大學因應個人資料保護法的具體做法與成果評估 --以臺北醫學大學為例

萬序恬[a] 蔡宛真[b] 李佩珊[a] 林建煌[b] 邱泓文[a]
[a]臺北醫學大學資訊處、[b]臺北醫學大學秘書處
wanhsu@tmu.edu.tw

摘要

繼個人資料保護法於民國 99 年通過，個人資料保護法施行細則也在民國 101 年 10 月 1 日公告施行。不論是政府機構或是私人企業，立刻就面臨訴訟賠款的可能，因此從正式公告實施以來，各大型機構紛紛提出建立管理流程、導入標準、個資盤點等各項措施，企圖降低風險，同時也達到個人資料保護法的立法目的-保護當事人權益。

臺北醫學大學資訊處自民國 96 年起即開始導入資訊安全管理系統，並於民國 98 年通過 ISO27001 驗證，由於個資法施行細則的公告實施，除了仍進行年度 ISO27001 驗證，同時亦展開個資法適法性查檢，試圖從行政流程面實質探討各項個資風險，歷經六個月的全面性查檢，完成本校 18 個行政單位共 361 項流程，2,144 項行為的個資風險評估。本次作業同時也針對校內行政用電腦進行電腦個資檔案普查，範圍涵蓋學術行政共 34 個單位 207 台電腦，實際普查率約四成，其中發現有高達九成的電腦藏有個資檔案，含個資之檔案總數量超過 34 萬個，進一步檢查檔案風險程度，發現高風險個資檔案約占 5%，其中人力資源處的高風險檔案比率達到 10.7%，為平均值之兩倍高。

本次盤點查檢的結果也發現行為流程中僅約四成是有電子檔或是有資訊系統輔助，顯見有許多的行為仍是以紙本保存或是流通。本次查檢成果將成為未來本校建立個資管理流程的基礎架構，其經驗也希望能分享給其他各大學作為參考。

關鍵詞：隱私權、個人資料保護、個資盤點、風險評估、適法性

Abstract

The Personal Information Protection Act (PIPA) has been passed in 2010. The Regulation of the PIPA has been passed in 2012 as well. To avoid huge lawsuits, either enterprises or organizations are seeking solutions to be compliant with the PIPA. These actions might include building a personal information management system (PIMS), or doing a personal information inventory check.

In order to fulfill the requirement of the PIPA, Taipei Medical University had made a decision on doing personal information inventory check first. During the past 6 months, the whole action has checked as many as 361 workflows with total 2,144 procedures. Moreover, in the digital files checking process, we've found that about 5% of 340 thousands files had been identified as "high risk" ones. The highest rate of high risk files were found in computers of the human resource department. It is 10.7%, about twice of the average.

In the action, we've also found that there are only about 40% of regular procedures involving digital files or systems. Thus, procedures done in paperwork should be paying more attention to.

The result of this action is valuable for TMU to build a suitable PIMS in the future. We also wish it is a good experience to share with other universities in Taiwan.

Keywords: Personal Information Protection Act, Personal Information Inventory Check, Risk Management, Legality.

1. 前言

1.1 個人資料保護法

民國 94 年大法官釋憲文第 603 號已說明隱私權為人民不可或缺的基本權利之一，係受憲法保障，其中包含個人自主控制其個人資料之資訊隱私權。[1] 由於資訊科技以及網路服務的發展，數位資訊隨著網通傳輸，個人資料的傳遞變成無遠弗屆，既迅速且傳遞又廣。在台灣，早在民國 84 年就訂定有「電腦處理個人資料保護法」，規範如何使用電腦處理個人資料，這是本國個人資料保護的濫觴。但有鑒於此法的範圍侷限性過大，於民國 99 年經立法院通過公佈實施「個人資料保護法」，以更全面性的角度規範個人資料的搜集、處理、利用原則，更重要的是加上團體訴訟規定，並提高罰則。隨後並於民國 101 年 10 月 1 日公告施行「個人資料保護法施行細則」。

自個人資料保護法上路以來，已有諸多的研究。諸如從法律面向探討此法的適法性，各國的法規發展現況、政府對應法規改善等[2]。也有從資訊科技面向探討隱私保護技術，例如如何去識別化、檔案加密、權限控管等。

賠償與訴訟的規範是此法備受矚目的原因之

一，根據日本經驗，2007 年遭外洩個資的人數超過三千萬人，因此付出的賠償金額，相當於八千六百億台幣，足以讓台積電蓋兩座十八吋晶圓廠。[3]

私立大學的主管機關雖然如同國立大學皆為教育部所管，但卻被定義為「非公務機關」，造成不少困擾。因此教育部於民國 102 年擬定「私立學校及學術研究機構個人資料檔案安全維護計畫辦法草案」，目前尚在研擬階段，希望未來能解決學校因個資法施行後所產生之問題與困難。

