

視察報告

(根據《個人資料(私隱)條例》第 48(1)條發表)

環聯資訊有限公司 的個人資料系統

報告編號：R22 - 0684

發表日期：2022 年 12 月 20 日

環聯資訊有限公司
的個人資料系統

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
2022 年 12 月 20 日

目錄

摘要.....	1
第 I 部 – 背景	7
第 II 部 – 視察方法	13
第 III 部 – 環聯的個人信貸資料系統.....	15
第 IV 部 – 主要視察結果.....	18
第 V 部 – 建議.....	28

附錄 A：保障資料原則

附錄 B：個人信貸資料實務守則第 3.11 至 3.13 條

視察報告

(根據《個人資料(私隱)條例》第 48(1)條發表)

環聯資訊有限公司 的個人資料系統

摘要

背景

環聯資訊有限公司(環聯)是香港一間信貸資料機構,其全資附屬公司環聯信貸資料服務有限公司於 2022 年 11 月 28 日獲香港銀行公會、香港持牌放債人公會及香港有限制牌照銀行及接受存款公司公會委任為「多家個人信貸資料服務機構(Multiple Credit Reference Agencies)模式」下的其中一間信貸資料機構。根據環聯提供的資料,其個人信貸資料庫載有超過 560 萬名消費者的個人資料和信貸紀錄。個人信貸資料屬性質敏感的個人資料,任何不當或未獲授權的查閱或存取相關的個人信貸資料可導致信貸提供者及資料當事人嚴重的財務損失。因此,環聯作為營運個人信貸資料庫的機構,除了向信貸提供者及資料當事人提供優質及準確的個人信貸資料及服務外,亦應根據《個人資料(私隱)條例》(第 486 章)(《私隱條例》)及《個人信貸資料實務守則》(《實務守則》)的規定採取適當的保安措施,持續監察及檢討資料庫的使用情況,藉以偵察及調查任何不尋常或不合常規的查閱或使用個人信貸資料的情況,以符合公眾期望,保障其持有的個人資料系統免受未經准許的或意外的查閱、處理、刪除、喪失或使用所影響。

個人資料私隱專員公署（私隱專員公署）在 2010 年曾根據《私隱條例》第 36 條以視察方式，視察環聯的個人資料系統，檢視環聯有否遵守《私隱條例》下六項保障資料原則及《實務守則》，並提出加強循規的建議。

隨著時代變遷，數碼資訊科技急速發展，加上環聯的服務被更廣泛地使用，社會對環聯的個人信貸資料庫的保安期望已大大提升。在這情況下，個人資料私隱專員（專員）認為有必要重新檢視環聯對其個人信貸資料系統的存取控制，並為監察可疑行為而採取的預防措施及審核程序。

專員遂依據《私隱條例》第 36 條的權力，對營運個人信貸資料庫的環聯進行視察（視察），審視其個人資料系統。由於本港現已引入多間個人信貸資料機構，專員期望在本視察中所得出的結果及建議，亦可讓其他個人信貸資料機構作為參考，協助他們遵從《私隱條例》及《實務守則》的規定。

主要視察結果

良好行事方式

在視察期間，專員欣悉環聯重視保障其持有的個人資料，在下述範疇樹立了良好的行事常規：

- (i) 環聯大致上把保障私隱納入其企業管治之中，並已落實建立個人資料私隱管理系統及委任專責人員作為保障資料主任。（第35及38段）
- (ii) 環聯在其個人信貸資料系統的營運過程及常規中採取了足夠的保障個人資料措施，其作業模式亦符合國際資訊科技保安標準。（第42至45段）
- (iii) 環聯就其個人信貸資料系統的內部存取控制，採取了良好的行事方式，包括：按職能設立存取權限、定期檢視存取權限、實施良好的密碼管

理，以及備存詳盡的員工活動日誌紀錄。同時，環聯透過合約規範方法對信貸提供者採取了適當的系統存取控制措施，配以恆常偵測及監察異常登入系統的情況，以減低未經准許存取個人信貸資料的風險。（第47至49段）

- (iv) 環聯對員工有多項提升個人資料私隱意識的政策及措施，致力保障個人資料私隱。（第52至53段）
- (v) 環聯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。（第57段）
- (vi) 環聯因應專員的建議，於2022年5月推行免費「信貸提示服務」，當訂閱「信貸提示服務」人士的信貸報告出現重要變動，環聯會透過電郵通知該人士，讓該人士知悉其信貸報告的變動，並可以預早作出防範或跟進。（第60至61段）
- (vii) 環聯亦應專員的建議，推出一項服務，讓被「起底」或懷疑被「起底」的人士，可在其信貸報告中加入備註，讓使用環聯個人信貸資料服務的信貸提供者（即銀行或財務機構）查閱該名人士的信貸報告時得悉此事，在審核該人士的信貸申請時可作參考。（第62段）

改善範疇

- (i) 專員建議環聯應更新相關的內部政策及程序，更具體地訂明保障資料主任的職責及角色，並安排他可以直接向最高管理層匯報。（第38段）
- (ii) 專員建議環聯就其全球政策制訂適用於香港公司的內部政策及標準，向個人信貸資料系統的管理人員及使用者在資料的保存、使用及保安等方

面提供更具針對性的指引。環聯亦應定期檢視其本地政策是否緊貼《私隱條例》的修訂，例如應該因應《私隱條例》於 2021 年 10 月生效有關「起底」的修訂條文，對有關政策進行修訂或更新。專員得悉環聯在視察小組的實地視察工作完成後，承諾會制訂適用於香港的內部政策及標準。（第39至41段）

