組織落實個人資料保護法執行方案之研究

作者[1]林美月　作者[2]孫思源
[1]國立高雄第一科技大學 maylin@nkfust.edu.tw
[2]國立高雄第一科技大學 sunnyy@nkfust.edu.tw

摘要

有鑑於保護個人資料愈來愈受重視，先進國加政府均立法規範，確保個人資料受到適當保護與運用，我國立法院於 2010 年 4 月 27 日三讀修正通過,並於 5 月 26 日公布個人資料保護法。

在未來組織無論規模大小、擁有個人資料數量多寡，都會受到個人資料保護法規範，此法進而影響組織在蒐集、儲存、利用、傳輸、及銷毀個人資料上，加上對於受罰組織負有刑法與民法之責，賠償金額最高可求償到兩億元，無疑對組織造成莫大衝擊。因此，組織該如何落實個人資料保護法執行方案是現階段重要的研究課題。

個人資料保護法在眾人的期盼下正式三讀通過，由於其牽涉範圍甚廣，個人資料保護法風暴來襲，組織面臨法規遵循，又要在不影響組織正常業務運作之下，如何利用公佈施行後的緩衝期來做好相關的準備，以免誤觸法而面臨鉅額求償，這些都是組織刻不容緩的工作。新個人資料保護法是繼勞基法、公平交易法及消費者保護法之後，對國內組織衝擊非常強的法律。顯示隨著新個人資料保護法實施在即，個人資料外洩議題已是各界不得不正視的問題。

本論文主要是採用文獻探討法、文件分析比較，在理論端先透過文獻探討方式，蒐集國內外個人資料管理系統(Personal Information Management System)、並與國內個人資料保護法結合，期望能夠提供一套個人資料保護管理對策，提供組織導入個人資料保護法解決方案，做為參考與遵循之用，幫助組織達成遵法目的，降低罰鍰與訴訟風險，且讓組織善盡個人資料保護與管理職責。

中文關鍵詞

個人資料保護法、個人資料管理制度、BS 10012、ISO 27001、PIMS

組織落實個人資料保護法執行方案之研究

第一章 緒 論

第一節 研究背景與動機

新舊版個人資料保護法之間的最大差異，在於新法的資料保護範圍，不限於電腦處理的資料，且凡是有蒐集、處理及利用他人個人資料的所有法人與自然人，皆在新法規範之列，不像舊法所規範的公務機關，與徵信、醫院、學校、電信、金融、證券、保險、大眾傳播等八大行業領域。更重要的是，新法增加了有關個人資料外洩舉證責任規定，亦即資料蒐集方，必須證明本身並無過失或無故意違法，因此，各種相關歷史資料都必須留存完整紀錄，以作為將來舉證之用。

在未來組織無論規模大小、擁有個人資料數量多寡，都會受到個人資料保護法規範，此法進而影響組織在個人資料蒐集、處理及各式的運用，另加上個人資料保護法對於受罰組織，在民事與刑事的加重處理，賠償金最高可求償 2 億元，且還可能面臨 5 年以下的有期徒刑，此法無疑對組織造成莫大衝擊。因此積極著手規劃及實行個人資料的資安防護是組織現階段重要的研究課題。

ISO 27001 是資訊安全管理系統的國際標準，但組織遵循 ISO 27001 無法代表對於個人資料保護工作的完整性。現有組織資訊安全主要重點均著重在組織運作機密資料，較少以個人資料的觀點出發，造成個人資料保護上有所不足，造成組織觸法的可能性。對組織來說，必須調整、建置合適的資訊安全架構，來控管個人資料作業流程，以符合個人資料保護法法規要求事項，就需要一套完整的管理機制做為依循標準。

本論文主要是採用 Gowin’s Vee 的研究策略，在理論端先透過文獻探討方式，蒐集國內外個人資料管理系統(Personal Information Management System)、並與國內個人資料保護法結合，期望能夠提供一套個人資料保護管理對策，提供組織導入個人資料保護法解決方案，做為參考與遵循之用，幫助組織達成遵法目的，降低罰鍰與訴訟風險，且讓組織善盡個人資料保護與管理職責。

第二節 研究目的

台灣個人資料保護法於2010年5月26日業經總統公布，唯其實施細則尚在研議中未公告，不過距離正式公告實施日期應屬不遠，但從法的角度而言，此法對各種組織機構，均會有相關，同時對執行業務上，也將造成或大或小的限制與困擾，如稍處理不當，將對組織機構帶來莫大的影響。

目前政府相關單位均積極大力的宣導、推廣中，不斷地告知，此法未來可能造成多大的衝擊，並呼欲應提早做完善的規劃、準備，唯獨敕少有具體、可行的執行步驟，供各組織機構來遵循。本研究目的是由法律的角度，再配合資訊安全的技術面、及組織管理面，對個人資料的風險進行風險評鑑，個人資料的安全儲存、處理、運用，及組織機構的特性，來探討組織機構於執行業務時，如何有效來執行、並遵守個人資料保護法，以免觸法。

新版個資法會要求保護個人資料的蒐集、處理、利用及國際傳輸，而ISO27001資訊安全管理系統(ISMS)著重於個人資料的”處理”階段，因此還須建立個人資訊管理系統(PIMS)，其主要內容為Plan(規劃)、Do(執行)、Check(檢查)、及Act(行動)四大循環，推

動符合個人資料保護法的管理體系。

從資訊的生命週期來看，個人資訊的產生、處理、傳遞、儲存、復原、銷毀等過程，都需要有適當的安全管控措施，這部份可以透過管理制度的規範，或是技術性的保護，來防止不當處理個資事件的發生。因此，組織必須要將個人資訊視為有價值的資產，無論其呈現的形式是什麼（例如紙本、聲音、影像、電子檔案等），都必須評估其可能存在的安全弱點，以及可能面臨的威脅，並且透過風險評鑑的過程，來找出其風險的高低，然後針對無法接受的風險，進行風險處理和後續改善行動。

隨著個資外洩事件不斷發生，目前已有許多政府單位與企業，對於個人資訊保護的問題日漸重視，但是卻往往不知該如何著手，找不到一套可以依循的規範與標準。本研究目的，正好可做為組織在建立個人資訊保護機制時的最佳參考，藉由標準所提供的基礎架構（Framework），配合 PDCA 的管理運作方法，能夠透過建立系統化的個人資訊管理制度，來達到保護個資的目的，更可進一步符合個人資料保護法法規的要求。

第二章 文獻探討

本章文獻探討總共分成四個章節，第一節為個人資料保護法議題演進、第二節為個人資料管理制度國際概況、第三節為台灣個人資料管理制度概況、第四節為ISMS與個人資料之關聯因素，其中第二節又分成四小節，第一小節為英國個人資料保護管理制度--BS 10012:2009標準、第二小節為日本個人資料保護管理制度--JIS Q 15001標準、第三小節為德國個人資料保護管理制度、第四小節為美國個人資料保護管理制度，以用來加強本研究模式發展的基礎。

第一節 個人資料保護法議題演進

個人資料之資訊隱私權，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭 露之決定權，並保障人民對其個人資料之使用有知悉與控制權、及資料記載錯誤之更正權。

在電腦普遍運用之後，個人資料的蒐集、處理與利用更是容易。這種趨勢無疑地已強烈威脅到個人資料的隱密性，當個人資料輕易地暴露於有心人的侵襲與操控之後，個人隱私及其權益尊嚴不免飽受威脅。由於傳統上對隱私權保障的思考，乃以「資 料保護」（Data Protection）為中心的思路，「資訊隱私權」（Information Privacy）的概念因應而生，以對抗資訊時代中隱私權所受到的衝擊。所謂「資訊隱私權」，是指「非侷限於不讓他人取得我們的個人資訊，而是應該擴張到由自己控制個人資訊的使用與流向」，更進一層指「在沒有通知當事人，並獲得其書面同意之前，資料持有者，不可以將當事人為某特定目的所提供的資料，用在另一個目的上」。

一、個人資料保護簡史

個人資料保護從 19 世紀末在美國已受重視，迄今 21 世紀初，全世界各國均紛紛制定符合自己國家的個人資料保護法，以下說明主要個人資料保護演進簡史：

1890 The Right to be Privacy(美國 Warrant,Brandeis)

1974 美國 隱私權法(Privacy Act)

