使用金融科技小貼士

PCPD
HK

PCPD.org.hk

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

消費者使用金融科技時，應採取以下措施，保障個人資料私隱：

1. 細閱私隱政策，尤其留意：

- 將被收集的個人資料的類別
- 個人資料的可能使用詳情
- 機構擬將個人資料轉交予哪些人士
- 消費者的權利和責任，例如查閱及改正資料、拒絕某些資料用途等的權利
- 機構採用保障個人資料的保安措施

2. 審慎評估索取個人資料的要求，檢視金融科技應用程式的私隱設定，並移除程式中的不必要查閱資料權限

3. 在安全環境下使用金融科技應用程式：

- 不要通過公共或不安全的Wi-Fi，或公共電腦使用金融科技應用程式
- 確保金融科技應用程式在其操作的裝置已開啟防盜功能，並在該裝置安裝最新保安程式和防毒軟件
- 使用複雜密碼，切勿與其他帳戶共享密碼

4. 定期監察帳戶，留意有否未經授權的交易或活動

建議金融科技供應商/營運者採取的良好行事方式

1. **私隱政策應具透明度，並以淺白語言向消費者解釋下列事項：**
   - 收集個人資料的類別和必要性
   - 收集個人資料的所有擬作用途
   - 獲轉交個人資料的所有可能人士
   - 消費者的權利和責任，例如查閱及改正資料、拒絕某些資料用途等的權利
   - 保障個人資料的保安措施
2. **收集和保留最少個人資料**
3. **就收集和使用個人資料向消費者提供清晰及真正的選擇**
   - 清晰選擇：能以顯眼的方式引起消費者注意，而不是藏於冗長的私隱政策之中
   - 真正選擇：消費者的選擇不會對其能否獲得服務、服務價格和效益有重大不利影響
4. **確保所使用的個人資料準確及公正**
5. **確保金融科技算法可靠和公平，並向消費者解釋金融科技作出的自動評估和決定（例如信貸評分）的理據**
6. **採取適當政策、程序和技術以確保資料安全**
7. **以合約或其他方式（例如實地審核），確保資料處理者能充份保障個人資料**
8. **開發金融科技期間或之前，進行私隱影響評估，以識別和妥善處理潛在私隱風險**
9. **金融科技的設計應貫徹尊重私隱**
10. **就資料外洩事故訂立處理程序**

下載本刊物

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 ： **enquiry@pcpd.org.hk**

二零一九年三月初版

金融科技

1. 引言

1.1 「金融科技」指用以提供金融服務的資訊及通訊科技。金融科技可涉及不同種類的科技，並以不同形式呈現。金融科技帶來創新的金融服務，逐漸改變金融行業的運作，並且滲入我們日常生活的不同範疇。

1.2 本單張旨在：

(a) 介紹一些較常用並對個人私隱有影響的金融科技；

(b) 解釋金融科技應用的私隱風險；

(c) 為消費者 / 使用者提供實用的提示，讓他們在使用金融科技時可保障自己的個人資料私隱；及

(d) 向金融科技供應商 / 營運者建議良好的作業方式，以應對金融科技帶來的私隱風險。

1.3 使用金融科技還可能與私隱以外的風險有關聯（例如金融風險）。此些其他風險超出《個人資料（私隱）條例》（香港法例第 486 章）（**條例**）及個人資料私隱專員（**私隱專員**）的監管範疇，因此不在本單張的討論範圍。金融科技供應商 / 營運者應了解清楚是否須要遵從與其行業相關的其他法規。

2. 金融科技的日常應用

2.1 金融科技並無明確的界限。電腦運算能力的提升、互聯網無遠弗屆的連接性、流動電話技術的進步，加上人們對便捷、低成本及個人化的金融服務需求強勁，令金融科技蓬勃發展。

2.2 金融科技會以不同形式呈現，並支援不同的金融服務和運作，例如：

(a) 電子支付及匯款（例如：電子錢包[1]）；

(b) 金融投資（例如：機械人投資顧問及算法交易）；

(c) 點對點融資（例如：點對點網貸及眾籌）；

(d) 支援金融機構運作的數據分析（例如：信貸評分）；

(e) 資訊共享（例如：開放應用程式介面）；及

(f) 分佈式分類帳技術（區塊鏈技術是分佈式分類帳技術的特定類型；分佈式分類帳技術的應用例子包括加密貨幣的交易及智能合約程式）。

2.3 金融科技中，並非全部皆涉及收集及處理個人資料。即使有涉及，對個人資料私隱所構成的風險程度亦因應所用的金融科技而有所不同，並 (除其他事宜外) 視乎個人資料的數量、敏感程度和擬定用途，以及金融科技供應商 / 營運者的數據管理。下文介紹一些常見的金融科技例子，這些金融科技涉及收集及 / 或處理個人資料，因而會對私隱構成風險。