- (iii) 專員建議環聯應就內部系統的日誌紀錄的管理方式訂定統一標準，該標準應訂明日誌紀錄所包含的資料類別，查核的權限、方法及頻率，及在偵測到可疑情況時的跟進方案等。此外，環聯亦應考慮配置電子方式協助有關查核，增加查核的準確性。環聯表示因應專員的建議，現正改良內部查核系統日誌紀錄的方法及頻率，並考慮採用電子方式協助有關查核以提升準確性。（第50段）
- (iv) 專員建議環聯修訂處理信貸提供者的懷疑異常查閱情況的政策，詳細述明當遇上有關情況時的調查及匯報程序，並設定一個比原有政策（即兩個月內）更短的通報時限，盡快就信貸提供者的懷疑異常查閱情況通知專員。（第51段）
- (v) 專員建議環聯應在與資料處理者簽訂的合約加入資料外洩的處理程序，好能讓雙方在資料外洩事件發生時，作出迅速的應變及補救措施。環聯亦應在聘請資料處理者處理個人資料之前對資料處理者的行事方式或程序進行私隱影響評估，以分析涉及的資料處理步驟，評估有關步驟所涉及的私隱風險，以便引入避免或減低對個人資料私隱產生不利影響的措施。而在委任資料處理者之後，應定期審視資料處理者處理個人資料的方式是否符合雙方訂定的標準，並在出現未能預見的私隱風險時，與資料處理者訂定應對方案。環聯在視察小組的實地視察工作完成後，於 2022年3月落實上述有關進行私隱影響評估的建議。（第57至58段）

總結

視察結果顯示，環聯採取了良好的行事常規，其個人信貸資料系統的保安措施符合國際標準。專員認為環聯在保障其持有的個人資料方面，符合《私隱條例》中附表1的保障資料第4原則有關個人資料的保安的要求。專員亦樂見環聯已經就視察小組的意見建立個人資料私隱管理系統並委任保障資料主任，有系統地建立一套遵從《私隱條例》規定的制度，循規地持有、處理及使用個人資料。雖然如此，根據本視察的觀察所得，專員建議環聯就其全球政策制訂適用於香港公司的內部政策及標準、更具體地訂明保障資料主任的職責及角色、就內部系統的日誌紀錄的管理方式訂定統一標準、修訂處理信貸提供者的懷疑異常查閱情況的政策，並定期對資料處理者處理個人資料的做法進行適時的檢視。

建議

專員希望透過本視察報告，向日常需要處理大量客戶個人資料的機構作出下述建議：

- (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：** 機構應明確制訂保障資料主任的角色及職責，包括監察遵從《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中。

- (iii) **制訂地區性政策：** 跨國企業在保障個人資料方面制訂全球通用的政策（包括保障個人資料及資訊保安方面的政策及規定）時，亦應考慮不同地區的法規而制訂更具體的地區性政策。
- (iv) **履行企業社會責任：** 公眾對機構的期望並不僅僅限於符合法律或監管要求。機構應履行社會責任，並實踐於日常營運中，致力加強保障客戶個人資料私隱。機構積極實踐社會責任可帶來雙贏的局面，為機構帶來更長遠的競爭優勢。
- (v) **監控個人資料的查閱情況：** 要有效地監察任何可疑的行為，機構應具備追查員工存取個人資料的機制，包括搜尋及更改紀錄的情況。機構應制訂政策進行及時及有效的持續監察，並訂明偵測到可疑情況時的跟進方案及匯報程序。
- (vi) **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。私隱影響評估有助機構分析相關的資料處理步驟，評估有關步驟所涉及的私隱風險，以便引入避免或減低對個人資料私隱不利影響的措施。而在委任資料處理者之後，機構應持續審視資料處理者處理個人資料的方式是否符合雙方訂定的標準，並在出現未能預見的私隱風險時，與資料處理者訂定應對方案。

第 I 部 – 背景

1. 根據香港法例第486章《個人資料（私隱）條例》（《私隱條例》）第8條，個人資料私隱專員（專員）須就遵守《私隱條例》條文作出監察及監管，以及促進對《私隱條例》的條文（尤其是各保障資料原則）的認識及理解以及遵守。就此，專員會派員巡視或檢視個別涉及大規模收集和使用個人資料的資料使用者所經營的場所或進行的活動，並會考慮發佈有關結果以推廣良好的行事方式。
2. 環聯資訊有限公司（環聯）是香港一間信貸資料機構¹，其全資附屬公司環聯信貸資料服務有限公司於2022年11月28日獲香港銀行公會、香港持牌放債人公會及香港有限牌照銀行及接受存款公司公會委任為「多家個人信貸資料服務機構（Multiple Credit Reference Agencies）模式」下的其中一間信貸資料機構。根據環聯提供的資料，其個人信貸資料庫載有超過 560 萬名消費者的個人資料及信貸紀錄。一般而言，如個人曾向信貸提供者²（例如銀行）申請信貸，他的個人信貸資料³便會儲存於環聯的個人信貸資料庫內。環聯收集借款人的信貸額、還款紀錄及欠債情況等個人信貸資料，然後向信貸提供者提供這些資料，以便信貸提供者決定是否向某貸款申請人提供貸款前，可評估申請人的財務狀況及信貸質

¹ 《個人信貸資料實務守則》（《實務守則》）第 1.11 條訂明，「信貸資料機構」是指信貸資料服務機構，即指從事提供個人信貸資料服務業務的任何資料使用者，不論該等業務是否該資料使用者的唯一或主要業務。根據《實務守則》第 1.9 條，「個人信貸資料服務」是指提供編製及/或處理個人資料（包括個人信貸評分）的服務，藉以向信貸提供者為個人信貸目的及執行任何與個人信貸交易直接有關的職能，向其發放該等資料或任何從中衍生的資料。

² 根據《實務守則》第 1.13 條，「信貸提供者」是指下述所指的任何人：

- (1) 《銀行業條例》（第 155 章）第 2 條所指的認可機構
- (2) 《銀行業條例》（第 155 章）第 2 條所指的認可機構的附屬公司
- (3) 根據《放債人條例》（第 163 章）獲發牌照的放債人
- (4) 其業務是為以租賃或分期付款方式取得貨物而提供資金的人（不論該人有否從事其他業務）

