國立大學如何因應個人資料保護法

周 天　主任

國立高雄第一科技大學
個人資料保護中心

壹、前言

個人資料保護法（以下簡稱「個資法」），自民國101年10月1日起正式施行，個資法並非新制定的法律，民國99年修法前，原名為「電腦處理個人資料保護法」，修法後，除了法律名稱的修正外，其適用範圍亦擴及所有的公務機關、非公務機關、團體與個人；此外，規範的內容也更為詳盡，違反個資法的法律責任，也較舊法更為嚴重。國立大學校院保有學生、教師、職員或廠商之個人資料眾多，日常校務運作涉及個人資料的蒐集、處理、利用、國際傳輸等行為，上述行為的適法性，除必須依據高等教育或技職教育等相關法規的規定外，尚且必須符合個資法及其施行細則的相關規定。

貳、個資事故頻傳與國際立法保護潮流

過去「隱私權」的觀念，往往被侷限於「個人身體的隱私」，故不肖之徒利用針孔相機偷拍之行徑，便構成侵犯隱私權的犯罪行為；但隨著隱私權概念的發展，其保護的範圍已拓展至「個人資料的自主控制」，以維護人性尊嚴。因此，自然人的姓名、身分證字號、銀行帳戶號碼、聯絡電話及住址等，皆屬於個資法保護的個人資料。

一、個資事故頻傳

今日電腦網路與行動通訊蓬勃發展，個人資料遭到濫用的情況日趨嚴重，例如：民國93年6月刑事警察局破獲駭客入侵網路銀行，竊取存款戶帳號密碼等個人

資料，進而以轉帳方式盜領存款，共計20萬筆個人之銀行帳號密碼遭竊，歹徒盜領的犯罪金額，高達新臺幣200餘萬元；民國96年3月駭客利用交友網站，騙得當事人出生年月日等個人資料，破解即時通密碼並下載當事人相簿中的私密清涼照片，進而恐嚇當事人；民國95年3月桃園一家私人診所停業後，將病歷等個人資料，以廢紙賣給資源回收廠商；民國98年11月醫美名醫洩露緋聞女主角病歷身份等個人資料，遭台北市衛生局約談等，上述非公務機關所發生的個資事故，層出不窮。

公務機關所發生的個資事故，亦時有所聞，例如：民國100年2月不肖員警及海巡人員，以每筆新臺幣三千至八千元不等代價，盜賣民眾個人資料，提供徵信社做為生財利器；同年9月高等法院庭長喪偶欲尋求第二春，私下利用司法院資訊系統，調查相親對象的個人資料，遭移送司法院處分；民國101年12月屏東縣政府環境保護局，針對該縣殯葬特區的環評報告書中，明列數十位地方陳情人士的之姓名、身分證字號、電話、地址等個人資料，未加以遮蔽，公布於縣府網站，當事人因此提起刑事告訴，並附帶民事訴訟求償新臺幣200萬元，此乃個資法正式施行後，首度發生的刑事告訴案件。

民國102年3月台北市立敦化國中訓導組長，將極機密的校內高度關懷學生名單當成廢紙回收利用，遭其他學生以手機拍下在校內流傳，名單中詳列14位學生之姓名、班級、座號、偏差行為、前科紀錄等；民國102年7月高雄市正修科技大學管理學院資訊創新服務中心，於網站更新資料備份時，被網路搜尋引擎所連結，因而外洩200餘名學生之姓名、身分證字號、E-mail帳號、手機、家裡電話、地址等。上述乃個資法正式施行後，於各級學校所發生的個資事故，皆引發軒然大波。

二、國際個資保護的立法潮流

類似的個資事件，也同樣發生在世界各國，因此，國際組織與各國政府皆認為有必要針對個資保護進行立法，以期能有效因應，例如：歐盟於1995年公布個人資料保護指令、日本於2005年公布個人資訊保護法等；國際上也陸續制訂有關個人資料管理系統驗證標準(Personal Information Management System)，包括：歐盟Euro Privacy Seal、英國BS 10012、日本JIS Q15001及聯合國ISO 29100。