1 電子錢包包括《支付系統及儲值支付工具條例》（香港法例第 584 章）所規管的儲值支付工具。不過，並非所有電子錢包均屬儲值支付工具，尤其是那些沒有儲值功能的電子錢包。

電子支付

2.4 電子支付是透過應用軟件 (通常在流動電話中運作) 支付款項。使用者可在實體或網上商店進行電子支付，或作點對點轉帳。要進行電子支付，可透過掃描二維碼、以流動電話輕拍商戶的非接觸式讀取器，或在流動應用程式中鍵入付款資料。

2.5 電子支付服務供應商或會在不同階段收集使用者的個人資料。例如，在登記電子支付服務時，使用者通常須向服務供應商提供其姓名、電郵地址、流動電話號碼及銀行帳戶資料。有些服務供應商亦會要求使用者提供身份證明（例如身份證副本），以完成金融規例所訂明的「認識你的客戶」程序。在運作階段，服務供應商會記錄付款詳情，例如付款日期、時間、金額及地點。電子支付服務的相關應用程式亦可能需要查閱使用者流動電話內的電話簿，以處理點對點付款。

信貸評分

2.6 信貸評分是指利用數學模型評估個人的信用可靠程度的方法。傳統上，貸款人會以個人與銀行交易紀錄、信貸歷史及入息證明等資料作出評估。隨著數據分析科技、大數據分析科技及評分算法科技的進步，現在可以利用這些科技來分析借款人的各類個人資料，以決定其信貸評分。在可能用於此類評估的個人資料包括購物紀錄、付款記錄、居住的社區、社交網絡及其他行為資料。

開放應用程式介面

2.7 應用程式介面可以讓機構內部或機構之間的不同應用軟件互動及溝通。應用程式介面可以便利數據在應用軟件之間在快捷及保安良好的情況下傳送。開放應用程式介面可以讓第三方程式開發商在最低程度的限制下查閱一個機構的數據，然後利用有關數據為消費者提供新服務。

2.8 在金融科技方面，開放應用程式介面可在顧客的授權下，讓銀行與第三方程式開發商共享有關顧客的帳戶資料（例如結餘或交易）[2]。開發商繼而可創造應用軟件，讓使用者在單一平台實時管理他們在不同銀行的帳戶。貸款人亦可利用銀行的開放應用程式介面上的可靠數據，評估其潛在借款人的信用可靠程度。開放應用程式介面亦會涉及共享非個人資料，例如銀行利率及服務收費。

分佈式分類帳技術及區塊鏈

2.9 分佈式分享帳技術是一種電子分類帳，容許記錄及共享交易數據和資料，並容許這些數據和資料在不同網絡參與者的分布式網絡同步進行。區塊鏈是分佈式分類帳技術中的特定類型，越來越多人應用。

2.10 在區塊鏈上，數據是以「區塊」儲存和傳輸，而各區塊是以「數碼鏈」串連。當一宗有效的交易達成時，便創造一個新區塊。至於數碼鏈，實際上是區塊的加密雜湊（cryptographic hash）組成。區塊鏈上每個區塊包含其之前區塊的加密雜湊，因此區塊可以一個接一個地相連成為一條鏈。加密雜湊有助確定區塊的真確性，並可為任何單一區塊追本溯源，找出其原始區塊。

2.11 區塊鏈屬分布式分類帳，因為每個參與者都持有整份相同的分類帳，即整條區塊鏈。區塊鏈利用加密及演算方法在整個網絡上記錄及同步數據。

2.12 區塊鏈上每項新交易均需網絡參與者確認。有關區塊然後會連接上現有的區塊鏈。當加入新區塊後，整條鏈便會加長。任何網絡參與者不能更改或刪除較早前的區塊。因此，區塊鏈設計原意是令交易記錄不能更改。

2.13 以目前科技水平來說， 區塊鏈如設計及建立恰當，一般認為是無法篡改的。在記錄的真確性方面，一般亦認為區塊鏈為參與者提供了保證。區塊鏈一般屬高度透明，因為所有交易是公開和可追溯的，並且永久儲存於區塊中。