1977 德國 聯邦資料保護法 Bundesdatenschutzg esetz

1980 OECD 八大原則；1984 英國資料保護法

1995 歐盟個人資料保護指令(95/46/EC)、台灣電腦處理個人資料保護法

1998 日本 Privacy Mark；1999 日本 JIS Q 15001 個人資料保護標準

2003 日本個人資料保護法

2004 APEC 個人資料九大原則、台灣提出個人資料法修正草案

2009 英國 BS10012：2010 台灣個人資料保護法通過

二、台灣個人資料保護法簡介

台灣個人資料保護法於 2010 年 4 月 27 日立法院第 7 屆第 5 會期第 10 次會議通過，於 2010 年 5 月 26 日業經總統公布。共分六章 56 條

第一章 總則(第 1~14 條)

第二章 公務機關對個人資料之蒐集、處理及利用(第 15~18 條)

第三章 非公務機關對個人資料之蒐集、處理及利用(第 19~27 條)

第四章 損害賠償及團體訴訟(第 28~40 條)

第五章 罰則(第 4 ~50 條)

第六章 附則(第 51~56 條)

第二節 個人資料管理制度國際概況

國際組織與個人資料保護之關係：

經濟合作既發展組織(Organization for Economic Co-operation and Development , OECD)

亞太經濟合作組織(Asian-Pacific Economic Cooperation , APEC)

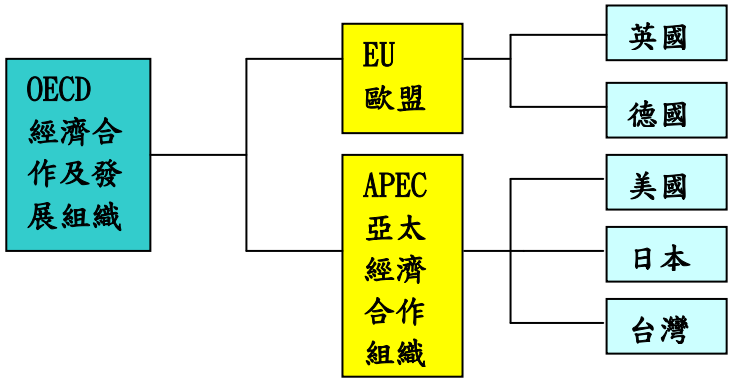

圖 1 國際組織與個人資料保護之關係

一、英國個人資料保護管理制度--BS 10012:2009 標準

（一）資料保護法

2000 年 3 月 1 日正式生效施行資料保護法(Data Protection Act of 1998)，資料保護法雖擴大將人工資料一併納入保護客體，但非謂所有之人工資料均受法保護，依法規定，受保護之人工資料，須該筆資料為相關建檔系統(relevant filing system)之一部份，或意圖作為相關建檔之一部份。

（二）BS 10012 個人資訊管理標準簡介

英國標準協會(BSI)於 2009 年正式發佈 BS 10012:2009 個人資訊管理系統（Personal Information Management System,PIMS）；個人資訊管理系統(PIMS)提供了一個架構，讓組織能維持和改善對資料保護法律及國際優良實務的遵循。

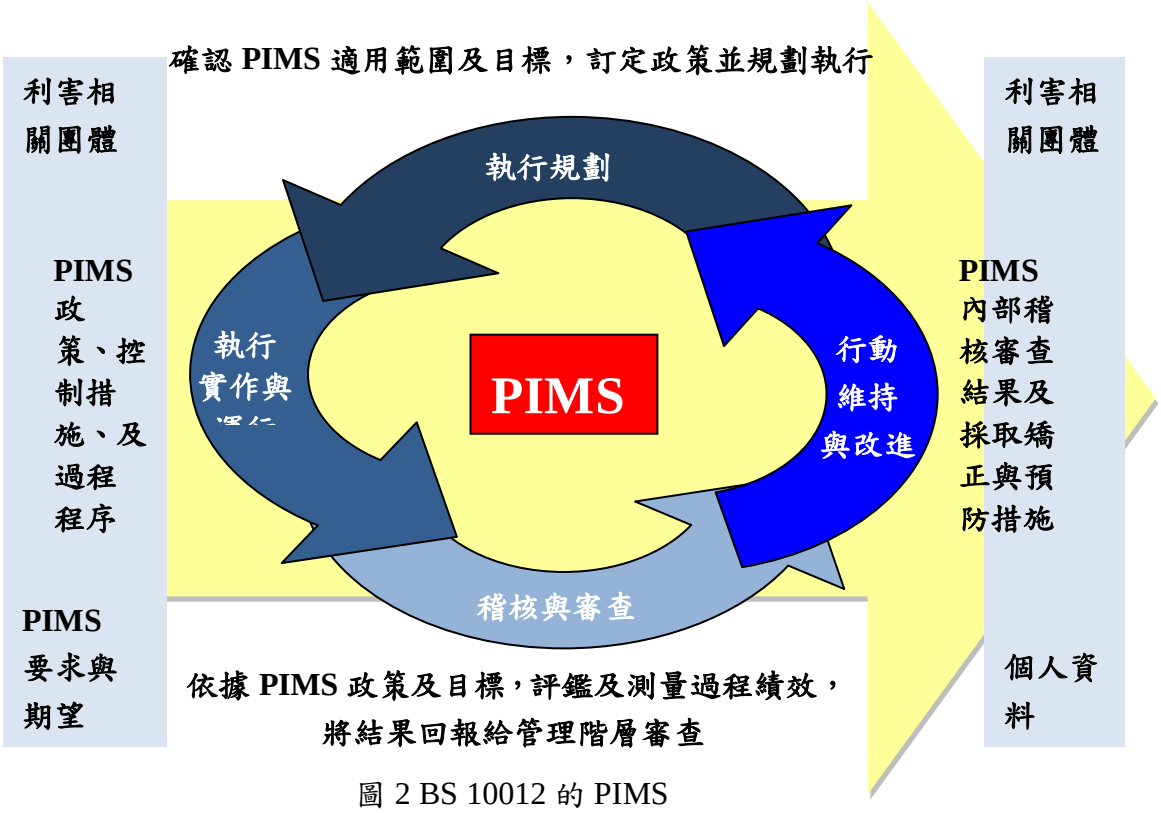

圖 2 BS 10012 的 PIMS

BS 10012 的全名為「資料保護－個人資訊管理系統之要求（Data protection–Specification for a personal information management system）」，其中 BS 指的是英國標準，後面則為標準編號，至於系統指的是文件化的管理制度，能作為有效的個資法規內外部的評鑑標準。

BS 10012 內容共有 7 章，第 0~2 章為標準介紹、適用範圍與名詞定義之說明，第 3~6 章則為個人資訊管理制度的架構要求。

計畫與建立 PIMS--第 0~2 章、實施與運作 PIMS--第 3 章、監督與審查 PIMS--第 4 章、維持與改善 PIMS--第 5 章、保護個資，刻不容緩--第 6 章。

二、日本個人資料管理制度--JISQ15001：2006 版

（一）個人資料保護法 (最新修正平成十五年七月十六日法律第 119 號)

日本於 2003 年制定「個人資料保護法」，俾謀求個人隱私可確切獲得保障。其綱要:第一章 總則(第 1~3 條)、第二章 國家暨地方自治團體之責任義務等(第 4~6 條)、第三章 個人資料保護之相關措施等(第 7~14 條)、第四章 個人資料處理業者之義務等(第 15~49 條)、第五章 雜則(第 50~55 條)；第六章 罰則(第 56~59 條) 。

日本個人資料保護法的主要內容：適用於處理 5000 人以上資料的所有機構或個人，這些機構或個人在處理資料時，必須遵守規範。

（二）個人資料管理制度-- JISQ15001：2006 版

日本情報處理開發協會（Japan Information Processing Evelopment Corporation，以下簡稱 JIPDEC）在經濟產業省指導下，依據日本「工業標準化法」之規定，及 2003 年日本政府公告「個人資料保護法」，並於 2005 年正式施行。於 2006 年修正 JIS Q 15001：2006 規範。成為現階段日本企業能否取得「隱私標章」(Privacy Mark：

