個資法保護個人資料的合理利用，是個令人期待的法令；惟對擁有大量個人資訊的政府機關，則是個令人頭痛的議題。

個資法及ISO 27001共通性與操作概述

◎黃小玲

壹、前言

人力資源部門內一位人事專員正在跟人事主管報告：昨天設計部門一位欲進用之新進人員說：我們詢問他是否有犯罪紀錄是違法的，因為個資法明載犯罪前科屬於特種個資，依法不得蒐集，所以他堅持不填那份員工基本資料表。

人事主管說：妳有沒有跟他說明這是我們組織資訊安全管理系統（Information Security Management System, ISMS）要求的必要事項，因為資訊部門導入ISMS時，就要求於新進人員進來之前應進行背景查證檢核（verification check）。

人事專員：我都跟他說了啊，那現在怎麼辦？

人事主管：先讓法務跟資訊部門好好溝通，我們再來決定怎麼辦？

人事專員：那這個新人……？

人事主管：先跟設計部門說暫緩進用吧！否則跟公司現行規範不合，恐怕會引起內部反彈。

貳、個資法議題

上述案例雖然有點因噎廢食，卻提供組織管理階層一個思考方向：若內部現行規範或管理制度與法令有所牴觸時，孰輕孰重？而或者可以設計一套兩全其美的方法，兼顧管理制度與法令遵循，以降低內部依循法令而造成之衝擊。

個人資料保護法（以下簡稱個資法）於民國99年４月27日通過，５月26日總統令公布此個人資料保護法。一時之間，大家閒聊的話題都是「你今天個資了沒？」同時也發現今年下半年度教育訓練的市場非常火熱，組織紛紛聘請法學專家或名人演說，此間大部分研討會亦多鎖定一個主題：什麼是個人資料保護法？經過教育訓練的專業解說後，卻還是有點像霧裏看花，不懂得如何開始。

現今「你今天個資了沒？」主題包括：

- 如果只有名字，算不算個人資料？
- 需要賠償時，誰來賠？國賠？
- 需要處以徒刑時，應該誰負責？
- 當事人請求刪除時，要不要出示刪除紀錄？
- 如果組織已通過ISO 27001驗證，是否能保證符合個資法？

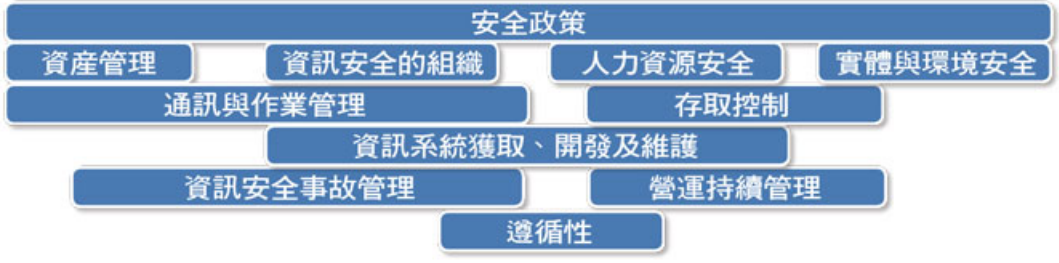
個資法顧名思義是保護個人資料之合理利用，應該是個令人期待的法令；惟若站在擁有大量個人資訊的政府機關來看，則是個令人頭疼的議題。

本文將概述資訊安全標準ISO 27001與個資法之共通性及操作方式，提供政府機關或民間企業已通過ISO 27001驗證之組織，參考如何加強個人資料之保護。

參、ISO 27001簡介

ISO 27001是資訊安全管理標準，此標準的提供主要是以建立、實作、運作、監視、審查、維持及改進資訊安全管理系統之模型。圖１所示為ISO 27001之11大控制領域，藉由控制領域下之控制措施可以確保組織之資訊安全。

圖１　ISO 27001控制領域



資料來源：本文自行整理

如果組織已通過ISO 27001的驗證，若要強調個資保護議題，似乎較為簡單，至少已有驗證公司之稽核保證。只是ISO 27001並不特別強調個人資料，所以若有個人資料出現在非重要業務流程時，可能相關風險就不會被清楚地凸顯。

個資法為公布之法令，自有遵守之必要；而ISO 27001資訊安全標準，所提供的是一個過程導向，以建立組織的資訊安全管理系統。現今，在政府大力推動資通安全的策略下，大部分政府機關皆已了解資訊安全之重要性；如何在這個框架下，加強個人資料之保護，可以讓整個資訊安全管理系統更加成熟，且可降低觸法之可能性。

肆、個資法與ISO 27001之共通點

個資法與ISO 27001標準有以下幾個共同之重點，值得組織之管理階層考量如何進行整併或解決衝突。

- 資產（個資）盤點之實作：如何確認與盤點所有組織內之個人資料。
- 背景審查（篩選）之必要性：如何在資訊安全與個人資料保護兩者之間取得平衡。
- 儲存與備份管理：如何確保資料的生命周期已妥善定義與管理。
- 存取管理：資料之存取管理如何加強。
- 資訊安全事故管理：如何整合事故通報與處置程序。
- 遵循性：適法性之必要。

