雲端運算指引

引言

本指引重點指出機構採用雲端運算時應考慮的因素。本指引闡釋《個人資料（私隱）條例》（條例）適用於雲端運算的相關要求，並提醒機構採用雲端運算時徹底評估雲端運算的益處、風險及了解其對保障個人資料私隱的影響。

何謂雲端運算？

「雲端運算」並沒有一個普遍認定的定義。一般而言，雲端運算模式能讓用戶隨時隨地、便捷地按需要透過網絡接達一系列可配置的電腦運算資源（例如網絡、伺服器、儲存器、應用系統及服務），這些資源只需透過少量的管理工作或與服務供應商少量的互動，便能迅速地準備妥當及發布。雲端運算的運作模式在成本上通常是根據使用量及租金來計算，而無需投放任何資本。

雲端運算的採用與條例的相關要求

資料使用者（即採用雲端運算的機構）在持有、處理[1]或使用[2]個人資料時須依從條例的規定，包括附表1的**保障資料原則**。在聘用雲端服務供應商時，尤其需留意保障資料第**2(3)**、**3**、**4**原則及條例第**65(2)**條的要求。

[1] 「處理」在條例第2條被定義為就個人資料而言，包括將資料修訂、擴增、刪去或重新排列（不論是否藉自動化方法或其他方法）。

[2] 「使用」在條例第2條被定義為就個人資料而言，包括披露或移轉該資料。

保障資料第 2(3) 原則規定，如資料使用者聘用（不論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[3]。

保障資料第 3 原則規定，個人資料不得用於新目的，除非已取得資料當事人或「有關人士」（如條例下的定義，包括父母親或監護人）的訂明同意（即明確及自願的同意，而該同意並無被撤回）。

保障資料第 4(1) 原則規定，資料使用者須採取所有合理地切實可行的步驟，以確保由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：

(a) 該資料的種類及如該等事情發生便能造成的損害；

(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。

保障資料第 4(2) 原則規定，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[4]。

條例**第 65(2) 條**規定，任何作為另一人的代理人並獲該另一人授權（不論是明示或默示，亦不論是事前或事後授權）的人所作出的任何作為或所從事的任何行為，須視為亦是由該另一人作出或從事的。換言之，資料使用者的承辦商（例如雲端服務供應商）所作出的資料外洩或濫用的行為，視乎情況而定，有機會被視為亦是由該資料使用者以及其承辦商作出的。資料使用者亦可能要對其承辦商的作為負上責任。

根據保障資料第 2(3)、3、4 原則及條例第 65(2) 條，資料使用者須保護資料當事人交託予他們的個人資料，防止資料被濫用，不論有關個人資料是否儲存於資料使用者的處所，抑或外判予承辦商或雲端服務供應商。

---

[3] 此規定的詳情可參閱個人資料私隱專員公署發出的《外判個人資料的處理予資料處理者》資料單張 (www.pcpd.org.hk/tc_chi/resources_centre/publications/files/dataprocessors_c.pdf)。

[4] 見註 3。

個人資料私隱的關注及其應對方法

資料使用者必須認識到資料使用者和雲端服務供應商一同承擔保護雲端環境內數據安全的責任。這共同責任不僅體現於資料使用者將個人資料交託予雲端服務供應商之前的初步評估[5]和雲端服務供應商所作的保證[6]，亦包括資料使用者和雲端服務供應商在整個採用雲端服務期間須遵守相關的私隱保障法律和要求。

從資料使用者的角度而言，在使用雲端運算時產生的個人資料私隱問題，主要是就已委托在雲端服務供應商的個人資料，他們失去或缺乏相關資料的使用、保留、刪除及保安的控制權有關。

雲端運算的商業運作模式有以下四項特點，與保障個人資料私隱特別有關，應審慎考慮[7]。這些特點及與之相關的私隱問題的建議解決方法，詳述如下：

I. 服務及部署模式

雲端服務供應商提供的服務模式包括「基礎設施即服務」(Infrastructure as a Service，簡稱為IaaS)、「平台即服務」(Platform as a Service，簡稱為PaaS)，及「軟件即服務」(Software as a Service，簡稱為SaaS)[8]。