P-MARK）之審查指標。

日本個人資料保護法，JIS Q 15001,Privacy Mark 隱私權標章

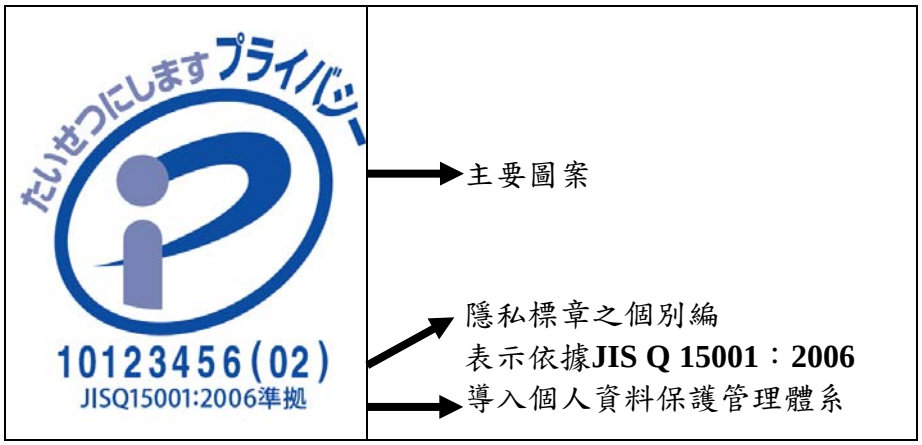

圖 3 JIS Q 15001,Privacy Mark 隱私權標章

三、德國個人資料保護管理制度

（一）個人資料保護法--聯邦資料保護法(Bundesdatenschutzgesetz)

2003 年 1 月 14 日公告最新聯邦資料保護法，計有 6 章共計 60 條條文，條文規範內涵包括與資料保護相關之各項原理原則，例如限制蒐集原則（又稱直接原則，如第 4 條第 2 項、第 13 條第 2 項第 1 句）、內容完整正確原則（如第 20 條第 1 項前句、第 35 條第 1 項）、目的明確原則（或稱目的拘束原則，如第 14 條、第 28 條第 1 項）、限制利用原則（如第 31 條）、安全保護措施原則（如聯邦資料保護專員制度措施及第 9 條第 1 句之附件明確規定之安全措施）、公開原則（第 13 條第 2 項前句之資料應向當事人蒐集、第 33 條關於告知之規定）及個人參與原則（如第 19 條至 21 條、第 33 至 35 條）及責任原則（如第 7 至 8 條之損害賠償與罰則）等。而其在立法體例架構上則依序由總則、公務機關之資料處理、非公務機關及公法上營利事業體之資料處理、特別規定、罰則及過渡條款分別規範之。

1. 資料保護法(德文版)：http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg03.htm
2. 資料保護法(英文版)：http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg01_eng.htm

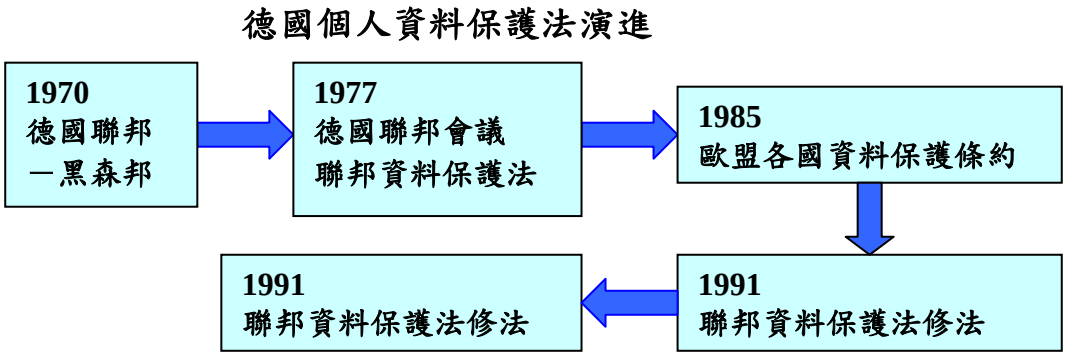

圖 4 德國個人資料保護法演進

（二）個人資料管理制度

・2009 年二月實施歐盟隱私權標章：由 8 個 EU 會員國中 9 個成員/公司參與

發展－ULD,ITA,TUVit,CNiL,Ernst&Young….

圖 5 歐盟隱私權標章-2009

・2010 年 5 月 EuroPriSe Criteria ：European Privacy Seal

圖 6 歐盟隱私權標章-2010

德國隱私權標章簡介

・在隱私與信賴的拉鋸間提供確保機制。

・從個人角度出發，涵蓋 C2B, C2G，乃至於 B2B

・促進隱私保障機制與保護技術的開發與提升。

・驗證隱私保護措施的符合性。

・藉由經濟活動與市場機制達成主動式的個人資料保護。

德國隱私權標章說明

Gütesiegel **•Voluntary product audit4B** **•Product/service suitable for use in public sector** **•Sect. 4 (2) LDSG and state ordinance, DSAVO** **•Since 2001**	**Audit** **•Voluntary process audit4P** **•Public sector only** **•Sect. 43 (2) LDSG and state ordinance, HDSA** **•Since 2001**

圖 7 德國隱私權標章

四、美國個人資料管理制度

（一）個人資料保護法

科技為我們帶來了便利，卻也帶來了意想不到的麻煩，小自個人隱私，大至企業甚至是國家機關之隱私，都有可能在電腦鍵盤觸動的瞬間被洩漏出去。因此，世界各國開始重視日益嚴重的資訊隱私侵害問題。像美國於一九七四年所通過的「隱私權法」，就特別強調「公平使用原則」，其認為：「在尚未通知當事人並獲得其書

面同意以前，資訊擁有者不得將人民為某種特殊目的所提供之資料，使用在另一個目的上」，在隱私權法施行後，更陸續於一九八六年推動電子通訊隱私權法、一九八七年通過電腦安全法等，以保護個人資訊之隱私。

第三節 台灣個人資料管理制度概況-- TPIPAS DP Mark 標章

經濟部商業司委託資策會研擬「台灣個人資料保護與管理制度(Taiwan Personal Information Protection and Administration System；TPIPAS)」，協助業者了解保護個人資料的重要性，並透過內化法令遵循的作法，建立個人資料管理與保護制度。

TPIPAS 係參考日本、德國等個資保護成效良好的制度規範所建構而成，經濟部商業司將協助與輔導企業導入此制度，並於通過驗證機制及程序後，發給「個人資料隱私保護標章（Data Privacy Protection Mark；DP Mark)」，以便消費者辨認業者是否合乎個資保護規範，藉此提升消費者對電子商務環境的安全信賴感。

TPIPAS 內容共有 9 章，第 0~3 章為標準介紹、適用範圍與名詞定義之說明，第 4~9 章則為個人資訊管理制度的架構要求。

計畫與建立 TPIPAS--第 0~3 章、實施與運作 TPIPAS--第 4 章 要求事項、第 5 章 管理責任、第 6 章 有效性量測、第 7 章 文件控管、監督與審查 TPIPAS--第 8 章 內稽控管、維持與改善 TPIPAS--第 9 章 改善。

第四節 ISMS 與個人資料之關聯因素--個資與 ISO 的相通性

比較 ISO 27001 資安認證和 BS 10012（英國個人資料保護標準）的資訊安全框架和個人資料保護的實務作法，ISO 27001 的資訊安全框架中，個人資料只是資訊資產中的一小部份而已，若單純以 ISO 27001 的資安管理框架來看，距離組織要做好個人資料保護，仍有一大段差距。因此，為了完善組織個人資料保護的實務作法，參考英國國家標準局（BSI）在 2009 年 6 月推出的 BS 10012 標準之個資保護管理實務上 PDCA 的作法。