不論組織是否已導入資訊安全管理系統，針對個資法的公告，組織都該有因應之措施。對於所有公務人員最想知道的應該是：組織內的所有個人資料該從何處確認是否已妥善保護？若有疏漏之處，又應如何啟動相關方案？以下將就部分之議題進行討論，同時提供部分操作手法供參。

伍、資產（個資）盤點之實作

ISO 27001中明定組織應明確識別所有資產，並針對重要資產製定清冊。資產分類通常分為以下數類：

- 資訊資產：檔案或資料庫、訓練教材或紀錄、使用者手冊、業務持續計畫等；書面文件包括合約、手冊、組織文件等。
- 軟體：應用軟體、系統軟體、開發工具等。
- 硬體：電腦、通訊設備及保險櫃等。
- 人員：員工及在組織場所提供資訊服務之廠商及其員工。
- 環境：辦公區域、檔案室、機房、空調、機電、消防等。

以上這些資產分類中，基於個資法的要求，組織應採行個人資料的辨識，例如在資料庫、訓練紀錄、業務持續計畫、合約及檔案室中，個人資料都極可能包括在內。

表１為ISO 27001資產管理與個資法中，定義個人資料的規範與定義何謂個人資料檔案。如何符合ISO 27001與個資法的第一步，皆是從資產清冊開始。相較來說，個資法的目標明確，是針對資產清冊內之個人資料進行規範動作。

表１　資產管理VS.個資法要求

ISO 27001資產管理	個資法
目標：達成及維持組織資產的適切保護。	為規範個人資料之蒐集、處理及利用， 以避免人格權受侵害，並促進個人資料之合理利用。
資產清冊：製作與維持所有重要資產的清冊。	資訊安全的組織

資料來源：本文自行整理

ISO 27001並未要求清楚區分紙本文件與電子文件等不同複本，同時評鑑資產價值時亦未特別評估個人資料的重要性。組織現在面臨的挑戰是如何從眾多的系統或紙本文件中進行個人資料之辨識，再加入之前若已將部分含有個資之系統資料列為非關鍵資產時，則又應如何凸顯其重要性？以下概述盤點個人資料之流程步驟，從業務流程分項，到最後資料產出的終點，詳見圖２。

圖２　個資分析流程

資料來源：本文自行整理

步驟１：定義業務流程。ISO 27001要求識別所有資產，通常只針對重要業務流程進行評估。確認列出所有業務流程，則為個人資訊識別的第一步。

步驟２：確認所有利害相關者。業務流程中的利害相關者，包括(1)客戶／使用者；(2)組織內部；(3)委外廠商；(4)供應者；(5)其他，以上種種表示業務資訊若在不同的資料生命週期，可能有不同的管理者，所以必須一一確認。

步驟３：支援流程。支援此主要業務流程，而需要建置之附屬系統。例如：檔案管理系統或備份管理系統等。

步驟４：個資流程。清楚說明在流程中，有關個人資訊之生命週期，例如：如何建立、傳送、儲存、封存及銷毀等現行之程序。

步驟５：個資類別。分別列在個資法中之一般個資與特種個資，並檢視組織內這些個人資訊蒐集之必要性。
步驟６：流程輸入。個資來源、需要蒐集個資的理由，以及個資蒐集的方式。
步驟７：流程輸出。個資以何種樣態出現，存在何種報表或文件中。

陸、背景審查（篩選）

資訊安全與個人資料保護對管理階層而言，有時就像在天平上的兩大難題。如何確保存取組織資訊之雇員沒有違反安全紀錄，同時又得保護其人格權不受侵害，往往很難拿捏分寸。ISO 27001於人力資源安全控制領域中要求組織於聘僱人員之前，應對所有聘僱之應徵者、承包者及第三方使用者的背景查證檢核。依據標準所建議之最佳實作，包括以下幾項：

- 是否有合格的品格推薦信。
- 應徵者的學經歷檢核。
- 確認應徵者所宣稱之學歷與專業資格。
- 獨立的身分檢核（護照等）。
- 更詳細地核對，如信用核對或犯罪紀錄檢核。

以上每種資料都是個人資料，有些甚至是個資法限定不得蒐集的個人資料。ISO 27001對背景審查的要求，似乎是與個資法最大的衝突部分。

在個資法未通過之前，因為只有電腦處理個人資料保護法，有限定適用範圍與主體，僅限於公務機關、非公務機關之八大行業及受指定之非公務機關。組織通常在討論內部適法性時，較少將電腦處理個人資料保護法納入，往往覺得不在適用主體範圍內。

ISO 27001要求進行篩選之前，應依照相關法律、法規及倫理，並兼顧營運要求的相稱性、所存取資訊的保密類別及所察覺的風險進行背景查證檢核。如此一來，在個資法通過後，可以確定的是除非有特例情況，否則前述所提及之犯罪紀錄應該不能要求當事人揭露。

