國外資訊系統對個人資料保護之相關做法

Personal Data Protection Practices and Relevant Rules for Information Systems: The Cases from Several Foreign Countries

■ 鄒鎮帆 Tsou, Chen-Fan
國家發展委員會檔案管理局文書檔案資訊組助理設計師
Assistant Systems Designer, Information Technology Division, National Archives Administration, National Development Council

壹、前言

「個人資料保護法」已於中華民國 99 年 5 月 26 日總統華總一義字第 09900125121 號令修正公布，中華民國 101 年 9 月 21 日行政院院臺法字第 1010056845 號令發布，定自民國 101 年 10 月 1 日施行，開啟臺灣新個資法時代（註 1）（註 2）。適用對象包括自然人、法人，規範客體不限於電子傳輸形式，公司企業內保存的客戶資料及員工資料動輒數萬筆，因此各界無不嚴陣以待。

「個人資料保護法」之前身為「電腦處理個人資料保護法」，參考經濟合作暨發展組織（Organization for Economic Co-operation and Development，簡稱 OECD）發布的個人資料保護 8 大原則，經過法務部審議小組、專家學者座談會、行政院審查後，在民國 84 年 7 月 12 日立法院三讀通過、該年 8 月 11 日總統公布施行。「電腦處理個人資料保護法」之問世，乃因應我國加入世界貿易組織（World Trade Organization，簡稱 WTO）後，配合國際經貿及相關規範而產生之法律，惟該法施行至今，規範之行政程序繁瑣、有些條文內容不明確、同時規範公務機關與非公務機關之要件與程序有不相當之處，加上新興網路商業交易盛行，舊法造成消費者個人隱私權被侵犯，是故新法「個人資料保護法」應運而生（註 3）。

對於個人資料保護之實際做法，可參考「個人資料保護法施行細則」第 12 條第 2 項（註 4）（註 5）之執行建議，配置專責資安管理人員、建立完善管理程序、落實事故預防及通報應變機制、使用紀錄皆要妥善保存。在資料備份、檔案加密、監控及銷毀過程中必須有所管制，避免機敏資料外洩的可能性。

貳、國外立法例及相關實務做法

不管是新法「個人資料保護法」抑或是舊法「電腦處理個人資料保護法」，在立法之初皆有參考國外立法例及相關實務做法。以下逐一介紹。

一、亞太經濟合作會議

「亞太經濟合作會議」(Asia-Pacific Economic Cooperation，簡稱 APEC）成立於西元（以下同）1989 年，為亞太區域最重要的經貿合作論壇，為我國實質參與之國際組織之一。其於 2004 年 10 月通過「APEC 隱私保護綱領」(APEC Privacy Framework)，針對 APEC 各會員體，推動整合性的個人資料保護措施，確保亞太地區各會員國間資訊的自由流動。此綱領旨在推廣亞太地區的電子商務，與經濟合作暨發展組織的個人資料保護指導方針相符，證實電子商務與個人資料保護密不可分(註6)。並於 2007 年 1 月進一步通過「跨境隱私保護規則」(Cross Border Privacy Rules，簡稱 CBPR)，制定民間企業跨國傳輸個人資料時所須遵循之各項重要規則(註7)。

2007 年 6 月起，針對前述的跨境隱私保護問題，推動「開路者倡議實驗計畫」(Pathfinder)，其中，第 2 項子計畫即明確要求各會員體應建立「標章組織」，以參與跨境隱私保護規則。

當使用者存取 APEC 所轄網站，非個人資料不會被網站存取，包括使用者 IP、作業系統、瀏覽器種類等。若使用者輸入個人資料（例如姓名、電子郵件），APEC 秘書處會採取對應措施保護這些個人資料。

二、經濟合作暨發展組織

OECD 所發布的個人資料保護 8 大原則（Basic Principles of National Application），至今仍高度影響各國個人資料保護立法。OECD 的 8 個使用個人資料的應用基本原則如下(註8)：

