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

2018 年抽查報告：
資料使用者實施
私隱管理系統的情況

2019 年 3月5日

目錄

I. 摘要 **2**

II. 抽查行動的目的 **3**

III. 抽查的方法 **4**

IV. 全球抽查行動 **5**

V. 公署抽查結果 **6**

VI. 結論及建議 **12**

附錄 **A**–抽查行動的問卷 **15**
附錄 **B** – 抽查行動的評分準則 **19**
附錄 **C** – 抽查行動統計數據 **22**

I. 摘要

在2018年，香港個人資料私隱專員公署（「**公署**」）連續第六年參與「全球私隱執法機關網絡」（Global Privacy Enforcement Network）的抽查行動。

2. 本年抽查行動的主題是「**私隱問責制的實施**」。18個來自世界各地的私隱執法機關（包括公署）參與了抽查行動。參與的私隱執法機關可挑選其認為合適的企業或機構進行抽查，根據參加機構對有關私隱問責制主要元素的提問所作出的回應，評估機構的私隱實務。

3. 抽查行動在2018年10月至11月期間進行。公署邀請了44間不同行業的機構參加抽查行動，當中26間機構（「**參加機構**」）回覆表示願意參加是次抽查行動。

4. 公署在抽查行動所得的主要觀察結果綜合如下：—

- 所有參加機構均有制訂符合法律要求的內部個人資料私隱政策，並將有關政策納入機構日常運作中
- 儘管並非《個人資料(私隱)條例》（「**私隱條例**」）的規定，大部份參加機構已委任高級人員負責私隱管治和管理的事宜
- 大部份機構均向員工提供全面的保障個人資料培訓
- 所有參加機構均將其私隱政策上載於機構的網站中，並易於查閱
- 幾乎所有參加機構有書面制訂資料外洩事故的處理程序
- 只有部份參加機構有就發生資料外洩事故時通知受影響的資料當事人及向監管機構匯報方面制訂相關程序
- 絕大部份參加機構在計劃推出新項目、產品或服務前，會進行私隱影響評估，並有書面紀錄
- 部份參加機構備有完整的個人資料庫存
- 部份參加機構有就轉移個人資料給第三方備存完整紀錄

5. 問責制已成為全球公認的資料保障的關鍵原則，並已被納入許多法律、法規及行業指引。機構所持有的個人資料是屬於資料當事人的，他

們把其個人資料交予所信任的資料使用者。因此，資料使用者在保障個人資料方面除了有法律上的責任外，亦有倫理道德上的責任。機構可從個人資料獲取利益，在營運上便不應抱有只依從最低監管要求的想法，而應恪守更高的道德標準，以符合客戶的期望。除了合規外，資料使用者亦應以尊重（respectful）、互惠（beneficial）和公平（fair）三大數據倫理道德價值處理個人資料。

II. 抽查行動的目的

6. 「全球私隱執法機關網絡」是按經濟合作與發展組織的建議於 2010 年成立，旨在促進私隱規管者在全球化環境下的跨境合作。抽查行動的目的是：—

- 加強公眾及商業機構對保障私隱的權利和責任的認識
- 找出值得關注的私隱議題
- 鼓勵業界遵從私隱法規

7. 公署自 2014 年起提倡各機構建立自己的私隱管理系統，由最高管理層（例如董事會）做起，將個人資料保障視為其企業管治責任，並將之納入處理業務中不可或缺的一環，由上而下貫徹地在機構中執行有關保障個人資料的政策，以顯示問責原則。這不但可加強客戶的信任，更可從而提升其商譽及加強競爭優勢。機構建立全面私隱管理系統已成為世界的大趨勢，而歐洲聯盟於 2018 年 5 月 25 日生效的《通用數據保障條例》亦已明確納入問責原則，資料控制者須展示其遵從處理個人資料的原則（《通用數據保障條例》第 5（2）條）。

8. 2018 年的抽查行動旨在透過分析機構實施私隱管理系統的情況，以評估機構在保障個人資料方面達致問責的程度，及他們在業務過程中管理私隱風險的能力。此外，公署亦希望了解機構在推行私隱管理系統時所遇到的實際困難，以便公署研究日後如何有效地協助機構推行私隱管理系統。