³ 根據《實務守則》第 1.8 條，「個人信貸資料」是指任何關於一名個人的個人資料，而該等資料是信貸提供者在提供個人信貸的過程中或與如此提供個人信貸有關而收集，或是由信貸資料機構在提供個人信貸資料服務的過程中或與提供此服務有關而收集或在其資料庫產生的任何個人資料（包括按揭宗數）。

素，減少借貸風險。個人信貸資料庫普遍存在於全球各地信貸市場。就個人而言，良好的信貸紀錄可為個人帶來更優惠的借貸條款，並提高成功獲取貸款的機會。

3. 個人信貸資料受到《私隱條例》所保障。專員亦依據《私隱條例》第12條發出了《個人信貸資料實務守則》（《實務守則》），就信貸資料機構及信貸提供者如何處理個人信貸資料提供實務指引。
4. 個人信貸資料屬性質敏感的個人資料，任何不當或未獲授權的查閱或存取相關的個人信貸資料可導致信貸提供者及資料當事人嚴重的財務損失。因此，環聯作為營運個人信貸資料庫的機構，除了向信貸提供者及資料當事人提供優質及準確的個人信貸資料及服務外，亦應根據《私隱條例》及《實務守則》的規定採取適當的保安措施，持續監察及檢討資料庫的使用情況，藉以偵察及調查任何不尋常或不合常規的查閱或使用個人信貸資料，以符合公眾期望，保障其持有的個人資料系統免受未經准許的或意外的查閱、處理、刪除、喪失或使用所影響。
5. 個人資料私隱專員公署（私隱專員公署）在2010年曾根據《私隱條例》第36條以視察方式，視察環聯的個人資料系統，檢視環聯有否遵守《私隱條例》下六項保障資料原則及《實務守則》，並提出加強循規的建議。
6. 隨著時代變遷，數碼資訊科技急速發展，加上環聯的服務被更廣泛地使用，社會對環聯的個人信貸資料庫的保安期望已大大提升。在這情況下，專員認為有必要重新檢視環聯對其個人信貸資料系統的存取控制，並為監察可疑行為而採取的預防措施及審核程序。
7. 《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，以協助專員作出關

於促進遵守《私隱條例》的建議。個人信貸資料屬性質敏感的個人資料，專員遂依據《私隱條例》第36條的權力，對營運個人信貸資料庫的環聯進行視察（視察），審視其個人資料系統。

8. 由於本港現已引入多間個人信貸資料機構，專員期望在本視察中所得出的結果及建議，亦可讓其他個人信貸資料機構作為參考，協助他們遵從《私隱條例》及《實務守則》的規定。

環聯的業務架構

9. 環聯是一間信貸資料機構，母公司為環聯集團，總部位於美國伊利諾伊州芝加哥。
10. 環聯向使用其個人信貸資料服務的信貸提供者，包括零售銀行、信用卡發行商、銀行附屬金融公司、放債人及其他金融機構提供編製及/或處理個人資料（包括個人信貸評分）的服務。環聯亦同時為消費者提供個人信貸資料服務，讓消費者可付費查閱自己的個人信貸資料。
11. 根據環聯提供的資料，他們的數據庫載有超過 3,500 萬名消費者信貸帳戶及超過 560 萬名資料當事人的個人資料。與此同時，超過160個信貸提供者訂閱了環聯的個人信貸資料服務。
12. 環聯在視察進行時聘有超過 140 名職員，而當中消費者互動部、會員支援服務部及資訊科技部的員工在日常運作中會查閱及處理個人信貸資料。

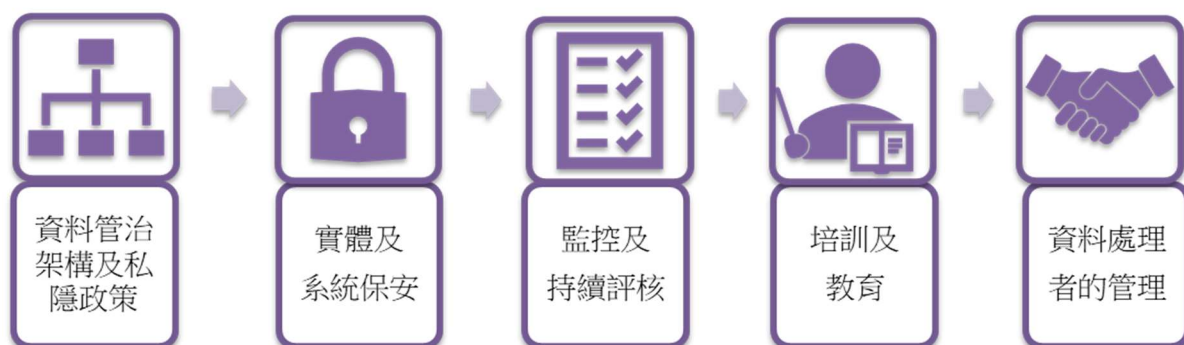
視察範圍

13. 環聯作為《私隱條例》下的資料使用者，在收集、保留、使用、保障個人信貸資料庫的個人資料方面，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。六項保障資料原則載列於**附錄A**。
14. 本視察聚焦環聯就控制存取個人信貸資料系統方面的保安措施。有關個人資料的保安，保障資料第 4(1) 原則訂明，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，尤其須考慮一

- (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。
15. 保障資料第 4(2) 原則訂明，如資料使用者聘用資料處理者⁴，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。
16. 《實務守則》第 3.11 條「信貸資料機構為資料保安及系統完整性所採取的措施」與本視察範圍有關，當中包括為準備提供信貸資料服務所採取的措施、日常運作所採取的措施及就信貸提供者的查閱等備存紀錄簿。相關守則的詳情載列於**附錄 B**。

