以 ISO 27550 落實 GDPR 的隱私工程要求

號稱最嚴格個資法的歐盟 GDPR (General Data Protection Regulation)上路，企業也需開始評估如何藉由標準導入來滿足 GDPR 的要求。

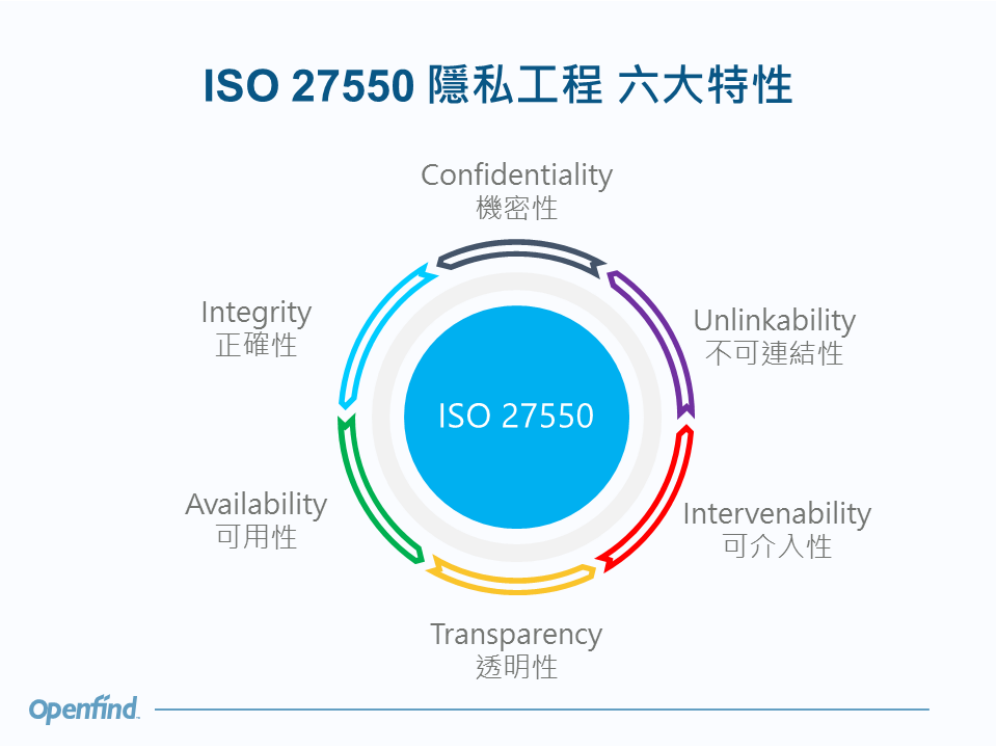
歐盟 GDPR 已在今年 5 月 25 日正式生效。一如資安業者宣導的，並非只有設籍於歐洲的公司才受到限制，而是只要客戶中有歐盟公民的廠商皆會受影響，包括在歐盟地區有設點、有員工；只要有提供歐盟公民服務、有蒐集、處理和利用歐洲公民個資的台灣企業皆無法自外於 GDPR 的管理。有時關係甚至來自意想不到的地方；SGS 台灣資訊治理部門經理何星翰舉例，外銷導向的台灣製造業近來經常被客戶問到他們提供的產品、關鍵元件是否符合隱私設計、隱私工程的概念，以及有沒有可能陷客戶於違反 GDRP 的風險？如果廠商說沒有，又要如何證明？

(SGS 雲端驗證全球產品經理 何星翰)

GDPR 首次將資料保護設計列為資料控管及處理者（Data Controller 和 Data Processor）的法定義務，明確提到產品和服務必須加入資料最小化和可使用擬匿名化等設計。這就涉及隱私設計或隱私工程(Privacy by Design/Privacy by Default)的概念。簡單來說，所有在歐盟提供的服務和產品，預設都必須能確保個人隱私，例如使用者可以要求 Google 搜尋服務刪除有關他／她的資料。根據 GDPR 資料保護原則，廠商必須在事先告知並獲得用戶明顯同意情況下，始得蒐集用戶個資，而且也僅可蒐集特定目的資料種類，不得毫無限制，之後也不能隨意用於其他目的。這些資料也僅得保存一段期限，超過期限的資料必須銷毀。此外，在保存期間，廠商更必須確保用戶個資的完整與機密性，不被他人存取、竄改或毀損。