2 參考資料：香港金融管理局於 2018 年 7 月 18 日發出的「銀行業開放應用程式介面框架」： https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf

2.14 目前，區塊鏈最廣為人知的用途是記錄加密貨幣（例如比特幣）的交易。區塊鏈或分佈式分類帳技術亦可用於很多其他的金融運作，例如國際支付及匯款、付款授權、結算及交收、證券買賣、按揭公證服務等。分佈式分類帳技術及區塊鏈的其他非金融用途包括供應鏈管理，以及客戶獎賞及忠誠計劃。

3. 金融科技的私隱風險

3.1 雖然金融科技可以為營運者及顧客帶來很多好處，但使用金融科技亦可能帶來私隱風險。

在使用者不知情或未有具意義的同意下收集及使用個人資料

3.2 隨著金融科技的應用，大量個人資料或會被收集或產生，而使用者不一定對此知情[3]。金融科技供應商 / 營運者或會在超越使用者的合理預期下，或未有使用者具意義的同意下使用或披露有關個人資料[4]。

電子支付

3.3 使用者在登記時除了提供流動電話號碼及身份證明外，電子支付服務供應商亦會在使用者知情或不知情下收集使用者的聯絡人名單、購物紀錄及位置資料。服務供應商所收集的個人資料可以併合使用者各方面的生活細節，並透過個人概況彙編準確地預測他們的行為、喜好及習慣。有些個人概況彙編或會揭露敏感的個人資料或使用者的私人秘密。所收集或推斷的個人資料繼而會在使用者不知情或未有其具意義的同意下被使用，例如用於個人化廣告及信貸評分。

信貸評分

3.4 信貸評分涉及使用大數據分析及評分算法，以評估個人的財務狀況。用於信貸評分的數據來源十分廣泛，可包括個人的購物模式、繳付帳單的準時度、在社交媒體的貼文及其他資訊。分析所用的數據或會超越個人的合理預期。低透明度亦會令個人無法控制其個人資料的使用及保障自己，例如對依據不準確或偏頗的個人資料所作的不當決定提出反對。如個人資料在當事人不知情下被用於信貸評分，當真相曝光後，當事人或會感到不受尊重及尊嚴受損。

開放應用程式介面

3.5 在開放應用程式介面，個人未必能完全了解哪些個人資料是與第三方開發商共用，及個人資料會如何被使用及進一步披露，尤其是當開放應用程式介面的查閱限制少，以及第三方開發商的私隱及資料保安的政策及實務模糊不清。

區塊鏈

3.6 在區塊鏈方面，網絡不時會有新參與者加入，而每個參與者會得到整份數碼分類帳的複本。現有的參與者不會知道日後誰人會查閱其記錄。這問題在公有區塊鏈中尤其嚴重。公有區塊鏈是公共網絡，容許任何人均可加入、閱讀有關內容及進行交易。相比之下，只限獲授權人士加入的私有區塊鏈網絡，帶來的私隱風險相對較低。

以不公平或歧視方式使用個人資料

信貸評分

3.7 信貸評分算法像很多其他大數據分析應用程式一樣，把大量由不同來源收集的公共、私有及個人資料混合和分析，評估個人的信用可靠程度。有些類別的個人資料是直接從個人收集的（例如聯絡資料），有些是在個人與貸款人互動時產生的（例如交易記錄），或是由數據分析工具推斷（例如某人是否購

3 條例附表 1 的保障資料第 1（3）原則規定，資料使用者須採取所有切實可行的步驟，以確保在收集資料當事人的個人資料之時或之前，已通知資料當事人該資料將會用於甚麼目的及可能轉移予甚麼人。

4 條例附表 1 的保障資料第 3 原則規定，資料使用者須得到資料當事人明確及自願的同意，才可將資料當事人的個人資料用於新目的。「新目的」指與原本收集個人資料的目的不同或不相關的目的。

物成癖）。因此，個人不可能完全掌握在信貸評估中收集或使用了甚麼資料，更遑論核實資料的準確性及相關性[5]。有些個人資料（例如個人的社交網絡及居住的社區）與個人的信用可靠程度之間的關係亦存疑。因此，在評估中所輸入的資料有可能是不準確、偏頗、不相關或過時。在此情況下，有關個人的信貸評分，及可得到的信貸安排，很可能受到不公平和不利的影響。