⁴ 不論是在香港或香港以外聘用

17. 考慮到環聯處理個人資料的數量和性質，專員訂明對環聯的個人信貸資料系統方面的保安政策及行事方式的主要評估範疇如下：



第 II 部 – 視察方法

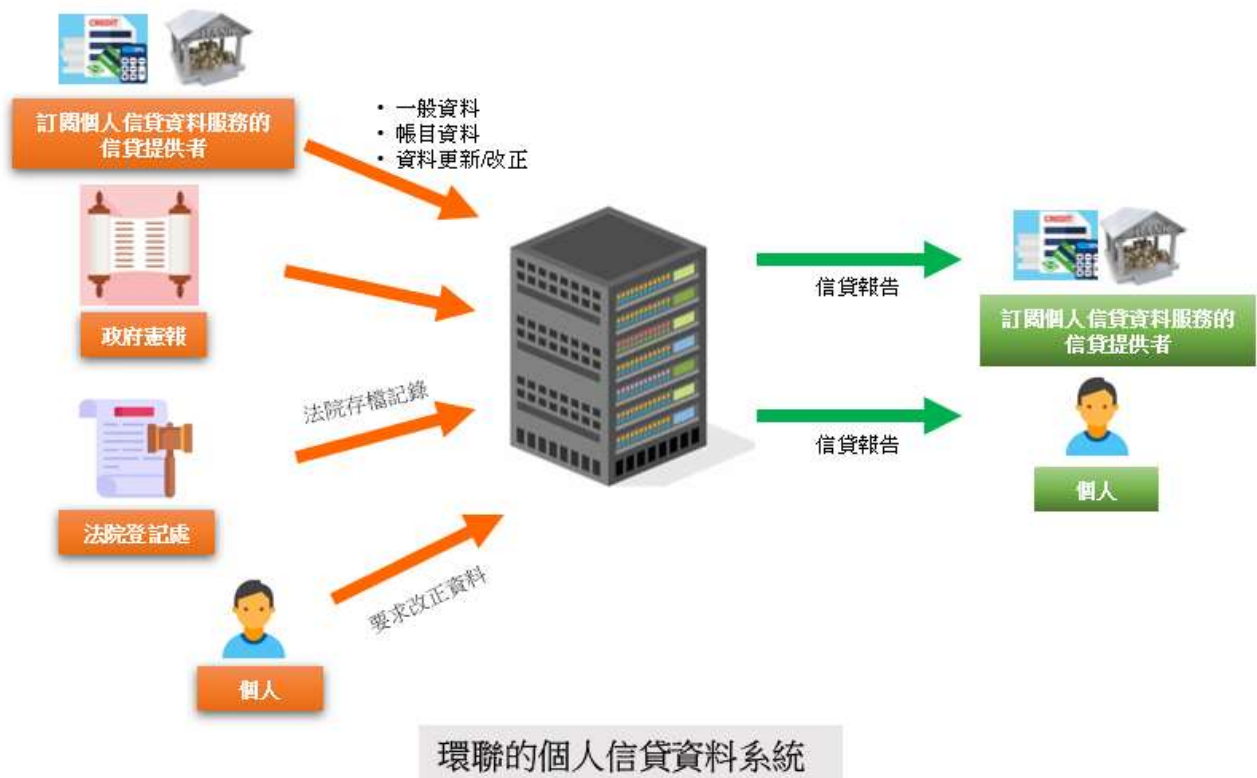
18. 專員致函環聯表達進行視察的意向後，視察小組⁵與環聯的香港區行政總裁所帶領的各部門代表舉行視察前會議。視察小組在會議上解釋視察目的，及了解環聯的個人信貸資料系統的運作及工作流程。
19. 為了視察環聯的個人信貸資料系統，以及員工及信貸提供者如何有效地遵從環聯的資料保安政策和行事方式，視察小組審閱了環聯相關的政策、手冊、指引、僱員行為守則、培訓資料，以及環聯與資料處理者的服務合約。
20. 此外，專員根據《私隱條例》行使進入處所的權力進行實地視察。2021年9月份，視察小組在各方同意下六次到訪環聯的總辦事處、客戶服務中心、數據中心及電話熱線中心。
21. 視察小組的實地視察工作包括：
 - (i) 與負責管理個人信貸資料系統的人員（包括環聯及外判公司的人員）面談；
 - (ii) 到訪環聯不同部門，了解個人信貸資料系統的實際運作及相關的存取控制機制；
 - (iii) 觀察環聯示範個人信貸資料系統的運作、如何透過系統存取個人資料、對員工存取個人資料的具體管理程序；及
 - (iv) 抽樣檢查環聯載有個人信貸資料的紙本紀錄及電腦檔案紀錄，當中包括個人信貸資料系統的員工活動日誌紀錄。

⁵ 視察小組包括一名首席個人資料主任、一名高級個人資料主任及兩名個人資料主任組成。

22. 視察小組亦曾安排神秘顧客到訪環聯的客戶服務中心，以了解環聯如何處理個別人士申請信貸報告的要求。

第 III 部 – 環聯的個人信貸資料系統

23. 環聯作為資料使用者須符合《私隱條例》的規定。同時，環聯是香港的信貸資料機構，須遵循《實務守則》的相關規定行事。除法律程序外，如資料使用者不遵守《實務守則》，則在向專員提出的任何個案中，有關情況會對該資料使用者不利。
24. 環聯的個人信貸資料系統⁶收集及使用個人資料的流程概述如下：



⁶ 環聯配置了數個獨立系統處理個人信貸資料。

個人信貸資料的收集

25. 根據《實務守則》第 3.1.1 至 第 3.1.8 條，環聯可以為提供個人信貸資料服務之目的而收集個別人士的個人資料。由環聯持有的個人資料來自三個主要來源：

- 使用環聯的個人信貸資料服務的信貸提供者（如銀行、財務公司及信用卡公司）；
- 公眾紀錄；及
- 個別人士。

26. 信貸提供者從個別人士因應非按揭貸款帳戶⁷或按揭帳戶⁸而收集了個人信貸資料，可根據《實務守則》第2.4條向環聯提供該人士的相關個人信貸資料。使用環聯的個人信貸資料服務的信貸提供者可透過兩種途徑向環聯的個人信貸資料系統提供個人信貸資料，經互聯網提供單一個別人士的資料及以分批的形式提供多名人士的資料。環聯收到個人信貸資料後，便會更新相關人士的個人信貸資料。

