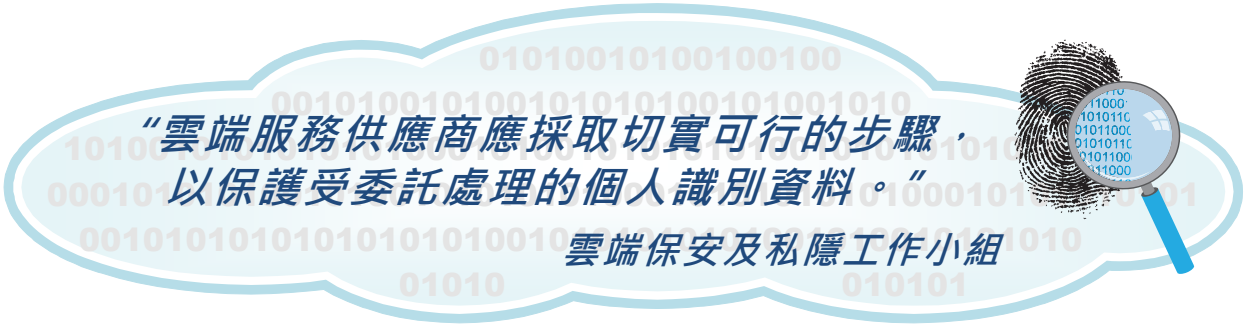
# 雲端服務供應商
## 在雲端平台上處理個人識別資料的資訊保安及私隱保障備忘事項




### 目的

雲端運算服務透過減少成本、增加彈性及縮短推出應用程式和服務所需的時間，為資訊科技帶來變革。這些服務可能涉及收集、儲存、處理或使用個人識別資料，一旦沒有採用適當防護措施，便有可能出現保安風險及私隱問題。本文件載列了有關資訊保安及私隱保障備忘事項，以供雲端服務供應商在雲端平台上處理個人識別資料時參考。

### 目標對象

本文件的主要目標對象是雲端服務供應商。雲端服務供應商以雲端運算技術為基礎向用戶提供資訊科技服務，而有關服務會涉及收集、儲存和處理個人識別資料。有關服務可能是由雲端服務供應商基於「軟件即服務」、「平台即服務」或「基礎設施即服務」而直接提供的解決方案，也可能是按用戶需要根據以上三類服務的不同組合而建立的解決方案。

### 討論範圍

香港制訂《個人資料（私隱）條例》（第 486 章）（下稱《條例》），以保障在世人士的「個人資料」私隱。個人資料包括任何直接或間接與一名在世人士（資料當事人）有關的資料、可切實用以確定有關人士身分的資料，以及其存在形式令查閱或處理均是切實可行的資料。《條例》適用於任何控制個人資料的收集、持有、處理或使用的人士（資料使用者）。當一個資料使用者外判個人資料處理工作予另一人（資料處理者）時，該資料使用者須遵守額外的法定責任[1]。

就《條例》而言，當雲端服務供應商為本身的目的而收集、持有、處理或使用個人資料，便可視作資料使用者。當供應商並非為了本身的目的而代表另一人處理個人資料，便可視作資料處理者。

單憑個人識別資料很多時不足以識別某一個人的身分。但個人識別資料加上其他資料，便可組成用以識別某人身分的個人資料。本文的討論範圍並不限於個人資料的嚴格涵義，從而推動為個人識別資料以至個人資料提供充分保護。在下文各段，「個人識別資料」及「個人資料」兩詞均會使用；但在特別參照《條例》而訂定的備忘事項，則使用「個人資料」一詞。

# 雲端服務供應商
## 在雲端平台上處理個人識別資料的資訊保安及私隱保障備忘事項



### 資訊保安及私隱保障對雲端服務供應商有甚麼影響？

在雲端服務的業務中，保護客戶的資料及私隱是十分重要的工作，也逐漸成為企業成功的關鍵因素。對雲端服務供應商而言，顯示有能力保護受委託處理的個人識別資料，便可得到客戶的信任及信心。相反的話，可能削弱客戶的忠誠度、產生負面的宣傳效果、失去潛在商機及導致法律訴訟。

