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

香港寬頻網絡有限公司

客戶資料庫遭入侵事件

報告編號：R19 – 5759

2019 年 2 月 21 日

香港寬頻網絡有限公司
客戶資料庫遭入侵事件

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，「[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《私隱條例》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
2019 年 2 月 21 日

摘要

香港個人資料私隱專員（**私隱專員**）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，就香港寬頻網絡有限公司（**香港寬頻**）於2018年4月16日發現一個已停用的資料庫遭黑客入侵，而導致近38萬名客戶及服務申請者的個人資料外洩的事件展開調查，並發表本報告。

事發時，香港寬頻將客戶資料儲存在三個資料庫內。遭黑客入侵的資料庫（資料庫甲）是一個已停用的資料庫，儲存截至 2012 年的客戶和服務申請者的個人資料；其餘兩個資料庫（資料庫乙和丙）則是現用資料庫，儲存現有客戶、舊客戶和服務申請者的個人資料。儲存在資料庫內的個人資料包括姓名、電郵地址、通訊地址、電話號碼、身份證號碼，和選擇以信用卡付款的人士的信用卡資料。於事發後，香港寬頻決定將已關閉帳戶及沒有結欠的舊客戶的個人資料保留期限由三年縮短至六個月。

私隱專員認為香港寬頻在系統遷移後沒有作全面及審慎的檢查致未有適時刪除資料庫甲。事發後發現且香港寬頻承認資料庫甲本應在 2012 年完成系統遷移後被刪除，卻因人為疏忽而被保留下來，並繼續連接內部網絡。香港寬頻遺忘了資料庫甲的存在，沒有如資料庫乙和丙般更新資料庫甲的修補程式及將資料庫甲作加密處理。即使香港寬頻在 2014 年和 2017 年均有外聘網絡安全顧問公司與內部審計部門共同進行保安審計，但都沒有發現資料庫甲仍然存在。

調查亦顯示香港寬頻在事發前沒有仔細考量舊客戶個人資料的保留期限和制定資料保留的內部指引，以及保留仍有結欠的舊客戶的資料時間過長。

另外，香港寬頻作為持有大量客戶個人資料的電訊商，妥善保障客戶的個人資料實屬客戶的合理期望。事實上，私隱專員知悉香港寬頻並非沒有在資訊保安上投放資源，除有制定政策、採取技術保安措施、進行網絡安全恆常測試和提供資訊科技相關培訓外，亦有外聘網絡安全顧問公司作保安審計。但調查顯示資料庫甲的保安措施不足，而香港寬頻亦未能充分掌握儲存有客戶和服務申請者的個人資料的資訊科技設備和保安措施的實施情況，最終發生了這宗原可避免的資料外洩事故。在此個案中，黑客利用一名有管理權限的資訊科技開發組員工的帳戶憑證，透過遠程接達服務進入

香港寬頻的網絡系統，最終成功竊取資料。該帳戶密碼並沒有按照香港寬頻資訊科技政策的要求每三個月作出更改，此反映香港寬頻未有採取技術措施強制定期更改密碼。

基於調查所得和香港寬頻所承認的事實，以及本個案的所有情況，私隱專員認為香港寬頻：（i）沒有採取所有切實可行的步驟刪除已不再需要的資料庫甲，加上保留舊客戶的個人資料時間過長，因而違反《私隱條例》第 26 條（資料刪除）和《私隱條例》附表 1 的保障資料第 2(2)原則（資料保留）；和（ii）沒有採取所有切實可行的步驟以確保資料庫甲內的個人資料受保障而不受未獲准許的查閱，因而違反《私隱條例》附表 1 的保障資料第 4(1)原則（資料保安）。私隱專員已根據《私隱條例》第 50(1)條向香港寬頻送達執行通知，以糾正及防止違規事宜。

背景

1. 成立於 1999 年，香港寬頻是一間香港上市的電訊商，其前身公司[1]由 1992 年起提供國際電訊服務。香港寬頻現時為個人及企業提供電訊服務，包括寬頻、流動服務、娛樂服務、話音通訊、雲端方案、數據設施及系統整合等。

2. 2018 年 4 月 18 日，香港寬頻向私隱專員作出資料外洩事故通報，表示發現一個已停用的客戶資料庫遭未經授權入侵。香港寬頻就事件發出新聞公報和在香港交易所作出公告，並透過短訊、電郵和郵件方式聯絡受影響人士[2]，設立專線接受查詢，以及通報通訊事務管理局辦公室。

