失的風險。

(ix) **提升員工意識的措施**：全面的保障資料培訓計劃有助機構內建立尊重及保障客戶個人資料的文化。為避免機構的資料庫成為「起底」活動的來源，機構應提醒其員工，未經准許存取客戶的個人資料或會構成《私隱條例》或其他法例下的刑事罪行。機構可把法庭對「起底」個案的裁決納入培訓材料中，以提醒員工「起底」可帶來的嚴重法律後果。

附表 1

[第 2(1)及(6)條]

保障資料原則

1. 第 1 原則——收集個人資料的目的及方式

(1) 除非 —

(a) 個人資料是為了直接與將會使用該資料的資料使用者的職能或活動有關的合法目的而收集；

(b) 在符合(c)段的規定下，資料的收集對該目的是必需的或直接與該目的有關的；及

(c) 就該目的而言，資料屬足夠但不超乎適度，

否則不得收集資料。

(2) 個人資料須以 —

(a) 合法；及

(b) 在有關個案的所有情況下屬公平，

的方法收集。

(3) 凡從或將會從某人收集個人資料，而該人是資料當事人，須採取所有切實可行的步驟，以確保 —

(a) 他在收集該資料之時或之前，以明確或暗喻方式而獲告知 — *(由 2012 年第 18 號第 2 條修訂)*

(i) 他有責任提供該資料抑或是可自願提供該資料；及

(ii) (如他有責任提供該資料)他若不提供該資料便會承受的後果；及

(b) 他 —

(i) 在該資料被收集之時或之前，獲明確告知 — *(由 2012 年第 18 號第 2 條修訂)*

(A) 該資料將會用於甚麼目的(須一般地或具體地說明該等目的)；及

(B) 該資料可能移轉予甚麼類別的人；及

(ii) 在該資料首次用於它們被收集的目的之時或之前，獲明確告知 — *(由 2012 年第 18 號第 2 條修訂)*

(A) 他要求查閱該資料及要求改正該資料的權利；

(B) 處理向有關資料使用者提出的該等要求的個人的姓名(或職銜)及其地址，*(由 2012 年第 18 號第 40 條代替)*

但在以下情況屬例外：該資料是為了在本條例第 8 部中指明為個人資料就其而獲豁免而不受第 6 保障資料原則的條文所管限的目的而收集，而遵守本款條文相當可能會損害該目的。

(由 2012 年第 18 號第 2 條修訂；編輯修訂—2013 年第 1 號編輯修訂紀錄)

2. 第 2 原則——個人資料的準確性及保留期間

(1) 須採取所有切實可行的步驟，以 —

(a) 確保在顧及有關的個人資料被使用於或會被使用於的目的(包括任何直接有關的目的)下，該個人資料是準確的；

(b) 若有合理理由相信在顧及有關的個人資料被使用於或會被使用於的目的(包括任何直接有關的目的)下，該個人資料是不準確時，確保 — *(由 2012 年第 18 號第 2 條修訂)*

(i) 除非該等理由不再適用於該資料(不論是藉着更正該資料或其他方式)及在此之前，該資料不得使用於該目的；或

(ii) 該資料被刪除；

(c) 在於有關個案的整體情況下知悉以下事項屬切實可行時 —

(i) 在指定日當日或之後向第三者披露的個人資料，在顧及該資料被使用於或會被使用於的目的(包括任何直接有關的目的)下，在要項上是不準確的；及

(ii) 該資料在如此披露時是不準確的，

確保第三者 —

(A) 獲告知該資料是不準確的；及

(B) 獲提供所需詳情，以令他能在顧及該目的下更正該資料。*(由 2012 年第 18 號第 2 條修訂)*

(2) 須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將其保存以貫徹該資料被使用於或會被使用於的目的(包括任何直接有關的目的)所需的時間。*(由 2012 年第 18 號第 2 及 40 條修訂)*

(3) 在不局限第(2)款的原則下，如資料使用者聘用(不論是在香港或香港以外聘用)資料處理者，以代該資料使用者處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者的個人資料的保存時間超過處理該資料所需的時間。*(由 2012 年第 18 號第 40 條增補)*