### 雲端服務供應商應該注意甚麼？

雲端服務供應商應該採取切實可行的步驟，以確保受委託處理的個人識別資料一直受到保護，免遭在未獲授權或無意的情況下被查閱、改動、處理、刪除或作其他用途。很多時候，保護個人識別資料跟保護其他資料相似，包括保護資料的機密性、完整性及可用性。本文件所載的備忘事項，提供建議在雲端平台保護個人識別資料所採取的良好作業模式。雲端服務供應商可視乎本身作為資料處理者或資料使用者的身分以作參考。該備忘事項未必能盡錄所有項目。雲端服務供應商應經常檢查本身的風險狀況，並採取最適合的保安措施。

### 《個人資料（私隱）條例》實用指南

如需要更多有關處理個人資料的指引，雲端服務供應商可參考由香港電腦學會出版的《IT管理層及專業人員「個人資料（私隱）條例」實用指南》[2]。

### 備忘事項的引言

在雲端運算上，資料處理設施不再完全由資料使用者擁有，令資料規管的角色和責任有所改變。本備忘事項闡述在雲端平台上處理個人識別資料的保護措施。

使用雲端運算平台及其服務並非把保護資料的責任轉移給雲端服務供應商。當收集個人識別資料時，收集者控制了有關資料的生命周期，並須負責履行《個人資料（私隱）條例》所訂明的責任。

### 詞彙

本備忘事項所採用的詞彙與《個人資料(私隱)條例》保持一致。

| 詞彙 | 定義 | 例子* |
|---|---|---|
| 資料當事人 | 指一名在世人士，其個人資料正在處理中。 | 信用卡申請人是資料當事人。 |
| 資料使用者 | 指擁有從資料當事人收集得來的資料的一個實體。該實體在數據的整個生命周期內，負責保護收集得來的資料。 | 發卡銀行是資料使用者。 |
| 資料處理者 | 指在收集、處理或儲存個人識別資料時向資料使用者提供服務或產品的一個實體。 | 發卡銀行選用的數據中心營辦商是資料處理者。 |

** 使用處理信用卡申請個案作為例子*

## 備忘事項

下表列出當涉及個人識別資料時，在資訊保安及私隱保障方面的良好作業模式。本列表為雲端服務供應商提供高層次的指引，以供在推行管理、運作及技術措施時參考使用。

| 保護個人識別資料的良好作業模式 | 雲端服務供應商擔任資料使用者的角色 | 雲端服務供應商擔任資料處理者的角色 |
|---|---|---|
| **政策管理** | | |
| 遵守《個人資料（私隱）條例》，特別是保障資料原則[3]。 | ✓ | ✓ |
| 了解及遵從收集和儲存個人識別資料所在的司法管轄區所適用的私隱法例，因為雲端平台可能超越香港特別行政區的司法管轄權範圍。 | ✓ | ✓ |
| 進行私隱影響評估[4]，以助識別及偵測任何對私隱造成的風險，包括在雲端平台上收集及儲存的個人識別資料，在未獲授權或無意的情況下被查閱、修改、處理、刪除或作出其他用途。 | ✓ | ✓ |
| 在機構內部制訂及執行清晰的保護資料或私隱保障政策，以符合收集、處理及儲存個人識別資料所在的司法管轄區的個人資料私隱法例。 | ✓ | ✓ |
| 定期進行風險評估及檢討，以確保有關保安風險受到妥善管理。 | ✓ | ✓ |
| 制訂妥善的合約條款(或至少評估合約條款的需要)，以規管有關保護個人識別資料的行為。 | ✓ | ✓ |
| **收集（保障資料第1原則）** | | |
| 以公平和合法的方式收集個人資料，而這些資料只可作與雲端服務功能和活動直接相關的用途。 | ✓ | |
| 只可在有實際需要時收集個人資料。所收集的資料不應超越原有收集的目的。 | ✓ | |
| 每當在網上收集個人識別資料時，必須向有關人士提供收集個人資料聲明。 | ✓ | |
| 通知客戶有關其個人資料會作何種用途，以及該等資料可能轉移予何人。 | ✓ | |