9. 公署邀請本港 44 間不同行業的機構（包括保險、金融、電訊、公用事業及交通運輸）參加是次抽查行動，而。挑選這些機構進行抽查是基於其規模及持有的個人資料數量龐大。公署最後收到 26 間機構提供回應/部份回應。

III. 抽查的方法

10. 公署是次抽查行動以下述方式進行：

- 瀏覽參加機構的網站，找出其私隱政策的位置
- 按一套預設問題向機構作出查詢（見下文第11段）

11. 所有參與的私隱執法機關均透過由全球私隱執法機關網絡制定的預設問題來進行評估，並可按需要提出其他問題。該些預設問題如下：—

- 機構有將符合法律要求的內部個人資料私隱政策納入機構日常運作中
- 機構有委任具備相關知識的高級人員負責私隱管治和管理的事宜
- 機構有向員工提供有關個人資料保障的培訓，並確保員工了解機構的私隱政策、處理個人資料的程序及最佳行事方式
- 機構有監督保障個人資料方面的表現標準（例如進行自我評估、審核私隱管理系統及與個人資料有關的投訴、查詢及事故）
- 機構有積極的政策說明如何處理個人資料，並易於讓客戶和公眾查閱得到相關資訊
- 機構有書面訂定資料外洩事故的處理程序
- 機構有就發生資料外洩事故時通知受影響的資料當事人及向監管機構匯報事件制訂相關程序
- 機構有詳細紀錄所有的資料外洩事故
- 機構有就回應個人的訴求和投訴，以及外界（例如監管機構）的查詢，制訂相關政策和程序
- 機構有記錄所有新產品、服務、技術和業務模式有關的風險評估流程（例如證明他們已完成私隱影響評估的紀錄）
- 機構有就所持有的個人資料備有個人資料庫存

- 機構備有轉移個人資料（例如向第三方轉移資料）的紀錄

12. 私隱執法機關會根據全球私隱執法機關網絡提供的評分準則，對機構就上述各個問題的回應，從「非常好」、「令人滿意」、「差勁」及「未有述明」中剔選所屬的類別。

13. 全球私隱執法機關網絡為今次抽查行動而制定的問卷及評分準則分別載列於**附錄A**及**附錄B**。

14. 由於部分問題需要評估人員作主觀判斷，為確保評估的客觀性，參加機構的回應分由五名公署職員進行檢視和分析。在作出檢視和分析前，五名公署職員先進行討論及協調，以達致統一的評分標準。

15. 此外，公署亦向參加機構提出其他查詢，以讓公署研究如何有效地協助機構推行私隱管理系統。該些問題包括：—

- 機構在推行私隱問責制時所遇到的實際困難
- 機構在保障個人資料方面的良好行事方式
- 機構期望公署提供哪些協助/支援，以協助機構推行私隱管理系統

IV. 全球抽查行動

16. 全球 18 個私隱執法機關（包括公署）共聯絡了356間不同行業的機構參加抽查行動，包括（但不限於）教育、電子商務、金融及保險、健康護理、法律、市場推廣、公共事業（包括中央及地區政府）、零售、電訊、旅遊、交通及康樂。全球抽查行動所得的主要結果如下：—

- 接近75%的機構有委任人員或團隊專責私隱管治和管理的事宜，以確保機構符合相關資料保障的法規
- 機構普遍有向員工提供良好的資料保障方面的培訓，但通常忽略了向員工舉辦重溫課程

- 在監控機構內部的資料保障表現方面，約25%的機構並無相關自我評估及/或內部審核的計劃
- 有相關自我評估及/或內部審核的計劃的機構普遍都能舉出有關的良好行事方式，例如會每年進行審核及/或定期進行自我評估
- 過半數機構表示有就處理資料外洩事故的制訂書面程序，並會紀錄機構發生的所有資料外洩事故。然而，有些機構表示並無制定任何既定程序處理資料外洩事故

V. 公署抽查結果

17. 機構處理個人資料及保障個人資料的政策和措施可能不斷更新或改變。因此，本報告的結果只能反映2018年10月至11月抽查行動期間的狀況。

18. 此外，抽查行動只屬研究性質，而非循規審查或正式調查。因此，公署不適宜透露個別機構的具體抽查結果。下述的抽查結果是根據參加機構所作出的回應而得出的整體性結果。