使用IaaS及PaaS服務模式的資料使用者傾向保留其對業務運作模式及營業工具的控制。然而，使用SaaS服務模式的資料使用者則必須使用雲端服務供應商提供的軟件，作為其營業工具的一部分。因此，資料使用者可能要調整其運作以使用這些軟件，或依賴雲端服務供應商為其操作這些軟件。在這些情況，資料使用者會較難直接控制他們所負責的個人資料。使用SaaS服務模式的資料使用者需要評估這種安排帶來的風險，並因應實際情況減低風險。雲端服務供應商可能會不時更新其雲端服務，以提供新服務特點或配置。因此，資料使用者應留意有關更新，並作出相應行動，包括更新相關軟件及／或調整適當的配置等。

至於部署模式，私有雲端一般比公共雲端允許資料使用者擁有更多控制權及私隱[9]。擬使用公共雲端的資料使用者應小心評估下述第II至IV段提出的問題，並設法應對。

---

5 資料使用者在進行初步評估時，可考慮利用國際間認可的認證及標準中完善的控制框架。相關例子請參閱本指引有關「ISO標準」及「其他標準」的部份。

6 雲端服務供應商可透過信譽良好的或國際間認可的第三方的證明或認證報告提供保證。

7 資料使用者應留意，在個別情況可能有其他應考慮的問題。資料使用者應小心盡職確保他們遵從條例的規定。

8 提供IaaS或PaaS的雲端服務供應商可分別被視為提供實體伺服器或裝有作業系統的伺服器的承辦商。兩種服務的客戶均需再安裝及管理軟件或應用程式，才能使用服務。SaaS則包括功能性的應用程式，例如客戶關係管理軟件、會計軟件等。

9 私有雲端由雲端服務供應商建立，只供一名客戶使用，通常由該客戶擁有及管理。公共雲端則由雲端服務供應商建立、擁有及管理，供公眾及機構共同使用。

防止未獲准許的或意外的查閱或處理

為防止儲存於雲端的個人資料受未獲准許或意外的查閱、處理、刪除、喪失或使用所影響，資料使用者應考慮實施下述措施：

- **日誌記錄**：資料使用者應保留雲端服務供應商提供的審計追蹤記錄，例如使用者登入記錄和個人資料變更記錄。資料使用者應定期檢視日誌以偵測異常情況。萬一發生未獲准許的查閱，審計追蹤記錄亦有助調查。此類日誌記錄應有足夠的保護，令入侵者無法查閱及更改日誌記錄以作掩飾。

- **適當的使用者配置**：資料使用者應充分了解配置的功能，確保雲端服務的使用權是按實際運作情況恰當地設定。使用權只應給予已獲授權的人士，尤其是在運作上有職責需要使用雲端服務的人士。

- **分隔**：分隔技術可以確保資料使用者的資料不會被相同雲端平台的其他客戶查閱或影響。資料使用者應考慮雲端服務供應商實施的措施是否能有效確保：

  (1) 資料使用者能夠控制儲存在雲端的個人資料的查閱權限；及

  (2) 他們的資料和雲端服務受到保護，免受同一個雲端服務供應商的另一名客戶所執行的惡意軟件侵害。

  為加強保障，資料使用者可以考慮利用雲端服務供應商提供的邏輯隔離及客戶共用的運算服務。

- **傳輸及靜態加密**：不受保護的數據在傳輸過程或靜態時都可能使機構面臨風險。由於雲端運算透過互聯網提供服務，個人資料應在傳輸過程中加密，防止遭竊聽或中間人攻擊。為保護靜態數據，儲存在雲端上的個人資料亦應加密，以防止攻擊者未經授權的存取。私隱專員公署亦建議資料使用者可選擇提供靜態加密服務的雲端服務供應商。