（一）限制蒐集原則（Collection Limitation)：經本人同意，以合法、公正手段於適當場所蒐集。

（二）資料內容原則（Data Quality)：符合資料使用之目的，並確保資料之正確性、完整性和時效性。

（三）目的明確化原則（Purpose Specification)：蒐集的目的必須在蒐集當時就闡述明確，爾後使用也必須受限於當初所訂之目的，不得挪作他用。

（四）限制使用原則（Use Limitation)：若非經資料本人同意或經法規許可，個人資料不得揭露、販售或用於明訂於第 3 條明確目的以外之用途。

（五）安全保護原則（Security Safeguards)：資料必須採取合理安全保護措施，以免資料遭遺失、盜用、毀損、竄改或揭露的風險。

（六）公開原則（Openness)：對個人資料之開發、運用、政策等必須採取一般的公開政策。

（七）個人參與原則（Individual Participation)：個人有權利：

1. 向資料管理人確認是否保有自己資料，保有哪些相關資料。
2. 資料管理人在合理時間內、以合理價格、可接受的態度及可理解的形式，向本人聯絡溝通協調其資料之保有與使用。
3. 如果本人提出以上 2 項請求被資料管理人拒絕，盡可要求合理解釋，並有權質詢此拒絕。
4. 有權質詢個人相關資料之外，若質詢不滿意可以要求刪除、校正、修改資

料直到完整無誤為止。

（八）責任義務原則（Accountability）：資料管理者必須確保落實公司政策與執行措施以遵守上述各項原則。

如果使用者讀取或下載 OECD 網站相關資料，OECD 會蒐集並自動儲存以下資訊：日期和時間、來源端 IP 地址、網域名稱、使用之作業系統及瀏覽器名稱。此外，IP 地址、期程編號（session ID），用戶 ID 等紀錄於 cookie 上之內容均會被加密處理。

三、日本

日本於 2003 年 5 月制定，2005 年 4 月施行「個人資料保護法」（JPIPA）。不分行業別、不論是行政機關或是民間機構，凡擁有 5,000 筆以上個人資料者，均負有建置資料外洩防範措施並妥善維護隱私之義務，使個人隱私可確切保障（如圖 1）。

在法案實施前，早期曾發生重大個人資料外洩的日本知名企業 NTT DATA 已開始採取明確、澈底的個人資料管理措施、減少有存取權限的人員並限縮其權限、增加檢核制度，並積極投入員工教育訓練，輔以完整的資料外洩防護系統。

另外，SEIKO 100% 投資的子公司－SIIData Service 株式會社（SDS），在法令實施前執行員工資安教育訓練，並要求 PC 內的檔案帶出公司時都要加密。而後 SDS 有感於資安政策澈底落實的難度，進而輔以資料防護系統，彌補管理上的不足（註 9）。