19. 公署的抽查結果大致與上述的全球抽查結果一致。公署在抽查行動所得的主要觀察結果會以下述標題論述：—

- 資料保障的政策、程序及管治
- 資料保障的監控、培訓及意識
- 透明度
- 資料外洩事故的回應及管理
- 紀錄風險評估、紀錄及資料流通

資料保障的政策、程序及管治

20. 所有參加機構（100%）均表示有制訂符合法律要求的內部個人資料私隱政策，並將有關政策納入機構日常運作中。

21. 儘管《私隱條例》沒有規定資料使用者必須委任保障資料主任一職，但大部份參加機構（19 間，73.08%）均有委任具備相關知識的高級人員負責私隱管治和管理的事宜，當中有機構更成立由各部門代表組成的委員會，負責私隱治理和管理的事宜。5 間參加機構（19.23%）有委任人員出任負責私隱治理和管理的事宜，但並非由高級人員出任。其餘 2 間參加機構（7.69%）表示有職員負責私隱治理和管理的事宜，但並無述明是否由高級人員負責處理。

22. 機構在上述範疇的表現令人鼓舞，亦反映了他們深明保障個人資料是業務中不可或缺的一環，願意投放資源及人手處理保障個人資料的事宜。

資料保障的監控、培訓及意識

23. 所有參加機構均表示明白向員工提供有關保障個人資料培訓的重要性。17 間參加機構（65.38%）有向員工提供全面的保障個人資料培訓，包括安排新入職員工接受相關培訓、定期為所有員工舉辦重溫課程，及參加由公署舉辦的保障個人資料專業研習班等，當中有 1 間機構更要求員工須定期進行及通過有關《私隱條例》的考核。另外 8 間參加機構（30.77%）雖然有向員工提供相關培訓，但略欠全面（例如沒有定期向所有員工舉辦重溫課程）。

24. 不過，有 1 間參加機構（3.85%）只要求員工簽署表示明白機構的私隱政策，但並無向員工提供任何相關培訓。公署認為有關做法並不理想。

25. 在機構的資料保障措施進行自我評估或審核方面，半數參加機構（13 間，50%）有定期就個人資料私隱保障符規方面進行審核，當中有機構委託獨立的第三方進行有關審核；11 間參加機構（42.31%）則會不定期就機構在個人資料私隱保障符規方面進行審核。其餘 2 間參加機構（7.69%）則沒有述明。

透明度

26. 所有參加機構（100%）都備有私隱政策，並在機構的網站中容易查閱得到。有待改善的地方是其中 1 間參加機構的私隱政策只備有中文版本。

27. 23 間參加機構（88.46%）在其私隱政策中有述明他們設有保障資料主任一職，並提供保障資料主任的聯絡方法（例如地址及電郵地址），但其餘 3 間參加機構（11.54%）則並無述明是否設有保障資料主任一職。在該 3 間機構中：—

- 其中 1 間只表示與私隱有關的事宜可聯絡公司經理
- 另外 2 間則表示有關查閱或改正個人資料可聯絡客戶服務部

資料外洩事故的回應及管理

28. 近期在香港發生的多宗個人資料外洩事故，引起公眾關注資料使用者是否能妥善保障他們所持有的個人資料。資料使用者有一套完善的機制及程序回應資料外洩事故，可幫助機構有效地處理事故，減低對資料當事人及機構聲譽方面造成的損害。

29. 除 1 間參加機構（3.85%）沒有述明是否有書面制訂相關程序外，其餘 25 間參加機構（96.15%）均表示有根據公署發出的《資料外洩事故的處理及通報指引》制訂書面的資料外洩事故的處理程序。這顯示機構明白不可輕視資料外洩事故可能引致的後果。