三、我國個資保護的立法與修法

我國針對個人資料的保護，肇始於民國84年的「電腦處理個人資料保護法」，但是個人資料必須是經由電腦處理，才適

用該法。因此，該法對於個人資料的保護，有其侷限性。該法於民國99年修正通過後，取消「電腦處理」的限制，將其保護的範圍，除擴及紙本個資外，並擴大適用於所有公務機關、非公務機關、團體與個人，凡有蒐集、處理或利用個人資料的行為，皆適用該法。惟為顧及社會各界針對上述修法之因應，延至民國101年10月1日才正式施行。

參、個資法解析與實務

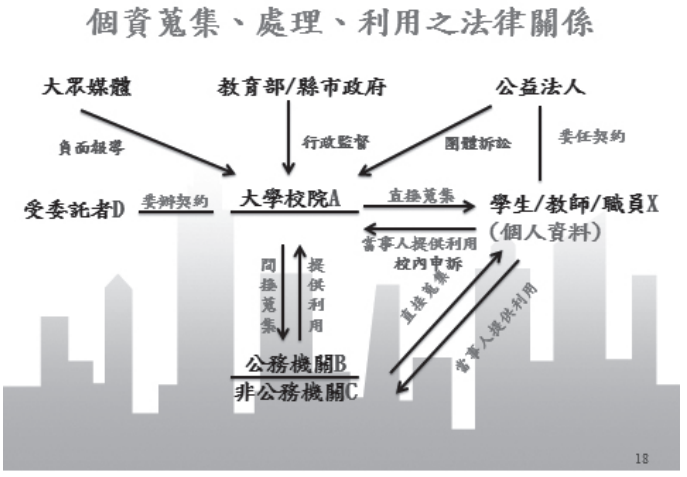
個資法之立法目的，係為規範個人資料之蒐集、處理及利用，以避免人格權遭受侵害，並促進個人資料之合理利用。個人資料，可分為「一般個資」與「特種個資」，一般個資是指自然人的姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭狀況、教育程度、職業、病歷、聯絡方式、財務狀況、社會活動及其他得以直接或間接方式識別該個人之資料。

「特種個資」，係指個資法第6條所規定之醫療、基因、性生活、健康檢查、犯罪前科等個人資料。由於上述個資多涉及敏感性之內容，故原則上不得加以蒐集、處理或利用，但如符合該條所規定之各款例外情形之一者，始得蒐集、處理或利用，例如：法律明文規定；或公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施；或當事人自行公開或其他已合法公開之特種個資；或公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，並經一定程序所蒐集、處理或利用之特種個資。

由於上述個資法第6條之規定，對於幼教業、計程車業、保全業等諸多行業，執行困難；而且「病歷」依該條之規定，屬於一般個資，而「醫療」卻屬於特種個資，兩者實務上區別不易，法律效果卻迥異。因此，個資法第6條之規定，目前暫緩施行，行政院已經提出個資法的修正草案，希望將特種個資的種類，增為六項，納入「病歷」，並且將其例外情形，增加：1. 經當事人書面同意；2. 維護公共利益所必要，以回應各界的呼籲。因此，該修正草案經立法院完成修法程序前，個資法第6條之規定，目前暫緩施行。

依據法務部目前對於教育機構適用個資法的解釋，公立大學校院屬於「公務機關」，私立大學校院屬於「非公務機關」，針對大學校院蒐集、處理及利用個人資料之法律關係，詳如以下圖解說明：

大學校院蒐集、處理、利用個人資料



圖一　個人資料蒐集、處理及利用的法律關係

之基本原則，包括應尊重當事人之權益、依誠實及信用方法、不得逾越特定目的之必要範圍，而且必須與蒐集之目的具有正當合理之關聯。同時，國立大學校院因屬「公務機關」，故其蒐集、處理、利用個人資料，應依據個資法第15條與第16條之規定。