3. 香港寬頻於 2018 年 4 月 16 日的系統保安檢查發現磁碟空間不足，從而發現遭到入侵。香港寬頻迅即中斷遠程接達服務、將受影響的伺服器下線、移取黑客植入的惡意軟件、封阻黑客的互聯網規約地址（IP 位址），和重置所有登錄密碼。2018 年 4 月 17 日，香港寬頻聘請了一間網絡安全顧問公司調查事件，並向警方報案。

[1] 香港寬頻的前身為香港電視網絡有限公司（前稱城市電訊（香港）有限公司），於1992年5月19日成立。

[2] 香港寬頻稱已於 2018 年 4 月 24 日通知所有受影響人士。

4. 2018 年 4 月 19 日，香港寬頻在中期業績發布會上就資料外洩向公眾致歉，並指是按香港法例第 112 章《稅務條例》(**《稅務條例》**)的要求保留資料。

5. 2018 年 4 月 23 日，香港寬頻召開另一記者會，表示錯誤理解《稅務條例》的要求並公布新的資料保留政策。

6. 2018 年 5 月 16 日，香港寬頻公布資料保留政策的落實時間表。

調查所獲得的證據和資料

7. 私隱專員在收到香港寬頻的資料外洩事故通報後隨即展開循規審查。在有合理理由相信事件涉及違反《私隱條例》的規定[3]後，私隱專員就香港寬頻（《私隱條例》第 2(1)條[4]所定義的資料使用者）展開調查。於循規審查及調查期間，香港個人資料私隱專員公署（**公署**）向香港寬頻作出查詢，審視香港寬頻提供的文件證據及其他公開資料，亦向稅務局了解《稅務條例》第 51C 條中有關備存業務紀錄的要求。就是次事件，公署共接獲 56 宗查詢[5]和 28 宗投訴[6]。以下為公署所獲得的相關證據及資料。

資料保留

涉及的個人資料

8. 香港寬頻保存了現有客戶、舊客戶和服務申請者的個人資料。涉及的

[3] 《私隱條例》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)

[4] 根據《私隱條例》第 2(1)條，「資料使用者（data user），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。」
(https://www.elegislation.gov.hk/hk/cap486!zh-Hant-HK?INDEX_CS=N&xpid=ID_1438403261131_001)

[5] 查詢者主要表達對資料遭外洩的不滿和查詢自我保護方法。

[6] 投訴人投訴香港寬頻保安不足及長時間保留其個人資料。

個人資料包括姓名、電郵地址、通訊地址、電話號碼、身份證號碼及選擇以信用卡付款的人士的信用卡資料，包括信用卡卡主姓名、號碼和到期日。

9. 事發時，香港寬頻將客戶資料儲存在三個資料庫內：

(1) 資料庫甲是一個已停用並應在 2012 年完成系統遷移後被刪除的資料庫。它儲存了以下人士的個人資料[7]：（i） 2003 至 2012 年間約 94,000 名固網客戶及 232,000 名 IDD 客戶；和（ii）截至 2012 年約 51,000 名服務申請者[8]；

(2) 資料庫乙是現用資料庫，用以儲存住宅固網、流動服務、IDD0030 和 OTT[9]服務的資料。它儲存了以下人士的個人資料：（i）約 1,390,000 名現有客戶；（ii）約 370,000 名已由 1998 年起終止服務（但至今尚有結欠）及由 2015 年起終止服務及沒有結欠的舊客戶；和（iii）約 10,000 名由 2016 年 12 月起計的服務申請者；及

(3) 資料庫丙是現用資料庫，用以儲存 IDD1666 服務的資料。它儲存了以下人士的個人資料：（i）約 816,000 名現有客戶；和（ii）約 48,000 名已由 2003 年起終止服務（但至今尚有結欠）及由 2016 年起終止服務及沒有結欠的舊客戶。

[7]下表列出資料庫甲儲存的各項個人資料的數量：

個人資料種類	**資料庫甲的紀錄（條）**
姓名	7,167
電郵地址	89,858
通訊地址	4,353
電話號碼	53,879
身份證號碼	311,879（涉及的 IDD 客戶身份證號碼數目為 232,252，比 IDD 客戶人數多 176，香港寬頻估計有 IDD 客戶曾提供錯誤的號碼之後再補回正確的號碼，導致數字有不同。）
信用卡卡主姓名	33,579
信用卡號碼	42,153
信用卡到期日	42,005