| 保護個人識別資料的良好作業模式 | 雲端服務供應商擔任資料使用者的角色 | 雲端服務供應商擔任資料處理者的角色 |
|---|---|---|
| **保留及準確性（保障資料第 2 原則）** | | |
| ☁ 保持個人資料準確、適時更新和穩妥，而保留期不應超過實際需要。 | ✓ | |
| ☁ 客戶所交託的個人資料的保留期不應超過實際需要。 | | ✓ |
| **使用及處理（保障資料第 3 原則）** | | |
| ☁ 須先徵求和取得客戶的同意，才可將他們的個人資料作資料收集目的以外的用途。 | ✓ | |
| ☁ 切勿將客戶交託的個人資料作任何未經客戶同意的用途。 | | ✓ |
| **保安防護 - 程序和步驟（保障資料第 4 原則）** | | |
| ☁ 記錄儲存於雲端平台上的個人識別資料的種類。 | ✓ | |
| ☁ 編製一份儲存了個人識別資料的軟件系統及位置清單，以助有效地進行監察。 | ✓ | |
| ☁ 避免把個人識別資料儲存於過多不同的應用程式及位置，因此舉可能增加保安風險，並會加重監察及偵測未獲授權查閱資料方面的工作。 | ✓ | ✓ |
| ☁ 訂出一份認可電腦設備清單，包括可用以管理雲端操作的流動裝置及其相應的保安要求。 | ✓ | ✓ |
| ☁ 制訂有關申請及審批資料查閱權的正式程序及詳細步驟。 | ✓ | ✓ |
| ☁ 制訂快速應變通訊方法以處理保安事故(包括懷疑被入侵的事故）。 | ✓ | ✓ |
| ☁ 定期覆檢電腦 / 網絡設備的記錄和審計追蹤記錄，以檢查是否存在異常情況和可能出現的攻擊。 | ✓ | ✓ |
| ☁ 透過持續監察及保安保證覆檢，不斷改善資料保護措施。 | ✓ | ✓ |

| 保護個人識別資料的良好作業模式 | 雲端服務供應商擔任資料使用者的角色 | 雲端服務供應商擔任資料處理者的角色 |
|---|---|---|
| **保安防護 - 技術措施（保障資料第 4 原則）** | | |
| 為個人識別資料加密或提供加密功能，讓客戶為其儲存在雲端平台上的個人識別資料加密。無論在甚麼情況下加密，都要小心保護加密密碼匙。 | ✓ | ✓ |
| 為透過開放網絡傳輸的個人識別資料加密。 | ✓ | ✓ |
| 應用或提供嚴格的認證方法，例如雙重認證，確保客戶通過認證才可查閱雲端平台上的個人識別資料。 | ✓ | ✓ |
| 在網絡通訊閘安裝保安裝置，例如防火牆、入侵偵測／防禦系統，以保護雲端服務免受外來攻擊。 | | ✓ |
| 確保電腦設備：<br>• 已安裝防病毒軟件及最新的電腦病毒定義檔案，啓動實時偵測功能和對系統進行定期全面掃描；以及<br>• 使用中的操作系統及軟件已安裝最新保安修補程式。 | | ✓ |
| 定期檢查系統保安漏洞，在切實可行情況下盡快實行補救措施。 | | ✓ |
| 定時進行資料備份及測試資料復原程式。 | ✓ | ✓ |
| 電腦設備內的個人識別資料未被完全刪除之前，禁止重用或棄置該電腦設備。 | | ✓ |
| **遵行規定（保障資料第 5 原則）** | | |
| 可以透過私隱政策聲明，告知客戶在保護其個人資料上所作出的承諾及推行的相關措施。 | ✓ | ✓ |
| **查閱與改正（保障資料第 6 原則）** | | |
| 開發及利用記錄管理系統以處理客戶查閱及改正個人資料的要求。 | ✓ | |