27. 環聯會從公眾紀錄取得個別人士的資料，包括向個人追收欠債的法律行動或關乎欠款的裁決、政府憲報刊登個別人士的破產聲明或解除破產資料，及法院登記處的民事訴訟案件。個別人士亦可向環聯提出更改個人資料要求。

⁷ 非因按揭貸款而收集的個人信貸資料包括姓名、地址、聯絡資料、出生日期、香港身份證號碼或旅行證件號碼、與按揭貸款無關的信貸申請資料（即有關個人已作出個人信貸申請、所申請的信貸類別及金額）及信用卡損失資料。

⁸ 因按揭貸款而收集的個人信貸資料包括姓名、個人的身份（即借款人、按揭人或擔保人）、香港身份證號碼或旅遊證件號碼、出生日期、地址、帳戶號碼、信貸種類、帳戶狀況（生效、已結束、已撤帳等）、帳戶結束日期及按揭申請資料。

個人信貸資料的使用

28. 使用環聯的個人信貸資料服務的信貸提供者可透過下述途徑作出信貸報告查詢：
- 主機到主機查詢：通過信貸提供者和環聯之間的專門租用線路進行查詢；及
 - 電腦網上查詢：登入環聯授權信貸提供者使用的系統進行查詢。
29. 個人信貸資料亦會按個別人士的要求以信貸報告的形式提供。個別人士可在網上購買信貸報告，或在預約後親身到環聯客戶服務中心購買自己的信貸報告。
30. 環聯的信貸報告一般包含以下資料：
- 個人資料：例如姓名、身份證件號碼、出生日期、地址及電話等；
 - 信貸帳戶資料：信貸使用情況及還款紀錄等；
 - 公眾紀錄：債務追討、破產及清盤訴訟；
 - 查詢紀錄：過去兩年內環聯會員的查閱紀錄；及
 - 信貸評分：概括信貸狀況的一個分數。

第 IV 部 – 主要視察結果

31. 本報告主要是根據整個視察過程中，包括環聯所提供的資料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》及《實務守則》的規定是環聯的法律責任。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。
32. 有關個人資料的保安，保障資料第 4(1) 原則訂明，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。保障資料第 4(2) 原則訂明，如資料使用者聘用資料處理者⁹，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。
33. 本報告針對第17段所述的範疇就個人資料保安方面作出評估，除指出環聯可以改善的地方之外，亦展示環聯保障其持有的個人信貸資料所採取的良好行事方式。

(I) 資料管治架構及私隱政策

個人資料私隱管理系統

34. 專員一直倡議機構應建立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處理及使用個人資料並符合《私隱條例》規定的系統¹⁰。

⁹ 不論是在香港或香港以外聘用

¹⁰ 有關如何制訂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

35. 專員認為環聯大致上把保障私隱納入其企業管治之中。然而，考慮到環聯管有龐大的個人信貸資料系統，其系統規模及所持有的個人資料數量和敏感程度，專員認為環聯應更全面地建立及執行個人資料私隱管理系統。
36. 根據環聯提供的一份於 2021 年 6 月生效，適用於香港的標準作業程序，保障資料主任由一名區域合規主管擔任。該標準作業程序僅簡單描述了保障資料主任的角色，包括就資料保障事宜向環聯提供獨立建議和監督，並確保定期向員工提供相關的培訓及指引等基本要求。
37. 專員認為該標準作業程序中對保障資料主任角色的描述流於表面，並無具體訂明保障資料主任的職責、工作範圍及與其他人員的匯報關係，而環聯提交的其他的個人資料私隱政策及相關文件亦未有描述保障資料主任的角色。
38. 考慮到環聯管有龐大個人信貸紀錄，專員認為環聯應委任一名專責人員作為保障資料主任，全面監督《私隱條例》及《實務守則》的遵從情況及推行個人資料私隱管理系統，並更新相關的內部政策及程序，更具體地訂明保障資料主任的職責及角色，並安排他可以直接向最高管理層匯報。專員欣悉環聯其後告知私隱專員公署，環聯已落實建立個人資料私隱管理系統及委任專責人員作為保障資料主任。

地區性私隱政策

39. 專員理解環聯隸屬美國環聯集團，有必要依循總公司制訂並適用於全球的政策行事，包括在保障個人資料及資訊保安方面的政策及規定。
40. 視察小組在本視察中發現環聯的一些與保障個人資料有關的政策僅備有總公司制訂的全球政策，而這些政策未必在所有情況下完全切合環聯在

香港的實際運作情況。例如由總公司制訂的活動日誌管理政策訂明了日誌資料保存期限及查核頻率，但視察小組發現環聯就個別載有個人信貸資料的系統採取了有別於總公司政策的做法，而這些做法並未見於任何適用於香港公司的政策文件。

41. 專員建議環聯就其全球政策制訂適用於香港公司的內部政策及標準，向個人信貸資料系統的管理人員及使用者在資料的保存、使用及保安等方面提供更具針對性的指引。環聯亦應定期檢視其本地政策是否緊貼《私隱條例》的修訂，例如應該因應《私隱條例》於 2021 年 10 月生效有關「起底」的修訂條文，對有關政策進行修訂或更新。專員得悉環聯在視察小組的實地視察工作完成後，承諾會制訂適用於香港的內部政策及標準。

(II) 實體及系統保安

42. 視察小組實地視察了環聯所採取的保障個人資料實體保安措施和系統保安。基於保安措施的保密性，相關細節不會在本報告詳述。然而，視察小組留意到，環聯界定個人信貸資料屬於「機密」級別，必須極為謹慎地儲存、使用及棄置，並一直參照國際標準化組織的標準，制訂資訊科技安全政策，提升資訊保安的防護能力，政策涵蓋系統防護、存取控制、實體保安等技術層面。
43. 專員亦欣悉環聯致力加強私隱保護的控制措施，採納國際標準化組織發佈的標準，制訂相關政策以建立、實施、維護和持續改善資訊安全方面的管理措施，減低私隱資訊所面臨的風險。
44. 自 2003 至 2021 年，環聯每年均聘用獨立審核人完成私隱循規審核，以協助評估其個人資料系統的完整性、準確性和保安程度。

