

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)

眾安銀行有限公司 的客戶個人資料系統

報告編號：R23 - 20950

發表日期：2023 年 10 月 9 日

眾安銀行有限公司
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
個人資料私隱專員
2023 年 10 月 9 日

第 I 部 – 背景

1. 本港銀行業近年積極發展金融科技，透過數碼渠道為客戶提供一站式金融服務體驗。銀行在提供便捷和高效的金融服務的同時，亦應致力保障其客戶個人資料系統，以符合市民的期望。
2. 自香港金融管理局（金管局）在 2019 年發出首批虛擬銀行牌照以來，至今共有 8 家虛擬銀行¹在港營運。虛擬銀行的主要服務對象為零售客戶，亦會為中小型企業提供商業銀行服務。相較於傳統銀行，虛擬銀行不設實體分行，而是透過互聯網、流動應用程式或其他形式的電子傳送渠道向客戶提供電子化銀行服務。
3. 虛擬銀行與傳統銀行同樣受金管局監管，須遵守同一套監管規定。虛擬銀行從開戶、辦理業務至系統維護的整個過程均涉及收集、處理、使用及保存大量屬性質敏感的客戶個人資料。加上虛擬銀行主要依賴互聯網提供銀行服務，在日益複雜和增多的網絡安全威脅下，虛擬銀行在處理客戶個人資料整個生命週期中所面臨的保安挑戰實在不容忽視。
4. 基於虛擬銀行日常會處理大量性質敏感的個人資料，個人資料私隱專員（私隱專員）遂根據香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）第 36 條，對眾安銀行有限公司（眾安銀行）進行視察，審視其客戶個人資料系統。

眾安銀行的業務架構

5. 眾安銀行為眾安科技（國際）集團有限公司於 2019 年成立的綜合金融品牌。眾安銀行在 2019 年 3 月獲金管局發出虛擬銀行牌照，並在 2020 年 3 月成為香港首間虛擬銀行。由於眾安銀行持有虛擬銀行牌照、證券交易牌照及保險代理牌照，其營運（包括處理個人資料

¹ 包括天星銀行有限公司、螞蟻銀行（香港）有限公司、富融銀行有限公司、理慧銀行有限公司、MOX BANK LIMITED、平安壹賬通銀行（香港）有限公司、匯立銀行有限公司及眾安銀行有限公司。

方面) 須同時符合金管局、證券及期貨事務監察委員會及保險業監管局的相關規定。

6. 眾安銀行為客戶提供存款、貸款、轉帳、消費、保險、基金投資及商業銀行等金融服務。截至 2023 年 6 月 30 日，眾安銀行的零售用戶數目接近 70 萬人，擁有存款餘額約 107 億港元，貸款餘額約 49 億港元²。
7. 於視察期內，眾安銀行聘有超過 150 名員工，而當中多個部門的工作均涉及客戶個人資料的查閱及處理，包括 (i) 前線員工負責審批開戶和借貸、監察並匯報異常交易、提供客戶服務及處理客戶投訴；(ii) 合規部門專職監察各部門遵守《私隱條例》、與處理客戶個人資料相關的監管規定及內部政策的情況，並推行個人資料私隱管理系統；(iii) 負責信貸風險管理的部門會審視客戶帳戶及信貸資料；(iv) 反洗錢部門應監管部門打擊洗黑錢及恐怖分子資金籌集的要求進行適時監察和調查可疑的帳戶活動；及 (v) 負責審核的部門會定期評估內部不同部門處理客戶個人資料的做法，並提出改善建議。

視察範圍

8. 眾安銀行作為《私隱條例》下的資料使用者，在收集、持有、處理及使用客戶個人資料方面，須遵從《私隱條例》的各項規定，包括附表 1 的六項保障資料原則³。本視察聚焦眾安銀行就客戶個人資料由收集、持有、處理、使用、保安以至銷毀的整個生命周期的管理機制。



² www1.hkexnews.hk/listedco/listconews/sehk/2023/0828/2023082800340_c.pdf

³ www.pcpd.org.hk/tc_chi/data_privacy_law/6_data_protection_principles/principles.html