[8] 香港寬頻表示沒有充足資料確定資料庫甲儲存了由哪年起申請服務的人士的資料。

[9] OTT 即 Over The Top 的簡稱，即在營運商不干預的情況下透過互聯網傳送音頻、視頻及其他媒體內容。

保留客戶資料的目的

10. 保留資料庫甲並沒有任何目的。香港寬頻承認，本應在 2012 年 12 月完成的系統遷移後刪除資料庫甲。然而，由於人為疏忽，資料庫甲沒有被刪除。香港寬頻已不再需要使用資料庫甲內的資料，亦無需將其他資料庫內的資料轉移到資料庫甲內儲存。

11. 資料庫乙和丙儲存了現有客戶和舊客戶的個人資料，資料庫乙同時儲存了服務申請者的個人資料，儲存資料的目的是為了提供服務。

12. 於事發後，香港寬頻將已關閉帳戶及沒有結欠的舊客戶的個人資料保留期限由三年縮短至六個月。尚有結欠的舊客戶的個人資料保留期限沒有改變。至於為何保留尚有結欠的舊客戶的個人資料長達 20 年，香港寬頻解釋正在向部份欠款人士追討債務，而當尚有結欠的舊客戶再向香港寬頻申請服務時，香港寬頻亦會向他們追討欠款。

13. 至於保留由 2016 年 12 月起曾向香港寬頻申請服務的人士的個人資料，香港寬頻解釋該些申請者正輪候香港寬頻的服務或與香港寬頻討論服務登記事宜。香港寬頻表示由於有些申請者居住的樓宇尚未被光纖電纜覆蓋以致香港寬頻未能提供服務，當香港寬頻可提供服務時，便會聯絡那些申請者。

資料保留政策及指引

14. 公署要求香港寬頻提供資料保留和刪除政策或指引和說明有何措施確保員工依循有關政策或指引。香港寬頻提供了兩份需員工簽署的文件，分別是《個人資料（私隱）（修訂）條例聲明[10]》和《保密和不披露聲明[11]》。前者訂明所有個人資料的收集、使用、傳送和／或保留均須「*根據*」《私隱條例》而行事。該文件明確要求員工須確保不保留資料超過所需要的時間。後者則訂明員工工作上接觸的客戶資料屬機密資料。兩份文件均沒有列明客戶及服務申請者的個人資料的保留期限。

[10] 香港寬頻提供的文件為英文版，標題為 Personal Data (Privacy) (Amendment) Ordinance Declaration。
[11] 香港寬頻提供的文件為英文版，標題為 Confidentiality and Non-Disclosure Statement。

15. 香港寬頻的《個人資料及私隱政策聲明[12]》訂明*「除非法律規定要求本公司須保存閣下的個人資料一段特定的時間，本公司只會將個人資料保存至達到收集個人資料之原來目的，或直接與其有關之目的為止。我們會根據本公司之內部程序按時篡輯、清洗、銷毀或以匿名方式處理本公司系統內不必要之個人資料。」*

16. 此外，香港寬頻的《資訊科技政策[13]》中有《資料保留政策》的章節，當中訂明「資訊科技部門」應確保仍有價值的電子紀錄可被繼續使用，以及符合銷毀條件的電子紀錄應被穩妥地銷毀，但沒有列明個人資料的保留期限。

<u>系統遷移後的資料刪除</u>

17. 香港寬頻解釋由於每次系統遷移的要求和情況不一，故此沒有制定系統遷移的內部指引。

18. 香港寬頻表示在2013年、2015年和2017年進行客戶資料庫遷移項目後，均有刪除舊資料庫內的資料。資料庫甲在2012年系統遷移後沒有被刪除，仍繼續連接內部網絡，屬單一事件。

資料保安

<u>遠程接達服務成為入侵入口</u>

19. 根據網絡安全顧問公司的推斷，黑客於 2018 年 3 月 30 日以香港寬頻一名資訊科技開發組員工的帳戶憑證，透過遠程接達服務進入香港寬頻的網絡系統。由於該名員工有伺服器的管理員權限，黑客得以植入惡意軟件獲取其他帳戶憑證。黑客其後進入其他網絡段間。

20. 黑客獲取另一名資訊科技開發組員工的帳戶憑證，該名員工可接達儲存有資料庫甲的後端伺服器。黑客在 2018 年 4 月 9 日至 4 月 16 日（即香港寬頻封阻黑客的互聯網規約地址的當天）期間於資料庫甲內竊取資料。

[12] http://www.hkbn.net/tnc/HKBN_PPS_CHI_201601.pdf
[13] 香港寬頻提供的文件為英文版，標題為 Information Technology Policy。

