法務部
公務機關個人資料保護方案計畫
研究成果報告書

總結報告書

財 團 法 人 資 訊 工 業 策 進 會

日期：民國101年05月

本報告為委託研究，僅供政府機關參考，
不代表法務部意見。

目錄

壹、 前言 1
一、 計畫背景說明 1
二、 問題評析 2
三、 計畫執行項目 5
貳、 建置個人資料保護法制研究報告及政策說帖 6
一、 建置個人資料保護法制研究報告 6
二、 政策說帖 108
參、 個資保護執行現況統計及試行成果報告 118
一、 試行機關成果問卷設計表 118
二、 統計個資保護執行與成果報告 127
肆、 公務機關個人資料保護執行程序暨考核作業研究 264
一、 個資執行暨考核作業程序及系統分析報告 264
二、 公務機關個人資料保護執行程序暨考核作業手冊 298
伍、 跨境隱私保護之國際合作機制 365
一、 國際合作及爭議案例處理研究報告 365
二、 APEC 跨境隱私國際執行合作文件 405
陸、 資料隱私及資訊透明國際研討會 416
一、 前言 416
二、 活動記錄 416
三、 意見調查統計 514
四、 效益分析 516
五、 結語 517
六、 簽到表 517
七、 活動照片 518
柒、 公務機關個人資料保護專責人員培訓教育訓練 525
一、 初階公務機關個資保護專責人員培訓教材 525
二、 中階公務機關個資保護專責人員培訓教材 571
三、 進階公務機關個資保護專責人員培訓教材 657
四、 公務人員及民眾認知宣導教材 694
五、 民眾認知宣導摺頁 713
六、 個人資料保護宣導摺頁說明手冊 715
七、 第一年度公務機關個人資料保護專責人員培訓教育之紀錄彙整及成果追踪報告 717
八、 第二年度公務機關個人資料保護專責人員培訓教育之紀錄彙整及成果追踪報告 734
附錄、公務機關個人資料保護執行程序暨考核作業手冊附錄 786
附錄一、管理制度之參考表單 786
附件一：個人資料保護管理政策 786
附件二：個人資料保護組織規定 787
附件三：個人資料保護管理制度作業計畫表 790
附件四：法規盤點程序 792

本報告之智慧財產權歸屬於法務部

附件五：個人資料盤點程序.....793
附件六：風險評估程序.....794
附件七：緊急應變程序.....795
附件八：個人資料作業管理規定.....797
附件九：個人資料維護及委外管理程序.....802
附件十：當事人權利行使程序.....805
附件十一：教育訓練計畫.....807
附件十二：文件紀錄管理規定.....809
附件十三：申訴諮詢程序.....812
附件十四：稽核程序.....814
附件十五：矯正、預防措施程序.....817
附件十六：持續改善程序.....820
附錄二、參考之程序表單.....822
表單一：文件紀錄一覽表之一.....822
表單二：文件紀錄一覽表之二.....823
表單三：文件紀錄一覽表之三.....824
表單四：個人資料盤點清冊.....825
表單五：委外廠商選擇評鑑表.....826
表單六：委外廠商管理一覽表.....827
表單七：當事人權利行使申請書.....828
表單八：當事人權利行使紀錄表.....829
表單九：全年內部稽核計畫書.....830
表單十：個別部門內部稽核計畫.....831
表單十一：個別部門內部稽核糾正事項確認表.....832
表單十二：風險分析表.....833
表單十三：內部稽核報告書.....834
表單十四：全年教育訓練計畫書.....835
表單十五：個別部門教育訓練計畫、執行紀錄.....836
表單十六：矯正預防措施報告書.....837
表單十七：機關代表人檢視修正會議紀錄.....838
表單十八：個資管理整體自評分析細項表.....839

本報告之智慧財產權歸屬於法務部

圖目錄

圖 1：新個資法對公務機關產生之困擾.....3
圖 2：個人資訊委外服務管理作業程序.....144
圖 3：陳情程序個人資料作業流程圖.....159
圖 4：陳情程序個人資料作業流程圖.....169
圖 5：內政部警政署學員出席狀況踴躍，排隊簽到及領取課程講義.....247
圖 6：內政部警政署學員出席狀況踴躍.....248
圖 7：資策會顧振豪組長為學員說明本次教育訓練活動的舉行目的.....248
圖 8：資策會廖淑君研究員講授「個人資料保護法介紹」.....249
圖 9：資策會陳秭璇律師負責講授「考核作業手冊」.....249
圖 10：楊光華研究員負責講授「個資盤點、作業流檢視與風險評鑑」，教學員辨識單位中的個資檔案.....250
圖 11：透過實例演練，讓學員自行思考並繪製個資流程圖，提升學學習成效.....250
圖 12：資策會施叔良顧問講授「委外與事件通報」，讓學員瞭解為何要建立事件通報機制.....251
圖 13：資策會顧振豪組長講授「個人資料保護法介紹」及「考核作業手冊」.....251
圖 14：內政部地政司學員參與的狀況非常踴躍.....252
圖 15：資策會張曉芸研究員負責講授「個資盤點與風險評估」.....252
圖 16：內政部地政司學員討論熱烈.....253
圖 17：資策會施叔良顧問負責講授「個人資料保護委外管理程序」.....253
圖 18：各組學員上台發表委外管理之實作結果.....254
圖 19：資策會顧振豪組長負責講授「個人資料保護法介紹」.....254
圖 20：資策會陳秭璇律師負責講授「考核作業手冊」.....255
圖 21：資策會張曉芸研究員負責講授「個人資料盤點與風險評估」.....255
圖 22：各組學員分享實例演練.....256
圖 23：資策會施叔良顧問負責講授「委外與事件通報」.....256
圖 24：各組學員發表委外管理之實作結果.....257
圖 25：公務機關個資自評管理系統流程圖.....267
圖 26：公務機關個資自評管理系統架構圖.....268
圖 27：公務機關個資保護教育訓練管理系統流程圖.....291
圖 28：公務機關個資保護教育訓練管理系統架構圖.....292
圖 29：PDCA 流程圖.....312
圖 30：個資保護管理建置流程圖.....323
圖 31：個資管理與資訊安全管理系統之整合建議.....345
圖 32：CBPRs In Practice: A Four Step Approach.....508
圖 33：Structure of the CBPR Joint Oversight Panel.....509
圖 34：外賓及長官合照.....518
圖 35：法務部　曾勇夫　部長.....518
圖 36：行政院科技顧問組　陳炳煇　執行秘書.....519
圖 37：資訊工業策進會　李世光　執行長.....519
圖 38：經濟部商業司　李鎂　副司長.....520

本報告之智慧財產權歸屬於法務部

圖 39：法務部法律事務司　鍾瑞蘭　副司長.....520
圖 40：美國商務部科技與電子商務司副司長暨 APEC 資料隱私次級工作小組副主席　Mr. Joshua Harris.....521
圖 41：澳洲資訊委員會政策部政策助理委員 Ms. Rachael Spalding.....521
圖 42：日本亞細亞大學法學院　加藤隆之　副教授.....522
圖 43：資訊工業策進會科技法律研究所　邱映曦　主任.....522
圖 44：JIPDEC 隱私標章推動中心　関本貢　副中心長.....523
圖 45：綜合座談.....523
圖 46：資訊工業策進會科技法律研究所　戴豪君　所長.....524
圖 47：參與人數踴躍.....524
圖 48：民眾認知宣導摺頁.....714
圖 49：個人資料保護宣導摺頁說明手冊.....716
圖 50：中區教育訓練課程於台中公務人力發展中心七樓簡報室舉行.....732
圖 51：法務部法律事務司鍾瑞蘭副司長為學員致詞.....732
圖 52：勤業眾信聯合會計師事務所游靖芬副理擔任講師.....733
圖 53：學員參加狀況踴躍.....733
圖 54：法務部邱銘堂專門委員致詞.....766
圖 55：學員出席情況踴躍.....766
圖 56：勤業眾信會計師事務所曾韵經理講授課程.....767
圖 57：中階台中場-法務部鍾瑞蘭副司長蒞臨致詞.....768
圖 58：中階台中場-學員參與狀況熱烈.....768
圖 59：中階台中場-資策會李彥震諮詢師精彩解說「個人資料保護執行管理暨考核作業手冊」.....769
圖 60：中階台中場-法務部胡美蓁編審、資策會顧振豪組長、李彥震諮詢師，以及勤業眾信會計師事務所宋子莉副理，回覆學員提問.....769
圖 61：中階台北場-法務部陳維練司長蒞臨致詞.....770
圖 62：中階台北場-學員參與踴躍.....770
圖 63：中階台北場-資策會顧振豪組長、施叔良資深業務經理、李彥震諮詢師，以及勤業眾信會計師事務所游靖芬副理，回覆學員提問.....771
圖 64：中階台北場-學員提問踴躍.....771
圖 65：中階高雄場-法務部邱銘堂專門委員致詞.....772
圖 66：中階高雄場-學員參與踴躍.....772
圖 67：中階高雄場-法務部胡美蓁編審、資策會顧振豪組長、施叔良資深業務經理、李彥震諮詢師，以及勤業眾信會計師事務所宋子莉副理，回覆學員提問.....773
圖 68：中階高雄場-學員積極提問.....773
圖 69：中階花蓮（東部）場-法務部郭全慶專門委員致詞.....774
圖 70：中階花蓮（東部）場-學員參與踴躍.....774
圖 71：中階花蓮（東部）場-資策會顧振豪組長、施叔良資深業務經理、李彥震諮詢師，以及勤業眾信會計師事務所游靖芬副理協助學員解答.....775
圖 72：中階花蓮（東部）場-資策會施叔良資深業務經理、勤業眾信會計師事務所游靖芬副理授課授課.....775
圖 73：進階台北場-法務部鍾瑞蘭副司長致詞.....776
圖 74：進階台北場-資策會顧振豪組長與勤業眾信會計師事務所曾韵經理為學員解答..776

本報告之智慧財產權歸屬於法務部

圖 75：進階台北場-學員提問熱烈.....777
圖 76：進階台北場-學員參與踴躍.....777
圖 77：進階台中場-法務部鍾瑞蘭副司長致詞.....778
圖 78：進階台中場-學員進行分組練習.....778
圖 79：進階台中場-學員分享實作結果.....779
圖 80：進階台中場-資策會顧振豪組長與勤業眾信會計師事務所陳鴻棋副理，解答學員提問.....779
圖 81：進階高雄場-法務部郭全慶專門委員致詞.....780
圖 82：進階高雄場-學員參與踴躍.....780
圖 83：進階高雄場-學員進行分組實例演練.....781
圖 84：進階高雄場-法務部胡美蓁編審、資策會顧振豪組長，以及勤業眾信會計師事務所陳鴻棋副理為學員解答.....781
圖 85：進階花蓮（東部）場-法務部邱銘堂專門委員致詞.....782
圖 86：進階花蓮（東部）場-學員分享實例演練心得.....782
圖 87：進階花蓮（東部）場-學員積極提問.....783
圖 88：進階花蓮（東部）場-資策會顧振豪組長與勤業眾信會計師事務所陳威棋副理，為學員解答.....783

本報告之智慧財產權歸屬於法務部

表目錄

表 1：我國個人資料保護原則建議.....30
表 2：非公務機關個人資料檔案安全維護計畫標準辦法草案.....46
表 3：公務機關或學術研究機構基於醫療衛生或犯罪預防目的蒐集、處理或利用特種個人資料辦法草案.....65
表 4：「非公務機關個人資料檔案安全維護計畫標準辦法草案」意見回覆表.....92
表 5：「公務機關或學術研究機構基於醫療衛生或犯罪預防目的蒐集、處理或利用特種個人資料辦法草案」修正說明表.....100
表 6：試行機關成果問卷設計表.....118
表 7：內政部地政司地政資訊作業科個資事故通報與紀錄單.....135
表 8：內政部地政司地政資訊作業科事件紀錄表.....137
表 9：內政部地政司地政資訊作業科機房工作日誌.....138
表 10：內政部地政司地政資訊作業科矯正預防計畫表.....139
表 11：內政部地政司資訊作業科內部人員及廠商通報表.....140
表 12：輸出文件表.....145
表 13：：授委託服務廠商個資保護現況自評表.....146
表 14：廠商暨人員保密切結書.....151
表 15：廠商資訊安全同意書.....152
表 16：委外服務廠商監控記錄表.....154
表 17：法務部受理陳情請願事件登記簿.....161
表 18：法務部行政執行署陳情程序之個人資料盤點清冊.....167
表 19：法務部檢察司陳情程序之個人資料盤點清冊.....176
表 20：內政部警政署 165 專線意見回饋表統計結果(課程、講師、行政).....258
表 21：內政部警政署 165 專線培訓教育訓練活動意見回饋表統計結果(教學方式).....259
表 22：內政部地政司培訓教育訓練活動意見回饋表統計結果(課程、講師、行政).....260
表 23：內政部地政司培訓教育訓練活動意見回饋表統計結果(教學方式).....261
表 24：法務部行政執行署與法務部檢察司培訓教育訓練活動意見回饋表統計結果(課程、講師、行政).....262
表 25：法務部行政執行署與法務部檢察司培訓教育訓練活動意見回饋表統計結果(教學方式).....263
表 26：角色權限對照表(公務機關個資自評管理系統).....269
表 27：個資管理整體自評分析細項表.....275
表 28：個資環境設備安全評估自評項目表.....286
表 29：角色權限對照表(公務機關個資自評管理系統).....293
表 30：個資保護流程與 100 年 10 月間預告之個資法施行細則修正草案對應表.....324
表 31：請求他國政府協助之表格 1.....409
表 32：請求他國政府協助之表格 2.....410
表 33：相關組織表.....410
表 34：相關資料當事人表.....411
表 35：我國政府聯絡窗口表.....412
表 36：講習活動統計.....416
表 37：議程.....417

本報告之智慧財產權歸屬於法務部

表 38：Scope of the Acts.....512
表 39：Competent Ministry.....513
表 40：100 年 11 月 2 日 意見調查表統計.....514
表 41：100 年 11 月 3 日 意見調查表統計.....515
表 42：培訓課程出席人數統計表.....717
表 43：初階高雄場議程.....720
表 44：初階台北場議程.....720
表 45：初階台中場議程.....721
表 46：初階教育訓練意見調查表回收統計表.....726
表 47：初階高雄場課程、講師、行政意見回饋表統計結果.....727
表 48：初階高雄場教學方式意見回饋表統計結果.....727
表 49：初階台北場課程、講師、行政意見回饋表統計結果.....728
表 50：初階台北場教學方式意見回饋表統計結果.....728
表 51：初階台中場 課程、講師、行政見回饋表統計結果.....729
表 52：初階台中場教學方式意見回饋表統計結果.....729
表 53：第二年度培訓課程出席人數統計表.....734
表 54：初階花蓮場議程.....738
表 55：中階台中場議程.....739
表 56：中階台北場議程.....739
表 57：中階高雄場議程.....740
表 58：中階花蓮場議程.....741
表 59：進階台北場議程.....741
表 60：進階台中場議程.....742
表 61：進階高雄場議程.....743
表 62：進階花蓮場議程.....743
表 63：第二年度教育訓練意見調查表回收統計表.....744
表 64：初階花蓮場滿意度回饋表統計結果.....745
表 65：初階花蓮場教學方式回饋表統計結果.....745
表 66：中階台中場滿意度回饋表統計結果.....746
表 67：中階台中場教學方式回饋表統計結果.....746
表 68：中階台北場滿意度回饋表統計結果.....747
表 69：中階台北場教學方式回饋表統計結果.....748
表 70：中階高雄場滿意度回饋表統計結果.....749
表 71：中階高雄場教學方式回饋表統計結果.....749
表 72：中階花蓮場滿意度回饋表統計結果.....750
表 73：中階花蓮場教學方式回饋表統計結果.....750
表 74：進階台北場滿意度回饋表統計結果.....751
表 75：進階台北場教學方式回饋表統計結果.....751
表 76：進階台中場滿意度回饋表統計結果.....752
表 77：進階台中場教學方式回饋表統計結果.....752
表 78：進階高雄場滿意度回饋表統計結果.....753
表 79：進階高雄場教學方式回饋表統計結果.....753
表 80：進階花蓮場滿意度回饋表統計結果.....754

本報告之智慧財產權歸屬於法務部

表 81：進階花蓮場教學方式回饋表統計結果.....754

本報告之智慧財產權歸屬於法務部

壹、前言

一、計畫背景說明

（一）計畫依據

1.依據行政院 98 年 12 月 30 日院臺經字第 0980099463 號函頒「行政院『塑造資安文化、推升資安產值』產業科技策略會議關鍵推動方案（99 年至 102 年）」辦理，以「資安」為主題，在應用面上，對於電子商務安全希望在「維護民眾隱私、確保網路應用安全」上，凝聚議題共識並形成策略，具體行動計畫中規劃「9.健全電子商務個人隱私保護與管理─貫徹隱私保護方案」，以強化並提升電子商務個人資料保護與資訊安全，達到強化民眾個資保護之政策目標。

2.總統政見執行追蹤事項之人權政策（編號 286）關於「政府資料庫不得恣意聯結、濫用個人資料、侵害人民隱私」之執行事項，該執行事項並受行政院研考會列管。

3.「貫徹隱私保護方案」為法務部中程施政計畫之一，將分年逐步推動機關之個人資料保護。

4.行政院國家資通安全會報、行政院反制電話詐騙專案協調會議及反詐騙聯防平台會議等相關會議之決議，與 APEC 相關國際會議之加強個人資料跨境隱私保護之要求。

（二）現況分析

1.自 1992 年經濟合作暨發展組織（The Organization For Economic Cooperation And Development, OECD）第一次推出資訊系統及網路安全指引以來，由於資訊技術持續進步並帶來巨大的利益，同時各種威脅與負面影響隨之出現，進而促使公私部門及個人更加重視資通訊安全。有鑑於此，我國亦已於民國 84 年頒布「電腦處理個人資料保護法」，而後於民國 99 年修訂「個人資料保護法」。隨著全球電腦及網際網路科技發展飛速，電子商務隨即席捲全球各類商務市場，在數位化日常生活中，個人隱私資料亟需受到保護，包括身分、財務、健康、生活與消費習慣、行事曆、以及個人地址、電話號碼等。民國 99 年修訂之個人資料保護法已擴大適用於所有事業、團體或個人，亦將人工紙本之個人資料部分納入保護之範圍，以更全面、全方位之方式保護所有個人資料。近來公務機關個資外洩事件屢有所聞，顯見政府部門在個人資料之保護及管理上亦亟待加強。由於政府的資料庫均甚為龐大，如在資料提供二次利用上未慎重為之，動輒觸法且須負擔高額國

本報告之智慧財產權歸屬於法務部

家損害賠償責任。準此，如何為合法之個人資料蒐集、處理或利用，並預防個人資料外洩事件發生或降低損害，是目前公務機關最應重視且最急迫需要解決的難題，時程上刻不容緩。

2.塑造資通安全文化已是國際潮流，資通安全文化漸受各國重視，而我國為達安全信賴的資訊化社會與安心優質的數位化生活之願景，勢必讓資通安全文化蔚為風潮，落實在每個公、私部門及每個人的日常生活中，並強化民眾及政府部門個資保護與資訊安全自身應對及防範能力，因而在支援策略所需的資訊資本日益重要，各行各業相繼投入資源以強化資訊力作為組織要務之際，資安與隱私的重要性尤其不應該被忽視。政府將透過資安來為組織的核心業務創造價值，贏取民眾的信賴，並協助企業達成未來的競爭優勢。

3.個人資料保護法通過後，相關主管機關可依修正法規授權指定保有大量且重要之個人資料檔案的非公務機關，訂定個人資料檔案安全維護計畫，或業務終止後之個人資料處理方法，且以此版本內容研議立法通過後的民眾推廣措施、公務體系行政指導、各項研討會議及政府組織研究議題，為當前可預期新版法案通過之工作事項。同時，我國參與亞太經濟合作會議（Asia-Pacific Economic Cooperation, APEC）的個資隱私保護討論議題中，在法務與經濟代表的意見交流下，增加我國辦理個資保護相關官員至國外訪問及學習，以瞭解個資隱私先進國家的當前政策、機制、民間氛圍，並在國際情勢允許之情形下，推動國際間跨境隱私保護之合作，為我國國人個人資料作更完善之保護措施。

二、問題評析

（一）個人資料保護法制與執行措施須隨科技環境而與時變動，新舊法之交接尤需注意新舊規定之落差

新修正之個人資料保護法雖已經公布，惟其修正乃源於「電腦處理個人資料保護法」，因而多數公務員對諸多主要條文之修正，恐有法律觀念模糊或對於認知或處理上尚停留在電腦處理個人資料的法制規定上；或對於法律要求遵行事項在認知上雖然瞭解，但於實際執行上仍有困難。其主要的問題可能在於：(1) 對於本法實施後的保護客體範圍不清；(2) 對於本法實施後，其適用的主體不清楚，或對於其所主管的目的事業，應盡的保護責任不清楚；(3) 對於民眾或當事人的權益或應遵行的行為規範不清楚；(4) 對於行政檢查實施或落實需要進一步了解；(5) 對於個人資料保護團體的管理工作需要了解。

本報告之智慧財產權歸屬於法務部

針對以上五項問題，公務機關人員在因應與擬定對應策略時，可能存在有多項困擾。本計畫團隊認為，公務機關除了複雜之業務授權行為可能導致之個資管理問題外，可能因此產生以下八種基本面之困擾，請見下圖 1。

資料來源：本計畫整理

圖 1：新個資法對公務機關產生之困擾

個人資料保護法實施後，對於法令遵循與善盡管理義務之主要工作，包含公務機關內對個人資料保護與資訊安全工作的落實，以及個人資料保護相關程序與行政檢查工作的展開，實有其重新檢視之必要。

（二）透過個人資料保護與管理制度提升公務機關內部管理能力，有其急迫性與必要性

公務機關針對敏感性資料與一般個人資料目前皆有基本管理作法，惟欠缺一致性的觀念，相關管理模式亦莫衷一是。公務機關應整合不同的管理制度，

本報告之智慧財產權歸屬於法務部

符合相關法律要求與資訊管理規範，藉此機會提升公務效率。在科技進步與數位生活的快速發展下，個人隱私資料亟需受到保護，然而個人資料洩漏事件、電話詐騙層出不窮，公務機關個資外洩事件亦時有耳聞，顯見政府部門在個人資料之保護及管理上亦亟待加強，而由於政府的資料庫均甚為龐大，如在資料提供二次利用上未慎重為之，動輒觸法而須負擔高額國家損害賠償責任。準此，如何為合法之個人資料蒐集、處理或利用與預防個人資料發生或降低損害，以利各機關業務之正常推動，是目前公務機關最受重視且最急迫需要解決的難題，時程上刻不容緩。

本案關於公務機關人員的訓練，除了於初階課程中以實施普遍性的個資法介紹課程外，於中階之課程係借鏡日本、德國、與英國等國之實務，並參酌目前我國政府機關對於資訊安全相關規範與因應策略以及以產生之實務內容，加以整合，並形成四個主要重點：(1) 個人資料管理；(2) 個人資料保護；(3) 資訊安全管理；(4) 資訊安全一般水準。對於個人資料法制實施後，公務機關應如何妥適地保護與管理個人資料，設計專業培訓課程，訓練公務機關專責人員，建立其對於個人資料保護之認知與執行。針對進階之教育訓練，則將重點置於實作面，規劃以研習會（workshop）之方式進行，配合「個人資料保護執行程序暨考核作業手冊要點」之重要內容，與參與課程之受訓人員進行互動式之訓練，使參與人員具備實作層次之了解，於個人資料保護法正式實施後，能因應各單位之實際狀況與需求，確切執行個人資料之保護。

（三）如何強化個人資料蒐集處理或利用過程各個環節之隱私保護與資訊安全標準作業流程

現行電腦處理個人資料保護法對於經電腦處理之個人資料之蒐集、處理或利用上均定有要件規範，且在責任上亦有民事損害賠償責任、刑事責任，同時非公務機關更有行政責任。為避免公務人員動輒觸法，實有必要訂定公務機關個人資料保護及管理程序標準作業化流程，以便提供全國公務人員統一之執行標準，透過標準化作業流程及考核程序，讓公務人員明確執行個資法之相關規範，包括對非公務機關之監督管理程序，提供非公務機關明確之遵守標準或綱領，徹底做好個人資料之保護工作，避免後續之相關責任發生。

由於塑造資通安全文化已是國際潮流，資通安全文化漸受各國重視，而我國為達安全信賴的資訊化社會與安心優質的數位化生活之願景，勢必須讓資通安全文化蔚為風潮，落實在每個公、私部門及每個人的日常生活中。同時，並應強化民眾及政府部門個資保護與資訊安全自身應對及防範能力，促使各行各

本報告之智慧財產權歸屬於法務部

業相繼投入資源以強化資訊力作為組織要務，確保資安與隱私的重要性不被忽視。政府將透過資安與隱私來為組織的核心業務創造價值，贏取民眾的信賴，並協助企業達成未來的競爭優勢。

公務機關個人資料保護及管理程序標準作業化流程除應加強內部考核程序外，同時須導入外部監督程序，尤其公務機關現行考核程序尚未納入個人資料保護法之應有稽核程序，亦未建立獨立監督之角色要求，建議未來應有外部第三人定期或不定期之監督程序，以強化公部門個資保護程序之有效性。此外，公務機關委外管理情形普遍，但目前針對委外之個人資料管理，普遍缺乏監督程序，亦應有所加強。

本整合性計畫的核心效益，即是貫徹隱私保護的具體方針，同時達到指導我國公務體系建立個資保護基本法制與執行原則，以及公務人員之認知與專責人員之能力建構，故本計畫兼具內容重要性、資源整合性及政策急迫性，希冀藉由本計畫之執行，建立我國政府資訊安全與保護之安心、信賴生活環境。

三、計畫執行項目

綜上所述，本案係以公務機關個人資料保護方案為核心，研擬「公務機關個人資料保護方案」之計畫，以「公務機關個人資料保護機制建置計畫」及「公務機關個人資料保護教育訓練計畫」兩大分項計畫為執行主軸，前者包括「編撰個人資料保護法制及機關相關規範報告」、「研訂公務機關個人資料保護執行程序暨考核作業手冊及系統建置」、「規劃推動跨境隱私國際合作機制」及「統計個資保護執行與成果」；後者則包括「建置各機關專責人員教育訓練」、「舉辦資料隱私及資訊透明國際研討會」，以及「辦理公務機關個人資料保護專責人員培訓（初階、中階、進階培訓）」與「教材編撰與編印」。透過本整合性計畫之制度建立，一方面落實憲法保障資訊隱私權之宗旨，另一方面建立安全、安心與信賴的資訊環境。

本報告之智慧財產權歸屬於法務部

貳、建置個人資料保護法制研究報告及政策說帖

一、建置個人資料保護法制研究報告

（一）前言

個人資料保護法施行在即，為了減低企業之經營成本並且確保產業界遵守相關規範，政府應適度訂立規範協助企業建立個人資料管理以及保護等相關制度。

據此，本報告將分析各國際組織、各國個人資料保護原則之內容，並比對我國目前之個人資料保護法後，提出我國之個人資料保護原則之建議。確立個人資料保護原則後，將可明確提供我國的公務機關以及非公務機於管理以及保護個人資料之索引。

另外，本報告亦將提出非公務機關個人資料檔案安全維護計畫標準辦法草案以及個人資料保護法第 6 條第 2 項辦法草案。我國前年五月（民國 99 年 05 月）修正公布個人資料保護法後，個資法第 27 條授權中央目的事業主管機關得指定保有大量且重要個人資料檔案之非公務機關，訂定個人資料檔案安全維護計畫，因此目的事業主管機關須訂定個人資料檔案安全維護計畫標準辦法，供受指定之產業可遵循；而個資法第 6 條第二項授權中央目的事業主管機關須會同法務部訂立特種個人資料蒐集、處理或利用之範圍、程序及其他遵行事項之辦法，本辦法將針對公務機關或學術研究基於特定目的而蒐集、處理或利用醫療、基因、性生活、健康檢查及犯罪前科等個人資料之情形，訂立應遵行程序。

除此之外，由於我國個人資料保護法擴大個人資料定義以及適用主體範圍，所以現行電腦處理個人資料保護法特定目的與個人資料類別已不敷使用。因此，個人資料保護法第 53 條授權法務部會同中央目的事業主管機關指定特定目的與個人資料類別。本報告將於最後章節介紹我國現行特定目的與個人資料類別項目，同時亦將參考英國、澳洲、美國與日本之立法例，分析個人資料特定目的以及個人資料類別應修正之方向。

本報告之智慧財產權歸屬於法務部

（二）個人資料保護基本原則

由於透過個人資料之蒐集與分析可了解當事人之情況以及背景[1]，故必須建立個人資料保護原則、法制以保護資料當事人之權利。個人資料保護原則之建立，除了使資料當事人得以管控其個人資料外，亦可降低濫用個人資料之風險。所謂個人資料濫用包含了信用評價被降低、保險歧視(insurance discrimination)、收到垃圾廣告郵件以及推銷電話等，上述情形除了浪費當事人之勞力、時間以及費用外，更降低了當事人對於個人資料系統之信心。故，建立個人資料保護原則可保護當事人之利益，且鞏固當事人對於個人資料利用之信心[2]。

目前各先進國家以及國際組織皆訂有個人資料保護原則或指導綱領，相關個人資料保護原則通常以個人資料之蒐集、儲存、移轉以及個人資料處理程序為規範內容，透過個人資料保護原則之建立，賦予當事人採取適當措施保護其個人資料之權利，同時也要求資料蒐集處理者必須尊重當事人對於其個人資料之自主決定、控制權並遵守相關義務。另外，各國際組織之個人資料保護原則皆提供使當事人參與個人資料處理過程之機會。據此，透過個人資料保護原則之建立，得以規範資料管理者之行為，亦得保護當事人對其個人資料之自主決定權。

目前各國以及國際組織間，對於個人資料保護之概念主要分為兩種。以歐盟個人資料保護指令（EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995）為例，其認為個資保護係為保護當事人之基本權利，故必須建立個人資料保護法制以保護當事人之隱私。然而，APEC 於討論個人資料保護原則時，其概念之出發點與歐盟不同，根據 APEC 隱私保護綱領（APEC Privacy Framework）之起草目的，保護個人資料之原因主要著眼於促進各會員經濟體的商業利益，增強消費者信心，以強化個人資料自由傳輸所帶來之經濟效益。雖然對於保護個人資料之概念不盡相同，但基本上各國際組織、各國所建立的個人資料保護原則大致類

[1]例如信用卡交易資訊、汽車貸款、房屋貸款等資訊，為統計個人信用之參考依據。

[2] Benjamin J. Keele ,Privacy By Deletion：The need for A Global Data Deletion Principle,16 INJGLS 363 , 363-369（2009）.

本報告之智慧財產權歸屬於法務部

似。

國際上對於保護個人資料之原則皆有相當建樹，各國際組織均訂立個人資料保護原則。不同於環保或經濟議題，國際間對於個人資料保護原則並無共識，目前尚無全球性的個人資料保護原則。除了國際間對於個人資料保護之看法、文化背景不同外，資訊產業之發展快速，也造成建立全球性個人資料保護原則之阻礙[3]。

以下將整理歸納各組織以及各國的個人資料保護原則，並且根據國際上對於個人資料保護原則之要求，嘗試提出我國個人資料保護之原則。

1.澳洲

澳洲就其個人資料保護原則目前訂有國家隱私權保護原則（National Privacy Principles）以及資訊隱私保護原則（Information Privacy Principles）。

（1）國家隱私原則

國家隱私權原則之內容為非公務機關蒐集個人資料時，必須遵守之相關原則，內容整理如下：

A. 蒐集個人資料時必須具有特定目的，並以合法且正當之手段為之。

B. 向當事人蒐集個人資料時，必須確認當事人已了解以下資訊：蒐集機關之身分以及聯絡方式、當事人可查閱其個人資料、蒐集個人資料之目的、接受個人資料之第三人身分、蒐集個人資料所依循之法律、告知當事人未提供其個人資料之影響。另外，若機關並非從當事人處蒐集個人資料時，必須告知當事人以上資訊以確認當事人了解其本身之權利，除非可能造成嚴重之生命或健康之威脅時，始得免除此告知。

[3] Ariel E. Wade, A New Age of Privacy Protection: A Proposal for an International Personal Data privacy Treaty, 42 GWILR 659,660（2010）.

本報告之智慧財產權歸屬於法務部

C. 利用當事人之個人資料時，必須與蒐集目的相符。若所蒐集之個人資訊屬於敏感性資料時，則利用目的必須與蒐集目的直接相關，除非於當事人同意或當事人可合理期待之情形下，始得將當事人之資料用於其他目的。除此之外，若是為了公共利益以及研究統計之必要時，於不洩漏當事人之個人資料並合法之前提下，可做目的外之利用。另外，若係無可能獲得當事人之同意時，亦可做目的外之利用。

D. 紀錄：要求機關於利用或揭露個人資料時，必須留下使用以及揭露之紀錄。

E. 資訊品質：組織必須確認個人資料係屬完整、準確且保持不斷更新之狀態。

F. 資訊保全：組織必須採取合理措施避免個人資料遭誤用、滅失或者遭盜用、無權修改或揭露之情形。若利用或揭露之目的不存在時，機關必須銷燬個人資料或使個人資料達不能辨別之程度，以保護當事人之個人資料。

G. 當事人查閱之權利：當事人得向機關查閱其個人資料。除非該查閱將造成嚴重立即之生命或健康威脅、當事人之請求無理由或可能造成他人隱私權受損時等其他情形時，機關始可拒絕當事人查閱之申請，另外，若機關拒絕當事人查閱之申請時，必須提供合理之說明。

H. 機關不得採納由政府機關、政府委託機關所編碼之個人資料。另外，機關亦不得將已編碼之個人資料給予政府或者政府之委託機關，除非係基於法定義務、法律規定等情形始得為之。

I. 匿名化：無論是否可行或者合法，當個人與組織間進行交易行為時，可選擇匿名化，使得其個人資料無法識別。

J. 國際傳輸：基本上，接受個人資料之他國必須遵守與國家隱私原則相關之規定，並且機關需合理相信該國將會妥善管理當事人之個人資料時，始可跨境傳輸個人資料。

K. 敏感資訊：基本上不得蒐集敏感性資訊，除非取得當事人

本報告之智慧財產權歸屬於法務部

同意、依法律、為避免生命或健康之威脅等情形始得蒐集敏感性個人資料。

（2）資訊隱私保護原則

另外澳洲另訂有資訊隱私保護原則，其內容整理如下：

A. 蒐集限制原則：個人資訊不得透過紀錄或者一般可得之公開發行物進行蒐集，除非蒐集個人資料之目的係基於法律且與蒐集者之功能或活動具有直接相關。另外，蒐集個人資料時，必須採取合法且正當之手段為之。

B. 告知原則：基本上，向當事人蒐集個人資料時，蒐集前或於資料蒐集後必須告知當事人蒐集個人資料之目的、法律依據等資訊。

C. 資料品質原則：若是經由一般公開之管道徵求個人資料時，蒐集資料者必須採取合理措施確認其已遵循蒐集資料之目的蒐集個人資料，並須確認該個人資料係完整精確且處於不斷更新之狀態，另外，亦須確認蒐集個人之資訊並未不合理侵害當事人之個人事務。而已持有個人資料者，必須於使用個人資料前，採取適當措施，確認使用個人資料目的之合理性、資料之準確性、不斷更新狀態以及完整性。除此之外，持有個人資料者，必須採取合理措施確認個人資料係精確的並且使用合於蒐集目的。同時，於當事人要求修改或更正其個人資料時，紀錄持有者應該採取相關步驟，並附上當事人要求之更正、刪除或者增加等相關文件。

D. 個人資料之儲存與保全：擁有與控制個人資料者必須以安全防護措施保護個人資料，以避免個人資料流失、無授權之侵入使用修改或者揭露及其他誤用情形。另外，若因持有個人資料者之相關服務而必須提供個人資料予他人時，持有個人資料者必須採取合理之措施防止無授權之使用或揭露該個人資料之情形。

本報告之智慧財產權歸屬於法務部

E. 個人資料持有者應紀錄之相關資訊：個人資料持有者必須針對持有個人資料種類、時間、目的、管控個人資料庫之情形等作紀錄。另外，必須建立程序使當事人有得以查閱其個人資料之管道。該紀錄必須交付影本予個人資料保護之專員。

F. 個人資料之當事人有權查閱其個人資料。

G. 限制使用原則：個人資料只能使用於個人資料相關之目的時，始可利用。另外，基本上個人資料不得作為目的外使用，除非具有以下情形，始得作為目的外之利用：獲得當事人之同意；蒐集目的外之使用對於減輕當事人或其他人健康、生命等即刻威脅且係必要的；經主管機關或依法律得進行特定目的外之使用；為執行刑法、與金錢相關之懲罰等相關程序或公共利益之保護；使用之目的與蒐集目的係具有直接相關的。

H. 揭露個人資料之限制：持有個人資料之紀錄持有者不得揭露當事人之個人資料予任何人、團體或者機關，除非具有以下情形：當事人合理可知其個人資料通常將被傳輸至個人、團體或機關；當事人同意該揭露行為；揭露對於減少、防止嚴重且立即生命與健康之威脅係有必要的；該揭露係經主管機關授權或者依法為之；該揭露對於執行刑法、與金錢相關懲罰以及保護公共利益係必要者。

2.OECD 隱私保護與個人資料跨境流通指導原則（Guidelines on the protection of Privacy and Transborder Flows of Personal Data）

由於資訊科技之發展，自動化處理個人資料之技術使得個人資料快速且容易被傳輸。然而，當各國紛紛制定其個人資料保護法制時，就產生了各國法之差異可能造成個人資料跨境傳輸時之障礙。有些行業，例如金融業以及保險業對於跨境個人資料傳輸有極大需求，但卻因為各國法制不同，而產生個人資料無法有效傳輸之情形。故如何解決個人資料跨境傳輸之問題，亦成為各國所共同面臨之議題，另外 OECD 會員國也認為有必要制訂個人資料保護法制以避免個人隱私權

本報告之智慧財產權歸屬於法務部

被侵害、個人資料被濫用等情形，因此，OECD 建立各國共通之指導原則以幫助調和各國之個人資料保護法制，並且在提升人權保護以及避免妨礙個人資料國際傳輸間尋求平衡點[4]。

隱私保護與個人資料跨境流通指導原則係於 1980 年 9 月 23 日被採納，該指導原則整合國際間對於個人資料蒐集以及管理制度之共識。OECD 指導原則係 OECD 於 1980 年提出的第一個全球性的隱私保護原則。該指導原則對於美國早期建立「公平資訊實務」具有深遠影響，除了美國之外，OECD 指導原則亦被各國接受為個人資料保護之基本原則，因此指導原則亦為各組織、各國所建立之個人資料保護原則之基本架構。另外，歐盟隱私權保護指令亦將 OECD 指導原則編入其內容。於 1981 年，個人資料自動化處理保護公約[5](Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data)與歐洲議會協商，要求公約簽署國必須於該國實行個人資料保護法制。

OECD 於 1980 年公佈「個人資料保護準則以及跨國資訊傳輸準則」(Recommendations of the Council Concerning Guidelines Government the Protection of Privacy and Trans-Border Flows of Personal Data)，列出七項原則；一、通知(Notice)：當個資被收集時，應通知當事人。二、目的(Purpose)：資料僅得以說明之目的為使用，不得作為其他目的之使用。三、同意(Consent)：未獲得當事人之同意時，不得揭露當事人之資訊。四、安全保障(Security)：需保障被蒐集之資料被濫用。五、揭露(Disclosure)：當事人應被告知誰在蒐集他們的資料。六、查閱(access)：當事人應可查閱其個人資料並且可改正任何不精確之個人資料。七、責任原則(Accountability)：當事人須被通知須負起個人資料蒐集使用以及管理責任者為何人。透過個人資料保

[4] OECD 網站，http://www.oecd.org/document/20/0,3746,en_2649_34255_15589524_1_1_1_1,00.html，最後瀏覽日 2011 年 9 月 28 日。

[5] 該公約係第一個具有拘束力之國際公約。其內容主要針對國際間針對保護個人資料不被濫用以及跨境資料傳輸之規範。除了關於個人資料處理以及蒐集之提供保證外，若缺乏對於敏感性資料適當之保護措施時，公約禁止處理種族、政治傾向、健康、宗教、性生活、犯罪紀錄等敏感性個人資料。另外，公約亦確認資料當事人有權了解其個人資料係被誰所儲存，於必要之情形下，當事人亦有修正其個人資料內容之權利。當具有更優先利益時，例如國家利益、國家防禦等情形，公約裡所規範之權利需受限制。除此之外，該公約更規定跨境傳輸個人資料時，若他國未提供相等之保護措施時，跨境傳輸行為須受限制。

本報告之智慧財產權歸屬於法務部

護準則以及跨國資料傳輸準則表達各國整合個人資料保護原則之共識，亦可了解 OECD 各會員國對於消除各國間對於個人資料保護差異以及建立更有效率之跨國個人資料傳輸制度有一致想法。

除了個人資料保護準則以及跨國資訊傳輸準則外，OECD 隱私保護與個人資料跨境流通指導原則主要包含八項原則，包含限制蒐集原則（The Collection Limitation Principle）、資料品質原則（The Data Quality Principle）、目的明確化原則（The Purpose Specification Principle）、限制使用原則（The Use Limitation Principle）、安全保護原則（The Security Safeguards Principle）、公開原則（The Openness Principle）、個人參與原則（Individual Participation Principle）、責任義務原則（Accountability Principle）。指導原則中，最重要的兩個基本思想為，保護個人隱私以及個人自由、促進各國間個人資料傳輸之流動，故為嘗試平衡保護個人隱私以及促進個人資料流通之兩項目標，於訂立個人資料蒐集原則之同時，亦強化推廣個人資料自由跨境流動之概念。

雖然 OECD 之指導原則希望能建立共通原則以消除各會員國國內法之差異，但 OECD 之指導原則係無拘束力的，例如，簽署 OECD 指導原則之美國並未將指導原則訂入其國內法內，故關於個人資料保護之法律於各會員國間仍互有異同，也由於 OECD 指導原則無拘束力而產生法制不一致、妨礙資料之自由傳輸之情形，歐盟執行委員會因此公佈具有拘束力之隱私權保護指令（Data Protection Directive）。以下整理 OECD 個人資料保護原則：

（1）限制蒐集原則（Collection Limitation Principle）：須以正當合法之手段蒐集當事人之個人資料；於適當情形下，必須經資料當事人之同意。

（2）資料品質原則（Data Quality Principle）：個人資料必須與使用個人資料之目的相關。並在使用目的之合理範圍內，確保個人資料係精確、完整並且是不斷更新之狀態。

（3）目的明確化原則（Purpose Specification Principle）：蒐集個人資料之特定目的必須在向當事人蒐集個人資料時即說明清楚。隨後之使用亦必須限制於蒐集目的或不違反蒐集目的之情形。

本報告之智慧財產權歸屬於法務部

（4）限制使用原則（Use Limitation Principle）：個人資料不得為第三項原則特定目的外之揭露、使用，除非具有以下之情形獲得當事人之同意或經法律授權

（5）安全保護原則（Security Safeguards Principle）：個人資料應以適當的安全防護措施加以保護，以避免遺失、盜用、毀損、竄改或者揭露之危險。

（6）公開原則（Openness Principle）：關於個人資料，應公開設立原則、程序操作、執行情形以及相關做法。

（7）個人參與原則（Individual Participation Principle）當事人應具有以下權利：(A)向資料管理者確認是否資料管理者擁有與當事人相關之個人資料以及擁有之個人資料範圍。(B)當事人得於適當合理之時間內，了解與其相關之個人資料。若需收費時，費用不得過高。資料管理人必須以淺顯易懂之方式使當事人了解其個人資料之程序。(C)若當事人向資料管理者了提出以上(A)、(B)兩項要求被資料管理者拒絕時，資料管理者必須給予當事人理由，並且給予當事人申訴之管道。(D)給予當事人要求刪除、校正、修改其個人資料之機會。

（8）責任義務原則（Accountability Principle）：資料管理者必須採取合理且適當措施以符合以上所述之原則。

3.歐洲高峰會條約（Council of Europe Convention）

於 OECD 指導原則被採納之一年後，歐盟高峰會公佈個人資料保護以及處理個人資料程序協定（the Convention for the Protection of Individual with Regard to the Collection and Processing of Personal Data on Information Highways, COE Convention）。基本上，該協定所採納之個人資料保護原則與 OECD 隱私保護與個人資料跨境流通指導原則大致上相同。唯有一點不相同之處為，一旦辨識當事人之需求已經不存在時，必須匿名化個人資料以避免洩漏當事人之個人隱私[6]。

[6] Benjamin J. Keele , Privacy By Deletion：The need for A Global Data Deletion Principle, 16 INJGLS 363, 371(2009).

本報告之智慧財產權歸屬於法務部

4.歐盟

觀察歐洲過去之歷史，有關於個人資訊之濫用等歷史事件，使得歐洲認為個人隱私權之保護係為基本人權之一，其實由人權條約以及各國對於個人資料保護法制之規定，亦可了解歐洲國家認為人對於其個人資料具有自我決定之基本權利(self-determination)、自由權之保護（protection of liberty）以及思想自由(freedom of thought)。如前所述，相較於歐盟對於個資隱私之概念，APEC 主要係著眼於政策利益，必須保障個人資料隱私，以使得個人對於其個資之利用具有信心，進而促進網路時代經濟之發展[7]。

於歐盟制訂個人資料保護指令前，1950 年代，歐洲普遍認為個人隱私屬於個人基本權之內容，基於這個概念，於 1960 年代歐盟理事會將自動化處理個人資料制定為保護個人資料之一環；1970 年代中期，歐洲更分別制定政府機關以及非政府機關保護個人資料之法律。但由於各國對於個人資料保護之原則各不相同，造成個人資料利用上產生窒礙難行之問題，據此，歐盟體認到需要制定一個得作為基本綱領之個人資料保護原則[8]。

為了使歐盟之會員國共同遵守保護個人資料之原則，歐盟於 1998 年 10 月發布隱私保護指令。相對其他國際組織所定的個人資料保護原則，歐盟之個人資料保護指令對於個人資料保護採取較高之標準，除此之外，歐盟保護指令亦以高執行標準要求各會員國依循該指令建立各國之個人資料保護法[9]，歐盟要求各會員國必須於指令公佈後，於各國法中依指令所訂之原則制定各國個人資料保護法制。故，歐盟境內各會員國之個人資料法制皆遵守幾項共通原則，包含建立最低標準之個人資料保護制度，以及消除會員國間個人資料傳輸之限制。然而，由於會員國眾多、各國法制仍有相異之處以及各國對於個人資料保護處理原則之解釋互不相同，造成私人機關適用各國之個人資料法制時，依然遭受極大困難以及必須負擔相當大之經濟成本，因此各國

[7] Stuart Hargreaves, Inadequate: The APEC Privacy Framework& Article25 of the European Data Protection Directive, 8 CANJLT1, 4（2010）.

