雲端運算

本資料單張旨在向有意採用雲端運算的機構提供應考慮的因素。本資料單張闡釋《個人資料(私隱)條例》(「條例」)與雲端運算的相關性，並指出資料使用者採用雲端運算時徹底評估其利益、風險及了解保障個人資料的重要性。

何謂雲端運算？

「雲端運算」並沒有一個獲普遍接受的定義。就本單張而言，雲端運算指以最少的管理需求或服務供應商的介入，將一些可按需求提供、可分享及可配置的電腦資源快速地提供予客戶。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

資料使用者須依從條例的規定，包括附表1的保障資料原則。在聘用雲端服務供應商時，保障資料**第2(3)**、**3**、**4原則**及條例**第65(2)條**尤其相關。

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[1]。

保障資料第3原則規定，個人資料不應用於新目的，除非已取得資料當事人或其「有關人士」(如條例下的定義)的訂明同意(即明確及自願的同意)。

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。

[1] 此規定的詳情可參閱個人資料私隱專員發出的《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)

保障資料第4(2)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[2]。

條例第65(2)條規定，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，會被視為亦是由該資料使用者及其承辦商作出的。換言之，資料使用者須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。

個人資料私隱的關注及其應對方法

資料使用者在使用雲端運算中產生的個人資料私隱問題，主要是與其使用，保留，刪除及保安失去或缺乏控制該等個人資料有關。

從保障個人資料私隱的角度而言，雲端運算的商業運作模式有以下四項與控制有關的特點，尤其值得關注[3]。

採用雲端服務的資料使用者把個人資料交託予雲端服務供應商前，應確保有關供應商能有效地處理這些問題。

這些特點及應該如何處理，詳述如下 ：

I. 快速的跨境資料轉移

在多個管轄區設有數據中心的雲端服務供應商，可能會以程式去優化盡用剩餘的儲存及運算資源，而將受託的個人資料由一個管轄區轉移至另一管轄區儲放及處理。

條例第33條有關限制將個人資料移轉至香港以外地方的條文尚未生效。不過，位處香港的資料使用者把他們收集的個人資料移轉至香港以外地方，他們應確保有關資料可獲得一如在香港的同樣類似程度保障，以符合資料當事人把個人資料交託予他們的的期望。此外，資料當事人亦應獲告知資料的跨境安排，以知悉其個人資料會獲得怎樣的保障[4]。

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客戶資料將會儲存的地點／管轄區，讓資料使用者從而也清楚告知資料當事人。資料使用者需要就這樣的儲存安排，考慮其對客戶的個人資料私隱的責任。例如，儲存於另一國家的個人資料須受該管轄區的法律規管 ；而在該管轄區的執法機構查閱有關資料方面，有關資料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，亦不能凌駕於該管轄區的法律之上。
- 資料使用者應選擇一些雲端服務供應商，而這些供應商是可以讓他們揀選／指定具有足夠法律／監管保障個人資料私隱的管轄區（例如，其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查閱）。

[2] 見註1
[3] 資料使用者應留意，這些問題並非徹底及毫無遺漏的。資料使用者應小心確保他們遵從條例的規定。
[4] 詳情可參閱個人資料私隱專員發出的《保障個人資料：跨境資料轉移指引》(www.pcpd.org.hk/tc_chi/resources_centre/publications/files/GN_crossborder_c.pdf)

II. 寬鬆的外判安排

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自己的承判商，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，這些外判安排可能會以寬鬆的合約或合作方式來進行。

使用雲端服務的資料使用者應留意這些安排，確保分包商仍有效地遵從資料保障規定。

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）及循規控制（監察及補救行動）的程度，同樣適用於其分包商。

III. 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，因此只會以標準合約條款向客戶提供少量的服務。

資料使用者如聘用只提供標準服務及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存在差距，資料使用者便須處理。

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客戶的要求，資料使用者應要求供應商調整服務／合約條款，以達到有關要求。如資料使用者未能處理這差距，會承受資料外洩及被濫用的風險，並在發生事故後受規管機構審查。
- 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，便可直接掌握循規的情況。但很多時這並不可能，資料使用者便只能接受雲端服務供應商提供的審計報告或其聲明，惟資料使用者仍需審視這些報告或聲稱的範疇、相關性及適用性。