在該法中，尚規定基於以下的情況，有可能會未經使用者同意而向第三者提供個人資料（同法第 23 條）（註 10）：

（一）基於法令情況。

（二）為保護人身生命安全和財產等必要情況

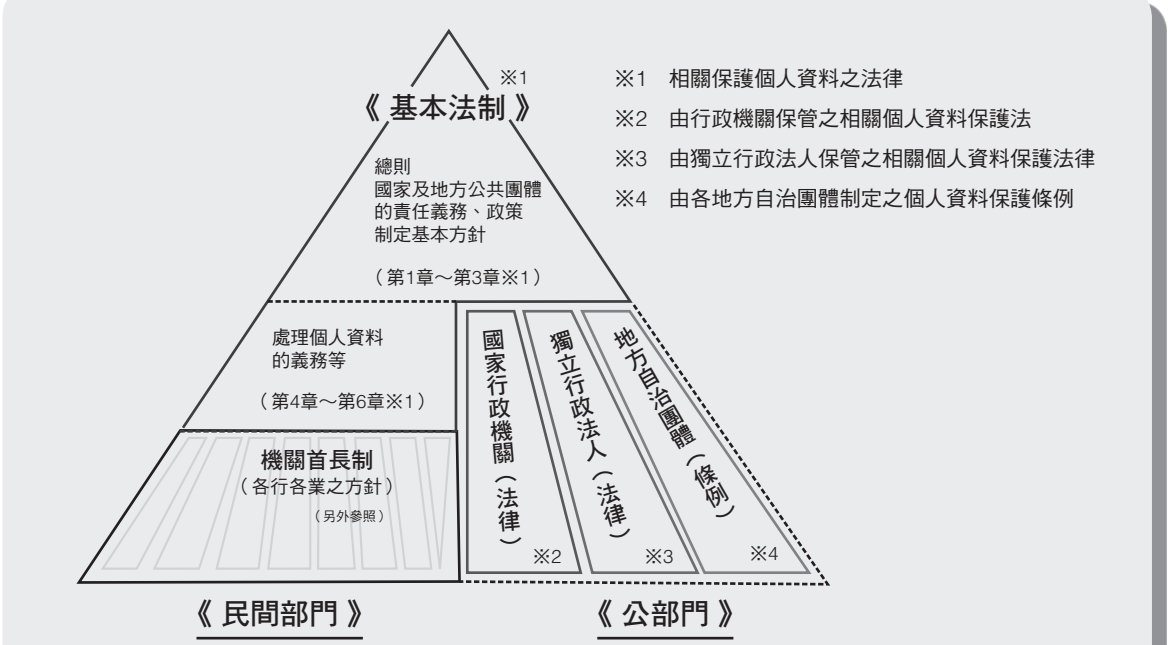

圖 1：個人資料保護之法制體系

資料來源：日本總務省行政管理局，〈個人情報保護に関する法体系イメージ〉。〈http://www.caa.go.jp/seikatsu/kojin/houtaikei_1.pdf〉（31 Mar.2014），作者翻譯。

下，得到使用者同意較困難時。

（三）為提高公共衛生和增進兒童的健康成長等特別必要的情況下，得到使用者同意較困難時。

（四）要協助國家機關或地方公共團體執行規定的法令事務的必要情況下，但經使用者同意會妨礙執行該事務時。

在我國「個人資料保護法」中第 16、20 條有類似規定。

提供給企業的個人資料有錯誤時，當事人可要求該企業訂正或刪除該個人資料。當事人申請訂正或刪除關於自己的個人資料時，企業將在第一時間內調查，如有訂正和刪除的必要，將在第一時間內訂正和刪除。

四、加拿大

加拿大早期受到美國影響，針對私部門個人資料保護僅採取「業界自律」（Self-Regulation）做法。但因應網路與數位科技發展，於 1995 年通過「個人資料保護及電子文件法案」（PIPEDA），全面強化私領域個人資料保護工作。PIPEDA 在 90 年代後期，促進電子商務中的消費者信任其資訊流之傳遞，以及向其他國家保證加拿大的隱私法案足以保護其他國籍的公民的個人資訊。其大致內容有：

（一）可以從個人（包括客戶、使用者和員工）蒐集哪些個人資料。

（二）蒐集個人資料前須獲得同意以及在什麼情況下蒐集。

（三）蒐集何種個人資訊。

（四）個人資料可能會如何使用或揭露。

（五）蒐集個人資料的目的及揭露的組織。

（六）當事人如何檢視他的個人資料及向該組織請求更正個人資料。

除了上開法案，尚有 1983 年 7 月 1 日通過的「隱私權法案」，此法令規定 250 個聯邦政府部門和機構有尊重隱私權之義務，限制蒐集、使用、揭露並保護這些個人資料。個人也有權利對這些聯邦政府組織請求更正自己所有的個人資訊。

自 2006 年以來，政府加強隱私保護，並實行嚴格通報機制有：

（一）向隱私權委員會通報隱私侵害事故，並採取迅速措施進行解決。

（二）完成隱私衝擊評估，以建置新的或實質性修正相關措施與行動。

（三）澈底落實隱私權保護措施命令，要求所有聯邦政府機構必須建置解決侵犯隱私事件的應變計畫。

（四）制訂隱私權保護政策，要求所有聯邦政府機構，若發現有任何可能侵害加拿大公民隱私的行為時，必須立即通知隱私權委員會辦公室。

（五）為因應各類新型侵害隱私權之事件，持續建立新的應變指引，協助各機構有統一的辨識標準和阻止措施（註 11）。

為因應行動商務，加拿大隱私權主管機關（Office of the Privacy Commissioner of Canada，簡稱 OPC）會同加拿大境內的阿爾伯特及不列顛哥倫比亞兩省各自之地方主管機關（其分別為 Office of the Information & Privacy Commissioner of Alberta 及 Office of the Information & Privacy Commissioner for British Columbia）撰寫指導文件，希望能提供當地應用程式（Application，簡稱 App）開發供應商建議方案。該項建議方案促使行動軟體開發供應商在設計與開發 App 時，必須顧及使用者隱私之保護，並提供協助方式與預