1.2 個人資訊管理系統

除了法規面項考量，根據經濟合作暨發展組織（Organization for Economic Co-operation and Development，簡稱 OECD）的資料保護八大原則所制定的 BS10012 標準則是目前全世界最通用的個人資料管理系統(PIMS)建立參考[4], 此八大原則為：受到公平合法的處理、僅為具體指明的目的取得、適當且不過渡、正確且最新、保留時間不超過必要程度、處理符合法律賦予之個人權益、獲得安全保障、移轉須受適當保護。以上皆可以作為個人資料保護實作時各項實際配套措施的檢核指標，國內目前也有機構通過這項驗證[5]。預計於 2013 年底公佈的新版 ISO27001 也將整併個資保護的內涵。個人資訊管理系統的建立勢必將來一定會成為各機構實作個資法適法性時的必要手段。

2. 實施過程與方法

行政管理學上推動的管理體系，大多都遵循 PDCA 的品管循環架構，亦即規劃(Plan)、執行(Do)、查檢(Check)、行動(Action)，以下分別說明。

2.1 規劃準備階段

臺北醫學大學導入 ISO 品質驗證系統多年，近年已通過 ISO9001, ISO14001, OSAS18001, AA1000 等多項品質認證。資訊處於 2007 年起即開始導入資訊安全管理系統(ISMS)，並於 2009 年通過 ISO27001:2005 驗證，因此對於資訊安全的管理與維護已有基礎。個資法的指導方針雖然於此版本中有提到一些，但是跟全校性的個資保護仍有距離，所以本校於 2012 年底開始規劃個資法的因應措施，其重點放在行政流程面向的行為盤點，並由本校秘書處統籌規劃盤點與後續之改善作業。

除了規劃作業外，全校性法規教育訓練也是此階段的重點，基本教育訓練涵蓋個資保護基本知識、法律條文、搜集處理利用定義、個資認定告知同意的要求等。

2.2 執行盤點階段

盤點作業主要分技術盤點及行為盤點兩大部分，分述如下：

技術盤點是使用 PrivacyID 工具查檢本校列管之行政用個人電腦，依據檔案機敏性、可辨識度及數量級距檢查含個資檔案之資產等級，進一步並可以作為風險評估的標準[6]。

機敏性分低、中、高三級：

- 低機敏性為依法可公開或是經同意公開的資料，如：公司負責人等。
- 中機敏性為一般個資，如：姓名、電話、生日等。
- 高機敏性為個人財務、安全影響較大的個資，如：特種個資、私密金鑰、信用卡號等。

第二部分為行為盤點，係召集各單位負責同仁清查含個資之行政流程，依照個資主體，搜集處理利用目的與方式逐條明列。

2.3 查檢階段

適法性查險領域依照台灣個資法共分為 14 項領域作業檢查(如圖 **1**)，查檢範圍涵括各項文書合約、作業使用表單及記錄、處理流程。與作業業務單位依照蒐集、處理、利用的順序進行查檢。

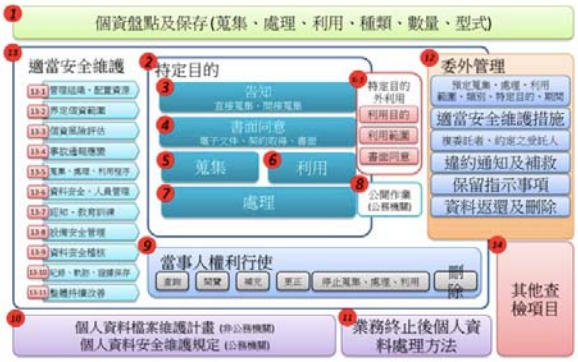

圖 1 14 項個資查檢項目

(資料來源：DeKnow Technology Service)

盤點時有請受盤單位填寫檔案種類，主要分為紙本或是以數位方式進行，如：存成電子檔傳遞、或是使用資訊系統。

此階段會完整記錄各項查檢結果，以供未來追蹤改善之用。

2.4 行動改善階段

聘請流程以及法律顧問針對盤點與查檢結果進行諮詢與改善建議。進行改善或後續行動方案的優先順序為：立即違法事項、待釐清事項、管理系統建立，並定時進行查檢作業，持續進行改善。

3. 實施結果

臺北醫學大學於 2013 年初確定施行的策略後，隨即於 2013 年 4 月開始正式作業，至 8 月上旬完成所有盤點工程，總計進行行為盤點及技術盤點兩大項，所有主要工作時數總計如表 **1** 所示，此表所載之時數主要以大家出席的時數為主，並不計個別單位人員所花費撰寫文件的時間。盤點結果則分述於以下兩節。

表 1 臺北醫學大學個資盤點作業實施結果

(單位：工時)

行為盤點				技術盤點	合計
教育訓練	流程盤點	告知文件	法律諮詢		
13	40	40	16	40	149

3.1 行為盤點結果

本次參與行為盤點共有 18 個校內行政單位參與，總計盤點 361 項流程。流程依照蒐集、處理、利用分別列出各項行為，總計有 2,411 項行為，其中蒐集行為佔 10.5%，處理行為佔 69.3%，利用行為佔 19.8%。其中行為數量最多的為教務處，共盤出 539 項行為，其次為研發處(324)、學務處(295) ，各處室各項行為盤點數量比例如圖 **1** 所示。