BS 10012 非常侷限在個人資料的保護，強調深度確保個人資料安全的實務作法。ISO 27001 資安認證的資訊資產，分七大類別:人員、文件、軟體、通訊、硬體、資料、環境，個人資料只是資料中的一部份，資料還包含營業資料、財務資料等等，因此 ISO 27001 資安廣度較個人資料保護為廣，但對於專門個資保護的深度較淺。ISO 27001 是資安的基本防護架構，而 BS 10012 則針對個人資料提供深度保護，兩者相輔相成。如此，企業也可趁此時利用 BS 10012 的個資保護框架，重新檢查每一個個資保護環節是否符合個資法的規範。

BS 10012 是一套個資保護框架，也是組織進行個人資料保護管理 PDCA 實務作法的國際標準，不僅符合臺灣《個人資料保護法》的立法精神，更是目前少數提供個人資料保護實務作法的標準。對於有真正落實、深化 ISO 27001 資安認證的企業，因應新版《個人資料保護法》的來臨，可以新增加 BS 10012 的實務作法，藉此完善企業對個人資料的保護措施。

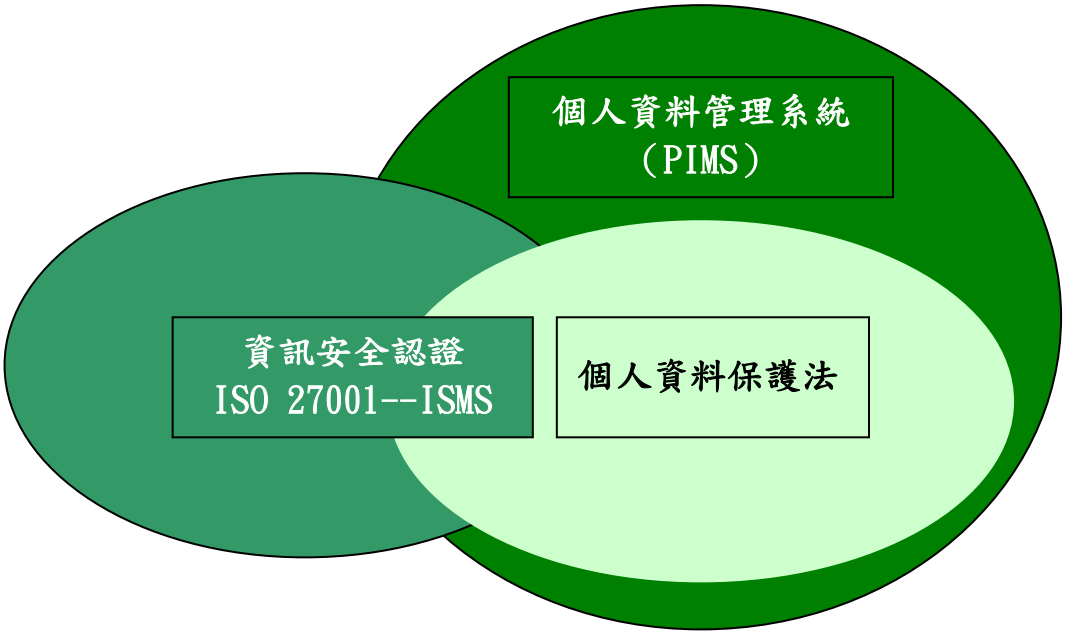

圖 8 個人資料保護法、個人資料管理系統、與 ISO 27001 之關聯圖

第三章 研究架構與方法

本章共分為二節，第一節主要是說明本研究提出之研究架構與研究流程；第二節說明本研究之文件資料收集、分析、比較方法。

第一節 研究架構與研究流程

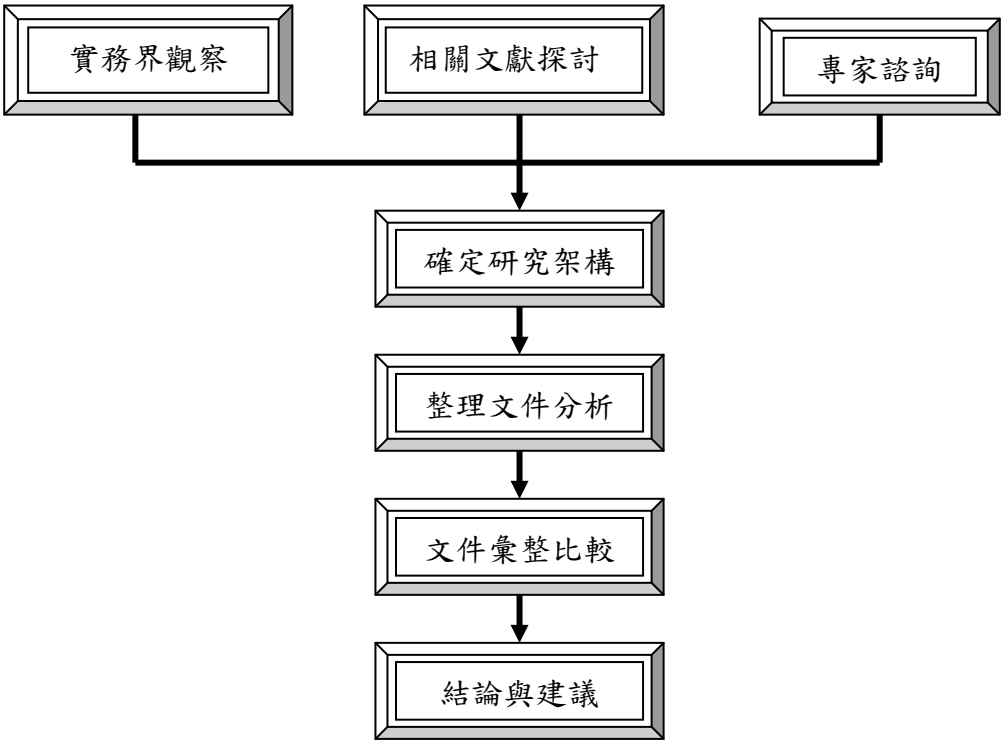

圖 9 研究架構與研究流程圖

第二節 文獻探討法、文件分析比較

本論文主要是採用 Gowin's Vee 的研究策略，在理論端先透過文獻探討方式，蒐集國內外個人資料管理系統(Personal Information Management System)、學者專家對個人資料管理制度的見解、並與國內個人資料保護法結合，再加上研究者在工作上的推動經驗進行研究，期望能夠提供一套個人資料保護管理對策，提供組織導入個人資料保護法解決方案，做為參考與遵循之用，幫助組織達成遵守個人資料保護法目的，降低罰鍰與訴訟風險，且讓組織善盡個人資料保護與管理職責。

一、文獻探討法

本研究先以文獻探討方式整理「國內外的個人資料保護法」、「國內外的個人資料保護管理制度」、及「ISO 27001-資訊安全認證(ISMS)」相關文獻，資料來源包括：

（一）國外的個人資料保護法--英國、美國、德國、日本

（二）國外的個人資料保護管理制度--英國、德國、日本

（三）台灣個人資料保護法、臺灣個人資料保護與管理制度規範(TPIPAS)

（四）ISO-27001-資訊安全認證(ISMS)

（五）學者之相關著作、學術單位之研究成果、及相關議題之期刊報導

二、文件分析比較

本研究在探討相關文獻之後，結合研究者在工作上的推動經驗，將相關文件彙整分析比較，提出一套個人資料保護管理對策，為了使結果更加周延，透過請教具有專業知識或實務經驗的專家學者「知識外顯化」，以達到「質化研究」目的

第四章 組織對個人資料管理對策

第一節 個人資料對組織之影響

當個人資料保護變成一定要遵循的法令時，除了「上有政策，下有對策」或是「靜觀其變」外，是否還有其他解決之道？而法令修訂之後的罰則可上看新台幣兩億元及五年以下有期徒刑，而所謂「能證明其無故意或無過失者」又尚無相應的規定或國家標準可以依循，所以雖說「國法不外乎人情」，但是已三讀通過之「個人資料保護法」顯然尚有不盡人情的地方。當法務部和媒體在為「公共利益」及許多「不確定法律概念」舉辦公聽會與討論時，台灣的民間企業正準備起因應之道。