防原則，提高使用者隱私受保護之程度；除必須使用清晰且易懂之方式，告知用戶的個人資料將進行何種用途外，在使用者下載前亦應告知被蒐集之資料類別及原因、資料儲存位置或地點、資料分享之可能及其原因、資料保存之期限及其他可能影響用戶隱私之事件；倘若廠商必須變更隱私政策與規定，則應使用明確易懂之方式，事先通知所有使用者了解進行何項變更，以強化用戶隱私與個人資料保護意識（註 12）。

醫療病歷資料也是個人資料的一部分。加拿大針對衛生保健資料遵循一套嚴格的隱私和安全政策。該政策指導全國如何蒐集、儲存、分析和傳播在加拿大衛生保健系統的資料。在一個醫療院所裡會有專責單位管理相關個人隱私資料，並推廣及宣導個人資料保護的法治觀念；還會敦聘一位法律顧問提供隱私適宜的諮詢意見。董事會也會成立一個隱私和資料保護委員會，要求員工接受相關衛生保健資訊保護事項的教育訓練。

五、美國

資訊隱私在美國是高度立法規範。不管是尋求就業、醫療護理、買車、買房或購物時都不可避免的需要紀錄客戶資料。只要當事人不同意，商家、企業組織、政府機構就不能隨意公開其資料。例如 1996 年健康保險可攜性責任法案（Health Insurance Portability and Accountability Act，簡稱 HIPAA）、1998 年保護兒童線上隱私法案（Children's Online Privacy Protection Act，簡稱 COPPA）和 2003 年公平和準確信用處理法案（Fair and Accurate Credit Transactions Act，簡稱 FACTA）等。美國於 1974 年所通過的「隱私權法」，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 1986 年推動電子通訊隱私權法、1987 年通過電腦安全法等，以保護個人資訊之隱私。其相關法律包括（註 13）：

（一）1970 U.S. Fair Credit Reporting Act
（二）1970 U.S. Racketeer Influenced and Corrupt Organization (RICO) Act
（三）1974 U.S. Privacy Act
（四）1980 Organization for Economic Cooperation and Development (OECD) Guidelines
（五）1984 U.S. Medical Computer Crime Act
（六）1984 U.S. Federal Computer Crime Act (strengthened in 1986 and 1994)
（七）1986 U.S. Computer Fraud and Abuse Act (amended in 1986, 1994, 1996 and 2001)
（八）1986 U.S. Electronic Communications Privacy Act (ECPA)
（九）1987 U.S. Computer Security Act
（十）1988 U.S. Video Privacy Protection Act
（十一）1990 United Kingdom Computer Misuse Act
（十二）1991 U.S. Federal Sentencing Guidelines
（十三）1992 OECD Guidelines to Serve as a Total Security Framework
（十四）1994 Communications Assistance for Law Enforcement Act
（十五）1995 Council Directive on Data

Protection for the European Union (EU)

（十六）1996 U.S. Economic and Protection of Proprietary Information Act

（十七）1996 Health Insurance Portability and Accountability Act (HIPAA) (requirement added in December 2000)

（十八）1998 U.S. Digital Millennium Copyright Act (DMCA)

（十九）1999 U.S. Uniform Computer Information Transactions Act (UCITA)

（二十）2000 U.S. Congress Electronic Signatures in Global National Commerce Act (ESIGN)

（廿一）2001 U.S. Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act

HIPAA 中，讓病人可以存取由健康照顧單位、醫院或保險公司等維護個人醫療紀錄，及授權如何使用或公布受保護之個人資訊的權利。醫生、醫院與其他健康照顧單位需要限制病患個人資訊的揭露，達到特定目的最低必要性。HIPAA 授權醫院照護系統建立電子醫療資訊交換，所建立的資料交換、建立、儲存標準及電子簽章已成為業界重要的發展依據，確保病人的就醫紀錄、健康資訊的隱私。

