開放「隱私資訊管理系統驗證方案」認證服務

驗證機構認證處/黃詠婕

● 本會開放「隱私資訊管理系統驗證方案」認證服務緣由及期程

近年來台灣個人資料外洩案例屢見不鮮，亦引發社會大眾高度關注，另社會詐騙事件多、詐騙產業鏈形成，造成民眾受害事件層出不窮，且個資外洩時常遭到犯罪集團不法利用，進而造成當事人權利損害。為此，政府高度重視，列出「打詐五法」(個人資料保護法是其中之一)，政府並提高規格設立「打詐專案辦公室」，在在顯示對個資保護之高度重視，而要完全杜絕個資洩露的風險，實務上是相當棘手的巨大挑戰。

我國《個人資料保護法》，簡稱《個資法》，取代電腦處理個人資料保護法，修正條文分別於 2012 年 10 月 1 日及 2016 年 3 月 15 日生效。2023 年 5 月 31 日個資法修正案，旨在建立個人資料保護獨立監督機制及大幅提高罰鍰。2024 年 12 月個人資料保護委員會籌備處，發布預告修正「個人資料保護法」草案，明定對高風險行業與非公務機關優先實施行政檢查，及增訂公務機關或經公告指定之非公務機關應置個人資料保護長及個人資料保護稽核人員等，主要係為賦予個資法之主管機關相關執法權限，以推動落實個資法。

鑑於國家對於個人資料保護法越趨重視，企業如何彰顯對個資保護之公信力、展現善盡管理之責任，採行國際標準是一個可行通用且可被接受的作法。本會為支持建立國內對個人資料保護強化之機制，於 2024 年 12 月 31 日公告開放 ISO/IEC 27701 隱私資訊管理系統(Privacy Information Management System, PIMS)驗證方案之認證制度並自 2025 年 2 月 1 日開放受理此認證服務。

● 「隱私資訊管理系統驗證方案」認證規範介紹

對身處資訊科技突飛猛進的現代人而言，臉書、IG、推特、line、YouTube 以及部落格等各種社群媒體使人與人之間的聯繫更加緊密，在數位的世界裡充滿新奇與大量資訊傳遞，但也同時帶來了風險，使用者個資外洩的問題更是時有所聞。因此，如何減少資安風險並保護大眾在網路上的隱私安全，實為刻不容緩之課題。國際標準化組織(ISO)於 2019 年 8 月公布了 ISO/IEC 27701「安全技術－擴展 ISO/IEC 27001 和 ISO/IEC 27002 的隱私資訊管理－要求和指導原則(Security

techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines)」，為世界上第一個用以幫助組織管理隱私資訊並滿足相關法規要求的國際標準。

ISO/IEC 27701 驗證標準提供了對個人資料保護的要求及指導，建立於 ISO/IEC 27001 資訊安全管理系統（ISMS)之基礎，延伸至隱私保護的個資管理系統國際標準，對於掌握大量個人可識別資訊 (Personally Identifiable Information, PII) 且高度資訊自動化處理之組織，可確保個人資料的適當保護及隱私合規性。

本會公告「隱私資訊管理系統驗證方案」之認證規範為 ISO/IEC TS 27006-2，驗證機構執行 ISO/IEC 27701 驗證需符合 ISO/IEC 17021-1 以及 ISO/IEC TS 27006-2 要求。ISO/IEC TS 27006-2 主要是以 ISO/IEC 27006 為架構，增加額外的 PIMS 相關規定與指引，其目的在協助認證機構更有效的評估各驗證機構所須適用之各項準則，如驗證人員能力、驗證文件內容要求，以及對稽核時間的計算準則。經本會認證之驗證機構，執行隱私資訊管理系統之驗證，必須基於相關之技術專業為國內個資防護把關，這些都是本會建立認證信賴之基礎，且每一個環節都攸關國內資訊安全領域、個人資料保護環境之健全及保障，亦突顯本項認證服務之重要性。

- **開放認證服務效益**

TAF 於 2015 年 10 月 21 日即成功簽署國際認證論壇(International Accreditation Forum,簡稱 IAF)資訊安全管理系統(ISO/IEC 27001)國際多邊相互承認協議(Multilateral Recognition Arrangement，簡稱 MLA)，TAF 基於資訊安全相關管理系統領域之認證基礎下，發展本項認證制度，對於國內法規法遵要求與個人資料保護，強化權責機關與企業足以信賴之驗證結果，為國內個人資料保護之驗證提供一個新的發展方向，以進一步保護個資，並建立社會大眾信心。