[8] Ariel E. Wade，A New Age of Privacy Protection: A Proposal for an International Personal Data Privacy Treaty, 42 GWILR 659, 669（2010）.

[9] Stuart Hargreaves, Inadequate: The APEC Privacy Framework& Article25 of the European Data Protection Directive, 8 CANJLT1, 1（2010）.

本報告之智慧財產權歸屬於法務部

法間缺乏和諧性仍係目前歐盟個人資料保護制度所遭受之最大批評[10]。

歐盟個人資料保護指令中，對於個人資料（Personal Data）係指任何可直接或間接辨認自然人之資料，例如識別碼或者是自然人之生理、心理特徵、經濟情況、文化或是社會身分。相較於其他個人資料保護法制之相關定義，歐盟對於個人資料係採取較為寬廣之認定方式。另外，歐盟不僅保護消費者之個人資料，亦保護勞工、供應商、攤販等其他連絡人之資料。

（1）歐盟隱私指令整理歸納

A. 該指令應用於自動化以及非自動化處理之個人資料。

B. 該指令將不適用於下類處理個人資料之情形：

a.自然人為單純個人或家庭之使用。

b.屬於歐洲共同體法以外之活動，例如公共利益之保護以及國家安全之防衛

C. 該指令基於保護個人資料隱私權制定以下指導原則，以決定個人資料之處理是否合法。指導原則為：

a.資料之品質(the quality of the data)：個人資料必須適當、且合法的被處理，並且須符合特定、清楚、正當之目的始得蒐集。另外，個人資料須保持精確以及不斷更新之狀態。

b.合法處理個人資料（the legitimacy of data processing）：個人資料僅在當事人給予清楚同意或者有必要時，始得處理之。另外，符合以下要件亦可為之：

[10] Elizabeth H. Johnson, Data Protection Law in the European Union,54-SEP FEDRLAW 44, 44-45（2007）.

本報告之智慧財產權歸屬於法務部

I.為了履行當事人參與之契約內容

II.為了達成資料管理者被要求之義務

III.為了保護資料當事人之重大利益

IV.為了達成保護公共利益之任務

V.為了達成資料管理者所欲達成之合法目的

c.特種資料之處理(special categories of processing)：禁止處理有關於種族、宗教、政治意見、哲學思想、工會會員以及有關於健康和性生活之個人資料。具有特殊情形始可搜集該類特種資料，例如為了重大利益而處理該資訊，或者為了預防性的醫學或醫藥診斷。

d.給予當事人之資訊：資料管理者必須提供當事人資料處理程序中所獲得有關當事人之資料。另外，資料管理者亦須提供資料管理者之身分，處理個人資料之目的，收受個人資料之人等資訊給當事人。

e.當事人得以查閱其個人資料(the data subject's right of access to data)：當事人有權利從資料管理員獲得以下資料

I.確認其個人資料是否被處理中以及資料處理之聯絡管道

II.對於未依循隱私指令所處理之個人資料、不完整或不精確之個人資料以及對於接受個人資料之第三方之通知，當事人皆有修正、調整之權利。

f.可免除之義務以及限制：關於個人資料品質之範圍以及原則，於保護國家安全、國家防衛、公共安全、刑事起訴

本報告之智慧財產權歸屬於法務部

程序、會員國重要之經濟以及金融利益或者保護當事人等情形時，可拒絕當事人查閱之申請、免除需提供給當事人之訊息以及須公開處理等義務。

g.當事人有拒絕處理其個人資料之權(the right to object to the processing of data)：於法律授權之情形下，當事人應有權拒絕他人處理其個人資料。於無論是否須收費之情形下，當事人均有權拒絕基於直銷目的之個人資料處理。於直銷之情形時，在揭露當事人資訊予第三人前，資料管理者必須通知當事人。另外，應清楚告知當事人具有拒絕該類揭露其個人資料之權利。

h.資料處理之保全及保密性(the confidentiality and security of processing)：受資料管理者委託處理個人資料之人，包含有權接觸當事人資料之資料管理者，本身應不得利用資料管理者所提供之方法外之其他方法處理當事人之資料。除此之外，資料管理者必須採取安全管理措施以保護當事人之個人資料，以避免個人資料意外、非法毀損滅失；變質；未經授權之揭露或者其他盜用當事人個資之情形。

i.通知個資監督主管機關之義務(the notification of processing to a supervisory authority)：於執行任何個人資料處理程序前，資料管理者必須通知個人資料監督主管機關。個人資料監督主管機關依循通知之內容進行前階段之檢查，確認該個人資料處理程序是否產生當事人權利或自由權之侵害風險。另外，應確認是否已採取合理措施公開該個人資料處理程序，個資監督主管機關必須記錄資料管理者對於處理程序之通報內容。

D. 對於有疑問、使當事人遭受權利侵害之個人資料處理程序，當事人依國內法具有可依司法程序提起損害賠償之權利。除此之外，因非法處理個人資料而遭受損害之資料當事人可接受其受損害之賠償。

本報告之智慧財產權歸屬於法務部

E. 將個人資料跨國傳輸至亦具有個人資料保護法制之第三國時，該個人資料傳輸行為須係可允許的。然而，除非具備相關例外情形[11]，若未確認第三國個人資料保護程度時，禁止跨國傳輸行為。

F. 個人資料保護指令目的係為了鼓勵歐盟之會員國起草各國之個人資料保護。

G. 各國應設立個資隱私保護小組，該小組係由各國個資監督主管機關之代表、歐盟組織或團體之個資監督主管機關之代表以及歐盟理事會之代表所組成。

（2）分析歐盟個人資料保護指令之原則

1995 年制定的歐盟個人資料保護指令主要包含兩個概念，首先是該指令主要以保護個人之基本權、自由權以及處理個人資料為前提，尊重個人之隱私權。另外，該保護指令亦確立了「會員國既不應該限制也不應該禁止個人資料之自由傳輸」[12]。為了達成以上概念，該指令主要包含六大原則：

A. 合法性(Legitimacy)：應以合法且正當之目的處理個人資料。

B. 合目的性(Finality)：僅得依特定且合法之目的蒐集個人資料，而且不得脫離原本蒐集目的進一步地處理個人資料。

C. 透明性(Transparency)：當事人有權利了解處理其個人資料之相關程序。

D. 比例性(Proportionality)：個人資料之蒐集或處理之目的必須與個人資料具有相關性，而且不得過度延伸目的。

E. 保密以及保護措施(Confidentiality and Security)：採取適合

[11] EU Directive 95/46/EC of The European Parliament and of The Council of 24 October 1005, Article 26.
[12] Ariel E. Wade, A New Age of Privacy Protection: A Proposal for an International Personal Data privacy Treaty, 42 GWILR 659, 670（2010）.

本報告之智慧財產權歸屬於法務部

之技術以及組織上之措施以避免處理個人資料過程中可能產生之風險，並保障個人資料之機密性與安全性。

F. 控制機制(Control)：個人資料保護之主管機關必須實行個人資料保護法律。

G. 保護指令第一章對於個人資料保護之相關名詞進行定義，提及自動化處理個人資料亦屬於個人資料處理之範圍。但是，若是家庭活動、保護國家利益等例外情形，則不在本指令討論範圍之內。歐盟保護指令之對象主要為自然人，尤其是自然人之隱私權。

於保護指令第二章內，歐盟個人資料保護指令將一般個人資料保護原則分為九個項目[13]說明：

A. 個人資料品質原則：會員國應規定個人資料須以合法、正當之手段且具特定目的之情形下蒐集之。且當處理個人資料之目的已消失時，必須採取適當手段將個人資料予以匿名化以保護個人資料。

B. 合法化個資處理程序準則：除了例外之情形外，處理當事人個人資料前必須取得當事人之同意。例外規定包含履行契約或者為了符合法律規範之情形。

C. 敏感性資料之處理：除了例外情形外，原則上禁止處理種族、政治意見、宗教信仰、公會會員身份、或者當事人之健康、性生活等敏感性個人資料。除此之外，針對表達自由所保護的新聞自由、文學以及藝術表現等，會員國被要求制定例外規定以平衡表達自由以及個人資料保護之權利[14]。

D. 須提供給個資當事人之資訊：資料管理者必須提供資料當事人其身分識別、處理個人資料之目的，以及其他可確認個人資料保護之相關資料。另外，於資料管理者非從當事

[13] Stuart Hargreaves, Inadequate: The APEC Privacy Framework& Article25 of the European Data Protection Directive, 8 CANJLT1, 12-14（2010）.

[14] EU Directive 95/46/EC of The European Parliament and of The Council of 24 October 1005, Article 8.

本報告之智慧財產權歸屬於法務部

人處獲得個人資料之情形下，在資料管理者第一次接觸到當事人之個人資料前，亦必須提供以上資料給當事人。

E. 個人資料當事人查閱其個人資料之權利：當事人有權利向資料管理者要求提供以下相關資料：確認當事人之個人資料已經依其蒐集以及使用目的處理之；已收受當事人個資者之資料；個人資料之來源；了解個人資料自動處理之過程中所為之程序。另外，依歐盟保護指令之規定，資料當事人亦有權要求終止個人資料之利用或修改其個人資料[15]；當事人亦有權利要求資料管理者通知接收當事人個資之第三人終止個人資料之利用以及修改其個人資料。

F. 例外與限制規定：於各會員國須保護其重大利益之情形時，得採取立法措施限制處理個人資料之權利、義務範圍[16]。所謂重大利益通常係指國家利益（national security）、其他自由權以及基本權（the rights and freedoms of others, etc）[17]。

G. 當事人得行使拒絕權之情形：於特定情形下（例如直銷），當事人得拒絕資料管理者處理其個人資料。另外，若自動處理個人資料之結果將造成當事人法律上或其他重大影響時，當事人得要求停止處理個人資料。

H. 個人資料處理程序之保密以及安全防護規定：個人資料管理者應採取適當程序上或組織上之措施以保護當事人之個人資料免於毀損、遺失、未經授權揭露或者遭他人截取等狀況。另外，處理個人資料者及其委託之人，必須依循資料管理者指示處理個人資料，以確保個人資料之安全[18]。

---

[15] Elizabeth H. Johnson, Data Protection Law in the European Union , 54-SEP FEDRLAW 44, 45（2007）.

[16] Ariel E. Wade, A New Age of Privacy Protection: A Proposal for an International Personal Data privacy Treaty, 42 GWILR 659, 672（2010）.

[17] 於歐盟保護指令下，個人隱私權之保護並不是絕對概念。除了科學研究、統計分析等目的外，保護指令臚列七項例外容許會員國於特定情形下，得限制個人隱私權之保護。七項例外包含了保護國家安全、國防利益、公共安全、國家經濟或財政利益、犯罪攻防或者調查違反職業道德之行為、有關公共安全、犯罪行為、違反職業道德、會員國之經濟與財政利益之相關法律規定、資料當事人或者其他人之自由權。

[18] Ariel E. Wade, A New Age of Privacy Protection: A Proposal for an International Personal Data

本報告之智慧財產權歸屬於法務部

I. 通知：除例外之情形外，資料管理者於進行任何處理個人資料程序前，必須通知相關個人資料主管機關，於資料管理者處理個人資料前，會員國應就資料管理者所提供之資料，考量可能產生之風險，除此之外，處理個人資料之過程亦應該登記並記錄在各國之個人資料主管機關。資料管理者必須提供以下資料給該國之個人資料主管機關，包含處理個人資料之目的、被處理之個人資料類型、接收個人資料者、以及任何預定在歐盟境外移轉個人資料之情形。

於歐盟保護指令第三、五、六、七章屬於程序上之相關規定。第三章主要規定了侵害保護指令之司法救濟以及裁罰程序。第五章要求會員國起草相關行為準則供個人資料管理者遵循。第六章則是要求各會員國成立各國主管個人資料保護之獨立機關，該機關負責監控歐盟個人資料保護指令於各國實施之情形，該機關並被賦予調查以及執行法律之權力。第七章則是提出歐盟個人資料保護指令應如何被執行之指示。

而歐盟保護指令第四章提及了個人資料跨境傳輸之議題。歐盟保護指令要求受移轉之人者必須採取適當程度之保護措施，以確保受移轉之個人資料之安全性;另外，除非歐盟會員國已採取適當之個人資料安全保護措施，歐盟之會員國不得將個人資料跨境移轉予非屬歐盟會員國之國家[19]，至於是否已經採行合適之措施保護個人資料，必須個案認定第三國之個人資料法制實施狀況。若非歐盟會員國之第三國未採取完善之個人資料保護法制時，於以下所述之情形時，歐盟會員國仍可將個人資料傳輸至第三國[20]：

A. 獲得當事人同意

B. 為了履行當事人與資料控制者間的契約或者訂約前之預備行為

---

privacy Treaty, 42 GWILR 659, 671（2010）.

[19] EU Directive 95/46/EC of The European Parliament and of The Council of 24 October 1005, Chapter Ⅳ Article 26.

[20] EU Directive 95/46/EC of The European Parliament and of The Council of 24 October 1005, Chapter Ⅳ Article 26 1.

本報告之智慧財產權歸屬於法務部

C. 為了實現資料管理者與第三人間對於資料當事人有利之契約

D. 基於法律要求或者實現重大公共利益，或者為了建立、實施法律聲明及防禦之目的

E. 為了保護資料當事人之重大利益

F. 為了提供一筆依法須提供予公眾的資訊、或是由具有法律上利益之人所查詢的資料。

若未具備歐盟保護指令第 26 條第一項之例外條件時，歐盟會員國仍有操作個人資料跨境傳輸之作法。依據歐盟保護指令第二項之規定，資料控制者依契約要求第三國之機關採取充分保護個人資料之措施以保護個人隱私權與其他人格權時，會員國仍可授權境內之機關傳輸個人資料至第三國[21]。

雖然歐盟看似對於個人資料跨境傳輸之規定較為嚴格，但其仍肯定個人資料自由跨境傳輸具有經濟上利益，因此，歐盟基本上鼓勵個人資料跨境流通之概念[22]。另外，依保護指令第 29 條之規定，各會員國須設立個人資料保護工作小組（Working Party on the Protection of Individual with regard to the Processing of Personal Data），工作小組必須就第三國推行個人資料保護之程度向歐盟理事會報告，但歐盟理事會並非一定要接受工作小組之建議，而歐盟所做之政策決定也必須通知工作小組。

如同歐洲高峰會之條約(COE convention)，歐盟個人資料保護指令於資訊品質原則中亦提及如所蒐集使用個人資料之目的已經達成者，應將當事人之個人資料予以匿名化[23]。

另外，歐盟保護指令賦予當事人有權利了解處理其個人資料程序，舉例而言，資料管理者必須在合理之時間內，且不要求當事人付出過度之勞力時間成本之情形下，使當事人得查閱其個人

[21] 可參考 2001/497/EC,2002/16/EC,以及 2004/915/EC 之歐盟跨境隱私契約範本。

[22] Stuart Hargreaves, Inadequate: The APEC Privacy Framework& Article25 of the European Data Protection Directive, 8 CANJLT1, 12（2010）.

[23] EU the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data(EU Directive) Article 6 ,1.(e)

本報告之智慧財產權歸屬於法務部

資料被處理之過程、確認資料管理者是否持有其個人資料、資料處理之目的、收受個人資料者之身分，另外，資料管理者也必須提供管道使當事人得以查閱並主張其權利[24]。

針對個人資料保護執行面，歐盟個人資料保護指令要求各國設立個人資料保護之政府監督機關，以監督資料管理者是否依循保護原則處理當事人之個資，同時亦提供當事人於其個人資料受侵害時相關法律救濟途徑[25]。

雖然歐盟個人資料保護指令制訂至今已有十六年的時間，且由於歐盟各國對於該指令之解釋有所出入，造成法律適用上之困難。但是不可否認的是，歐盟個人資料保護指令對於商業運行仍有重大影響。例如，要求企業主提供其僱員、勞工、客戶個人資料之處理資訊、限制個人資料之跨境傳輸或者是向個人資料處理機關註冊等，皆對於企業之運作有所規範。

歐盟保護指令除了對於歐盟會員國具有約束力外，對於非歐盟會員國亦具有相當之拘束力，該拘束力主要反映於歐盟保護指令對於跨境資料傳輸時之規範。於歐盟保護指令中，若第三國之國內法對於個人資料保護不足時，歐盟執行委員會禁止會員國傳輸個人資料至該國[26]，之後歐盟執行委員會將會嘗試與該國協商修改其國內法，以達成歐盟個人資料保護原則之標準，因此許多非歐盟會員國之國家依循歐盟個人資料保護指令之規範訂定其國內之個人資料保護法制，例如杜拜、俄羅斯以及南非等國家，以爭取個人資料跨國傳輸之機會[27]。

5.英國個人資料保護法（Data Protection Act 1998）

1984 年通過之資料保護法(the Data Protection Act 1984)，將英國之個人資料保護原則法制化，1984 年版本之個人資料保護法包含處理

[24] EU the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data(EU Directive), Article 12.
[25] EU the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data(EU Directive), Article22-24
[26] EU Directive 95/46/EC of The European Parliament and of The Council of 24 October 1005, Chapter Ⅳ Article 25 (2).
[27] Elizabeth H. Johnson, Data Protection Law in the European Union , 54-SEP FEDRLAW 44, 48（2007）.

本報告之智慧財產權歸屬於法務部

個人資料之正當性原則之規範。但由於該法對於個人資料(personal data)和處理過程(processing)之定義過於狹窄，引發爭議，因此，英國於 1998 年通過 1998 年資料保護法(the Data Protection Act 1998)，除此之外，對於個人資料(personal data)以及資料處理(processing)之定義，該法亦採取歐盟隱私保護指令之定義。

1998 年資料保護法明確規範當事人有權利向資料管理者要求接觸其個人資料，而當資料管理者處理當事人之個人資料時，必須通知資料當事人。再者，資料管理者必須提供淺顯易懂之表格予當事人，使當事人有清楚之管道向資料管理者提出查閱個人資料之要求，除此之外，當自動處理個人資料之結果對於當事人有重大影響時，當事人亦有權了解個人資料自動處理過程之資訊[28]。以下整理英國隱私保護原則：

（1）應以正當且合法之行為處理個人資料。除非具備以下情形，否則不得處理個人資料：

A. 至少須符合以下其中一項之情形：當事人同意、履行契約、資料管理者為履行法定義務、執行司法行政事項、執行議會功能、政府功能之執行等

B. 於敏感性資料而言，必須符合以下其中一項之情形：當事人明確之同意、為了履行僱傭關係中相關之權利義務、為了滿足特定之情形。

（2）必須具備特定目的始得獲得個人資料，且不得以不符合目的之方式進一步處理個人資料。

（3）必須以充分、相關聯並且合理限度之目的處理個人資料。

（4）於必要情形下，個人資料必須保持準確，且不斷更新之狀態。

[28] Scott Rempell, Privacy personal data and subject access rights in the European data directive and implementing UK statute：Durant V. Financial Service authority as a paradigm of data protection nuances and emerging dilemmas, 18 FLJIL807, 817-820 (2006).

本報告之智慧財產權歸屬於法務部

（5）不得超出必要期間保存依任何目的所處理之個人資料。

（6）應採取適當措施以及設立相關組織以避免當事人個人資料意外遺失、毀損、破壞或遭盜用。

（7）除非已確認他國亦採取適當程度之保護措施保護個人資料，否則不得傳輸個人資料至歐洲經濟領域外之其他區域。

6.APEC 隱私保護綱領（APEC Privacy Framework）

為了推廣亞太地區的電子商務，2004 年 APEC 發佈隱私保護綱領以符合 OECD 隱私保護與個人資料跨境流通指導原則，此綱領除了規範個人資料保護原則外，更提供 APEC 經濟體內之企業組織清楚且明白之行為原則，為了保護個人資料不受濫用及侵害，並且促使 APEC 會員國執行一套有關個人資料處理以及利用之全球化標準程序，隱私權保護綱領提供 APEC 會員國對於各國個人資料保護法之制定參考[29]。

APEC 隱私保護綱領之制定主要係以會員經濟體之經濟利益為出發點，因此有認為 APEC 隱私保護綱領是目前世界組織對於個人資料保護規範中，規範強度稍低之公約；另外，亦有相關批評認為 APEC 缺乏程序性規定，將造成當事人無管道去主張個人資料保護之權利[30]。

APEC 隱私保護綱領主要包括預防損害原則(the Preventing Harm Principle)、告知原則（the Notice Principle）、蒐集限制原則（the Collection Limitation）、個人資料利用原則(Uses of Personal Information Principle)、當事人自主原則（the Choice Principle）、個人資料完整性原則（the Integrity of Personal Information Principle）、安全管理原則（Security Safeguard Principle）、查閱及更正原則（Access and Correction Principle）、責任原則(Accountability Principle)[31]。惟 APEC

[29] Stuart Hargreaves, Inadequate: The APEC Privacy Framework& Article25 of the European Data Protection Directive, 8 CANJLT1, 11（2010）.
[30] Stuart Hargreaves, Inadequate: The APEC Privacy Framework& Article25 of the European Data Protection Directive, 8 CANJLT1, 27（2010）.
[31] 參照 APEC 網站，http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx，最後瀏覽日 2011 年 10 月 17 日。

本報告之智慧財產權歸屬於法務部

隱私權保護綱領並未提及特定司法救濟管道或者相關裁罰之規定，僅提及一般性的損害賠償概念。以下將介紹 APEC 隱私保護綱領之內容：

（1）預防損害原則（the Preventing Harm Principle）

基於個人隱私的合理期待，個人資訊隱私保護制度應著重於防止個人資訊遭到濫用。另外，必須採取適當之保護措施以防止此種損害之產生，而對於當事人因其個人資料遭到不當蒐集、利用和傳遞而產生損害時，應提供當事人法律救濟途徑以填補損害。

（2）告知（the Notice Principle）

個人資料管理者對於其所蒐集與持有之個人資料應向當事人提供清楚且容易取得之隱私保護政策聲明。該聲明包含以下內容：個人資料已遭蒐集的事實聲明；蒐集個人資料之目的；揭露個人資料之對象；個人資料管理者的身分以及聯絡地址；關於當事人得以請求查閱、更正；限制其個人資料之利用及揭露範圍的選擇和方法。

資料管理者應採取合理的措施以確保當事人於其個人資料蒐集前或蒐集時已知悉其隱私保護政策。除此之外，一旦資料管理者之隱私保護政策開始實行時，必須立即告知當事人此保護政策。

當資料管理者所蒐集或利用之個人資料為公開可獲得之個人資料時，不適用本原則。

（3）蒐集限制（the Collection Limitation）

個人資料之蒐集應限於與蒐集目的相關的範圍，依合法或正當方法為之，並在適切的情況下告知當事人並取其同意。個人資料之蒐集應與蒐集目的具有關聯性。但於某些情形下，並無法告知當事人或取得同意時，得不告知當事人或取得其同意。

本報告之智慧財產權歸屬於法務部

（4）個人資料之利用（Uses of Personal Information Principle）

個人資料之利用僅限於與蒐集目的一致或相關範圍內。除非取得當事人同意、為提供當事人所要求之產品或服務所要求者或經法律明文規定者。

（5）當事人自主（the Choice Principle）

於合適之情形下，個資管理者應提供當事人對於其個人資料之蒐集、利用或揭露方式選擇機制。但若資料管理者所蒐集之個人資料係公開可獲得之資料時，不適用於本規定。

（6）個人資料之完整性（the Integrity of Personal Information Principle）

個人資料之內容應保持精確、完整，並依利用目的於必要之限度內保持更新狀態。

（7）安全管理（Security Safeguard　Principle）

資料管理者必須採取安全防護措施以保護當事人之個人資料，以防止滅失、未經授權而截取、利用、修改或揭露個人資料。安全防護措施必須依循可能發生之風險加以決定其防護措施。另外，敏感性資料必須定期檢視並且重新評估。

（8）查閱及更正（Access and Correction Principle）

當事人應可從資料管理者確認是否資料管理者持有其資料的資訊；於當事人提供資料管理者可供識別之身分後，資料管理者需於合理期間、合理費用（若需收費，費用不得過高）、合理方式並且以當事人可理解之方式提供相關資訊予當事人。於合適之情形下可請求修正、補充或者刪除其個人資料。

資料管理者應提供當事人查閱以及更正其個人資料之機會，除非提供個人查閱其個人資料之成本過高，或與個人隱私受

本報告之智慧財產權歸屬於法務部

侵害之風險不成比例時，可拒絕當事人查閱之申請。

若當事人提出以上查閱、更正之申請遭資料管理者拒絕時，資料管理者必須說明其理由。

（9）責任（Accountability Principle）

資料管理者應負責採取措施，以符合以上原則。傳輸個人資料予第三人時（無論本國或跨境），資料管理者必須獲得當事人之同意，或者資料管理者須採取合理步驟確認第三人將採取與隱私保護綱領原則一致之措施保護個人資料。

7.訂定我國個人資料保護基本原則之建議

由於科技發展快速，蒐集處理個人資料之速度相較於過去更加簡便以及快速，因此對於個人資料保護法制具有強烈之迫切性。以國際之發展為例，目前世界上超過六十的國家皆訂有個人資料保護法制，而各國際組織亦定有個人資料保護指令或者協議以供各會員國參考。雖然對於個人資料保護的概念不盡相同，但所採取的原則仍存有許多共通點，各國法以及國際組織皆對於蒐集、使用以及揭露個人資料之行為要求其正當性、合法性以及合目的性，另外亦要求蒐集、處理及管理資料之資料管理人必須提供清楚之管道供當事人查詢相關個人資料使用之狀況，並且賦予當事人可修改、更正或刪除其個人資料之權利，除此之外，各國間對於敏感性資料之保護亦有共識。基於以上所述之原則，可對於個人資料之保護描繪出較為清楚之輪廓，希冀繼環保、經濟議題後，個人資料保護可獲得全球性的共識。

基於幾項個人資料保護基本原則，各國分別訂定其國內之個人資料法制，而我國於前年五月（民國 99 年 05 月）所通過個人資料保護法中，亦可見國際個人資料保護原則之蹤影。然而，目前缺乏完整之個人資料保護原則，以宣示政府對於個人資料保護之中心思想與概念，故訂立個人資料保護原則實有必要。另外，除了個人資料保護法外，金融控股公司法第 42 條[32]、銀行法第 48 條第二項[33]、電信法第 6

[32] 金融控股公司法第 42 條第一項，金融控股公司以及其子公司對於客戶個人資料、往來交易資料及其他相關資料，除了法律或主管機關另有規定者外，應保守秘密。

本報告之智慧財產權歸屬於法務部

條[34]、稅捐稽徵法第 33 條[35]，亦定有因相關業務所蒐集之個人資料之保密義務，只是上述法律僅說明保密義務，並未對於相關個人資料之保護措施做進一步之規定，故對於個人資料之相關規範仍須以個人資料保護法為依歸。

觀察我國目前通過之個資法後，發現個資法中包含蒐集限制原則[36]、利用限制原則[37]、資料品質原則[38]、敏感性資料處理原則[39]、告知原則[40]、個人參與原則[41]、安全管理原則[42]、國際傳輸原則[43]以及責任原則等[44]。經整理我國目前個資法之內容，並且參考國際組織以及外國之立法例後，以下試提出我國之個人資料保護原則。

表 1：我國個人資料保護原則建議

原則	說明
蒐集限制原則：公務機關以及非公務機關於蒐集個人資料時，必須依循合法以及正當方法為之。並於符合特定目的之情形下，蒐集個人資料。	澳洲之國家隱私原則、資訊隱私保護原則、OECD 隱私保護與個人資料跨境流通指導原則、歐盟個人資料保護指令、英國個人資料保護法、APEC 隱私保護指令皆訂有蒐集限制原則。蒐集原則之內容主要為，必須依循正當且合理之手段蒐集個人資料，並且必須依循其蒐集資料之特定目的處理個人資料。
資料品質原則：公務以及非公務機關蒐集、處理或使用個人資料時，必須確保個人資料之完整性、正確性。	澳洲之國家隱私原則、資訊隱私保護原則、OECD 隱私保護與個人資料跨境流通指導原則、歐盟個人資料保護指令、

[33] 銀行法第 48 條第二項，銀行對於客戶之存款、放款或匯款等有關資料，應保守秘密。
[34] 電信法第 6 條，電信業以及專用電信處理之通信，他人不得盜接、盜錄或以其他非法之方法侵犯其秘密。
[35] 稅捐稽徵法第 33 條，對於納稅義務人之財產所得、營業或納稅等資料，除了法定人員或機關外，應絕對保守秘密。
[36] 個資法第 6、15、19 條
[37] 個資法第第 5、16、20 條
[38] 個資法第 11 條第 1 項
[39] 個資法第 6 條
[40] 個資法第 7 條、第 8 條、第 9 條、
[41] 個資法第 11 條第 2、3 項
[42] 個資法第 12 條、第 18 條、第 27 條
[43] 個資法第 21 條
[44] 當事人受侵害時，賦予救濟管道。個資法第 28、29 條。

本報告之智慧財產權歸屬於法務部

原則	說明
	英國個人資料保護法、APEC 隱私保護指令皆訂有資料品質原則。由於個人資料之使用以及揭露將影響當事人之利益，故必須確保當事人之個人資料屬正確無誤者。根據我國個人資料保護法第11 條，公務機關以及非公務機關必須確保當事人之個人資料係屬於完整並且正確之狀態，事實上，國外立法例另要求資料管理必須確保當事人之個人資料屬於最新狀態（up-to-date），此為我國個人資料保護法中未規定之要件，可再予參酌。
敏感性資料處理原則：公務機關以及非公務機關原則上不得蒐集有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，除非符合個人資料保護法所訂之相關例外情況。	澳洲國家隱私原則、歐盟個人資料保護指令、英國個人資料保護法、APEC 隱私保護綱領皆清楚對於敏感性（又稱特種個人資料）個人資料訂有原則性之規範。由於各國之國情不同，故對於需要特別予以保護之敏感性個人資料有不同之種類，基本上只要該類個人資料屬於極其敏感、足使當事人之人格受貶抑、個資外洩可能遭歧視或差別待遇時，該類個人資料即須列入敏感性格人資料範圍內，一旦該類資料列入敏感性個人資料之範圍後，原則上，禁止蒐集、處理以及利用該類個人資料，唯有符合嚴格之法定要件時，始得為之。除了我國所列出之種類外，有些立法例亦列入個人徵信資料（銀行信用）以及工作表現等種類為其敏感性個人資料之類型。
告知原則：公務機關以及非公務機關於蒐集、處理或利用當事人之個人資料時	澳洲之國家隱私原則、資訊隱私保護原則、OECD 隱私保護與個人資料跨境流

本報告之智慧財產權歸屬於法務部

原則	說明
必須向當事人說明機關之身分、蒐集之目的、個人資料之類別、個人資料利用之相關資訊、當事人可行使之權利。	通指導原則、歐盟個人資料保護指令、英國個人資料保護法、APEC 隱私保護指令皆訂有告知原則。告知原則對於個人資料保護係屬於必要之原則，透過告知當事人之程序，使當事人掌握並了解其個人資料被使用之情形，也得以確立當事人自我決定權之地位。
利用限制原則：利用當事人之個人資料時，必須與蒐集之目的具有正當合理之關聯時。除非符合法律明文或獲得當事人同意等例外情形時，始得為特定目的外之利用。	澳洲之國家隱私原則、資訊隱私保護原則、OECD 隱私保護與個人資料跨境流通指導原則、歐盟個人資料保護指令、英國個人資料保護法、APEC 隱私保護指令也訂有利用限制原則。透過利用限制原則之確立，明確規範公務機關以及非公務機關於利用個人資料時，必須符合蒐集目的，此為利用個人資料正當合理手段之要求，以確保個人資料不會遭到資料管理者之濫用，而造成當事人之損害。
個人參與原則：當事人有查閱、更正其個人資料之權利。另外，當事人可主動要求公務機關以及非公務機關刪除、停止處理或利用該個人資料。	澳洲之國家隱私原則、資訊隱私保護原則、OECD 隱私保護與個人資料跨境流通指導原則、歐盟個人資料保護指令、英國個人資料保護法、APEC 隱私保護指令皆賦予當事人查閱、更正以及行使權利之管道，落實當事人自主控制其個人資訊之概念。
安全管理原則：公務機關以及非公務機關必須採取適當之安全措施、設立相關組織，以防止當事人之個人資料被竊取、竄改、毀損、滅失或洩漏。而公務機關與非公務機關若違反本規定而導致個人資料被竊取、洩漏、竄改或其他侵害時，查明後應通知當事人，以減低	澳洲之國家隱私原則、資訊隱私保護原則、OECD 隱私保護與個人資料跨境流通指導原則、歐盟個人資料保護指令、英國個人資料保護法、APEC 隱私保護指令要求資料管理者必須採取適當的個人資料安全維護措施或成立個人資料管理組織管控其所擁有之資料，以確

本報告之智慧財產權歸屬於法務部

原則	說明
損害之程度。	保個人資料之安全。資料管理者必須依循可能發生之風險加以決定其防護措施，除此之外，敏感性資料必須定期檢視及評估。
國際傳輸原則：非公務機關跨境傳輸個人資料時，必須受到中央目的事業主管機關之限制。	各國以及各國際組織對於跨境傳輸之規定並未達成一致的共識，例如歐盟採取了較為嚴格之要件規定，此規範模式使得個人資料跨境傳輸較為不易，而觀諸我國之個人資料保護法，並未採取如同歐盟個人資料保護指令之嚴格規定，僅交由中央目的事業主管機關限制之。事實上，採取寬鬆或者嚴格的立法方式皆有利弊，若採取寬鬆的跨境傳輸規定，將可以使個人資料跨境傳輸更簡便、成本更低，但卻提高了個人資料可能遭受不當利用之風險。相對的，若採取嚴格之跨境傳輸規定，雖然對於當事人之個人資料提供更妥善之保護，但卻大大的增加了資料傳輸者以及資料接受者之成本，反而造成了個人資料跨境傳輸之阻礙。
責任原則：資料管理者應採取適當之措施，以符合以上之原則。	OECD 隱私保護與個人資料跨境流通指導原則、歐盟個人資料保護指令以及 APEC 隱私保護指令皆訂有責任原則。觀諸我國目前之個人資料保護法制並沒有責任原則之規定，僅賦予當事人於權利受侵害時之司法救濟途徑，可再予參酌。

資料來源：本計畫自行整理

本報告之智慧財產權歸屬於法務部

（三）非公務機關個人資料安全維護計畫標準辦法草案範本

依據個人資料保護法第 27 條第 1 項規定，非公務機關應定有適當之安全維護措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏，而某些行業如銀行業、電信業、醫院、保險業等，因其所保有之個人資料檔案數量龐大且敏感性較高，牽涉個人隱私權或經濟上利益亦較為密切，因此該等行業所負之安全保管責任應較一般行業為重。故本法第 27 條第 2 項授權中央目的事業主管機關得指定特定之非公務機關，要求其訂定個人資料檔案安全維護計畫以加強管理，確保個人資料之安全維護。且依本法第 27 條第 3 項，各中央目的事業主管機關應訂定安全維護計畫標準之辦法，使非公務機關於訂定安全維護計畫時有所依循。法務部本於法令主管機關之職責，爰參酌國際組織規範以及相關國家之法制、指引或作業程序，訂定非公務機關個人資料檔案安全維護計畫標準辦法之範本，供各中央目的事業主管機關參考，以便各中央目的事業主管機關得再依據其主管行業之特性，訂定各行業之安全維護計畫標準辦法。

非公務機關保有個人資料檔案時，應建立內部之個人資料管理組織，及蒐集、處理及利用時之相關安全管理程序，以下將分別闡述辦法範本草案逐條條文之要旨。

1.本辦法之法源依據

本辦法範本第一條即明示，未來所訂定之安全維護計畫標準之辦法，均依據個人資料保護法第二十七條第三項規定訂定。

2.本辦法之主要意旨

本辦法範本第二條規定：「非公務機關為落實個人資料檔案之安全維護與管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏，經中央目的事業主管機關指定後，應訂定個人資料檔案安全維護計畫（以下簡稱計畫）。

本辦法第四條至第二十九條所規定之相關組織及程序要求，應訂

本報告之智慧財產權歸屬於法務部

定於計畫內。」非公務機關為落實個人資料檔案之安全維護，經中央目的事業主管機關指定後，應訂定相關安全維護計畫，以建立並執行相關管理程序或制度，本條第一項明示此旨。計畫標準辦法內所規定之相關組織及程序要求，受指定之非公務機關應訂定於安全計畫內，本條第二項明示此旨。

3.本辦法用詞定義

本辦法範本第三條規定：「本辦法用詞定義如下：一、個人資料管理代表：非公務機關之負責人或負責人直接授權，擔任督導計畫之規劃、訂定、執行、修訂及相關決策之人員。二、個人資料內評代表：由非公務機關之負責人授權，負責督導相關內評人員評核計畫之執行成效之人員。三、所屬人員：執行業務之過程必須接觸個人資料之人員，包括公司之定期或不定期契約人員及派遣員工。

本辦法所未定義之名詞，以本法第二條為準。」此條特別針對本辦法中所設計，維運本計畫所需要之相關人員加以定義，包括個人資料管理代表、個人資料內評代表以及所屬人員。

欲有效達成管理組織之運作，組織內必須有一角色擔任督導計畫之規劃、訂定、執行、修訂及相關決策，並擔任負責人與管理組織間橋樑之工作，個人資料管理代表即為計畫中賦予此一任務之角色。

非公務機關為確保計畫之落實，應有相關人員負責於非公務機關內部評核計畫落實之狀況，而個人資料內評代表則負責統整相關評核之結果。

為確保個人資料檔案之安全維護，凡執行業務之過程必須接觸個人資料之人員，包括公司之定期或不定期契約人員及派遣員工，均應為遵守計畫之相關程序並執行之。此外，本條針對本辦法相關名詞加以定義，所未定義之名詞，則以個人資料保護法第二條為準。

4.管理組織之建立及配置相當資源

本辦法範本第四條規定：「非公務機關為訂定並執行計畫，應建立個人資料檔案安全維護管理組織，並配置相當資源。

本報告之智慧財產權歸屬於法務部

前項管理組織之任務如下：一、規劃、訂定、執行與修訂安全維護計畫相關程序。二、管理代表應定期向事業之負責人就前款事項提出書面報告。

第一項之管理組織至少應包括個人資料管理代表與個人資料內評代表。」非公務機關欲有效訂定與執行安全維護計畫，應建立相當組織與投注相當資源。該管理組織應其任務即為安全維護計畫相關程序之規劃、訂定、執行與修訂，且為使非公務機關之負責人能盡其督導及監督之責，管理代表應定期向事業之負責人以書面報告相關事項。而為有效督導並評核安全維護計畫執行之成效，除個人資料管理代表外，管理組織亦應有監督或評核計畫是否落實執行之個人資料內評代表。

5.個人資料管理政策之擬定

本辦法範本第五條規定：「非公務機關應依其組織與事業特性訂定個人資料保護管理政策，經非公務機關之負責人核可，並公開周知，使其所屬人員均明確瞭解。

前項政策至少應包括下列事項之說明：一、遵守我國個人資料保護相關之法令規定。二、以合理安全之方式，於特定目的範圍內，蒐集、處理及利用個人資料。三、以可期待之合理安全水準技術保護其所蒐集、處理、利用之個人資料檔案。四、設置聯絡窗口，供當事人行使關於個人資料之權利或提出相關之申訴與諮詢。五、規劃緊急應變程序以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。六、如有委託蒐集、處理及利用個人資料時，妥善監督受託機關。七、持續維運計畫，以確保個人資料檔案之安全。」為使非公務機關全體人員對於個人資料之保護能有所體認，進而能落實計畫，故非公務機關應訂定個人資料保護管理政策，將計畫相關重點事項於政策內闡明。且為達上述目的，該等政策應加以公開周知，且由非公務機關之負責人核可，以明示保護個人資料之旨。而關於保護個人資料檔案權所應注意之重點事項即包括：遵守我國個人資料保護相關之法令規定、合法正當蒐集、處理及利用個人資料；應以適當之技術保護個人資料；應提供當事人行使權利之方式；規劃緊急應變程序以處理事故；監督

本報告之智慧財產權歸屬於法務部

受託機關之責任；持續維運計畫之義務。

6.個人資料保護相關法令之檢視

本辦法範本第六條規定：「非公務機關應定期檢視非公務機關所應遵循之個人資料保護相關法令，並依據法令訂定或修訂計畫。」非公務機關因其種類、特性及其所蒐集、處理、利用之個人資料範圍之不同與變動，其所應適用之個人資料保護法令亦可能有所不同，事業為符合法令之規定，自應依據上述事業自身狀況清查適用之個人資料保護相關法令。而個人資料保護相關法令規定，因時事變遷而有隨之變更之可能，非公務機關自應定期檢視，以持續修訂其安全維護計畫。

7.清查個人資料並建立清冊

本辦法範本第七條規定：「非公務機關應依據個人資料保護相關法令，清查非公務機關所保有之個人資料，界定其納入計畫之範圍並建立清冊，且定期確認其是否有所變動。」個人資料保護法施行細則第九條第一項第二款規定，安全維護計畫中應就界定個人資料範圍相關事項加以規定，本條即進一步闡明該規定之意旨。非公務機關需先掌握於其內部之個人資料之種類與數量，方能有效對其所保有之個人資料加以控管。

8.個人資料業務流程之風險分析及管控措施

本辦法範本第八條規定：「非公務機關應根據前條所界定之個人資料，及其相關業務流程，分析可能產生之風險，並根據風險分析之結果，訂定適當之管控措施。」個人資料保護法施行細則第九條第一項第三款規定，安全維護計畫應就個人資料之風險評估及風險管理加以規定，本條即在進一步闡明該規定之意旨。非公務機關應依據其相關業務流程，判斷於蒐集、處理及利用之過程中，個人資料可能發生之危險，以及其危險性之高低，方能進一步以適當之方式保護個人資料並降低其風險。

9.事故之應變、通知及預防程序

本報告之智慧財產權歸屬於法務部

本辦法範本第九條規定：「非公務機關為因應所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，應就下列事項建立相關程序：一、採取適當之應變措施，以控制事故對當事人之損害。二、查明事故之狀況並適時通知當事人。三、避免類似事故再次發生。」當個人資料被竊取、竄改、毀損、滅失或洩漏等事故發生時，常造成資料當事人財產及非財產上之損害，非公務機關為降低或控制損害之範圍，應訂定相關之因應機制，本條即明示此旨。事故應變之首要目標即根據事故之類型，採取應變措施以降低或控制損害之範圍。其次，應讓當事人瞭解相關狀況，使當事人亦能採取相關措施防止損害發生或擴大。最後，避免類似事故再次發生亦為應變措施之重點。

10.委託蒐集、處理及利用個人資料之監督程序

本辦法範本第十條規定：「非公務機關委託他人蒐集、處理或利用個人資料之全部或一部時，為對受託人為適當之監督，應就下列事項建立相關程序：一、確認所委託蒐集、處理或利用之個人資料之範圍、類別、特定目的及其期間。二、確認受託人應採取必要安全措施。三、有複委託者，確認其複委託之對象。四、受託人或其受僱人違反個人資料保護法令或委託契約條款時，要求其向委託人通知相關事項。五、與受託人約定委託人所保留指示之事項。六、委託關係終止或解除時，要求受託人返還或銷毀因委託事項所交付之個人資料載體，及刪除因委託事項所儲存於受託人之個人資料。七、確認受託人執行上述要求事項之狀況。」非公務機關如將個人資料之蒐集、處理或利用委託他人為之，仍應對受託人為適當之監督，以使資料之蒐集、處理或利用仍符合事業安全維護計畫之要求；本條即規定非公務機關應就此建立一定之程序。

11.個人資料蒐集應注意之事項及告知義務之履行

本辦法範本第十一條規定：「非公務機關為確保個人資料之蒐集符合個人資料保護相關法令要求，應就下列事項建立相關程序：一、確認蒐集個人資料之特定目的。二、確認具備法令所要求之特定情形或其他要件。」依本法第十九條第一項規定，蒐集個人資料應有特定目的並具備一定之法定情形，而若其他法令有特別要求，亦應遵守

本報告之智慧財產權歸屬於法務部

之，故應建立相關程序以確認之。

本辦法範本第十二條規定：「非公務機關為遵守本法第八條及第九條關於告知義務之規定，應就下列事項建立相關程序：一、確認是否得免告知。二、依據資料蒐集之情況，採取適當之告知方式。」依個人資料保護法第八條及第九條規定，非公務機關應適時履行告知義務，故除確認有例外情況無須告知外，均應依據資料蒐集之情況，採取適當之告知方式，以有效履行告知義務。

12.確保於特定目的內利用個人資料及特定目的變更之程序

本辦法範本第十三條規定：「非公務機關為確保個人資料之利用符合個人資料保護相關法令要求，應就下列事項建立相關程序：一、確保資料之利用符合特定目的。二、確認是否得進行及如何進行特定目的外利用。」依個人資料保護法第二十條第一項規定，個人資料應於蒐集之特定目的必要範圍內利用，但於特定情形下，得為目的外之利用。因此應建立一定程序，以確保資料之利用符合特定目的。若有必要為特定目的外利用時，亦應確認其是否合法，及特定目的外利用之相關情事。

本辦法範本第十四條規定：「非公務機關如欲新增或變更特定目的時，應依下列程序為之：一、依本辦法第十二條之程序為之。二、取得當事人書面同意，但法令別有規定者，不在此限。」於前條規定非公務機關於特定情形下，得將所保有之個人資料為特定目的外之利用，惟該條規定乃針對個別情況下得否及如何為特定目的外之利用。若非公務機關若欲繼續性地對於其所保有之個人資料進行特定目的之新增或變更時，應先依相關告知義務之程序為之。其次，除法令別有規定外，原則上應取得當事人之書面同意，方能為特定目的之新增或變更。

