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

資料單張

雲端運算

引言

本資料單張旨在向有意採用雲端運算的機構就應考慮的因素提供意見。本資料單張闡釋雲端運算的商業模式與《個人資料(私隱)條例》(下稱「條例」)之間的關係，重點指出資料使用者徹底評估雲端運算對私隱及資料保障的利益、風險及影響的重要性。

何謂雲端運算？

「雲端運算」並沒有一個獲普遍接受的定義，但一般是指以最少的管理工作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。雲端運算的成本模式通常是根據使用及租賃情況而定，而不需要任何資本性的投資。

雲端運算的服務模型式通常有三種：「基建設施即服務」(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**)。

IaaS - 雲端服務供應商向客戶提供基本運算基建(例如中央處理器、網絡頻寬及儲存容量)，客戶則負責自行安裝作業系統及應用程式。

PaaS - 雲端服務供應商向客戶提供基本運算基建及平台(例如作業系統、資料庫及網絡伺服器)，客戶則負責自行安裝應用程式。

SaaS - 雲端服務供應商向客戶提供基本運算基建、平台及應用程式(例如電郵系統、人力資源及客戶關係管理系統)，客戶純粹使用該等應用程式。

在調配方面，雲端運算有下述模型式：

私有 - 私有雲端只供一名客戶或實體使用，可以由客戶、雲端供應商或兩者結合擁有、管理及/或營運。雲端設置在客戶的處所與否皆可。

社群 - 社群雲端是為一群擁有共同關注(例如對政策、保安及循規)的客戶或實體而設，可以由社群中一名或以上的客戶、雲端供應商或兩者結合擁有、管理及/或營運。雲端設置在客戶的處所與否皆可。

公共 - 公共雲端只供公眾(包括機構)使用，可以由一個雲端供應商、一間機構或兩者結合擁有、管理及/或營運。雲端通常設置在服務供應商的處所。

混合 – 混合雲端是私人、社群及/或公共雲端模型的結合，以達成災難復原的目的或處理容量滿溢的問題。

無論採用哪一種雲端服務或調配模型式，如雲端所儲存的資料包含個人資料，資料使用者便有責任根據條例的規定，保障個人資料的安全。

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。

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。

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。

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，須被視為亦是由該資料使用者作出的。

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。

個人資料私隱關注

從保障個人資料私隱的角度而言，雲端運算以下的一些商業模式的特點 (而非其服務模式或相關技術)尤其值得關注的：

1. ***迅速的跨境資料轉移***

在多個管轄區擁有數據中心的雲端服務供應商，會以程式去優化盡用剩餘的儲存及運算資源，因此受託的個人資料可能會定期由一個管轄區流游至另一管轄區。

2. ***寬鬆的外判安排***

雲端服務供應商可能會聘用自己的承辦商，而這些承辦商可能會再聘用自己的分包商，以便極快地取得所需的容量，滿足客戶不斷變化的運算需要。為保持商業靈活性，此等外包安排可能會以寬鬆的合約或合作方式來維持。

3. ***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，因此只向客戶提供少數類型的標準服務合約。

客戶在考慮採用雲端運算時應注意或了解甚麼？

資料使用者在考慮把個人資料儲存到雲端時，不論採用甚麼服務或調配模式時，他們至少應確保他們已考慮過下述事宜。由於雲端運算技術及有關市場正不斷演變及成長，並非所有雲端服務供應商皆可以有效地處理下述事宜及提供令人滿意的解決方案。有意採用雲端運算的客戶把個人資料交託予雲端服務供應商前，應向他們了解下述事宜。資料使用者應留意，下述事宜並非包羅無遺。資料使用者必須因應雲端運算的特點及功能，謹慎尋找遵從條例規定的最佳方式。

1. ***迅速的資料跨境轉移***

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，如以香港為基地的資料使用者容許他們所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獲得猶如資料是在香港一樣相類似程度的保障，以符合資料當事人把個人資料交託予他們的的預期。此外，資料當事人亦應獲告知資料的跨境安排，以了解其個人資料會如何被保障。