30. 就機構是否有制訂程序，在發生資料外洩事故時通知受影響的資料當事人及在有需要時向監管機構匯報方面，抽查結果顯示情況有欠理想：—

- 只有 16 間參加機構（61.54%）有制訂相關程序
- 4 間參加機構（15.38%）沒有制訂相關程序，而只會在發生資料外洩事故後才決定如何處理

- 6 間參加機構（23.08%）沒有述明是否有制訂相關程序

31. 此外，24 間參加機構（92.31%）表示備有紀錄簿，詳細紀錄所有資料外洩事故。其餘 2 間參加機構（7.69%）則沒有述明是否備有相關紀錄簿。

32. 就回應個人的訴求和投訴，以及外界（例如監管機構）的查詢方面，24間參加機構（92.31%）有制訂相關政策和程序，當中有些機構設立特別團隊專責處理有關事宜。有1間參加機構（3.85%）雖然有既定程序處理客戶的一般要求，但在回應監管機構的查詢或所轉介的投訴個案方面卻沒有制訂任何政策和程序。其餘1間參加機構則沒有述明是否有制訂相關政策和程序。

<u>紀錄風險評估、紀錄及資料流通</u>

33. 只在發生違規事件後才作出被動的補救行動並非對保障個人資料負責任的做法。機構在推出新項目、產品或服務前進行私隱影響評估，並對所持有的個人資料進行紀錄，能協助機構及早發現及評估潛在的私隱風險，並作出改善，以防患於未然。

34. 23間參加機構（88.46%）在計劃推出新產品、服務、科技及業務模式前，會進行私隱影響評估，以了解潛在的私隱風險，並有書面紀錄；另外2間參加機構（7.69%）則沒有就有關評估作書面紀錄；其餘1間機構（3.85%）則沒有述明。這反映了機構明白防患於未然的重要性。

35. 只有少部份參加機構（7間，26.92%）備有完整的個人資料庫存，紀錄所持有的個人資料的類別、儲存的地點、保留期間、使用及所採取的保安措施。大部份機構（14間，53.85%）所備有的個人資料庫存略欠完整，當中只紀錄客戶的個人資料，但未有包括員工的個人資料。另外4間參加機構（15.38%）只對個別部門/項目所持有的個人資料備有個人資料庫存，有1間參加機構（3.85%）表明並無就其所有持有的個人資料備有個人資料庫存。其餘1間參加機構則沒有述明是否備有個人資料庫存。這顯示了機構對於所持有的個人資料缺乏充份的了解。

36. 機構在處理個人資料時，可能會將個人資料轉移給第三方。紀錄個人資料的流向有助機構了解個人資料的來源及被轉移的詳情，以便於日後翻查。抽查結果顯示參加機構在這方面的表現欠理想，僅7間參加機構（26.92%）有就轉移個人資料給第三方備存完整紀錄；另外7間參加機構雖然有備存相關紀錄，但內容並不詳細；6間參加機構（23.08%）更沒有在這方面備存任何紀錄；其餘6間參加機構則沒有述明。

37. 有關抽查行動的統計數據，詳見**附錄 C**。

38. 就公署向參加機構提出的其他問題（見上文第 15 段），所得的回應綜合如下：—

<u>在推行私隱問責制時所遇到的實際困難</u>

39. 半數參加機構表示公署發出的《私隱管理系統—最佳行事方式指引》，有效協助他們在機構內推行私隱管理系統，故在推行過程中並沒有遇到重大的困難。

40. 其他參加機構所遇到的實際困難歸納如下：—

- 缺乏足夠的資源，包括財政、專才及相關工具
- 部份員工的工作並不涉及個人資料處理，難以提高他們保障個人資料私隱的意識
- 相對其他法規（例如打擊洗黑錢及貪污等）對有關違規行為施加嚴重的罰則，有些員工認為違反《私隱條例》的後果不嚴重，故將保障個人資料放在次要位置
- 機構內各部門有自己的需要及做法，難以整合一個通用的處理個人資料的做法。此外，在大規模機構內就處理個人資料的流程作紀錄亦難以實行
- 大規模機構使用多個複雜的處理個人資料系統，難以擬備一個完整的個人資料庫存

在保障個人資料方面的良好行事方式

41. 部份參加機構亦向公署分享他們在保障個人資料方面有以下的良好行事方式：—

私隱政策方面

- 清晰的個人資料管治框架，述明不同部門的角色及職責。此外，於機構內聯網上載保障個人資料手冊及指引，讓員工知悉最新的個人資料法規
- 採納收集最少量個人資料的原則
- 機構的董事局公開表示支持及指令保障個人資料是機構內其中一個最重要的任務