21. 資訊科技開發組員工獲授權接達儲存有資料庫甲的後端伺服器，以處理日常工作包括程式開發和系統維護。接達儲存有資料庫乙和丙的後端伺服器只提供予資訊科技系統管理員，而不包括資訊科技開發組員工。事件發生後，接達資料庫乙和丙的後端伺服器的權限只授予三名資訊科技系統管理員。

22. 香港寬頻和網絡安全顧問公司均不能確定黑客最初是如何得悉資訊科技開發組員工的帳戶憑證，但卻發現該帳戶的密碼超過三個月沒有更改，另外，沒有發現黑客以「字典攻擊[14]」、「暴力攻擊[15]」或「鍵盤側錄程式[16]」等方法嘗試進入網絡系統或登錄失敗的記錄。

23. 香港寬頻和網絡安全顧問公司隨後的測試確認資料庫乙和丙沒有遭到入侵。

24. 香港寬頻的 1,300 名員工中，約有 300 名員工可以其用戶名稱和密碼使用遠程接達服務，當中約有 80 名資訊科技員工因資訊科技維護和營運需要而獲授權使用此服務。其他獲授權的員工來自銷售、網絡技術、人才管理和市場部，他們只可登入相關的虛擬桌面界面。接達權由部門主管按需要授權和批准。

<u>資訊科技政策和實施</u>

25. 香港寬頻設有《資訊科技政策》，對存取控制、密碼、加密、防毒、網絡保安、資料保留等均有規定。《資訊科技政策》於2013年12月初次發出，於2014年6月和2017年12月作修訂，計劃每年最少檢視一次。

加密

26.《資訊科技政策》指出在合理及必要時需以加密方式來保障公司資料，香港寬頻確認除資料庫甲外，資料庫乙和丙已作加密處理。香港寬頻沒有應本公署要求解釋為何資料庫甲沒有作加密處理。

[14] 字典攻擊是使用字典中可找到的字，用以破解加密或認證系統的一種技術。

[15] 暴力攻擊是嘗試所有可能性以破解加密或認證系統的技術。

[16] 鍵盤側錄程式是一個裝置或程式，用作擷取輸入裝置的活動。黑客會利用鍵盤側錄程式去擷取輸入到電腦系統的個人資料。

修補程式

27.《資訊科技政策》訂明修補程式需要適時更新，關鍵的修補程式需於一個月內更新，而非關鍵的修補程式亦需於三個月內更新。但由於資料庫甲本應被刪除，故此在系統遷移後一直沒有更新修補程式。

密碼

28.《資訊科技政策》訂明密碼三個月需更改一次、密碼需附合特定的長度和組合要求（相關敏感資料的詳情不會在此報告中披露）及不得共用密碼。然而，事發前系統只於首次登入時強制更新預設密碼，並沒有設定於每三個月強制更新登入密碼一次。被盜的登入密碼估計是屬於資訊科技開發組員工並已超過三個月沒有更新，香港寬頻保證所有密碼已在事發後更新。

29. 是次事件雖不涉及以「字典攻擊」、「暴力攻擊」或「鍵盤側錄程式」等方法進入網絡系統，亦沒有發現登入失敗的紀錄。然而，機構一般均會於系統中設置有關密碼處理的保安功能，包括在嘗試登入失敗達特定次數後，系統會自動鎖起有關帳戶，並限制該帳戶只能經系統／保安管理員以人手處置重啟。事發前，香港寬頻的系統會將登入失敗五次的帳戶自動鎖起30分鐘。事發後香港寬頻將監控提升，香港寬頻的系統會將登入失敗五次的帳戶自動鎖起120分鐘。然而，無論事發前或後，重啟帳戶均無需系統／保安管理員人手處置。

<u>保安審計</u>

30. 香港寬頻設有內部審核及風險部門，監督保安系統的定期審查。香港寬頻於 2014 年和 2017 年均有外聘網絡安全顧問公司共同進行保安審計。

31. 2017 年的保安審計的目的是評估網絡漏洞，當中包括模擬網絡攻擊和模擬釣魚郵件攻擊。然而，即使有進行保安審計，但沒有發現資料庫甲仍然存在的問題。網絡安全顧問公司認同香港寬頻採用的網絡安全產品和解決方案可提供多重防禦，亦有就內部網絡設有接達控制，以減低潛在網絡襲擊。同時，該保安審計亦發現若干保安漏洞，包括在網上應用系統的漏洞評估中發現系統管理員的帳戶憑證，在模擬網絡攻擊中採用的惡意程式可依附於電郵附件內而避過偵測，而在模擬