  此外，用作加密傳輸過程和儲存個人資料的密鑰必須得到充分保護和審慎管理，以避免未經授權的人可輕易查閱。如資料使用者希望加強管控，他們應考慮實施只有資料使用者（而非雲端服務供應商）才可解密及查看個人資料的加密方法。

- **多重身份認證**：應考慮盡量為帳戶（尤其是特權帳戶）啟用多重身份認證功能。登入步驟可以包括下述兩個不同因素以增強安全性：
  - 你所知道的資訊－例如密碼或安全問題的答案
  - 你擁有的東西－例如保安編碼器或智能卡

- **匿名化**：匿名化為儲存於雲端的個人資料提供一層額外的保護。把個人資料匿名化，是指從數據集移除當中任何人讀取後，足以識別某人身份的資料，當中亦涉及考慮被重新識別身份的風險。

- **備份**：雲端服務供應商應制定有效的備份和復原策略和程序。如資料使用者認為儲存在雲端的個人資料重要，資料使用者應確保他們可以從雲端服務供應商取得營運資料離線備份副本，以便在需要時進行復原。

- **修補程式管理**：根據雲端服務供應商提供的服務及部署模式，資料使用者應確保其雲端服務供應商有適當的修補程式管理流程來識別、評估、驗證和應用必要的修補程式和安全更新，以保護儲存在雲端上的個人資料。

II. 標準服務及合約

有些雲端服務供應商以薄利多銷形式營運，只會以標準合約條款向客戶提供少量指定的服務。

資料使用者如聘用只提供標準服務及不可協商合約條款的雲端服務供應商時，必須小心評估有關服務及合約條款是否完全符合所需的保安及個人資料私隱保障這兩方面的標準。如所提供的保障與所需要的標準存在差距，資料使用者便須處理相關不足。

例如，使用雲端服務的資料使用者應考慮以下問題：

- **如雲端服務供應商的標準保安程度或所承諾的個人資料保障未能符合資料使用者的要求，資料使用者應要求供應商調整服務及協商合約條款，以達到有關要求。**如資料使用者未能處理相關不足，將會承受資料外洩及被濫用的風險及後果，包括受規管機構審查及聲譽受損。

- **資料使用者應決定以甚麼方式核實雲端服務供應商承諾提供的資料保障及保安措施。**若資料使用者有權審核雲端服務供應商的營運，便可直接掌握供應商遵守相關個人資料私隱要求的情況。由於很多時候這並非切實可行，資料使用者便需考慮雲端服務供應商所提供的審計報告或聲明，資料使用者應小心審視這些報告或聲明的範疇、相關性、可靠性及真實性。

III. 外判安排

為可以極快地取得所需的容量，以滿足客戶不斷變化的運算需要，雲端服務供應商可能會聘用承判商，而這些承判商可能會再聘用自己的分包商。為保持商業靈活性，部分雲端服務供應商的外判安排可能會以寬鬆的合約或非正式的合作方式來進行。

使用雲端服務的資料使用者應留意這些安排，確保分包商遵從資料保障規定。

使用雲端服務的資料使用者應考慮以下問題：

- **資料使用者需要確定雲端服務供應商是否有外判安排。**如有外判安排，資料使用者應確保獲得雲端服務供應商在合約內承諾，其保障（技術及行政）及循規管控（監察及補救行動）的水平同樣適用於其分包商。如雲端服務供應商因外判商違反了資料使用者與雲端服務供應商之間的協議所規定的條款，雲端服務供應商須對資料使用者負責。

IV. 跨境資料轉移

在多個司法管轄區設有數據中心的雲端服務供應商，可能會為優化儲存及運算資源，而將受託的個人資料由一個司法管轄區轉移至另一司法管轄區儲存及處理。由於處理儲存於離岸數據中心或在離岸數據中心之間轉移的個人資料可能受到離岸數據中心所屬司法管轄區的法律所規管，在決定是否在離岸數據中心儲存或處理個人資料前，應慎重考慮。