45. 總體來說，專員認為環聯在其個人信貸資料系統的營運過程及常規中採取了足夠的保障個人資料措施，並樂見其作業模式亦符合國際資訊科技保安標準。

(III) 監控及持續評核

46. 專員考慮到環聯的業務性質，特別是環聯的個人信貸資料庫規模龐大並載有性質敏感的個人信貸資料，認為環聯應對其個人信貸資料系統使用方面持續作出監控及審核員工在系統中的活動。專員注意到環聯有相關政策清楚告知員工，環聯會就員工使用公司裝置及系統進行監察。

環聯對系統的內部存取控制

47. 環聯就個人信貸資料系統的內部存取控制，採取了下述良好的行事方式：
- **按職能設立存取權限：**按「有需要知道」的原則授予員工的存取權限，並確保該等權限與員工的職級、職能及責任相符。
 - **定期檢視存取權限：**在授予個別員工任何存取權限之前，必須取得書面批准。環聯設有系統，定期提醒及要求各部門主管重新檢視所屬部門所有員工的存取權限，並重新在系統內確定各員工的存取權限。
 - **實施良好的密碼管理：**環聯制訂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，登入者的帳戶會被鎖定。

- **備存詳盡的員工活動日誌紀錄：**環聯就其個人信貸資料系統，備存了員工活動的日誌紀錄。環聯會定期對這些日誌紀錄進行檢視，以察看是否出現不尋常存取資料的情況。

環聯對信貸提供者的存取控制

48. 環聯擁有龐大的個人信貸資料數據庫，而信貸提供者為業務需要有必要獲取個別人士的個人信貸資料，以衡量批出信貸的風險、預防詐騙及追討債務。根據環聯提供的資料，有超過 160 個信貸提供者使用環聯的個人信貸資料服務。
49. 視察小組留意到，環聯透過合約規範方法對信貸提供者採取了適當的系統存取控制措施，配以恆常的偵測及監察異常登入系統的情況，以減低未經准許存取個人信貸資料的風險。

專員就環聯存取控制的建議改善範疇

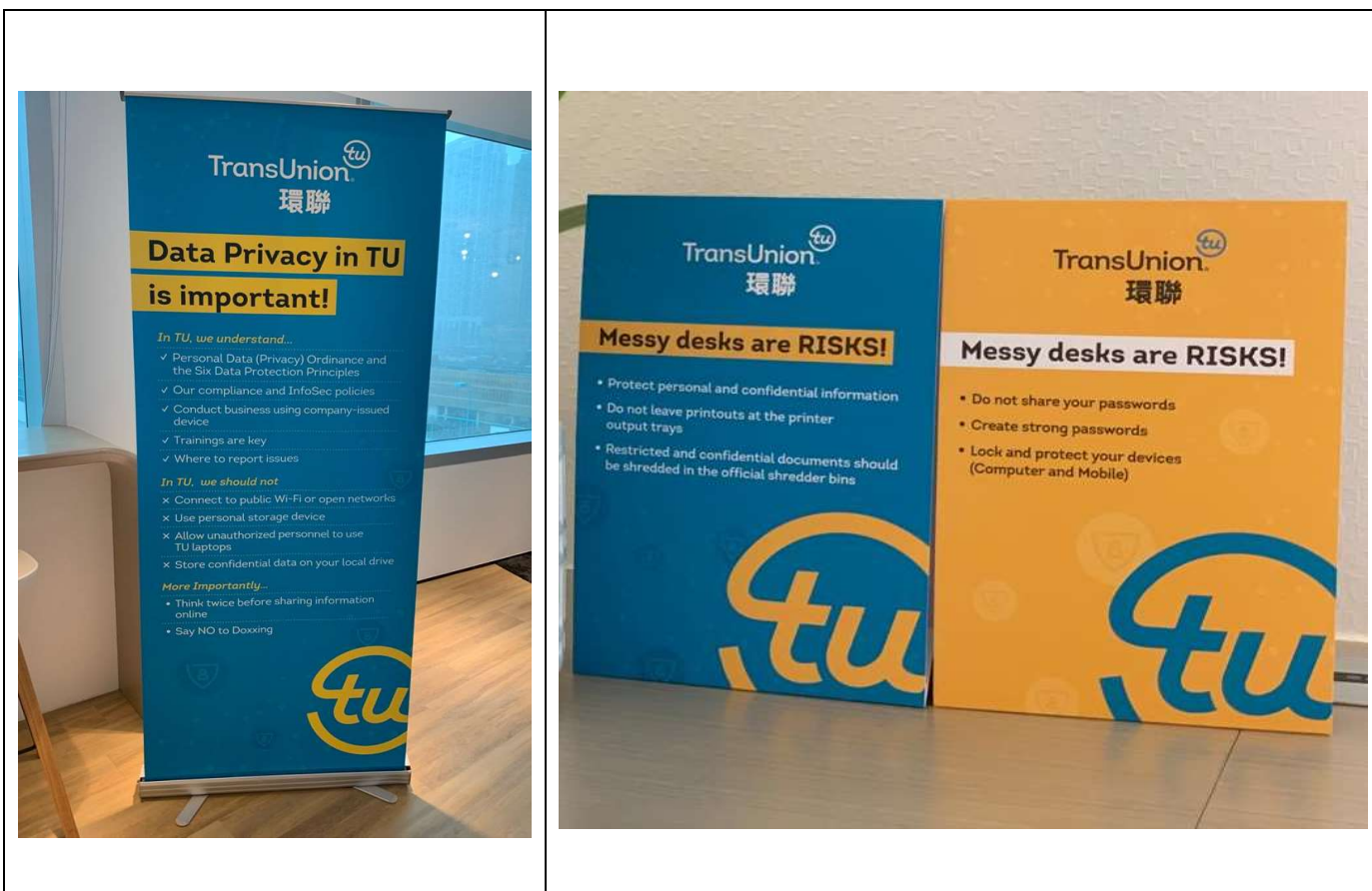
50. 視察小組亦留意到，環聯不同部門對日誌紀錄的查核頻率及方式各異，反映環聯在這方面沒有較為統一的準則。此外，環聯是透過人手查核內部系統日誌紀錄，並未配置任何電子方式協助有關查核。考慮到環聯內部系統日誌紀錄的數據量，專員建議環聯應就內部系統的日誌紀錄的管理方式訂定統一標準，該標準應訂明日誌紀錄所包含的資料類別，查核的權限、方法及頻率，及在偵測到可疑情況時的跟進方案等。此外，環聯亦應考慮配置電子方式協助有關查核，增加查核的準確性。環聯表示因應專員的建議，現正改良內部查核系統日誌紀錄的方法及頻率，並考慮採用電子方式協助有關查核以提升準確性。