13.利用個人資料行銷之程序

本辦法範本第十五條規定：「非公務機關於利用個人資料行銷時，應就下列事項建立相關程序：一、確保當事人表示拒絕接受後，立即停止利用其個人資料行銷。二、確保首次行銷時，當事人表示拒

本報告之智慧財產權歸屬於法務部

絕接受行銷無須支付任何費用。」依個人資料保護法第二十條第二項及第三項規定，當事人有拒絕行銷之權利，因此應建立程序以確保當事人表示拒絕接受後，立即停止利用其個人資料行銷。其次，於首次行銷時，並應提供當事人表示拒絕接受行銷之方式，並支付相關費用，以符合本法要求第二十條第三項之要求。

14.蒐集、處理及利用特種個人資料之程序

本辦法範本第十六條規定：「非公務機關針對本法第六條之特種個人資料，應就下列事項建立相關程序：一、確認所蒐集、處理及利用之個人資料是否包含特種個人資料。二、確保蒐集、處理及利用特種個人資料，符合相關法令之要求。」依個人資料保護法第六條規定，非公務機關原則上不得蒐集、處理及利用醫療、基因、性生活、健康檢查及犯罪前科之個人資料，故非公務機關應先建立程序以確認是否有蒐集相關特種個人資料。如有蒐集時，並應確保蒐集、處理及利用特種個人資料，符合相關法令之要求。

15.因應限制國際傳輸個人資料之程序

本辦法範本第十七條規定：「非公務機關進行個人資料國際傳輸前，應確認是否受中央目的事業主管機關限制並遵循之。」依個人資料保護法第二十一條規定，中央目的事業主管機關得於一定情形下，限制非公務機關對於個人資料進行國際傳輸，因此非公務機關應建立程序以確認主管機關是否有所限制並加以遵守之。

16.提供當事人行使權利之程序

本辦法範本第十八條規定：「非公務機關為提供資料當事人行使個人資料保護法第三條所規定之權利，應就下列事項建立相關程序：一、如何提供當事人行使權利。二、確認當事人身分。三、確認是否有本法第十條及第十一條得拒絕當事人行使權利之情況。四、適時回覆當事人請求。」依個人資料保護法第三條規定，當事人就其個人資料得行使包含查詢或請求閱覽等五項權利，且依據個人資料保護法第十條及第十一條，非公務機關除有法所規定之正當理由外，應於一定

本報告之智慧財產權歸屬於法務部

期間內回覆當事人之請求，本條即規定非公務機關應建立相關程序以供資料當事人行使權利。

為使當事人得有效行使其權利，提供一定方式，如常設之聯絡窗口，包含聯絡電話或聯絡之電子郵件信箱等，即為首要之程序。其次，避免資料不當提供給第三人或不當刪除，故非公務機關於提供當使人行使權利前，應先建立程序以確認當事人身分。最後，個人資料保護法第十條及第十一條規定於一定情形下非公務機關得拒絕當事人行使權利，故應有程序確認是否符合該等拒絕之情況，如並無該等情況，則應於本法所規定之時限內，適時回覆當事人之請求。

17.確認個人資料正確性之程序

本辦法範本第十九條規定：「非公務機關為確認其所保有個人資料之正確性，應就下列事項建立相關程序：一、確保資料於處理過程中，正確性不受影響。二、當確認資料有錯誤時，應適時更正。三、定期檢查資料之正確性。

因可歸責於非公務機關之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象之程序。」非公務機關所保有之個人資料之正確性，攸關非公務機關是否能有效利用當事人之個人資料以提供當事人相關服務，並避免當事人發生因資料不正確所產生之損害。因此非公務機關應建立程序，確保資料於處理過程中不會發生錯誤，若資料仍有錯誤之情況，應適時更正，且應定期檢查資料之正確性。若非公務機關曾提供所保有之個人資料予他人，且因可歸責於非公務機關之事由，未更正或補充致使個人資料不正確時，自應課以該蒐集機關於更正或補充個人資料後，通知曾提供利用該資料之對象，以使該不正確之資料能即時更新，避免當事人權益受損，爰參酌個人資料保護法第十一條第五項，訂定第二項。

18.保有個人資料之特定目的消失或期限屆滿時之程序

本辦法範本第二十條規定：「非公務機關應定期確認其所保有個人資料之特定目的是否消失，或期限是否屆滿，若特定目的消失或期限屆滿時，應遵守本法第十一條第三項規定。」非公務機關蒐集、處

本報告之智慧財產權歸屬於法務部

理或利用個人資料均應於特定目的必要範圍內為之，若蒐集、處理、利用個人資料之特定目的已消失或期限已屆滿，則應遵守個人資料保護法第十一條第三項之規定，加以刪除或停止處理利用。

19.安全管理措施之要旨

本辦法範本第二十一條規定：「為防止個人資料發生被竊取、竄改、毀損、滅失或洩漏等遭受侵害之情事，非公務機關應依據業務性質、個人資料存取環境、個人資料種類與數量及個人資料傳輸工具與方法等因素，採取第二十二條至第二十五條之管理措施。」對於個人資料之保護，除於組織面給予整體規劃，及法令遵循程序之設計外，尚應考慮安全管理措施之部分，而如何規劃安全管理措施，則應綜合考量非公務機關之業務性質、個人資料存取環境、個人資料種類與數量及個人資料傳輸工具與方法等因素。安全管理措施可分為人員管理、作業管理、物理環境管理、技術管理之不同要求，本辦法第二十三條至第二十六條將分別針對上述要求加以規定。

20.人員管理措施之事項

本辦法範本第二十二條規定：「非公務機關應採取下列人員管理措施：一、確認蒐集、處理及利用個人資料之各相關業務流程之負責人員。二、依據作業之必要，設定所屬人員不同之權限並控管之，以一定認證機制管理其權限，且定期確認權限內容設定之適當與必要性。三、要求所屬人員負擔相關之保密義務。」針對人員管理之部分，首先應先確認實際進行個人資料之蒐集、處理及利用之負責人員為何，方可確認相關管理程序之權責歸屬。非公務機關所屬人員與個人資料相關之各項作業，若有設定權限控管之必要，則應以一定認證機制管理之，並確認其權限設定是否適當或必要。避免人員取得不適當之權限，得以接觸非於作業必要範圍內之個人資料。而非公務機關與其所屬人員應要求所屬人員負擔相關之保密義務，使所屬人員能明瞭其責任，必要時亦可以訂定契約條款之方式為之，以作為相關權責之紀錄。

21.作業管理措施之事項

本報告之智慧財產權歸屬於法務部

本辦法範本第二十三條規定：「非公務機關應採取下列作業管理措施：一、訂定蒐集、處理及利用之作業注意事項。二、運用電腦及相關設備處理個人資料時，應訂定使用可攜式儲存媒體之規範。三、針對所保有之個人資料內容，確認是否有加密之必要，如有必要，應採取適當之加密機制。四、傳輸個人資料時，因應不同之傳輸方式，確認是否有加密之必要，如有必要，應採取適當之加密機制，並確認資料收受者之正確性。五、非公務機關應依據所保有資料之重要性，評估個人資料是否有備份必要，如有必要應予備份。對於備份資料應確認是否有加密之必要，如有必要，採取適當之加密機制，儲存備份資料之媒體亦應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。六、儲存個人資料之媒體於廢棄或移轉與他人前，應確實刪除媒體中所儲存之資料，或以物理方式破壞之。七、妥善保存認證機制及加密機制中所運用之密碼，如有交付他人之必要，亦應妥善為之。」針對個人資料蒐集、處理及利用的個別相關作業，非公務機關應基於計畫之原則規定，訂定具體之作業注意事項，使所屬人員有所依循。使用可攜式儲存媒體，可能提高處理個人資料之電腦及相關設備遭受惡意程式攻擊及個人資料外洩之風險，因此若有使用可攜式儲存媒體之情況，應定相關使用規範。針對個人資料處理之不同態樣，包括儲存、傳輸及備份之狀況，如資料有加密之必要，即應採取適當之加密機制。於傳輸個人資料之情況，除有必要時採取加密機制，並應確認資料收受者之正確性，以避免資料不當外洩。針對有備份必要之個人資料，除有必要時採取加密機制，儲存備份資料之媒體亦應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。儲存個人資料之媒體於廢棄或移轉與他人前，應確實刪除媒體中所儲存之資料，或以物理方式破壞之，以避免資料不當外洩。如作業程序中相關認證機制與加密機制有運用密碼之必要時，該密碼亦應妥善加以保存。

22.物理環境管理措施之事項

本辦法範本第二十四條規定：「非公務機關應採取下列物理環境管理措施一、依據作業內容之不同，實施必要之門禁管理。二、妥善保管個人資料之儲存媒體。三、針對不同作業環境，建置必要之防災

本報告之智慧財產權歸屬於法務部

設備。」在實體之物理環境管理方面，非公務機關亦應針對不同之作業內容、作業環境及個人資料之種類與數量，實施必要之門禁管理，以適當方式或場所保管個人資料之儲存媒體，並建置必要之防災設備。

23.技術管理措施之事項

本辦法範本第二十五條規定：「非公務機關利用電腦或相關設備蒐集、處理或利用個人資料時，應採取下列技術管理措施：一、於電腦、相關設備或系統上設定認證機制，對有存取個人資料權限之人員進行識別與控管。二、認證機制使用帳號及密碼之方式時，使其具備一定安全之複雜度並定期更換密碼。三、於電腦、相關設備或系統上設定警示與相關反應機制，以對不正常之存取為適當之反應與處理。四、對於存取個人資料之終端機進行身分認證，以識別並控管之。五、個人資料存取權限之數量及範圍，於作業必要之限度內設定之，且原則上不得共用存取權限。六、採用防火牆或路由器等設定，避免儲存個人資料之系統遭受無權限之存取。七、欲使用能存取個人資料之應用程式時，確認使用者具備使用權限。八、定期測試權限認證機制之有效性。九、定期檢視個人資料之存取權限設定正當與否。十、於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼。十一、對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。十二、定期瞭解惡意程式之威脅，並確認安裝防毒軟體及修補程式後之電腦系統之穩定性。十三、具備存取權限之終端機不得安裝檔案分享軟體。十四、測試處理個人資料之資訊系統時，不使用真實之個人資料，如有使用真實之個人資料之情形時，明確規定其使用之程序。十五、處理個人資料之資訊系統如有變更時，確認其安全性並未降低。十六、定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形。」非公務機關若利用電腦或相關設備蒐集、處理或利用個人資料時，針對相關電腦系統技術，亦應有相應之管理措施，本條即臚列相關技術管理措施，供非公務機關視其實際作業之必要予以實施。

本條所臚列之技術管理措施約可分為：

（1）系統存取權限之設定及實施：以認證機制，對有存取個人資料

本報告之智慧財產權歸屬於法務部

權限之人員進行識別與控管，若認證機制使用密碼之方式時，並應有適當之管理方式，並定期測試權限機制之有效性（第一款至第四款、第八款）。

（2）系統存取權限之控管：系統存取權限之設定應於必要範圍內為之，避免非作業必要之人員得存取相關資料，增加個人資料不當外洩之風險。且應定期檢視存取權限之必要性及是否需要調整（第五款、第九款）。

（3）採用防火牆或路由器等設定，避免儲存個人資料之系統遭受無權限之存取（第六款）。

（4）存取個人資料之應用程式之控管（第七款）。

（5）避免惡意程式與系統漏洞對作業系統之威脅（第十款至第十二款）。

（6）檔案分享軟體之控制（第十三款）。

（7）系統測試時，使用個人資料之程序（第十四款）。

（8）資訊系統變更時，其安全性之確認（第十五款）。

（9）系統之使用狀況與個人資料存取之情形（第十六款）。

24.認知宣導及教育訓練

本辦法範本第二十六條規定：「非公務機關應對於所屬人員施以認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業程序。」若欲使計畫相關管理程序能落實執行，應使非公務機關之所屬人員均能明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業程序，故應透過認知宣導及教育訓練為之。

25.計畫稽核及改善程序

本辦法範本第二十七條規定：「非公務機關為確保計畫之有效性，應定期檢查計畫是否落實執行。」計畫以及非公務機關依據計畫

本報告之智慧財產權歸屬於法務部

所訂定之相關程序，非公務機關所屬人員是否皆已落實執行，必須通過一定之檢查機制方能確定。

本辦法範本第二十八條規定：「為持續改善計畫，非公務機關應建立下列程序：一、計畫發生未落實執行時之改善程序。二、如計畫有變更之需要時，其變更之程序。」於前條檢查過程中，若發現有未落實執行之情況，非公務機關應建立程序，協助相關所屬人員加以改善。若計畫有窒礙難行或因應法令之增修，而有變更之需要時，亦應有變更之相關程序。

26.紀錄機制

本辦法範本第二十九條規定：「關於計畫各項程序之執行，非公務機關至少應保存下列紀錄：一、因應事故發生所採取行為之紀錄。二、確認受託人執行委託人要求事項之紀錄。三、提供當事人行使權利之紀錄。四、確認資料正確性及更正之紀錄。五、權限新增、變動及刪除之紀錄。六、違反權限行為之紀錄。七、備份及還原測試之紀錄。八、個人資料交付、傳輸之紀錄。九、個人資料刪除、廢棄之紀錄。十、存取個人資料系統之紀錄。十一、定期檢查處理個人資料之資訊系統之紀錄。十二、教育訓練之紀錄。十三、計畫稽核及改善程序執行之紀錄。」為確認計畫以及非公務機關依據計畫所訂定之相關程序是否落實執行，以及釐清個人資料於蒐集、處理及利用過程之相關權責，非公務機關應保存相關紀錄以供查驗。

表 2：非公務機關個人資料檔案安全維護計畫標準辦法草案

條文	說明
第一章、總則	**第一章章名**
第一條　本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。	本辦法之法源依據。
第二條　非公務機關為落實個人資料檔案之安全維護與管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏，經中央目的事業主管機關指定後，應訂定個人資料檔案安全維護計畫（以	一、非公務機關為落實個人資料檔案之安全維護，經中央目的事業主管機關指定後，應訂定相關安全維護計畫，以建立並執行相關管理程序或制度，本條第一項明示此旨。

本報告之智慧財產權歸屬於法務部

條文	說明
下簡稱計畫)。 本辦法第四條至第二十九條所規定之相關組織及程序要求，應訂定於計畫內。	二、計畫標準辦法內所規定之相關組織及程序要求，受指定之非公務機關應訂定於安全計畫內，本條第二項明示此旨。
第三條　本辦法用詞定義如下： 一、個人資料管理代表：非公務機關之負責人或負責人直接授權，擔任督導計畫之規劃、訂定、執行、修訂及相關決策之人員。 二、個人資料內評代表：由非公務機關之負責人授權，負責督導相關內評人員評核計畫之執行成效之人員。 三、所屬人員：執行業務之過程必須接觸個人資料之人員，包括公司之定期或不定期契約人員及派遣員工。 本辦法所未定義之名詞，以本法第二條為準。	一、欲有效達成管理組織之運作，組織內必須有一角色擔任督導計畫之規劃、訂定、執行、修訂及相關決策，並擔任負責人與管理組織間橋樑之工作，個人資料管理代表即為計畫中賦予此一任務之角色。 二、非公務機關為確保計畫之落實，應有相關人員負責於非公務機關內部評核計畫落實之狀況，而個人資料內評代表則負責統整相關評核之結果。 三、為確保個人資料檔案之安全維護，凡執行業務之過程必須接觸個人資料之人員，包括公司之定期或不定期契約人員及派遣員工，均應為遵守計畫之相關程序並執行之。 四、本條針對本辦法相關名詞加以定義，所未定義之名詞，則以本法第二條為準。
第四條　非公務機關為訂定並執行計畫，應建立個人資料檔案安全維護管理組織，並配置相當資源。 前項管理組織之任務如下： 一、規劃、訂定、執行與修訂安全維護計畫相關程序。 二、管理代表應定期向事業之負責人就前款事項提出書面報告。 第一項之管理組織至少應包括個人資料管理代表與個人資料內評代表。	一、非公務機關欲有效訂定與執行安全維護計畫，應建立相當組織與投注相當資源。該管理組織應其任務即為安全維護計畫相關程序之規劃、訂定、執行與修訂，且為使非公務機關之負責人能盡其督導及監督之責，管理代表應定期向事業之負責人以書面報告相關事項。 二、為有效督導並評核安全維護計畫執行之成效，除個人資料管理代表外，管理組織亦應有監督或評核計畫是否落實執行之個人資料內評

本報告之智慧財產權歸屬於法務部

條文	說明
	代表。
貳、一般程序	**第二章章名**
第五條　非公務機關應依其組織與事業特性訂定個人資料保護管理政策，經非公務機關之負責人核可，並公開周知，使其所屬人員均明確瞭解。 前項政策至少應包括下列事項之說明： 一、遵守我國個人資料保護相關之法令規定。 二、以合理安全之方式，於特定目的範圍內，蒐集、處理及利用個人資料。 三、以可期待之合理安全水準技術保護其所蒐集、處理、利用之個人資料檔案。 四、設置聯絡窗口，供當事人行使關於個人資料之權利或提出相關之申訴與諮詢。 五、規劃緊急應變程序以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。 六、如有委託蒐集、處理及利用個人資料時，妥善監督受託機關。 七、持續維運計畫，以確保個人資料檔案之安全。	一、為使非公務機關全體人員對於個人資料之保護能有所體認，進而能落實計畫，故非公務機關應訂定個人資料保護管理政策，將計畫相關重點事項於政策內闡明。且為達上述目的，該等政策應加以公開周知，且由非公務機關之負責人核可，以明示保護個人資料之旨。 二、該相關重點事項包括：遵守我國個人資料保護相關之法令規定、合法正當蒐集、處理及利用個人資料；應以適當之技術保護個人資料；應提供當事人行使權利之方式；規劃緊急應變程序以處理事故；監督受託機關之責任；持續維運計畫之義務。
第六條　非公務機關應定期檢視非公務機關所應遵循之個人資料保護相關法令，並依據法令訂定或修訂計畫。	一、非公務機關因其種類、特性及其所蒐集、處理、利用之個人資料範圍之不同與變動，其所應適用之個人資料保護法令亦可能有所不同，事業為符合法令之規定，自應依據上述事業自身狀況清查適用之個人資料保護相關法令。 二、個人資料保護相關法令規定，因時事變遷而有隨之變更之可能，非公

本報告之智慧財產權歸屬於法務部

條文	說明
	務機關自應定期檢視，以持續修訂其安全維護計畫。
第七條　非公務機關應依據個人資料保護相關法令，清查非公務機關所保有之個人資料，界定其納入計畫之範圍並建立清冊，且定期確認其是否有所變動。	本法施行細則第九條第一項第二款規定，安全維護計畫中應就界定個人資料範圍相關事項加以規定，本條即進一步闡明該規定之意旨。非公務機關需先掌握於其內部之個人資料之種類與數量，方能有效對其所保有之個人資料加以控管。
第八條　非公務機關應根據前條所界定之個人資料，及其相關業務流程，分析可能產生之風險，並根據風險分析之結果，訂定適當之管控措施。	本法施行細則第九條第一項第三款規定，安全維護計畫應就個人資料之風險評估及風險管理加以規定，本條即在進一步闡明該規定之意旨。非公務機關應依據其相關業務流程，判斷於蒐集、處理及利用之過程中，個人資料可能發生之危險，以及其危險性之高低，方能進一步以適當之方式保護個人資料並降低其風險。
第九條　非公務機關為因應所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，應就下列事項建立相關程序： 一、採取適當之應變措施，以控制事故對當事人之損害。 二、查明事故之狀況並適時通知當事人。 三、避免類似事故再次發生。	一、當個人資料被竊取、竄改、毀損、滅失或洩漏等事故發生時，常造成資料當事人財產及非財產上之損害，非公務機關為降低或控制損害之範圍，應訂定相關之因應機制，本條即明示此旨。 二、事故應變之首要目標即根據事故之類型，採取應變措施以降低或控制損害之範圍。其次，應讓當事人瞭解相關狀況，使當事人亦能採取相關措施防止損害發生或擴大。最後，避免類似事故再次發生亦為應變措施之重點。
第十條　非公務機關委託他人蒐集、處理或利用個人資料之全部或一部時，為對受託人為適當之監督，應就下列事項建立相關程序： 一、確認所委託蒐集、處理或利用之	一、非公務機關如將個人資料之蒐集、處理或利用委託他人為之，仍應對受託人為適當之監督，以使資料之蒐集、處理或利用仍符合事業安全維護計畫之要求；本條即規定

本報告之智慧財產權歸屬於法務部

條文	說明
個人資料之範圍、類別、特定目的及其期間。 二、確認受託人應採取必要安全措施。 三、有複委託者，確認其複委託之對象。 四、受託人或其受僱人違反個人資料保護法令或委託契約條款時，要求其向委託人通知相關事項。 五、與受託人約定委託人所保留指示之事項。 六、委託關係終止或解除時，要求受託人返還或銷毀因委託事項所交付之個人資料載體，及刪除因委託事項所儲存於受託人之個人資料。 七、確認受託人執行上述要求事項之狀況。	非公務機關應就此建立一定之程序。 二、參酌本施行細則第八條之規定。
參、法令遵循程序	**第三章章名**
第十一條　非公務機關為確保個人資料之蒐集符合個人資料保護相關法令要求，應就下列事項建立相關程序： 一、確認蒐集個人資料之特定目的。 二、確認具備法令所要求之特定情形或其他要件。	依本法第十九條第一項規定，蒐集個人資料應有特定目的並具備一定之法定情形，而若其他法令有特別要求，亦應遵守之，故應建立相關程序以確認之。
第十二條　非公務機關為遵守本法第八條及第九條關於告知義務之規定，應就下列事項建立相關程序： 一、確認是否得免告知。 二、依據資料蒐集之情況，採取適當之告知方式。	依本法第八條及第九條規定，非公務機關應適時履行告知義務，故除確認有例外情況無須告知外，均應依據資料蒐集之情況，採取適當之告知方式，以有效履行告知義務。
第十三條　非公務機關為確保個人資料之利用符合個人資料保護相關法	依本法第二十條第一項規定，個人資料應於蒐集之特定目的必要範圍內利

本報告之智慧財產權歸屬於法務部

條文	說明
令要求，應就下列事項建立相關程序： 一、確保資料之利用符合特定目的。 二、確認是否得進行及如何進行特定目的外利用。	用，但於特定情形下，得為目的外之利用。因此應建立一定程序，以確保資料之利用符合特定目的。若有必要為特定目的外利用時，亦應確認其是否合法，及特定目的外利用之相關情事。
第十四條　非公務機關如欲新增或變更特定目的時，應依下列程序為之： 一、依本辦法第十二條之程序為之。 二、取得當事人書面同意，但法令別有規定者，不在此限。	於前條規定非公務機關於特定情形下，得將所保有之個人資料為特定目的外之利用，惟該條規定乃針對個別情況下得否及如何為特定目的外之利用。若非公務機關若欲繼續性地對於其所保有之個人資料進行特定目的之新增或變更時，應先依相關告知義務之程序為之。其次，除法令別有規定外，原則上應取得當事人之書面同意，方能為特定目的之新增或變更。
第十五條　非公務機關於利用個人資料行銷時，應就下列事項建立相關程序： 一、確保當事人表示拒絕接受後，立即停止利用其個人資料行銷。 二、確保首次行銷時，當事人表示拒絕接受行銷無須支付任何費用。	一、依本法第二十條第二項及第三項規定，當事人有拒絕行銷之權利，因此應建立程序以確保當事人表示拒絕接受後，立即停止利用其個人資料行銷。 二、其次，於首次行銷時，並應提供當事人表示拒絕接受行銷之方式，並支付相關費用，以符合本法要求第二十條第三項之要求。
第十六條　非公務機關針對本法第六條之特種個人資料，應就下列事項建立相關程序： 一、確認所蒐集、處理及利用之個人資料是否包含特種個人資料。 二、確保蒐集、處理及利用特種個人資料，符合相關法令之要求。	依本法第六條規定，非公務機關原則上不得蒐集、處理及利用醫療、基因、性生活、健康檢查及犯罪前科之個人資料，故非公務機關應先建立程序以確認是否有蒐集相關特種個人資料。如有蒐集時，並應確保蒐集、處理及利用特種個人資料，符合相關法令之要求。
第十七條　非公務機關進行個人資料國際傳輸前，應確認是否受中央目的事業主管機關限制並遵循之。	依本法第二十一條規定，中央目的事業主管機關得於一定情形下，限制非公務機關對於個人資料進行國際傳輸，因此非公務機關應建立程序以確認主管機關是否有所限制並加以遵守之。

本報告之智慧財產權歸屬於法務部

條文	說明
第十八條　非公務機關為提供資料當事人行使個人資料保護法第三條所規定之權利，應就下列事項建立相關程序： 一、如何提供當事人行使權利。 二、確認當事人身分。 三、確認是否有本法第十條及第十一條得拒絕當事人行使權利之情況。 四、適時回覆當事人請求。	一、依本法第三條規定，當事人就其個人資料得行使包含查詢或請求閱覽等五項權利，且依據本法第十條及第十一條，非公務機關除有法所規定之正當理由外，應於一定期間內回覆當事人之請求，本條即規定非公務機關應建立相關程序以供資料當事人行使權利。 二、為使當事人得有效行使其權利，提供一定方式，如常設之聯絡窗口，包含聯絡電話或聯絡之電子郵件信箱等，即為首要之程序。 三、避免資料不當提供給第三人或不當刪除，故非公務機關於提供當使人行使權利前，應先建立程序以確認當事人身分。 四、其次，本法第十條及第十一條規定於一定情形下非公務機關得拒絕當事人行使權利，故應有程序確認是否符合該等拒絕之情況，如並無該等情況，則應於本法所規定之時限內，適時回覆當事人之請求。
第十九條　非公務機關為確認其所保有個人資料之正確性，應就下列事項建立相關程序： 一、確保資料於處理過程中，正確性不受影響。 二、當確認資料有錯誤時，應適時更正。 三、定期檢查資料之正確性。 因可歸責於非公務機關之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象之程序。	一、非公務機關所保有之個人資料之正確性，攸關非公務機關是否能有效利用當事人之個人資料以提供當事人相關服務，並避免當事人發生因資料不正確所產生之損害。因此非公務機關應建立程序，確保資料於處理過程中不會發生錯誤，若資料仍有錯誤之情況，應適時更正，且應定期檢查資料之正確性。 二、若非公務機關曾提供所保有之個人資料予他人，且因可歸責於非公務機關之事由，未更正或補充致使個人資料不正確時，自應課以該蒐集機關於更正或補充個人資料

本報告之智慧財產權歸屬於法務部

條文	說明
	後，通知曾提供利用該資料之對象，以使該不正確之資料能即時更新，避免當事人權益受損，爰參酌本法第十一條第五項，訂定第二項。
第二十條　非公務機關應定期確認其所保有個人資料之特定目的是否消失，或期限是否屆滿，若特定目的消失或期限屆滿時，應遵守本法第十一條第三項規定。	非公務機關蒐集、處理或利用個人資料均應於特定目的必要範圍內為之，若蒐集、處理、利用個人資料之特定目的已消失或期限已屆滿，則應遵守本法第十一條第三項之規定，加以刪除或停止處理利用。
肆、安全管理措施	**第四章章名**
第二十一條　為防止個人資料發生被竊取、竄改、毀損、滅失或洩漏等遭受侵害之情事，非公務機關應依據業務性質、個人資料存取環境、個人資料種類與數量及個人資料傳輸工具與方法等因素，採取第二十二條至第二十五條之管理措施。	一、對於個人資料之保護，除於組織面給予整體規劃，及法令遵循程序之設計外，尚應考慮安全管理措施之部分，而如何規劃安全管理措施，則應綜合考量非公務機關之業務性質、個人資料存取環境、個人資料種類與數量及個人資料傳輸工具與方法等因素。 二、安全管理措施可分為人員管理、作業管理、物理環境管理、技術管理之不同要求，本辦法第二十三條至第二十六條將分別針對上述要求加以規定。

本報告之智慧財產權歸屬於法務部

條文	說明
第二十二條　非公務機關應採取下列人員管理措施： 一、確認蒐集、處理及利用個人資料之各相關業務流程之負責人員。 二、依據作業之必要，設定所屬人員不同之權限並控管之，以一定認證機制管理其權限，且定期確認權限內容設定之適當與必要性。 三、要求所屬人員負擔相關之保密義務。	一、針對人員管理之部分，首先應先確認實際進行個人資料之蒐集、處理及利用之負責人員為何，方可確認相關管理程序之權責歸屬。 二、非公務機關所屬人員與個人資料相關之各項作業，若有設定權限控管之必要，則應以一定認證機制管理之，並確認其權限設定是否適當或必要。避免人員取得不適當之權限，得以接觸非於作業必要範圍內之個人資料。 三、而非公務機關與其所屬人員應要求所屬人員負擔相關之保密義務，使所屬人員能明瞭其責任，必要時亦可以訂定契約條款之方式為之，以作為相關權責之紀錄。
第二十三條　非公務機關應採取下列作業管理措施： 一、訂定蒐集、處理及利用之作業注意事項。 二、運用電腦及相關設備處理個人資料時，應訂定使用可攜式儲存媒體之規範。 三、針對所保有之個人資料內容，確認是否有加密之必要，如有必要，應採取適當之加密機制。 四、傳輸個人資料時，因應不同之傳輸方式，確認是否有加密之必要，如有必要，應採取適當之加密機制，並確認資料收受者之正確性。 五、非公務機關應依據所保有資料之重要性，評估個人資料是否有備份必要，如有必要應予備份。對於備份資料應確認是否有加密之必要，如有必要，採取適當	一、針對個人資料蒐集、處理及利用的個別相關作業，非公務機關應基於計畫之原則規定，訂定具體之作業注意事項，使所屬人員有所依循。 二、使用可攜式儲存媒體，可能提高處理個人資料之電腦及相關設備遭受惡意程式攻擊及個人資料外洩之風險，因此若有使用可攜式儲存媒體之情況，應定相關使用規範。 三、針對個人資料處理之不同態樣，包括儲存、傳輸及備份之狀況，如資料有加密之必要，即應採取適當之加密機制。 四、於傳輸個人資料之情況，除有必要時採取加密機制，並應確認資料收受者之正確性，以避免資料不當外洩。 五、針對有備份必要之個人資料，除有必要時採取加密機制，儲存備份資料之媒體亦應以適當方式保管，且

本報告之智慧財產權歸屬於法務部

條文	說明
之加密機制，儲存備份資料之媒體亦應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。 六、儲存個人資料之媒體於廢棄或移轉與他人前，應確實刪除媒體中所儲存之資料，或以物理方式破壞之。 七、妥善保存認證機制及加密機制中所運用之密碼，如有交付他人之必要，亦應妥善為之。	定期進行備份資料之還原測試，以確保備份之有效性。 六、儲存個人資料之媒體於廢棄或移轉與他人前，應確實刪除媒體中所儲存之資料，或以物理方式破壞之，以避免資料不當外洩。 七、如作業程序中相關認證機制與加密機制有運用密碼之必要時，該密碼亦應妥善加以保存。
第二十四條　非公務機關應採取下列物理環境管理措施： 一、依據作業內容之不同，實施必要之門禁管理。 二、妥善保管個人資料之儲存媒體。 三、針對不同作業環境，建置必要之防災設備。	在實體之物理環境管理方面，非公務機關亦應針對不同之作業內容、作業環境及個人資料之種類與數量，實施必要之門禁管理，以適當方式或場所保管個人資料之儲存媒體，並建置必要之防災設備。
第二十五條　非公務機關利用電腦或相關設備蒐集、處理或利用個人資料時，應採取下列技術管理措施： 一、於電腦、相關設備或系統上設定認證機制，對有存取個人資料權限之人員進行識別與控管。 二、認證機制使用帳號及密碼之方式時，使其具備一定安全之複雜度並定期更換密碼。 三、於電腦、相關設備或系統上設定警示與相關反應機制，以對不正常之存取為適當之反應與處理。 四、對於存取個人資料之終端機進行身分認證，以識別並控管之。 五、個人資料存取權限之數量及範圍，於作業必要之限度內設定之，且原則上不得共用存取權限。	一、非公務機關若利用電腦或相關設備蒐集、處理或利用個人資料時，針對相關電腦系統技術，亦應有相應之管理措施，本條即臚列相關技術管理措施，供非公務機關視其實際作業之必要予以實施。 二、本條所臚列之技術管理措施約可分為： （一）系統存取權限之設定及實施：以認證機制，對有存取個人資料權限之人員進行識別與控管，若認證機制使用密碼之方式時，並應有適當之管理方式，並定期測試權限機制之有效性（第一款至第四款、第八款）。 （二）系統存取權限之控管：系統存取權限之設定應於必要範圍內為之，避免非作業必要之人員得存取相關

本報告之智慧財產權歸屬於法務部

條文	說明
六、採用防火牆或路由器等設定，避免儲存個人資料之系統遭受無權限之存取。 七、欲使用能存取個人資料之應用程式時，確認使用者具備使用權限。 八、定期測試權限認證機制之有效性。 九、定期檢視個人資料之存取權限設定正當與否。 十、於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼。 十一、對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。 十二、定期瞭解惡意程式之威脅，並確認安裝防毒軟體及修補程式後之電腦系統之穩定性。 十三、具備存取權限之終端機不得安裝檔案分享軟體。 十四、測試處理個人資料之資訊系統時，不使用真實之個人資料，如有使用真實之個人資料之情形時，明確規定其使用之程序。 十五、處理個人資料之資訊系統如有變更時，確認其安全性並未降低。 十六、定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形。	資料，增加個人資料不當外洩之風險。且應定期檢視存取權限之必要性及是否需要調整（第五款、第九款）。 （三）採用防火牆或路由器等設定，避免儲存個人資料之系統遭受無權限之存取（第六款）。 （四）存取個人資料之應用程式之控管（第七款）。 （五）避免惡意程式與系統漏洞對作業系統之威脅（第十款至第十二款）。 （六）檔案分享軟體之控制（第十三款）。 （七）系統測試時，使用個人資料之程序（第十四款）。 （八）資訊系統變更時，其安全性之確認（第十五款）。 （九）系統之使用狀況與個人資料存取之情形（第十六款）。
伍、認知宣導及教育訓練	**第五章章名**
第二十六條　非公務機關應對於所屬人員施以認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業	若欲使計畫相關管理程序能落實執行，應使非公務機關之所屬人員均能明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業程序，故應

本報告之智慧財產權歸屬於法務部

條文	說明
程序。	透過認知宣導及教育訓練為之。
陸、計畫稽核及改善程序	**第六章章名**
第二十七條　非公務機關為確保計畫之有效性，應定期檢查計畫是否落實執行。	計畫以及非公務機關依據計畫所訂定之相關程序，非公務機關所屬人員是否皆已落實執行，必須通過一定之檢查機制方能確定。
第二十八條　為持續改善計畫，非公務機關應建立下列程序： 一、計畫發生未落實執行時之改善程序。 二、如計畫有變更之需要時，其變更之程序。	一、於前條檢查過程中，若發現有未落實執行之情況，非公務機關應建立程序，協助相關所屬人員加以改善。 二、若計畫有窒礙難行或因應法令之增修，而有變更之需要時，亦應有變更之相關程序。
柒、紀錄機制	**第七章章名**
第二十九條　關於計畫各項程序之執行，非公務機關至少應保存下列紀錄： 一、因應事故發生所採取行為之紀錄。 二、確認受託人執行委託人要求事項之紀錄。 三、提供當事人行使權利之紀錄。 四、確認資料正確性及更正之紀錄。 五、權限新增、變動及刪除之紀錄。 六、違反權限行為之紀錄。 七、備份及還原測試之紀錄。 八、個人資料交付、傳輸之紀錄。 九、個人資料刪除、廢棄之紀錄。 十、存取個人資料系統之紀錄。 十一、定期檢查處理個人資料之資訊系統之紀錄。 十二、教育訓練之紀錄。 十三、計畫稽核及改善程序執行之紀錄。	為確認計畫以及非公務機關依據計畫所訂定之相關程序是否落實執行，以及釐清個人資料於蒐集、處理及利用過程之相關權責，非公務機關應保存相關紀錄以供查驗。
捌、施行日期	**第八章章名**
第三十條　本辦法自發布日施行。	本辦法施行日期。

本報告之智慧財產權歸屬於法務部

資料來源：本計畫撰寫

（四）公務機關或學術研究機構基於醫療衛生或犯罪預防目的蒐集、處理或利用特種個人資料辦法草案

依據個人資料保護法第 6 條第 2 項之規定，中央目的事業主管機關應會同法務部訂立本法第 6 條第 1 項第 4 款之個人資料蒐集、處理或利用範圍之辦法。本辦法針對之情形為「公務機關或學術研究基於醫療、衛生、或犯罪預防目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料」。依此，本辦法將針對公務機關或學術研究基於特定目的而蒐集、處理或利用醫療、基因、性生活、健康檢查及犯罪前科等個人資料之情形，訂立應遵行程序，共計十七條，以下將分別闡述本辦法草案逐條條文之要旨：

1.本辦法之法源依據

本辦法第一條即明示，未來公務機關或學術研究基於醫療、衛生、或犯罪預防目的，為統計或學術研究而有必要，所為蒐集、處理或利用個人資料之相關程序，均依據個人資料保護法第六條第二項規定訂定。

2.本辦法名詞定義

本辦法重要用詞之定義，係參考我國人體生物資料庫管理條例、研究用人體檢體採集與使用注意事項關於編碼、加密及去連結之定義。所謂編碼，係指以代碼取代當事人姓名、身分證統一編號等可以直接或間接方式識別該個人之資料，使達到難以辨識個人身分之作業方式；加密則是指將足以辨識當事人個人身分之資訊訊息，轉化為無可辨識之過程；至於去連結是指於資料編碼後，使其與可供辨識參與者之個人資料、資訊，永久無法以任何方式連結、比對之作業。

3.倫理委員會之設置

醫療、基因、性生活、健康檢查或犯罪前科之個人資料屬高度敏

本報告之智慧財產權歸屬於法務部

感性個人資料，相關蒐集、處理或利用程序應有嚴謹之倫理監理機制，爰參考我國人體生物資料庫管理條例及我國人體研究倫理政策指引第七點之規定，規定倫理委員會之任務及組成方式。

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，蒐集有關醫療、基因、性生活、健康檢查或犯罪前科之個人資料時，應設置倫理委員會，就蒐集、處理或利用之程序與相關事項進行審查及監督。

前項委員會應置審查委員○人至○人，由機關或機構選任之，並報請主管機關備查，其中○人（或比例）以上應為法律專家及社會公正人士；並應有○人（或比例）為非該機關或機構之人員。

4.倫理委員會之審查

為確保公務機關或學術研究機構確為統計或學術研究而有必要進行特種資料之蒐集、處理或利用，規定於事前應先擬定相關計畫書，送交倫理委員會審查通過。前述計畫書內容應包含統計或研究規劃、計畫主持人之最新履歷、蒐集、處理或利用個人資料之範圍與程序、採取之安全措施，若有委託之情形，與受委託單位之約定。惟考量研究或統計執行之性質、機構之規模與業務量，對於部分小型學術研究機構而言，獨立設置倫理委員會可能將大幅增加其負擔，爰於第一項但書規定得由主管機關訂定其他審查程序。

參考美國衛生暨人類事務部（Department of Health and Human Service）所頒布之聯邦人類研究對象之保護政策（Federal Policy of the Protection of Human Subjects）及我國醫療機構人體試驗委員會組織及作業基準，於草案第五條規定倫理委員會審查時應注意之重點項目及相關程序，包括計畫主持人的資格及經驗之適當性、統計或研究規劃與目的之合理關聯性及統計或研究方法之合理性與必要性、蒐集、處理或利用個人資料之範圍與程序是否符合相關規定、安全措施之妥適性，若有委託之情形，機構或機關與受委託單位約定是否符合相關規定。

此外，本辦法亦規定倫理委員會召開審查會議，應有半數以上之委員出席，且倫理委員會非經討論，不得逕行決定審查結果，而未直

本報告之智慧財產權歸屬於法務部

接參與討論之委員不得參與決定。審查結果得為核准、修正後複審、不核准或是中止或終止原核准之計畫，並於決定之日起，○日內以書面為通知。

經為核准之決定，應作成決定書載明統計或研究計畫之名稱及日期、計畫主持人姓名、機構或機關名稱、決定作成之日期、決定之內容、其他附帶之建議，以及後續定期追蹤之程序與要求。作成修正後複審之決定時，應明確載明應修正之處，並通知計畫主持人複審之程序。若倫理委員會作成不核准之決定時，應說明不核准之理由。

公務機關或學術研究機構為統計或學術研究而有必要進行特種資料之蒐集、處理或利用前，除經倫理委員會審查通過外，亦應報主管機關備查後始得為之。

5.倫理委員會之監督與管理

為確保公務機關或學術研究機構依倫理委員會審查通過之計畫而為特種資料之搜集、處理或利用，爰參考我國醫療機構人體試驗委員會組織及作業基準第五章，規定倫理委員會應對於所審核之計畫建立監督機制，追蹤審查經核准統計或研究計畫之執行情形與進度，並應遵循相關程序，倫理委員會為執行監督，應於決定書載明與計畫主持人間之持續溝通方式。

追蹤審查應訂定追蹤審查之委員人數及審查程序，並應依計畫特性訂定追蹤審查之期間，每年不得少於一次。倫理委員會於追蹤審查後所為之決定應通知計畫主持人，並載明原決定之變更、中止或終止，或確認原決定仍然有效。若統計或研究計畫中止或終止時，公務機關或學術研究機構應向倫理委員會通知其原因，以及統計或研究情形，同時也需報經主管機關核備。統計或研究計畫完成時，應將執行情形及結果以書面通知倫理委員會，並報經主管機關核備。

6.倫理委員會紀錄

為確認倫理委員會之運作，爰參考我國醫療機構人體試驗委員會組織及作業基準第六章之規定，要求倫理委員會應保存倫理委員會應

本報告之智慧財產權歸屬於法務部

保存機關或機構送審之計畫書、會議紀錄、追蹤審查紀錄、與統計或研究計畫執行相關人員往返之信件，以及倫理委員會成員名單等紀錄，且至少應保存至計畫結束後三年。

7.告知義務

特種個人資料之性質較為特殊或具敏感性，如任意蒐集、處理或利用，恐會造成社會不安或對當事人造成難以彌補之傷害。為使當事人明知其個人資料被何人蒐集及其資料類別、蒐集目的等，爰於第七條第一項規定蒐集時應告知當事人之事項，包括公務機關或學術研究機構名稱、蒐集之目的、個人資料之類別、個人資料利用之期間、地區、對象及方式、當事人依本法第三條規定得行使之權利及方式等事項，若當事人得自由選擇提供個人資料時，公務機關或學術研究機構亦應告知不提供將對其權益之影響，俾使當事人能知悉其個人資料被他人蒐集之情形。

另考量間接蒐集之情形，亦規定公務機關或學術研究機構於處理或利用前，向當事人告之個人資料來源及前述所列事項，惟已經處理而無從識別特定當事人之資料，對於當事人權益應無影響，爰於第二項但書規定得無須踐行告知義務之情形。

統計或研究計畫可能涉及專業術語，為使當事人了解其其個人資料被蒐集之用途，爰規定公務機關或學術研究機構應以一般人能理解之方式為告知。

8.蒐集之範圍

特種個人資料之性質較為特殊或具敏感性，為避免蒐集者任意蒐集，爰限制其應於達成其目的之必要範圍內為之。

9.處理及利用之範圍

為避免資料蒐集者巧立名目或理由，任意的蒐集、處理或利用個人資料，爰明定公務機關或學術研究機構對於依本辦法蒐集個人資料之處理及利用，應與蒐集之目的有正當合理之關聯，不得逾越蒐集之

本報告之智慧財產權歸屬於法務部

目的範圍，亦不得與其他目的作不當之聯結。

為保護當事人特種個人資料，爰規定為統計或學術研究之必要處理或利用個人資料時，應以編碼、加密、去連結或其他無從識別當事人之方式為之。惟考量部份統計或學術研究需長期觀察或追蹤，而需要識別當事人，爰明定得毋需以無從識別當事人之方式為處理或利用。

10.公務機關蒐集、處理或利用程序

本法第十五條規定公務機關對於一般個人資料之蒐集或處理應符合特定情形，考量特種資料之敏感性，爰規定公務機關公務機關基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，蒐集或處理有關醫療、基因、性生活、健康檢查或犯罪前科之個人資料，應於執行法定職務必要範圍內或於當事人書面同意之情形，始得為之。

公務機關為執行法定職務必要範圍，以衛生署統計室為例，其為提供各類生命與衛生統計，以彰顯當前公共衛生與國民健康狀況，以及其未來可能發展趨勢，作為政府衛生政策制訂之依據與施政之參考，即可為之。至於當事人書面同意之情形，既已得當事人之同意，公務機關自得蒐集相關個人資料。

值得一提的是，本法第十六條規定於特定情形時得為特定目的外之利用，惟考量特種個人資料具高度敏感性，若允許為特定目的外之利用，對當事人隱私權益影響極大，爰規定公務機關不得於特定目的外利用之。

11.學術研究機構蒐集、處理或利用程序

本法第十九條規定非公務機關對於一般個人資料之蒐集或處理應符合特定情形，考量特種資料之敏感性，爰規定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，蒐集或處理有關醫療、基因、性生活、健康檢查或犯罪前科之個人資料時，僅得在當事人已自行公開或已合法公開或經當事人書面同意之情

本報告之智慧財產權歸屬於法務部

形，始得為之

本法第二十條規定於特定情形時得為特定目的外之利用，惟考量特種個人資料具高度敏感性，若允許為特定目的外之利用，對當事人隱私權益影響極大，爰規定學術研究機構不得於特定目的外利用之，應於蒐集之特定目的必要範圍內為之。

12.國際傳輸之限制

為保障資料當事人之權益，避免統計或研究人員將所蒐集之特種個人資料傳輸至第三地，藉由較寬鬆法規管制，規避我國法律之管制，而侵害國人之權益，爰參考我國人體生物資料庫管理條例第十五條之規定，禁止將依本辦法蒐集、處理或利用之特種個人資料為國際傳輸。惟經處理而無從識別特定當事人之個人資料，由於已無法辨識當事人，則不受此限制。