有意使用雲端服務的客戶應考慮以下幾點：

1.1 雲端服務供應商能否披露資料將會被儲存的地點/管轄區，讓資料當事人清楚知悉？資料當事人是否知道如此儲存的影響(例如，被移轉至另一國家的個人資料須受該管轄區的法律規管；不論合約訂得如何完善，亦不能凌駕於該外國管轄區的法律之上)？

1.2 雲端服務的客戶能否指定個人資料只可以被儲存於他們合理地肯定具有足夠法律/監管保障的管轄區(例如，其監管機制與香港大致相同嗎)？

1.3 雲端服務的客戶是否知道海外執法機構如何可以查閱其管轄區內雲端所儲存的資料？他們知否這些機構有否司法程序需要經過特定的監管，以保障資料不受任意查閱？

2. ***寬鬆的外判安排***

雲端服務供應商普遍會透過承包及分包提供服務。使用雲端服務的資料使用者應留意此等安排，確保資料保障規定仍有效地獲得遵從。

有意使用雲端服務的客戶應考慮以下幾點：

2.1 雲端服務供應商有否與其他承辦商有分包安排？這些承辦商會否把其工作再分包給其他人？這些雲端服務供應商及其承辦商/分包商的哪些僱員可以查閱雲端所儲存的個人資料？查閱資料是否只限於「有需要」的原則？是否設有適當的登入/存取控制(及穩固的日誌記錄)？有甚麼措施以確保這些承辦商/分包商及其僱員遵從保障資料原則的規定？

2.2 如有分包安排，這些分包商會否有效地遵從客戶與雲端服務供應商的合約中的所有保障資料原則規定？

2.3 雲端服務的客戶可以如何確保分包商會如雲端服務供應商般對雲端上的個人資料提供同樣的保障？

2.4 如承辦商/分包商沒有保護其雲端上的個人資料，是否須按合約作出補救或受當地規管機構的制裁？

3. ***標準服務及合約***

資料使用者如聘用只提供標準服務及合約的雲端服務供應商時，必須小心評估有關服務及合約是否完全符合所需的保安及個人資料私隱保障兩方面的標準。如所提供的與所需要的存在差距，資料使用者必須有方法處理這差距。

有意使用雲端服務的客戶應考慮以下幾點：

3.1 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，該供應商會否調整其服務，以符合客戶的要求？

3.2 雲端服務的客戶可以採取甚麼切實可行的步驟，以確保雲端服務供應商會兌現其就保安或個人資料保障的承諾？該供應商會否對其措施及程序提供獨立驗證，以確保這些措施及程序符合合約的規定？

4. ***其他外判事宜***

上述的關注主要針對雲端服務供應商的外判安排。由於聘用雲端服務供應商亦屬於外判安排的其中一個形式，資料使用者亦應留意下述有關外判的一般事宜。

4.1 一般來說，資料使用者只可對雲端服務供應商執行雲端服務合約的條文，而不可對該雲端供應商的承辦商/分包商這樣做；

4.2 資料使用者是最終負責保障所收集及持有的個人資料的一方。把個人資料的處理或儲存外判予第三者，是不會減低資料使用者對保障所收集及持有的個人資料的法律責任。如雲端服務供應商可以單方面更改合約或限制其責任，將會令安排出現更多問題；

4.3 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，及解決問題和投訴。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它履行這些責任；

4.4 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；

4.5 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行動/要求後、合約完結或終止後，會如何把個人資料刪除及/或交還資料使用者(或其替代供應商)；

4.6 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，包括確保作出迅速補救、繼續業務、履行法律責任及進行公關工作。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。

4.7 資料使用者應確保其《收集個人資料聲明》及/或私隱政策聲明(或同等文件)以清楚易明的方式，通知資料當事人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；

4.8 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督保障個人資料所必需的所有控制措施，他們應認真考慮在採用雲端服務時實施全面及妥善管理的加密系統，以傳輸及儲存個人資料。

此外，為協助資料使用者在外判個人資料的處理時遵從保障資料第 2(3) 及 4(2) 原則的規定，私隱專員發出了《外判個人資料的處理予資料處理者》資料單張[1]，資料使用者應予以參考。

[1] 請參閱 http://www.pcpd.org.hk/chinese/publications/files/dataprocessors_c.pdf

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 12 樓
網址：www.pcpd.org.hk
電郵：enquiry@pcpd.org.hk