就香港而言，當資料使用者將個人資料轉移至香港以外地方時，仍須遵守條例的相關規定，包括六個保障資料原則。尤其是：

(a) 如資料使用者擬將個人資料轉移至香港境外的雲端伺服器，在直接向資料當事人收集個人資料時，應採取所有切實可行的步驟，確保資料當事人獲明確告知其個人資料可能轉移至甚麼類別的人（即香港境外的資料接收者），以及資料將會用於甚麼目的（保障資料第1原則）。

(b) 如個人資料是為新目的[10]而轉移至香港以外地方，除非該轉移屬於條例第8部的豁免範圍，否則該轉移必須取得資料當事人的訂明同意[11]（保障資料第3原則）。

如資料使用者聘用資料處理者，以代該資料使用者在香港以外地方處理個人資料，資料使用者須採取合約規範方法或其他方法保障個人資料，以(i)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）；以及(ii)防止該資料受未獲准許的或意外的查閱、處理、刪除、喪失或使用（保障資料第4(2)原則）。

資料使用者可參考以下個人資料私隱專員公署（私隱專員公署）有關跨境轉移個人資料的指引：

(a)《跨境資料轉移指引：建議合約條文範本》[12]（2022年指引）（2022年出版），包括載於其附表內的兩套建議合約條文範本，其中包含跨境資料轉移的核心條文，此範本可供中小企業採用；

(b)《保障個人資料：跨境資料轉移指引》[13]（2014年出版），包括載於其附表內的建議條文範本，其中包含更廣泛的跨境資料轉移合約條款，除2022年指引所包含的核心條文外，這些條款較適合涉及複雜的跨境個人資料轉移的跨國公司或機構採用；及

(c) 跨境資料轉移指引：《粵港澳大灣區（內地、香港）個人信息跨境流動標準合同》[14]（2023年出版），包括載於其附表內的標準合同，其中包含資料使用者擬將個人資料轉移至註冊於（適用於組織）或位於（適用於個人）粵港澳大灣區九個內地城市的接收方時可採用的合約條文[15]。

---

10 「新目的」指原先收集資料時擬使用或與其直接有關的目的以外之任何目的。

11 「訂明同意」指資料當事人明確和自願給予及沒有以書面撤回的同意。

12 可於此網站下載：https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/guidance_model_contractual_clauses.pdf

13 可於此網站下載：https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/GN_crossborder_c.pdf

14 可於此網站下載：https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/standard_contract_gba.pdf

15 如資料使用者（註冊於或位於香港）及其雲端服務供應商（註冊於或位於大灣區）擬將個人資料由香港轉移至大灣區任何一個內地城市，私隱專員公署鼓勵雙方考慮採用標準合同進行相關的轉移。

此外，使用雲端服務的資料使用者應考慮以下問題：

- **雲端服務供應商應向資料使用者披露資料將會儲存或處理的地點／司法管轄區，讓資料使用者從而也能清楚告知資料當事人。**同時，資料使用者要就這樣的儲存或處理安排，考慮其保障個人資料私隱的責任。例如，於另一司法管轄區儲存或處理的個人資料須受該司法管轄區的法律規管；而在該司法管轄區的執法機構查閱有關資料方面，未必有與香港相同的保障。資料使用者與雲端服務供應商在合約中所訂的查閱資料限制，亦不能凌駕於該司法管轄區的法律之上。

- **資料使用者所選擇的雲端服務供應商，應該是可以讓他們揀選或指定具有足夠法律／監管保障個人資料私隱的司法管轄區**（例如，該等司法管轄區的監管機制與香港大致相同，以及有司法程序監管執法機構，以保障資料不受任意或不合法查閱）。