13.當事人權利行使之限制

依本辦法為蒐集、處理或利用之個人資料，其目的在於醫療、衛生或犯罪預防，並為統計或學術研究而有必要者，涉及群體性，雖自當事人之個人資料出發，惟並不涉及個別利用問題。為調和統計與學術研究之特性，以及當事人隱私權之保障，爰參考歐盟資料保護指令第十三條當事人資料近用權利規定，於本條明定除可辨識當事人個人資料之外，原則上排除當事人請求閱覽、複製、補充或更正等權利。

14.委託蒐集、處理或利用

為避免受委託之第三人對於當事人之特種個人資料有濫用或使用不當之情形，爰規定委託人應盡其選任與監督受託人之責，並於委託契約中載明特定事項，以保護當事人之權益。

公務機關或學術研究機構依委託他人蒐集、處理或利用個人資料之全部或一部時，應依相關法令為之，並將法令要求事項載明於與第三人簽訂之書面契約中。而公務機關或學術研究機構就該書面契約之保存期間，至少應與個人資料之保存期間一致。

本報告之智慧財產權歸屬於法務部

15.保密義務

為避免公務機關及學術研究機構人員於蒐集、處理或利用特種個人資料時，洩漏因業務知悉之相關資訊，爰於本辦法第十五條明定相關人員之保密義務：「公務機關或學術研究機構應要求相關人員，於涉及本辦法蒐集、處理或利用之個人資料，負有保密之義務，並應定期實施教育訓練，使相關人員了解個人資料保護相關法令之要求。」

16.安全措施

公務機關或學術研究機構為維護所蒐集、處理或利用之個人資料，應對於個人資料之使用、保存與管理實體個人資料及檔案之實體場所，訂定相關管理及安全措施：「公務機關或學術研究機構依本辦法對於個人資料之蒐集、處理或利用，應訂定符合下列規定之管理及安全措施：

（1）與業務有關之登入、製作、查閱、增刪、修改、存取、複製等相關之權限設定與管控機制。

（2）公務機關或學術研究機構內非執行統計或研究計畫人員之權限設定、管控機制與保密措施。

（3）運用各項系統時所需之密碼、憑證或其他身分確認措施。

（4）蒐集、處理或利用之特種個人資料被違法或不當使用時，應採取之應變措施。

（5）保存與管理特種個人資料之相關場所或設備之管控機制。」

（6）除實體安全及管理措施外，公務機關或學術研究機構為透過資訊系統蒐集、處理或利用之個人資料，為達成維護系統安全的目的，亦應對於資訊系統訂定相關管理及安全措施：「公務機關或學術研究機構對於依本辦法蒐集、處理或利用特種個人資料所涉及之資訊系統，應訂定符合下列規定之管控及應變措施：

（7）設定系統建置、維護、管制之標準作業程序，並就系統之維護，製作相關紀錄以供查核。

本報告之智慧財產權歸屬於法務部

（8）維護資料傳輸安全之加密及其他相關機制。

（9）設置系統故障時之緊急應變機制。

（10）定期評估系統風險及弱點之機制。

（11）相關資訊系統應定期為資料備援與回復處置機制。

（12）保持資訊系統時間正確之機制，並據以執行。」

17.施行日

本辦法自發布日施行

表 3：公務機關或學術研究機構基於醫療衛生或犯罪預防目的蒐集、處理或利用特種個人資料辦法草案

條文	說明
第一條（法源依據） 本辦法依個人資料保護法（以下簡稱本法）第六條第二項規定訂定之。	本辦法之法源依據
第二條（名詞定義） 本辦法用詞，定義如下： 一、編碼：指以代碼取代當事人姓名、身分證統一編號等可以直接或間接方式識別該個人之資料，使達到難以辨識個人身分之作業方式。 二、加密：指將足以辨識當事人個人身分之資訊訊息，轉化為無可辨識之過程。 三、去連結：指於資料編碼後，使其與可供辨識參與者之個人資料、資訊，永久無法以任何方式連結、比對之作業。	本辦法重要用詞之定義，係參考我國人體生物資料庫管理條例、研究用人體檢體採集與使用注意事項關於編碼、加密及去連結之定義。

本報告之智慧財產權歸屬於法務部

條文	說明
第三條（倫理委員會之設置） 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，蒐集有關醫療、基因、性生活、健康檢查或犯罪前科之個人資料時，應設置倫理委員會，就蒐集、處理或利用之程序與相關事項進行審查及監督。 前項委員會應置審查委員○人至○人，由機關或機構選任之，並報請主管機關備查，其中○人（或比例）以上應為法律專家及社會公正人士；並應有○人（或比例）為非該機關或機構之人員。	醫療、基因、性生活、健康檢查或犯罪前科之個人資料屬高度敏感性個人資料，相關蒐集、處理或利用程序應有嚴謹之倫理監理機制，爰參考我國人體生物資料庫管理條例及我國人體研究倫理政策指引第七點之規定，規定倫理委員會之任務及組成方式。
第四條（倫理委員會之審查） 醫療、基因、性生活、健康檢查或犯罪前科資料之蒐集、處理或利用，應擬定計畫書，經由倫理委員會審查。但主管機關得考量研究或統計執行之性質、（學術研究）機構之規模，訂定其他審查程序。 前項計畫書內容應包含統計或研究規劃、計畫主持人之最新履歷、蒐集、處理或利用個人資料之範圍與程序、採取之安全措施，若有委託之情形，與受委託單位之約定。 第一項個人資料之蒐集、處理或利用經倫理委員會審查通過後，應報主管機關備查後始得為之。	為確保公務機關或學術研究機構確為統計或學術研究而有必要進行特種資料之蒐集、處理或利用，規定於事前應先擬定相關計畫書，經倫理委員會審查通過並報主管機關備查。惟考量研究或統計執行之性質、機構之規模與業務量，對於部分小型學術研究機構而言，獨立設置倫理委員會可能將大幅增加其負擔，爰於第一項但書規定得由主管機關訂定其他審查程序。

本報告之智慧財產權歸屬於法務部

條文	說明
第五條（倫理委員會之審查程序） 倫理委員會應就下列事項進行審查： 一、計畫主持人的資格及經驗之適當性。 二、蒐集、處理或利用個人資料之範圍與程序是否符合相關規定。 三、安全措施之妥適性。 四、若有委託之情形，機構或機關與受委託單位約定是否符合相關規定。 倫理委員會召開審查會議，應有半數以上之委員出席。 倫理委員會非經討論，不得逕行決定審查結果。未直接參與討論之委員不得參與決定。 審查結果得為下列決定，並於決定之日起，○日內以書面為通知： 一、核准 二、修正後複審 三、不核准 四、中止或終止原核准之計畫 經為核准之決定，應作成決定書載明下列事項： 一、統計或研究計畫之名稱及日期。 二、計畫主持人姓名。 三、機構或機關名稱。 四、決定作成之日期。 五、決定之內容。 六、其他附帶之建議。 七、後續定期追蹤之程序及要求。 作成修正後複審之決定時，應明	參考美國衛生暨人類事務部（Department of Health and Human Service）所頒布之聯邦人類研究對象之保護政策（Federal Policy of the Protection of Human Subjects）及我國醫療機構人體試驗委員會組織及作業基準，規定倫理委員會審查時應注意之重點項目及相關程序。

本報告之智慧財產權歸屬於法務部

條文	說明
確載明應修正之處，並通知計畫主持人複審之程序。 作成不核准之決定時，應說明不核准之理由。	
第六條（倫理委員會之監督與管理） 倫理委員會應建立監督機制，追蹤審查經核准統計或研究計畫之執行情形與進度。 倫理委員會為執行監督，應於決定書載明與計畫主持人間之持續溝通方式。 追蹤審查應辦理下列事項： 一、訂定追蹤審查之委員人數及審查程序。 二、依計畫特性訂定追蹤審查之期間，每年不得少於一次。 追蹤審查之決定應通知計畫主持人，並載明原決定之變更、中止或終止，或確認原決定仍然有效。 統計或研究計畫中止或終止時，應向倫理委員會通知其原因，以及統計或研究情形，並報經主管機關核備。 統計或研究計畫完成時，應將執行情形及結果以書面通知倫理委員會，並報經主管機關核備。	為確保公務機關或學術研究機構依倫理委員會審查通過之計畫而為特種資料之搜集、處理或利用，爰參考我國醫療機構人體試驗委員會組織及作業基準第五章，規定倫理委員會應對於所審核之計畫為監督管理，並應遵循相關程序。
第七條（倫理委員會紀錄） 倫理委員會應保存機關或機構送審之計畫書、會議紀錄、追蹤審查紀錄、與統計或研究計畫執行相關人員往返之信件，以及倫理委員會成員名單。	為確認倫理委員會之運作，爰參考我國醫療機構人體試驗委員會組織及作業基準第六章之規定，要求倫理委員會應保存相關紀錄。

本報告之智慧財產權歸屬於法務部

條文	說明
前項紀錄至少應保存至計畫結束後三年。	
第八條（告知義務） 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，向當事人蒐集有關醫療、基因、性生活、健康檢查或犯罪前科之個人資料時，應明確告知當事人下列事項： 一、公務機關或學術研究機構名稱。 二、蒐集之目的。 三、個人資料之類別。 四、個人資料利用之期間、地區、對象及方式。 五、當事人依本法第三條規定得行使之權利及方式。 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。 公務機關或學術研究機構蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告之個人資料來源及前項所列事項，但經處理而無從識別特定當事人者，不在此限。 前二項所稱告知，應以當事人易於理解之方式為之。	一、 特種個人資料之性質較為特殊或具敏感性，如任意蒐集、處理或利用，恐會造成社會不安或對當事人造成難以彌補之傷害。為使當事人明知其個人資料被何人蒐集及其資料類別、蒐集目的等，爰於第一項規定蒐集時應告知當事人之事項，俾使當事人能知悉其個人資料被他人蒐集之情形。另考量間接蒐集之情形，亦規定公務機關或學術研究機構於處理或利用前，向當事人為告知，惟已經處理而無從識別特定當事人之資料，對於當事人權益應無影響，爰於第二項但書規定得無須踐行告知義務之情形。 二、 統計或研究計畫可能涉及專業術語，為使當事人了解其個人資料被蒐集之用途，爰規定公務機關或學術研究機構應以一般人能理解之方式為告知。
第九條（蒐集範圍） 公務機關或學術研究機構依前條蒐集個人資料，應於達成其目的之必要範圍內進行。	特種個人資料之性質較為特殊或具敏感性，為避免蒐集者任意蒐集，爰限制其應於達成其目的之必要範圍內為之。
第十條（處理及利用範圍） 公務機關或學術研究機構對於	一、為避免資料蒐集者巧立名目或理由，任意的蒐集、處理或利用個人

本報告之智慧財產權歸屬於法務部

條文	說明
依本辦法蒐集個人資料之處理及利用，不得逾越蒐集之目的範圍，並應以編碼、加密、去連結或其他無從辨識當事人身分之方式為之。但為持續統計或研究而有必要識別當事人者，不在此限。	資料，爰明定個人資料之蒐集、處理或利用，應與蒐集之目的有正當合理之關聯，不得與其他目的作不當之聯結。 二、為保護當事人特種個人資料，爰規定為統計或學術研究之必要處理或利用個人資料時，應以無從識別當事人之方式為之。惟考量部份統計或學術研究需長期觀察或追蹤，而需要識別當事人，爰明定得毋需以無從識別當事人之方式為處理或利用。
第十一條（國際傳輸之限制） 依本辦法蒐集、處理或利用之特種個人資料不得為國際傳輸，但無從識別特定當事人者，不在此限。	為保障資料當事人之權益，避免統計或研究人員將所蒐集之特種個人資料傳輸至第三地，藉由較寬鬆法規管制，規避我國法律之管制，而侵害國人之權益，爰參考我國人體生物資料庫管理條例第十五條之規定，禁止將之輸出境外。惟經處理而無從識別特定當事人之個人資料，由於已無法辨識當事人，則不受此限制。
第十二條（當事人權利行使之限制） 依本辦法所為個人資料之蒐集、處理或利用，當事人不得請求閱覽、複製、補充或更正。但屬可辨識當事人個人之資料者，不在此限。	依本辦法為蒐集、處理或利用之個人資料，其目的在於醫療、衛生或犯罪預防，並為統計或學術研究而有必要者，涉及群體性，雖自當事人之個人資料出發，惟並不涉及個別利用問題。為調和統計與學術研究之特性，以及當事人隱私權之保障，爰參考歐盟資料保護指令第十三條當事人資料近用權利規定，於本條明定除可辨識當事人個人資料之外，原則上排除當事人請求閱覽等權利。

本報告之智慧財產權歸屬於法務部

條文	說明
第十三條（委託蒐集、處理或利用） 公務機關或學術研究機構依委託他人蒐集、處理或利用個人資料之全部或一部時，應依相關法令為之，並將法令要求事項載明於與第三人簽訂之書面契約中。 公務機關或學術研究機構就該書面契約之保存期間，至少應與個人資料之保存期間一致。	為避免受委託之第三人對於當事人之特種個人資料有濫用或使用不當之情形，爰規定委託人應盡其選任與監督受託人之責，並於委託契約中載明特定事項，以保護當事人之權益。
第十四條（保密義務） 公務機關或學術研究機構應要求相關人員，於涉及本辦法蒐集、處理或利用之個人資料，負有保密之義務，並應定期實施教育訓練，使相關人員了解個人資料保護相關法令之要求。	明定相關人員之保密義務。
第十五條（安全措施） 公務機關或學術研究機構依本辦法對於個人資料之蒐集、處理或利用，應訂定符合下列規定之管理及安全措施： 一、與業務有關之登入、製作、查閱、增刪、修改、存取、複製等相關之權限設定與管控機制。 二、公務機關或學術研究機構內非執行統計或研究計畫人員之權限設定、管控機制與保密措施。 三、運用各項系統時所需之密碼、憑證或其他身分確認措施。 四、蒐集、處理或利用之特種個人資料被違法或不當使用時，應採取之應變措施。	公務機關或學術研究機構為維護所蒐集、處理或利用之個人資料，應對於個人資料之使用、保存與管理實體個人資料及檔案之實體場所，訂定相關管理及安全措施。

本報告之智慧財產權歸屬於法務部

條文	說明
五、保存與管理特種個人資料之相關場所或設備之管控機制。	
第十六條（控管措施） 公務機關或學術研究機構對於依本辦法蒐集、處理或利用特種個人資料所涉及之資訊系統，應訂定符合下列規定之管控及應變措施： 一、設定系統建置、維護、管制之標準作業程序，並就系統之維護，製作相關紀錄以供查核。 二、維護資料傳輸安全之加密及其他相關機制。 三、設置系統故障時之緊急應變機制。 四、定期評估系統風險及弱點之機制。 五、相關資訊系統應定期為資料備援與回復處置機制。 六、保持資訊系統時間正確之機制，並據以執行。	公務機關或學術研究機構為透過資訊系統蒐集、處理或利用之個人資料，為達成維護系統安全的目的，應對於資訊系統訂定相關管理及安全措施。
第十七條（施行日） 本辦法自發布日施行。	本辦法之施行日期。

資料來源：本計畫撰寫

本報告之智慧財產權歸屬於法務部

（五）個人資料特定目的暨個人資料類別修正

1.修正緣由

個人資料保護法已於去（99）年 4 月修正通過，其中對於個人資料定義範圍擴大，無論是紙本或電子文件皆為個人資料保護法所規範之範圍，因此提高應受保護資料範圍圈定的困難度；此外，由於適用主體擴大，公務機關與非公務機關皆全面適用，現行電腦處理個人資料保護法特定目的與個人資料類別是否足夠，即生疑義。因此，個人資料保護法第 53 條授權法務部會同中央目的事業主管機關指定特定目的與個人資料類別。以下將介紹我國現行特定目的與個人資料類別項目，同時亦將參考英國、澳洲、美國與日本之立法例。

2.我國現行特定目的與個人資料類別項目

法務部[45]於民國 85 年 8 月 7 日會銜財政部[46]、經濟部[47]、教育部[48]、交通部[49]、行政院新聞局[50]，以及行政院衛生署[51]訂定發布電腦處理個人資料保護法之 101 項特定目的與 133 項個人資料類別，提供公務機關參考外，亦適用於目前受電腦處理個人資料法規範之非公務機關，包括徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人、醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業，另外尚有期貨業、台北市產物、人壽保險商業同業公會、中華民國產物保險商業同業公會、財團法人台灣更生保護會、財團法人犯罪被害人保護協會、不動產仲介經紀業、利用電腦網路開放個人資料登錄之就業服務業、登記資本額為新臺幣一千萬元（含）以上之股份有限公司之組織型態，且有採會員制為行銷方式之百貨公司業及零售式量販業、除語文類科外之文理類補習班、無店面零售業、錄影節目帶出租

[45] 法務部（85）法令字第 19745 號令。
[46] 財政部（85）台財規字第 852278722 號令。
[47] 經濟部（85）經商字第 85021615 號令。
[48] 教育部（85）台人（三）字第 85514910 號令。
[49] 交通部（85）交資字第 04898 號令。
[50] 行政院新聞局（85）聞法字第 10694 號令。
[51] 行政院衛生署（85）衛署資訊字第 85038901 號令。

本報告之智慧財產權歸屬於法務部

業、無店面零售業中之電視購物頻道供應者、運動場館業等經法務部會同中央目的事業主管機關指定之業別。

3.國外立法例參考

（1）英國

英國於 1998 年資料保護法(Data Protection Act of 1998)中規定，蒐集、處理或利用個人資料，必須有特定目的(specified purposes)，此外，處理或利用個人資料不得逾越特定目的範圍，並應向個人資料之當事人告知特定目的，使其知悉。

1998 年資料保護法對於資料控管者(data controllers)如何使個人資料之當事人知悉特定目的亦有規定，資料控管者可於蒐集個人資料時於隱私通知(privacy notice)中向當事人揭露，或向資訊隱私委員辦公室(Information Commissioner's Office, ICO)登記。除非符合免除規定，原則上所有資料控管者均需向 ICO 登記及通知。通知內容分為兩部份，第一部份包括資料控管者名稱及地址、聯絡資訊、處理個人資料之特定目的、個人資料項目(data subjects)、個人資料類別(data classes)、個人資料接收者名單(a list of the recipients of data)、是否傳輸個人資料至非 EEA 地區。第二部份則包括安全聲明(security statement)、公司名稱(trading names)、(statement of exempt processing)、自願通知(voluntary notification)、代表人資料與費用。

1998 年資料保護法中並未明確列出特定目的與個人資料類別之項目，惟在 ICO 公佈之資料保護通知手冊(Data Protection Notification Handbook- A complete guide to notification)中，除說明資料控管者向 ICO 登記及通知之程序與相關事項之外，亦列出特定目的與個人資料類別之項目。

特定目的分為一般商業目的以及其他目的，一般商業目的包括人事行政管理、廣告、行銷、公關，與營業相關紀錄；而其他目的則包括會員管理、福利管理、犯罪預防及刑事偵查與執行、

本報告之智慧財產權歸屬於法務部

資訊及資料庫管理、個人資料交易或分享等 28 項[52]，該資料保護通知手冊中同時也針對各項列出之特定目的有細部說明與解釋，舉例來說，針對福利管理特定目的，手冊中即說明，福利管理係指各種福利之行政管理，資料控管者應於告知當事人時同時明確表示為行政管理之特定福利名稱與類別。值得一提的是，手冊中明白指出，若手冊列舉之 28 項特定目的均不適用，資料控管者得自行以文字描述特定目的。

資料保護通知手冊中亦列出個人資料之類別，將之區分為一般性資料與敏感性資料。一般性資料包括個人資料（Personal details）、家庭、生活習慣與社會情況（Family, lifestyle and social circumstances）、教育與專業（Education and training details）、僱佣資料（Employment details）、財務資料（Financial details），以及商品或服務提供（Goods or services provided）；敏感性資料則包括種族（Racial or ethnic origin）、政治傾向（Political opinions）、宗教信仰（Religious or other beliefs of a similar nature）、工會成員（Trade union membership）、生理或心理健康狀況（Physical or mental health or condition）、性生活（sexual life）、犯罪嫌疑與紀錄（Offences, including alleged offences），以及刑事程序與判決結果（Criminal proceedings, outcomes and sentences）。手冊中對於一般性資料之各類別亦有更為詳細之說明，例如僱佣資料指得是任何與僱佣關係有關之資料，包括工作經驗、出席狀況、健康安全紀錄、訓練紀錄等。

[52] 會計（accounting and auditing）、司法行政（Administration of justice）、會員管理（Administration of membership records）、廣告、行銷、公關（Advertising, marketing and public relations for others）、稅務評估（Assessment and collection of taxes and other revenue）、福利管理（Benefits, grants and loans administration）、招攬選民支持（Canvassing political support amongst the electorate）、選區服務（Constituency casework）、諮詢顧問服務（Consultancy and advisory services）、信用調查（Credit referencing）、犯罪預防及刑事偵查與執行（Crime prevention and prosecution of offenders）、債務承購與行政（Debt administration and factoring）、教育（Education）、募款（Fundraising）、健康服務（Health administration and services）、資訊及資料庫管理（Information and databank administration）、保險（Insurance administration）、傳媒（Journalism and media）、法律服務（Legal services）、發照與登記（Licensing and registration）、宗教行政（Pastoral care）、退休、養老金行政（Pensions administration）、治安（Policing）、私人調查（Private investigation）、非營利組織事務（Processing for not-for-profit organisations）、財產管理（Property management）、金融服務（Provision of financial services and advice）、慈善機構之目標實現（Realising the objectives of a charitable organization or voluntary body）、研究（Research），以及個人資料交易或分享（Trading/sharing in personal information）。

本報告之智慧財產權歸屬於法務部

（2）澳洲

澳洲於 1988 年隱私法(Privacy Act of 1988)中揭櫫適用於澳洲政府機關之資訊隱私原則（Information Privacy Principles, IPPs）與適用於一般私人機構之國家隱私原則[53]（National Privacy Principles, NPPs）。

資訊隱私原則一中規定，聯邦政府機關僅能在有合法目的且蒐集資訊與該目的直接相關時始能為蒐集；原則二則規定，聯邦政府機關向當事人直接蒐集個人資料時，應告知其蒐集目的、法源依據及個人資料利用之對象；原則十另規定，利用個人資料不得逾越蒐集目的範圍。

國家隱私原則 1.1 規定，一般機構僅能在有合法目的且蒐集資訊與該目的直接相關時始能為蒐集;向當事人直接蒐集個人資料時，應確認當事人知悉機構名稱、當事人得行使之權利、蒐集目的、（國家隱私原則 1.3），由此可知一般機構於直接向當事人蒐集個人資料時，應告知當事人機構名稱、當事人得行使之權利、蒐集目的、法源依據、個人資料利用之對象及當事人不提供資料將對其權益之影響。國家隱私原則 2 亦規定，利用個人資料僅限於主要蒐集目的範圍。

由以上可知，資訊隱私原則與國家隱私原則中皆對於告知個人資料當事人特定目的有所要求，惟並未列明特定目的之項目。

（3）美國

美國個人資料保護相關規範散見於各法規中，包括 1974 年隱私法（Privacy Act of 1974）、1996 年醫療保險可攜與責任法（Health Insurance Portability and Accountability Act, HIPAA），以及 1999 年金融服務現代化法（Gramm-Leach-Bliley Act, GLBA），分別規範了聯邦政府機構、醫療機構與金融機構隱私保護相關議題。與歐盟於 2000 年簽署之安全港協定（U.S.-EU

[53] 詳細內容請參見：http://www.privacy.gov.au/materials/types/infosheets/view/6583（Last visited Oct. 24, 2011）。

本報告之智慧財產權歸屬於法務部

Safe Harbor Agreement）中亦提及隱私保護之原則。

1974 年隱私法主要適用於聯邦政府機構，其中 5 U.S.C. § 552a(e)(3)規定，聯邦政府機構於蒐集前，應告知個人資料當事人其蒐集與利用之目的，使當事人知悉。而在 HIPAA 中則要求醫療機構應於隱私通知中載明個人健康資料被利用與揭露之方式。若醫療機構係為診斷、付款、醫療健保營運、公益或研究目的而蒐集個人健康資料，無需取得當事人同意即可利用，惟仍應如前述，於隱私通知中告知當事人其個人資料如何被利用與揭露。

GLBA 中並未對於金融機構於取得當事人個人資料時是否應告知蒐集或處理之特定目的有所規範，惟於其標準隱私通知範本（GLBA model privacy form）當中，列出金融機構應向客戶告知其分享客戶個人資料之原因，包括營業目的（例如交易、維持帳戶資料、通報信用機構等）、行銷目的（例如提供相關產品及服務）、提供關係企業營業目的，以及提供關係企業為行銷。

為因應歐盟之資料保護指令，避免被認定對個人資料保護措施不足（not deemed “adequate”），個人資料之傳送因而受到干擾，美國商務部（Department of Commerce）遂與歐盟執委會（European Commission）共同發展出安全港架構，以確保由歐盟傳送至美國之個人資料不受干擾。其中要求機構必須通知（notify）消費者有關收錄及使用個人資訊之目的，並提供消費者有關請求（inquiries）或抱怨管道之資訊，及對第三者揭露個人資訊之型式、機構賦予第三者使用及揭露個人資訊之選擇（choices）及方式（means）等之資訊。於一般個人資料之情形，機構得對第三者公開揭露當事人之個人資料，亦得將之用於非原始資料蒐集目的，惟必須提供消費者選擇機會（opt out choice），換言之，消費者得明確表示不願意向第三者揭露其個人資料，或要求機構僅得於原始資料蒐集目的範圍內使用其個人資料。至於敏感性資料（sensitive information），當機構擬將資料對第三者揭露或另有用途時，須獲得消費者本人肯定或明確（affirmative or explicit）之同意（opt in choice）始得為之。

本報告之智慧財產權歸屬於法務部

（4）日本

日本個人資料保護法於 2005 年正式施行，規定個人資料處理業者於處理個人資料時，應盡可能特定其利用目的[54]，而處理個人資料時，未經本人事先同意，不得超出為達特定利用目的所必須之範圍[55]。此外，個人資料處理業者於取得個人資料後，除已事先公布其利用目的之情形外，應儘速告知本人其利用目的或予以公布[56]。若個人資料處理業者於與本人締結契約，同時取得契約書及其他書面文件上所載之本人之個人資料，以及取得其他由本人直接記載於書面之個人資料，應事先向本人明示其利用目的[57]。

各目的事業主管機關亦公布適用於其所管轄產業別之指針，例如金融廳訂有金融領域個人資料保護指針，以及厚生勞動省訂定福利關係事業業者合法正當處理個人資料指針、醫療看護關係事業業者合法正當處理個人資料指針、國民健康保險工會合法正當處理個人資料指針，與國民健康保險團體聯合會合法正當處理個人資料指針，提供相關產業遵循個人資料保護法之相關程序與作法，其中亦包含各產業可能涉及之特定目的項目。

以金融產業為例，金融領域個人資料保護指針中即說明金融領域之特定目的應為提供金融商品或服務，至於提供金融商品或服務所指為何，該指針中亦例示數項供金融產業參考，包括接受存款、授信判斷、授信管理、承接保險、支付保險金、本公司及相關公司、合作公司的金融商品、服務的銷售、推銷投保本公司及相關公司、合作公司的保險、本公司內部的市場調查及金融商品、服務的研發、研究、購買特定金融商品、服務時確認購買資格等。

厚生勞動省訂定之福利關係事業業者合法正當處理個人資料指針，則說明福利相關業者之特定目的包括依法令社會福利事

[54] 日本個人資料保護法第 15 條第 1 項。
[55] 日本個人資料保護法第 16 條第 1 項。
[56] 日本個人資料保護法第 18 條第 1 項。
[57] 日本個人資料保護法第 18 條第 2 項前段。

本報告之智慧財產權歸屬於法務部

業者明確記載所應執行之義務[58]、依法令福利關係業者明確記載的任意執行事項[59]，以及為因應行政機關的徵收報告、進入檢查所間接附加之義務[60]等。

厚生勞動省醫療看護指針中則訂有醫療機構之特定目的與看護機構之特定目的。醫療機構之特定目的可包括對病患提供醫療的必要利用目的及其他利用目的，例如醫療機構對病患提供的醫療服務、醫療保險事務、入出院的醫院管理、會計事務、報告醫療事故維護、改善醫療、看護服務及業務的基本資料、協助醫療機構內部所進行學生實習、醫療機構內部所進行病例研究等。看護機構之特定目的則包括對看護使用人提供看護之必要利用目的及其他利用目的，例如該看護機構對受看護人提供的看護服務、看護保險事務、入出所的管理、會計事務、報告事故、有關損害保險香保險公司諮詢或申請、維護、改善看護服務及業務的基本資料、協助看護機構內部所進行學生實習等。

（5）小結

觀察上述各國立法例，英國於 1998 年資料保護法中訂特定目的之規範，原則上資料控管者原則上應向 ICO 登記，登記之項目包括所蒐集之個人資料類別與特定目的，ICO 並於資料保護通知手冊中列舉特定目的與個人資料類別之項目，供資料控管者登記時參考，若無適用之特定目的，資料控管者亦得自行以文字明確描述之。

澳洲則於 1988 年隱私法中 IPP 與 NPP 兩個原則中揭露特定目的之相關規範，包括應告知個人資料當事人蒐集之特定目的、利用個人資料時不得逾越特定目的之範圍，惟澳洲並未於法規或相關指引中訂定特定目的與個人資料類別之項目。

[58] 日本生活保護法第 48 條第 4 項、防止兒童虐待法第 6 條、兒童福利法第 25 條、相關厚生勞動省令等。

[59] 日本生活保護法第 48 條第 2 項、精神保健福利法第 51 條之 4。

[60] 日本社會福利法第 70 條、生活保護法第 44 條 1 項、身障者福利法第 39 條、智能障礙者福利法第 21 條、智能障礙者福利法第 21 條、兒童福利法第 21 條之 15、身障者福利法第 17 條之 15、智能障礙者福利法第 15 條之 15、兒童福利法第 21 條之 15、統計法第 5 條。

本報告之智慧財產權歸屬於法務部

美國 1974 年隱私法、2000 年安全港協議以及 HIPAA 皆有要求資料蒐集者應告知個人資料當事人蒐集或利用個人資料之特定目的，GLBA 則規定金融產業於隱私通知範本說明分享客戶個人資料之原因，但皆未明確訂定特定目的之項目。

日本則於 2005 年個人資料保護法中有特定目的之規範，另由特定事業主管機關訂立相關指針，提供所管轄之產業參考，各產業之個人資料保護指針亦列舉各產業蒐集個人資料時之特定目的。

4.修正方向探討

比較我國電腦處理個人資料保護法與新修正個人資料保護法之規範方向，並參考各國立法例，於以下提出修正現行特定目的與個人資料類別之相關建議。

觀察現行電腦處理個人資料保護法特定目的與個人資料類別之項目，可發現有許多「其他」項目或抽象類別。參酌電腦處理個人資料保護法修正條文對照表之修正說明，第八條關於告知義務之要求，乃為使當事人知其個人資料被何人蒐集及其資料類別、蒐集目的等，而為使當事人了解，告知事項應具體明確，因此若能避免使用「其他」項目或抽象類別，應更容易使當事人理解。此外，由於個人資料保護法施行後適用範圍擴大，涉及之業務眾多，恐無法將可能之特定目的項目全數列出，若無適用之特定目的項目，或許可參考英國之作法，由蒐集個人資料之機關或機構自行填寫，惟我國並未設有類似於英國 ICO 之個人資料保護主管機關，於機關或機構自行填寫之情況，仍需各業別主管機關認定之；另一種可能之方式為參考日本之立法方向，由各目的事業主管機關於個人資料保護法適用指針中訂定該產業別之特定目的與個人資料類別之項目，提供產業依循之方向，此時產業與目的事業主管機關間之協調聯繫機制亦為值得討論之重點。

（六）建置個人資料保護法制研究報告會議紀錄及意見回覆

1.「非公務機關個人資料檔案安全維護計畫標準辦法草案座談會」座談會議紀錄

本報告之智慧財產權歸屬於法務部

日期：2011 年 10 月 14 日上午 9：30 - 12：00

地點：法務部二樓簡報室

紀錄：陳秭璇法律研究員

（1）主要議題：

A. 標準辦法設立之管理組織組成之問題

a.吳永乾教授

簡報中提出，管理組織應包含管理以及內評代表。管理組織中之管理以及內評代表都是督導性質，而組織內卻無設立執行人員，故草案第 4 條（簡報第 5 頁）是否遺漏執行人員？另外，建議使用應採取管理人、稽核人員、監察人為組織之名詞。

b.范姜真媺教授

草案對於管理機構、計畫執行以及管理代表等之職責有重複問題。另外，計劃落實並未規定由誰執行。

c.金管會代表

建議將管理機構訂成一個章節，再做任務編組。

d.銀行公會代表

基本上，實際上銀行產業執行資安制度時，銀行本身就有稽核制度。目前銀行本身之稽核制度是否符合安全維護計畫草案第 3 條內評人員之資格？

本報告之智慧財產權歸屬於法務部

e.資策會蘇柏毓研究員回應

針對第 3 條管理組織之設置，管理代表只是針對管理組織之計畫規劃以及執行，之所以列管理代表，因為實際執行面很多細節，故管理代表只是一個統籌名詞。另外，內評人員也只是組織之主管。用詞部份可以再更改。除此之外，會再修改內部稽核人員職稱之設計，並修正任務連結之問題。

B. 標準辦法所討論之範圍為何?是否包含母法第 27 條第 2 項所授權的業務終止後個人資料處理方法?

a.吳永乾教授

此辦法係依據母法第 27 條第 3 項，但除了安全維護計畫，仍有業務終止的處理辦法。是否應適當於辦法中說明，本安全維護計畫辦法草案相對應母法授權之範圍？

b.經濟部代表

業務終止處理辦法以及個人資料維護計畫之相互性質為何？

c.農委會代表

母法第 27 條對於授權內容，仍包含業務終止之處理辦法，是否應該分別訂立？或者應該合併訂立？

d.法務部鍾瑞蘭副司長

請資策會討論是否加入業務終止辦法

本報告之智慧財產權歸屬於法務部

e.資策會顧振豪組長

原本就是以安全維護計畫為目標，可能要與法務部再討論，決定是否加入業務終止部分。

C. 標準辦法是否需要再度訂立蒐集要件以及告知義務之說明?

a.吳永乾教授

法規遵循程序中關於蒐集要件以及告知義務之說明，是否需要在此辦法再度重複？由於此辦法主要提供具體標準予非公務機關遵循，是否應該聚焦在安全維護措施的法規即可？

b.衛生署代表

依母法第 27 條第 2 項，必須考量授權範圍以制定個人資料檔案安全維護辦法。然而，於法規遵循部份，亦規定蒐集利用個人資料之程序，是否踰越母法所授權之範圍（參照個資法第 27 條第一項，為了防止個人資料竊取、毀損、竄改、滅失或洩漏）？

c.通訊傳播委員會代表

草案的訂定方向應鎖定如何防止資料被洩露或竊取。

D. 標準辦法應以何種方式呈現?

a.吳永乾教授

由於此辦法是提供非公務機關，故應該提供具

本報告之智慧財產權歸屬於法務部

體、細項化的方式呈現。

b.范姜真媺教授

標準辦法若包含特種資料之蒐集處理以及利用，要綱式的規範方法較好。

c.廖緯民教授

草案第 27 以及第 28 條之規定，對於非公務機關可能過於複雜，是否應該採取簡化、要項式的規定方式？但可於說明欄增加說明部份，使非公務機關可清楚了解標準計畫之內容。

d.內政部代表

資策會版本很像公務機關版本法條，屬於原則性的，非公務機關恐怕無力執行。

e.銀行公會代表

草案中有些不是很明確之觀念（例如第 4 條，何謂配置相當資源？），若可以訂立清楚時，請於草案定義。否則業者不知道怎麼遵循。除此之外，標準辦法草案提及風險分析，風險的定義範圍為何？

f.法務部鍾瑞蘭副司長

關於草案中名詞定義問題之問題，此為訂立標準草案的兩難。

g.資策會蘇柏毓研究員

本報告之智慧財產權歸屬於法務部

對於非公務機關標準辦法之性質，依據母法第 27 條之規定，此為範本之性質，特此說明。

E. 標準計畫草案所訂定之法規遵循章節

a.吳永乾教授

個資法第 27 條已規定清楚，其前提為非公務機關已保有個人資料檔案者，故需重新檢視標準計畫草案關於法規遵循部份，部分條文可能與個資法第 27 條之規定衝突。

b.廖緯民教授

針對法規遵循部份，這個部份的名詞可以再討論（以國外立法例為例，法規遵循包含法律面以及資訊安全），法規遵循是否真的要和資安部分切開？是否將資安部分也納進法規遵循章節，可以再考慮一下。

c.資策會蘇柏毓研究員

第三章以及第四章之法規遵循議題，後續會再與法務部長官討論並研議。

F. 中央目的事業主管機關如何選定哪些非公務機關須訂立個人資料檔案安全維護計畫辦法？

a.范姜真媺教授

澳洲以資本額為標準，日本以其 database 能夠識別特定資料（未超過 5000 人）為判斷標準。值得一提的是，日本對於高敏感度個人資料，包含個人信用、醫療、通訊資料，特別進行規範。

本報告之智慧財產權歸屬於法務部

b.廖緯民教授

何謂大量的個人資料？一般碰到母法第 6 條時，一定要指定相關產業，例如醫療、保險、金融、電信、電子商務產業，係一定要指定的業務範圍。

c.經濟部代表

針對母法第 27 條中央機關得指定非公務機關訂立個人資料檔案安全維護計畫，所謂「得指定」之標準為何？建議訂相關標準，提供參考。另外，本辦法草案總說明提到某些產業很重要，但何謂保有大量資料，是否有一定標準？

d.法務部鍾瑞蘭副司長

各中央目的事業主管機關應如何指定非公務機關訂定個人資料檔案安全維護計畫標準辦法，並不在法務部被授權範圍，因此法務部無法提供各目的事業主管機關標準。除此之外，指定產業時，各中央目的事業主管需要考慮產業是否有辦法操作規範。

e.法務部黃荷婷科長

I. 中央機關得指定之標準，必須由各主管機關自行指定，無法由法務部提供認為何產業重要，代替各目的事業主管機關進行指定。

II. 日本針對金融證券、保險、醫療等產業皆訂有特別規定。日本目前之作法為，由個資主管機關定方針後，各部會再去定指導方針，各部會要採取概括性方針或者是選定行業各別訂方針，須由各部會決定。

本報告之智慧財產權歸屬於法務部

（2）其他議題

A. 范姜真媺教授

a.就保有個人資料之性質而言，公務機關以及非公務機關所保有之個人資料性質有很大的差異，此點於公務機關訂立非公務機關個人資料檔案安全維護計畫標準辦法時，須特別注意。

b.草案第 16 條和母法第 6 條第 1 項第 4 款是否能夠契合？此辦法是否包含母法第 6 條特種資料之蒐集以及處理？

c.另外，非公務機關所蒐集的個人資料之性質差異不同，如果以細項規範，會有所困難。除此之外，亦涉及營業自由的問題。

d.直銷部份，草案說明需建立說明、確保首次行銷無須支付費用，但其他國家（日本）是認為，須明白告訴當事人可拒絕直銷，另外需要提供方法、管道以及程序與當事人使用。

e.依據草案第 18 條，如果當事人被拒絕時，當事人有何救濟管道可以行使？

B. 廖緯民教授

a.須確認本草案之性質。其實該草案係法務部提供其他主管機關參考　之文件，故嚴格而言並非法規，而是參考性文件。應改名「標準辦法範本草案」。

b.於目的事業主管指定時，非公務機關需要依循主管機關所訂之辦法訂立其個人資料檔案安全維護計畫標準辦法。若主管機關指定該行業訂立安全維護辦法時，則目的事業主管所制訂之辦法僅屬於輔導性質。

本報告之智慧財產權歸屬於法務部

c.我國新通過之個資法，並未採取絕對不可蒐集之立場，但其基本原則為，如果機關無法採取安全維護計畫時，就不要蒐集數量龐大的個人資料。但如果機關使用大量的個人資料並進行分析、傳輸個人資料時，就必須受到個資法之規範。據此，工協會必須思考，其本身所蒐集之資料之性質、用途，如果很龐大的話，需要仔細思考此範本。

d.另外，辦法草案所提及之教育訓練，對將來若發生法律爭議時，亦有相當之幫助，原因在於，於教育訓練時，非公務機關必須建立完整之文件，而相關文件將可能作為未來法庭上證明之文件。

e.第 26 條稽核規定，係為了外部稽核機制做準備，因為外部稽核才有公信力以及說服力。除此之外，紀錄機制是最重要的，要記錄到什麼程度使非公務機關得證明其已盡善良管理人義務，但要求紀錄之強度又可能牽涉人民之自由，這個部分必須再予參酌。

f.本辦法所採取的負責人核可制，對於非公務機關而言，亦屬於將來發生法律訴訟可使用之有力書面資料。

g.如果主管機關已經指定相關產業須訂立個人資料安全維護辦法後，有些國家的作法並不需要將標準辦法留存各主管機關。僅留存於非公務機關本身，只要以後法律程序時可以提出即可。

h.若不訂立標準辦法，依母法第 48 條以及第 50 條是有相關罰則的。

C. 農委會代表

a.中央目的事業主管機關指定非公務機關後，如何要求非公務機關多須於多久期間內訂立安全維護計畫？另外，

本報告之智慧財產權歸屬於法務部

如何認定非公務機關是否已經訂了標準辦法？

b.若非公務機關已經訂標準辦法，是否需要呈請通知中央目的事業主管機關？

c.針對此問題，法務部鍾瑞蘭副司長說明：此部份需要再與法規會做研議。

D. 法務部鍾瑞蘭副司長

a.若非公務機關受中央目的事業主管之要求應訂立而未訂立個人資料檔案安全維護計畫時，不只是行政規範，亦可能有民事以及刑事問題。

b.會後有意見也可以提供給法務部作參考。

E. 資策會顧振豪組長

各主管機關需自行決定於多久時間內要求非公務機關訂立個人資料檔案安全維護計畫標準辦法。

F. 內政部代表

a.本計劃標準辦法草案必須要對於規範內容清楚劃分，建議以類別式方法區分。

b.由於內容過於龐雜無法進行查核，主管機關對於維護計畫只能備查。

G. 體委會代表

a.是否可設立個資專責團體，做為外部稽核之機關。

b.對於辦法草案中所指之強制委託規定不清楚，亦需要個

本報告之智慧財產權歸屬於法務部

資專責團體之協助。

c.辦法草案是否有建立教育訓練之必要？另外制度如何建立對於非公務機關是有困擾的，此時亦需要個人資料專責人員或機關之協助。

H. 經濟部貿易局代表

草案第 18 條，提到確認當事人身分。是否可進一步說明，若無法確認當事人身分時，應如何處理？

I. 通傳會代表

a.但有些單位不是用電腦，而是使用紙本之方式處理個人資料。故如果非公務機關使用紙本時，如何適用本標準辦法？

b.非公務機關所訂的標準辦法是否需成立自我審查小組，或者由主管機關審查？建議由非公務機關成立自我審查小組。

J. 金管會代表

a.針對本草案第 22 條第 2 款之認證機制，若為紙本處理是否也需要認證機制？

b.草案第 23 條第 5 款應如何進行？第六款，若於移轉前破壞，後續如何移轉個人資料？應再檢視條文文字。

c.草案第 25 條第 3 款，如發生不正常存取之情形時，應該直接拒絕，並保留軌跡。第 5 款，應考慮於一定範圍可共用存取權。

K. 銀行公會

本報告之智慧財產權歸屬於法務部

a.草案第 29 條關於留存紀錄之規定，金融機構的資安部門認為執行有困難。

b.中央目的事業主管機關是否有增訂緩衝期的可能性？

c.非公務機關違反此辦法的法律效果為何？

d.將提供銀行公會之書面意見與法務部參考。

L. 針對以上議題，資策會蘇柏毓研究員回應：

a.針對范姜老師詢問第 16 條之部分是否包含特種資料之問題，依據母法第 6 條第 1 項第 4 款所指之「一定程序」，並不是本草案之範圍。另外，特種資料之一般蒐集利用，則包含在此草案內。故草案中於風險分析時，會對於特種資料進行處理。

b.針對范姜老師詢問關於直銷之問題，對於第 15 條、第 18 條有關於直銷之情形，將針對國外資料研究後進行修正。

c.針對機關詢問草案中所指之紀錄保存，會後將再訂立紀錄保存之期限。

d.另外，確認當事人身分之方式，因為不同行業有不同作法，故可透過非公務機關所保有之其他紀錄作判斷。但須注意的是，仍需由非公務機關決定應如何執行機制。

本報告之智慧財產權歸屬於法務部

2.附錄二：「非公務機關個人資料檔案安全維護計畫標準辦法草案」意見回覆

表 4：「非公務機關個人資料檔案安全維護計畫標準辦法草案」意見回覆表

條文內容	修正建議	意見回覆
第四條　非公務機關為訂定並執行計畫，應建立個人資料檔案安全維護管理組織，並配置相當資源。 前項管理組織之任務如下： 三、規劃、訂定、執行與修訂安全維護計畫相關程序。 四、管理代表應定期向事業之負責人就前款事項提出書面報告。 第一項之管理組織至少應包括個人資料管理代表與個人資料內評代表。	♦ 吳永乾教授： 管理組織中之管理以及內評代表都是督導性質，而組織內卻無設立執行人員，草案第 4 條似乎遺漏執行人員。另建議使用應採取管理人、稽核人員、監察人為組織之名詞。 ♦ 范姜真嫩教授： 草案對於管理機構、計畫執行以及管理代表等之職責有重複問題。另外，計劃落實並未規定由誰執行。 ♦ 金管會： 建議將管理機構訂成一個章節，再做任務編組。 ♦ 銀行公會： 目前銀行業執行資安制度時，本身就有稽核制度。現行銀行之稽核制度是否符合安全維護計畫草案第 3 條內評人員之資格？	管理代表僅針對管理組織之計畫規劃與執行，列管理代表之原因為實際執行面有許多細節，因此事實上管理代表只是一個統籌名詞。另外，內評人員也僅為組織之主管。用詞部份將考慮修改，而對於內部稽核人員職稱之設計，將配合個資法相關規範整體調整，並須確認任相關資安管理標準，方可完成相關修正。
參、法令遵循程序 肆、安全管理措施	♦ 吳永乾教授： 個資法第 27 條已規定清楚，其前提為非公務機關已保有個人資料檔案者，	♦ 本辦法草案章節架構之調整，需配合個資法相關規範整體調整，並確認任相關資安管理標準，方