無論美國或加拿大，在資訊系統建置上大致上包含了：風險評估（或風險管理分析）、制定預防政策、依政策進行系統維護與補強、人員教育訓練、稽核等事項，落實 BS10012 中 PDCA 的宗旨。

六、俄羅斯

隨著 2005 年和 2006 年俄羅斯聯邦頒布資料保護（隱私）法，資料保護（隱私）在俄羅斯迅速發展。關於個人資料（第 152-FZ），俄羅斯聯邦法律於 2006 年 7 月 27 日，構成俄羅斯隱私法律的骨幹，需要個人資料之企業採取「組織必須作必要的技術措施以保護個人資料免受非法或意外窺視」。俄羅斯聯邦即成立一個專責政府機構，專門監督通訊、資訊技術和大眾傳播的法規遵循事項、制訂保護個人資料的程式，功能類似國內的國家通訊傳播委員會（National Communications Cominission，簡稱 NCC）。

2013 年 5 月，俄羅斯簽署了於 1981 年制定的歐洲理事會第 108 號公約，該公約在 45 個國家施行，賦予保護個人隱私資料的法律約束力，包括行政規則，確保公平的處理資料和依法蒐集、處理、利用；個人擁有存取權限，更正或刪除他們的資料。簽署國還必須設置一個獨立的機構，確保遵守保障資料原則並說明防止任何侵權行為。公約簽署後，送往歐洲理事會，於 9 月 1 日生效，俄羅斯成為該公約的第 46 個成員國。

七、德國

德國為保障個人權益不致因儲存、傳遞、更正及刪除等資料處理過程而受損，遂於 1977 年 1 月 27 日即制定「資料處理個人資料濫用防制法」（Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung），簡稱「聯邦資料保護法」（Bundesdatenschutzgesetz），並於 1979 年生效。後因歐洲聯盟成立，為轉置

歐盟指令、保障個人資料及資訊自由流通，而於 2001 年 5 月 18 日修正其內容。2003 年 1 月 14 日修法，其內容旨在保障個人資料自主權，並落實歐盟有關建立共同資料保護標準之指令（註 14）。最近一次的修法日為 2009 年 8 月 14 日，並於同年 9 月 1 日起施行。除了聯邦層級之個人資料保護法外，德國在個別法上也制定了法律，尤其為因應網路時代來臨，並分別制定公布通信服務個人資料保護法及電信通訊法（Telekommunikationsgesetz，簡稱 TKG）等個人資料保護之個別性法律（註 15）。現行「個人資料保護法」第 6 條參酌歐盟 2012 年「一般資料保護規則」草案第 9 條規定、「德國聯邦個人資料保護法」第 13 條第 2 項及「奧地利聯邦個人資料保護法」第 9 條等外國立法例修正之。

德國的聯邦個人資料保護法有以下的原則（註 16）：

（一）直接原則：即個人資料應直接向本人蒐集。

（二）更正原則：即為了保護個人資料的內容完整與正確，本人有權利修改其個人資料，以使其在特定目的的範圍內保持完整性、正確性。

（三）目的明確原則：即在蒐集個人資料時必須有明確的目的，禁止公務機關和非公務機關非法超出目的範圍蒐集、儲存個人資料。

（四）安全保護原則：即個人資料應該處於安全的保護中，避免可能發生的個人資料的洩漏、意外滅失和不當使用。

（五）公開原則：即個人資料的蒐集、利用與處理一般應當保持公開，本人有權利知道個人資料的蒐集、利用和處理狀況。

（六）限制利用原則：即個人資料在使用時應該嚴格限定在蒐集範圍目的內，不應作蒐集目的以外的使用。

德國聯邦個人資料保護法對公務與非公務組織之隱私權保護機制實質上有相當周全的規定，例如：規定須設置「個人資料保護委員會」對公務機關處理個人資料的情況進行監督。個人資料保護委員會委員一般由大學教授或法官擔任。同時對於非公務機關，要求設立「資料保護人」對非公務機關處理個人資料進行監督，此「資料保護人」即西方公司內部所稱之「隱私長」（Chief Privacy Officer），由各組織自行任命，以其具備必要的專業知識和良好品行為任命之基本要件。有專責機構或專人負責維護隱私權，使得德國人民在各個組織中的隱私權受到充分尊重。

