ISO/IEC 27018

公有雲個人資料(PII)處理者之個資保護作業規範

常見問答

ISO/ IEC 27018 是第一個為在公有雲上保護個人資料（PII：Personal Identifiable Inforam-tion）所提供的專業國際標準。BSI 台灣已開始提供 ISO/ IEC 27018 的驗證服務。

Q 什麼是 ISO/IEC 27018?

A ISO/IEC 27018 是第一個針對雲端服務提供商如何於公共雲保護個人資料的國際標準。通過 ISO/IEC 27018 驗證的雲端服務提供商得以宣告在此國際標準的架構基礎下，不論個人資料的蒐集限制、正確性及透明性等各方面均受到保護。

Q 將個人資料存放在雲端風險大嗎?

A 在沒有可信賴的驗證機制下，風險是無法評估的。由於業者藉由外包來抑制成本的作法相當普遍，個人資料存放在何處以及雲端服務提供商是否遵照契約內容執行等議題都不夠透明，無法有效建立使用者對於雲端服務的信賴感，如：個人資料的處理會不會再向外轉包? 個人資料有沒有對外揭露?

Q 要取得 ISO/IEC 27018 驗證必需具備哪些條件?

A 由雲端服務提供商管理的資訊不應僅被視為單純的資料，而應考慮「含有個人資料」的情況下能否合理的運用。雖然提供雲端服務的業者日益增長，但多數卻把其所管理的資訊視為單純的資料。ISO/IEC 27018 要求在委託者同意的前提下，其個人資料生命週期的各項歷程均須加以保護。同時，雲端服務提供商有義務對委託者充分說明資料的正確性及透明性等議題。因此，與委託者原意不符的個資蒐集、處理及利用等作業需儘早改善。

Q 接受驗證有哪些好處呢?

A 有鑑於ISO/IEC 27018制定的個資保護規範相當完備，由第三方進行獨立稽核及現場審查雲端服務的管理作為是否嚴格遵循此國際標準，對提升利害關係者的信賴度上是一大優點。

Q 目前全世界有幾家機構取得 ISO/IEC 27018 驗證?

A 國際知名的雲端服務提供商如 Microsoft Azure、Microsoft Office 365、Amazon AWS、Dropbox、香港的Ribose、及日本的TKC等組織已經通過ISO/IEC 27018驗證。

BSI 英國標準協會
+886 2 26560333
infotaiwan@bsigroup.com
www.bsigroup.tw

BSI 訓練學苑
雲端服務之資訊安全
暨個資保護相關課程>
training.taiwan@bsigroup.com

bsi.