(4) 在第(3)款中 —

資料處理者 (data processor)指符合以下兩項說明的人 —

(a) 代另一人處理個人資料；及

(b) 並不為該人本身目的而處理該資料。*(由 2012 年第 18 號第 40 條增補)*

3. 第 3 原則——個人資料的使用

(1) 如無有關的資料當事人的訂明同意，個人資料不得用於新目的。*(由 2012 年第 18 號第 40 條修訂)*

(2) 資料當事人的有關人士可在以下條件獲符合的情況下，代該當事人給予為新目的而使用其個人資料所規定的訂明同意 —

(a) 該資料當事人 —

(i) 是未成年人；

(ii) 無能力處理本身的事務；或

(iii) 屬《精神健康條例》(第 136 章)第 2 條所指的精神上無行為能力；

(b) 該資料當事人無能力理解該新目的，亦無能力決定是否給予該項訂明同意；及

(c) 該有關人士有合理理由相信，為該新目的而使用該資料明顯是符合該資料當事人的利益。*(由 2012 年第 18 號第 40 條增補)*

(3) 即使資料使用者為新目的而使用資料當事人的個人資料一事，已得到根據第(2)款給予的訂明同意，除非該資料使用者有合理理由相信，如此使用該資料明顯是符合該當事人的利益，否則該資料使用者不得如此使用該資料。 *(由 2012 年第 18 號第 40 條增補)*

(4) 在本條中 —

新目的 (new purpose)就使用個人資料而言，指下列目的以外的任何目的 —

(a) 在收集該資料時擬將該資料用於的目的；或

(b) 直接與(a)段提述的目的有關的目的。*(由 2012 年第 18 號第 40 條增補)*

4. 第 4 原則——個人資料的保安

(1) 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 —*(由 2012 年第 18 號第 40 條修訂)*

(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。*(由 2012 年第 18 號第 2 條修訂)*

(2) 在不局限第(1)款的原則下，如資料使用者聘用(不論是在香港或香港以外聘用)資料處理者，以代該資料使用者處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用。*(由 2012 年第 18 號第 40 條增補)*

(3) 在第(2)款中 —

資料處理者 (**data** processor)具有第 2 保障資料原則第(4)款給予該詞的涵義。*(由 2012 年第 18 號第 40 條增補)*

5. **第 5 原則——資訊須在一般情況下可提供**

須採取所有切實可行的步驟，以確保任何人 —

(a) 能確定資料使用者在個人資料方面的政策及實務；

(b) 能獲告知資料使用者所持有的個人資料的種類；

(c) 能獲告知資料使用者持有的個人資料是為或將會為甚麼主要目的而使用的。

6. **第 6 原則——查閱個人資料**

資料當事人有權 —

(a) 確定資料使用者是否持有他屬其資料當事人的個人資料；

(b) 要求 —

(i) 在合理時間內查閱；

(ii) 在支付並非超乎適度的費用(如有的話)下查閱；

(iii) 以合理方式查閱；及

(iv) 查閱採用清楚易明的形式的，

個人資料；

(c) 在(b)段所提述的要求被拒絕時獲提供理由；

(d) 反對(c)段所提述的拒絕；

(e) 要求改正個人資料；

(f) 在(e)段所提述的要求被拒絕時獲提供理由；及

(g) 反對(f)段所提述的拒絕。

附錄 B

僱員調查問卷

香港個人資料私隱專員現根據《個人資料（私隱）條例》（《私隱條例》）第 36 條，視察[公司名稱]的客戶個人資料系統。本問卷屬是次視察的一部分，以不記名方式進行，所收集的資料僅供綜合性分析之用 。