本次個人資料保護法之修訂，不論適用主體、保護客體以及行為規範，更為嚴格，對於組織日常營運將產生一定程度之影響。因此，對於個人資料有蒐集、處理或利用需求之組織，宜於個人資料保護法施行前，先行檢視組織之內部控制相關規定及實施，對於個人資料之保護均已採取必要因應措施，以確保日常業務進行均符合新法規定，避免個人資料保護法施行後對於業務造成過大衝擊。個人資料對組織之影響，可分個人資料之生命循環週期、對公務機關、及對非公務機關三個構面來看。

一、個人資料之生命循環週期構面

個人資料之生命循環週期:蒐集/取得(Acquisition)、紀錄、輸入、儲存(Storage)、編輯、更正、複製、使用/檢索(Archive)、刪除、輸出、連結、內部傳送/分享(Sharing)、利用(Use)、國際傳輸/分享(Sharing)、銷毀(Destruction)等循環週期，說明如下:

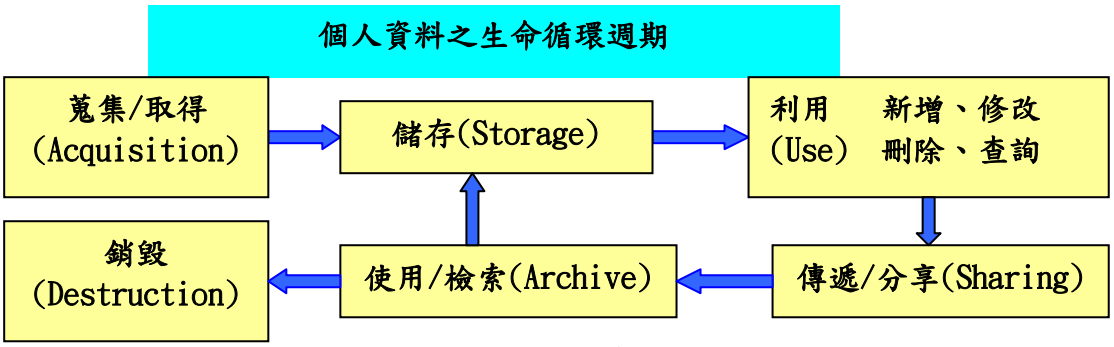

圖 10 個人資料之生命循環週期圖

二、公務機關構面--違反個人資料保護法應負之相關法律責任

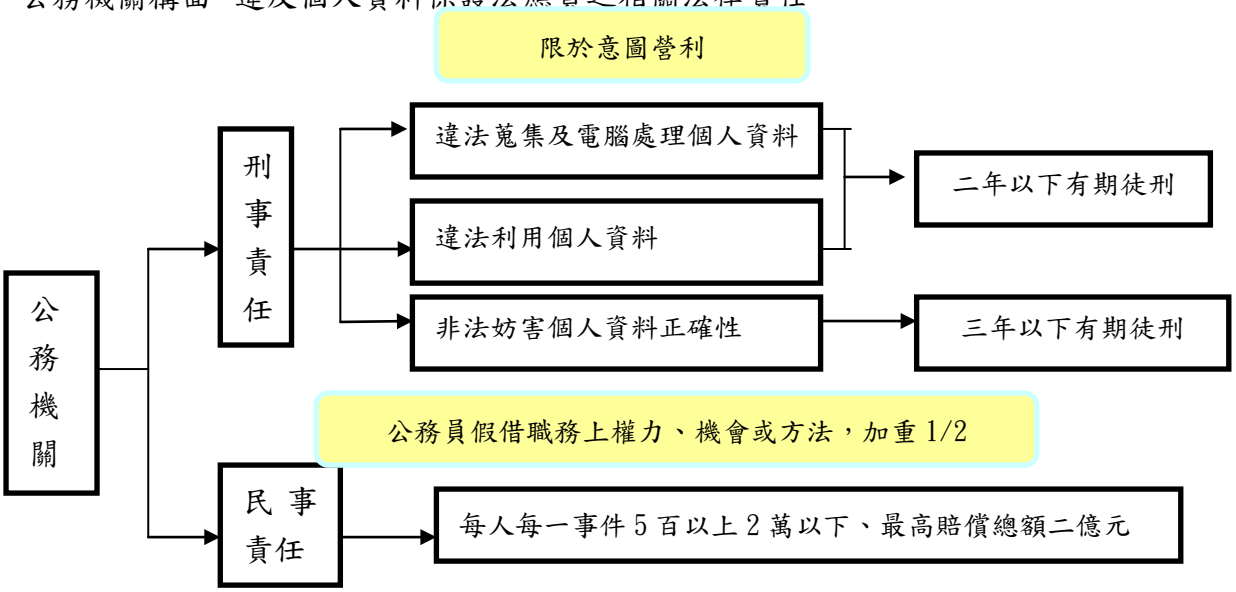

圖 11 公務機關構面--違反個人資料保護法應負之相關法律責任

三、非公務機關構面--違反個人資料保護法應負之相關法律責任

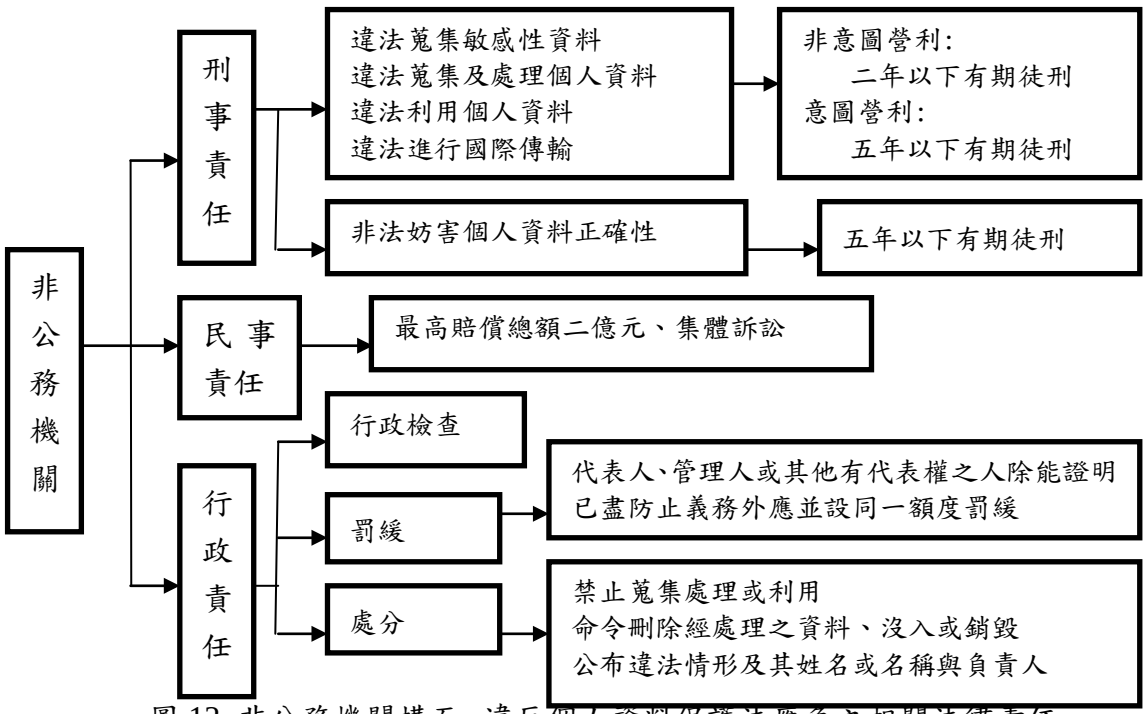

圖 12 非公務機關構面--違反個人資料保護法應負之相關法律責任

第二節 組織落實個人資料執行之方案

組織落實個人資料執行之對策方案，除採用 ISO 27001 資安認證的資訊安全框架和 BS 10012（英國個人資料保護標準）的個人資料保護的實務作法外，還得從訴訟原則上的「沒有故意」、「沒有過失」、「善盡善良管理人之責」、和「沒有不可抗力因素」的角度上，來擬訂一套方法論的框架。目前惟缺對應施行細則，仍有一些細節需等各個業別之施行細則公告後，再加以調整，但對整體企業組織個人資料保護方向仍是正確的。

一、組織落實個人資料保護管理因應之道，可由下圖來探其究竟:

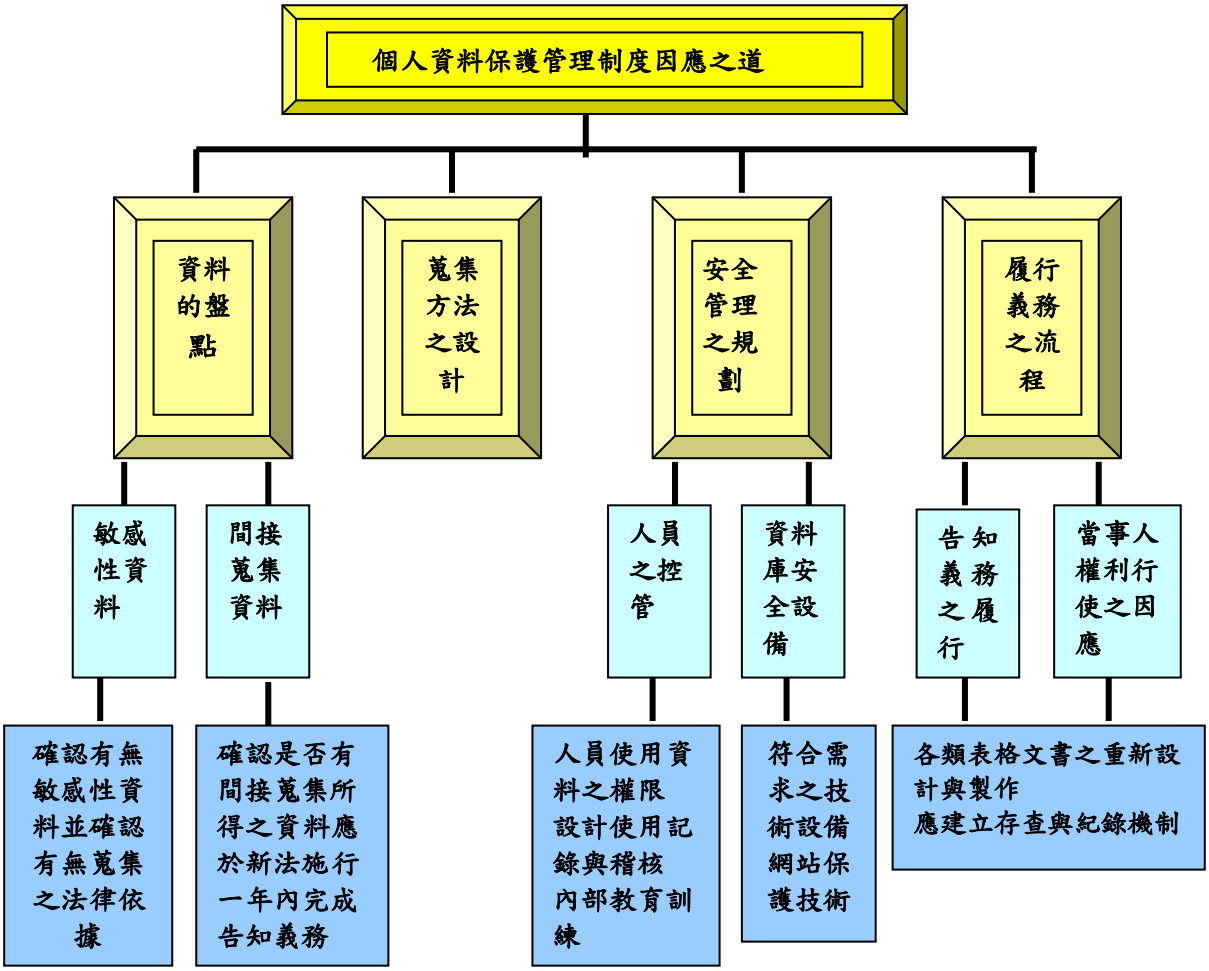

圖 13 個人資料保護管理因應之道

二、組織落實個人資料執行之對策方案執行要項，說明如下:

1.文件建置--採 ISO 組織訂定的四階文件制度

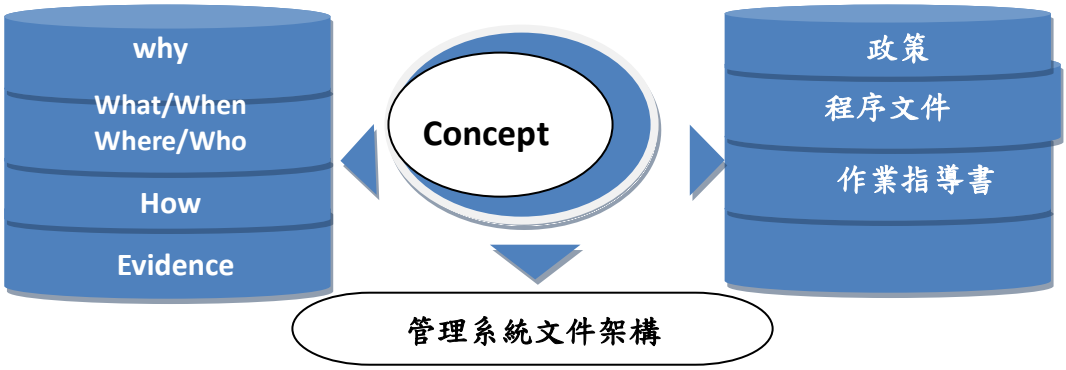

圖 14 個人資料管理系統文件架構

2. 對策方案做法---依文件內部進行

2.1 形成內部共識，制定個人資料保護政策

個人資料保護法通過後，將直接衝擊許多組織內部現有的作業流程，而內部如何因應這樣的衝擊是否有共識，如果有共識，第一件事情就是制定個資保護的政策，設立一個專責的個資管理單位，稱之為「Data Controller」，負責個資的蒐集、使用、傳遞、銷毀和保存。個資發送給誰、又被轉送給誰，中間所有傳遞的軌跡流程，都應該有專責的人或單位負責。才是組織是否已經做好個人資料保護法應對的證明。

新版個人資料保護法中的「可歸責性」（Accountability）是一個重要的立法精神，由於未來新法加重組織刑事責任和提高民事賠償上限，組織面臨個資外洩或不當使用的風險比以往高出許多，個人資料的保護就不能由兼職單位或人員負責控管，制訂個人資料保護政策、成立管控個人資料專責單位，則是組織正視新版個人資料保護法衝擊的第一步。

2.2 審視組織目前擁有之個人資料盤點，進行確定範圍

個人資料保護法通過後，組織也必須回頭審視手邊擁有的個人資料，是否是當事人提供或間接蒐集而來，而這些個人資料使用目的是否已有變更，這些個資狀態都攸關組織未來在使用這些個人資料時，是否必須再取得當事人同意。

各組織應該從業務流程的資訊流，去盤點組織目前所擁有的個人資料種類、數量和形式等，組織必須盤點到底有哪些個人資料，而這些個人資料來源是直接或者是間接蒐集而來的。要做個人資料盤點，應從資料的生命周期來看個資盤點是最適當的方式之一，從規畫、教育訓練、個人資料盤點，並產生類別清單、個人資料流向、個人資料歷程等，就可以清楚掌握每一個資料的來龍去脈。

因應新版個資法規定，管理上就必須意識到有紙本個人資料的管理，但因為電子檔形式的資料庫儲存個人資料量大，相關的管制措施就應該更為嚴格、謹慎才是。

2.3 進行個人資料隱私權衝擊分析、風險評估

隱私權衝擊分析（Privacy Impact Assessment，簡稱 PIA）主要是為了點出可能觸發的個人資料和隱私權議題。一般而言，為了讓隱私權衝擊分析更有效率，這會是日常流程的一部份，而透過隱私權衝擊分析，組織可以確保執個人資料的過程中，都能符合各種法規遵循、公司治理、客戶和商業隱私保護的需求。

2.4 採用 BIF 方法論，進行個人資料生命周期

BIF（Business Information Framework）方法論就是從業務流程去看個人資料的資訊流向，並針對各種業務執行作分析，確認組織內部所儲存的個人資料和儲存位置，也可以進一步了解目前組織控管程度和法規遵循的程度。