一、個人資料之蒐集

大學校院蒐集個人資料之情形很多，例如學生參加入學考試時，招生簡章報名表中，有許多關於個人資料的欄位，要求考生填寫；教師或職員就職報到時，人事室也會提供人事資料表單要求填寫。因此，大學校院提供紙本或利用網路，要求當事人填寫個人資料，乃「直接蒐集」當事人的個人資料。此外，大學校院向學生、教師或職員過去所就讀的學校或服務的單位，要求提供學生、教師或職員的個人資料，這種向當事人以外的第三人，要求提供個資的行為，便是「間接蒐集」當事人的個人資料。

二、個人資料之處理

經由直接蒐集或間接蒐集，大學校院將所蒐集之當事人個資，為建立或利用個人資料檔案，加以記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸入、連結或內部傳送，便是個資的「處理」行為，例如：建立學生或教師的e-Portfolio個資檔案，或各系將教師的紙本個人資料，透過校內公文傳遞，傳送給人事室等單位。對於上述蒐集或處理的個人資料，大學校院必須履行善良管理人的注意義務，以維護個人資料的正確性與安全性，避免遭受竊取、洩漏、竄改、毀損或滅

失，若有不法濫用或洩漏之情形，大學校院便須對受害的教師、學生或職員，負擔法律上的責任。

惟大學校院因受限於人力或技術，常見將個資的蒐集、處理或利用的工作，委由第三人代為處理，例如：職員證或學生證的委外印製，大學校院進行上述勞務採購的委外作業時，必須盡其監督義務，慎選投標廠商，例如：以其是否通過資訊安全或個資安全驗證，做為廠商投標資格之一；或在委辦契約條款中，明訂發生個資事件因而造成大學校院之民事賠償責任時，大學校院有向廠商求償之權利。

三、個人資料之利用

大學校院將學生、教師或職員的個人資料，提供給校外的其他單位，例如：大學校院將教師或學生的個人資料，上傳登錄至教育部的網站系統；或大學校院將教師的研究計畫申請表單，郵寄給國科會等，便是大學校院對於個人資料的「利用」行為。上述利用行為，必須與其當初蒐集或處理之特定目的相符，如有不相符合，則大學校院必須具有個資法所明定的各款例外情形之一者，始得將教師或學生的個人資料，做為特定目的外的利用。

四、當事人之權利

由於當事人對其個人資料的「自主控制權」，大學校院的學生、教師或職員等，對於其個人資料可以主張的權利，包括：1.請求查詢或閱覽；2.請求製給複製本；3.請求補充或更正；4.請求停止蒐集、處理或利用；5. 請求刪除，且上述權利不得預先拋棄或以特約限制。

例如：大學校院的教師或學生，想知道其過去在圖書館的個人借書記錄？這些個人借書紀錄，都是屬於借閱者的個人資料，大學校院的圖書館應提供借閱者透過網頁上的個人帳號與密碼，提供個人查詢、閱覽或借閱紀錄複製本的實務作法。借閱者向圖書館提出上述請求時，除非符合個資法第10條所明定的三種例外情形之一者，否則圖書館不得拒絕借閱者的請求，上述例外情形包括：1.妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益；2.妨害公務機關執行法定職務；3.妨害該蒐集機關或第三人之重大利益。

此外，面對學生、教師或職員請求大學校院停止蒐集、處理或利用，或請求刪除其個人資料時，依據個資法第13條的規定，大學校院必須在30天內回應當事人的上述請求，各單位業務同仁勢必面臨相當壓力，因此對於所主管業務範圍內的相關法源依據，必須更加嫻熟，除非有明確的