在「聯邦資料保護法」中，6b. 公共空間電子監視器之監控及 6c. 活動式個人資料儲存處理媒介之規範，為我國現行個人資料保護法中尚未規範之部分，也是我國未來因應資訊時代的努力方向。

德國目前關於資料保護驗證機制於法律上並無具體的規定。但在產業面針對於資訊安全的驗證，則有國際標準 ISO/IEC 27001 與資訊安全局制定的資訊保護基準法 ITBPM。在德國，現行法中已規定，自動化資料處理必須適時的告知企業資料保護人。除此之外，應加強其職權，並在法令上保障其職位。落實資料保護亦是公司治理的標準之一，納入政府提出的「公司治理」方針中，並加重公司負責人在資料保護上的責任。

有關當事人同意之方式，我國「個人資料保護法」參照德國聯邦個人資料保護法規定，必須以書面方式為之；但德國為因應網路

及電子化科技之發展，已於電信法第 94 條針對電子化同意而為特別規定，因此，德國聯邦對於取得當事人書面同意之方式，可以透過網路或其他電子傳輸方式，藉由加密數位簽章之電子郵件，或其他可確認寄件人身分之電子郵件取得當事人之同意。但如涉及法律爭議案件時，原則仍不得以電子郵件取得同意，例外如需以電子郵件方式取得同意之必要時，則應將電子簽章方式、加密演算法告知資料當事人（註 17）。

八、西班牙

西班牙現行的「個人資料保護組織法」（Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.），係於 1999 年 12 月 13 日制頒，取代 1992 年制定的「資料自動化處理規範組織法」（Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos）。旨在有關個人資料處理上保障公眾自由及自然人之基本權利，特別是與其名譽、個人及家庭隱私相關之權利（註 18）。與我國「個人資料保護法」比較，現行的「個人資料保護組織法」規範公務機關、非公務機關的相關權利與義務，以及資料保護原則、個人權利之行使等概念相去不遠，惟第 29 條「提供有關資產及信貸支付能力之資訊服務」、第 30 條「以廣告及商業銷路調查為目的之處理」、第 31 條「廣告名冊」及第六編「西班牙資料保護局組織法源」是和我國法律有差異部分（註 19）。

近日相關消息是 Google 在 2013 年 3 月在沒有提供充分的資訊下，便整合了各種服務的使用者資訊，且大多數使用者都不知道他們已失去對自己個人資訊的控制權，例如未解釋蒐集哪些使用者資料或是如何使用這些資料等，同時 Google 亦無限期地保存這些資料。此項新政策引起西班牙的資料保護組織（Agencia Española de Protección de Datos，簡稱 AEPD）不悅，經過調查，認為 Google 這三項都違反了當地法令，因此對 Google 開罰 90 萬歐元（約 123 萬美元），並要求 Google 必須採取必要的措施來符合當地的法令（註 20）。

參、結論

鑑於資訊安全在現今網路時代中已為顯學，在公務機關及非公務機關中，如何於管理面、組織面、技術面上達成保護個人資料，並兼顧資訊安全與管理效率，強化管理防禦力，是企業組織必須正視之課題。由全球推動資訊安全管理制度（Information Security Management System，簡稱 ISMS）的過程經驗中，最基礎且最重要的便是人員的資安觀念與管理知識。組織抗拒、人員反彈、高階長官的態度等因素往往左右企業中資訊安全落實的成功與否。資通安全應達到「均衡」管理原則，「七分管理，二分技術，一分稽核」（註 21）。鑑於網路科技傳輸發達，個人一不小心就陷入「楚門的世界」裡，容易被詐騙集團或電話行銷、網路行銷業者趁機勒索或推銷。破財事小，人格權喪失事大。各位也應提高自我警覺，不管是電子資料或是紙本資料，隨時保護個資，使用完畢立即銷毀，避免遭冒用。

強化個人資料安全之維護措施，可分以下幾點說明：

一、資料安全：做好資料備份、檔案加密、檔案監控、檔案銷毀、實體隔離。

二、網路安全：建立防火牆、防毒軟體、入侵防禦系統、上網行為管理等基礎網路硬體設施。

三、系統安全：系統備份、存取控管、身分認證、弱點掃描、程式源碼檢測、滲透測試等工作。

四、端點安全：防毒軟體、端點控管、虛擬桌面。

做好個資保護，必須建立一套企業內部可遵循之標準做法，全面落實稽核管控制度，從日常生活灌輸保護觀念，促進民眾參與，降低個資外洩風險。

註釋

註 1：立法院國會圖書館網站，〈首頁〉。〈http://npl.ly.gov.tw/do/www/homePage〉（31 Mar. 2014）.