欠缺有效方式刪除或改正過時或不準確的個人資料

區塊鏈

3.8 區塊鏈在設計上是不能改變及防篡改的。儘管區塊內的資料已過時或不準確，該區塊也不能刪除或修改。保留及持續提供不準確或過時的個人資料，會損害個人的資料私隱權利[6]。

電子支付、信貸評分、開放應用程式介面等

3.9 由於資料的價值在數碼經濟中越來越高，金融科技服務供應商 / 營運者傾向盡可能收集及保留最多的個人資料，即使有關資料可能不準確、 不相關或過時。他們未必具備有效的機制以確保適時地刪除或改正不準確、不相關或過時的資料。這種做法不單損害個人的資料私隱權利，亦會增加資料外洩的風險和影響，而且可能違法[7]。

資料保安風險

3.10 收集及 / 或處理個人資料無可避免會帶來資料保安風險[8]。例如，電子支付及開放應用程式介面涉及以電子方式在不同機構與用戶之間傳輸個人資料，這會增加資料外洩或在傳輸過程中遭截取的風險。金融科技供應商 / 營運者的資料庫內所儲存的個人資料及金融資訊是黑客的寶藏，尤其是在數碼年代，資料價值高，增加了挪用資料的誘因。個人資料外洩令個人容易遭人冒充身份、蒙受詐騙、騷擾、身份盜竊及其他違法行為。

資料使用者[9]及資料處理者[10]的身份模糊不清

3.11 在金融科技的使用及運作過程中，個人資料的處理及保存或會涉及不同機構及人士。例如，金融科技營運者所收集的數據可能會由其雲端服務供應商儲存，然後由第三方數據分析公司進行分析。在開放應用程式介面，大量開發商可查閱同一人的個人資料，而在區塊鏈，數碼分類帳的分散性質，意味沒有中央管理人或權限對網絡的運作或參與者的行為負責。這些風險可能導致須負管理和保障個人資料責任的資料使用者及資料處理者的身份模糊不清[11]。因此，個人或無法確定誰人須對其個人資料的外洩或不當處理負上法律責任。

---

5 條例附表 1 的保障資料第 2（1）原則規定，資料使用者須採取所有切實可行的步驟，以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下，該個人資料是準確的。資料使用者如有合理理由相信該個人資料是不準確時，必須停止使用或刪除該個人資料。

6 條例第 26 條及保障資料第 2（2）原則規定，資料使用者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達成收集目的（包括任何直接有關的目的）所需的時間。條例第 22 條及保障資料第 6（e）原則規定，個人有權改正其不準確的個人資料。

7 條例的相關條文：
- 條例第 26 條及保障資料第 2（2）原則有關個人資料的保留；及
- 條例第 22 條及保障資料第 6（e）原則有關個人資料的改正。（見上述註 6）

8 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，以確保其管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 根據條例第 2（1）條，「資料使用者」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。

10 根據條例附表 1 的保障資料第 2（4）原則，「資料處理者」指代另一人處理個人資料，及並不為該人本身目的而處理該資料的人。

11 條例的條文對資料使用者具約束力。條例附表 1 的保障資料第 2（3）及 4（2）原則就資料處理者如何保留及保障個人資料對資料使用者施加額外的責任。

4. 給金融科技使用者的提示

4.1 就本單張而言，金融科技使用者是指使用金融科技作個人用途的消費者。下述提示的目的是幫助使用者在使用金融科技時保障其個人資料私隱，但相關提示不能盡錄。

細心閱讀私隱政策

4.2 當金融科技營運者收集個人資料時，應提供私隱政策。使用者應細心閱讀私隱政策，以了解其權利及責任。使用者尤其應留意下述事宜：

(a) 營運者會收集個人資料的種類；

(b) 營運者會將個人資料用於甚麼可能的目的；

(c) 個人資料會轉移予甚麼人士；

(d) 使用者就其個人資料可享的權利（例如查閱及改正資料的權利；拒絕某些用途的權利）及須負的責任；及

(e) 營運者會採取的保安措施，以保障傳輸中及儲存中的個人資料。

審慎評估個人資料要求及檢視私隱設定

4.3 不同種類的金融科技會視乎其功能而需要不同的個人資料。例如，電子支付服務供應商及信貸評估人可能需要使用者的身份證明，以遵從反清洗黑錢規例，但是，他們未必需要查閱使用者的地理位置資料及流動電話內的電話簿。因此，使用者應首先審慎評估金融科技的功能、所索取的個人資料種類及其目的，然後才決定是否提供資料或使用其服務。