IV. 服務及調配模式

雲端服務供應商通常以「基礎設施即服務」（即Infrastructure as a Service，簡稱為IaaS）、「平台即服務」（即Platform as a Service，簡稱為PaaS），及「軟件即服務」（即Software as a Service，簡稱為SaaS）的形式提供服務[5]。使用IaaS及PaaS服務模式的資料使用者傾向保留對其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可能要調整其運作，或依賴雲端服務供應商為其提供及／或操作部分營業工具或軟件。在這些情況，資料使用者對其負責的個人資料會較難直接控制。使用SaaS服務模式的資料使用者需要量化這種安排帶來的風險 ；並因應實際情況，減低影響。

資料使用者一般對私有雲端的控制較公共雲端的為多[6]。因此，擬使用公共雲端的資料使用者應小心評估上述第I至III段提出的問題，並設法應對。

[5] 提供IaaS或PaaS的雲端服務供應商可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使用應用程式，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。

[6] 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。

其他外判事宜

由於聘用雲端服務供應商都是外判安排的其中一種形式，資料使用者亦應留意下述有關外判的事宜：

- 資料使用者是保障所收集及持有個人資料最終負責的一方。把個人資料的處理或儲存外判給第三者，是不會免除資料使用者對保障所收集及持有的個人資料的法律責任。此外，如雲端服務供應商可以單方面更改合約以調低保障的標準，或減免責任，均會造成問題；
- 根據條例，資料使用者的責任包括容許客戶查閱其個人資料、要求作出改正，解決問題和處理投訴。因此，資料使用者必須確保它與雲端服務供應商簽訂的合約容許其履行這些責任；
- 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（及雲端服務供應商在合約期間可能收集的任何其他個人資料）只可用於收集資料時的原本目的或直接有關的目的；
- 資料使用者亦應確保合約中有條文列明在資料使用者作出要求後、合約完結或終止後，如何把個人資料刪除及／或交還資料使用者；
- 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，包括確保能迅速補救、繼續業務、履行法律責任、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／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，通知客戶他們有意把個人資料的處理外判予雲端服務供應商，其個人資料可能會在另一管轄區儲存或處理，及可能會被該管轄區的執法機構及國家安全機構查閱；
- 不論個人資料是由資料使用者抑或雲端服務供應商管理／持有，資料使用者應確保個人資料會獲得同等程度的保障。如資料使用者不能直接監察所有必要的控制措施以保障個人資料，他們應認真考慮在採用雲端服務時實施端到端、全面及獲妥善管理的加密系統[7]，以傳輸及儲存個人資料。

ISO標準

國際標準組織(ISO)於2014年8月推出《ISO/IEC 27018個人可識別訊息處理者在公共雲端保障實務守則》（「ISO 27018標準」）[8]。

ISO 27018標準是針對個人資料私隱保障的一般原則及關注範疇而制定。這套標準就廣為接受的資訊科技保安標準《ISO 27002資訊保安控制實務守則》所定義的14項保安種類[9]，及「ISO 29100私隱框架」[10]所述的11項私隱原則[11]，提供適用於雲端服務供應商的具體指引。

7 端到端加密指只限資料使用者（不是雲端服務供應商）可以解密及查看資料的加密系統。
8 www.iso.org/iso/catalogue_detail?csnumber=61498
9 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。
10 www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123
11 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。

本單張的範疇未能涵蓋ISO 27018標準的所有細節。有興趣人士可自行了解該標準的詳情。然而，資料使用者在聘用聲稱已依從這標準的雲端服務供應商時，必須了解ISO 27018標準的限制及適用範圍。

雖然ISO 27018標準解決了本單張提出的關注問題，但並不表示資料使用者聘用依從ISO 27018標準及獲認可的雲端服務供應商，便可保證其服務是符合條例要求。因為ISO 27018標準在某些方面只述明需要處理甚麼，但沒有提及處理的方法。

ISO 27018標準還需時間才能被理解和普及應用。然而，這標準的出現，能協助資料使用者揀選雲端服務供應商，滿足了在這方面對綜合參考的需要。

香港個人資料私隱專員公署
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12樓
網址 ： www.pcpd.org.hk
電郵 ： enquiry@pcpd.org.hk