企業資安新革命

個資法全面保護個人隱私

新版「個人資料保護法」於2012年10月1日正式上路，不論是個人或企業在進行任何活動，凡是需要蒐集、處理或利用到個人資料的行為，包括紙本紀錄和電腦資訊，若不留意，都有可能牴觸了個資法的規範。企業及民眾應了解相關規範，並採取因應之道來面對個資法所帶來的衝擊。

◎撰文／林品賓 圖片提供／達志影像

為了加強保護民眾的個人資訊隱私權益，2010年5月，立法院三讀通過「個人資料保護法」（後稱「個資法」），並於2012年10月1日正式上路施行，因此有關個資保護的內容與影響，已成為時下企業與民眾的熱門討論議題。

面對已經正式上路兩個月的個資法，不論是關心自己個資權益的民眾，或政府機關及民間企業的行政或法務人員，都應熟悉個資法的規範內容，這不但可以確保本身的隱私權益不被侵害，更得以避免因不慎觸法而受到法律的裁罰。

個人與企業全面納入規範

事實上，這次新版個資法的上路，已經打破舊法中行業別的限制，規範對象全面擴大至所有民營企業、團體與個人，例如，新法要求蒐集個人資料時，應該把相關事項告知當事人。而這些項目包括：蒐集者身分、蒐集目的、個人資料類別、利用期間、地區、對象及方式、當事人權益事項等等。如果這些資料是由當事人直接提供時，應將相關注意事項在蒐集的當時進行告知，而若資料來源非當事人直接提供時，則應於利用資料之前向當事人進行告知。不過，新法中也規定，在「依法律規定」、「蒐集乃為履行法定義務所必要」、「當事人明知應告知之內容」、「大眾傳播業者基於新聞報導之公益目的」等情況下可免告知。

理律法律事務所曾更瑩律師表示，企業在蒐集個人資料之前，應先檢視是否有「特定目的」及是否符合個資法所定之合法蒐集要件。而對於客戶資料的取得，企業可主張因為與客戶進行交易構成「契約關係」，或為與客戶協商進而完成交易，而有「類似契約關係」等合法要件。

舉例而言，這與過去企業常見為行銷目的而成立會員俱樂部等組織，定期舉辦活動促銷或提供優惠資訊行為類似，會員關係就類同契約關係，符合個資法之要件。如果，沒有符合個資法之蒐集要件，企業必須取得「當事人書面同意」，另外，為了降低觸犯個資法的風險，企業應減少所持有之個人資料之質與量，非必要的項目應避免蒐集。

企業間個資流通有保密義務

至於，過去最容易造成個資外洩的資料委外處理部分，因為個人資料在不同企業或團體間流通時，隨時都有違法風險。因此，曾更瑩律師指出，除了明定由當事人授權之交叉行銷行為外，個人資料在委外處理時，因為並未超過特定目的外的行為，無須當事人額外書面同意。

而且既然是委外，受託者即無權私自使用所取得之個資，因此對於資料的保護將更為重要。目前新版的個資法規定中，如受委託者違反個資法時，違法的責

任除接受委託的企業必須負擔責任外，原本委託的企業也須負擔責任，因此在委外時，應該要求受委託者必須遵守個資法規範、對個人資料加以保密、採行適當維護資訊安全等，有關事項建議應有合約文件保障，否則企業將負擔全部責任。

舉例來說，各大百貨公司每年都會舉行週年慶，顧客在搶購商品時，業者會以寄發商品目錄、特價資訊，以客戶服務等為理由，要求客戶留下相關個資，之後，百貨公司也藉由這些資料的委外處理，將優惠訊息等資料寄送給客戶。而在這過程當中，如果有資料控管不嚴謹，或是有心人士刻意竊取下，就容易造成個資外洩的情況。

一旦發生個資外洩情況，百貨公司雖已將資料委外處理，而且洩密的管道也屬於委外廠商，但因為個人資料是由百貨公司所取得，因此百貨公司也必須負擔連帶責任。以這樣的實例來看，企業為防止個資外洩的風險，應遵循新法規定，使得業者負有資安義務，業者在選擇委外單位時，除有法律文件保障外，應特別注意受託單位的執行能力，才能確實保障各方權益。