4.4 使用者亦應檢視金融科技應用軟件的私隱設定，並移除當中不必要的查閱權限。

在安全環境下操作金融科技應用軟件

4.5 在使用金融科技的過程中，可能會處理及傳輸敏感的個人資料，例如銀行帳戶資料及密碼。因此，金融科技應用軟件，例如電子支付應用程式，只應在安全的環境下操作，例如：

(a) 不要使用公共或不安全的 Wi-Fi 操作金融科技應用軟件；

(b) 不要在公共電腦操作金融科技應用軟件；

(c) 確保操作應用軟件的裝置已開啟防盜功能（例如屏幕鎖、尋找電話及遙距刪除資料），並安裝最新的保安修補程式及防毒軟件；及

(d) 使用者的帳戶採用複雜密碼，不要把同一密碼用於敏感程度較低的服務，例如社交網絡。

定期監察帳戶活動

4.6 使用者應定期監察交易記錄或帳戶活動，以查看是否出現未經授權的交易 / 活動。如有發現，應盡快將有關交易 / 活動向金融科技供應商 / 營運者通報。

5. 建議金融科技供應商/營運者採取的良好行事方式

5.1 就本單張而言，金融科技供應商 / 營運者是指提供金融科技（例如電子支付應用程式）予消費者使用的人士，及 / 或利用金融科技提供金融及相關服務的人士。金融科技供應商 / 營運者通常是單獨或聯同其他人士共同控制個人資料的收集、持有、處理或使用。在此情況下，金融科技供應商 / 營運者屬於在條例規管下的資料使用者。下述建議的良好行事方式是為協助供應商 / 營運者應對金融科技的主要私隱風險。然而，有關建議並非就遵從條例規定提供全面指引。

透明度

5.2 金融科技供應商 / 營運者的私隱政策及措施應具透明度。私隱政策應該採用淺白易明的語言，以：

(a) 解釋所收集的個人資料的種類、為何必需收集有關資料，以及顧客拒絕提供個人資料的後果；

(b) 說明擬將個人資料用於甚麼用途；

(c) 說明可能將個人資料轉移予的人士（包括資料處理者）；

(d) 解釋使用者就其個人資料可享的權利（例如查閱及改正資料的權利，及拒絕某些用途的權利）及須負的責任（例如提供資料的責任）；及

(e) 解釋所採取的保安措施，以保障傳輸中及儲存中的個人資料。

5.3 金融科技供應商 / 營運者應在收集個人資料之時或之前，應以《收集個人資料聲明》的形式提供上述資料[12]。《收集個人資料聲明》，以長度、複雜程度、字體大小及查閱的容易程度的標準作考量而言，應易於閱讀及理解。

5.4 除了《收集個人資料聲明》，金融科技供應商 / 營運者亦須就處理個人資料的私隱政策及實務措施提供一般的聲明，即《私隱政策聲明》。要符合條例下的開放及透明度的規定，《私隱政策聲明》必須時刻可讓公眾取覽[13]。

5.5 如《收集個人資料聲明》或《私隱政策聲明》無可避免需要較長篇幅（例如基於資料處理活動的複雜性），金融科技供應商 / 營運者應以顯眼的方式向顧客展示簡明扼要及清晰易明的《收集個人資料聲明》或《私隱政策聲明》的摘要[14]。

收集及保留最少的個人資料

5.6 金融科技供應商 / 營運者應收集及保留最少數量的個人資料，並應適時刪除過時的個人資料或將資料去識別化。

5.7 在可能情況下，金融科技供應商 / 營運者只應要求索取操作其金融科技所必需或直接有關的個人資料，而不應一開始便要求使用者提供所有類別的個人資料。

清晰及真正的選擇

5.8 金融科技供應商 / 營運者應就個人資料的收集及使用向顧客提供清晰及真正的選擇。例如，對於那些聊勝於無但並非操作金融科技所必需的個人資料，顧客應獲清晰及真正的選擇，自行決定是否拒絕提供資料，而對於無需要或與操作金融科技無直接關係的個人資料使用或披露（例如用於個人化的廣告），顧客應獲清晰及真正的選擇以決定接受或拒絕。