註 2：法務部，《個人資料保護法規及參考資料彙編》（臺北：法務部，民 102），頁 1-163。

註 3：李震山，〈「電腦處理個人資料保護法」之回顧與前瞻〉，《中正法學集刊》14（2004 年 1 月）：35-82。〈http://ccu.lawbank.com.tw/essays/02260003.pdf〉（31 Mar. 2014）.

註 4：同註 2。

註 5：iThome 雜誌社，《iThome 個資法專刊 2—戰勝個資法》特刊（臺灣：電週文化，民 101 年 10 月），頁 128-130。

註 6：鄧永基，〈隱私權和個人資料保護的介紹與歐美發展趨勢簡介〉，《財金資訊季刊》62（2011 年 6 月）。〈https://www.fisc.com.tw/tc/knowledge/quarterly1.aspx?PKEY=ea685431-6453-468c-8f44-6fa25cdc9cd4〉（31 Mar. 2014）.

註 7：臺灣個人資料保護與管理制度網頁，〈TPIPAS 簡介〉。〈http://www.tpipas.org.tw/model.aspx?no=160〉（31 Mar. 2014）.

註 8：范肇鈞，〈【個資法專題系列之二】：個人資料保護法的企業因應原則與 BS 10012:2009 國際標準〉，《企業通電子報》130（民 99 年 8 月）。〈http://www.dsc.com.tw/newspaper/130/130-9.htm〉（31 Mar. 2014）.

註 9：林婉玲，〈淺談日本個人情報保護法與企業因應對策〉，《精品科技 FineArt Express》2009 年夏季號（2009 年 5 月）：12-13。〈http://www.fineart-tech.com/download/FineArtExpress/FineArt%20Express-2009-S2.pdf〉（31 Mar. 2014）.

註 10：RON の六法全書 off LINE，〈個人情報の保護に関する法律〉。〈http://www.ron.gr.jp/law/law/kojinjoh.htm〉（31 Mar. 2014）.

註 11：資策會科技法律研究所，〈加拿大政府致力捍衛個人資料隱私〉（2013 年 6 月）。〈http://stli.iii.org.tw/ContentPage.aspx?i=6213〉（31 Mar. 2014）.

註 12：資策會科技法律研究所，〈加拿大提供 App 開發供應商指導方針解決因隱私保護所引發之問題〉（2013 年 2 月）。〈http://stli.iii.org.tw/ContentPage.aspx?i=5970〉（31 Mar. 2014）.

註 13：同註 1。

註 14：公務出國報告資訊網，〈考察歐盟、比利時與德國個人資料保護法規之規劃及施行情形報告〉（民 101 年 9 月 17 日）。〈http://report.nat.gov.tw/ReportFront/report_detail.jspx?sysId=C10102817〉（31 Mar. 2014）.

註 15：同註 14。

註 16：江啟先，〈員工資訊隱私權與企業在網路監控協調之研究〉（碩士論文，國立政治大學法律科際整合研究所，2008），頁 34-36。

註 17：同註 14。

註 18：同註 1。

註 19："de Protección de Datos de Carácter Personal," *noticias juridicas,* 6 Mar. 2011,〈http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html〉（31 Mar. 2014）.

註 20：iThome，〈Google 因侵犯隱私被西班牙判罰 90 萬歐元〉（2013 年 12 月 20 日）。〈http://www.ithome.com.tw/node/84387〉（31 Mar. 2014）.

註 21：國立成功大學資通安全研發中心，〈BS 7799 理論與實務〉。〈http://www.icsc.ncku.edu.tw/_doc/BS%207799.pdf〉（31 Mar. 2014）.