培訓及教育方面

- 機構的律師親自向員工講解《私隱條例》的規定，以加強員工在使用個人資料方面的意識
- 舉辦具互動性的培訓課程，提高機構內保障個人資料的文化意識
- 測試員工在接受培訓後是否能應用有關知識
- 聘請具有保障個人資料方面的知識及經驗的人士

資料外洩事故處理方面

- 設立資料外洩事故的匯報電子平台，除了方便員工匯報任何潛在的私隱風險事故，機構亦可以恰當地追蹤及監控事故發展

溝通方面

- 推薦不同職級的員工作為資料保障聯繫人
- 每季舉行一次私隱會議，跟進、解決及管理所有與私隱有關的問題
- 保障資料主任領導由不同部門的代表組成的工作小組。工作小組定期舉行會議商討與私隱有關的問題，並分享良好的行事方式。有事故發生時，跟進的進度及結果會向最高管理層匯報

持續評估及修訂方面

- 每年審核機構的政策是否符合《私隱條例》規定，並視乎風險及影響的程序，審核結果會向最高管理層匯報
- 檢視私隱影響評估報告內所設的問題是否全面，而私隱影響評估報告須交由相關委員會批核

期望公署提供哪些協助或支援，以協助機構推行私隱管理系統

42. 參加機構亦希望公署可提供下述的協助或支援，以協助他們推行私隱管理系統：—

- 舉辦培訓講座，包括為不同行業度身訂造培訓課程、定期的個案分享
- 提供多些私隱管理系統的樣本以供參考
- 以機構管理層為對象的培訓講座
- 定期發出通訊，分享機構在處理個人資料方面常見的錯誤
- 繼續出版各類指引及良好行事方式，以指導不同行業應如何處理個人資料
- 認證及公開機構良好的保障個人資料私隱做法，讓其他機構借鏡

43. 公署會積極考慮機構的上述建議。事實上，公署一直發出/修訂各類指引，務求讓機構在處理個人資料方面能與時並進。此外，公署成立的保障資料主任聯會每月會發出通訊，述明公署及與私隱事宜有關的最新消息。未來，公署將繼續推出更多有關私隱管理系統的講座及專業研習班，協助機構擬備私隱管理系統操作手冊，建立全面的私隱管理系統。

VI. 結論及建議

44. 與歐洲聯盟的《通用數據保障條例》不同，香港的《私隱條例》沒有明確列明問責制及相關的私隱管理措施。公署倡議採納私隱管理系統以顯示問責制。委任保障資料主任及進行私隱影響評估是為達致問責制而建議的良好行事方式。

45. 值得注意的是，是次的抽查結果顯示，對比其他一些將個人資料私隱問責原則明確納入法規的國家，香港的機構在透過推行自願性質的私隱管理系統的表現並不遜色，這反映了香港的機構重視個人資料保障，並願意投放資源以維護個人資料私隱權益。儘管如此，公署對機構在推行私隱管理系統方面有以下建議：

- **提供足夠的保障資料培訓**：隨著企業對數碼化的使用，機構內的大部份員工均有機會在日常工作中接觸同事或客戶的個人資料，故機構必須確保員工了解《私隱條例》的規定及有遵守機構有關保障個人資料的政策。在這方面，機構應提供足夠及定期的培訓，除了向新入職員工講解機構保障個人資料的政策及解釋《私隱條例》的規定外，亦應定期舉辦相關培訓課程。如機構處理個人資料的政策或《私隱條例》有修訂，機構應立即通知員工

- **定期進行審核**：定期由專責人員/獨立的第三方審核機構處理個人資料的做法是否符合《私隱條例》的規定，以及是否有優化的空間

- **資料外洩事故的處理**：制訂書面程序，述明發生資料外洩事故時通知受影響的個人及向監管機構匯報所需考慮的因素、機制及行事方式。雖然機構有制訂私隱政策以符合法例的規定，但由於資料外洩事故通報並非法律的規定，故機構不會將焦點放在制訂處理資料外洩事故的程序。然而，網絡攻擊是非常切身的問題，機構沒有制定資料外洩事故通報的程序所帶來的風險可以非常嚴重