問卷旨在了解你對保障客戶個人資料的意識和態度，以及你的僱主在保障客戶個人資料方面的情況。請詳閱各題目，然後選擇合適的答案，並於[　　]前遞交。感謝你的協助。

1. **你認為你的同事對保障客戶個人資料的意識是否足夠？**

（6 分為非常足夠，最低 1 分）

不足夠　1　2　3　4　5　6　非常足夠

2. **你是否同意你的僱主已在機構的管治架構內培養尊重客戶個人資料私隱的文化？**

（6 分為非常同意，最低 1 分）

不同意　1　2　3　4　5　6　非常同意

3. **你認為遵守《私隱條例》的規定是否容易？**

（1 分為非常容易，6 分為非常困難）

非常容易　1　2　3　4　5　6　非常困難

4. **你認為你的僱主向你提供有關保障個人資料私隱的培訓是否足夠？**

（6 分為非常足夠，最低 1 分）

不足夠	1	2	3	4	5	6	非常足夠

5. **你認為你的僱主為確保資料安全而向在家工作的僱員提供的支援是否足夠？**

（6 分為非常足夠，最低 1 分）

不足夠	1	2	3	4	5	6	非常足夠

6. **你認為快捷地完成工作重要或是謹慎處理個人資料較為重要？**

（6 分為謹慎處理個人資料至為重要，1 分為快捷地完成工作至為重要）

快捷地完成工作	1	2	3	4	5	6	謹慎處理個人資料

7. **你的僱主有否：（可選擇多於一項）**

☐ 透過不同渠道（例如員工會議或通告），向全體員工表達支持建立尊重個人資料私隱的文化

☐ 透過《收集個人資料聲明》及《私隱政策聲明》，讓員工及客戶清楚知道機構收集、使用及披露個人資料的目的，以及保留資料多久

☐ 清楚告知員工如有需要提出有關處理客戶資料的問題或關注時可聯絡的專責職員

☐ 分配足夠的資源（包括財政及人手）以推行私隱管理系統

☐ 以上皆否

8. **你認為下列哪些個人行為涉及干犯《私隱條例》下的罪行？（可選擇多於一項）**

☐ 意外地刪除了客戶於機構系統內的帳戶資料

☐ 擅自將客戶的電話號碼儲存於自己的手提電話內，以便在家工作時聯絡客戶

☐ 將客戶的姓名及電話號碼披露予一名友人，以便該名友人向客戶介紹其他機構的優惠服務或產品

☐ 在社交平台上對客戶作出「起底」行為，披露了客戶的真實姓名及居住的屋苑名稱，但沒有披露居所的樓層或單位號碼

9. **你認為「起底」行為可能涉及下列哪些罪行？（可選擇多於一項）**

☐ 《私隱條例》下有關披露未經資料使用者同意而取得的個人資料的規定

☐ 刑事恐嚇

☐ 有犯罪或不誠實意圖而取用電腦

☐ 藐視法庭（違反與起底有關的禁制令）

10. **據你所知，《私隱條例》下有關個人資料保安的規定包含以下哪些事宜？（可選擇多於一項）**

☐ 保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用

☐ 確保負責處理個人資料的員工具備良好操守

☐ 機構在發生資料外洩事故時必須通報受影響的資料當事人

☐ 確保所聘用的資料處理者依從資料保安要求

11. 你會每隔多久更改登入機構電腦系統的密碼？（請選擇其中一項）

☐ 至少每個月更改一次
☐ 至少每三個月更改一次
☐ 至少每六個月更改一次
☐ 只會在系統要求時更改密碼

12. 你過去有沒有因工作需要，將登入機構電腦系統的密碼告知其他同事，或使用其他同事的密碼登入系統處理公事？（請選擇其中一項）

☐ 有，事前沒有取得上司的同意
☐ 有，事前已取得上司的同意
☐ 沒有

13. 你過去有沒有使用公共電腦及／或公共 **Wi-Fi** 登入機構電腦系統？（請選擇其中一項）

☐ 有
☐ 沒有

14. 你過去有沒有把機構的紙本文件從辦公室帶回家中工作？（請選擇其中一項）

☐ 有
☐ 沒有

15. **你已取得上司的同意？（請選擇其中一項）**

☐ 有

☐ 沒有

16. **你有否採取以下的措施？（可選擇多於一項）**

☐ 離開辦公室前先將紙本文件中的個人資料遮蓋或移除

☐ 備存清單，記錄帶回家中的文件

☐ 攜帶紙本文件途中份外小心，慎防遺失

☐ 在家中會將紙本文件鎖進安全的儲物櫃或抽屜，防止未經授權的取閱

☐ 以上皆否

17. **如你需要使用外置式儲存裝置（例如 USB 記憶體、硬碟機等）儲存客戶的個人資料，你會：（可選擇多於一項）**

☐ 先獲得部門主管的同意

☐ 只使用機構批准的裝置

☐ 不儲存屬敏感度高的個人資料，如身份證號碼

☐ 只在機構範圍內使用有關裝置

- 完 -

PCPD HK
PCPD.org.hk
指引資料
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

在家工作安排下的個人資料保障指引：機構篇

引言

1. 2019冠狀病毒病疫情期間，機構需不時實施在家工作安排。就此，機構或許有需要透過僱員的家居網絡及個人電子裝置查閱或傳送資料及文件。相對於由專業人員管理的公司網絡及電子裝置，僱員的家居網絡及個人電子裝置的保安較弱，資料保安及個人資料私隱的風險無可避免會上升。