2.5 利用 RACI(Responsibility、Accountability、Consultation、Informed)矩陣

RACI 矩陣模型的 R 是 Responsibility 表誰來負責、解決問題之意，A 是 Accountability 表誰來承擔、批准之意，C 是 Consultation 表誰來諮詢、提供意見

之意，I 是 Informed 表誰被告知之意，RACI 矩陣模型是一個很適合用來釐清個資所有權的工具。

從個人資料盤點到隱私權衝擊分析，到掌握個人資料資訊流在每一個業務執行和儲存空間的個人資料流向後，接下來就是要釐清個人資料管理的責任，在這個 RACI 模型中，左側可以記錄各種個人資料類型，上方則記錄所有的個人資料資訊流管控者或窗口，在相對應的方格中，填入 R、A、C、I，辨別每一種個人資料類型和負責人的對應關係。

2.6 評估個人資料存放的風險

個人資料保護除了要考慮個人資料生命周期的變化，資料生命周期和組織內部環境高度相關，組織要結合營運狀況和資訊技術，為個人資料提供一個控管架構，用來確認組織對這些存放個人資資訊設備所採用的安控措施，是否做到適當的風險控管。如果有風險控管不當的項目，就可以進一步修改或調整。

2.7 建置以 ISO 組織的 PDCA 個人資料保護與監控制度

在資料處理的流程中，IT 和負責個資管控的主管必須選擇合適的個人資保護和監控工具。組織在解讀、評估個人資料保護法對組織造成的衝擊與挑戰時，組織主應該正視組織對個人資料保護的重要性，企業應該先從架構一個「組織對個人資料保護概念框架」著手。

所謂的組織對個資保護概念框架，是從組織是否設定隱私保護組織、政策、規範的治理面開始，逐步延伸到掌控資料處理流程，並對應部署合適的管控措施，對於所有的個資資訊流進行保護，並執行相關的監控措施和進行相關的分析報告。這個完整的過程，就是組織在面對個資保護時，從組織角度，一直到實際監控作為所架構出來的個資保護概念框架。

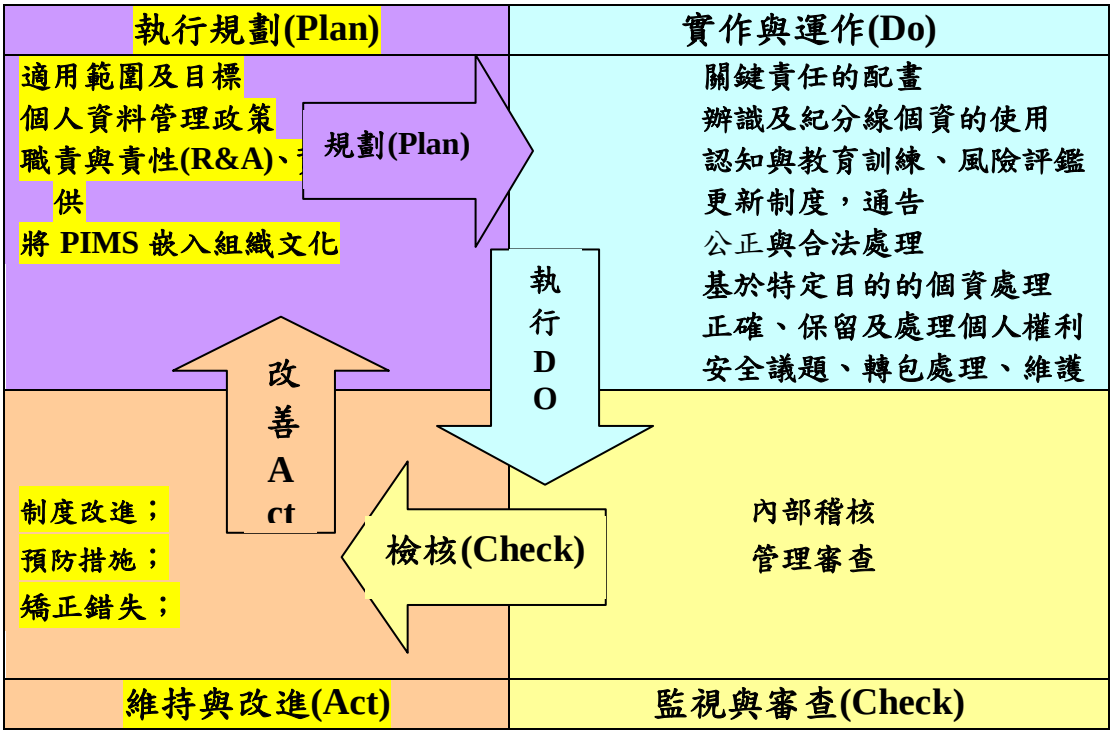

圖 15 PDCA 個人資料保護

2.8 依 2.1-2.7 分別建置程序表文件，標準作業流程文件(含執行紀錄表單)

個人資料保護管理制度文件管理規範,期使個人資料保護管理制度文件能獲得適切控管，以確保文件之機密性、完整性及可用性。

2.9 執行個人資料保護與管理制度時，落實記錄與保存執行軌跡

組織參考個人資料類別和風險高低,選擇合適的個人資料防護措施之後，為了能夠保存每一筆個資異動的軌跡,重要資安設備和資安事件的 Log 檔(登錄檔)都必須留存。

2.10 強化組織對個人資料保護內控與稽核管理

個人資料的資料來源除了來自外部客戶、內部員工、還有第三方合作或委外廠商。委外廠商是許多組織在個人資料防護上，最脆弱的一個環節。

2.11 檢視組織個人資料防護訴訟策略

「個人資料外洩基本上是一種組織對當事人的侵權行為」，而所有的犯罪在追究責任時，檢察官主要的任務就是追查犯罪動機、掌握犯罪工具，以及確認犯罪事實。所以，組織在評估《個人資料保護法》施行後的各種影響層面時，對於組織應該盡哪些義務、負擔哪些責任，尤其受損害的當事人提告之後，上法院訴訟時，就可以從「有無故意」、「有無過失」、「有無善盡善良管理人責任」以及「有無不可抗力之因素」來看相關的衝擊與挑戰。

3.組織因應個人資料保護法之道，說明如下:

3.1 制定個人資料保護內規

組織依個人資料保護法架構及隱私權保護之觀點，制定個人資料保護內規，以確立組織內部對於個人資料管理、保護、及利用之原則。

3.2 加強個人資料保護法教育訓練

除制定個人資料保護內規外，組織得另就隱私權保護議題，對內部員工進行教育訓練，以強化員工保護當事人權益之意識。

3.3 建立告知當事人之標準程序

組織對個人資料進行蒐集、處理或利用，不論該資料是否由當事人自行提供，均須負一定之告知義務，因此，組織得針告知事項，建立標準告知程序，藉符法規之要求；此外，個人資料保護法修正前，非由當事人提供之資料，亦應於施行日起一年內補行告知程序。

3.4 迅速檢視組織內擁有之個人資料內容

凡涉及醫療、基因、性生活、健康檢查、及犯罪紀錄等敏感性資料，原則上不得予以蒐集、處理或利用。因此，組織得針對資料儘速進行檢視，確認個人資料內容是否包括敏感性資料。此外，針對資料屬性進行分類建檔，以增進個人資料管理之效率。

3.5 建立個人資料管理之標準作業流程

基於維護個人資料正確之義務，個人資料蒐集機關須主動或依當事人請求，就個人資料為補充或更正，因此，組織得建立標準作業流程，以隨時檢視所管理

之個人資料是否有進行更新之需求。

3.6 強化個人資料管理內控及稽核制度

組織保有之個人資料是否安全，多與個人資料管理流程是否確實執行有關，因此，蒐集個人資料之組織得定期或不定期檢查內部個人資料管理流程是否完善、適當；如發現不足，亦應立即為適當之補救措施，以確保個人資料之安全。

3.7 建置個人資料保護違法運用之處理機制

個人資料保護法規定，個人資料之蒐集、處理或利用等行為有違法時，應主動或依當事人請求刪除、停止蒐集、處理或利用該資料，因此，組織宜事先建置標準處理機制，以便發現有違法情事時，得立即為相應之處理。