第 II 部 – 視察方法

9. 視察由為 2022 年 1 月開始。因應 2019 冠狀病毒病疫情，實地視察於 2022 年 7 月 11 至 26 日進行。私隱專員派出視察小組⁴視察眾安銀行的客戶個人資料系統、其員工及服務提供者如何遵從眾安銀行的資料保安政策和行事方式，並透過與眾安銀行七次書面查詢（包括實地視察後的書面查詢）中累計審閱了 104 份共超過 2,770 頁的政策、手冊、指引、僱員行為守則、培訓資料及顧問報告，以及眾安銀行與服務提供者的服務合約。在視察過程中，視察小組亦參考了 16 份金管局有關持牌銀行收集、處理及保障客戶個人資料的監管政策手冊及相關通函。
10. 此外，私隱專員根據《私隱條例》行使進入處所的權力進行實地視察。2022 年 7 月份，視察小組在各方同意下合共七次到訪眾安銀行的辦事處及數據中心。視察小組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，當中包括眾安銀行的 8 位部門主管、10 位高級員工及 10 位前線員工；
 - (ii) 到訪眾安銀行 9 個部門及與電話服務中心員工作視像會面，了解客戶個人資料系統的實際運作及相關存取控制機制；
 - (iii) 觀察眾安銀行員工示範客戶個人資料系統的運作、透過系統存取個人資料的做法以及員工存取個人資料的具體管理程序；及
 - (iv) 抽樣檢查眾安銀行載有客戶個人資料的紙本紀錄及電腦檔案紀錄，當中包括客戶個人資料系統的員工活動日誌紀錄。
11. 視察小組亦曾以神秘顧客的形式，透過眾安銀行指定的流動應用程式「ZA Bank」（該流動應用程式）⁵登記成為眾安銀行的零售客戶，以全面了解眾安銀行處理客戶申請的流程（詳見附錄 1），並透過該流動應用程式向前線員工作出查詢。

⁴ 視察小組由一名首席個人資料主任、一名高級個人資料主任、兩名個人資料主任及兩名助理個人資料主任組成。

⁵ 該流動應用程式除了可於蘋果及谷歌的流動應用程式商店下載外，眾安銀行亦在其官方網站提供超連結讓安卓手機用戶直接下載安卓 APK 安裝檔。

第 III 部 – 主要視察結果

12. 本報告主要是根據整個視察過程，包括眾安銀行所提供的資料及視察小組於實地視察留意到的事宜而作出的。本報告除指出眾安銀行可以改善的地方之外，亦指出眾安銀行管理其客戶個人資料系統所採取的良好行事常規。本報告的視察結果及建議不會影響或損害私隱專員根據《私隱條例》行使任何權力或履行任何職能。

良好行事常規

13. 經視察後，私隱專員大致滿意眾安銀行就保障客戶個人資料所採取的措施，私隱專員留意到眾安銀行在下述範疇建立了良好的行事常規：

(1) 建立個人資料私隱管理系統

14. 個人資料私隱管理系統的其中一環是委任保障資料主任及／或設立保障資料部門，以全面監督機構保障個人資料私隱的措施是否符合《私隱條例》的規定。私隱專員欣悉眾安銀行除了委任合規部門的主管，亦設有專職的保障資料主任，就其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）進行持續監察，並直接向最高管理層匯報。
15. 根據眾安銀行的資料政策，客戶的個人資料被界定為「機密」資料，須謹慎地儲存、使用及棄置。眾安銀行的客戶個人資料系統備有個人資料庫存，當中的資訊包括所收集的個人資料的類別、保留期限以及如何處理個人資料。眾安銀行亦會定期檢視其個人資料庫存，確保所收集的個人資料屬必須但不超乎適度，符合收集最少資料的原則。
16. 眾安銀行的保障資料主任亦擬備了私隱風險評估問卷，作為風險評估工具。營運部門在改動或開展涉及客戶個人資料的新計劃前，須