法律依據，得據以拒絕當事人之請求，否則便須同意當事人的請求。

五、受託者之角色

受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於個資法適用範圍內視同委託機關。此外，個資法明定委託機關對於受託者具有監督義務，包括：1.預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間；2.受託者就個資法第12條第二項採取之措施；3.有複委託者，其約定之受託者；4.受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施；5.委託機關如對受託者有保留指示者，其保留指示之事項；6.委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

六、蒐集個資之告知義務與例外

大學校院蒐集由當事人提供之個人資料時，無論使用紙本表單或利用網頁欄位，均應對於當事人履行告知義務，且告知之內容，應包括下列事項：1.大學校院之名稱；2.蒐集之特定目的；3.個人資料之類別；4.個人資料利用之期間、地區、對象及方式；5.當事人依據個資法第3條規定得行使之權利及方式；6.當事人得自由選擇提供個人資料時，不提供對其權益之影響。大學校院蒐集非由當事人提供之個人資料時，應於處理或利用前，向當事人告知個人資料來源及上述各項告知內容。

大學校院履行上述告知義務時，其得以選擇的告知的方式，包括：言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式，實務上最簡單的方式，便是在紙本表單或網頁欄位上加註警語，以便填寫紙本表單或網頁欄位的當事人，得以清楚知悉大學校院正在蒐集其個人資料。反之，大學校院如符合下列各款情形之一者，始得免除上述的告知義務，包括：1.依法律規定得免告知；2.公務機關執行法定職務或非公務機關履行法定義務所必要；3.告知將妨害公務機關執行法定職務；4.告知將妨害第三人之重大利益；5.當事人明知應告知之內容。

七、個資安全維護措施

大學校院保有學生、教師及職員之個人資料，故必須在技術上與組織上，採行必要的安全維護措施，以避免個人資料發生被竊取、洩漏、竄改、毀損或滅失，上述安全維護措施，得包括下列事項：

1.配置管理之人員及相當資源：例如：大

學校院成立「個人資料保護委員會」，建議可由該校副校長以上主管擔任召集人，委員會成員包括各行政單位及各教學單位的代表，並編列個資安全維護相關預算經費。

2. 界定個人資料之範圍：大學校院各單位進行個資清查，完成個資清冊，加以妥善管理。個資清查時，必須檢視各種個資表單中，所要求填寫的欄位是否具有特定目的？是否逾越特定目的之必要範圍？是否與蒐集之特定目的具有正當合理之關聯？
3. 個人資料之風險評估及管理機制：個資清查時，可以發現哪些個人資料檔案，係存放於哪部電腦中？或存放於哪個系統伺服器中？上述個資的存取權限如何？有無做好安全機制？哪些紙本個資檔案，係存放在哪裡？如何做好安全措施？根據上述個人資料之風險評估，建立適當的安全管理機制。
4. 事故之預防、通報及應變機制：根據上述個人資料之風險評估，建立適當的安全管理機制，並且預防可能發生的個資安全事故，如果一旦發生個資安全事故，大學校院應有通報當事人及主管機關的機制，並採行適當的應變措施。
5. 個人資料蒐集、處理及利用之內部管理程序：針對學生、教師或職員個人資料之蒐集、處理及利用，大學校院必須制訂各校個人資料保護政策、管理辦法、內部管理之標準作業流程，包括：程序書、作業說明書及相關表單。
6. 資料安全管理及人員管理：大學校院必須建立內部個人資料安全的管理制度，以及人員管理的制度。
7. 認知宣導及教育訓練：大學校院針對內部同仁，必須進行的認知宣導及教育訓練，包括：個人資料保護法及其施行細則、高等教育或技職教育相關法規、各校之資訊安全管理制度等，並應將教育訓練相關檔案、照片加以保存，以供日後佐證所需。
8. 設備安全管理：大學校院有關資訊安全之相關硬體、軟體、設備安全之管理制度，必須加以建立並落實執行。
9. 資料安全稽核機制：大學校院應就其個人資料管理制度之執行，進行內部稽核或外部稽核，並提供稽核報告與矯治措施，以供該校個資管理委員會，進行各單位績效評估之參考，並可做為日後持續改善之依據。
10. 使用記錄、進行軌跡資料及證據之保存：有關個人資料的蒐集、處理及利用之記錄、軌跡資料及證據，大學校