對企業員工個資亦須建立標準保護流程

不過，新個資法的上路，除了一般企業、團體、法人等相關負責人在資料授權或取得過程必須注意外，企業內員工的個資也應檢視其處理流程。因為任何公司不論大小，除非是一人公司，否則都會有員工。有員工，就必然有姓名、身分證字號、戶籍地址、現住地址、手機號碼、勞健保與退休金資料、薪資單、銀行帳戶、扣繳憑單、打卡單、請假單及曠職紀錄等，甚至還可能會有警察局所核發的良民證、聯合徵信中心出具的信用報告等特別項目。所以，蒐集員工上述個資，雖然未必都有正當性。像是員工家庭成員有哪些人、分別在哪裡上班？員工以前信用如何？這些資料多半在任職時經員工書面同意，所以爭議程度小。

但個資的「處理」，包括記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或傳送，則對公司內部經手員工薪資、勞健保及勞退、人事檔案等個人資料的同仁來說最為困擾。一旦違規檢索、複製、刪除、輸出、傳送，將由實際上的行為人負刑責。因此，公司員工的個資處理必須要有安全的控管機制。

全球各國陸續立法重視個資安全

目前，全球先進國家也在近年來陸續加入個資保護制度化的行列。歐盟自1993年由原來的「歐洲共同體」更名後，隨即於1995年公布「個人資料保護指令」（Directive 95/46/EC），並且於1998年生效，成為最早頒布個資保護法令的地區。

歐盟這個保護個資法令的施

為了獲得百貨公司的商品目錄、特價優惠資訊，消費者容易留下相關個資，因此百貨業者更要謹慎處理個資防護問題。

行精神，在於防止自然人資料被隨意的使用、複製、甚至轉移到缺乏適當個人資料保護法令的國家。而相較於歐盟，美國則是沒有統一的個人資料保護法令，而是由各單位制定出相關的法令細則。如「健康保險與流通保護法案」、「電子通訊隱私權法」、「有線通訊政策法」等分屬各單位管轄的法令。

世界各國陸續建立個資保護制度後，也接連傳出相關訴訟案例。其中，2008年5月，4名加拿大渥太華大學法律系學生控告知名社群網站Facebook，主張在未取得用戶授權同意之下，Facebook任意披露用戶資料給予廣告商，違反「個人資料保護及電子文件法案」。

不過，Facebook對於控告也反駁表示，學生的投訴忽視該Facebook政策的關鍵條款。最後，該案以和解調停收場。

金融電信衝擊大
個資保護提高經營成本

而這次新個資法的公告施行，衝擊影響最大的就屬電信與金融業。因為，其中第54條規定，業者在直接取得個資的當下就必須告知擁有者，並取得對相關個資的使用、複製、告知權利。至於，對間接蒐集到的個資，相關單位目前還沒有確定要多久時間、或什麼方法進行告知。但是，如果業者對於間接蒐集到的個資需立即使用、複製、轉告相關個人資料，則仍必須在使用前確切告知，否則將有違法之虞。這項規定對金融業、電信業影響最大，因補行告知的成本大，恐將衝擊獲利。

銀行業者表示，以信用卡業務來說，國內的信用卡用戶超過6千萬人次，要在當前有限的人力下一一告知個人資料的擁有者，業者已經直接或間接取得個資，如此動作勢必增加銀行的經營成本，而且也將拖長作業時間。

此外，個資法第6條規定的敏感性「特種資料」，包括醫療、基因、性生活、健康檢查、犯罪前科等敏感性個資，原則上不得蒐集、處理或利用，即使當事人出面同意也不能蒐集，這樣的規定也引發醫療機構緊張反彈。

因應新法
企業資安投資增加

不過，雖然在條文規定讓各界仍有意見，但是，對於保護個資的初衷與做法仍有高度評價。因此，為了因應新法上路，目前各大企業也開始積極準備。

法務部法律事務司科長黃荷婷表示，根據統計，為了因應個資法的上路，國內已經有36%的企業開始進行相關的準備，包括編列預算、重新設定個資保護流程等，這樣的比例較2011年的29.5%要高出許多。