釣魚郵件攻擊中亦有部份員工程誤按郵件中的超連結。

32. 香港寬頻其後採取了網絡安全顧問公司的建議，更改網上應用系統軟件的原始碼以移除十大保安風險[17]，向所有員工提供資訊保安認知培訓，以及加強伺服器資料的存取控制。

內部培訓和認證

33. 香港寬頻於 2011 年至 2013 年、2016 年和 2017 年均有舉辦《私隱條例》講座[18]，員工亦要簽署同意遵從《私隱條例》要求的聲明。

34. 香港寬頻已獲取支付卡行業資料安全標準[19]認證，亦參考資訊安全管理系統標準（即 ISO 27001）作為資訊保安的行事方式。

議題

(1) 香港寬頻在系統遷移後有沒有採取步驟刪除資料庫甲的個人資料?

35. 資料庫甲由 2012 年 12 月完成系統遷移後超過五年沒有被刪除。私隱專員明白系統遷移後可能需要待資料的完整性獲確認才可刪除原來的資料庫，因而有需要保留原來的資料庫一段時間。然而，私隱專員發現香港寬頻遺忘了資料庫甲的存在。即使在 2014 年和 2017 年均有外聘網絡安全顧問公司與內部審計部門共同進行保安審計，但卻沒有發現資料庫甲仍然存在這問題。香港寬頻亦沒有就系統遷移制訂內部指引。

(2) 香港寬頻保留舊客戶和服務申請者的個人資料的時間是否過長?

36. 香港寬頻沒有制訂明確的政策列明客戶和服務提供者個人資料的保留期限。實際操作上，香港寬頻在事發前保留（i）沒有結欠的舊客戶的個人資料三年；（ii）尚有結欠的舊客戶的個人資料達 20 年及

[17] 指由 Open Web Application Security Project 發布的網上應用系統十大保安漏洞。Open Web Application Security Project 是一個致力提高軟件安全性的全球非牟利組織。

[18] 2011 年至 2013 年間為員工舉辦了五次《私隱條例》講座，但在 2014 年和 2015 年則未有舉辦類似講座。

[19] 英文全寫為：Payment Card Industry Data Security Standard，簡稱「PCI DSS」。

（iii）服務申請者的個人資料少於兩年。香港寬頻在事發後檢討其操作，將沒有結欠的舊客戶的個人資料保留期限由三年縮短至六個月，其他客戶及服務申請者的個人資料保留期限則不變。

(3) 香港寬頻有沒有實施可行的措施來保護客戶和服務申請者的個人資料?

37. 香港寬頻設有《資訊科技政策》，該政策不時更新，就加密要求、更新修補程式等亦有明文規定。香港寬頻亦在網絡安全、接達控制等方面採取技術保安措施，進行網絡安全恆常測試，為員工提供資訊科技相關培訓，及外聘網絡安全顧問公司與內部審計部門共同進行保安審計，並因應保安審計的發現進一步加強資訊保安。

38. 事件中，黑客被發現以香港寬頻一名資訊科技開發組員工的帳戶憑證，透過遠程接達服務進入香港寬頻的網絡系統，而該名員工有管理員權限。黑客其後得以從沒有加密的資料庫甲下載資料。資料庫甲由 2012 年起沒有更新程式。被盜的登入密碼並未按照香港寬頻《資訊科技政策》的要求三個月更新一次。此外，在事件中被用作入侵入口的遠程接達服務僅以用戶名稱和密碼核實用戶身份。

法例

《私隱條例》

39.《私隱條例》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《私隱條例》附表 1 的六項保障資料原則[20]的規定。香港寬頻，作為資料使用者，須遵守《私隱條例》的規定。《私隱條例》中與本個案有關的條文如下：

(1) 資料刪除

《私隱條例》第 26(1)條規定：

[20] 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《私隱條例》附表 1 。
(https://www.elegislation.gov.hk/hk/cap486!zh-Hant-HK@2013-04-25T00:00:00/sch1?clpid=228384)

「凡資料使用者持有的個人資料是用於某目的（包括與該目的有直接關係的目的），但已不再為該等目的而屬有需要的，則除在以下情況外，該資料使用者須採取所有切實可行步驟刪除該資料 ——