將個人資料交託予資料使用者的資料當事人應知悉有關跨境安排及其個人資料將如何受到保障。

其他外判事宜

由於聘用雲端服務供應商亦可被視為其中一種外判安排，資料使用者也應留意下述有關外判的一般事宜：

- 資料使用者對保障所收集及持有的個人資料需要負上最終責任。**把個人資料的處理或儲存外判給第三者，不會減低資料使用者對保障所收集、持有、處理及使用的個人資料的法律責任。**因此，任何雲端服務合約都不適宜讓雲端服務供應商可以單方面更改條款及條件以提供較低保障的標準，或減免責任。

- **根據條例，資料使用者的責任包括按客戶要求供客戶查閱其個人資料、處理客戶的改正要求，以及解決問題和處理投訴。**因此，資料使用者必須確保他與雲端服務供應商簽訂的合約容許他履行這些責任。

- **資料使用者應確保在與雲端服務供應商簽訂的合約中，有條文限制個人資料**（包括雲端服務供應商在履行合約期間可能收集的其他個人資料）**只可用於資料使用者當初收集資料時的目的或直接有關的目的。**

- **在選擇雲端服務供應商時，資料使用者應謹慎考慮雲端服務供應商使用的實體硬件和雲端環境方面的安全，以確保數據受充分保護。資料使用者應從雲端服務供應商取得相關的保證或國際認可的第三方提供的認證報告。**一旦資料使用者轉移資料至並非由其管理的數據中心，資料的保安控制權將轉移至雲端服務供應商。任何能進入數據中心的人士都有機會接觸到持有客戶數據的實體裝置。私隱專員公署建議資料使用者仔細評估雲端服務供應商的基礎架構和運作有效性，以滿足資料使用者的安全要求。

- **資料使用者應確保合約中有條文列明雲端服務供應商在資料使用者作出要求後、或在合約完結或終止時，刪除或交還持有的個人資料予資料使用者。**

- **資料使用者應在與雲端服務供應商簽訂的合約中加入條文，規定雲端服務供應商有責任及時向資料使用者通報資料外洩事件。**強制雲端服務供應商作出通報，可讓資料使用者適時地處理資料外洩事件，包括向私隱專員公署及受影響的資料當事人作出資料外洩事故通報、迅速作出補救工作及維護業務的持續性。這有助資料使用者履行法律責任，以及有效地處理客戶及公關的工作。資料使用者亦應確保雲端服務供應商的承辦商及分包商（如適用）遵從這項規定。

- **資料使用者須確保其《收集個人資料聲明》及／或《私隱政策聲明》以清楚易明的方式，通知客戶他們會把個人資料的儲存及／或處理外判予雲端服務供應商，其個人資料可能會在另一司法管轄區儲存或處理。**

- **如轉移至雲端服務供應商的個人資料會在香港以外的司法管轄區儲存或處理，資料使用者應確保有關的跨境資料轉移符合相關司法管轄區資料保護法的跨境要求，並在有需要時尋求專業法律意見。**

- 不論個人資料是由資料使用者或雲端服務供應商管理或持有，資料使用者應確保個人資料會獲得相類似的保障。

ISO標準

國際標準組織(ISO)推出了多套適用於使用雲端服務的標準：

(i) 《ISO/IEC 27018:2019資訊科技－安全技術－個人可識別訊息處理者在公共雲端保障個人可識別訊息實務守則》於2019年修訂[16]，並根據ISO/IEC 29100公共雲端運算環境中的私隱原則，制定獲廣泛認可的控制目標、控制措施及指引，以保障個人可識別訊息。這套標準亦就《ISO/IEC 27002:2022資訊安全、網路安全及私隱保障資訊保安控制》[17]所定義的14項保安種類[18]，及《ISO/IEC 29100:2024資訊科技－安全技術－私隱框架》[19]所述的11項私隱原則[20]，提供適用於雲端服務供應商的具體指引。