先評估實際程序對個人資料私隱的影響，以及就各項潛在風險制訂解決方法，包括資料事故應變計劃和通報機制。

17. 在審閱文件的過程中，視察小組得悉眾安銀行已就不同範疇⁶制訂相應的政策及指引，並會定期或按需要覆檢和修訂。為了確保有關政策及指引持續地遵從《私隱條例》的規定，眾安銀行已委派內部審核部門定期審核不同營運單位，並就這些單位處理客戶個人資料方面的做法提出改善建議。此外，眾安銀行亦曾聘請外部顧問審核其資訊科技保安系統，並已就相關審核結果採取了相應糾正措施。
18. 考慮到眾安銀行管有數量龐大的客戶個人資料系統及其所持有的個人資料的敏感度，私隱專員對眾安銀行以負責任的態度處理客戶個人資料及遵守《私隱條例》的規定表示滿意。

(2) 實行無紙化辦公環境

19. 由於虛擬銀行只透過指定的流動應用程式向零售客戶提供銀行服務，因此在相當程度上減少營運上產生的紙本紀錄，相應減低因錯誤存放或意外遺失紙本紀錄而造成的個人資料外洩風險。
20. 私隱專員樂見眾安銀行大致上實行無紙化日常營運，除了處理監管機構、執法機關及政府部門索取個人資料的要求，以及其他僱傭相關事宜外，眾安銀行的大部份工作均透過其內聯網系統完成，無須另行打印或彙整成紙本紀錄存檔。
21. 而因應監管機構、執法機關及政府部門索取個人資料的要求而產生的紙本文件則被儲存於裝有閉路電視鏡頭及智能卡門禁系統的獨立房間，以防止有未經准許或授權的人士進入。此外，眾安銀行亦在辦公範圍放置上鎖的廢紙收集桶，妥善處理員工棄置載有個人資料或敏感資料的文件。

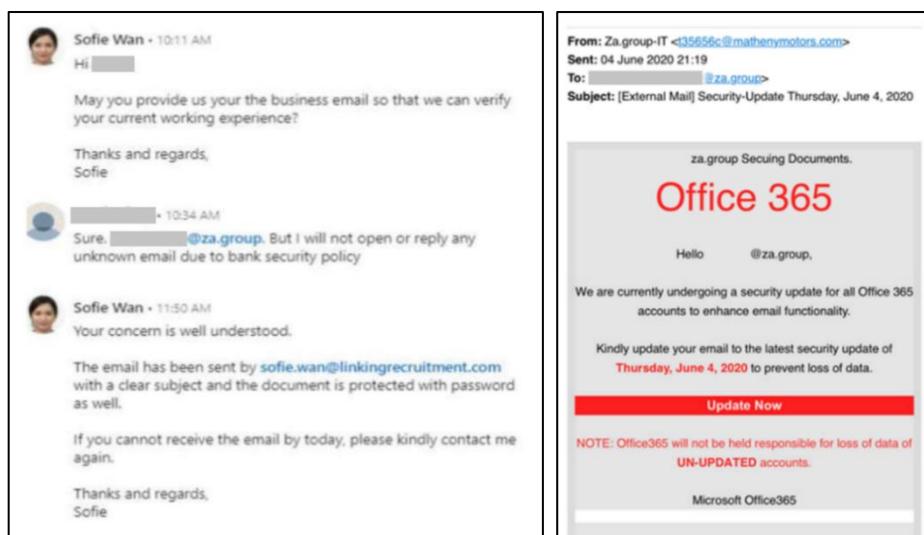
⁶ 包括資料保留及刪除、個人資料保安、網絡安全、修補程式管理、帳戶及密碼管理等。

22. 總體來說，私隱專員認為眾安銀行在保障載有客戶個人資料的紙本紀錄免遭未經准許的或意外的查閱、處理、刪除、喪失或使用方面採取了足夠的保安措施。

(3) 防範釣魚襲擊的威脅

23. 黑客經常針對持有大量個人資料的機構進行釣魚襲擊，輕則干擾其系統的正常運作，重則入侵其管理員帳戶甚或惡意加密其系統內的檔案。因此機構須制訂有效的防範策略，以及早識別和減低釣魚襲擊的威脅。