院均應妥善保存，以供日後佐證所需。

11.個人資料安全維護之整體持續改善：大學校院應依據內部稽核或外部稽核所提供之稽核報告與矯治措施，持續改善相關缺失，以便精進整體的個資安全管理制度。

八、通知當事人之義務

大學校院若發生個資外洩事故，必須立即調查事故發生原委，並以適當方式即時通知當事人。所謂「適當方式」，包括：言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之，但如需耗費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之，並敘明個資被侵害之事實及已採取之因應措施，提醒當事人留意詐騙電話，並請變更相關帳號密碼，以免遭到非法盜用。

九、公務機關之蒐集、處理、利用個資

依據法務部目前對於教育機構適用個資法的解釋，公立大學校院屬於公務機關，公務機關蒐集或處理個資時應有特定目的，並符合下列各款情形之一者：1.執行法定職務必要範圍內；2.若非執行法定職務之必要範圍內，則必須經當事人書面同意；3.如果前二種情形皆不符合，則蒐集或處理個資，必須對當事人權益不會造成侵害。

至於個資的利用，公務機關應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符，如果與當初蒐集之特定目的不相符合，公務機關便不得提供外部利用該個資。雖然如此，但如果符合個資法第16條所明定的下列各款例外情形之一者，便得為特定目的外之利用，包括：1.法律明文規定；2.為維護國家安全或增進公共利益；3.為免除當事人之生命、身體、自由或財產上之危險；4.為防止他人權益之重大危害；5.公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式，無從識別特定之當事人；6.有利於當事人權益；7.經當事人書面同意。

十、公務機關個資檔案公開及專人管理義務

與非公務機關不同，公務機關必須將所保有之個人資料檔案名稱、保有機關名稱及聯絡方式、個人資料檔案保有之依據及特定目的，以及個人資料之類別，於網站上公開並提供公眾查閱。另外，公務機關應指定專人，辦理個資安全維護事項。所謂「專人」，係指具有管理及維護個資

檔案之專業能力，且足以擔任機關檔案安全維護經常性工作之人員，而公務機關為使專人具有辦理安全維護事項的能力，必須辦理或使專人接受相關之教育訓練。

十一、違反個資法之民事責任

公務機關或非公務機關如果違反本法，導致個資不法蒐集、處理、利用或其他侵害當事人權利者，應負損害賠償責任，如為公務機關並適用國家賠償法相關規定，若非財產上之損害，亦得請求賠償相當之金額，並回復其名譽。每人每一事件，以新臺幣五百元以上二萬元以下，計算其賠償之金額，對於多數當事人權利受侵害之事件，合計最高賠償總額，以新臺幣二億元為限。

違反個資法的行為態樣不一，例如：違法蒐集個資、應履行告知義務而未告知、應通知當事人而未通知、逾期保存或利用個資、或其他個資被竊取、洩漏、竄改、毀損或滅失等情形。一旦發生個資侵害事故，往往受害人人數眾多，牽涉數量龐大的個人資料，如有二十位以上之受害人，以書面委任公益團體，便可由公益團體以自己的名義擔任原告，對於侵害個資之公務機關或非公務機關，提起團體訴訟。

團體訴訟之成本，遠低於個人訴訟之成本，且因受害人人數眾多，一旦形成社會事件，民氣可用，法院往往傾向保護一般民眾，且因個資侵權訴訟，以公務機關為被告時，採無過失責任，以非公務機關為被告時，採舉證責任倒置，皆對原告有利，極易造成公務機關或非公務機關面臨高額賠償責任。