再依企業別來看，金融業和醫療業都有近7成的企業編列預算，而高科技製造業和一般製造業的比例較低，其中，金融業的因應步調是最快的，有79.2%的金融業者已經著手因應個資法。彰化銀行資訊處長曾芳明指出，銀行業本身就是過去「電腦處理個人資料保護法」適用的8大行業之一，面對新版的個資法，額外增加的因應工作，是必須納入紙本資料的控管，以及各種記錄控管程序等等。

國際票券資訊部經理楊松達則說，現階段公司也成立審查部門，並且將法務部門納入，全面負責個資法的因應事宜，而資訊部門則是負責搭配個資法所需的應用程式開發。不過，他指出，國際票券的客戶主要是企業，持有的一般用戶個資比銀行同業少，目前比較大的問題在於，紙本資料的保存與控管的處理，例如企業用戶營利事業登記證影本、存摺影本等。

除了金融業外，另外還有過半的政府和學校單位（54.6%）和醫療業（52.3%）也展開個資法因應工作，政府部門因有依法行政需求，第一時間做好法規遵循是必然的。臺安醫院資訊室主任林明賢表示，醫院會積極因應新版個資法，主因多數醫院都擁有較敏感的個資，目前該醫院由資

安委員會負責，2011年的工作是阻絕各種電子資料可能的外洩管道，在2012年的任務則是控管紙本資料。

至於，傳統產業方面，由於資料敏感性與即時性不如金融業、電信業、或醫療業，相關的因應動作也就平緩許多。以阿瘦皮鞋為例，編列的因應預算不到百萬元，阿瘦皮鞋管理處協理林文政表示，主要用來改善系統和報表的資料呈現，例如，遇到需要顯示個資的報表就必須進行資料部分遮蔽等。另外，由於新版個資法特別強調蒐集、處理和利用個人資料前，一定要取得當事人同意，所以，林文政表示，預計今年會重新推出會員卡，徵求會員對其蒐集、處理和利用個資的同意權。

網購、傳統產業應加強個資保護

不過，透過網路會員行銷來達成交易的網購業者，就比傳統實體通路業者要來得謹慎。博客來網路書店在2007年，就已開始評估個資法對於企業的影響，博客來總經理室資訊安全經理蔡嘉達表示，因應個資法過關，正逐步推動會員資料的簡化，未來新會員申請不需要提供身分證字號，只要提供能確認出貨的資料即可，但相對的，手機和電子郵件的確認就更為重要。

為了確保網站的安全性，網站業者需設置相關安全防護檢核措施，避免個資外洩。

蔡嘉達表示，為了確保博客來網站的安全性，除在閘道端採購可以提供安全防護的設備和服務外，也已在系統內設計資安檢核點。另外，博客來總經理室公共事務經理楊雅雯說：「新服務或系統上線前，一定要先通過資安和法務部門評估。」除提供員工相關的資安教育訓練外，蔡嘉達指出，博客來也成立資安推動小組，每個部門至少有1名資安種子加入，提高員工的資安意識。

信義房屋很早就進行內部系統的e化，透過e化系統提供業務人員更便利的查詢服務。信義房屋資訊部執行協理江元麒表示，除了做好權限控管外，面對數位化文件，信義房屋2008年第一優先就是完成數位版權保護（DRM）系統的導入，同時做到網頁文件的保護。

也因為有愈來愈多駭客盯緊Web伺服器的漏洞，信義房屋目前在推出客戶的入口網站查詢服務時，除了謹慎監控異常流量，確保所有登錄檔、日誌都完整留存外，信義房屋的Web服務仍以提供內部服務為主，信義房屋網站提供客戶專區查詢資料，必須經過身分驗證，並與內部網路的Web服務比對後，才可放行資料查詢。江元麒表示，這種做法不讓客戶資料直接暴露在網路上，對客戶資料也是一種保障。

總之，要因應新版個資法施行，應先從企業員工做起，配合企業整體政策，建立個資法保護的共識與標準作業流程（SOP）才是當務之急，再擴大到企業，由於新版個資法所涵蓋範圍，幾乎牽涉每個組織中的人事、行政、業務等單位，個人資料保護，絕對是需要大家一起配合，加強宣導與教育，才可避免觸法。■