51. 此外，根據《實務守則》的規定，環聯如發現信貸提供者有任何懷疑異常查閱情況¹¹，應在合理地切實可行的情況下，盡快向信貸提供者的高層管理人員及專員報告此懷疑異常查閱情況。私隱專員公署的紀錄顯示環聯曾在懷疑異常查閱情況事發後九個月才向專員作出匯報，而專員注意到環聯自 2020 年起已備有處理懷疑異常查閱情況的政策，當中訂明環聯一般會在發現信貸提供者出現《實務守則》訂明的懷疑異常查閱情況後兩個月內，連同相關信貸提供者就事件的解釋向專員作出匯報。專員建議環聯修訂處理信貸提供者的懷疑異常查閱情況的政策，詳細述明當遇上有關情況時的調查及匯報程序，並設定一個比原有政策（即兩個月內）更短的通報時限，盡快就信貸提供者的懷疑異常查閱情況通知專員。

(IV) 培訓及教育

52. 環聯對員工有多項提升個人資料私隱意識的政策及措施，致力保障個人資料私隱，包括向員工提供一系列有關資料保障方面的入職培訓，並透過內部電子平台持續為員工安排保障個人資料的培訓課程，而資訊安全部會定期透過電郵向員工提供資訊保安提示。
53. 以下為視察小組在實地視察期間留意到環聯在辦公範圍的保障個人資料私隱的提示：

¹¹ 同一信貸提供者在任何 31 日內根據《實務守則》第 2.9.1.2、2.9A.2、2.9A.4、2.9A.5、2.10A.2、2.10A.3 或 2.10A.4 條，為檢討向某特定個人已提供的現有個人信貸安排而曾五次或以上查閱信貸資料機構所持有該個人的信貸資料。



(V) 資料處理者的管理

54. 資料使用者將處理個人資料的工作外判予代理人日益普遍。如外判人員（資料處理者¹²）沒有採取足夠的步驟，保障受託的個人資料，可導致資料外洩，對受影響的資料當事人造成嚴重及不可挽回的損害。
55. 保障資料第 4(2) 原則訂明，如資料使用者聘用資料處理者¹³，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

¹² 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，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，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。

¹³ 不論是在香港或香港以外聘用

法，以防止轉移予該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。

56. 視察小組留意到環聯有將個人資料外判予第三方服務供應商處理，包括負責運作電話熱線中心、數據中心的服務供應商，以及負責運送和保管備份磁帶的保安公司。
57. 專員認為環聯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。不過，專員建議環聯應在與資料處理者簽訂的合約加入資料外洩的處理程序，好能讓雙方在資料外洩事件發生時，作出迅速的應變及補救措施，將外洩事故的傷害減至最低。
58. 專員亦建議環聯在聘請資料處理者處理個人資料之前對資料處理者的行事方式或程序進行私隱影響評估，以分析涉及的資料處理步驟，評估有關步驟所涉及的私隱風險，以便引入避免或減低對個人資料私隱產生不利影響的措施。而在委任資料處理者之後，應定期審視資料處理者處理個人資料的方式是否符合雙方訂定的標準，並在出現未能預見的私隱風險時，與資料處理者訂定應對方案。專員欣悉環聯在視察小組的實地視察工作完成後，於2022年3月落實上述有關進行私隱影響評估的建議。

(VI) 進一步的資料保障措施

59. 公眾對機構的期望並不僅僅限於符合法律或監管要求。機構在爭取營運成果的同時，亦應履行企業的社會責任。

免費信貸提示服務

60. 視察期間，環聯會為個別已登記及每月繳費人士提供「信貸提示服務」。如該人士的信貸報告出現重要變動時（見下圖），如新開立帳戶或信貸查詢，環聯會發送電郵及／或電話短訊通知該人士。



資料來源：<https://www.transunion.hk/zh/product/credit-report>

61. 環聯表示理解市民對保障個人資料私隱日漸關注，在視察的過程中，環聯應專員的建議，於2022年5月推行免費「信貸提示服務」。公眾人士只要在環聯網站完成身份驗證後，便可選擇免費訂閱「信貸提示服務」，過程中毋須訂購任何信貸報告。當訂閱「信貸提示服務」人士的信貸報告出現重要變動（即上圖所述情況），環聯會透過電郵通知該人士，讓該人士知悉其信貸報告的變動，並可以預早作出防範或跟進。

在信貸報告加入備註

62. 視察期間，因應視察人員的查詢，環聯向視察人員表示，他們注意到自2019年中出現嚴重的「起底」行為，多名人士的個人資料在公共領域或

社交平台被發佈，有人利用被「起底」人士的個人資料進行不法用途，當中包括進行借貸。有見及此，環聯因應專員的建議，推出一項服務，讓被「起底」或懷疑被「起底」的人士，可在其信貸報告中加入備註，讓使用環聯個人信貸資料服務的信貸提供者（即銀行或財務機構）查閱該名人士的信貸報告時得悉此事，在審核該人士的信貸申請時可作參考。