3.8 提高個人資料保護危機處理能力

組織如發現個人資料已外洩或遭竊取，宜立即採取相應之措施，以維護個人資料當事人之權益。

3.9 無保存需求之個人資料制定作業準則

如個人資料之保存目的消失，或已屆保存期限，組織即無保存該資料之需求，此時，組織得事先制定個人資料刪除或銷毀之作業準則，以避免個人資料流出後，對於當事人權益造成損害。

4.組織個人資料保護工作事項

4.1 個人資料保護及安全原則：

a.組織應指定單位副首長為組織召集人、專人依相關法令辦理安全維護及保管事項。設置並指定「個人資料保護聯絡窗口」。

b.個人資料檔案應定期備份，並防止被竊取、竄改、毀損、滅失或洩露。

g.個人資料檔案儲存於電腦者，應設置可辨識身份之登入通行碼。

d.含有個人資料之紙本，宜建立相關之授權、監督及行為記錄機制。

e.內部傳遞或與其他組織交換個人資料時，應選擇可靠且具備保密機制之傳遞方式，並對轉交或傳輸行為加以記錄流向備查。

f.對於個人資料之調閱宜經申請並核准，並記錄其調閱身分及行為。

g.以電腦處理個人資料時，需核對個人資料是否與原件相符。

h.組織管理之網站或網頁內容，公佈個人資料時，需經所屬單位主管核准，且依相關法律及規範處理。

4.2 參考注意事項：

a.處理個人資料之資訊設備使用、設備管理，應制訂資訊安全相關管制注意事項。

b.處理個人資料之人員管理，應制訂資訊安全相關管制注意事項。

c.含個人資料之系統開發及委外管理，應加強制訂資訊安全相關管制注意事項。

4.3 個人資料保護檢核表

自訂個人資料保護檢核表，表內至少涵蓋個人資 料保護與安全、資訊設備管理、人員管理、系統開發及委外管理等四大部份。提供組織內相關人員進行自我檢核，以落實執行個人資料保護法。

第五章 結論與建議

第一節 結論

未來在新版個人資料保護法正式施行後，對於擁有大量個人資料的公務與非公務機關而言，最重要的轉變，可能是要接受個人資 料的保護，已不再是「資訊單位」的責任，應是組織內只要涉及個人資料之各單位，皆有責任，話說是全體同仁。

若僅限於機房實體防護、主機與應用系統、資料庫定期弱點掃瞄與滲透測試，就能確保個人資料的安全性，當然，上述工作實有其存在之必要性，但唯除資訊單位外的每個環節、每個持有、操作、傳遞、儲存與銷毀的同仁， 都必須落實合乎規定，稍有不慎，則機敏的個人資料就會外流至惡意或無惡意的組織或個人，對照前述所提及之罰鍰與處分，以及連帶可預期組織形象的損失，在在考驗組織面對此一議題所需投入的精神與資源，然而，個人資料保護之要求，卻已是各個組織無可迴避的使命。

組織在落實 ISO 27001 資訊安全認證時，係針對電子資料(數位化資料)為主，但個人資料保護法中的個人資料，除了電子資料外，尚有大批非電子資料，及傳統人工作業流程運作，因此組織務必建置一套個人資料保護與管理制度，惟獨目前尚未有 ISO 國際組織標準可認證，現階段尚得仰賴人為管理為主，資訊科扳(IT)為輔的制度來運作。

另外從法的角度而言，未來如有訴訟時，組織必需提出原始憑證，原始憑證必需是個資個人親筆簽章，組織未來要如何留下原始憑證(即資料正本)，恐將是一大難題，也是未來深具研究的課題之一。

第二節 建議

無論是英國、日本、德國的個人資料保護與管理制度認證，均未涵蓋到台灣個人資料保護法中第二十二條「中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料」，即是泛指公務機關之「行政檢查」權，此一領域尚有待未來研究者進一步探討。

另外現階段國內僅經濟部在推動的「臺灣個人資料保護與管理制度規範 TPIPAS」計畫，但此計畫係針對電子商務業者為主要對象，即是就電子商務業量身訂制的「臺灣個人資料保護與管理制度規範 TPIPAS」，未來是否適合全臺灣各行各業，如金融業、銀行、教育機構、醫療院所、交通運輸業、、等不同行業，有待未來研究者進一步探討。

參考文獻

中文部分

日本資訊處理開發協會，2009，Privacy Mark System，隱私權標章推進中心。
周慧蓮，2005，英國個人資料保護最新案例發展及其對我國法制之啟示，科技法律透析，17 卷，1 期，55。
花俊傑，2010，初探 BS 10012 個人資訊管理標準簡介，因應個資法修法，建立有效的個人資訊保護制度，網管人雜誌，51 期。
范姜真媺，2009，他律與自律共構之個人資料保護法制-以日本有關民間法制為主，東吳法律學報，20 卷，1 期，163-200。
郭戎晉，2010，企業如何因應新版個人資料保護法，2010 資策會電子商務中高階主管研習會教材。
章鈺，2010，從個人資料保護法看組織如何保護個人資料，BSI 英國標準協會。
曾更瑩，2010，正視新個資法對企業之影響，貿易雜誌，232 期，46-49。
萬幼筠，2010，學習英國個資保護標準從根本做好個資保護，iThome 電腦報週刊，463 期。
蒲樹盛，2005，資訊安全管理系統(ISMS)ISO17799/BS7799 國際認證體系與稽核驗證介紹，研考雙月刊，29 卷，1 期，91-104。
蒲樹盛，2010a，全球風險下的個人資訊保護方案 BS 10012:2009 個人資訊管理系統 Personal Information Management System(PIMS)，品質月刊，46 卷，6 期，28-29。

英文部分

BSI(2009),BS 10012:2009 Data protection –Specification for a personal information management system。
BSI(2005),ISO/IEC 27001:2005 - Information Technology -- Security Techniques -- Information Security Management Systems – Requirements。
] George Lawton(2008),”New Technology Prevents Data Leakage”, Technology News, Vol.41, Issue 9。
E. Eugene Schultz,(2002) “A framework for Understanding and Predicting Insider Attacks”, Computers & Security, Vol. 21, Issue 6。

Enforcement Program of Organizations and the Personal Data Protection Law

Meei -Yueh Lin [1] Szu-Yuan Sun [2]

[1] **National Kaohsiung First Univeristy of Science and Technology**

maylin@nkfust.edu.tw

[2] **National Kaohsiung First Univeristy of Science and Technology**

sunnyy@nkfust.edu.tw

Abstract

Due to the increasing importance of personal date protection, the governments all over the world have legislative norms to ensure the personal data properly protected. The Legislative Yuan of Taiwan has passed the third reading of personal protection act on April 27, 2010 and the disclosure was right on the next following month.

Regardless of the size of the organization, amount of the personal information are all subject to personal data protection act, thereby affecting the organization in collection, storage, use, transfer, and destruction of personal information. Meanwhile, the organizational responsibilities include criminal law and civil law which have the maximum amount of compensation claims to two hundred thousand NT dollars. Therefore, how to implement the enforcement program of personal data protection act is the top priority at this stage.

Personal data protection act has caught everyone's attention and has been passed the third reading on 2010. Organizations now began to face a serious situation which is how to operate the organization under the Act. What organizations need to do is not only the personal data protection act has its wide range of specification that might change the previous operations but also avoidance of huge claims deriving from violating the law. The latest personal data protection act has a strong impact on organizations after other domestic laws such as the Labor Law, Fair Trade and Consumer Protection Act. This shows that with the personal data protection act will be soon implemented, leakage of personal information is one of the most important issues to be considered.

The thesis will be using methods of literature review, article analysis and comparison and will try to explore and collect Personal Information Management System through the article reviewing. Also, with the combination of the domestic personal data protection act, a personal data protection management measure and a reference into organizational solution can be provided, helps organizations to reduce the risk of fines and litigation. Moreover, the implementation of personal data protection act therefore can truly enable organizations to take their responsibilities on personal data protection and management.

Keywords:

BS 10012、ISO 27001、Personal Information Management System（PIMS）、Personal Information Protection Ac