| 保護個人識別資料的良好作業模式 | 雲端服務供應商擔任資料使用者的角色 | 雲端服務供應商擔任資料處理者的角色 |
|---|---|---|
| **分判商的管理** | | |
| 只有在提供所需服務的情況下，才可以把客戶的個人識別資料向分判商披露。分判商不得使用個人識別資料作任何其他用途。 | ✓ | ✓ |
| 對於處理儲存在雲端平台上的個人識別資料的分判商或任何第三方，規定他們須制訂適切的資訊科技保安機制及相關程序。 | ✓ | ✓ |
| 監察所有可查閱儲存於雲端平台上的個人識別資料的分判商，並備存一份載列該等分判商的清單。 | ✓ | ✓ |
| **員工管理** | | |
| 就儲存在雲端平台上的個人識別資料而言，應訂明員工在資源控制上所擔任的工作和職責。例如，指定一名管理人員負責執行決策，授權查閱儲存在雲端平台上的個人識別資料。 | ✓ | ✓ |
| 指派員工處理儲存在雲端平台上的個人識別資料及採用職務分工原則。 | ✓ | ✓ |
| 制訂嚴格的密碼政策及確保員工沒有使用共用帳戶。 | ✓ | ✓ |
| 根據個別員工的職責，定期覆檢他們的查閱權限，以確定或重新確定其是否適合進行查閱。例如，當機構內某名員工離職或調任到機構的其他單位，該員的所有查閱權限及帳戶必須予以撤銷。 | ✓ | ✓ |
| 向負責處理儲存在雲端平台上的個人識別資料的員工提供充足的指導及培訓。 | ✓ | ✓ |

## 參考資料

1. 參考 http://www.pcpd.org.hk/chinese/publications/files/dataprocessors_c.pdf
   有關個人資料私隱專員公署出版的《外判個人資料的處理予資料處理者》資料單張
2. 參考 http://www.hkcs.org.hk/en_hk/home/publication/PDPO/
   有關個人資料私隱專員公署出版的《IT 管理層及專業人員「個人資料（私隱）條例」實用指南》
3. 參考 http://www.pcpd.org.hk/chinese/ordinance/ordglance1.html#dataprotect
   有關《個人資料(私隱)條例》的保障資料原則
4. 參考 http://www.pcpd.org.hk/chinese/publications/files/PIAleaflet_c.pdf
   有關個人資料私隱專員公署出版的《私隱影響評估》資料單張

如需要進一步資料，請瀏覽我們的網站：
**www.infocloud.gov.hk**

*「雲資訊網」是一站式入門網站，由雲端運算服務和標準專家小組建立，方便市民和企業（特別是中小企）有效取得有關雲端運算技術的資訊和資源。該網站提供用例、相關指引和良好作業模式，讓市民和企業在採用雲端運算模式時達到預期效益。*

*雲端運算服務和標準專家小組由香港特區政府屬下的政府資訊科技總監辦公室成立，透過廣納業界、學術界、專業團體及政府的專業知識，推動香港雲端運算的應用和發展，以及促進本港雲端運算專家彼此交流及與內地專家互相交流。雲端保安及私隱工作小組是一個在專家小組轄下設立的工作小組。*

*此文件由雲端保安及私隱工作小組發表，載述了有關雲端保安及私隱的良好作業模式和指引。工作小組成員透過通力合作，制訂有關措施，以推動並促進本地業界，更廣泛應用雲端運算和安全使用雲端服務。*