本報告之智慧財產權歸屬於法務部

條文內容	修正建議	意見回覆
	故需重新檢視標準計畫草案關於法規遵循部份，部分條文可能與個資法第 27 條之規定衝突。 ♦ 廖緯民教授： 針對法規遵循部份，此部份名詞建議可再討論（以國外立法例為例，法規遵循包含法律面以及資訊安全），法規遵循是否要與資安部分切開？是否將資安部分一併納入法規遵循章節，可再考慮。 ♦ 通訊傳播委員會： 有些單位不是用電腦，而是使用紙本之方式處理個人資料。若非公務機關使用紙本時，應如何適用本標準辦法？ ♦ 金管會： 草案第 22 條第 2 款之認證機制，若為紙本處理是否也需要認證機制？	可完成相關修正。 ♦ 本辦法草案事實上已包含紙本資料之安全管理措施，例如人員管理之措施，無論是電腦處理或紙本處理之個人資料皆可適用；惟草案第 25 條為針對利用電腦或相關設備蒐集、處理或利用個人資料時所應採取之技術管理措施，僅於以電腦處理個人資料時始有適用。
第十六條　非公務機關針對本法第六條之特種個人資料，應就下列事項建立相關程序： 三、確認所蒐集、處理及利用之個人資料是否包含特種個人資料。 四、確保蒐集、處理及利用特種個人資	♦ 范姜真媺教授： 草案第 16 條和母法第 6 條第 1 項第 4 款是否能夠契合？此辦法是否包含母法第 6 條特種資料之蒐集以及處理？	依據母法第 6 條第 1 項第 4 款所指之「一定程序」，並非本草案之範圍。惟特種資料之一般蒐集、處理或利用則包含在此草案內。故草案中於風險分析時，會對於特種資料進行處理。

本報告之智慧財產權歸屬於法務部

條文內容	修正建議	意見回覆
料，符合相關法令之要求。		
第十八條　非公務機關為提供資料當事人行使個人資料保護法第三條所規定之權利，應就下列事項建立相關程序： 五、如何提供當事人行使權利。 六、確認當事人身分。 七、確認是否有本法第十條及第十一條得拒絕當事人行使權利之情況。 八、適時回覆當事人請求。	♦ 范姜真嫩教授： 依據草案第 18 條，如果當事人被拒絕時，當事人有何救濟管道可以行使？ ♦ 經濟部貿易局： 草案第 18 條提到確認當事人身分。若無法確認當事人身分時，應如何處理？	♦ 當事人被拒絕，若為合法拒絕，則無救濟之問題；若為非法拒絕，或當事人認為是非法拒絕，依據母法僅得透過民事訴訟或行政救濟流程為之。至於非公務機關，本需建立相關部門提供申訴或當事人之權利行使。若此處所指之救濟為相關申訴或諮詢的話，則應由該部門為之。 ♦ 確認當事人身分之方式應為操作細節，應無須於安全計畫中呈現。

資料來源：本計畫自行整理

3.「非公務機關個人資料檔案安全維護計畫標準辦法草案」座談會簽到表（因簽到表內含有參與人員之個人資料，故在此予以移除，詳細簽到資料已附於呈繳法務部之「建置個人資料保護法制研究報告」）。

本報告之智慧財產權歸屬於法務部

4.「公務機關或學術研究機構基於醫療衛生或犯罪預防目的蒐集、處理或利用特種個人資料辦法草案」座談會議紀錄

日期：2011 年 10 月 31 日上午 10：00 – 12：00

地點：政大公企中心 C705 會議室

紀錄：郭俊仁研究助理

（1）主要議題：

A. 設置倫理委員會之必要性

a.范姜真媺教授

規模較小的機構，是否有能力成立倫理委員會？是否可以採取較為彈性的方式而作處理。例如，各機構間聯合成立一個倫理委員會，抑或得否委託其他機構所成立的委員會加以審查。另外，倫理委員會散佈於各機構，是否能發揮其功能？

b.陳銘雄教授

醫學期刊刊登時應經過 IRB 審查的証明，這已是醫學界的慣例，但我們現在討論到的醫療資訊可能是由非醫學人員蒐集處理，刊登在非醫學期刊，其對於這個議題的重視及了解可能還不夠周全，是否可以考慮將期刊刊登時應經過 IRB 審查予以明文化？當然在法規位階上是否可以來處理是另一個問題，不過從精神上來看，非醫療期刊刊登有關醫療研究時，如果用這種方式來保護應該會更為周到。

關於倫理委員會之設置地點，考量到間接蒐集之態樣，例如說健保局的人員於某研究所就讀，撰

本報告之智慧財產權歸屬於法務部

寫論文時引用健保局資訊，而這些資訊並非由這位健保局的人員自行蒐集，而是由健保局，這邊倫理委員會的設置與功能是否較偏向直接面對當事人才有適用？

c.周道君視察

以倫理委員會管理是一個比較高密度管制之情形，因為風險較高，現在醫療法規裡對於人體試驗有倫理委員會審查之要求，不過在研究的部份，有的機構會設置 IRB，但有的機構並不會設置，因此有聯合 IRB（稱為 JIRB）的產生，也就是數個機構聯合去設置一個聯合的審查委員會，當自己的機構沒有設置 IRB 時，就可以送到聯合審查委員會審理。未來因應個人資料保護要設置倫理委員會，可能也需要類似的彈性措施。否則可能發生較小型的學術研究機構沒有能力成立審查委員會之情形。

公務機關是否一定要成立倫理委員會？在學術研究領域可能已經有經過倫理委員會審查的習慣，不過對於公務機關而言並沒有這種習慣，公務機關似乎不太一定要成立倫理委員會，是否有其他機制可處理？

d.董玉芸科長

草案第 6 條第 5 項關於統計或研究計畫終止時應向倫理委員會通知其原因，是否也應考量向主管機關核備？

B. 個人資料保護法第 6 條第 1 項第 1、2、3 款與第 4 款之適用關係

本報告之智慧財產權歸屬於法務部

a.范姜真媺教授

個人資料保護法第六條第一項各款之間的適用關係？例如同時符合第一項第二款及第四款時，是適用第一款而可以蒐集？或是需按照第四款而進入第六條第二項之審查？

b.廖緯民教授

第六條第一項規定不夠明確，造成這四款之間的適用有所疑問，也是我們討論所應注意的一個重點。

c.陳錡雄教授

第六條第一項之間的關係，既然第二項規定只有第一項第四款適用之，我想就應該限縮，而在第一項前三款等情形，其實就應該不需要適用第四款的規定。

C. 學術研究機構範圍之界定

a.陳錡雄教授

對於學術機構的定義，是否能夠授權主管機關來自行定義？

b.周道君視察

學術研究機構應如何定義，其範圍界定究應多廣？能否先請行政機關就此先做出定義。

c.胡美蓁編審

本報告之智慧財產權歸屬於法務部

對於學術機構的範圍做出定義，事實上有其難度，過猶不及，目前的作法是不嘗試去作定義，而是讓主管機關依照個案情形而分別作認定。

（2）其它綜合討論

A. 范姜真嫩教授

a.日本就個人資料的保護，依照各式各樣的目的而作區分，並依照不同的個人資料而作不同的規範，以學術研究目的為例，若有違背，則不能將該研究結果刊登於期刊，此種分別規範以及違背的後果，值得我國參考。

b.辦法草案第 12 條限制當事人權利行使似乎與母法第 3 條有所衝突。

B. 廖緯民教授

a.母法本身對於醫療、健康檢查等之定義似乎不夠明確，舉例而言，病歷、敏感資料、健保財務資料等，是否包含在內？

b.辦法草案整體法規範偏向靜態性的審查，可參考德國法制中，對於資訊安全設備的部份會要求各機構實際進行測試，藉此，亦可以進一步提昇個人資料保護的標準。

C. 陳錡雄教授

a.若是透過間接蒐集的方式而取得資料，由於不會接觸到當事人，此時應如何按照辦法草案第八條而遵行告知義務？

b.辦法草案所稱編碼、加密、去連結化，係指於蒐集過程中，抑或得出研究成果時所應採取之動作？

本報告之智慧財產權歸屬於法務部

c.第六條第四款是為了特殊目的而為之，例如以學術研究為目的而蒐集資料，若過度要求程序，可能有礙於學術的發展。

D. 王榮濱理事

研究與臨床應當並重，就特定的法定傳染病，例如 HIV、TB 等，由於必須列入保密，然而對於臨床人源於接觸該等病患時、若無法得知相關資訊，對於第一線的醫療人員的保障將有所損害。

E. 羅惠玲律師

保險業者基於風險的考量，會委由保發中心進行投保人個人資料的收集，此一部份，可能比較偏向於第六條第二項中關於犯罪（保險詐欺）的研究，而進行特種資料的蒐集。

F. 徐建業理事長

a.目前法規對於醫療資訊並沒有針對不同的資訊，而作不同強度的規範，例如，基因、檢體、或病人平時服用的藥物等，應當予以區分而作不同強度的規範。

b.若依照辦法草案所規劃而成立倫理審查委員會，將使各機構的成本提高，就實際層面而言，將造成執行上的困難。

G. 周道君視察

a.草案第六條中，對於統計或研究計畫中止或終止時，僅需向倫理委員會通知其原因，以及統計或研究情形。然而，對於終止後的個人資料，亦應當同受保障,，而受倫理委員會審查，例如終止後對個人資料的處置以及後續如何保護等，也應當有相當之審查程序。

本報告之智慧財產權歸屬於法務部

b.草案第十五條第十六條中的安全與控管措施，似乎僅針對電腦資訊處理的部份，建議應將紙本的資料一同列入控管。

c.關於醫療、健康檢查、病歷等定義，衛生署目前正在研議中，未來將續送法務部審核。

d.本辦法草案第十三條與施行細則第八條是否有重複規定？

5.「公務機關或學術研究機構基於醫療衛生或犯罪預防目的蒐集、處理或利用特種個人資料辦法草案」修正說明

表 5：「公務機關或學術研究機構基於醫療衛生或犯罪預防目的蒐集、處理或利用特種個人資料辦法草案」修正說明表

條文內容	說明	修正參考
第四條（倫理委員會之審查） 醫療、基因、性生活、健康檢查或犯罪前科資料之蒐集、處理或利用，應擬定計畫書，經由倫理委員會審查。但主管機關得考量研究或統計執行之性質、（學術研究）機構之規模，訂定其他審查程序。 前項計畫書內容應包含統計或研究規劃、計畫主持人之最新履歷、蒐集、處理或利用個人資料之範圍與程序、採取之安全措施，若有委託之情形，與受委託單位之約定。	為確保公務機關或學術研究機構確為統計或學術研究而有必要進行特種資料之蒐集、處理或利用，規定於事前應先擬定相關計畫書，經倫理委員會審查通過並報主管機關備查。惟考量研究或統計執行之性質、機構之規模與業務量，對於部分小型學術研究機構而言，獨立設置倫理委員會可能將大幅增加其負擔，爰於第一項但書規定得由主管機關訂定其他審查程序。	依范姜真媺教授、周道君視察就設置倫理委員會之必要性之意見補充說明。 ♦ 范姜真媺教授： 規模較小的機構，是否有能力成立倫理委員會？是否可以採取較為彈性的方式而作處理。例如，各機構間聯合成立一個倫理委員會，抑或得否委託其他機構所成立的委員會加以審查。另外，倫理委員會散佈於各機構，是否能發揮其功能？ ♦ 周道君視察： 以倫理委員會管理是一個比較高密度管制之情形，

本報告之智慧財產權歸屬於法務部

條文內容	說明	修正參考
第一項個人資料之蒐集、處理或利用經倫理委員會審查通過後，應報主管機關備查後始得為之。		因為風險較高，現在醫療法規裡對於人體試驗有倫理委員會審查之要求，不過在研究的部份，有的機構會設置 IRB，但有的機構並不會設置，因此有聯合 IRB（稱為 JIRB）的產生，也就是數個機構聯合去設置一個聯合的審查委員會，當自己的機構沒有設置 IRB 時，就可以送到聯合審查委員會審理。未來因應個人資料保護要設置倫理委員會，可能也需要類似的彈性措施。否則可能發生較小型的學術研究機構沒有能力成立審查委員會之情形。
第六條（倫理委員會之監督與管理） 倫理委員會應建立監督機制，追蹤審查經核准統計或研究計畫之執行情形與進度。 倫理委員會為執行監督，應於決定書載明與計畫主持人間之持續溝通方式。 追蹤審查應辦理下列事項： 三、訂定追蹤審查之委員人數及審查程序。 四、依計畫特性訂定追蹤審查之期間，每	為確保公務機關或學術研究機構依倫理委員會審查通過之計畫而為特種資料之搜集、處理或利用，爰參考我國醫療機構人體試驗委員會組織及作業基準第五章，規定倫理委員會應對於所審核之計畫為監督管理，並應遵循相關程序。	依董玉芸科長及周道君視察之建議修正。 ♦ 董玉芸科長： 草案第 6 條第 5 項關於統計或研究計畫終止時應向倫理委員會通知其原因，是否也應考量向主管機關核備？ ♦ 周道君視察： 草案第六條中，對於統計或研究計畫中止或終止時，僅需向倫理委員會通知其原因，以及統計或研究情形。然而，對於終止後的個人資料，亦應當同

本報告之智慧財產權歸屬於法務部

條文內容	說明	修正參考
年不得少於一次。 追蹤審查之決定應通知計畫主持人，並載明原決定之變更、中止或終止，或確認原決定仍然有效。 統計或研究計畫中止或終止時，應向倫理委員會通知其原因，以及統計或研究情形，並報經主管機關核備。 統計或研究計畫完成時，應將執行情形及結果以書面通知倫理委員會，並報經主管機關核備。		受保障,，而受倫理委員會審查，例如終止後對個人資料的處置以及後續如何保護等，也應當有相當之審查程序。
第八條（告知義務） 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，向當事人蒐集有關醫療、基因、性生活、健康檢查或犯罪前科之個人資料時，應明確告知當事人下列事項： 七、公務機關或學術研究機構名稱。 八、蒐集之目的。 九、個人資料之類別。 十、個人資料利用之期間、地區、對象及方式。 十一、當事人依本法第三條規定得行使之權利及方式。	三、特種個人資料之性質較為特殊或具敏感性，如任意蒐集、處理或利用，恐會造成社會不安或對當事人造成難以彌補之傷害。為使當事人明知其個人資料被何人蒐集及其資料類別、蒐集目的等，爰於第一項規定蒐集時應告知當事人之事項，俾使當事人能知悉其個人資料被他人蒐集之情形。另考量間接蒐集之情形，亦規定公務機關或學術研究機構於處理或利用前，向當事人為告知，惟已經處理而無從識別特	陳錡雄教授、徐建業理事長及周道君視察均建議增加間接蒐集樣態時之告知義務，爰依建議修正。 ♦ 陳錡雄教授： 若是透過間接蒐集的方式而取得資料，由於不會接觸到當事人，此時應如何按照辦法草案第八條而遵行告知義務？ ♦ 徐建業理事長： 辦法草案第八條對於間接蒐集時之告知義務並無規定。 ♦ 周道君視察： 間接蒐集時是否有告知義務之要求應予考量。

本報告之智慧財產權歸屬於法務部

條文內容	說明	修正參考
十二、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。 公務機關或學術研究機構蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告之個人資料來源及前項所列事項，但經處理而無從識別特定當事人者，不在此限。 前二項所稱告知，應以當事人易於理解之方式為之。	定當事人之資料，對於當事人權益應無影響，爰於第二項但書規定得無須踐行告知義務之情形。 四、統計或研究計畫可能涉及專業術語，為使當事人了解其個人資料被蒐集之用途，爰規定公務機關或學術研究機構應以一般人能理解之方式為告知。	
第十三條（委託蒐集、處理或利用） 公務機關或學術研究機構依委託他人蒐集、處理或利用個人資料之全部或一部時， 應依相關法令為之，並將法令要求事項載明於與第三人簽訂之書面契約中。 ~~三、委託人及受託人之責任。~~ ~~四、個人資料之安全管理相關事項。~~ ~~五、再委託之相關事項。~~ ~~六、向委託人報告關於個人資料處理狀況之內容以及報告週期。~~	為避免受委託之第三人對於當事人之特種個人資料有濫用或使用不當之情形，爰規定委託人應盡其選任與監督受託人之責，並於委託契約中載明特定事項，以保護當事人之權益。	依周道君視察之建議刪除與施行細則草案重複規定之處，惟考量特種資料之蒐集、處理與利用應予以更為嚴格之保護，仍保留「將相關法令要求監督項目載明於與第三人簽訂之書面契約」，以及「書面契約之保留期間應至少與個人資料保存期間一致」部分。 ♦周道君視察： 辦法草案第十三條與施行細則草案（預告版）是否有重複規定之必要？

本報告之智慧財產權歸屬於法務部

條文內容	說明	修正參考
~~七、委託人可確認受託人已有遵守契約內容之事項。~~ ~~八、未遵守契約內容時之措施。~~ ~~九、發生事故時之報告及聯絡等相關事項。~~ ~~十、受託者個人資料教育訓練。~~ ~~十一、受委託者之保密義務~~ 公務機關或學術研究機構就該書面契約之保存期間，至少應與個人資料之保存期間一致。		

資料來源：本計畫自行整理

6.「公務機關或學術研究機構基於醫療衛生或犯罪預防目的蒐集、處理或利用特種個人資料辦法草案」座談會簽到表（因簽到表內含有參與人員之個人資料，故在此予以移除，詳細簽到資料已附於呈繳法務部之「建置個人資料保護法制研究報告」)。

7.「個人資料特定目的暨個人資料類別修正座談會」座談會議紀錄

日期：2011 年 8 月 30 日上午 9：30 - 12：00

地點：法務部二樓簡報室

紀錄：許耀庭 研究助理

（1）針對「指定特定目的與個人資料類別項目是否仍有必要」

A. 范姜真媺教授

本報告之智慧財產權歸屬於法務部

a.因為現在沒有登記制度，而「特定目的」就是為了登記制度而來，既然現在沒有登記制度，就沒有規定的必要。個資法第 53 條不可行。

b.日本個資法未擴及一般個人，僅限定在業者；被蒐集資料的個人與業者之間是私法自治的範圍，國家不應介入；既然個人要提供資料給業者，就是合意之所在，是一種交易的風險，被蒐集資料的個人就應該要評估，如果特定目的是有問題的，被蒐集資料的個人可以要求業者停止利用。日本認為，特定目的的問題應該在後階段處理，而不是在一開始就規定什麼是特定目的。

B. 廖緯民教授

a.認同「特定目的」的制度，政府應該公布，並且要精確化，甚至提供更多的資訊服務。

b.認為登記制度並沒有消失：個資法第 53 條明文規定，且第 8 條要求公務機關或非公務機關向當事人蒐集個人資料時，應明確告知當事人蒐集之目的、第 27 條中央目的事業主管機關得指定非公務機關必須要申報。

c.蒐集的目的範圍如何，反應安全維護義務高低，「特地目的」精確化做的越好，各產業在法院裡賠錢的機會就越小。

d.產業蒐集個人資料，若沒有特定目的或是特定目的過於廣泛，就可能有違法之虞。法院審查順序：

I.先看「是什麼特別目的」(目的拘束性)：因為這個目的而可以蒐集個人資料蒐集、使用、維護到什麼程度。

II.蒐集資料是否容許？

本報告之智慧財產權歸屬於法務部

III.蒐集此資料是否必要？

IV.當事人知不知道你蒐集這些資料是做什麼？(透明性)

V.如何維護？

C. 資策會科法所科應中心顧振豪組長

特定目的確實有其必要性。

(2) 針對「特定目的項目與個人資料類別應具體明確，並應避免使用『其他』」

A. 范姜真媺教授

日本的「其他」概括條款，因是規範業者，因此至少可以對應回章程裡登記的「營業項目」的範圍。

B. 吳永乾教授

特定目的和個人資料的分類，本來就有先天上的困難，因此「其他」的類別恐怕是不得不的作法；但是對「其他」可以有審查機制，當選擇其他敘述時，應要明確，且要不能逾越該機關的職能或是設立目的

C. 法務部黃荷婷科長

「電腦處理個人資料保護法之特定目的」第 93 項以後規定的「其他」其實有一定的範圍，像是產業的部份就一定要在「營業項目、章程鎖定的範圍內」去訂特定目的；但是畢竟「其他」還是很抽象，是不是可能有新的特定目的公告，平衡產業的需要及消費者的保護，或是仍然訂「其他」交給交易的雙方去決定最後由法院去判斷等，也是其中一個選項。

本報告之智慧財產權歸屬於法務部

D. 資策會科法所科應中心顧振豪組長

「電腦處理個人資料保護法之特定目的」第 93 項以後的「其他」是否可能有類型化區分的說明，在一定的要件、範圍內，在做更細緻化的規範。

（3）針對「電腦處理個人資料保護法之特定目的」修正

A. 法務部法律事務司鍾瑞蘭副司長、法務部林秀蓮參事

應修正，不合時宜。

B. 吳永乾教授

a.個人資料特定目的或個人資料類別的指定，是需要由各目的事業主管機關做一個界定，再提出於法務部。

b.就特定類別的指定應區分：

I.公務機關：依其「法定職掌」有關

II.非公務機關：由目的事業主管機關，就經管的行業的個別特色或是公司章程、財團或社團的設立目的，作基本的指針，再作具體的分類。至於

c.個人資料的分類，因其處理規定不同，應分為一般及特殊敏感性資料。

C. 范姜真媺教授

a.太多東西很抽象，有諸多問題：

I.是例示還是列舉？

II.在登記時，可以登記一項、兩項，還是可以把所有的

本報告之智慧財產權歸屬於法務部

項目都登記進去？

III.登記之後，可以變更嗎？日本法規定可以變更，我們以前沒有現在有，那要如何處理變更呢？

b.非公務機關（業者），其特定目的的指定應區分為：

I.勞工個資管裡：健康、薪資等

II.提供服務對象（顧客）：可以依各行業與顧客的接觸，以提供的服務作出綱要、列出項目。

8.「個人資料特定目的暨個人資料類別修正座談會」座談會簽到表（因簽到表內含有參與人員之個人資料，故在此予以移除，詳細簽到資料已附於呈繳法務部之「建置個人資料保護法制研究報告」）。

二、政策說帖

（一）前言

本政策說帖之內容主要為金融、醫療與電信產業之隱私保護議題、非公務機關個人資料檔案安全維護計畫標準辦法草案以及公務機關或學術研究機構基於醫療衛生或犯罪預防目的蒐集、處理或利用特種個人資料辦法草案。

我國前年五月（民國 99 年 05 月）通過個人資料保護法（以下簡稱個資法）後，其適用範圍擴張，並課予資料蒐集者告知義務，勢必造成產業適用上之衝擊，因此於本政策說帖中，將探討金融、醫療與電信產業之隱私保護議題，並提供法規遵循方向建議。此外，個資法第 27 條授權中央目的事業主管機關得指定保有大量且重要個人資料檔案之非公務機關，訂定個人資料檔案安全維護計畫。據此，目的事業主管機關須訂定個人資料檔案安全維護計畫標準辦法，供受指定之產業可遵循；而個資法第 6 條第 2 項授權中央目的事業主管機關須會同法務部訂立特種個人資料蒐集、處理或利用之範圍、

本報告之智慧財產權歸屬於法務部

程序及其他遵行事項之辦法，本辦法將針對公務機關或學術研究基於特定目的而蒐集、處理或利用醫療、基因、性生活、健康檢查及犯罪前科等個人資料之情形，訂立應遵行程序。本政策說帖除了說明兩個草案之要旨外，亦將附上草案之範本以供參考。

（二）金融、醫療與電信產業之隱私保護議題

1.金融產業隱私保護議題

隨著資訊科技之發展，個人資料之流通較以往更為普遍而迅速，對大多數現代人而言，銀行帳號、金融卡、信用卡及保險單等金融服務或商品已成為生活中不可或缺之一部分，而當消費者欲申請上述服務或商品時，需提供諸如姓名、地址、電話、身分證字號、薪資所得、信用紀錄等個人資料，甚至有時需提供第三人資料（例如保證人），因此，金融機構將取得許多消費者之個人資料，而其如何使用、處理及保護眾多個人資料，也成為消費者相當關注的議題。

金融隱私（financial privacy）係指個人控制、蒐集、揭露和使用關於其金融交易事務的權利，換言之，個人有權要求其交易相對人（金融機構）在金融領域（包含銀行、證券、保險）之交易中，不得任意透露或不當使用其個人相關資訊。我國對於個人資料之蒐集、使用、處理或分享之法律規範，主要為電腦處理個人資料保護法（於個人資料保護法正式施行後則為個人資料保護法），為一般原則性之規定，而針對金融方面之個人資料保護，則散見於各金融法規。現行電腦處理個人資料保護法（以下稱「個資法」）第 3 條第 7 款將金融業、證券業及保險業列為適用個資法非公務機關相關規定之行業別，並且針對金融業、證券業及保險業訂立「金融業申請電腦處理個人資料登記程序許可要件及收費標準」、「個人資料檔案維護計畫標準」及「接受個人資料查詢閱覽製給複製本之程序與收費標準」，其中於「金融業申請電腦處理個人資料登記程序許可要件及收費標準」中明確說明金融業、證券業及保險業之範圍。至於其他金融法規中關於金融隱私之相關規定，於以下分述之：

（1）金融控股公司法

本報告之智慧財產權歸屬於法務部

金融控股公司法第 42 條規定:「金融控股公司及其子公司對於客戶個人資料、往來交易資料及其他相關資料,除其他法律或主管機關另有規定者外,應保守秘密。主管機關得令金融控股公司及其子公司就前項應保守秘密之資料訂定相關之書面保密措施,並以公告、網際網路或主管機關指定之方式,揭露保密措施之重要事項。」同法第 43 條第 1 項及第 2 項則規定:「金融控股公司之子公司間進行共同行銷,應由金融控股公司事先向主管機關申請核准,且不得有損害其客戶權益之行為。金融控股公司之子公司間進行共同行銷,其營業、業務人員及服務項目應使客戶易於識別。共同使用客戶資料時,除個人基本資料外,其往來交易資料及其他相關資料,應先經客戶書面同意,且不得為使用目的範圍外之蒐集或利用;客戶通知不得繼續共同使用其個人基本資料、往來交易資料或其他相關資料時,應即停止共同用。」由以上可知,金融控股公司及其子公司之間得共同使用客戶之個人基本資料,但於共同使用客戶之交易資料及其他相關資料前,必須取得客戶之書面同意始可為之。

金融控股公司法亦規定,有關申請核准共同行銷之應具備之條件、應檢附之書件、申請程序、可從事之業務範圍、資訊交互運用、共用設備、場所或人員之管理,及其他應遵行事項之辦法,應由主管機關訂定之。金管會據此於 2009 年 10 月 21 日頒布「金融控股公司子公司間共同行銷管理辦法」,以規範金融控股公司子公司間之共同行銷行為,並確保客戶權益。該辦法所稱之「共同行銷」,係指同一金融控股公司之子公司,在其營業場所辦理銀行、證券、期貨及保險等同一金融控股公司之子公司之一定範圍之業務。金融控股公司之子公司間進行共同行銷時,其營業、業務人員及服務項目應使客戶易於識別,並應依該辦法所定之各相關規定辦理。

同一金融控股公司之子公司間依使用目的,得交互運用其客戶資料進行行銷。此客戶資料係指金融控股公司子公司客戶之基本資料、往來交易資料及其他相關資料。其中基本資料包括姓名、出生年月日、身分證統一編號、電話及地址等資料;而往來交易資料及其他相關資料,則包括帳務資料、信用資料、投資資

本報告之智慧財產權歸屬於法務部

料及保險資料。

金融控股公司之各子公司根據其與客戶之往來契約，除了有關客戶資料之使用條款，應訂定讓客戶選擇是否同意提供往來交易資料或其他相關資料，作為行銷建檔、揭露、轉介或交互運用之欄位及簽名處，並應列明其將運用資料之子公司名稱，供客戶勾選與簽名之外，並且應該明確地告知或約定客戶得隨時要求停止對其相關資訊交互運用之簡易方式（例如：提供專線電話號碼，以方便客戶通知）。

金融控股公司之子公司間交互運用客戶資料進行共同行銷時，不得為使用目的範圍外之蒐集或利用。金融控股公司之子公司於接獲客戶通知，請求停止不得繼續共同使用其個人基本資料、往來交易資料或其他相關資料時後，應立即停止金融控股公司及其所有子公司間相互使用該客戶資料。

金融控股公司之子公司與客戶訂立之既有往來契約，於終止該業務往來契約時(例如信用卡剪卡、結清存款帳戶等情形)，金融控股公司及其所有子公司間均 不得再繼續使用該客戶之資料進行行銷。但若經客戶書面同意繼續提供基本資料、往來交易資料或其他相關資料作為行銷使用者，不在此限。

（2）金融控股公司及其子公司自律規範

依據金融控股公司法第 43 條第 2 項之授權，由銀行公會訂定之「金融控股公司及其子公司自律規範」中明定金融控股公司與其子公司應向客戶揭露保密措施，包括資料蒐集方式、資料儲存及保管方式、資料利用目的、客戶資料變更修改方式及行使退出選擇權之方式等。而揭露保密措施及修訂內容除應以書面或電子郵件通知客戶，亦應於公司網頁、營業處所、大眾媒體等公告之。

（3）銀行法

銀行法第 48 條第 2 項規定，銀行對於客戶之存款、放款或

本報告之智慧財產權歸屬於法務部

匯款等有關資料，除法律另有規定外，原則上應保守秘密。違反第 48 條之規定者，依同法第 129 條第 11 款得處二百萬元以上、一千萬元以上罰鍰。

（4）票券商金融管理法

票券商金融管理法第 25 條規定，票券商辦理營業所需業務時，對於顧客之財務、業務或交易有關資料負保密義務。違反規定者得處新台幣五十萬元以上二百五十萬元以下之罰鍰。

（5）金管會函釋

金融監督管理委員會對於金融控股公司交互運用客戶資料於 93 年 11 月 19 日金管銀（六）字第 0936000587 號函規定，金融控股公司之子公司依據金融控股公司法第43條及第48條交互運用客戶資料進行共同行銷時，應於與客戶之往來契約中，增訂讓客戶選擇是否同意提供資料作為共同行銷建檔、揭露、轉介或交互運用之欄位及簽名處，簽名處應能明確區分僅同意提供基本資料（包括姓名、出生年月日、身分證統一編號、電話及地址等）或同意提供帳務、信用、投資及保險等其他資料，且應以黑字體提醒客戶注意，另需告知或約定客戶得隨時要求停止對其相關資訊交互運用之最簡易方式，並於接獲客戶通知停止使用其資料後，立即依其通知辦理。

綜上所述，現行金融法規中關於金融隱私相關之規範，主要在於共同行銷之資訊共享、金融機構通知客戶其個人資料蒐集與運用，以及政府或執法機關向金融機構要求提供客戶財務資料之情形。就共同行銷之資料共享方面而言，我國相關法令皆規定金融機構對客戶之個人資料或交易相關資料負有保密義務；金融控股公司與其子公司得共同使用客戶個人資料，但使用客戶之交易資料及其他資料時必須取得客戶書面同意始可為之。而針對金融機構通知客戶個人資料蒐集與運用方面，除在個資法中有所要求之外，於金融控股公司及其子公司自律規範中亦要求金融控股公司之揭露或保密措施及其修訂內容應以書面或電子郵件方式通

本報告之智慧財產權歸屬於法務部

知客戶，或於公司網頁等媒體公告之。至於政府或執法機關基於行政及司法調查之需要，而向金融機構要求提供客戶資料之情形，政府機關僅得於特定情況下透過金融機構取得客戶交易資料，惟政府機關於取得客戶交易資料時，並無通知客戶之義務。不過，值得注意的是，新修訂之個人資料保護法第 9 條已對此作出規範，規定機關於蒐集非由當事人提供之個人資料時應於處理或利用前告知當事人。

未來個人資料保護法正式施行後，原則上金融產業仍需遵循個人資料保護法之相關規範，而在金融法規有特別規定之情形，始適用該特別規定。從規範面而言，主管機關應檢視現行相關金融法規與個人資料保護法之相異規範外，同時也應針對金融產業較具特殊性之部分訂立相關規範；產業則應瞭解目前由客戶提供資料情形、適時歸納並配合修訂相關表格、修正蒐集、處理或利用個資之告知方式，以及客戶同意書類例稿。

2.醫療產業之隱私保護議題

除了前述金融產業有隱私保護之議題外，醫療產業亦屬須處理大量個人資料之產業（尤其是敏感性資料）。由於醫療產業本身之特性，醫療行為需要當事人提供其個人資料，始能進行醫療服務。一般民眾的醫療資訊內容包括基本資料，例如姓名、性別、出生日期、身分證字號、通訊地址、電話、病歷號碼等；就醫記錄，例如看診科別、掛號日期、診治醫生等；檢驗報告，例如檢查項目與報告、病理檢驗報告等。

醫療資訊被認為是重要的隱私資訊，對病患而言，其所罹患的疾病或健康狀態等資訊，若被不當外洩，可能將造成其工作、交友、結婚、保險等權利受到重大影響，對於其個人身心、名譽與權益亦可能產生傷害。除此之外，醫療資訊的正確與完整性，涉及病患的生命安全，若醫療資訊受到不當竄改，或是因人為疏失造成資訊錯誤，將可能導致診斷錯誤或其他重大醫療事件發生。因此，保護醫療資訊之意義在於維護當事人隱私與權益，並提供適當且正確的醫療服務。現行個資法第 3 條第 7 款將醫院列為適用個資法非公務機關相關規定之行

本報告之智慧財產權歸屬於法務部

業別，其他醫療隱私相關規範，於以下分述之：

（1）醫師法與醫療法

醫師法第 23 條要求醫師對病人的病歷資訊，負有保密的義務，非經合法的程序不得無故洩漏之。若有違反，不僅要面臨損害賠償的求償，同時也將面臨刑法的責任。另外，依據醫療法第 72 條之規定，其他參與醫療的醫療機構以及其人員，也負有同樣的保密義務，若醫療單位違反其保密義務，主管機關可處一萬元以上五萬元以下罰鍰，如未改善得連續罰緩[61]；此外，醫療法為了保護病人的醫療資訊使用接近權(right to access)，特別明文規定醫療機構提供病歷副本的義務[62]。

（2）醫療機構電子病歷製作及管理辦法

由於病歷電子化能帶來相當大的效益，衛生署持續推行電子病歷的計畫，惟病歷電子化後，將對以往病歷保管的規定產生衝擊，甚至產生無法適用的結果，因此衛生署於 2005 年，基於醫療法第 69 條之授權，制定「醫療機構電子病歷製作及管理辦法」，規定相關電子病歷的實施辦法，其中即規定應就病歷所有的電子活動進行紀錄，並要求病歷資訊系統之建置應符合特定項目，以維護資訊應用的透明性[63]。

（3）個人資料保護法相關規定

我國現行個資法就資料蒐集、處理及利用的單位區分為公務機關與非公務機關，據此適用不同的管制藍圖。依現行個資法之規定，醫院屬於非公務機關，因此適用非公務機關之相關規定。惟現行個資法對於個人資料的保護僅限於「電腦處理」的個人資料，但在「個人資料保護法」修正正式施行後，該法保護的範圍將擴及所有形式的個人資料，包括電子文件與紙本，以病歷為

[61]醫療法第 102 條第 1 項。
[62]醫療法第 71 條。
[63]醫療機構電子病歷製作及管理辦法第 3 條

本報告之智慧財產權歸屬於法務部

例，未來不論是電子或是紙本病歷，都將納入個人資料保護法的適用範圍。此外，個人資料保護法第 6 條特別規定特種個人資料之概念，將醫療、基因、性生活、健康檢查及犯罪前科納入特種個人資料之範疇，除非符合法律之規定，否則原則上不得為蒐集、處理或利用。雖於電腦處理個人資料保護法施行細則修正草案預告版當中，已對於病歷、醫療個人資料、基因個人資料、性生活、健康檢查資料，以及犯罪前科為定義，惟仍有法規適用上的疑慮，舉例而言，健保財務資料係屬一般個人資料或醫療個人資料，即生疑義。

個人資料保護法的架構，主要區分為兩大類，以適用之資料係由「公務機關」或「非公務機關」來進行蒐集、處理或利用，來決定適用何種規定。醫療個人資料屬於特種資料，其蒐集、處理或利用應另依第 6 條第 2 項授權訂定之辦法為之;至於病歷則為個人資料保護法定義下的一般個人資料,因此適用個人資料保護法的規定,惟我國醫療機構可大致可分為公立與私立兩種經營模式，在適用個人資料保護法時，也可能將產生如何適用個人資料保護法「公務機關」與「非公務機關」的疑慮。

對於醫療產業而言，未來修正後個人資料保護法正式施行後，不再限於以電腦處理之資料始受保護，病患資訊載體管理面項及難度均增加；病患資料範圍也將擴張，「得以直接或間接識別該個人之資料」均包含在個人資料保護法之規範範圍內；此外，特定目的外利用病患資料須經本人特別書面同意，此「同意」書面之製作及相關同意程序可能將大幅增加醫療機構之營運成本。而從規範面而言，主管機關應檢視現行相關醫療法規與個人資料保護法之適用關係外,同時也應針對醫療產業較需高度保護之部分訂立相關規範。

3.電信產業之隱私保護議題

電信業者為滿足消費者個人化之需求，利用所擁有之用戶個人資料與通訊資料，以提供該用戶最適化之服務，個人資料被他人蒐集、利用與處理之機會也隨之增加，電信業使用個人資料的行為如果未經

本報告之智慧財產權歸屬於法務部

適當規範，也可能將造成對個人資料隱私的威脅，因此，如何將該個人資料為有效之利用，並兼顧用戶隱私權之保障，已成為電信產業當前之重要課題。

電信產業相關之隱私資料種類也相當多，流量資料係指使用者使用通訊服務，在使用的過程中所發生的交易資料，例如通話對象、持續時間、費率、經過的中繼點等。除了做為計價的依據外，電信業者亦可藉由蒐集此類資料，分析個別使用者的使用習慣、偏好，可作為往後進行行銷之用。位置資料則是指使用者所使用的終端設備所在的地理位置，以及行進的方向、速度，例如 GPS 定位功能。位置資料將使個人何時位於何處的資訊不再為個人所專有，而處於他人可得知的狀態。用戶資料係指消費者於通訊服務訂約時，所提供的個人相關資料，例如申請固網電話，用戶所填寫之申請單，可能須提供用戶姓名、身分證字號、出生日期、住址等資訊，若用戶以金融機構自動扣款繳交相關費用，亦須提供金融帳戶號碼。電信業者蒐集若將上述訂約資料、流量資料、位置資料，將資料中可確認個人身分之部分去除，再將所有的資料加以分析，即可做為經營決策的參考。此種資料已將識別個人之部分去除，已非屬個人資料，惟若去名化之過程有瑕疵，仍可能使個人資料被混雜在其他資料中被外洩。而即使資料去名化之過程無瑕疵，若可以藉由交互查詢、與其他資料比對，將總合統計資料恢復為個人資料而找出特定人，仍屬修正後個人資料保護法之規範範圍。

電信業為適用現行個資法之非公務機關之一，除此之外，電信相關法規中亦有隱私規範。電信法第 7 條規定，電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密。若電信事業用戶需查詢本人之通信紀錄，於電信事業之電信設備系統技術可行，並支付必要費用後，電信事業應提供之，惟應遵循「電信事業處理有關機關查詢電信通信紀錄實施辦法」之相關規範為之。

新修正個人資料保護法施行後，電信產業除了需遵循電信法規外，也需注意新增之告知義務、提供資料當事人拒絕行銷之方式等規範。值得一提的是，電信產業跨境傳輸之情形普遍，未來在罰則加重之情況下，更需注意國際傳輸之限制。對於主管機關而言，應盡監督之責，國家通訊傳播委員會已於今（2011）年 10 月預告訂定「限制

本報告之智慧財產權歸屬於法務部

非公務機關國際傳遞個人資料之命令」(通傳營字第 10041054820 公告)，即是考量大陸地區之個人資料保護法令尚未完備，爰限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區。

4.小結

新修正個人資料保護法施行後，在適用範圍方面有兩個面向之擴張，第一是不再限於特定機關，公務機關、各產業及一般個人均受到新法規範；第二則是適用之個人資料不再限於經電腦或類似設備處理之資料檔案，紙本資料以及任何可留存之資料類型都是規範之對象。新法也增加機關於蒐集、處理或利用個人資料前，應告知資料當事人相關事項之義務。若非公務機關合法於特定目的外利用個人資料行銷時，應提供當事人表示拒絕接受行銷之方式並支付所需費用，而在當事人表示拒絕接受行銷時，也應立即停止利用該個人資料。另外，為使當事人能夠即時得知個人資料外洩之情形，儘速採取因應措施，新法也規定機關於違法外洩當事人個人資料時之通知義務。

新法適用範圍之擴大，將衝擊許多原本未受電腦處理個人資料保護法規範之產業，而對於原本即受舊法規範之產業而言，亦有許多須調整之處。為協助產業遵循新法相關規定，各目的事業主管機關應審慎考量其所管轄之事業類型，訂立或修正相關法規命令或指引，提供產業使用與參考。

（三）非公務機關個人資料安全維護計畫標準辦法草案範本(詳見本報告第 34-58 頁）

（四）公務機關或學術研究機構基於醫療衛生或犯罪預防目的蒐集、處理或利用特種個人資料辦法草案（詳見本報告第 58-72 頁）

本報告之智慧財產權歸屬於法務部

參、個資保護執行現況統計及試行成果報告

一、試行機關成果問卷設計表

（一）緣起

財團法人資訊工業策進會(以下簡稱資策會) 法務部之「99 年度公務機關個人資料保護方案委辦計畫」，執行法務部編定各公務機關「個人資料保護執行程序暨考核作業手冊」相關工作。本報告為本案計畫需求項目 2、統計個資保護執行與成果報告之交付文件「試行機關成果問卷設計表」。

（二）目的

本報告主要目的係依據個人資料保護法、100 年 10 月間預告之個資法施行細則修正草案，並參考國際個人資料保護相關標準(NIST SP800-122、BS10012 等)，編訂「試行機關成果問卷設計表」(以下簡稱本問卷)，提供各政府機關做為法令要求及單位內個資保護現況之差異評估比較，以做為後續改善依據，本問卷係屬參考性質，政府機關可參考本問卷，就組織特性、業務需求，以符合個人資料保護法與其它相關法令及細則要求，修正組織所需版本。

（三）適用對象

本問卷適用於政府機關執行與個資相關業務之所有人員。

表 6：試行機關成果問卷設計表

試行機關名稱：_____
機關主要業務說明：
_____
_____
機關人數：☐10 以下 ☐11-30 ☐31-50 ☐51-70 ☐71-90 ☐100 人以上
資訊人員：☐無 ☐1-5☐6-10 ☐11-15 ☐16-20 ☐21 人以上
問卷填寫人：
填寫人單位名稱：
聯絡人電話：

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
1	組織	機關是否已指派單位內負責個人資料管理的人員？					
2	組織	機關是否已組成個人資料保護組織，同時可清楚說明維護機關內部個人資料之管理作業權責？					
3	組織	承上題，上述要求是否已有文件化，載明成立個人資料保護管理組織及角色，並配置相當資源？					
4	組織	單位是否指派專人進行個人資料檔之管理及維護？					
5	組織	機關是否已清楚了解機關內有關個人資料之蒐集、處理、利用之範圍？					
6	組織	機關是否已辨識單位個資與個人資料保護法之適法性？					
7	組織	單位是否訂定經首長或其授權之人核准之員工及非員工個人資料如何與何時被蒐集、利用、以及保護之個人資料管理政策？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
8	告知	機關直接蒐集個人資料是否已取得當事人書面、電話、傳真或電子方式同意？（法令授權免通知者除外）					
9	告知	機關是否設置網站供公眾查閱個人資料檔案名稱、機關名稱、聯絡方式、資料檔案保有依據及特定目的、個人資料類別等？(公務機關)					
10	告知	機關依法向當事人直接蒐集個資時，是否明確說明蒐集個人資料的機關名稱,目的,個資類別,期間,地區,對象,處理方式/當事人行使權利及方式/不提供之影響？					
11	告知	機關是否提供清楚與明顯的說明予組織內或組織外人員，有關個人資料的安全維護方式？					
12	告知	機關是否提供清楚與明顯的說明予組織內或組織外人員，有關當事人如何查詢或存取其個人資料？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
13	告知	機關是否提供清楚與明顯的說明予組織內或組織外人員，有關當事人如何更正或刪除其個人資料？					
14	告知	機關內間接蒐集之個人資料是否已規劃告知當事人？					
15	告知	機關是否設計提供當事人申訴程序與管道？					
16	蒐集處理利用	機關是否有盤點組織內所有的個人資料，並建立清冊以利管理？					
17	蒐集處理利用	機關內是否針對各項個人資料之蒐集、處理、利用及銷毀建立資料流程圖以掌握資料流向及管理方式？					
18	蒐集處理利用	機關進行個人資料蒐集時是否遵循所屬主管機關的法規或公約（例如 金融、保險、社會安全、健康照護等）？					
19	蒐集處理利用	機關內是否識別間接蒐集之個人資料之適法性及特定目的之合理性？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
20	蒐集處理利用	機關是否針對特種個資（醫療、基因、性生活、健康檢查、犯罪前科）進行蒐集、利用及處理？					
21	蒐集處理	機關若有蒐集特種資料是否取得法令依據？					
22	蒐集處理	機關若有蒐集特種資料是否清楚了解機關內有關特種資料之用途？					
23	蒐集處理	機關若有蒐集特種資料，是否有適當之安全維護計畫？					
24	蒐集處理利用	機關之個人資料管理是否有建立必要之使用紀錄、軌跡資料（Log Files）及證據之保存措施？					
25	蒐集處理利用	機關內是否有針為個人資料分級進行衝擊分析及風險評鑑？（含備份檔案及軌跡檔案）					
26	蒐集處理利用	機關內是否有針為個人資料不同等級處理進行安控措施？（含備份檔案及軌跡檔案）					
27	蒐集處理	機關是否執行資料安全管理？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
	利用						
28	蒐集處理利用	機關是否執行人員安全管理？					
29	蒐集處理利用	機關否執行設備安全管理？					
30	蒐集處理利用	機關內是否有針對個人資料顯示進行適當的去識別化？					
31	蒐集處理利用	機關與其它單位個人資料交換是否已識別個人資料之適法性及特定目的利用之合理性？					
32	蒐集處理利用	機關與其它單位個人資料交換是否已採取適當保護措施？					
33	蒐集處理利用	對於個資(紙本及數位資料)之存取及利用是否保有完整的紀錄、軌跡資料					
34	蒐集處理利用	機關是否已針對受委託處理個資案件之單位，於契約上訂有個資保護法令及機關內部個資相關規定要求？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
35	蒐集處理利用	機關是否已針對受委託單位，於契約上訂有明確的監督要求?並執行監督?					
36	蒐集處理利用	機關是否有將資料傳送於境外，該境外地區是否有個資保護法令(規範)，且已取得中央目的主管機關同意?					
37	訓練	機關是否已進行有效的個人資料保護全面性（含新人）人員宣導及教育訓練？					
38	訓練	機關是否針對負責管理及維護個人資料檔案之專人進行有效的專業教育訓練？					
39	程序	機關是否已建立個人資料內部管理程序或規則，以確保單位內個人資料蒐集、處理、利用、刪除及傳輸符合特定目的要求？					
40	程序	機關是否有設計當事人查詢、變更、刪除資料之程序？					
41	程序	機關是否有設計當發生個人資料被竊取、洩漏、竄改或其它侵害事件之主動					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
		通知程序?					
42	程序	機關是否有設計風險評估及管理程序？					
43	程序	機關內是否有設計個資事故通報程序？					
44	程序	機關內是否有設計個資事故應變處理程序？					
45	程序	機關內是否有設計內部稽核程序？					
46	程序	機關是否有設計文件管理程序？					
47	程序	機關是否有設計當個人資料蒐集目的消失或屆滿之資料刪除程序？					
48	程序	是否訂有個人資料檔案維護計畫及業務終止後個人資料處理方法等相關事項之辦法(中央目的主管機關)					
49	程序	是否訂有個人資料檔案維護計畫					
50	程序	是否訂有業務終止後個人資料處理方法					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
51	程序	是否訂有申訴程序					
52	程序	是否訂有証據保存程序					
53	程序	是否訂有維護資料正確性程序					
54	程序	是否有盤點單維護機制					
55	PDCA	機關對於個資之蒐集、處理與利用之流程，是否進行內部稽核？					
56	PDCA	機關是否定期檢視個資政策及個資保護執行結果？					
57	PDCA	機關是否有實施個人資料安全維護之整體持續改善規劃？					
58	其它	機關是否取得品質管理系統(ISO9000)認證（請說明認證範圍）？					
59	其它	機關是否取得資訊安全管理系統(ISO27001)認證(請說明認證範圍）？					