(a) 該等刪除根據任何法律是被禁止的；或

(b) 不刪除該資料是符合公眾利益（包括歷史方面的利益）的。」

(2) 資料保留

《私隱條例》附表 1 的保障資料第 2(2)原則規定：

「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。」

(3) 資料保安

《私隱條例》附表 1 的保障資料第 4(1)原則規定：

「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。」

40. 根據《私隱條例》第 2(1)條，「切實可行」指合理地切實可行。

《稅務條例》

41. 香港寬頻在 2018 年 4 月 19 日的中期業績發布會上表示儲存截至 2012 年的客戶資料是為了符合《稅務條例》中有關保留紀錄七年的規定。《稅務條例》第 51C 條有關的條文如下:

> *"(1) 除第(2)款另有規定外，每名在香港經營某行業、專業或業務的人，須就其入息及開支以英文或中文備存足夠的紀錄，以便該行業、專業或業務的應評稅利潤能易於確定，並須在該紀錄所關乎的交易、作為或營運完結後，將該紀錄保留為期最少 7 年。*
>
> *(2) 第(1)款並不規定須保存以下紀錄 ——*
>
> *(a) 已被局長指明無須保存的紀錄；或*
> *(b) 屬於已解散法團的紀錄。*
>
> *(3) 就本條而言，**紀錄(records)**包括 ——*
> *(a) 紀錄收入及付款，或入息及開支的帳簿(不論是否以能閱讀或不能閱讀形式藉電腦或其他方式備存)；及*
> *(b) 憑單、銀行結單、發票、收據及用以核實(a)段所指帳簿內的記項所需的其他文件。"*

42. 稅務局發出的《保存業務紀錄須知說明書》指出，就供應的貨物或服務，納稅人應向顧客發出包括以下資料的發票：發票號碼、發出日期、顧客姓名和地址、納稅人的業務名稱和地址、交易日期、貨物或服務摘要（包括數量和價錢）和價錢總額。

43. 根據稅務局對本公署的回覆，納稅人可用電腦保存業務紀錄，但仍須保存原本文件（例如：支票存根、發票），以證明其收入及開支。不同業務各有其買賣或服務類別、經營方式及會計系統，納稅人須按《稅務條例》第51C條規定，判定備存何等紀錄，以能易於確定業務的應評稅利潤，及在稅務局審核業務時，提供足夠資料。

結論

違反《私隱條例》

44. 基於調查所得和香港寬頻所承認的事實，以及本個案的所有情況，私隱專員認為香港寬頻以下做法違反《私隱條例》第 26 條（資料刪除）、《私隱條例》附表 1 的保障資料第 2(2)原則（資料保留）和第 4(1)原則（資料保安）。

45. 有關《私隱條例》第 26 條（資料刪除）、《私隱條例》附表 1 的保障資料第 2(2)原則（資料保留）及《稅務條例》：

(1) 在 2012 年完成系統遷移後，香港寬頻已無需保留資料庫甲，但資料庫甲卻因人為疏忽而沒有被刪除。香港寬頻未能妥善跟進或檢查，以確保資料庫甲已被刪除。

(2) 香港寬頻沒有制定指引，訂明系統遷移後刪除已停用資料庫內的個人資料的步驟和時限。

(3) 香港寬頻在事發前並沒有深究保留客戶和服務申請者的個人資料的目的。事實上，香港寬頻最初曾稱保留資料庫甲是為了符合《稅務條例》的要求，但在書面回覆公署時，則坦承無需再保留資料庫甲。由此可見，香港寬頻未能掌握保留資料庫甲的目的。事發後，香港寬頻決定將所有已關閉帳戶及沒有結欠的客戶的個人資料的保留期限由三年縮短至六個月，亦顯示香港寬頻在事前沒有充分評估保留各項資料的時間，以致事發前保留舊客戶的個人資料時間過長。

(4) 香港寬頻在資料庫乙和丙保留仍有結欠的舊客戶的個人資料 15 年以上。根據香港寬頻的回覆，只有部份欠款個案正在進行追討程序，其餘的欠款個案香港寬頻只選擇被動地等待欠款人再次申請服務時才向他們追討，在此情況下，私隱專員認為香港寬頻保留已終止服務但仍有結欠的舊客戶的個人資料時間過長。