2. 本指引旨在為機構（包括業務實體）提供實用建議，以提升在家工作安排下的資料保安及個人資料私隱的保障。

在家工作安排的基本原則

3. 不論是在辦公室或在家工作，個人資料的保安以及保障個人資料私隱的標準是相同的。機構在實施在家工作安排時應遵守以下原則：

   (1) 為在家工作安排下的資料處理（包括個人資料）制定清晰的政策[1]；以及

   (2) 採取所有合理切實可行的步驟確保資料安全，特別是當涉及使用資訊及通訊科技以便利在家工作，或涉及將資料和文件轉移予僱員[2]。

給機構的實用建議

4. 機構作為資料使用者及僱主，在確保資料安全及保障僱員的個人資料私隱方面負有主要責任。因此，機構應落實以下的措施以體現上述在家工作安排的基本原則。

風險評估

5. 對很多機構而言，在家工作是前所未有或是全新的安排。因此，機構應評估有關安排對資料保安及僱員個人資料私隱構成的風險，從而制定合適的保障措施。

政策及指引

6. 機構應按照風險評估的結果，審視現有政策及常規，作出適當的修訂，以及為僱員提供充足的指引。有關的政策及指引可包括以下方面：

   (1) 將資料及文件轉移離開機構的處所及公司網絡的安排；

   (2) 遙距接達公司網絡及存取資料的安排；

   (3) 刪除及銷毀非必要的資料的安排；以及

   (4) 資料外洩事故的處理。

僱員培訓及支援

7. 機構應為在家工作的僱員提供足夠培訓及支援，以確保資料安全。相關的培訓及支援可包括以下方面：

   (1) 資料保安的方法，例如密碼管理、資料加密以及安全地使用 Wi-Fi；以及

   (2) 對網絡保安威脅及趨勢的意識，例如網絡釣魚、惡意軟件及電話騙案。

8. 機構應指派專責的職員解答僱員的疑問和提供適切的支援。

電子裝置管理

9. 機構如為在家工作的僱員提供電子裝置（例如智能電話和手提電腦），應採取以下措施確保儲存於電子裝置內的資料（包括個人資料）安全：

   (1) 安裝適合的防惡意程式軟件、防火牆及最新的保安修補程式；

   (2) 定期更新電子裝置系統；

   (3) 確保儲存於電子裝置內、與工作有關的資料已進行加密處理；

---

[1] 《個人資料（私隱）條例》（香港法例第486章）附表1的保障資料第5原則
[2] 保障資料第4原則

(4) 設定嚴格的存取控制，例如要求使用高強度密碼（包含英文字母、數字及符號的組合）、要求定期更改密碼以及使用多重身份認證，並且限制登入失敗的次數；

(5) 防止從公司的裝置轉移資料至個人電子裝置；

(6) 開啟遙距資料抹除功能，當電子裝置遺失時可刪除儲存在裝置內的資料；以及

(7) 避免在電子裝置上顯眼地展示機構的名稱、標誌及其他標識，以免引起不必要的注意。

虛擬私人網絡 (VPN)

10. VPN是在家工作安排中一樣重要和普及的工具，因為VPN可讓僱員遙距地以及比較安全地接達公司網絡。為確保VPN的安全，機構應採取以下措施：

(1) 連接VPN時使用多重身份認證；

(2) 及時更新VPN平台的保安設定；

(3) 採用握手協議（handshake protocol）（例如互聯網安全協定（IPSec）、保密插口層（SSL）、傳輸層保安（TLS）等）以為僱員電子裝置與公司網絡之間建立安全通訊渠道；

(4) 在可行情況下選擇全隧道VPN（只在必要的情況下選擇分割隧道VPN，例如當頻寬不足時）；以及

(5) 封鎖不安全的電子裝置。

遙距接達

11. 除了使用VPN外，機構應對公司網絡的遙距接達採取進一步保安措施。實際措施可包括：

(1) 採用網絡分段將整個網絡區分成不同的網段或子網絡，以減低資料外洩事故的風險和嚴重程度，並提升對重要和敏感資料的保護；

(2) 按實際需要給予僱員存取權限，例如採用以職能為基礎的存取控制（role-based access control）；

(3) 開啟帳戶鎖定功能，封鎖多次登入失敗的帳戶；以及

(4) 檢視遙距接達的紀錄以識別可疑活動。

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong
PCPD.org.hk

私隱公署網頁

查詢熱線 ： **(852) 2827 2827**
傳真 ： **(852) 2877 7026**
地址 ： **香港灣仔皇后大道東248號陽光中心13樓1303室**
電郵 ： **communications@pcpd.org.hk**

下載本刊物

二零二零年十一月初版