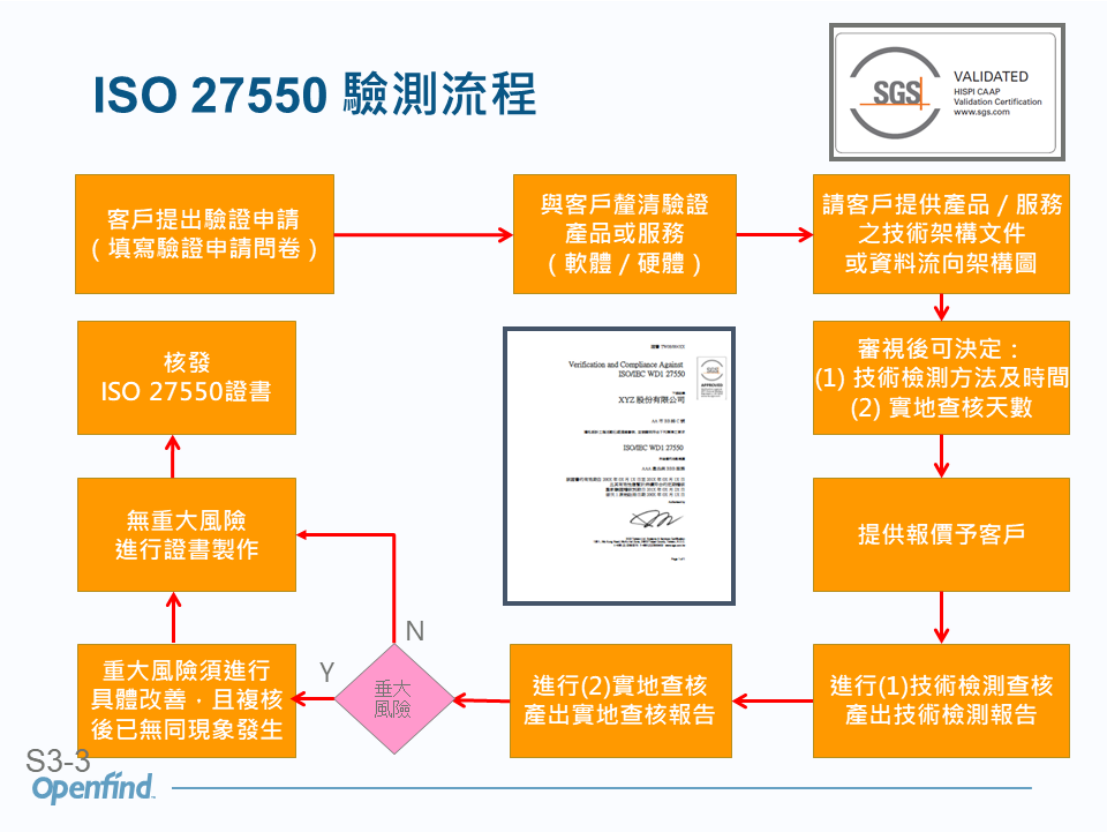
但是對台灣企業而言，想要符合隱私工程其實有頗大挑戰。台灣歷來普遍沒有隱私設計、隱私工程的概念，目前市面上也缺乏相關訓練課程，自然也欠缺相關的人才。因此在產品製造上，隱私工程要做到什麼程度才能滿足 GDPR 的要求？企業可能會想問：有沒有一套制度化的最佳實作或是國際及產業標準？如果有標準可循，台灣企業就能對客戶明文證明自己產品符合 GDPR 的要求。

事實上，產業界已經有了解答。包含德國獨立資料保護中心組織(ULD)及美國國家標準與技術研究院 (NIST) IR 8062 標準的隱私保護精神的 ISO 27550 Information technology - Security techniques - Privacy engineering 之標準草案中，揭櫫「隱私工程活動」應涵蓋知識管理、風險管理、需求分析、架構設計等關鍵之系統開發流程，並需融入隱私工程六大特性，包括機密性(Confidentiality)、正確性(Integrity)、可用性(Availability)、不可連結性(Unlinkability)、透明性(Transparency)和可介入性(Intervenability)。



（ISO 27550 包含的隱私工程六大特性，有助於 GDRP 的遵循）

外部第三方驗證機構如 SGS 可針對管理流程面及產品技術面，分別提供流程稽核及技術檢驗。在企業一切都重新調整到位，這些第三方單位將能對產品及服務做 ISO 27750 的符合性宣告，而有利於客戶或供應商信任台灣廠商的 Privacy by Design 成熟度及遵循性，已經滿足 GDPR 第 25 條的法規遵循要求。



（ISO 27550 驗測流程包含流程稽核及技術檢驗兩個面向的檢驗）