24. 私隱專員注意到眾安銀行除了設定電郵系統、防範及過濾可疑電郵外，亦會為員工安排「釣魚襲擊演習活動」，模擬工作場所內發生網絡騙案，鼓勵員工主動舉報懷疑詐騙電郵，從而提高員工的警覺程度。眾安銀行向視察小組表示自推行「釣魚襲擊演習活動」以來，未曾有員工點擊相關模擬釣魚電郵的超連結。



「釣魚襲擊演習活動」的訊息（左）及電郵（右）樣本

25. 私隱專員認為眾安銀行的上述演習活動成效良好，有助眾安銀行防範網絡攻擊。

(4) 推動工作場所的私隱友善文化

26. 健全的個人資料私隱管理系統有賴機構內所有員工對保障客戶個人資料私隱的努力。私隱專員樂見眾安銀行備有以下各項提升員工對保障個人資料私隱的意識的政策及措施，令他們致力保障個人資料私隱：

- (i) 新入職的員工（不論全職或兼職）必須接受個人資料保障培訓，並在入職時簽署確認已經閱讀僱員行為守則及有關個人資料保障的手冊；
- (ii) 定期舉辦研討會或工作坊，教育員工為帳戶設定高強度密碼，以及提醒員工須遵守《私隱條例》、保障資料原則及「起底」罪行的相關規定及違反規定的嚴重法律後果；
- (iii) 推行桌面清理政策，並由保障資料主任定期巡查工作間，查看載有客戶個人資料的文件是否獲妥善保存，或員工有否於電腦螢幕或電腦貼有顯示密碼的便利貼或紙張。如發現有員工未有遵從，該員工會收到警告標貼提醒；及
- (iv) 在辦公範圍內張貼以資料保安、防範網絡詐騙及密碼管理等主題的宣傳海報及告示，以提升員工保障個人資料的意識。



眾安銀行在辦公範圍張貼的宣傳海報

可以改善範疇

27. 除上述的良好行事常規，私隱專員亦留意到眾安銀行在保障客戶個人資料方面有以下可改善的地方：

(1) 加強對資料處理者的管理

28. 私隱專員留意到眾安銀行將部分涉及處理客戶個人資料的工作外判予第三方服務供應商（即資料處理者⁷）處理，包括製作實體提款卡及追收結欠款項。雖然如此，眾安銀行向視察小組確認所有獲委聘處理客戶個人資料的資料處理者均事先經過金管局審核，確保涉及處理客戶個人資料的做法符合相關監管要求。

29. 視察小組曾經以書面向眾安銀行索取涉及製作實體提款卡及追收結欠款項的服務合約及相關現場審核報告。視察小組留意到服務合約包括萬一發生資料外洩的處理程序，要求資料處理者一旦發現有個人資料外洩事故，必須盡快通報眾安銀行以作跟進。私隱專員樂見眾安銀行有採取合約規範方法，以防止轉移予資料處理者的個人資料在未獲准許或意外的情況下被查閱、處理、刪除、喪失或使用。

30. 不過，私隱專員留意到眾安銀行未有定期對負責製作實體提款卡的資料處理者進行現場審核，確保負責製作實體提款卡的資料處理者遵守服務合約的規定，採取適當的保安措施保障及適時銷毀眾安銀行客戶的個人資料。因應視察小組對此事表達的關注，眾安銀行表示已於 2023 年 2 月派員進行有關現場審核。

31. 雖然私隱專員理解眾安銀行礙於 2019 冠狀病毒病爆發而實施的出入境限制，未能如期派員現場審核資料處理者，惟私隱專員認為眾安銀行應考慮聘用獨立審核人員代替眾安銀行員工完成私隱循規審

⁷ 資料處理者是指非為本身目的而是代另一人處理個人資料的人。資料處理者並不受《私隱條例》直接規管，但如資料使用者聘用資料處理者（不論是在香港或香港以外聘用），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（保障資料第 2(3)原則），及有關個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用（保障資料第 4(2)原則）。