資料來源：本計畫自行設計

本報告之智慧財產權歸屬於法務部

二、統計個資保護執行與成果報告

（一）目的

本報告係依據法務部之「99 年度公務機關個人資料保護方案委辦計畫」(以下簡稱本計畫)，制定之「個人資料保護執行程序暨考核作業手冊」，特選定內政部地政機關及內政部警政機關進行試辦導入工作，以做為手冊修改之參考依據，確保制定文件之可用性。

（二）試行機關

1.試行機關包括：（1）本部及所屬機關、（2）戶政、地政、警政及衛生機關至少擇 2 類機關。另依本部申請行政院國家科學技術發展基金補助計畫書所定試行機關部分，以中央機關（3 個）及其所屬機關（2 個）與地方政府機關（1 個）進行示範導入作業。

2.本計畫選定之試行機關為：（1）本部檢察司、（2）行政執行署、（3）內政部地政司及（4）內政部警政署刑事警察局（165 專線）；另選擇上開 2 個機關程序相關之縣市政府或所屬機關共同參與。

（三）名詞定義

1.個資自評：各機關依據個資法的要求，依特定基準表，自我評量符合度。

2.個資教育訓練：公務機關依據個資法施行細則第九條之安全維護措施要求，對組織同仁安排之教育訓練課程。

（四）導入成果報告

配合個資法之實施，經法務部選定內政部地政司中部辦公室及內政部警政署刑事警察局 165 專線分別試行導入「個資通報管理程序」及「個人資訊服務委外管理作業程序」。

由於內政部地政司中部辦公室資訊科原已導入資訊安全管理制

本報告之智慧財產權歸屬於法務部

度（ISMS）取得認證，制度內已建構資安事件通報程序，因此本計畫是以該組織之資安事件通報程序配合個資法之要求要項,進行討論修訂，在進行試行導入的討論過程中，本計畫同時邀請台北市政府地政局及新北市政府地政局共同參與，藉由試行導入及討論的過程中，同時做為台北市政府地政局及新北市政府地政局未來推動之參考依據，詳細成果文件請參考附件一及附件二。

內政部警政署刑事警察局 165 專線因尚無導入 ISMS 制度,因此本計畫就該組織之工作性質，依組織之特性為該單位設計「個人資訊服務委外管理作業程序」,討論的過程中亦邀請台北市政府警察局資訊科共同參與討論，藉由試行導入及討論的過程中，同時做為台北市政府警察局未來推動之參考依據。

另外，法務部亦選定檢察司以及所屬之行政執行署為試行機關。本計畫擇定機關之陳情程序作業流程作為試行之程序。透過陳情程序之流程，以盤點出機關內所蒐集、處理以及利用之個人資料。

先就檢察司而言，由於其為法務部之幕僚單位，因此，其所經手之陳情案件主要都係由其他機關所轉來之個人資料，故大多屬於間接蒐集處理個人資料之情形，另外，個人資料之載體主要也為電子文件之方式，紙本之形式較為少見。於試行盤點個資後，建議機關可針對內部權限控管以及處理流程進行管理，並且提供個資盤點清冊以及個人資料作業流程圖供機關參考。

而行政執行署之情形與檢察司比較不同之處在於，行政執行署直接面對民眾之情形比較普遍，因此民眾多直接透過電子郵件、紙本信函等方式直接遞交陳情書，所以行政執行署直接蒐集個人資料之情形較為普遍。對此，於試行盤點個人資料之作業流後，建議機關針對蒐集個人資料之方法、紙本個人資料之管控作法、公文交換等流程進行管理。

（五）參考文獻

1.法務部，個人資料保護執行（管理）暨考核作業手冊，2011 年 12 月 30 日。

本報告之智慧財產權歸屬於法務部

2.內政部地政司地政資訊作業科事件通報管理程序書

（1）目的

為有效處理各類資訊事件，防止事件可能造成之傷害擴大，故制定本管理程序書，以暢通回報管道，尋求更快速、更有效之處理方式。

（2）範圍

A. 因天災、人禍或其他因素造成下列狀況時：

B. 資訊系統故障、停頓、或出現無法解決的錯誤訊息。

C. 發現資訊系統漏洞、系統遭到病毒或駭客侵入。

D. 人員作業明顯違反本科作業規定，而影響業務運作者。

E. 發現實體環境遭破壞、侵入。

F. 發現資料遭竊取、外洩。

（3）定義資安事件：任何危害資訊作業安全之事件

A. 個資侵害事件:個人資料或機敏性資料遭侵犯或不當使用。

B. 網路資安事件:由 Internet 引起而中斷本科系統作業之資安事件。

C. 侵入事件:「未獲授權人員」強行進入本大樓之事件。

D. 實體安全威脅：對本大樓之完整性有立即威脅之事件(如火災、水災)。

E. 一般事件：各類資訊系統操作時發生之系統錯誤或次要資訊設備故障之狀況。

F. 注意事件：各類資訊系統操作時發現之可能系統漏洞、主要資訊設備故障或其他影響本科作業而未列之項目。

本報告之智慧財產權歸屬於法務部

G. 重大事件：資安事件或網路資安事件造成機密資料遺失或損毀、或造成主要資訊設備癱瘓；侵入事件、實體安全威脅或其他導致本科作業中斷而未列之項目。

H. 主要資訊設備：若故障後可能導致某系統作業中斷之資訊設備，如主機、伺服器、集線器、路由器...等。

I. 次要資訊設備：若故障後可能影響人員作業速度之資訊設備，如個人電腦、印表機...等。

（4）相關表單

A. 緊急聯絡電話一覽表

B. 事件紀錄表

C. 各系統之「維護紀錄單」

D. 機房工作日誌

E. 矯正預防計畫表

F. 內部人員及廠商通報表

G. 個資事故通報與紀錄單

（5）內容

任何人遭遇定義內之各種事件時，必須在發現之第一時間內依照以下通知各相關承辦人員處理。

A. 一般事件

系統在操作時若發現操作錯誤時應立即通知該系統之承辦人或代理人。承辦人接到通知時須登入「資安(ISMS) e 化管理系統」紀錄於「機房工作日誌」及「事件紀錄表」，若需維護廠商進行維護，則需詳細紀錄於各系統之「維護紀錄單」。紀錄之內容須包含：

本報告之智慧財產權歸屬於法務部

a.發生時間、地點

b.系統名稱

c.發生位置(程式、表單名稱或硬體)

d.操作流程及輸入資料

e.產生之錯誤訊息或錯誤結果

f.承辦人員確認完成改善。

B. 注意事件

系統在操作時若發現可能之系統漏洞或硬體故障時應立即通知該系統之承辦人或代理人。承辦人接到通知時須登入「資安(ISMS) e 化管理系統」詳細紀錄發生於「事件紀錄表」及「矯正預防計畫表」。若需進行維護，則詳細紀錄發生狀況及處理情形於各系統之「維護紀錄單」。紀錄之內容須包含：

a.發生時間、地點

b.系統名稱

c.發生位置(程式、表單名稱或硬體)

d.操作流程及輸入資料

e.產生之狀況或結果

f.承辦人員須將「事件紀錄表」之編號登錄於「機房工作日誌」及「矯正預防計畫表」。若有進行系統維護，亦需登錄於各系統之「維護紀錄單」，以便於後續之追蹤檢討。

g.立即通知廠商限期修正，並依照『矯正預防作業管理作

本報告之智慧財產權歸屬於法務部

業規範』進行後續處理後回報業務主管及科長。

C. 重大事件

遇重大事件時發現者在第一時間內可對事件做緊急處置，再行通知相關人員。並依照「矯正預防管理程序書」啟動矯正預防作業。依以下各種不同狀況處置：

a.資安相關事件：

I.通知機房人員並暫時停止相關系統服務。

II.通知廠商處理。

III.回報業務主管及科長。

IV.若為網路資安事件，則通報「國家資通安全會報技術服務中心」協助後續調查。

V.回報主管及科長處理結果。

b.人員侵入事件：

I.以現有之通訊工具通知所有人員注意入侵之歹徒(廣播、哨子、大喊…等)。

II.通知值日人員。

III.通知台中市警察局第四分局(110 或 22515452)及政風處中部綜合科（黎明）。

IV.事件結束後大樓安全承辦人回報主管、科長及政風處中部綜合科（黎明）處理結果。

c.實體安全威脅：

本報告之智慧財產權歸屬於法務部

I.以現有之通訊工具通知所有人員注意(廣播、哨子、大喊…等)。

II.通知值日人員。

III.通知台中市消防局黎明分隊(119 或 22528462) 及政風處中部綜合科（黎明）。

IV.事件結束後大樓安全承辦人回報主管、科長及政風處中部綜合科（黎明）處理結果。

V.依照『矯正預防管理程序書』登入「資安(ISMS) e 化管理系統」，登記於「事件紀錄表」及「矯正預防計畫表」後循程序呈核。

VI.承辦人員追蹤矯正預防作業完成後回報業務主管。

VII.為個資事件時須補填寫「個資事故通報紀錄單」，進行個資影響分析、證據保存及對外溝通協調等相關工作。

VIII.應立即指派適當處理人員紀錄事件取得之管道及相關資訊，如通報單位、通報姓名、通報日期、連絡電話、電子郵件、與本機關關係，並由資安事件執行人負責追蹤。

D. 個資事故識別

由處理人員負責查明個資事故實際發生及最早被發現日期及時間，並掌握已被揭露的個資資料範圍(ex：資料內容)、概述該資料來源管道、使用目的及該個資儲存方式等資訊。

E. 個資事故影響

本報告之智慧財產權歸屬於法務部

進行評估該外洩個資內部業務相關之系統、人員及組織

評估外洩個資受影響之當事人人數、影響程度(ex：造成詐騙集團利用、名譽受損…)及各影響程度與人數可能對公司造成之損失。

F. 個資事故診斷與調查

a.為避免事件排除作業造成重要資料或鑑識證據遺失，應先完成重要設定檔、資料與鑑視紀錄檔之備份與保存

b.備份完成後應確認備份資料之有效性及可用性。

c.研判個資事故發生之根因，以作為後續處理之參考

G. 對外通報分析

a.評估是否須要通報相關機關、人員、通報內容方式及時機。

b.機房人員應定期登入「資安(ISMS) e 化管理系統」，將該期間內所有事件紀錄(含機房工作日誌、廠商維護紀錄、事件紀錄表及矯正預防計畫表)彙整統計，列印成事件紀錄彙整表。

本報告之智慧財產權歸屬於法務部

表 7：內政部地政司地政資訊作業科個資事故通報與紀錄單

內政部地政司地政資訊作業科

個資事故通報與紀錄單

編號：

通報單位		通報姓名		通報日期	
連絡電話		電子郵件		與本機關關係	(民眾/媒體/同仁..)
處理單位		處理人員		處理日期	
個資事故識別					
個資事故發生與發現之日期與時間： 遭受揭露之個資範圍與敘述： 遭受揭露個資之儲存媒體：					
個資事故影響分析					
內部影響範圍(包含系統、人員、組織)： 當事人影響程度、人數與損失評估：					
個資事故診斷與調查					
個資事故相關採證程序之紀錄、證據保存方式及負責人員： 個資事故根因分析結果：					
對外通報分析					
是否需(或已)通報主管機關、執法單位或媒體：					

本報告之智慧財產權歸屬於法務部

是否需(或已)向社會大眾公告： 通知個資事故當事人之通報對象、內容、方式及時機：
處理紀錄：(包含內部處理過程、對外連繫對象、時間及處理人姓名) ：
執行人：　　主管：

資料來源：本計畫設計

本報告之智慧財產權歸屬於法務部

表 8：內政部地政司地政資訊作業科事件紀錄表

內政部地政司地政資訊作業科

事件紀錄表

編號：

登錄人		日期		時間	A M_____ ： _____. P
事件描述					
事件類型：□資安事件　□個資侵害事件(須填寫個資事故通報與紀錄單) 個資事故通報與紀錄單編號：					
事件等級：□一般事件　□注意事件　□重大事件					
事件狀況： 事發原因： 事件處理狀況：					
執行人：　　主管：					

資料來源：修改原地政司中部辦公室表單

本報告之智慧財產權歸屬於法務部

表 9：內政部地政司地政資訊作業科機房工作日誌

內政部地政司地政資訊作業科

機房工作日誌

年　月　日

<table>
<tr><td colspan="2">開機時間</td><td>未關機</td><td>關機時間</td><td>未關機</td></tr>
<tr><td colspan="2">電力系統</td><td>正常</td><td>消防系統</td><td>正常</td></tr>
<tr><td colspan="5">異 常 情 形</td></tr>
<tr><td>狀況摘要</td><td colspan="4"></td></tr>
<tr><td>處理情形</td><td colspan="4"></td></tr>
<tr><td>備忘事項</td><td colspan="4"></td></tr>
<tr><td colspan="3">填表人員</td><td colspan="2">機房管理人員</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td colspan="3">安全官</td><td colspan="2">科　　長</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td colspan="5">執行人：　　主管：</td></tr>
</table>

資料來源：地政司中部辦公室表單

本報告之智慧財產權歸屬於法務部

表 10：內政部地政司地政資訊作業科矯正預防計畫表

內政部地政司地政資訊作業科

矯正預防計畫表

編號：

<table>
<tr><td>登錄人</td><td></td><td>日期</td><td></td><td>時間</td><td>AM_____ ： _____.
P</td></tr>
<tr><td colspan="6">事件描述</td></tr>
<tr><td colspan="6">事件紀錄表編號：</td></tr>
<tr><td colspan="6">矯正措施（ □是 □否 須經核准後方可實施 ）</td></tr>
<tr><td colspan="6">實施日期： 執行人： 主管：</td></tr>
<tr><td colspan="6">預防措施（ □是 □否 須經核准後方可實施 ）</td></tr>
<tr><td colspan="6">年 月 日至 年 月 日
實施日期： 年 月 日起經常辦理
執行人： 主管：</td></tr>
<tr><td colspan="3">完工確認</td><td colspan="3">有效性確認</td></tr>
<tr><td colspan="3">執行人： 主管：</td><td colspan="3">管理審查委員代表：</td></tr>
<tr><td colspan="6">執行人： 主管：</td></tr>
</table>

資料來源：地政司中部辦公室表單

本報告之智慧財產權歸屬於法務部

表 11：內政部地政司資訊作業科內部人員及廠商通報表

內政部地政司資訊作業科

內部人員及廠商通報表

單位/公司名稱	聯絡人	電話	行動電話	E-mail/MSN
執行人：		主 管：		

資料來源：修改原地政司中部辦公室表單

本報告之智慧財產權歸屬於法務部

3.內政部警政署刑事警察局預防科 165 反詐騙諮詢專線個人資訊委外服務管理標準作業程序

（1）目的

為建立內政部警政署刑事警察局預防科 165 反詐騙諮詢專線（以下簡稱本專案）符合我國個人資料保護法及 100 年 10 月間預告之個資法施行細則修正草案之資訊委外服務管理要求，對廠商進行簽約前、專案執行中及專案結束的活動管理及監督，特訂定本作業程序，以便本專案同仁皆能有效遵循資訊委外服務處理之規範。

（2）適用範圍

凡本專案所進行含個人資料之資訊委外服務計畫，皆適用本作業程序之規範。

（3）權責

A. 需求/發包單位

B. 依作業流程提出需求並進行委外招標發包作業

C. 權責主管

D. 核准招標案件相關文件與預算、訂定底價及准予進行招標與發包作業

（4）名詞定義

A. 簽約前活動：意指本機關對於資訊委外服務計畫，確定委託廠商並完成簽約前之廠商招募活動

B. 專案執行中活動：意指本機關完成委外採購程序，確定委託廠商並完成簽約後之廠商計畫執行活動

本報告之智慧財產權歸屬於法務部

C. 專案結束活動：與廠商之委託關係因計畫完成而終止或因其它因素造成計畫解除時，所進行的活動

（5）遵循法規

A. 政府採購法令彙編（行政院公共工程委員會編印）：

a.政府採購法。

b.政府採購法施行細則。

c.機關委託資訊服務廠商評選及計費辦法。

d.最有利標評選辦法。

e.採購評選委員會組織準則。

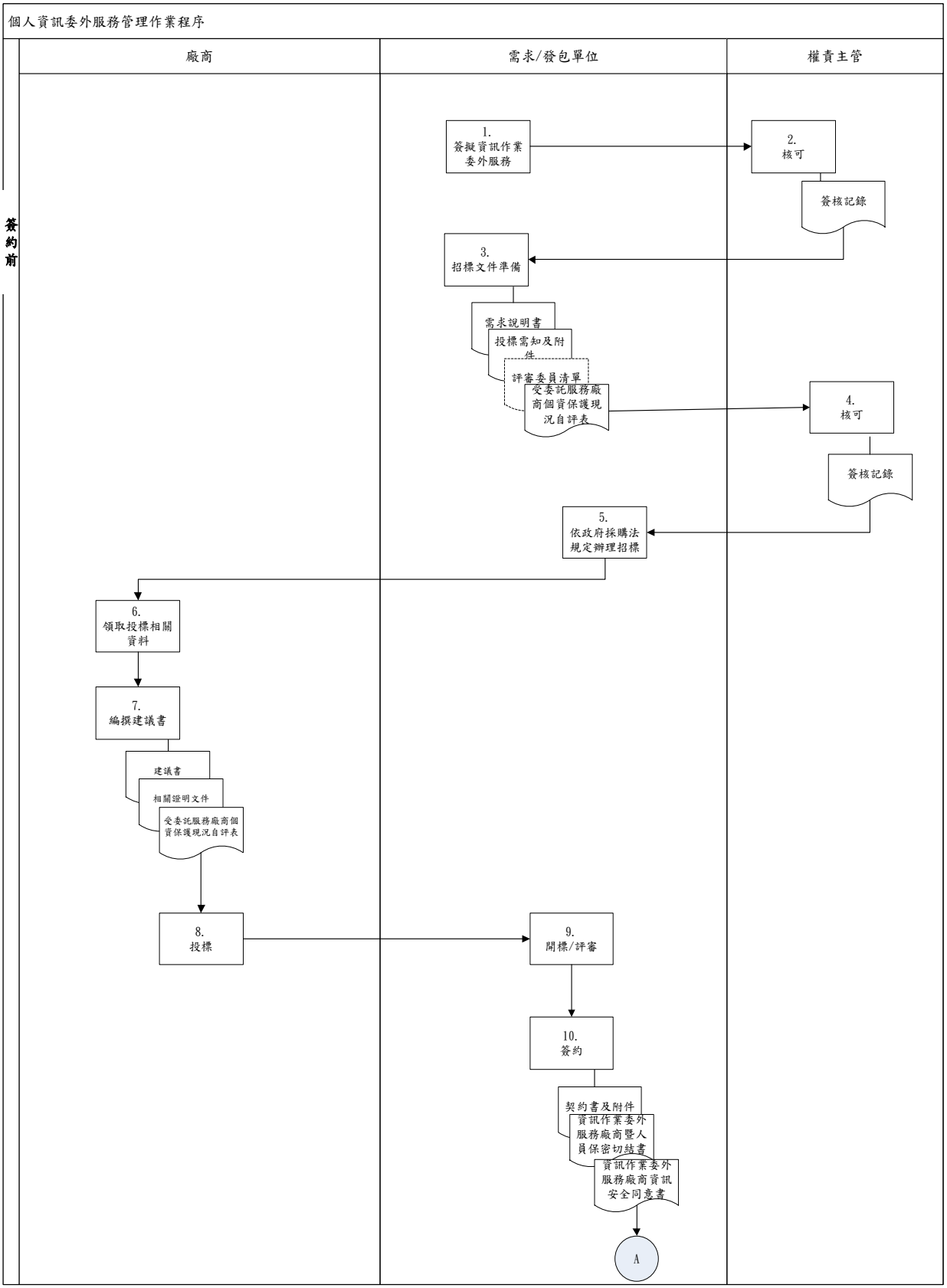
B. 其他有關之規章、辦法或規定，如：各機關資訊作業委外服務實施要點（行政院台 83 速授審字第 0205 號）

（6）相關文件

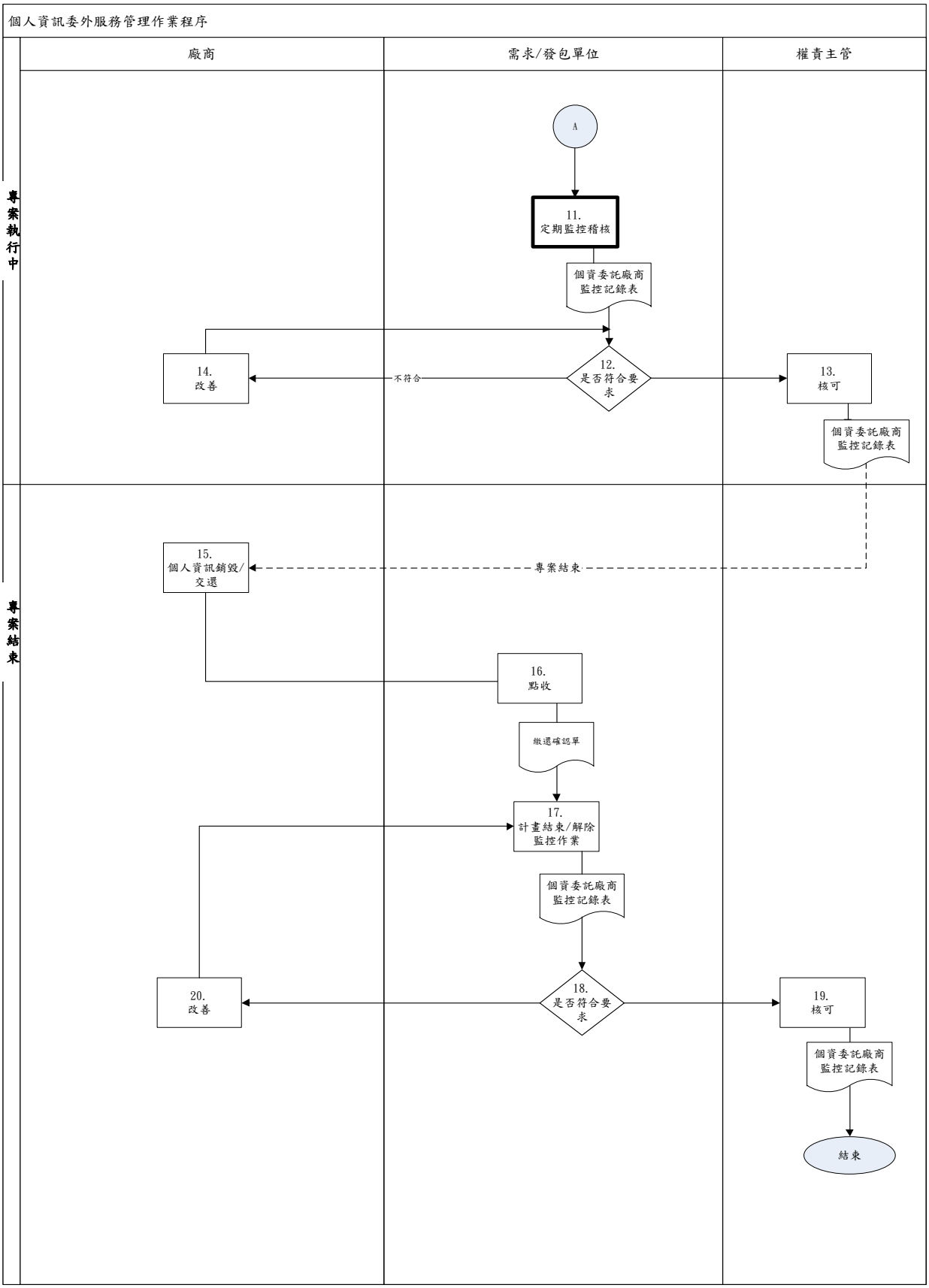
資訊安全監控暨事件通報處理程序(若有誤以警政署資訊單位實際名稱為準

本報告之智慧財產權歸屬於法務部

（7）作業流程



本報告之智慧財產權歸屬於法務部



資料來源：本計畫設計

圖 2：個人資訊委外服務管理作業程序

本報告之智慧財產權歸屬於法務部

（8）輸出文件

表 12：輸出文件表

文件名稱	編號	保存年限
受委託服務廠商個資保護現況自評表	XXX-X-XXX-XXX-011	5 年
資訊作業委外服務廠商暨人員保密切結書	XXX-X-XXX-XXX-011	5 年
資訊作業委外服務廠商資訊安全同意書	XXX-X-XXX-XXX-011	5 年
個資委託廠商監控記錄表	XXX-X-XXX-XXX-011	5 年

資料來源：本計畫整理

本報告之智慧財產權歸屬於法務部

表 13：：授委託服務廠商個資保護現況自評表

機密等級：一般

受委託服務廠商個資保護現況自評表

填表日期:XX/XX/XX

<table>
<tr><td>機關(構)</td><td></td><td>廠商
名稱</td><td colspan="4"></td></tr>
<tr><td>契約名稱</td><td></td><td>業務負責人</td><td colspan="4"></td></tr>
<tr><td rowspan="3">*風險評估
(由廠商填寫)</td><td colspan="2">評估項目</td><td>是</td><td>否</td><td>不適用
(須填寫說明)</td><td>廠商提供佐證資訊</td></tr>
<tr><td colspan="2">1. 受委託廠商是否成立個人資料管理組織，並配置適當資源</td><td>☐</td><td>☐</td><td>☐</td><td>☐說明
_____
☐詳附件
_____</td></tr>
<tr><td colspan="2">2.受委託廠商是否已界定個人資料範圍</td><td>☐</td><td>☐</td><td>☐</td><td>☐說明
_____
☐詳附件
_____</td></tr>
</table>

本報告之智慧財產權歸屬於法務部

	3.受委託廠商是否已進行個人資料風險評估及管理機制	□	□	□	□說明 _____ □詳附件 _____
	4.受委託廠商是否有事故之預防、通報及應變機制	□	□	□	□說明 _____ □詳附件 _____
	5.受委託廠書是否訂有個人資料蒐集、處理及利用之內部管理程序	□	□	□	□說明 _____ □詳附件 _____
	6.受委託廠商是否已進行資料安全管理及人員管理	□	□	□	□說明 _____ □詳附件 _____
	7.受委託廠商是否已進行認知宣導及教育訓練	□	□	□	□說明 _____ □詳附件 _____
	8.受委託廠商是有已進行設備安全管理	□	□	□	□說明 _____ □詳附件 _____

本報告之智慧財產權歸屬於法務部

	9.受委託廠商是否已建立資料安全稽核機制	□	□	□	□說明 _____ □詳附件 _____
	10.受委託之工作涉及個資部份，是有已建立必要之使用記錄、軌跡資料及證據之保存	□	□	□	□說明 _____ □詳附件 _____
	11.受委託廠商是否已執行個人資料安全維護之整體持續改善	□	□	□	□說明 _____ □詳附件 _____
	12.受委託廠商過去無洩漏的個資的情況	□	□	□	□說明 _____ □詳附件 _____
	13.受委託廠商已建立個人資料保護管理制度	□	□	□	□說明 _____ □詳附件 _____
	14.受委託廠商毋須再下包或轉包其所受託之業務	□	□	□	□說明 _____ □詳附件 _____

本報告之智慧財產權歸屬於法務部

	15.契約中可配合明定終止時委託廠商須繳回所有曾取得之個人資料，或全部進行銷毀及不可保留之規範	□	□	□	□說明 _____ □詳附件 _____
	16.委託廠商發生過失之事件時，具有能力可負擔應負之責任	□	□	□	□說明 _____ □詳附件 _____
補充說明					

*結果評估 (委託單位填寫)	
評估基準	■達 13 個風險評估項目以上為【是】方可進行委託 ■廠商所提供之說明及資訊是否具有良善管理管理及可信任度。
評估結果	*□高風險　(完全未符合評估基準) *□中風險　(部分符合評估基準:達 8 個風險評估項目以上為【否】) *□低風險　(完全符合評估基準)
	□可進行委託 □不可進行委託 □未達受託基準，但須委託，說明:_____

本報告之智慧財產權歸屬於法務部

其他風險說明	
備註	

業務負責人	主管
月　　日	月　　日

資料來源：本計畫自行設計

本報告之智慧財產權歸屬於法務部

表 14：廠商暨人員保密切結書

機密等級：密件

ＸＸＸＸＸＸ資訊作業委外服務

廠商暨人員保密切結書

具保密切結廠商（或人員）　　（以下簡稱乙方）
於民國　　年　　月　　日起因承攬ＸＸＸＸＸＸ（以下簡稱甲方）
（資訊作業名稱）委外服務作業，特訂定以下條款：

乙方已充分了解中華民國「電腦處理個人資料保護法（個人資料保護法）」、「國家機密保護法」、「檔案法」等相關法規之內容，並承諾願意遵守該等法規，以確實保障甲方維護機密之權利。

所知悉甲方機密資訊，將遵守契約保密責任條文負責保密，且非經甲方之書面同意，乙方不得將所知悉資訊以任何之方式洩漏或交付予第三人。

乙方因執行本合約，而自甲方取得之一切資料、文件，均應於本合約期間屆滿時無條件歸還甲方。

因本合約所生之一切爭議，雙方同意以甲方所在地之地方法院為第一審管轄法院，經由訴訟程序解決。

乙方如有違誤願負法律上之責任，對於甲方因而所致之一切損失，均應依實際損失情形負起全部之損害賠償責任。本合約期間屆滿後亦同。

簽署人：　　（公司由負責人簽署）

地址：

統一編號（身份證字號）：

中　華　民　國　　年　　月　　日

資料來源：本計畫自行設計

本報告之智慧財產權歸屬於法務部

表 15：廠商資訊安全同意書

機密等級：一般

ＸＸＸＸＸＸ資訊作業委外服務廠商資訊安全同意書

委外服務廠商　　（以下簡稱乙方)於民國　　年　　月　　日起因承攬ＸＸＸＸＸＸ（以下簡稱甲方）　　（資訊作業名稱）委外服務作業，為確保乙方之服務符合甲方資訊安全政策與規範、遵循相關法令並保護智慧財產權，特訂定以下條款：

甲方已經或即將交付乙方有關業務機密及相關資訊（料)、具備智慧財產權之價值、涉及甲方業務內容或安全控制，乙方已充分認知業務機密及相關資訊(料)，須符合「電腦處理個人資料保護法（個人資料保護法)」、「刑事訴訟法」及「警察職權行使法」等相關法規要求，並不得洩漏、告知、交付、移轉或以任何方式提供第三人，亦不得自行以非本案工作目的之任何方式加以使用或利用。

前項所稱「業務機密及相關資訊(料)」，其內容包括一切以物理方式表達，包括但不限於書面、口頭、磁帶、磁碟片、光碟片、模型或其他產品，及經甲方列為密、機密、極機密之資訊（料）及紀錄報告等。

除外規定

下列情形乙方不負保密責任：

已公開為眾所周知之資訊（料)。

甲方書面同意公開者。

基於法律之規定或法院之命令而揭露者。但乙方應於揭露前通知甲方。

乙方存取甲方系統或連接甲方網路，須提出申請並經甲方許可，使用時亦需經甲方同意(核准)始得執行。

乙方同意採取必要合理之措施維護資訊之安全性與個人資料保護，甲方得定期查核乙方提供甲方服務之過程，是否按照本署資訊安全政策及相關規範，以及是否有效維持必要合理之措施以維護提供甲方服務過程之資訊安全。乙方同意於本合約期間暨本合約正式終止後一年內，甲方得至乙方場所檢查其資料保管、資訊安全管理及個人資料蒐集、處理及利用情形，以防機密資料外洩，確保資訊安全與

本報告之智慧財產權歸屬於法務部

個人資料保護管理之要求。

乙方人員因處理委託案，需存取甲方之資訊設施，須經甲方之同意並簽署「資訊作業廠商人員保密切結書」後，始得為之。

乙方提供甲方服務之過程中，如發生影響甲方資訊安全之事件時應即通報甲方，並按甲方之「資訊安全監控暨事件通報處理程序」(若有誤以警政署資訊單位實際名稱為準)處理。

乙方因執行委外服務作業，而自甲方取得之一切資料、文件，甲方得要求於合約期間屆滿時無條件歸還，同時乙方不得自行進行複印、複製、攝錄影及拍照等各式保存行為。

乙方或乙方人員如有違誤上述資訊安全要求，甲方因而所致之一切損失，均應依實際損失情形負起全部之損害賠償責任。

立同意書人：[公司全名]　　〔蓋章〕

代　表　人：[姓名]　　〔蓋章〕

日期：中華民國　　年　　月　　日

資料來源：本計畫自行設計

本報告之智慧財產權歸屬於法務部

表 16：委外服務廠商監控記錄表

機密等級：一般

委外服務廠商監控記錄表

填表日期:XX/XX/X

機關(構)		廠商			
契約名稱		廠商代表			
評估項目			是	否	不適用
廠商是否已將受委託之個人資料定義及建立一份個人資料清冊？			☐	☐	☐
所委託之個人資料計畫廠商是否已指派專人進行個人資料檔之管理及維護？			☐	☐	☐
廠商對委託之個人資料是否有訂定使用與保存期限？			☐	☐	☐
廠商是否有定期檢核程序及記錄，以避免個人資料使用超出特定目的外利用？			☐	☐	☐
廠商承接本合約是否有複委託者?且已取得本機關同意?			☐	☐	☐
單位是否有設計當發生個人資料被竊取、洩漏、竄改或其它侵害者事件之主動通知本機關程序?			☐	☐	☐
廠商是否已針對交付管理之個人相關資訊進行適當的安全管理措施			☐	☐	☐
廠商受委託管理含有個人資料之資訊系統，是否已建立必要之使用紀錄、軌跡資料（Log Files）及證據之保存措施？			☐	☐	☐
廠商對於個資(紙本及數位檔案)之存取及利用是否保有記錄、軌跡資料			☐	☐	☐
廠商對於遠端存取管理作業，是否可選擇禁止或嚴格限制遠端存取個人資訊？如允許遠端存取，組織是否有確保傳輸過程是經過加			☐	☐	☐

本報告之智慧財產權歸屬於法務部

密。			
廠商對受委託之檔案的儲存是否進行加密。(組織)	□	□	□
廠商是否定期對內部員工舉辦個人資料保護相關教育訓練或宣導？	□	□	□
廠商對於媒體淨化作業，是否已針對個人資料之數位／非數位媒體，於丟棄或釋出再使用之前，先予以淨化處理？例如，硬碟的消磁處理－使用磁場方式讓硬碟無法使用。	□	□	□
廠商員工離職或合約終止時，是否依規定繳回其使用或保管之資訊資產(如個人電腦)，新承接人員是否變更系統密碼？	□	□	□
廠商人員於離座位時是否會鎖定螢幕且加密	□	□	□
廠商是否有設計當個人資料蒐集目的消失或屆滿之資料刪除程序？	□	□	□
計畫結束時,廠商是否實際執行個人資料銷毀或繳還本公司,並留相關記錄	□	□	□
審查結論	重大議題及應改善事項說明：		

業務負責人	主管
月　　日	月　　日

資料來源：本計畫自行設計

本報告之智慧財產權歸屬於法務部

4.法務部行政執行署陳情程序

（1）目的

本報告係依據法務部之「99 年度公務機關個人資料保護方案委辦計畫」(以下簡稱本計畫)，制定之「個人資料保護執行程序暨考核作業手冊」，特選定法務部檢察司與法務部行政執行署之陳情程序進行試辦導入工作，以做為手冊修改之參考依據，確保制定文件之可用性。

（2）適用對象

本報告適用於法務部法律事務司、檢察司、行政執行署陳情程序之業務管理人員參考。

（3）名詞定義

個資作業流程圖：各公務機關依據個資法之要求，將現有作業流程圖轉化為個人資料作業流程圖，以作為個人資料盤點之基礎。

個資教育訓練：公務機關依據 100 年 10 月間預告之個資法施行細則修正草案第九條之安全維護措施要求，對組織同仁安排之教育訓練課程。

（4）導入成果報告

配合個資法之實施，經法務部選定檢察署及行政執行署就兩單位之陳情程序試行導入「個資盤點程序」。

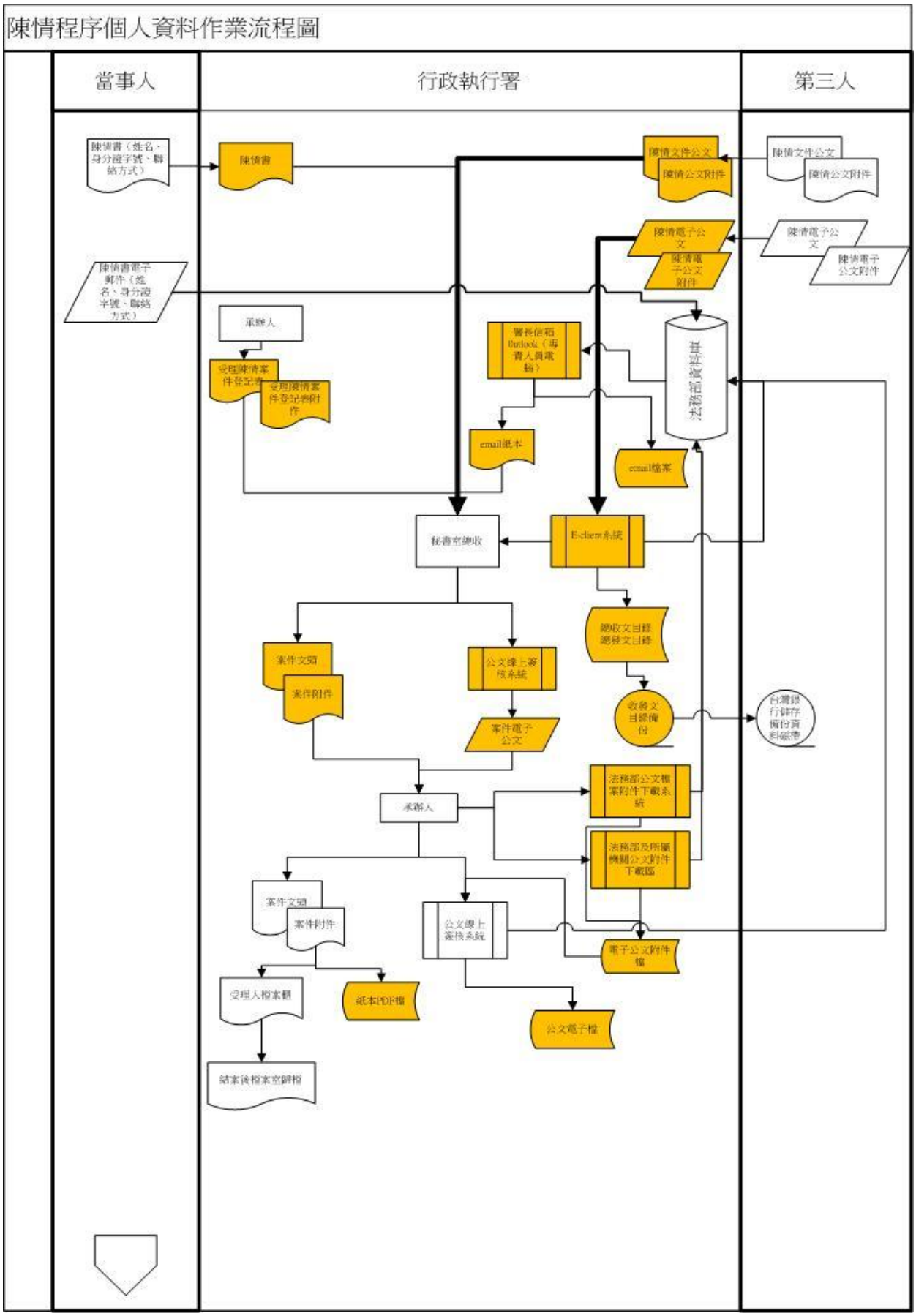
由於檢察司及行政執行署均第一次導入個人資料保護管理制度，因此本計畫選定陳情程序，就兩單位之陳情程序實際作業流程進行訪談，並協助兩單位就陳情作業流程所可能蒐集之個人資料進行個資作業流程圖繪製，以符合個資法就「界定個人資料

本報告之智慧財產權歸屬於法務部

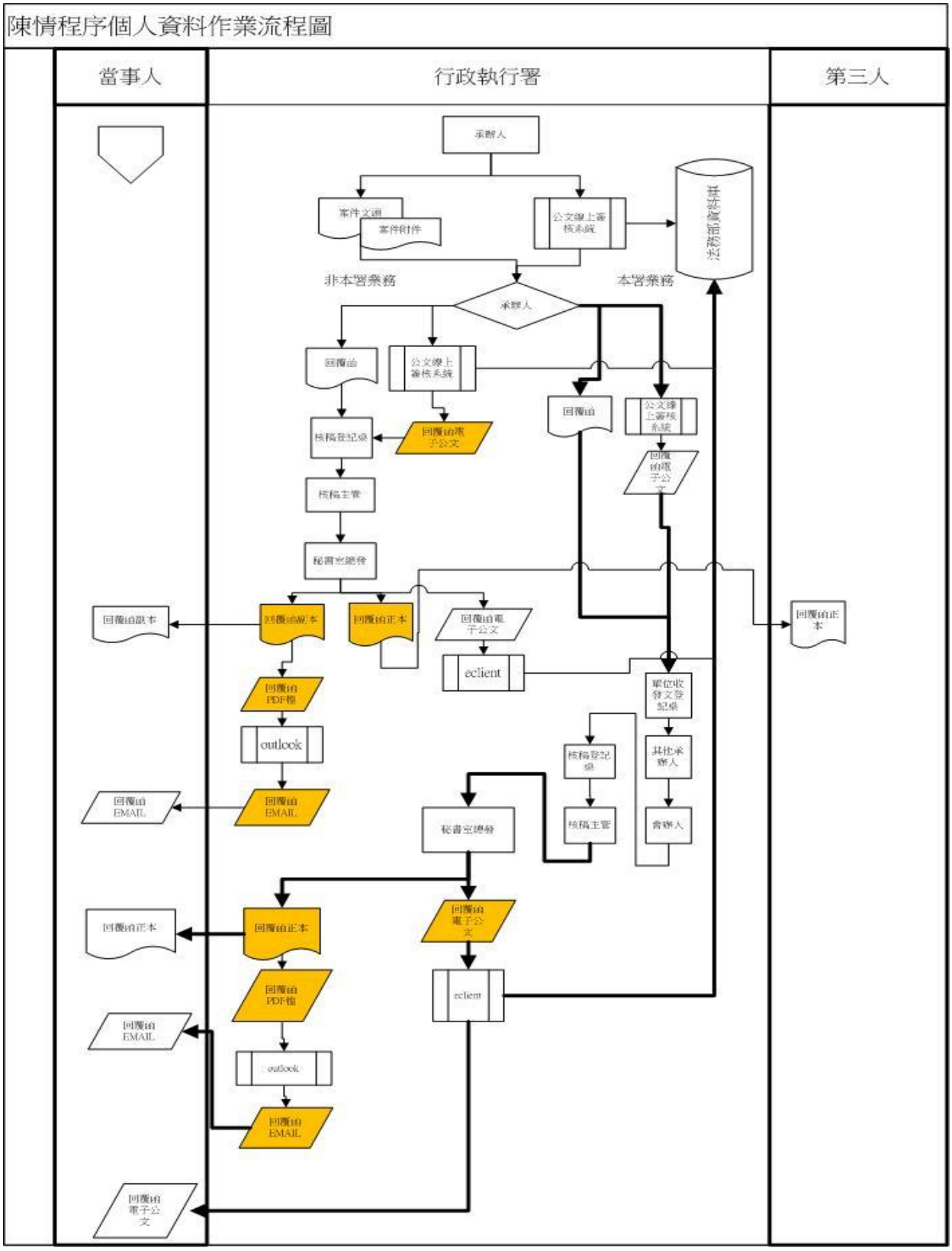
範圍」之要求要項。另外，本活動亦針對流程圖及轉填至個資盤點清冊之項目進行討論修訂，藉由試行導入及討論的過程中，做為將來公務機關處理陳情程序個資盤點作業之參考依據，詳細流程文件請參考（5）。