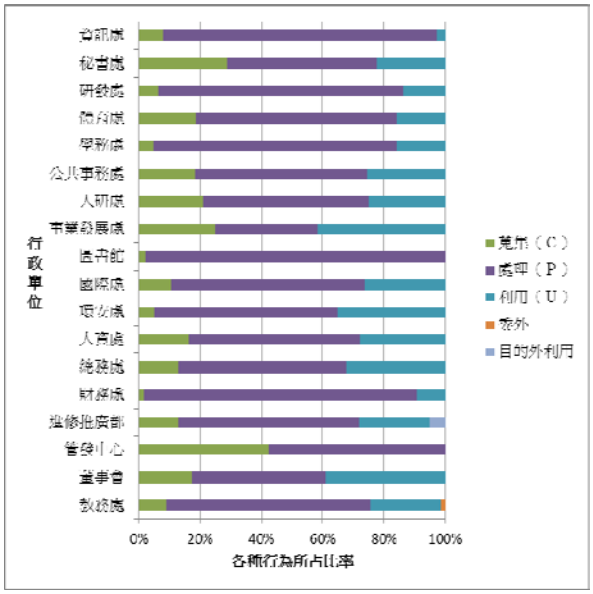

圖 2 各單位個資行為盤點比例

個資資料檔案形式中，紙本佔 60.35%，數位形式佔 39.65%。

行為盤點後，再由顧問進行法規面適法性評估，共有 151 項待改善，佔 7%。主要需改善項目為未正確告知個資主體個資利用範圍，其次為須定義管理權責單位，以利後續管理。

3.2 技術盤點結果

總計全校預計盤點行政用電腦共 225 台，最後成功盤點 92 台電腦(40.9%)，其中 83 台電腦含有個資檔案，佔已盤電腦的 90.2%。

本次盤點出含個資的檔案有 342,514 個，若將檔案依照敏感程度分高、中、低三級區分，則高風險檔案數為 17,610 個，佔 5.14%，最多的個資是姓名、電話、身分證號。若依照盤點之行政單位分析，則人資處所抽樣盤點的電腦檔案中有 10.68%的檔案為高風險檔案，為比例最高的單位，其次為學務處，有 7%的檔案為高風險檔案，皆高於全校平均值。

另外，此次盤點作業中有約一成的電腦因為查檢程式與該電腦系統程式有衝突，導致作業失效。

4. 討論

本校過往已進行多項品質驗證系統並獲得通過，也於民國 102 年初獲得教育部同意可進行自我校務評鑑，顯見本校平時皆已妥善準備各項評鑑指標的品質管理流程管理，因此對於整體個資盤點作業，行政配合度高，作業時程短。惟校內目前尚未建立完整的個人資料管理系統，因此盤點時會發現不論是從資料保存或是告知層面，各行政單位對於個人資料管理的落差是存在的，導致在盤點時步調不一，亟需如「私立學校及學術研究機構個人資料檔案安全維護計畫辦法草案」中所訂定之作法如管理制度制訂、指定專責單位人員負責處理相關事務等，並妥善制訂詳細的員工教育訓練計劃，詳細要求教職員要具備一定的個資保護知識以及了解標準作業準則。

同時在教育面向也應同時設計類似課程，以指導學生了解相關的法律議題，特別是本校為醫學衛生類組學校，學生未來將有機會處理大量的特種個資如病歷、健康記錄等。同時可了解如何保障自己也可銜接職場需求。

本校此次盤點作業在技術盤點的部分，也明顯看出教職員對於個資法的認知不清，導致成功盤點比例較低，宜多加宣導並加強盤點工具的使用說明。

另外，由本校盤點的結果來看，數位檔案僅佔約四成，顯見在教育機構中，使用紙本處理的流程相當多，因此個資法的適法性查檢除了資訊安全查檢中經常查驗的數位系統部分，一般行政作業流程中的紙本作業項目也是非常重要的部分，並非完全是資訊單位的業務範圍。

參考文獻

[1] 中華民國大法官解釋，釋字第 603 號。

[2] 黃銘輝，翁清坤，“個人資料保護法施行後現行臺北市法規之衝擊與因應.” Dec. 2012.

[3] 黃昭勇，謝明玲，何榮幸，“一次搞懂個資法(3)：風暴解析○○又××，個資法保護了誰？” http://www.cw.com.tw/blog/blogTopic.action?id=258&nid=3004. Jan. 2013.

[4] 章鈺，“如何架構個人資料管理系統，以符合個人資料保護法要求”，財金資訊季刊, No.71, pp.13-18, Jun. 2012.

[5] 中央通訊社，“個資防護領先全國，中興大學獲 BS10012 國際認證”, Jan. 2013.

[6] PrivacyID User Manual, amXecure Co. Ltd. 2012.