核，以持續監察資料處理者處理眾安銀行客戶個人資料的行事方式是否符合相關服務合約的規定。

32. 除此之外，私隱專員審閱負責提供追收結欠款項服務的資料處理者的現場審核報告時，發現眾安銀行員工未有在審核報告中具體指出資料處理者採取了哪些實體及系統保安措施，以及有否適時刪除逾期的客戶個人資料。即使私隱專員信納眾安銀行員工曾經逐一確認相關範疇，但為了進一步提升現場審核的問責程度及一致性，私隱專員建議眾安銀行在現場審核報告中羅列所有現場審核的項目清單及審核結果以作紀錄。在本報告發表前，眾安銀行表示已採納私隱專員的上述建議，修訂供員工使用的審核報告表格，完善有關工作紀錄。

(2) 提升資料遺失防護系統的監察能力

33. 在到訪辦事處期間，眾安銀行曾經向視察小組示範其資訊保安防護能力，範圍涵蓋系統防護、存取控制及實體保安等技術層面，當中涉及的技術措施包括資料遺失防護系統及端點保安等⁸。
34. 視察小組注意到眾安銀行設定資料遺失防護系統時，有規則偵測對外發送的電郵包含的個人資料，並適用於所有員工（不受不同類別員工或權限所限制）。
35. 私隱專員認為要有效防止個人資料被濫用或用於「起底」等非法用途，觸發系統警告的條件應該以角色為本。因此，私隱專員建議眾安銀行根據不同員工的職能及權限設定相應規則，或將經常往來的監管機構及執法機關的電郵地址域名列入白名單⁹，審慎區別不同崗位於日常營運中的需要，以盡早偵測可疑行為。

⁸ 基於保安技術的敏感性及保密性，有關詳情被略去。

⁹ 在白名單中，只有符合系統預先設定的條件才予以允許，其他則全部過濾或刪除。
(www.infosec.gov.hk/tc/best-practices/business/securing-web-application)

(3) 限制員工查閱客戶個人資料的時間

36. 視察小組在眾安銀行示範系統操作期間發現有負責審批開戶申請的前線員工可以查閱其出任該職位兩年以來所有經其審批的開戶申請詳情，當中包括申請人的姓名、身份證明文件、通訊地址、電話號碼及電郵地址等個人資料。
37. 負責營運部門的主管在回應視察小組口頭查詢時表示，該部門會每月隨機覆檢開戶申請以確保資料的準確性，但承認該名前線員工在完成開戶審批程序後，在一般情況下並無工作需要重新查閱所有經其審批的申請詳情以及申請人的個人資料。
38. 私隱專員認為眾安銀行在系統管理上大致採用「有需要知道」¹⁰的原則，授予員工最小的查閱權限以完成工作。儘管如此，眾安銀行須因應員工的工作需要限制其查閱工作紀錄的時間，減低客戶個人資料被濫用或外洩的風險。私隱專員欣悉眾安銀行已經因應視察小組在示範期間即場表達的關注，與資訊科技部門檢視有關系統的設定，避免有員工可以不必要地逾時查閱客戶的個人資料。

(4) 集中管理內部政策及指引

39. 有效的內部溝通是個人資料私隱管理系統賴以成功的因素之一。機構應採取所有切實可行的步驟，以清晰及易於理解的方法告知員工機構的個人資料政策及實務指引，並讓員工容易獲取相關資訊。
40. 視察小組在眾安銀行示範系統操作及與負責管理客戶個人資料系統的人員面談期間，得悉眾安銀行有關僱員行為守則、資料分類、資料保安及事故報告等指引及手冊均由各個部門個別彙集並存放於其共用資料夾。個別部門的全職員工可以透過眾安銀行內聯網瀏覽有關指引及手冊，不過有關頁面並未完全開放予眾安銀行所有部門。有個別員工在面談時向視察小組表示不清楚如何取得眾安銀行有關指引及手冊的文本。

¹⁰ 眾安銀行在授予個別員工任何存取權限前，須由所屬部門主管提交申請以取得書面批准。在員工調職時，部門主管亦須及時檢視及更新存取權限。

41. 私隱專員認為眾安銀行應該讓所有員工容易獲取機構的個人資料政策及實務指引的資訊，並且應由保障資料主任在機構層面集中管理，確保有關指引及手冊於日後修訂或更新時能夠適時知會所有員工。私隱專員樂見眾安銀行已經因應視察小組在示範期間即場表達的關注採取跟進措施，於 2022 年 9 月 30 日起開放內聯網相關頁面予所有員工，並於同日發出內部電郵通知所有員工，以便他們了解和遵從眾安銀行有關個人資料政策及實務指引。