十二、違反個資法之刑事責任

違反個資法第6條第一項、第15條、第16條、第19條、第20條第一項規定，或中央目的事業主管機關依第21條限制國際傳輸之命令或處分，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。雖然非意圖營利，犯前項之罪者，例如：洩漏個人資料，仍有刑事責任。若是意圖營利，犯前項之罪者，例如：盜賣個人資料，則處五年以下有期徒刑，並得併科新臺幣一百萬元以下罰金，刑責加重。

由於非意圖營利之違反個資法行為，目前已有民事賠償責任與行政處罰之相關規定，如果再課以刑事處罰，法律責任有過重之嫌，故行政院已經提出個資法修正草案，擬將非意圖營利之違法行為，加以除罪化，只處罰意圖營利的違法行為，但在上述修正草案完成立法程序前，非意圖營利之違法行為，仍有刑事責任。

十三、違反個資法之行政責任

中央目的事業主管機關或直轄市、縣（市） 政府，得行使行政檢查權，派員進入檢查、扣留或複製檔案，亦得強制為之，屆時得率同資訊、電信或法律等專業人員共同為之，例如：教育部對於大學校院，得進行個資保護業務的訪視或評鑑，聘請上述相關專長之專家學者，藉由訪視或評鑑，督導各大學校院落實個人資料保護，如有違反個資法相關規定之大學校院，教育部得處以行政罰，例如：扣減對於大學校院的獎補助款。

十四、不適用個資法之情形

下列二款情形之一者，不適用個資法：1.自然人單純為個人或家庭活動之目的，蒐集、處理或利用之個人資料。例如：某人不小心遺失手機，導致手機中所蒐集之親朋好友個資外洩，由於上述個資是自然人單純為其個人或家庭活動之目的所蒐集的個資，故不適用個資法，遺失手機者無須負擔法律責任；2.於公開場所或公開活動中，所蒐集、處理或利用之未與其他個人資料結合之影音資料，例如：大學校院舉辦運動會、畢業典禮或其他公開活動，參與上述公開活動的自然人，雖被攝入影片或照片中，但因沒有與其他個人資料相結合，故不得主張個資法之保護。

十五、個資法修正施行前之個人資料

個資法修正施行前，非由當事人提供之個人資料，依個資法第9條之規定，應於處理或利用前告知當事人，並應自個資法修正施行之日起一年內，完成向當事人告知個人資料來源及下列各款事項：1.公務機關或非公務機規名稱；2.蒐集之目的；3.個人資料之類別；4.個人資料利用之期間、地區、對象及方式；5.當事人依個資法第3條規定得行使之權利及方式，凡逾期未告知而處理或利用上述個資者，以違反個資法第9條規定論處。

由於金融業、電信業等諸多行業反應，過去保有非由當事人所提供之個人資料數量極為龐大，執行困難且成本浩大，勢必無法於本法施行後一年內，完成補行告知當事人之義務，因此本條目前暫緩施行，並由行政院提出修正草案，刪除本法施行後一年內，對當事人完成補行告知之規定，公務機關或非公務機關僅須於處理或利用該個資前，對當事人完成補行告知即可。

肆、大學校院的因應之道

大學校院保有學生、教師、職員或廠商之個人資料眾多，日常校務運作涉及個人資料的蒐集、處理、利用、國際傳輸等

行為，上述行為的適法性，除必須依據高等教育或技職教育等相關法規的規定外，尚且必須符合個資法及其施行細則的相關規定，教育部是各大學校院的中央目的事業主管機關，更應善盡督導管理之責。

一、教育部之因應

教育部電子計算機中心，一直是教育部推動個人資料保護的聯繫窗口，法務部研修個資法施行細則時，曾請教育部通知所屬各級學校針對個人資料的特定目的與個人資料類別，表示相關意見。教育部曾配合法務部之執法時程，要求國立大學校院於民國100年7月31日前完成下列事項：1.個人資料檔案清查作業；2.特定目的、資料類別修正作業。其後，並配合法務部「公務機關個人資料保護事項公開作業」，要求國立大學校院辦理個人資料保護事項公開作業。