(5) 香港寬頻沒有向公署提交事發前各項個人資料的保留期限的內部文件。雖然《私隱條例》沒有要求資料使用者必須就個人資

料的保留期限訂立指引，但私隱專員認為一間持有過百萬客戶個人資料的公司，管理層應當書面訂立清晰的個人資料保留期限和監管機制以確保資料按時刪除。

(6) 稅務局回應公署查詢時解釋《稅務條例》只要求保留原本文件（例如：支票存根、發票）最少七年，以讓局方易於確定納稅人的應評稅利潤。可是，《稅務條例》並沒有就納稅人利用原本文件的資料整合成的客戶資料庫訂立保留時間。香港寬頻在事發後承認錯誤理解《稅務條例》的要求。私隱專員認為香港寬頻無需為符合《稅務條例》的要求而保留資料庫甲，亦不能以此作為長時間保留資料庫甲的理由。

46. 綜上所述，私隱專員認為香港寬頻沒有採取所有切實可行的步驟刪除已不再需要的資料庫甲，加上保留舊客戶的個人資料時間過長，因而違反《私隱條例》第 26 條（資料刪除）和《私隱條例》附表 1 的保障資料第 2(2)原則（資料保留）。

47. 就《稅務條例》方面，由於《稅務條例》第 51C 條只要求機構保留原本文件最少七年，但並沒有訂明儲存原本文件的資料的資料庫的保留時間，私隱專員認為相關條文並不適用於本個案。

48. 有關《私隱條例》附表 1 的保障資料第 4(1)原則（資料保安）：

(1) 私隱專員認為香港寬頻作為一間持有大量重要個人資料的上市電訊商，必須實施穩健的保安措施以符合《私隱條例》附表 1 的保障資料第 4(1)原則（資料保安），而顧客對香港寬頻能妥善保存他們的個人資料抱有期望亦十分合理。

(2) 香港寬頻直至發生入侵事故後才察覺資料庫甲仍然存在，此反映香港寬頻欠缺有效機制充分掌握資訊科技設備和保安措施的實施情況。

(3) 資料庫甲雖然儲存了客戶和服務申請者重要的個人資料，包括身份證號碼和信用卡號碼，但卻沒有作加密處理。香港寬頻的《資訊科技政策》指出在合理及必要時需以加密方式來保障公司資料。將資料作加密處理是防止黑客查閱客戶和服務申請者的個人資料的最後防線，香港寬頻亦確認資料庫乙和丙均有作加

密處理。

(4) 黑客是透過遠程接達服務進入香港寬頻的網絡系統。香港寬頻共有約 300 名員工獲授權使用遠程接達服務。事發前，香港寬頻的遠程接達服務是透過核實用戶名稱和密碼來驗證用戶的身份，未有採取雙重認證。此外，資訊科技開發組員工享有管理員權限，而被盜的登入密碼被發現超過三個月沒有更新，這顯示香港寬頻缺乏機制確保密碼政策得以有效執行。事發後，香港寬頻提升系統，如戶口密碼於 90 日到期後沒有更新，戶口便會自動停止。

49. 在調查期間，香港寬頻保證於事發後已減少儲存的資料及採納網絡安全顧問提出的建議，包括：

(1) 刪除所有已關閉帳戶及沒有結欠超過六個月的客戶的全部個人資料；
(2) 以「代碼」取代信用卡號碼以完成與銀行之間的交易，資料庫不再儲存信用卡號碼；
(3) 刪除前線人員系統內客戶身份證號碼的其中兩個及括號內的號碼（ 例 A12XX56(X)）；而完整的身份證號碼則將儲存在後勤系統 ，只有三名資料庫管理員有訪問權；
(4) 於內部網絡段間加設防火牆；
(5) 分隔桌上電腦或端點至伺服器以及分隔前端器、後端和資料庫伺服器間的通訊；
(6) 遠程接達需雙重認證；
(7) 加強網絡安全意識培訓；及
(8) 成立先進的內部保安營運中心，該中心備有最新的進階威脅防護工具，並會 24 小時全天候監察香港寬頻的網絡及伺服器的活動。

50. 基於調查所得的事實及香港寬頻於事發後所承諾採納的糾正措施，私隱專員認為香港寬頻沒有採取所有切實可行的步驟以確保資料庫甲所存有的個人資料受保障而不受未獲准許的查閱，因而違反《私隱條例》附表 1 的保障資料第 4(1)原則（資料保安）。

執行通知

51. 根據《私隱條例》第 50(1)條，私隱專員在完成調查後，如認為有關的資料使用者正在或已經違反《私隱條例》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。

52. 私隱專員考慮到香港寬頻新的個人資料保留期限，《稅務條例》的要求和香港寬頻所加強的保安措施，私隱專員決定根據《私隱條例》第50(1)條向香港寬頻送達執行通知，以糾正及防止違規事宜。私隱專員指令香港寬頻：