5.9 如果提供予顧客的選擇能以顯眼的方式引起使用者的注意，而不是埋藏於冗長的私隱政策內，該選擇屬清晰者。

5.10 如顧客的選擇不會對他們能否得到有關服務、服務的價格和效益有重大不利影響，那就是真正的選擇。

數據準確度及算法可靠度

5.11 金融科技（例如信貸評分算法）的供應商 / 營運者應確保所用的個人資料準確及公正。如對個人資料的準確性有懷疑，應與有關人士澄清。

5.12 供應商 / 營運者應該對金融科技的算法的可靠及公平程度進行測試，尤其是當運算結果可能對有關人士的利益、權利及自由帶來重大影響（例如影響個人的信貸評分及可否得到信貸）。如運算結果能客觀反映有關個人的特性及特質，便是公平可靠的結果。例如，大數據分析或顯示那些經常在深宵外出用膳的人通常有較少的儲蓄，較可能拖欠還款。然而，對於那些因為夜班工作而經常在深宵用膳的人，如把這項觀察結果應用到他的信貸評估而給予他較低信貸評分，則很可能對他們不公平。

5.13 金融科技供應商 / 營運者應向個人解釋由金融科技作出的自動評估及決定（例如信貸評

12 有關條例附表 1 的保障資料第 1（3）原則下的透明度規定，請參閱上述註 3。

13 條例附表 1 的保障資料第 5 原則訂明，資料使用者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。

14 有關擬備《收集個人資料聲明》及《私隱政策聲明》的詳細指引，請參閱私隱專員發出的《擬備收集個人資料聲明及私隱政策聲明指引》：https://www.pcpd.org.hk//chinese/resources_centre/publications/files/GN_picspps_c.pdf

分）的理據，以確保算法透明。

資料安全

5.14 金融科技供應商 / 營運者應確保具有行政（例如政策及程序）及技術（例如邏輯存取控制及加密）措施，為傳輸中及儲存中的個人資料提供足夠的保障，以防止內部職員或外部人士未獲准許或意外地查閱、處理、刪除、喪失或使用有關資料。一般而言，供應商 / 營運者應採用廣為接受的資訊科技保安標準及保安漏洞掃描。

5.15 金融科技供應商 / 營運者應就資料外洩事故訂立處理的程序。一旦發生資料外洩事故，金融科技供應商 / 營運者應立即通知以下人士 （如適用）：

a) 受影響的個人；

b) 執法部門；

c) 相關的監管機構，例如（在涉及外洩個人資料的情況下）私隱專員，及 / 或相關範疇的其他相關監管機構，例如財務或金融領域的監管機構；及

d) 其他持份者，例如從其收集相關資料的金融機構 [15]。

資料處理者

5.16 如聘用資料處理者處理及 / 或儲存個人資料，金融科技供應商 / 營運者應採取合約及 / 或其他方式（例如實地審核），以確保資料處理者：

a) 沒有保留個人資料超過所需的時間；

b) 採取足夠的保安措施保障個人資料；

c) 不會為任何未獲准許的目的而處理、使用或披露個人資料；及

d) 在發生資料外洩事故後，立即通知金融科技供應商 / 營運者。

5.17 金融科技供應商 / 營運者亦應清楚知道其資料處理者儲存及 / 或處理個人資料的地點。如有關儲存及 / 或處理涉及轉移個人資料至香港以外地方，供應商 / 營運者應採取合約或其他方式，以確保有關個人資料在這些地點獲得足夠程度的保障 [16]。

私隱影響評估及「貫徹私隱的設計」

5.18 在金融科技的開發期間或之前，供應商 / 營運者應進行私隱影響評估 [17]，以識別及妥善處理在整個資料處理流程（即由資料收集、儲存、處理、使用，以至銷毀）當中的潛在私隱風險。金融科技應從一開始便採用尊重私隱的設計及預設設定。

15 有關處理資料外洩事故的詳情，請參閱私隱專員發出的《資料外洩事故的處理及通報指引》：https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/DataBreachHandling2015_c.pdf

16 有關在跨境資料轉移中保障個人資料的詳情，請參閱私隱專員發出的《保障個人資料：跨境資料轉移指引》：https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/GN_crossborder_c.pdf

17 有關私隱影響評估的詳情，請參閱私隱專員發出的《私隱影響評估》資料單張：https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/InfoLeaflet_PIA_CHI_web.pdf

下載本刊物

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 ： **enquiry@pcpd.org.hk**

二零一九年三月初版