（5）行政執行署相關程序表單（請見下頁圖 3）

本報告之智慧財產權歸屬於法務部



本報告之智慧財產權歸屬於法務部



資料來源：本計畫自行製作

圖 3：陳情程序個人資料作業流程圖

本報告之智慧財產權歸屬於法務部

（6）法務部行政執行署個人資料盤點程序

A. 目的

為建立法務部行政執行署符合我國個人資料保護法及 100 年 10 月間預告之個資法施行細則修正草案之界定個人資料範圍之管理要求，特訂定本作業程序，以便法務部行政執行署同仁皆能有效遵循個資盤點之規範。

B. 遵循法規

a.行政程序法第 168 條至第 173 條（民國 94 年 12 月 28 日修正）

b.行政院暨所屬各機關處理人民陳情案件要點（中華民國九十一年十一月廿二日行政院院臺秘字第 0910058540 號函修正第六點、第八點、第十三點，九十一年十一月二十八日會研字第 09100249251 號函分行，並定自民國九十二年一月一日起施行）

c.法務部陳情請願疏處小組作業要點（中華民國八十九年十一月一日法務部 (89) 法秘決字第 000507 號函修正發布）

C. 相關文件

詳見下頁表 17：法務部受理陳情請願事件登記簿

本報告之智慧財產權歸屬於法務部

表 17：法務部受理陳情請願事件登記簿

<table>
<tr><td colspan="7">法務部受理陳情請願事件登記簿</td></tr>
<tr><td colspan="2">時間</td><td rowspan="2">受理陳情人員</td><td>單位</td><td>職稱</td><td colspan="2">姓名</td></tr>
<tr><td colspan="2">年　月　日</td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>陳情人
姓名</td><td>住所暨
電話號碼</td><td colspan="4">陳情內容</td><td>處理情形</td></tr>
<tr><td></td><td></td><td colspan="4"></td><td></td></tr>
<tr><td>批示</td><td></td><td>召集人副召集人</td><td></td><td>報告人</td><td colspan="2"></td></tr>
</table>

資料來源：法務部

本報告之智慧財產權歸屬於法務部

D. 個資盤點程序

本機關各部門業管人員針對行政業務項目或服務相關的個人資料進行盤點，並經個人資料保護管理召集人審核及核決。

a.由各個部門清查所持有的個人資料。

b.清查個人資料應考量下列事項進行。1.個資的生命週期 2.蒐集、處理利用程序 3.業管人員 4.保存形式 5.保存處所 6.委託提供流向 7.刪除銷毀方法 8.其他

E. 登載個人資料

盤點出本機關應管理之個人資料，由該○○部門主管向個人資料保護管理召集人報請核決後，登載於「個人資料盤點清冊」。

F. 個人資料盤點清冊檢視及修訂

○○部門業管人員為維持個資盤點清冊為最新之狀態，應定期於每年○月，或於機關行政業務項目、範圍有新增變動時，或個人資料保護法及其他相關法令規範有修訂，或利害關係人有所請求時，不定期檢視「個資盤點清冊」並修訂之。

G. 法務部行政執行署個資盤點輔導訪談記錄

a.第一次訪談

I.訪談地點：行政執行署 2 樓會議室

II.訪談時間：民國 101 年 4 月 30 日

III.訪談人：資策會科法所楊光華研究員

IV.受訪人：資訊室以及業務承辦人員

V.訪談內容：

i. 訪談人提問：行政執行署陳情程序蒐集個人資料方法及個人資料項目有哪些？

本報告之智慧財產權歸屬於法務部

承辦人員：行政執行署陳情程序蒐集個人資料的方法如網頁陳情程序處理流程圖所表示的有陳情人用郵寄或傳真、陳情人親自遞交陳情書、陳情人以言詞提出後由陳情承辦人填寫受理陳情請願事件登記簿、從網路的民意信箱及首長信箱等幾個管道；所蒐集的個人資料有具體陳訴事項、姓名、國民身分證統一編號或其他身分證件號碼及包括電話、住址、傳真號碼或電子郵件位址的聯絡方式。陳情書並沒有固定的格式，只要陳情人有填寫陳情事項、姓名、身份證件號碼、聯絡方式的書面就足夠了。

ii. 訪談人提問：除了陳情處理流程以外是否還有其他蒐集陳情人個人資料的管道？

承辦人員：除了陳情處理流程圖所表的管道之外，還有從其他機關移送或需要協調有關機關協同處理的陳情案件，這種都會透過秘書室的電子公文交換系統轉到陳情承辦人。

iii. 訪談人提問：從網路上的民意信箱與首長信箱的網頁，雖然網址不全部相同，但都是以首長信箱的格式為首頁，在行政執行署內部處理上有什麼不同？

承辦人員：民意信箱的的電子 EMAIL 是由政風室收件，之後列印紙本送到秘書室總收去掛文號後，就會轉到陳情承辦人處理。首長信箱則是由專人負責收件，由專人列印紙本後，也是送到秘書室總收掛文號，之後也是轉到陳情承辦人處理。

iv. 訪談人提問：有關陳情程序所蒐集的陳情人個人資料型式是紙本跟電子檔兩種都有？

承辦人員：是的。

v. 訪談人：今天的訪談到此為結束，謝謝兩位的合作，下次再就行政執行署內部處理流程進行訪談。

b.第二次訪談

I.訪談地點：行政執行署 3 樓會議室

本報告之智慧財產權歸屬於法務部

II.訪談時間：民國 101 年 5 月 3 日

III.訪談人：資策會科法所楊光華研究員、張曉芸研究員、廖淑君研究員

IV.受訪人：資訊室以及業務承辦人員

V.訪談內容：

i. 訪談人提問：上次針對行政執行署陳情程序蒐集個人資料方法及個人資料項目進行訪談，今天是要針對行政執行署內部處理、利用個人資料流程進行確認。請問行政執行署在從郵寄、傳真、親自遞交、言詞提出、電子信箱及電子公文交換後，是怎麼處理這些資料的？

業務人員：行政執行署在收到這些資料資後都先送到秘書室總收掛文號，再依照是紙本還是電子公文分別以紙本或電子公文線上簽核系統轉到陳情承辦人。

ii. 訪談人提問：秘書室總收那邊是如何處理收文程序？

業務人員：秘書室總收將紙本公文透過電子公文交換系統掛文號後，將案件文頭以紙本列印後，開始跑紙本公文簽核程序；電子公文的話，就在電子公文交換系統上掛文號之後，以電子公文型式，開始跑公文線上簽核系統。秘書室總收那邊會有總收文目錄來管理所有掛文的文號跟文頭。

iii. 訪談人提問：陳情文件在掛文號之後在陳情承辦人是如何處理？

業務人員：如陳情處理流程圖所示，陳情承辦人在分到文之後，會先判斷是否為行政執行署業務範圍，如果不是行政執行署業務範圍，就依照是紙本還是電子公文的不同，擬具回覆函，按照紙本簽核程序或公文線上簽核系統經核稿登記桌再經過核稿主管簽核；之後在依照是紙本還是電子公文，以紙本回覆函或是 EMAIL 回覆陳情人，但是要副知其他機關的回覆函都是以電子公文型式，由秘書室總發的電子公文交換系統交換

本報告之智慧財產權歸屬於法務部

到其他機關。如果是行政執行署業務範圍的陳情案件，先由陳情承辦人擬具回覆函，再看需不需要會辦屬內其他單位，如果不需要，就按紙本簽核程序或公文線上簽核系統經核稿登記桌、核稿主管簽核後，以紙本或電子 EMAIL 型式回覆陳情人；如果需要會辦其他單位，就會在經過該單位的收發登記桌，再轉到會辦人手上，之後再回到陳情承辦人單位，在經過核稿登記桌、核稿主管簽核後，以紙本或 EMAIL 或電子公文回覆陳情人。

iv. 訪談人：今天的訪談到此為結束，謝謝兩位的合作，下次再就行政執行署內部處理流程進行訪談。

c.第三次訪談

I.訪談地點：行政執行署 2 樓會議室

II.訪談時間：民國 101 年 5 月 9 日

III.訪談人：資策會科法所楊光華研究員

IV.受訪人：資訊室以及業務人員

V.訪談內容：

i. 訪談人提問：上次針對行政執行署於陳情程序處理及利用陳情當事人個人資料的方法進行確認，今天要對行政執行署儲存陳情程序當事人個人資料進行確認。從陳情人陳情開始，陳情業務承辦人、會辦人及公文簽核流程中如何保存及儲存相關資料的？

業務人員：紙本陳情書文件就會透過紙本簽核程序，紙本資料結案前會先存在承辦人檔案櫃中，在結案之後就會轉到檔案室保存。簽核流程應該沒有人會另外留存影本資料。署長信箱是透過署長秘書的 OUTLOOK 信箱來收信，所以署長秘書的電腦會有相關 EMAIL 的電子檔，收信後列印成紙本，就按照紙本簽核程序來跑，之後也是轉到檔案室留存。民意信箱是由政風室收件，政風室承辦人於收信後，也是列印紙本跑公文簽核

本報告之智慧財產權歸屬於法務部

程序，最後也是轉到檔案室留存。由其他機關移送或需協調的陳情案件都是透過電子公文交換過來，如果附件檔案過大，就會列印成紙本，跑紙本公文簽核流程，在簽核完畢會轉成電子檔，在透過電子公文交換系統交換出去，紙本資料也是轉到檔案室留存；如果是檔案小的，就會按照按電子公文簽核流程進行簽核，再由電子公文交換系統交換出去。

ii. 訪談人提問：在前面處理流程中，各個承辦人會留存資料嗎？

業務人員：除了剛剛所提到署長秘書的 OUTLOOK 電子信箱會存，政風室承辦人也會存在電腦中，秘書室總收掛文號也會存，會辦人會辦簽核會存，核稿登記桌要修改回覆函稿，所以也會存，秘書室總發也會存，陳情承辦人要擬回覆函稿，所有的資料也一定會存，另外紙本資料也會掃瞄成 PDF 檔留存；資訊室會備份秘書室總發的電子公文交換系統資料，所以也會備份到磁帶裡。

iii. 訪談人：所以儲存的資料除了紙本之外，電子檔有儲存於個人電腦硬碟、有儲存於資料庫、磁帶的各種型態嗎？

業務人員：目前的狀況是這樣的。

iv. 訪談人：今天的訪談到此為止，謝謝兩位的合作，會將這三次訪談的結果所繪製行政執行署內部個人資料作業流程圖及盤點清冊完成後，請二位檢視。

本報告之智慧財產權歸屬於法務部

（7）法務部行政執行署陳情程序之個人資料盤點清冊

表 18：法務部行政執行署陳情程序之個人資料盤點清冊

核決	個人資料保護管理召集人
製表	單位:

個人資料盤點清冊

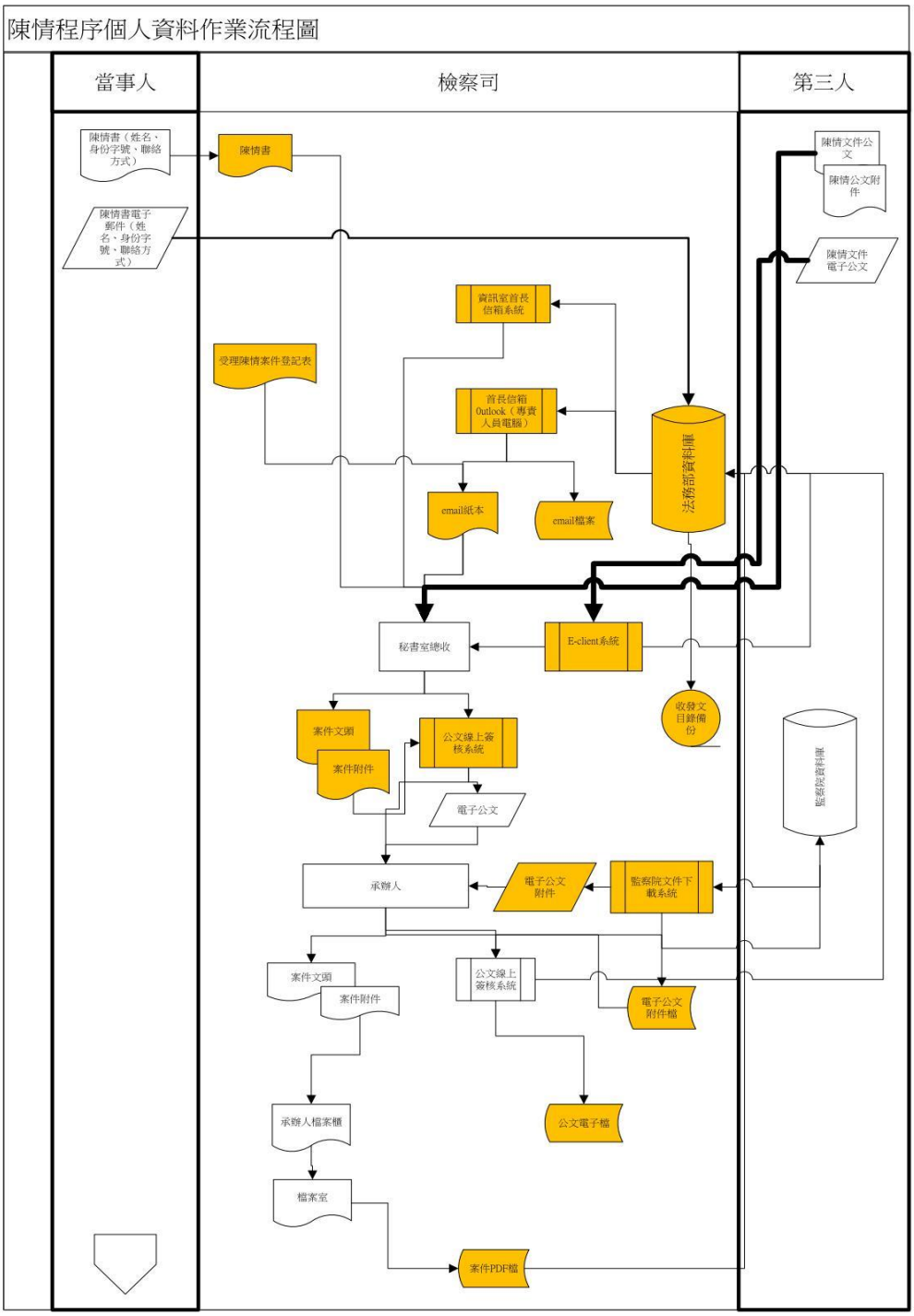
No	作業流程名稱	個人資料文件、檔案名稱	個人資料項目	特定目的	特定情形	蒐集方法	保存場所	保存形態	保存期間	件數	廢棄方法	管理人	存取權限	當事人權利行使對象	委託提供
1	陳情程序	陳情書	姓名、身份證字號、聯絡方式	陳情	執行法定職務（行政程序法§170Ⅰ）	直接	承辦人檔案櫃	紙本	10年			承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
2	陳情程序	受理陳情案件登記表	姓名、身份證字號、聯絡方式	陳情	執行法定職務（行政程序法§170Ⅰ）	直接	承辦人檔案櫃	紙本	10年			承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
3	陳情程序	受理陳情案件登記表附件		陳情	執行法定職務（行政程序法§170Ⅰ）	直接	承辦人檔案櫃	紙本				承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
4	陳情程序	陳情文件公文	姓名、身份證字號、聯絡方式	陳情	執行法定職務（行政程序法§170Ⅰ）	間接	承辦人檔案櫃	紙本				承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
5	陳情程序	陳情公文附件		陳情	執行法定職務（行政程序法§170Ⅰ）	間接	承辦人檔案櫃	紙本				承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
6	陳情程序	陳情電子公文	姓名、身份證字號、聯絡方式	陳情	執行法定職務（行政程序法§170Ⅰ）	間接	公文線上簽核系統（法務部資料庫）	電子檔				承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
7		陳情電子公文附件		陳情	執行法定職務（行政程序法§170Ⅰ）	間接	公文線上簽核系統（法務部資料庫）	電子檔				承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有

資料來源：本計畫自行製作

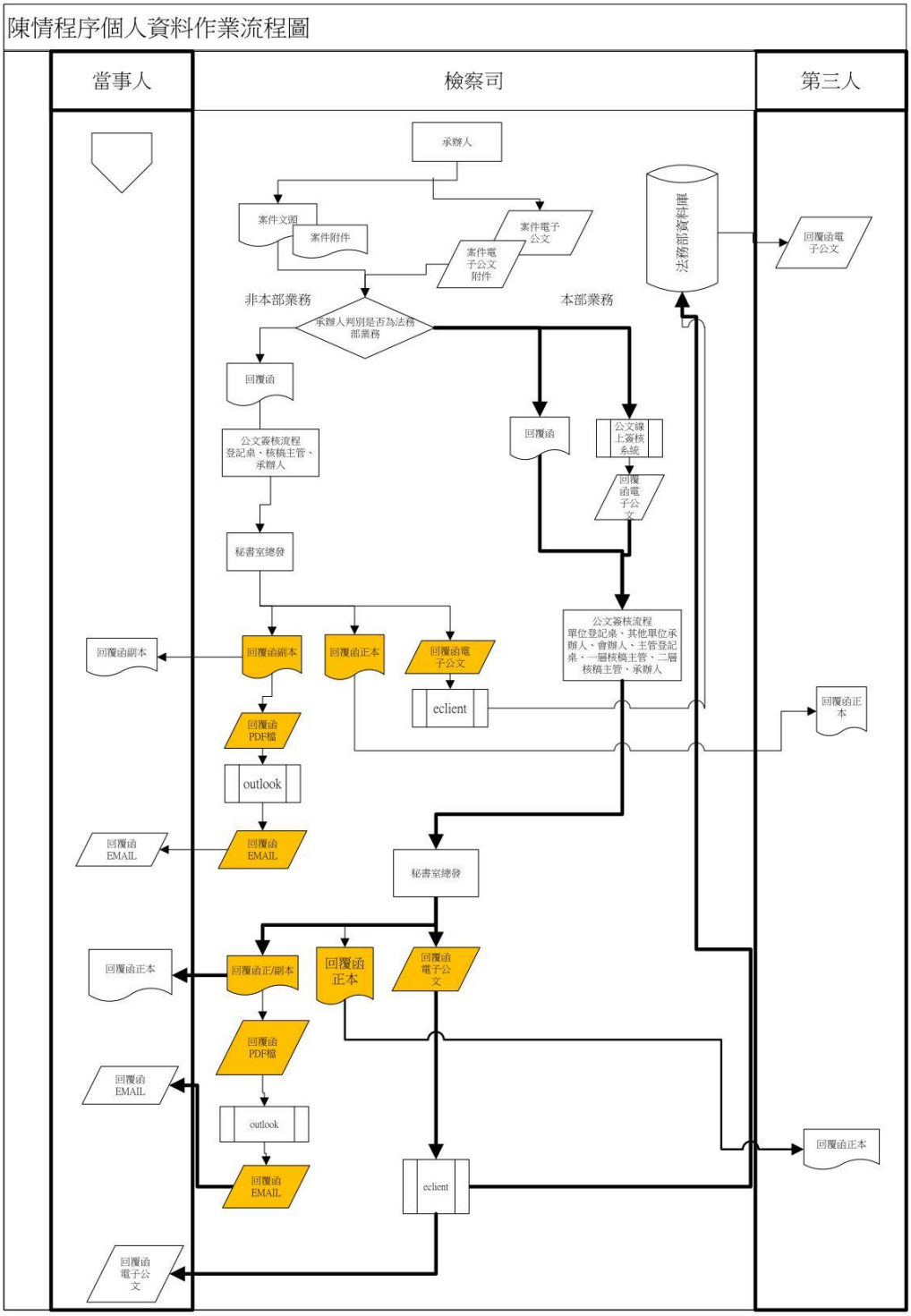
本報告之智慧財產權歸屬於法務部

5.法務部檢察司陳情程序

（1）陳情程序個人資料作業流程圖



本報告之智慧財產權歸屬於法務部



資料來源：本計畫自行製作

圖 4：陳情程序個人資料作業流程圖

本報告之智慧財產權歸屬於法務部

（2）法務部檢察司個人資料盤點程序

A. 目的

為建立法務部檢察司符合我國個人資料保護法及 100 年 10 月間預告之個資法施行細則修正草案之界定個人資料範圍之管理要求，特訂定本作業程序，以便法務部檢察司同仁皆能有效遵循個資盤點之規範。

B. 遵循法規

a.行政程序法第 168 條至第 173 條（民國 94 年 12 月 28 日修正）

b.行政院暨所屬各機關處理人民陳情案件要點（中華民國九十一年十一月廿二日行政院院臺秘字第 0910058540 號函修正第六點、第八點、第十三點，九十一年十一月二十八日會研字第 09100249251 號函分行，並定自民國九十二年一月一日起施行）

c.法務部陳情請願疏處小組作業要點（中華民國八十九年十一月一日法務部 (89) 法秘決字第 000507 號函修正發布）

C. 相關文件

詳見表 17：法務部受理陳情請願事件登記簿

本報告之智慧財產權歸屬於法務部

D. 個資盤點程序

本機關各部門業管人員針對行政業務項目或服務相關的個人資料進行盤點，並經個人資料保護管理召集人審核及核決。

a.由各個部門清查所持有的個人資料。

b.清查個人資料應考量下列事項進行。1.個資的生命週期 2.蒐集、處理利用程序 3.業管人員 4.保存形式 5.保存處所 6.委託提供流向 7.刪除銷毀方法 8.其他

E. 登載個人資料

盤點出本機關應管理之個人資料,由該○○部門主管向個人資料保護管理召集人報請核決後，登載於「個人資料盤點清冊」。

F. 個人資料盤點清冊檢視及修訂

○○部門業管人員為維持個資盤點清冊為最新之狀態,應定期於每年○月，或於機關行政業務項目、範圍有新增變動時，或個人資料保護法及其他相關法令規範有修

G. 法務部檢察司個資盤點輔導訪談記錄

a.第一次訪談

I.訪談地點：法務部 4 樓會議室

II.訪談時間：民國 101 年 5 月 3 日

III.訪談人：資策會科法所楊光華研究員

IV.受訪人：承辦科長

V.訪談內容：

ⅰ. 訪談人提問:檢察司陳情程序蒐集個人資料方法及個人資料項目有哪些？

本報告之智慧財產權歸屬於法務部

承辦科長：檢察司陳情程序蒐集個人資料的方法有陳情人用郵寄或傳真、陳情人以言詞提出後由陳情承辦人填寫受理陳情請願事件登記簿、從網路的民意信箱及首長信箱等幾個管道；所蒐集的個人資料有具體陳訴事項、姓名、國民身分證統一編號或其他身分證件號碼及包括電話、住址、傳真號碼或電子郵件位址的聯絡方式。陳情書並沒有固定的格式，只要陳情人有填寫陳情事項、姓名、身份證件號碼、聯絡方式的書面就足夠了。

ii. 訪談人提問：除了剛剛所說的陳情管道以外是否還有其他蒐集陳情人個人資料的管道？

承辦科長：除了剛剛所提的管道之外，由其他機關，特別是監察院移送過來的陳情案件數量為最多，這種移送陳情案件都會透過秘書室的電子公文交換系統轉到陳情承辦人。

iii. 訪談人提問：從網路上首長信箱的網頁，所蒐集陳情案件的個人資料是由什麼管道轉給陳情承辦人的？

承辦科長：首長信箱會區分為兩個系統，一個是法務部資訊室的首長信箱系統，另一個是首長信箱；法務部資訊室的首長資訊系統的陳情案件，會由資訊室收件後，以電子公文型式送到秘書室總收掛文號，之後就會轉到檢察司陳情承辦人處理。首長信箱則是由專人負責收件，由專人列印紙本後，也是送到秘書室總收掛文號，之後也是轉到檢察司陳情承辦人處理。

iv. 訪談人提問：有關陳情程序所蒐集的陳情人個人資料型式是紙本跟電子檔兩種都有？那監察院移送過來的電子公文跟附是透過什麼方式取得？

承辦科長：所蒐集的資料紙本跟電子檔兩種型式都有；監察院移送過來的陳情案件是透過電子公文交換系統，之後會給一組 ID 跟密碼，讓承辦人自行到監察院文件下載系統去下載。

v. 訪談人提問：由秘書室總收掛文號之後，陳情承辦人如何處理陳情案件？

vi. 承辦科長：秘書室總收將紙本公文透過電子公文交換系統掛文

本報告之智慧財產權歸屬於法務部

號後，將案件文頭以紙本列印後，開始跑紙本公文簽核程序；電子公文的話，就在電子公文交換系統上掛文號之後，以電子公文型式，開始跑公文線上簽核系統。秘書室總收那邊會有總收文目錄來管理所有掛文的文號跟文頭。陳情承辦人在分到文之後，會先判斷是否為法務部業務範圍，如果不是法務部業務範圍，就依照是紙本還是電子公文的不同，擬具回覆函，按照紙本簽核程序或公文線上簽核系統經核稿登記桌再經過核稿主管簽核；之後在依照是紙本還是電子公文，以紙本回覆函或是 EMAIL 回覆陳情人，但是要副知其他機關的回覆函都是以電子公文型式，由秘書室總發的電子公文交換系統交換到其他機關。

vii. 訪談人：今天的訪談到此為結束，謝謝科長的合作，下次再就法務部檢察司內部處理流程進行訪談。

b.第二次訪談

I.訪談地點：法務部 4 樓會議室

II.訪談時間：民國 101 年 5 月 7 日

III.訪談人：資策會科法所楊光華研究員

IV.受訪人：承辦科長

V.訪談內容：

i. 訪談人提問：如果是法務部業務範圍的陳情案件陳情承辦人會如何處理？

承辦科長：如果是法務部業務範圍的陳情案件，先由陳情承辦人擬具回覆函，再看需不需要會辦屬內其他單位，如果不需要，就按紙本簽核程序或公文線上簽核系統，再視是否要經一級簽核或二級簽核，分別經過核稿登記桌、核稿主管司長簽核後，或核稿登記桌、核稿主管司長再轉送到部內一級主管的部長或次長核決，之後再以紙本或電子 EMAIL 型式回覆陳情人；如果需要會辦其他單位，就會在經過該單位的收發登記

本報告之智慧財產權歸屬於法務部

桌，再轉到會辦人手上，之後再回到陳情承辦人單位，在經過核稿登記桌、核稿主管司長再視是否要經一級簽核或二級簽核，分別經過核稿登記桌、核稿主管司長簽核後，或核稿登記桌、核稿主管司長，再視是否要經過二級簽核，如果是二級簽核就再轉送到部內一級主管的部長或次長核決，簽核後，以紙本或 EMAIL 或電子公文回覆陳情人。

ii. 訪談人提問：從陳情人陳情開始，陳情業務承辦人、會辦人及公文簽核流程中如何保存及儲存相關資料的？

承辦科長：紙本陳情書文件就會透過紙本簽核程序，紙本資料結案前會先存在承辦人檔案櫃中，在結案之後就會轉到檔案室保存。簽核流程應該沒有人會另外留存影本資料。首長信箱是透過專人的 OUTLOOK 信箱來收信，所以專人的電腦會有相關 EMAIL 的電子檔，收信後列印成紙本，就按照紙本簽核程序來跑，之後也是轉到檔案室留存。資訊室首長信箱系統是由法務部資訊室收件，資訊室承辦人於收信後，就以線上公文簽核系統跑公文簽核程序，最後也是轉到檔案室留存。由其他機關如監察院移送的陳情案件都是透過電子公文交換過來，都會透過公文下載系統下載為電子檔，以線上公文簽核系統跑公文簽核流程，於完成簽核會透過電子公文交換系統交換出去，紙本資料也是轉到檔案室留存。

iii. 訪談人提問：在前面處理流程中，各個承辦人會留存資料嗎？

承辦科長：除了剛剛所提到專人的 OUTLOOK 電子信箱會存，資訊室承辦人也會存在電腦資料庫中，秘書室總收掛文號也會存，會辦人會辦簽核會存，核稿登記桌要修改回覆函稿，所以也會存，秘書室總發也會存，陳情承辦人要擬回覆函稿，所有的資料也一定會存，另外紙本資料也會掃瞄成 PDF 檔留存；資訊室會備份秘書室總發的電子公文交換系統資料，所以也會備份到磁帶裡。

iv. 訪談人提問：所以儲存的資料除了紙本之外，電子檔有儲存於個人電腦硬碟、有儲存於資料庫、磁帶的各種型態嗎？

本報告之智慧財產權歸屬於法務部

承辦科長：目前的狀況是這樣的。

v. 訪談人：今天的訪談到此為止，謝謝科長的合作，會將這兩次訪談的結果所繪製檢察司內部個人資料作業流程圖及盤點清冊完成後，請科長檢視。

本報告之智慧財產權歸屬於法務部

（3）法務部檢察司陳情程序之個人資料盤點清冊

表 19：法務部檢察司陳情程序之個人資料盤點清冊

核決	個人資料保護管理召集人
製表	單位:

個人資料盤點清冊

No	作業流程名稱	個人資料文件、檔案名稱	個人資料項目	特定目的	特定情形	蒐集方法	保存場所	保存形態	保存期間	件數	廢棄方法	管理人	存取權限	當事人權利行使對象	委託提供
1	陳情程序	陳情書	姓名、身份證字號、聯絡方式	陳情	執行法定職務（行政程序法§170Ⅰ）	直接	承辦人檔案櫃	紙本	10年			承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
2	陳情程序	受理陳情案件登記表	姓名、身份證字號、聯絡方式	陳情	執行法定職務（行政程序法§170Ⅰ）	直接	承辦人檔案櫃	紙本	10年			承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
4	陳情程序	陳情文件公文	姓名、身份證字號、聯絡方式	陳情	執行法定職務（行政程序法§170Ⅰ）	間接	承辦人檔案櫃	紙本				承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
5	陳情程序	陳情公文附件		陳情	執行法定職務（行政程序法§170Ⅰ）	間接	承辦人檔案櫃	紙本				承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
6	陳情程序	陳情電子公文	姓名、身份證字號、聯絡方式	陳情	執行法定職務（行政程序法§170Ⅰ）	間接	公文線上簽核系統	電子檔				承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
7	陳情程序	陳情電子公文附件		陳情	執行法定職務（行政程序法§170Ⅰ）	間接	公文線上簽核系統	電子檔				承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
8	陳情程序	首長信箱EMAIL檔案	姓名、身份證字號、聯絡方式	陳情	執行法定職務（行政程序法§170Ⅰ）		署長秘書個人電腦OUTLOOK文件夾	電子檔			無	專人	專人	可	有
9	陳情程序	OUTLOOK系統					署長秘書個人電腦					專人	專人	不可	無

資料來源：本計畫自行製作

本報告之智慧財產權歸屬於法務部

6.確認單

（1）內政部地政司地政資訊作業科

（2）內政部警政署刑事警察局預防科 165 反詐騙諮詢專線

（3）法務部行政執行署

（4）法務部檢察司

（因確認單內含有參與人員之個人資料，故在此予以移除，詳細確認單已附於呈繳法務部之「統計個資保護執行與成果報告」）

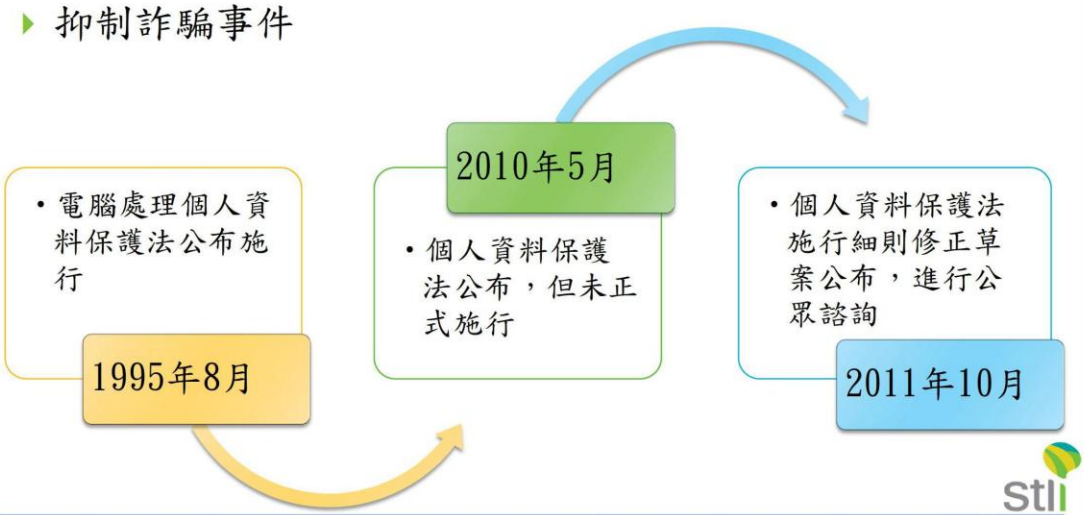
本報告之智慧財產權歸屬於法務部

7.試行機關導入演練課程簡報

本報告之智慧財產權歸屬於法務部

個人資料保護法的修法緣由與歷程

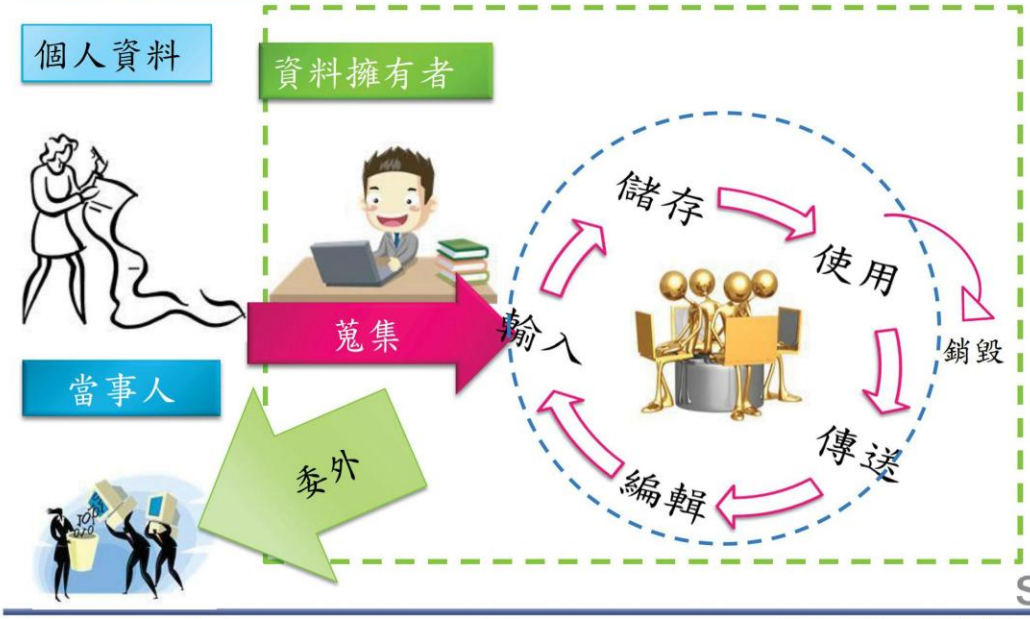
- 適用主體與保護客體範圍有限，未能因應社會發展趨勢
- 與國際資訊隱私保護發展趨勢接軌
- 抑制詐騙事件



 © 2012資訊工業策進會

個人資料保護法架構(1/2)

個人資料生命週期



 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個人資料保護法架構(2/2)

第一章　總則（第1條至第14條）

- 目的 / 定義 / 當事人權利 / 委外/個人資料的蒐集、處理與利用原則 / 特種個人資料/書面同意 /當事人告知 /答覆當事人查詢、提供閱覽或複製本/ 個人資料的正確性/個資違法事件通知/回覆當事人權利行使/費用收取

第二章　公務機關對個人資料之蒐集、處理與利用（第15條至第18條）

- 特定目的內/特定目的外/個人資料持有資訊之公開/個人資料檔案之安全維護事項

第三章 非公務機關對個人資料之蒐集、處理與利用（第19條至第27條）

- 特定目的內/特定目的外/國際傳輸/行政檢查/違反個資法之行政處分/行政檢查結果公布/個人資料檔案之安全維護事項

第四章 損害賠償及團體訴訟（第28條至第40條）

第五章 罰則（第41條至第50條）

第六章 附則（第50條至第56條）

© 2012資訊工業策進會

個人資料保護法vs.公務機關

個人資料的蒐集、處理與利用者

- 保護客體-個人資料
- 適用主體-公務機關
- 當事人權利保護及行使
- 個人資料的蒐集、處理與利用
- 個人資料之保存、維護與銷毀
- 個人資料持有資訊之公開
- 委外
- 損害賠償
- 罰則

對非公務機關蒐集、處理、利用個人資料的管理與監督

- 行政監督

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

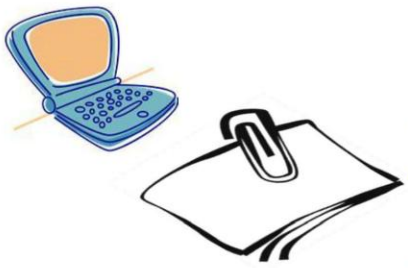
政府機關：
個人資料的蒐集、處理與利用者

保護客體-個人資料
適用主體-公務機關
當事人權利保護及行使
個人資料的蒐集、處理與利用
個人資料之保存、維護與銷毀
個人資料持有資訊之公開
委外
損害賠償
罰則

科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

 © 2012資訊工業策進會

保護客體：個人資料



自然人之姓名、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、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料（個資法§2）

本法第二條第一款所稱得以間接方式識別該個人之資料，指僅以該資料不能識別，須與其他資料對照、組合、連結等，始能識別該特定個人者。但查詢困難、需耗費過鉅或耗時過久始能特定者，不在此限。(個人資料保護法施行細則草案§3)

不適用個人資料保
1. 自然人為單純個
利用個人資料
2. 於公開場所或公
其他個人資料結合

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

特種個人資料(個資法§6)

- 醫療：指病歷以外，其他以治療、矯正或預防人體疾病、傷害、殘缺為目的，所為之診察、診斷及治療；或基於診察、診斷結果，以治療為目的，所為之處方、用藥、施術、或處置等行為全部或一部所產生之個人資料
- 基因：由一段去氧核醣核酸構成，為生物體控制特定功能之遺傳單位訊息
- 性生活：性取向或性慣行之個人資料
- 健康檢查：對於無明顯疾病症狀，非出於對特定疾病診斷或治療之目的，以醫療行為所為診察行為之全部或一部之總稱
- 犯罪前科：指經緩起訴、職權不起訴或法院判決有罪確定之紀錄

(個資法施行細則草案§4)

 © 2012資訊工業策進會

適用主體：公務機關

- 公務機關：指**依法行使公權力**之中央或地方機關或行政法人 (個資法§2)
- 受委託機關
  - 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，於本法適用範圍內，視同委託機關 (個資法§4)
  - 受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之 (個資法施行細則草案§7)

•行政法人：指國家及地方自治團體以外，由中央目的事業主管機關，為執行特定公共事務，依法律設立之公法人（行政法人法§2）
•全國第一個行政法人機構：國立中正文化中心

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

當事人權利保護及行使

- 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

不得預先拋棄
或以特約限制

個人資料保護法第3條

當事人通知

公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或 其他侵害者，應查明後以適當方式通知當事人（個人資料保護法第12條）

以適當方式通知當事人

- 本法第十二條所稱適當方式通知，係指即時以書面、電話、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、新聞媒體或其他足以使公眾得知之方式為之(個資法施行細則草案§18)
- 依本法第十二條通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施(個資法施行細則草案§18)

本報告之智慧財產權歸屬於法務部

個人資料之查詢、閱覽與複本請求

公務機關或非公務機關依當事人請求，就其所蒐集之個人資料，答覆查詢、提供閱覽、或製給複製本(個人資料保護法第10條)

- 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
- 妨害公務機關執行法定職務
- 妨害該蒐集機關或第三人之重大利益

回覆期間

應於15日內，為准駁之決定；必要時，得予延長，延長之期間不得逾15日，並應將其原因以書面通知請求人(個人資料保護法第13條)

費用收取

查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收 必要成本費用(個人資料保護法第14條)

© 2012資訊工業策進會

個人資料之正確性&當事人請求更正與補充

個人資料之正確性

- 公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請 求更正或補充之
- 個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但 因執行職務或業務所必須並註明其爭議或經當事人書面同意者，不在此限
- 因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料， 應於更正或補充後，通知曾提供利用之對象

(個人資料保護法第11條)

回覆期間

應於15日內，為准駁之決定；必要時，得予延長，延長之期間不得逾15日，並應將其原因以書面通知請求人

(個人資料保護法第13條)

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個人資料之刪除、停止處理或利用

個人資料之刪除、停止處理或利用

•個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求， 刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。
•違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求， 刪除、停止蒐集、處理或利用該個人資料。
（個人資料保護法第11條）

回覆期間

應於15日內，為准駁之決定；必要時，得予延長，延長之期間不得逾15日，並應將其原因以書面通知請求人
（個人資料保護法第13條）

© 2012資訊工業策進會

個人資料之蒐集、處理與利用

原則

- 尊重當事人權益
- 依誠實信用方法
- 於特定目的之必要範圍內
- 與蒐集目的間具有正當合理之關聯

一般個人資料

- 當事人告知
- 特定目的內利用
- 特定目的外利用

特種個人資料

原則不得蒐集、處理與利用
例外情形

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個人資料之蒐集、處理與利用原則

- 特定目的之必要範圍內為之
- 與蒐集目的間具有正當合理之關聯
- 尊重當事人之權益
- 依誠實及信用方法為之

蒐集

以任何方式取得個人資料

處理

為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、 編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送

利用

將蒐集之個人資料為處理以外之使用

資料來源：個人資料保護法第2條&第5條

© 2012資訊工業策進會

一般個人資料之蒐集、處理與利用：對於當事人之告知

一般個人資料

自然人之姓名、出生年月日、國民身分證統[illegible]指紋、婚[illegible]病歷、聯[illegible]活動及其[illegible]別該個人[illegible]

直接蒐集

於蒐集時，**告知**當事人

間接蒐集

於處理或利用前，**告知**當事人；得於首次對當事人為利用時併同為之

告知之方式，得以書面、電話、傳真、電子文件或其他適當方式為之(個資法施行細則草案§13)

資料來源：個人資料保護法第8條&第9條

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

對於當事人之告知：直接蒐集

- 告知事項
  - 公務機關機關名稱
  - 蒐集之目的
  - 個人資料之類別
  - 個人資料利用之期間、地區、對象及方式
  - 當事人依第三條規定得行使之權利及方式
  - 當事人得自由選擇提供個人資料時，不提供將對其權益之影響

- 免告知之情況
  - 依法律規定得免告知
  - 個人資料之蒐集係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
  - 告知將妨害公務機關執行法定職務
  - 告知將妨害第三人之重大利益
  - 當事人明知應告知之內容

© 2012資訊工業策進會

對於當事人之告知：間接蒐集

- 告知事項
  - 個人資料來源
  - 公務機關機關名稱
  - 蒐集之目的
  - 個人資料之類別
  - 個人資料利用之期間、地區、對象及方式
  - 當事人依第3條規定得行使之權利及方式

- 免告知之情況
  - 依法律規定得免告知
  - 個人資料之蒐集係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
  - 告知將妨害公務機關執行法定職務
  - 告知將妨害第三人之重大利益
  - 當事人明知應告知之內容
  - 當事人自行公開或其他已合法
  - 不能向當事人或其法定代理人
  - 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限
  - 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料

指個人資料以代碼、匿名或其他揭露方式，無從辨識該特定個人，或需費過鉅或耗時過久始能予以辨識者(個資法施行細則草案§14)

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

一般個人資料：特定目的內利用

- 個人資料的**蒐集或處理**(個資法§15)

- 公務機關對個人資料之**利用**，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(個資法§16)

 © 2012資訊工業策進會

一般個人資料：特定目的外利用

- 法律明文規定
- 為維護國家安全或增進公共利益
- 為免除當事人之生命、身體、自由或財產上之危險
- 為防止他人權益之重大危害
- 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
- 有利於當事人權益
- 經當事人書面同意

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

書面同意-特定目的內

- 當事人經蒐集者告知本法所定應告知事項後，所為允許之書面意思表示（個資法§7）
- 書面意思表示之方式，如其內容可完整呈現，並可於日後取出供查驗者，經蒐集者及當事人同意，得以電子文件為之(個資法施行細則草案§11)

直接蒐集

✓公務機關或非公務機關名稱
✓蒐集之目的
✓個人資料之類別
✓個人資料利用之期間、地區、對象及方式
✓當事人依個資法第3條規定得行使之權利及方式
✓當事人得自由選擇提供個人資料時，不提供將對其權益之影響

間接蒐集

✓個人資料來源
✓公務機關或非公務機關名稱
✓蒐集之目的
✓個人資料之類別
✓個人資料利用之期間、地區、對象及方式
✓當事人依第3條規定得行使之權利及方式

 © 2012資訊工業策進會

書面同意-特定目的外

- 當事人經蒐集 者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響 後，單獨所為之書面意思表示(個資法§7)
- 單獨所為之書面意思表示，如係與其他意思表示於同一書面為之者，應於適當位置使當事人得以知悉其內容後並確認同意(個資法施行細則草案§12)
- 書面意思表示之方式，如其內容可完整呈現，並可於日後取出供查驗者，經蒐集者及當事人同意，得以電子文件為之(個資法施行細則草案§11)

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

特種個人資料之蒐集、處理與利用

特種個人資料

有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料

- 法律明文規定
- 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
- 當事人自行公開或其他已合法公開之個人資料
- 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，且經一定程序所為蒐集、處理或利用之個人資 料

資料來源：個人資料保護法第6條

 © 2012資訊工業策進會

適當安全維護措施

- 本法所稱適當安全維護措施、安全維護事項或適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之必要措施
- 必要措施，以所須支出之費用與所欲達成之個人資料保護目的符合適當比例者為限