(1) 制定清晰的程序，訂明系統遷移後刪除不再需要的資料庫內的個人資料的步驟、時限和監察措施；

(2) 制定清晰的資料保留政策，訂明客戶及服務申請者個人資料的保留期限，不得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所需的時間；

(3) 制定清晰的資料保安政策，訂明定期檢視用戶權限及遠程接達服務的保安措施；

(4) 實施有效的措施，確保有關員工知悉和執行上述第(1)、(2)及(3)項所訂的政策及程序；及

(5) 根據上述第(2)項所訂的資料保留政策，刪除所有超過保留期限的客戶及服務申請者的個人資料。

53. 香港寬頻須於收到執行通知的 90 天內完成上述事宜，並隨即提交有關證明文件供私隱專員參閱。

其他意見

54. 此個案源於一名黑客入侵一間電訊商的網絡及從一個已停用的資料庫中下載客戶資料。如電訊商在系統遷移後已適時妥善刪除資料庫，事

件對客戶造成的損害本能避免。

55. 電子紀錄並非如紙張紀錄般佔用空間，加上現今儲存電子紀錄的成本愈見下降，按時刪除電子紀錄容易被忽略。本公署自 2014 年起提倡私隱管理系統，其中一項系統管理措施是個人資料庫存。按時更新的個人資料庫存可讓機構清楚了解所持有的個人資料種類、儲存資料的地點及保留期限等。保留較少客戶的電子紀錄可減輕網絡攻擊所能造成的損害。私隱專員因此建議機構（尤其是儲存大量個人資料的機構）慎重檢視資料庫存和保留期限，以免成為黑客入侵的受害者。

56. 一般而言，為了處理稅務的目的而保存舊客戶的資料七年並不違反《私隱條例》。根據公署向稅務局的查詢 ，稅務局要求保留最少七年的原本文件（例如：支票存根、發票），目的是讓稅務局易於確定納稅人的應評稅利潤。但《稅務條例》並沒有就納稅人利用原本文件的資料再整合成的客戶資料庫訂立保留時間。機構應按客戶資料庫內各項個人資料的使用目的訂立保留期限，並在保留期限完結後刪除資料。

57. 機構在營運思維上應摒棄只需依從最低監管要求的想法，恪守更高的道德標準，以符合持份者的期望。就此，私隱專員建議機構應採納問責原則，將數據管治和管理以至數據道德倫理（包括尊重 、互惠和公平）納入機構管治之中，並從最高管理層做起，由上而下貫徹地在機構中執行有關保障個人資料的政策。長遠而言，一個具備健全的私隱保障基建輔以恒之有效的檢討及監察程序的私隱管理系統，方為機構應對個人資料私隱的不二方案。建立全面的私隱管理系統不但可促使機構符合法律規定，更可加強客戶的信任、從而提升其商譽及加強競爭優勢。

58. 鑑於近年資料外洩事故頻生，私隱專員認為社會應重新討論是否應向違反《私隱條例》附表 1 的保障資料原則的資料使用者判處行政罰款。現時私隱專員未獲授權判處罰款，私隱專員只獲授權在合適的情況下發出執行通知，要求資料使用者採取措施，以糾正違反《私隱條例》的行為。資料使用者違反執行通知，才屬觸犯刑事罪行，法院定罪後可判最高刑罰港幣 5 萬元及監禁兩年。私隱專員同時亦注意到現行機制中，有其他法定機關獲賦予行政罰款的職能和權力。此外，歐盟於 2018 年 5 月 28 日實施新的《一般資料保護規則》，亦賦予監管

機構判處行政罰款的權力，未能遵守該規則的商業機構最高可被私隱監管機構判以全球營業額的 4%或 2000 萬歐元（以較高者為準）的罰款。故此，私隱專員認為有必要檢討應否對違規者判處類似行政罰款，以增阻嚇作用。

59. 現時《私隱條例》並無強制機構在發生資料外洩事故後必須通報有關監管機構或資料當事人。儘管如此，香港寬頻仍能於發現事故後盡快通報私隱專員及通知受影響的客戶，此實屬良好的舉措。

60. 私隱專員歡迎香港寬頻於事發後所執行及承諾採納的糾正措施，但提醒香港寬頻仍需繼續致力加強保障客戶的個人資料。

61. 私隱專員亦樂見香港寬頻於循規審查及調查期間的坦承態度，並願意採取與承諾採納糾正措施，及公布有關詳情。

---完---

本報告可於本公署網頁下載：

https://www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/invest_report.html