(ii) 《ISO/IEC 27017:2015基於ISO/IEC 27002的資訊技術－安全技術－雲端服務資訊保安控制實務守則》於2021年修訂，包含適用於雲端服務的提供和使用的資訊保安控制指引[21]。

(iii) 《ISO/IEC 27701:2019安全技術－延伸ISO/IEC 27001和ISO/IEC 27002的私隱資訊管理－要求和指引》於2019年推出，以延伸ISO/IEC 27001和ISO/IEC 27002的形式，訂定建立、實施、維護和持續改進私隱資訊管理系統的要求並提供指引，以在機構內進行私隱管理[22]。

(iv) 《ISO/IEC 27001:2022資訊安全、網絡安全及私隱保障－資訊保安管理系統－要求》於2022年修訂，訂定在各行業各規模的機構建立、實施、維護和持續改進資訊保安管理系統的要求並提供指引，亦包括因應機構的需要而評估和處理資訊保安風險的要求[23]。

私隱專員公署建議資料使用者遵從相關的ISO標準，而視乎個案情況，私隱專員公署在評估資料使用者是否有遵守條例時會考慮他們是否已遵從相關的標準。

---

16 *"ISO/IEC 27018:2019, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors"*：https://www.iso.org/standard/76559.html

17 *"ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection – Information security controls"*：https://www.iso.org/standard/75652.html

18 即1.資訊保安政策、2.資訊保安架構、3.人力資源保安、4.資產管理、5.查閱控制、6.密碼技術、7.實體及環境保安、8.運作保安、9.通訊保安、10.系統採購、開發及維修、11.供應商關係、12.資訊保安事故管理、13.商業持續管理的資訊保安及14.符規。

19 *"ISO/IEC 29100:2024, Information technology – Security techniques – Privacy framework"*：https://www.iso.org/standard/85938.html

20 即1.同意及選擇、2.目的合法性及說明、3.收集限制、4.資料最少性、5.使用、保留及披露限制、6.準確性及質素、7.透明度及通知、8.個人參與及查閱、9.問責性、10.資訊保安及11.私隱符規。

21 *"ISO/IEC 27017:2015, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services"*：https://www.iso.org/standard/43757.html

22 *"ISO/IEC 27701:2019, Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines"*：https://www.iso.org/standard/71670.html

23 *"ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements"*：https://www.iso.org/standard/27001

其他標準

除上述ISO標準外，其他可能適用於使用雲端運算的標準包括[24]：

(i) 由內地當局發布的GB/T 31167-2023《信息安全技術　雲計算服務安全指南》；

(ii) 由內地當局發布的GB/T 31168-2023《信息安全技術　雲計算服務安全能力要求》；

(iii) 美國商務部國家標準與技術研究院發布的標準，例如《公共雲端運算安全和私隱指引》[25]；及

(iv) 新加坡標準理事會轄下新加坡資訊技術標準委員會(Information Technology Standards Committee)發布的標準，例如SS 584:2020多層雲端運算安全標準(Specification for Multi-Tiered Cloud Computing Security)[26]。

本單張的範疇未能涵蓋上述標準的所有細節。資料使用者可進一步查閱有關標準，參考相關細節，如有需要亦可尋求專家的意見。

[24] 資料使用者亦可留意美國會計師協會發布的「系統與組織控制」(SOC)的相關要求。SOC為美國註冊會計師就服務組織的系統層級控制措施或其他組織的組織層級控制措施訂定一套報告。相關SOC報告會於審計組織內部控制措施時製作，以提供與該措施有關的資訊及保證：https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

[25] https://www.nist.gov/publications/guidelines-security-and-privacy-public-cloud-computing

[26] https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/industry-committees-and-working-groups/it-standards-committee

私隱專員公署網頁
pcpd.org.hk

下載本刊物

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

電話 ： **2827 2827**
傳真 ： **2877 7026**
地址 ： **香港灣仔皇后大道東248號大新金融中心13樓1303室**
電郵 ： **communications@pcpd.org.hk**

二零二五年一月（第二修訂版）