- **完整的個人資料庫存**：機構內有多個載有個人資料的系統，令機構更有需要擬備個人資料庫存。機構內各部門可擬備部門所屬的個人資料庫存，就轄下載有個人資料的系統作紀錄。完整的個人資料庫存絕對有助機構充份了解所持有的個人資料，對於機構在個人資料的生命週期中處理個人資料時有莫大幫助

- **轉移個人資料的紀錄**：對所轉移的個人資料備存紀錄，日後如有需要，便可迅速地翻查有關資料

46. 機構最佳的行事方式是建立及全面執行私隱管理系統。數據管治應涵蓋整體業務常規、操作程序、產品和服務設計、實體建築，以至網絡基礎設施。在策略層面，機構可採用私隱管理系統作為框架，輔以行之有效的檢討及監察程序，建立健全的私隱保障基建，藉以配合機構遵從《私隱條例》的規定，與顧客及員工共享公平、尊重和互惠。

附錄A — 抽查行動的問卷

Statement	Assessment			Evidence
	Achieved	Partially achieved	Not Achieved	*Please describe how each area has been achieved in practice, and provide evidence where possible.*
Your organisation has an internal data privacy (consistent with legal requirements) policy which has been embedded into everyday practices				
Your organisation has allocated someone at a sufficiently senior level to be responsible for privacy governance and management				
Your organisation ensures staff are given training regarding the protection of				

personal information, and you inform them of organisational privacy policies, procedures and best practices				
Your organisations performance is monitored in relation to data protection standards (i.e by conducting self-assessments and/or audits of your privacy programme and in relation to complaints / enquiries / breaches)				
Your organisation actively maintains policies to explain how you handle personal data, and these easily accessible to customers and the general public				
Your organisation maintains a documented				

incident response procedure				
In the event of a breach, your organisation has a procedure in place to notify affected individuals and report the breach to the regulator where necessary				
Your organisation maintains an incident log detailing all breaches that occur				
Your organisation has policies and procedures in place to respond to requests and complaints from individuals, and other external enquiries (such as the regulator)				
Your organisation has documented processes in place to assess the risks associated with new products,				

services, technologies and business models (for instance, you conduct privacy impact assessments)				
Your organisation maintains an inventory of your personal data holdings				
Your organisation maintains an inventory of any data flows (for example, data transfers to third parties)				

附錄B — 抽查行動的評分準則

RATING CRITERIA

The below criteria is for consideration when rating each organisation's response to PEA's queries. These examples are for guidance only, and PEAs may choose to adopt their own grading criteria.

Very Good

The organisation demonstrated that they have implemented the essential elements of accountability into everyday business practices and policies (as broken down into common indicators).

Examples of good practice may include:

- The organisation maintains a data privacy framework (consistent with legal requirements) which has become embedded into everyday practices.
- A data protection officer / privacy officer has been appointed, and/or there is someone at a sufficiently senior level responsible for privacy governance and management.
- Regular data protection training is given to staff (this would include training for new starters and refresher training for current employees).
- The organisation conducts regular self-audits, and regularly reviews its performance in relation to data protection standards.
- The organisation demonstrated that they maintain a clear privacy policy, which is easily accessible to customers and the general public.
- The organisation demonstrated that they have a documented incident response procedure, and has steps in place to notify affected individuals and the regulator.
- The organisation maintains an incident log which is regularly kept up to date.
- The organisation has policies and procedures in place to respond to requests and complaints from individuals, and other external enquiries (such as the regulator).
- The organisation has a documented processes in place to assess the risks associated with new products, services, technologies and business models (for instance, it conducts privacy impact assessments for all new projects).
- The organisation maintains an inventory of the personal data held by them and records data flows.

Satisfactory

The organisation showed some evidence of having implemented the essential elements of accountability (as broken down into common indicators), into business policies and practices, but they are lacking in some aspects and require improvement.