教育部電算中心自民國102年1月1日起，升格為教育部資訊及科技教育司，主導教育機構個資保護政策，預計於民國102年12月完成研擬「教育體系個人資料保護安全管理措施」及「私立大專校院個人資料保護管理架構」。

未來教育部與法務部應針對大學校院特種個資之蒐集、處理或利用之範圍、程序及其他應遵行事項之法規命令，共同研擬商訂。同時，教育部得指定各私立大學校院訂定個人資料檔案安全維護計畫，要求各校依據個資法之相關規定，管理並維護校內學生、教師及職員個人資料之安全。教育部亦得訂定有關大學校院業務終止後，個資處理方法標準之法規命令，例如：大學校院個人資料保存的期限，以及保存期限屆滿後，個資銷毀或刪除之處理流程等相關規定。

二、大學校院之因應

個資法自民國101年10月1日起正式施行，教育部預計於民國102年12月始完成研擬「教育體系個人資料保護安全管理措施」及「私立大專校院個人資料保護管理架構」，大學校院面對違反個資法的法律責任風險，教育部上述相關因應措施顯然緩不濟急。

目前全國大學校院大多皆已導入「教育機構資訊安全驗證標準（Information Security Management System，以下簡稱ISMS）」，但各校ISMS驗證範圍有其侷限性，往往僅偏重資訊系統安全，無法涵蓋個人資料蒐集、處理、利用等完整流程的管理，並且未能納入全校各單位一體適用，不符合個資法的相關規定。

故目前若干大學校院，自主選擇導入「個人資料管理系統（Personal Inform-

ation Management System，以下簡稱PIMS）」之國際驗證標準，例如：聯合國國際標準組織所公布之ISO/IEC 29100:2011，但因PIMS涉及法律、資訊與流程三源管理架構，在各校人力精簡的現實環境下，難以現有的組織與人力，完成建置個人資料保護管理制度，故有必要委託外部輔導機構，藉由其專業知識與經驗，建置該校個人資料保護管理制度，並就其導入之個資管理制度，進行個資法適法性評估，以確保符合個資法及其施行細則之相關規範，並向第三方驗證機構，申請國際標準驗證，通過上述驗證並取得證書。

上述相關配套工作，包括訂定各校的「個人資料保護管理辦法」，並執行下列工作項目，包括：1.成立跨單位的「個人資料保護管理委員會」，並由副校長以上之主管，擔任委員會召集人，委員會成員涵蓋各行政與教學單位，並配置相當資源； 2.透過個資清查，建立個資清冊，界定個人資料之範圍；3.進行個人資料的風險評估及管理機制； 4.針對事故預防、通報及應變機制，進行個資事故模擬演練；5.建立個人資料蒐集、處理及利用之內部管理程序； 6.明訂資訊安全管理及人員管理法規、流程及表單； 7.進行認知宣導及教育訓練； 8.建立設備安全管理； 9.建立個人資料安全稽核機制；10.使用紀錄、軌跡資料及證據之保存；11.個人資料安全維護之整體持續改善。

伍、檢討與展望

大學校院保有學生、教師、職員或廠商之個人資料眾多，數量龐大，日常校務運作中，除可能面臨當事人查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用、請求刪除個人資料外，如果發生違反個資法之事故，將可能面臨當事人的行政申訴或司法訴訟、新聞媒體的負面報導、教育部或縣、市政府的行政檢查（訪視或評鑑），不但有損校譽，學校與相關承辦人員都可能因此負擔法律責任。

個資法的施行，對於大學校院的各項業務，產生重大影響，由於各校個資保護涉及法制規範、資訊安全與管理制度，故必要時建議委託外部輔導機構，藉由其專業知識與經驗，建置該校個人資料保護管理制度，並就其導入之個資管理制度，進行個資法適法性評估，以確保符合個資法及其施行細則之相關規範，並向第三方驗證機構，申請國際標準驗證，通過上述驗證並取得證書。