(5) 持續定期檢視個人資料系統

42. 私隱專員留意到，眾安銀行委派的特定部門會定期為不同部門進行內部審核，以識別各部門在風險管控方面的不足之處，並提出相應的改善建議。

43. 雖然眾安銀行在視察前未曾單獨審核其個人資料系統，但私隱專員從眾安銀行提交兩份分別於 2021 年 12 月及 2022 年 1 月完成的內部審核報告中得悉，眾安銀行在處理客戶個人資料方面有以下不足之處：

- (i) 部分管理員帳戶採用弱密碼；
- (ii) 未有適時移除可查閱客戶信貸資料的離職員工帳戶；
- (iii) 未曾檢視辦公範圍的實體保安措施；
- (iv) 關於管理端點及流動裝置的政策未有涵蓋棄置端點／儲存裝置，以及註冊／註銷自攜裝置的程序；及
- (v) 聘請第三方或外判服務前未有依從內部政策訂明的程序。

44. 儘管如此，私隱專員樂見眾安銀行已經落實審核報告內的建議，以改善上述不足之處。

45. 作為擁有數量龐大的客戶個人資料系統的資料使用者，私隱專員鼓勵眾安銀行持續定期檢視其個人資料系統（包括相關的政策、指引及程序）是否符合行業良好行事方式或作業指引，以減低日常營運中系統所面對的風險。

總結

46. 視察結果顯示，眾安銀行在處理客戶個人資料上大致符合《私隱條例》中附表 1 保障資料原則的規定。私隱專員欣悉眾安銀行建立了個人資料私隱管理系統並委任專職的保障資料主任，有系統並負責任地建立一套遵從《私隱條例》規定的制度，循規地管理客戶的個人資料。私隱專員同時建議眾安銀行加強對資料處理者的管理、提升資料遺失防護系統的監察能力、限制員工查閱客戶個人資料的時間、集中管理內部政策及指引，並持續定期檢視其個人資料系統。

第 IV 部 – 建議

47. 私隱專員希望透過本視察報告，提醒日常需要處理大量客戶個人資料的機構加強措施確保數據安全，包括：-
- (i) **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，並建立個人資料庫存。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。
 - (ii) **委任專責人員作為保障資料主任**：機構應委任專責人員作為保障資料主任，明確制訂保障資料主任的角色及職責，包括監察機構遵從《私隱條例》的情況，並向高級管理層匯報，以及把員工提出的保障資料事宜和涉及客戶資料外洩事故的經驗及教訓納入機構的培訓材料之中。
 - (iii) **制訂全面的系統保安政策及程序**：在「數據猶如資產」的世代，企業及機構須加強保障客戶個人資料私隱，減低個人資料外洩或遭濫用的風險。機構應制訂符合國際準則的系統保安政策及程序，定期進行適時的保安風險評估，並持續定期審視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等威脅。
 - (iv) **按員工職能存取客戶資料**：機構應採用「最小權限」的原則，授予員工盡可能小的存取權限以完成工作，並將適當的角色分配給員工（即採取以角色為本的存取管控，包括限制存取資料的數量和時間）。機構亦應定期覆檢員工的存取權限（例如當員工離職或重新調配職位時更改存取權限），適時刪除不必要的帳戶和存取權限，避免客戶的個人資料被外洩、用於「起底」或其他不法用途。

- (v) **審慎聘任及管理資料處理者**：機構在聘請資料處理者處理個人資料之前應進行私隱影響評估¹¹，以避免引入對個人資料私隱不利的措施。當委任資料處理者後，機構應持續監察資料處理者處理個人資料的方式是否符合合約訂定的規範及標準，並在出現未能預見的私隱風險時，與資料處理者制訂應對方案。

—完—

¹¹ www.pcpd.org.hk/tc_chi/resources_centre/publications/files/InfoLeaflet_PIA_CHI_web.pdf

零售客戶使用眾安銀行流動應用程式開立戶口的流程