Examples may include:

- The organisation is either in the process of implementing a data privacy framework (consistent with legal requirements) or they have a partial framework which they aim to implement into everyday practices.
- A data protection officer / privacy officer has been appointed, but there is nobody at a sufficiently senior level responsible for privacy governance and management.
- Some data protection training is given to staff, but the organisation may fail to give refresher training, or only provides training for some employees.
- The organisation shows evidence of having conducted self-audits and reviews its performance in relation to data protection standards, but reviews should be more thorough and/or held more regularly.
- The organisation demonstrated that they have a privacy policy, but this may not be easily accessible to the general public, lacking key principles of data protection, or outdated.
- The organisation has some measures in place to deal with privacy-related concern and queries, and their ability to appropriately deal with a data breach was satisfactory, but may lack some essential steps and requires improvement.
- The organisation indicated that they records incidents, but may fail to keep this up to date, or fail to have set processes in place.
- The organisation shows some understanding of the importance of assessing risks associated with new products, services, technologies and business model, but may not have a written process and requires improvement.
- The organisation has some understanding of the sort of data they hold, but fails to maintain an adequate inventory of the personal data held by them and/or record data flows.

Poor

The organisation was not able to show any understanding of the practices which form the essential elements of accountability (as broken down into common indicators).

- The organisation demonstrates little to no understanding of privacy frameworks necessary in the everyday course of business.
- No data protection officer/privacy officer has been appointed.
- No data protection training is given to employees.
- The organisation does not monitor it performance by conducting reviews of its adherence to data protection standards.
- The organisation does not have a privacy policy.
- The organisation has no measures in place to deal with privacy related concerns or queries, and/or is unequipped to appropriately deal with a data breach.
- The organisation does not record or log incidents/breaches when they occur.
- The organisation demonstrates little to no understanding of the importance of assessing risks associated with new products, services, technologies and business model.
- The organisation has little to no understanding of the sort of data they hold, and fails to maintain an adequate inventory and/or record data flows.

附錄 C — 抽查行動統計數據

制訂內部個人資料私隱政策，並將有關政策納入機構日常運作中	數目	百分比
非常好	19	73.08%
令人滿意	7	26.92%
差勁	0	0%
未有述明	0	0%

委任有足夠高職級的人員負責私隱管治和管理	數目	百分比
非常好	19	73.08%
令人滿意	5	19.23%
差勁	0	0%
未有述明	2	7.69%

向員工提供有關個人資料保障的培訓，並確保員工了解機構私隱政策、處理個人資料的程序及最佳行事方式	數目	百分比
非常好	17	65.38%
令人滿意	8	30.77%
差勁	1	3.85%
未有述明	0	0%

監督保障個人資料方面的表現標準（透過自我評估、審核私隱管理系統及與個人資料有關的投訴、查詢及事故）	數目	百分比
非常好	13	50.00%
令人滿意	11	42.31%
差勁	2	7.69%
未有述明	0	0%

積極的政策說明如何處理個人資料，並易於讓客戶和公眾查閱得到相關資訊	數目	百分比
非常好	25	96.15%
令人滿意	1	3.85%
差勁	0	0%
未有述明	0	0%

書面訂定資料外洩事故的處理程序	數目	百分比
非常好	24	92.31%
令人滿意	1	3.85%
差勁	0	0%
未有述明	1	3.85%

制訂與發生資料外洩事故時通知受影響的個人及在有需要時向監管機構匯報事件的程序	數目	百分比
非常好	12	46.15%
令人滿意	4	15.38%
差勁	4	15.38%
未有述明	6	23.08%

詳細紀錄所有的資料外洩事故	數目	百分比
非常好	23	88.46%
令人滿意	1	3.85%
差勁	0	0%
未有述明	2	7.69%

就回應個人的訴求和投訴，以及外界（例如監管機構）的查詢，制訂相關政策和程序	數目	百分比
非常好	19	73.08%
令人滿意	5	19.23%
差勁	1	3.85%
未有述明	1	3.85%

記錄所有新產品、服務、技術和業務模式有關的風險評估流程（例如證明他們已完成私隱影響評估的紀錄）	數目	百分比
非常好	16	61.54%
令人滿意	7	26.92%
差勁	2	7.69%
未有述明	1	3.85%

備有個人資料庫存	數目	百分比
非常好	7	26.92%
令人滿意	14	53.85%
差勁	4	15.38%
未有述明	1	3.85%

備有個人資料轉移（例如向第三方轉移資料）的紀錄	數目	百分比
非常好	7	26.92%
令人滿意	7	26.92%
差勁	6	23.08%
未有述明	6	23.08%