總結

63. 視察結果顯示，環聯採取了良好的行事常規，其個人信貸資料系統的保安措施符合國際標準。專員認為環聯在保障其持有的個人資料方面，符合《私隱條例》中附表 1 的保障資料第4原則有關個人資料的保安的要求。專員亦樂見環聯已經就視察小組的意見建立個人資料私隱管理系統並委任保障資料主任，有系統地建立一套遵從《私隱條例》規定的制度，循規地持有、處理及使用個人資料。雖然如此，根據本視察的觀察所得，專員建議環聯就其全球政策制訂適用於香港公司的內部政策及標準、更具體地訂明保障資料主任的職責及角色、就內部系統的日誌紀錄的管理方式訂定統一標準、修訂處理信貸提供者的懷疑異常查閱情況的政策，並定期對資料處理者處理個人資料的做法進行適時的檢視。

第 V 部 – 建議

64. 專員希望透過本視察報告，向日常需要處理大量客戶個人資料的機構作出下述建議：

- (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：**機構應明確制訂保障資料主任的角色及職責，包括監察遵從《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中。
- (iii) **制訂地區性政策：**跨國企業在保障個人資料方面制訂全球通用的政策（包括保障個人資料及資訊保安方面的政策及規定）時，亦應考慮不同地區的法規而制訂更具體的地區性政策。
- (iv) **履行企業社會責任：**公眾對機構的期望並不僅僅限於符合法律或監管要求。機構應履行社會責任，並實踐於日常營運中，致力加強保障客戶個人資料私隱。機構積極實踐社會責任可帶來雙贏的局面，為機構帶來更長遠的競爭優勢。
- (v) **監控個人資料的查閱情況：**要有效地監察任何可疑的行為，機構應具備追查員工存取個人資料的機制，包括搜尋及更改紀錄的情

況。機構應制訂政策進行及時及有效的持續監察，並訂明偵測到可疑情況時的跟進方案及匯報程序。

- (vi) **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。私隱影響評估有助機構分析相關的資料處理步驟，評估有關步驟所涉及的私隱風險，以便引入避免或減低對個人資料私隱不利影響的措施。而在委任資料處理者之後，機構應持續審視資料處理者處理個人資料的方式是否符合雙方訂定的標準，並在出現未能預見的私隱風險時，與資料處理者訂定應對方案。

《個人資料（私隱）條例》

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。

《個人信貸資料實務守則》（節錄）

信貸資料機構為資料保安及系統完整性所採取的措施

為準備提供信貸資料服務所採取的措施

3.11 在向信貸提供者提供個人信貸資料服務之前或之時，信貸資料機構應採取適當的措施，以防所持有的個人信貸資料受到不當查閱或不當處理，包括：

3.11.1 與作為該等服務的用戶之信貸提供者簽訂正式書面合約，具體列明下述事項：

3.11.1.1 在提供及使用個人信貸資料服務時，雙方均有責任遵守本守則的規定；

3.11.1.2 在何種情況下信貸提供者可查閱信貸資料機構所持有的個人信貸資料；及

3.11.1.3 信貸提供者在查閱信貸資料機構的資料庫時所適用的管制措施及程序；

3.11.2 制訂管制措施，確保只發放予用戶其有權取得的資料；

3.11.3 就條例及本實務守則的規定為職員提供培訓，特別是良好保安措施方面的培訓；

3.11.4 就職員、外間承辦商或用戶正當行使查閱權力方面，擬備書面指引及紀律或合約程序；及

3.11.5 確保已有足夠保障措施，盡量減低任何人在未獲授權的情況下進入資料庫或截查來自或輸入資料庫的通訊之風險。

日常運作所採取的措施

3.12 信貸資料機構在日常運作中應採取適當的措施，以防所持有的個人信貸資料受到不當查閱或不當處理，包括：

3.12.1 定期及經常檢討密碼的管制措施，確保只有獲授權的職員才可查閱資料庫；

3.12.2 定期及經常監察及檢討資料庫的使用情況，藉以偵察及調查任何不尋常或不合常規的查閱或使用模式；

3.12.3 確保在刪除及棄置資料方面採取妥善保安措施，特別是當記錄資料或磁碟會被棄置於機構以外的地方，或由外間承辦商負責棄置時，這點尤為重要；

3.12.4 就所有經證實違反保安措施或涉嫌違反保安措施的事件備存記錄簿，當中顯示受影響的記錄、當時的情況，以及所採取的行動。

就信貸提供者的查閱等備存記錄簿

3.13 在不影響上文第 3.12 條的一般性原則情況下，信貸資料機構應：

3.13.1 如發現信貸提供者有任何懷疑異常查閱情況，應在合理地切實可行的情況下，盡快向信貸提供者的高層管理人員及專員報告此懷疑異常查閱情況；

3.13.2 備存記錄簿，記錄信貸提供者曾對其資料庫作出的所有查閱，記錄簿須包括：

3.13.2.1 查閱資料的信貸提供者的身份；

3.13.2.2 查閱資料的日期及時間；

3.13.2.3 被查閱資料的有關個人的身份；

3.13.2.4 查閱是根據第 2.8、2.9、2.9A 或 2.10A 條所規定的何種情況下進行(由信貸提供者根據第 2.11.1 條作出確認)；

3.13.2.5 如查閱是根據第 2.9.1.2、2.9A.2、2.9A.4、2.9A.5、2.10A.2、2.10A.3 或 2.10A.4 條為檢討現有個人信貸安排而作出，根據第 2.9.3、2.9.4 或 2.9.5 條的規定所考慮過的具體事宜(由信貸提供者根據第 2.11.2 條作出確認)；及

3.13.2.6 信貸資料機構向信貸提供者的高層管理人員及專員所報告的任何懷疑異常查閱情況；

及保留該記錄簿最少兩年，以供循規審核人及/或專員審閱(視情況而定)。