柒、儲存、備份及存取管理

ISO 27001通訊與作業管理領域是屬於實際作業面之控制措施，於本文摘錄部分條文對照個資法，詳見表２。分別從不同面向，概述從作業面，組織應如何符合資訊安全標準與個資法之要求。

表２　通訊與作業管理VS.個資法要求

ISO 27001通訊與作業管理	個資法
目標：確保正確與安全地操作處理措施。	規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用。
資訊備份：依據所議定的備份政策，定期進行資訊與軟體的備份與測試。	處理：…資料之記錄、輸入、儲存…刪除…或內部傳送。
資訊處置程序：建立資訊的處置及儲存程序，以保護此資訊免於未經授權的揭露或誤用。	
交換協議：組織與外部團體間資訊與軟體的交換應建立協議。	利用：指將蒐集之個人資料為處理以外之使用。
監控系統的使用：應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果。	
存取控制：控制資訊的存取。	當事人其個人資料依個資法規定行使查詢…補充或更正…停止蒐集、處理或利用…刪除之權利。

資料來源：本文自行整理

- 資訊備份：資訊應保留多久才是最佳時機呢？對資訊擁有者或管理者而言，若沒有規範應該留存多久，就等同「永久保留」之意。個資法通過之後，組織除考量資訊備份之機制安全外，亦應加入留存期間之規範，避免個人資料洩漏之風險。
- 資訊處置程序：考量部分資訊之「遮蔽機制」，不全然揭露所有資訊。例如：身分證字號，遮蔽幾碼不顯示，改以星號***替代；資料加密機制，以確保資料外洩時，無法被輕易解密。
- 交換協議：個人資料交換時，應建置適切之管理程序、責任及技術標準。
- 監控系統的使用：使用監控工具監控網路使用者時，應考量個人之隱私，同時基於個資法規範，能否取得當事人之書面同意接受監控，亦屬一大難題。
- 存取控制：當事人要求查詢或請求閱覽時，如何控制其相關權限？是否開放當事人依權限存取？或是提供不同的作法。

捌、資訊安全事故管理

發生資訊安全事故或是個人資料外洩時，組織常先採取保護自己的作法，最保險的方法是封鎖消息，通盤否認。一旦成為被指責對象時，又將矛頭指向是委外廠商的錯誤。

個資法要求組織若查明確屬於內部管控不當，導致資料外洩，得通知當事人。因為個資法規範是以「適當方式」通知，不知會不會發生像某知名廠商在召修產品時，都是號稱公告在網站周知，且可能公告兩個星期就悄悄移除相關訊息。如何定義「適當方式」，可能也得期盼施行細則訂出明確的說明。

建議的作法是，個人資料外洩，可以視同組織之安全事件。表３為ISO 27001要求建立適切之通報管道與程序，以確認權責人員收到通報時，應採取的行動方案。

表３　資訊安全事故管理VS.個資法要求

ISO 27001資訊安全事故管理	個資法
目標：確保與資訊系統相關的資訊安全。	
通報資訊安全事件：應循適切的管理通道，儘速通報資訊安全事件。	公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。
通報安全弱點：所有員工、承包者及第三方使用者，應注意並通報任何觀察到或可疑的安全弱點。	

資料來源：本文自行整理

玖、遵循性

此部分之ISO 27001條文明確指出要通過ISO 27001標準之驗證，得識別適用之法條與應確保個人資訊的資料保護與隱私，詳見表４。至於如何確保個人資料保護與相關隱私，除前述幾項操作面之作法外，標準所論述之最佳實作為指定一資料保護專員（data protection officer）後，由此專員對管理者、使用者和服務提供者，提供其各自的責任及應遵照的特定程序。

表４　遵循性VS.個資法要求

ISO 27001遵循性	個資法
目標：避免違反任何法律、法令、法規或契約義務，以及任何安全要求。	
識別適用之法條。	為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用。
個人資訊的資料保護與隱私。	

資料來源：本文自行整理

拾、結論

個資法的通過對已取得ISO 27001的驗證者，具有加乘之效。針對涉及個人資料部分可以加強其管理之效度，同時檢視相關之技術配套措施是否足夠。政府機關要求機關內應有資訊安全長的角色，以負責資訊安全等規劃與統籌調度業務；個資法則要求公務機關對於保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩露。不知是否應由資訊安全長兼任此個人資料保護之重責大任，或是另行權責分配，另設一位資訊隱私長？個資法通過後，指派專責人員開始通盤檢視組織中之個人資料保護，實屬燃眉之急。

對組織而言違反個資法，將會面臨損害賠償及團體訴訟等問題。因此在個資法施行細則公布以前，組織應思考如何因應法令，加強內部個人資料之有效管理，以降低日後可能發生之訴訟問題。

（作者現任財團法人資訊工業策進會與行政院國家資通安全會報技術服務中心組長）

▲Top