- 成立管理組織，配置相當資源
- 界定個人資料之範圍
- 個人資料之風險評估及管理機制
- 事故之預防、通報及應變機制
- 個人資料蒐集、處理及利用之內部管理程序
- 資料安全管理及人員管理
- 認知宣導及教育訓練
- 設備安全管理
- 資料安全稽核機制
- 必要之使用紀錄、軌跡資料及證據之保存
- 個人資料安全維護之整體持續改。

個資法施行細則草案§9

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個人資料之保存、維護與銷毀

個人資料的保存與維護

公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏(個資法§18)

個人資料的刪除與銷毀

- 依當事人請求(個資法§3)
- 特定目的消失或期限屆滿(個資法§11)
- 違反個資法規定蒐集、處理或利用個人資料者（個資法§11）

 © 2012資訊工業策進會

個人資料的保存與維護

- 公務機關保有個人資料檔案者，應訂定個人資料安全維護規定，其內容應包括第9條第2項所定事項(個資法施行細則草案§20)
- 個資法第18條所稱專人，指具有管理及維護個人資料檔案之專業能力，且足以擔任機關檔案資料安全維護經常性工作之人員(個資法施行細則草案§21)
- 公務機關為使專人具有辦理安全維護事項之能力，應辦理或使專人接受相關專業之教育訓練(個資法施行細則草案§21)

- 成立管理組織，配置相當資源
- 界定個人資料之範圍
- 個人資料之風險評估及管理機制
- 事故之預防、通報及應變機制
- 個人資料蒐集、處理及利用之內部管理程序
- 資料安全管理及人員管理
- 認知宣導及教育訓練
- 設備安全管理
- 資料安全稽核機制
- 必要之使用紀錄、軌跡資料及證據之保存
- 個人資料安全維護之整體持續改善

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

EX: 法務部個人資料保護管理要點(1/2)(尚未下達生效)

- 總則：
  - 明定本要點及法務部個人資料保護管理執行小組設置之目的、執行小組之任務、執行小組召集人、執行秘書及委員之組成及幕僚工作之負責單位、執行小組會議召開之期間、主持人及得邀請出列席之人員、指定專人及其辦理事項、設置個人資料保護聯絡窗口及其辦理事項。（草案第一點至第六點）
- 個人資料範圍：
  - 明定本部保有特種資料之個人資料檔案名稱、本部保有個人資料特定目的之項目以本部依適當方式公開者為限，有變更者亦同。（草案第七點及第八點）
- 個人資料之蒐集、處理及利用：
  - 明定個人資料之蒐集、處理或利用之正當法律程序、告知義務之程序、取得當事人書面同意之程序、個人資料補充或更正之程序、資料正確性有爭議之處理程序、刪除、停止處理或利用個人資料之程序、個人資料遭到竊取、洩漏、竄改或遭其他方式侵害之通知處理程序。（草案第九點至第十八點）

資料來源：法務部 http://www.moj.gov.tw/ct.asp?xItem=215772&ctNode=28007&mp=001

 © 2012資訊工業策進會

EX: 法務部個人資料保護管理要點(2/2)(尚未下達生效)

- 當事人行使權利之處理：
  - 明定當事人請求答覆查詢、提供閱覽、製給複製本、更正、補充、停止蒐集、處理、利用或刪除之處理程序、請求查詢、閱覽或製給個人資料複製本適用「法務部及所屬機關提供政府資訊收費標準」之規定並依「法務部受理申請提供政府資訊及閱覽卷宗須知」辦理、明定本部保有之個人資料檔案仍適用政府資訊公開法或相關法律規定，限制公開或不予提供。（草案第十九點至第二十三點）
- 個人資料檔案安全維護：
  - 明定專人應依本要點及相關法令規定辦理個人資料檔案安全維護事項、建立個人資料檔案應建立管理制度及人員安全管理規範、明定個人資料檔案安全稽核之組織及程序規定、個人資料檔案發生非法入侵情事之緊急應變與通報程序、個人資料檔案安全維護工作應符合本要點、行政院及本部訂定之相關資訊作業安全與機密維護規範。（草案第二十四點至第二十八點）
- 附則：
  - 明定本部委託蒐集、處理或利用個人資料者，亦適用本要點。（草案第二十九點）

資料來源：法務部 http://www.moj.gov.tw/ct.asp?xItem=215772&ctNode=28007&mp=001

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個人資料持有資訊之公開

- 公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同(個資法§17)
  - 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
  - 個人資料之類別

•公務機關依本法第十七條規定為公開時，應於建立個人資料檔案後一個月內為之；變更時，亦同。公開方式應予以特定，並避免任意變更
•本法第十七條所稱其他適當方式，指利用新聞紙、雜誌、政府公報、電子報或其他可供公眾查閱之方式為公開
(個資法施行細則草案§19)

 © 2012資訊工業策進會

Ex:法務部保有個人資料檔案公開項目彙整表

項目 編號	個人資料檔案名稱	保有依據	個人資料類別	保有單位
1	記者採訪證申請表	法務部組織法第 2 條	識別類（C001 識別個人者、C003 政府資料中之辨識者）	綜合規劃司
2	立法院立法委員助理名冊	法務部組織法第 2 條	識別類（C001 識別個人者）	綜合規劃司
3	立法委員通訊錄	法務部組織法第 2 條	識別類（C001 識別個人者）	綜合規劃司
4	行政院人權保障推動小組委員名單	法務部組織法第 2 條 法務部處務規程第 7 條	識別類（C001 識別個人者、C003 政府資料中之識別者）、特徵類（C011 個人描述）、社會狀況（C038 職業）、教育、技術或其他專業（C054 職業專長）	法制司
			識別類（C001 識別個人者、C003 政府資料中之識別	

資料來源：法務部
http://www.moj.gov.tw/ct.asp?xItem=257410&ctNode=28007&mp=001

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個人資料蒐集、處理或利用之委外(1/2)

- 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，於本法適用 範圍內，視同委託機關 (個資法§4)
- 受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之 (個資法施行細則草案§7)

© 2012資訊工業策進會

個人資料蒐集、處理或利用之委外(2/2)

公務機關

適當監督

受委託機關

- 應對受託人為適當之監督
- 委託人應定期確認受託人執行之狀況，並將確認結果記錄之(個資法施行細則草案§8)

- 僅得於委託人指示之範圍內，蒐集、處理或利用個人資料
- 受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人

- 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
- 受託人就施行細則第9條第2項應採取之必要措施
- 有複委託者，其約定之受託人
- 受託人或其受僱人違反個人資料保護法規或委託契約條款時，應向委託人通知之事項及採行之補救措施
- 委託人對受託人保留指示之事項
- 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

損害賠償(1/2)

- 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害 當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限(個資法§28)
- 損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同(個資法§30)
- 損害賠償，除依本法規定外，公務機關適用國家賠償法之規定 (個資法§31)
- 依本法規定對於公務機關提起損害賠償訴訟者，專屬該機關所在地之地方法院管轄(個資法§33)

 © 2012資訊工業策進會

損害賠償(2/2)

•財產損害賠償
•非財產損害
•回復名譽之適當處分

不易或不能證明其實際損害

如被害人不易或不能證明其實際損害額時，得請求法院依 侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算

資料來源：個人資料保護法第28條

➢對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害 賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益 超過新臺幣二億元者，以該所涉利益為限

➢同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受定每人每一事件最低賠償金額新臺幣五百元之限制

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

罰則(1/2)

•**違法蒐集、利用及處理個人資料**， 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

•**意圖營利**犯前項之罪者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金

（個人資料保護法§41）

•**意圖為自己或第三人不法之利益或損害他人之利益**，而對於個人資料檔案為**非法變更、刪除或以其他非法方法**，致**妨害個人資料檔案之正確而足生損害於他人者**，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金 （個人資料保護法§ 42）

 © 2012資訊工業策進會

罰則(2/2)

- 中華民國人民在中華民國領域外對中華民國人民犯前二條之罪者，亦適用之(個資法§43)
- 公務員假借職務上之權力、機會或方法，犯本章(第5章罰則)之罪者，加重其刑至二分之一(個資法§44)
- 本章(第5章罰則)之罪，須告訴乃論。但犯第四十一條第二項之罪者，或對公務機關犯第四十二條之罪者，不在此限(個資法§45)
- 犯本章(第5章罰則)之罪，其他法律有較重處罰規定者，從其規定(個資法§46)

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

政府機關：
對非公務機關蒐集、處理、利用個人資料的管理與監督

行政檢查
行政處罰
採取必要處分，以保護當事人權益不被繼續侵害

科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

© 2012資訊工業策進會

對各行業個資保護之行政監督

1. 行政檢查(個人資料保護法第22條)
2. 經非公務機關同意，得公布檢查結果(個人資料保護法第26條)

依法裁處罰鍰(個人資料保護法第47條與48

採取必要處分，以保護當事人權益不被繼續侵害(個人資料保護法第25條)

- 禁止蒐集、處理或利用個人資料
- 命令刪除經處理之個人資料檔案
- 沒入或命銷燬違法蒐集之個人資料
- 公布非公務機關之違法情形，及其姓名或名稱與負責人

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

行政檢查&公布檢查結果 (1/2)

- 行政檢查(個資法§22)
  - 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。
  - 中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之
  - 對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之

 © 2012資訊工業策進會

行政檢查&公布檢查結果(2/2)

- 中央目的事業主管機關或直轄市、縣（市）政府為第一項檢查時，得率同 資訊、電信或法律等專業人員共同為之
- 對於第1項及第2項之進入、檢查或處分，非公務機關及其相關人員不得 規避、妨礙或拒絕
- 參與檢查之人員，因檢查而知悉他人資料者，負保密義務
- 公布檢查結果(個資法§26)
  - 中央目的事業主管機關或直轄市、縣（市）政府依第22條規定檢查後，**未發現有違反本法規定之情事者，經該非公務機關同意後**，得公布檢查結果

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

依法裁處罰鍰(1/3)

- 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之(個資法§47)
  - 違反第六條第一項規定(特種個人資料之蒐集、處理與利用)
  - 違反第十九條規定(非公務機關對一般個人資料之蒐集、處理與利用)
  - 違反第二十條第一項規定(非公務機關對一般個人資料之特定目的外利用)
  - 違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分(國際傳輸)

© 2012資訊工業策進會

依法裁處罰鍰(2/3)

- 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰(個資法§48)
  - 違反第八條或第九條規定(當事人告知)
  - 違反第十條、第十一條、第十二條或第十三條規定(當事人權利行使)
  - 違反第二十條第二項或第三項規定(非公務機關利用個人資料行銷者)
  - 違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

依法裁處罰鍰(3/3)

- 非公務機關無正當理由違反第二十二條第四項規定者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二十萬元以下罰鍰(個資法§49)(進入非公務機關進行檢查)
- 非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定(第48條至49條)受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰(個資法§50)

© 2012資訊工業策進會

採取必要處分，以保護當事人權益不被繼續侵害

- 非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣（市）政府除依本法規定裁處罰鍰外，並得為下列處分(個資法§25)
  - 禁止蒐集、處理或利用個人資料
  - 命令刪除經處理之個人資料檔案
  - 沒入或命銷燬違法蒐集之個人資料
  - 公布非公務機關之違法情形，及其姓名或名稱與負責人。
- 中央目的事業主管機關或直轄市、縣（市）政府為前項處分時，應於防制違反本法規定情事之必要範圍內，採取對該非公務機關權益損害最少之方法為之(個資法§25)

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

對於個人資料保護法通過之因應

科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

 © 2012資訊工業策進會

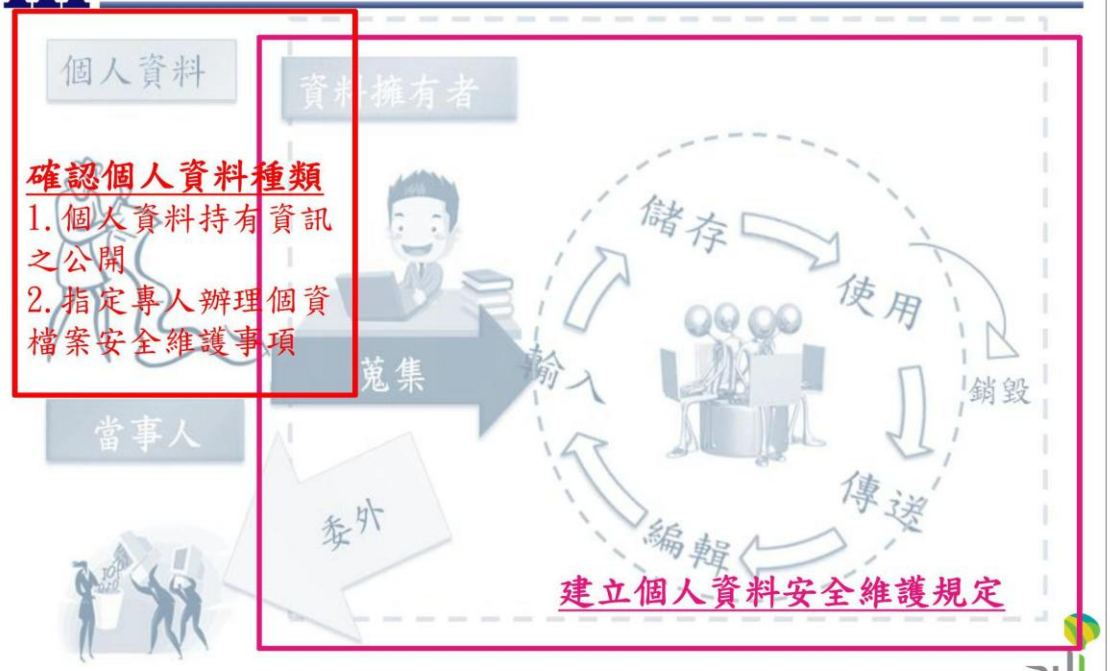
新法實施後...公務機關面臨之難題

- 對於保護客體與規範主體之範圍認識不清
- 不確定資料主體之權利及行使程序
- 欠缺行政檢查工作之實施及項目之概念
- 如何整合個資管理制度與現行機關內之管理程序
- 如何確認公務機關同仁對於個資保護已具備基礎概念

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

對於個人資料保護法通過之因應(1/2)



 © 2012資訊工業策進會

對於個人資料保護法通過之因應(2/2)

- 個人資料持有資訊之公開
  - 應將特定事項公開於電腦網站供公眾查詢，例如法務部公告“法務部保有個人資料檔案公開項目彙整表”
- 各公務機關應指定「專人」辦理個人資料檔案安全維護事項
  - 例如:法務部設置個人資料保護管理執行小組
- 公務機關保有個人資料檔案者，訂定個人資料安全維護規定
  - 例如:法務部草擬“法務部個人資料保護管理要點”
- 公務人員個資保護認知及法治概念之增進

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

資料來源：資策會科法所

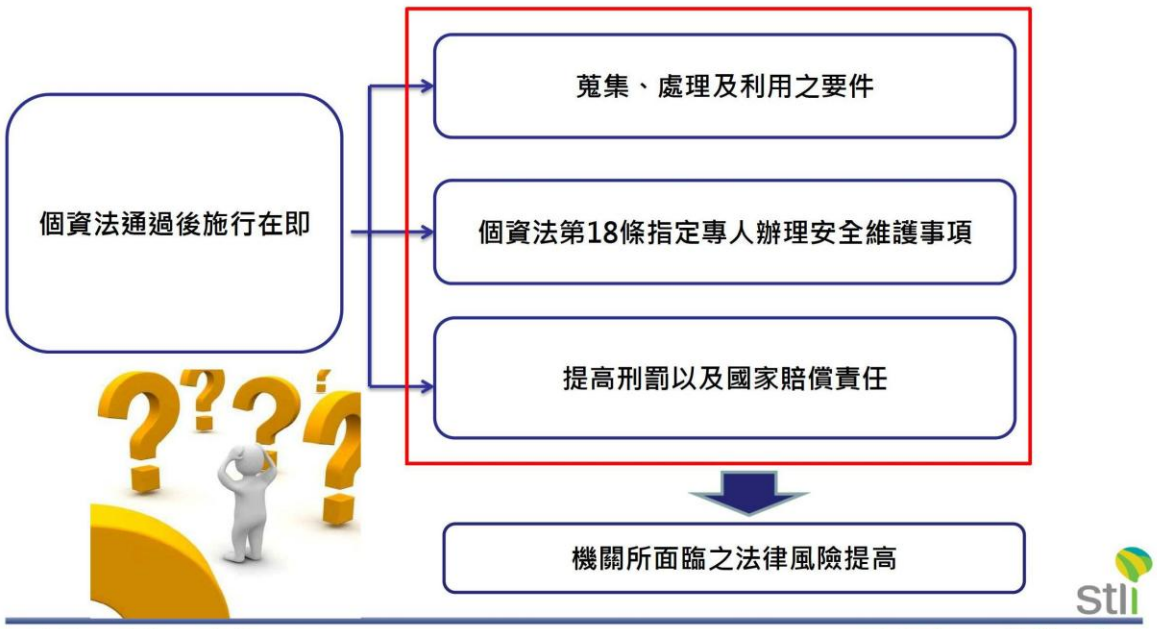
本報告之智慧財產權歸屬於法務部

個人資料保護執行管理暨考核作業手冊(草案)介紹

資訊工業策進會　科技法律研究所
陳秭璇 律師
irenechen@iii.org.tw
2012年5月15日

© 2012資訊工業策進會

前言



© 2012資訊工業策進會

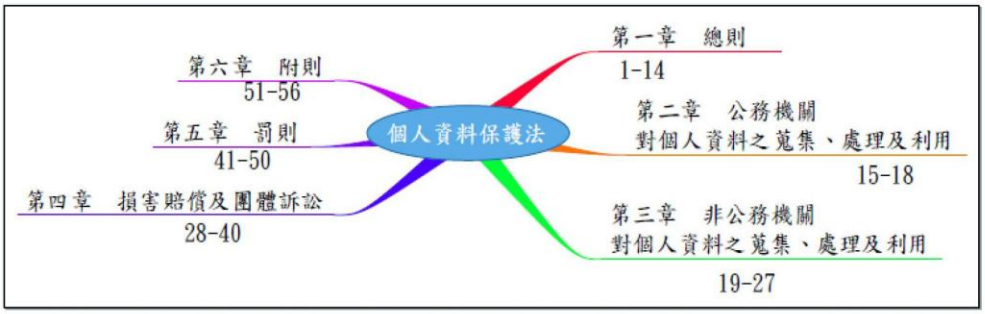
本報告之智慧財產權歸屬於法務部

大綱

◆目的

◆作業手冊介紹

個資法之法規範目的

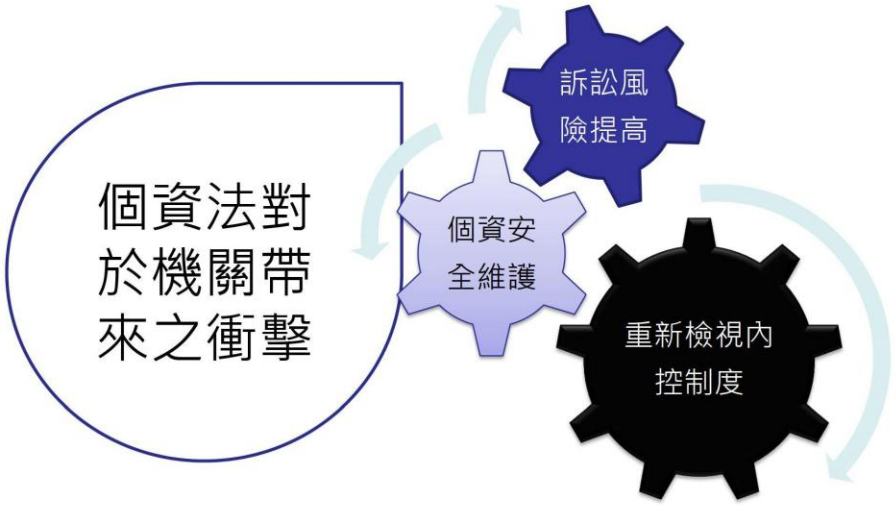


•目的

規範個人資料之蒐集、處理及利用，
以避免人格權受侵害，
並促進個人資料之合理利用

本報告之智慧財產權歸屬於法務部

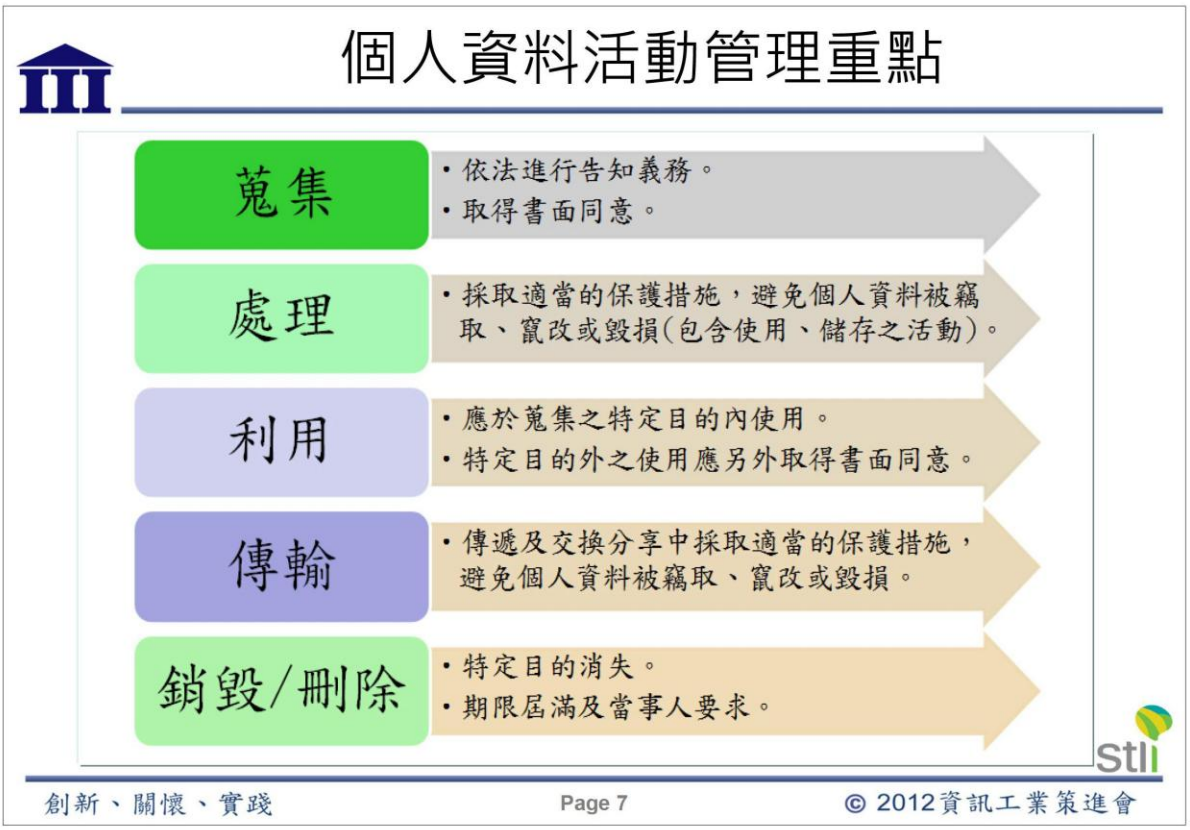
因應個人資料保護法對機關之影響

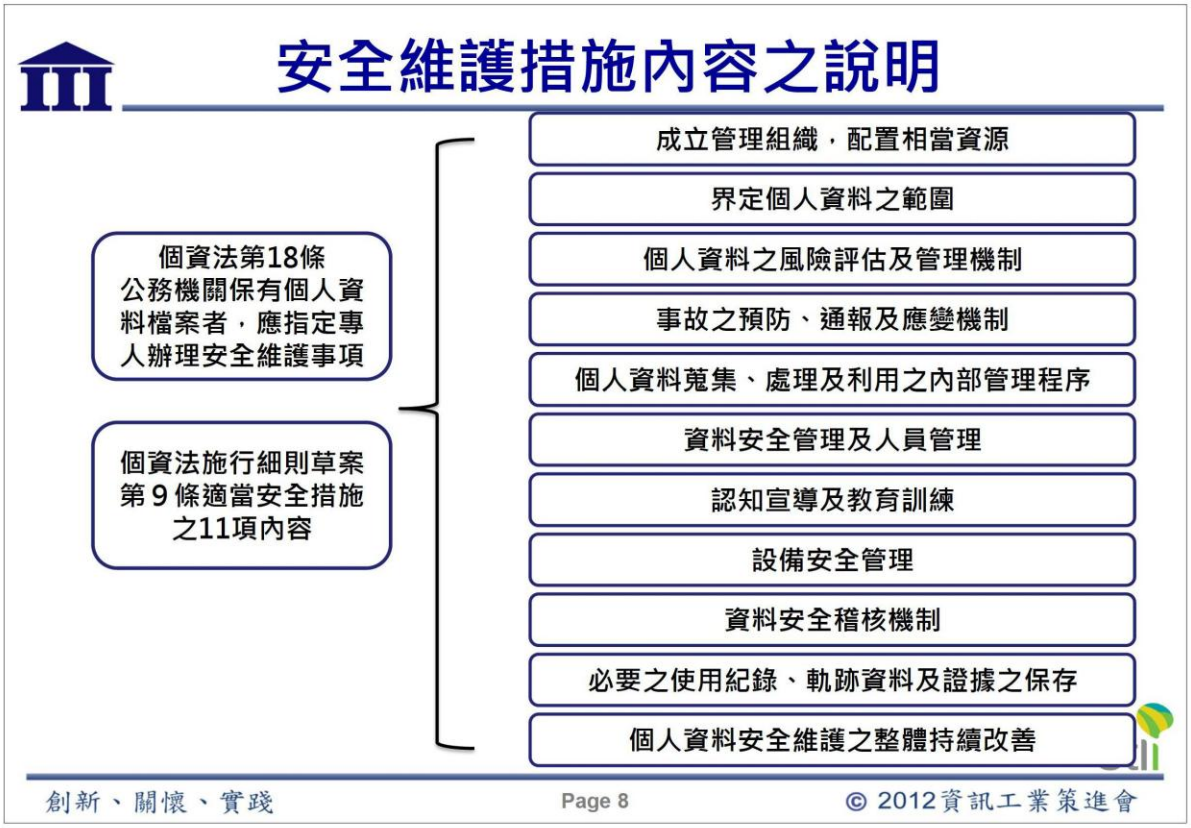


個資管理制度之五大挑戰

流程與習慣改變	需告知當事人與取得書面同意之法定責任。 特種資料的蒐集、處理及利用。 當事人行使查詢、調閱、補正及刪除等等權利。
權責界定釐清	涉及個資之委外(託)關係及民事責任、刑事責任的認定。 區分委託者與受託者的權利義務關係，含單位與內部員工。
資訊公開與當事人權益	公務機關應將所擁有個資之相關事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同。 提供當事人行使權利之機制。
紀錄與存證	舉證責任倒置之過失責任。 鑑別個資遺失資料之時間點，為法令失效前或後遺失。 因應面對團體訴訟的挑戰。
民、刑事及行政處罰	更高的民刑事賠償。 更嚴格的刑事責任。 行政責任。

本報告之智慧財產權歸屬於法務部





本報告之智慧財產權歸屬於法務部

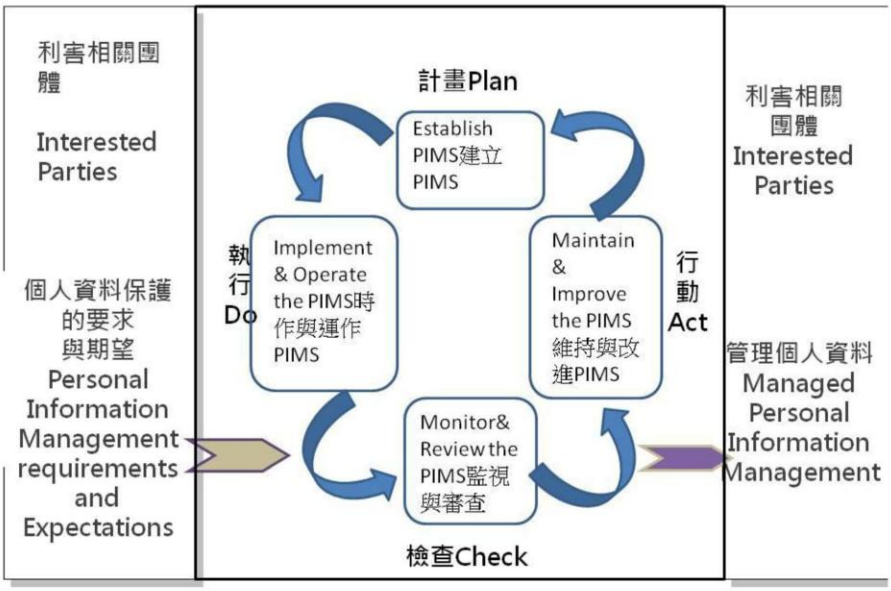
手冊之目的

- 本手冊為政府機關訂定內部個資保護程序之參考，因此手冊係屬建議性質，政府機關可參考本手冊，就組織特性以及業務需求，修正組織所需版本，以符合個人資料保護法與相關施行細則內容、國際隱私保護原則、個資管理標準之要求。

作業手冊介紹

本報告之智慧財產權歸屬於法務部

個人資料保護之PDCA架構



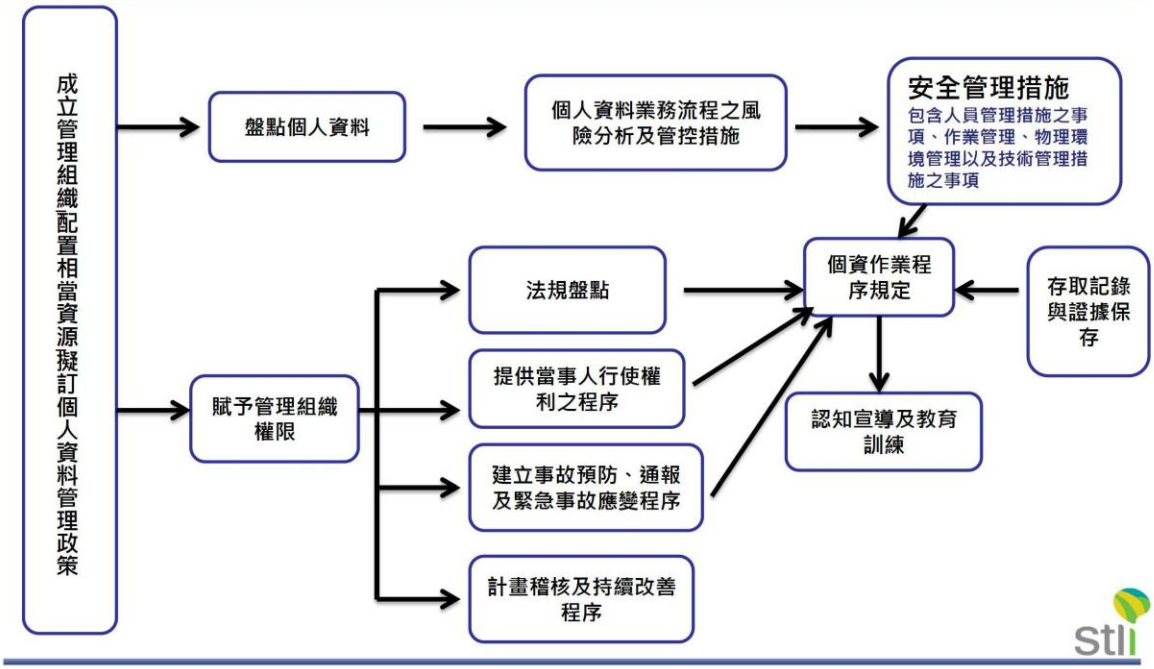
本圖出處：**BS10012**個人資料管理制度

章節架構

- **前言**
  - 目的、章節架構
- **個人資料保護相關規範**
  - 法規範介紹
  - 建議公務機關應立即研辦之事項
- **個資保護政策與架構**
  - 個資保護目標、個資保護流程之方法論
  - 個資保護政策、個資保護管理執行作業
- **個資保護管理建置流程**
  - 分為計劃、執行、檢視及持續改善四步驟
- **整合資訊安全管理制度與個資保護管理制度作業之作法**
- **考核監督作業**
  - 個資管理內部考核監督作業
  - 委外作業監督考核機制

本報告之智慧財產權歸屬於法務部

建立安全維護事項之簡要流程圖



 © 2012資訊工業策進會

個資保護管理建置流程-計劃

步驟一
訂定個人資料保護管理政策

- 機關推動個人資料保護管理作業之理由
- 機關個人資料保護管理上所必須採取之作法

步驟二
成立個人資料保護管理執行小組

- 機關代表人透過各部門主管及業管人員進行任務編組，以成立個人資料保護管理執行小組。執行小組須根據個人資料保護管理政策之內容，建置個人資料保護管理制度，由機關代表人指定召集人領導執行小組並指示機關所屬單位協助執行

步驟三
建置個資管理制度時程表

- 執行小組應於訂定建置作業時程表後，通知相關業務人員並請求協助

步驟四
公告個資保護政策

- 執行小組將機關代表人所訂定之個人資料保護管理政策向機關組織內部全體從業人員公告周知並宣導

步驟五
盤點法規命令

- 機關須先確認本身有無關於蒐集、處理、利用個人資料之相關法令與上級機關所訂定之相關法令規範

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個資保護管理建置流程-計畫

步驟六 盤點個人資料	◆ 盤點個人資料之目標在於找出機關所要保護之個人資料 ◆ 建立盤點清冊
步驟七 進行個人資料風險評估並擬定風險對策	◆ 盤點個人資料後，依個人資料之生命週期尋找出可能產生之風險 ◆ 找出風險後必須分析並評估風險之根本原因、發生可能性以及發生之影響，以設定風險管理等級，並據此擬定風險對策
步驟八 確保必要資源	◆ 執行小組須判斷建置個資保護管理制度所必須之經營資源
步驟九 訂定個人資料保護管理制度內部規範	◆ 將步驟一至步驟八經決定執行之事項歸納為內部規範 ◆ 例如盤點法規程序、盤點個資程序、風險評估及對策之程序、緊急應變程序、當事人權利行使程序、內部稽核程序等
步驟十 實施個資保護管理制度教育訓練	◆ 機關應由教育訓練負責人實施教育訓練。同時，也應留下教育訓練之記錄，以供日後參考並符合個資法規範之要求。

© 2012資訊工業策進會

個資保護管理建置流程-執行

步驟十一 開始運作個人資料保護管理制度	◆ **機關依步驟一至步驟十之內容建立計畫，規定執行程序，準備必要資源，並規定各部門各層級負責人之責任、權限以及訓練後，開始運作個人資料保護管理制度**

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個資保護管理建置流程-檢視

步驟十二
個資管理
報告檢視

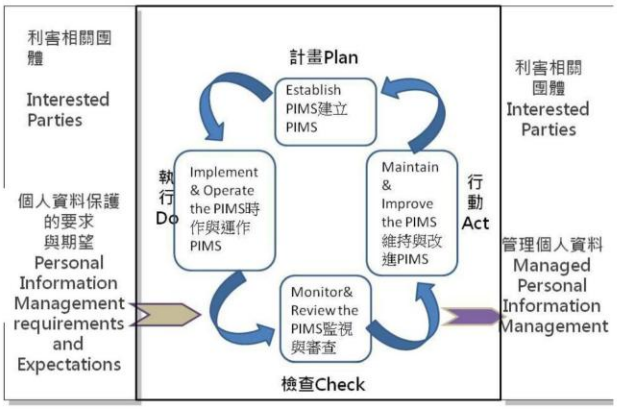
◆檢視個人資料保護管理制度之運作情形，並進行改善

1. 由稽核負責人於個資管理制度開始運作後，檢查個資保護管理制度之運作情形，並且給予適當評價
2. 稽核之目的在於確認管理制度之運作情形，並且確認組織是否落實考核手冊所訂定之事項
3. 機關代表人收到稽核報告後，做出修正之指示。承上，執行小組須依指示進行改善個資保護管理制度
4. 除此之外，執行小組也必須修改內部個人資料保護管理制度文件，以充分反映改善之內容

個資保護管理建置流程-持續改善

步驟十三
實施修正個人資料保護管理制度

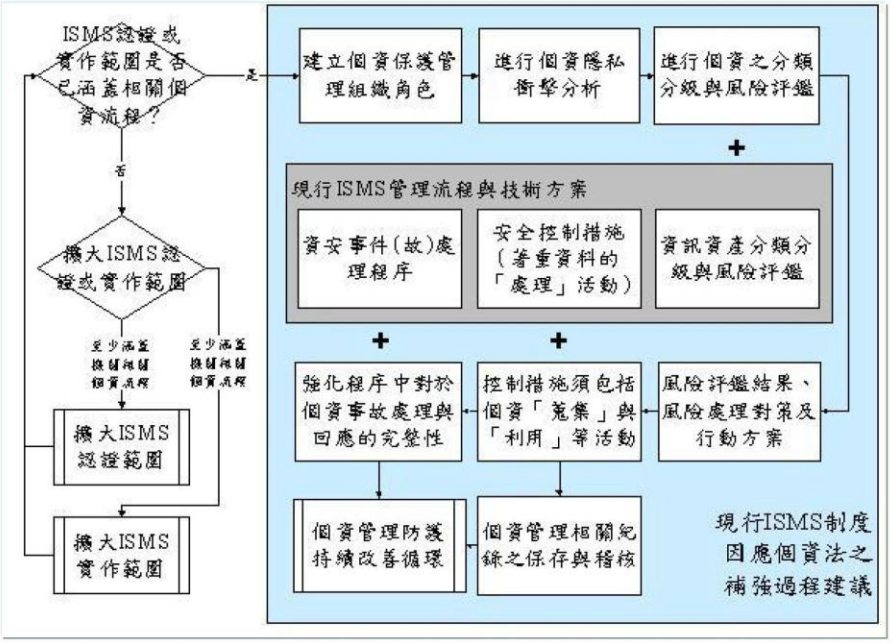
◆ 經過機關代表人修正內部個人資料管理程序以及相關規定，檢討現行個人資料保護管理制度是否適當，並依必要實施改善措施。



本圖出處：**BS10012**個人資料管理制度

本報告之智慧財產權歸屬於法務部

ISMS與個資保護導入之整合



 © 2012資訊工業策進會

個資外洩處理原則

◆公務單位

- 遭民眾抱怨申訴時或媒體揭露報導時，應該怎麼處理？
- 媒體採訪時，應如何應對 ？

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個資事件/故應變

- 結合現有國家資通安全應變機制、公務機關事件分級之通報與處理以及研考會所公告之風險管理及危機處理作業手冊。
- 整合組織單一事件/故通報與處理程序
  - ➢如增列個資外洩類別
- 考量個資法之要求
  - ➢如查明後通知當事人之方式
- 定期演練測試
- 處置態度
  - ➢危機處理

© 2012資訊工業策進會

應變應有之步驟程序

事前	事中	事後
準備	偵測與分析 減緩與復原	事後處置
• 建立組織 • 建立通報與應變機制 • 建立應變程序 • 事件通知程序-當事人、媒體及內部人員 • 定期演練機制 • 結合軌跡資料之留存 • 啟動必要之系統日誌 • 記錄個資存取活動 • 分析可疑事件	• 評估、調查判斷發生來源 • 決定優先處理順序 • 判斷影響範圍 • 鑑識分析及證據留存 • 調查結果確認 • 避免個資事故擴大 • 確保個資事故與處理後，個資之完整性 • 依法通報個資當事人	• 持續觀測 • 提出個資事故報告 • 召開事件檢討會議 • 應變計畫維護 • PDCA • 準備後續可能法律程序

© 2012資訊工業策進會

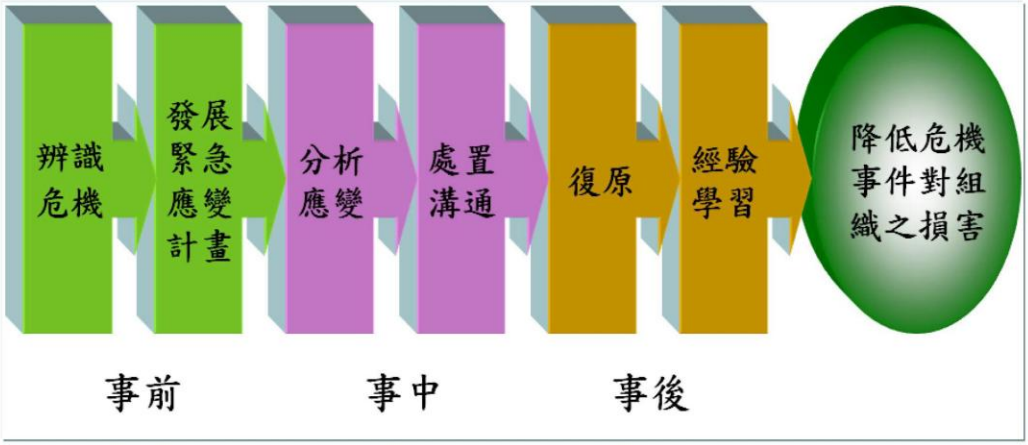
本報告之智慧財產權歸屬於法務部

危機管理

◆是組織從因應危機至危機解除、復原的一個不斷學習、適應的連續過程。

危機處理

危機管理



 © 2012資訊工業策進會

危機處理作業基準

- 「行政院所屬各機關風險管理及危機處理作業基準」--危機處理專章。

危機處理應與風險管理架構相呼應，並預為規劃預防、應變與復原措施。

應針對危機事件訂定緊急應變計畫，並透過測試演練，驗證有效性。

各部會應強化危機處理整體概念及內外部協調整合機制。

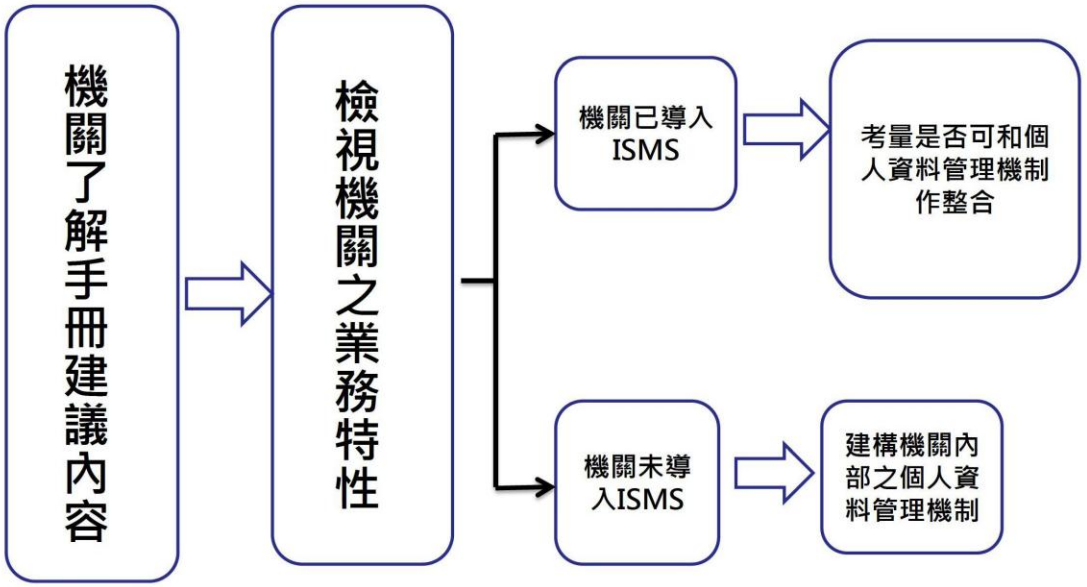
各部會應適時成立危機應變小組或陳報上級成立跨部會小組，爭取第一時間解決。

各部會應透過處理案例持續學習及檢討改進。

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

手冊應用流程



 © 2012資訊工業策進會

結論

- 個資保護管理建置流程
  - 提供機關於導入個資保護系統之參考，因而發展出一套適用於各機關面對個資法實施時，如何建立機關內個資管理機制之參考步驟。
- 個資保護管理建置流程分為計畫、執行、檢視及持續改善等四個階段
  - 計畫：步驟一至步驟十
  - 執行：步驟十一
  - 檢視：步驟十二
  - 持續改善：步驟十三

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

資料來源：資策會科法所

本報告之智慧財產權歸屬於法務部

個人資料盤點與風險評估

資訊工業策進會 科技法律研究所
張曉芸 法律研究員
dorishychang@iii.org.tw
2012年5月15日

© 2012資訊工業策進會

個人資料盤點與風險評估的意義
個人資料盤點與風險評估注意事項
個人資料盤點方法與執行
風險評估方法與執行
總結

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個人資料盤點與風險分析的意義

為什麼要做個資盤點與風險分析?

由機關所處理的資料中盤點出應受保護的個人資料（個資盤點）

從個人資料作業的識別各個情境、評估風險，並訂定風險對策（風險評估）

實施所訂定的風險對策，合法適當地處理個人資料，以達到保護當事人的權益

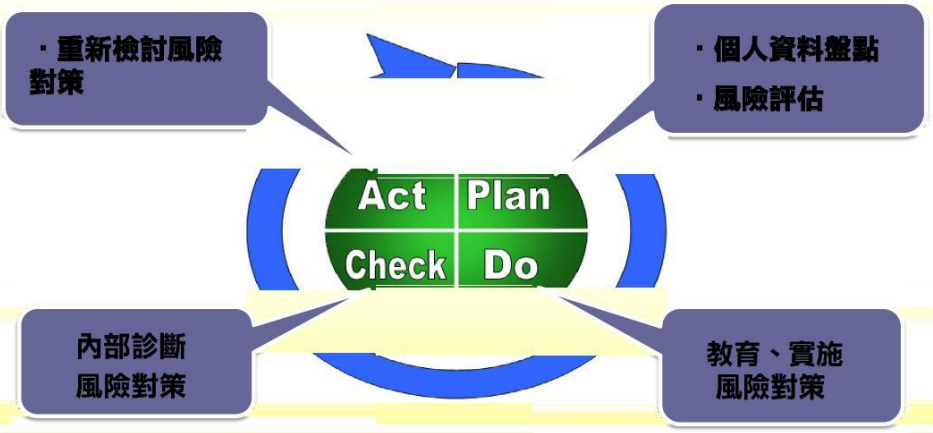
合法適當地使用個人資料，並得到民眾的信賴，以提高機關行政服務品質

 © 2012資訊工業策進會

個人資料盤點與風險分析意義

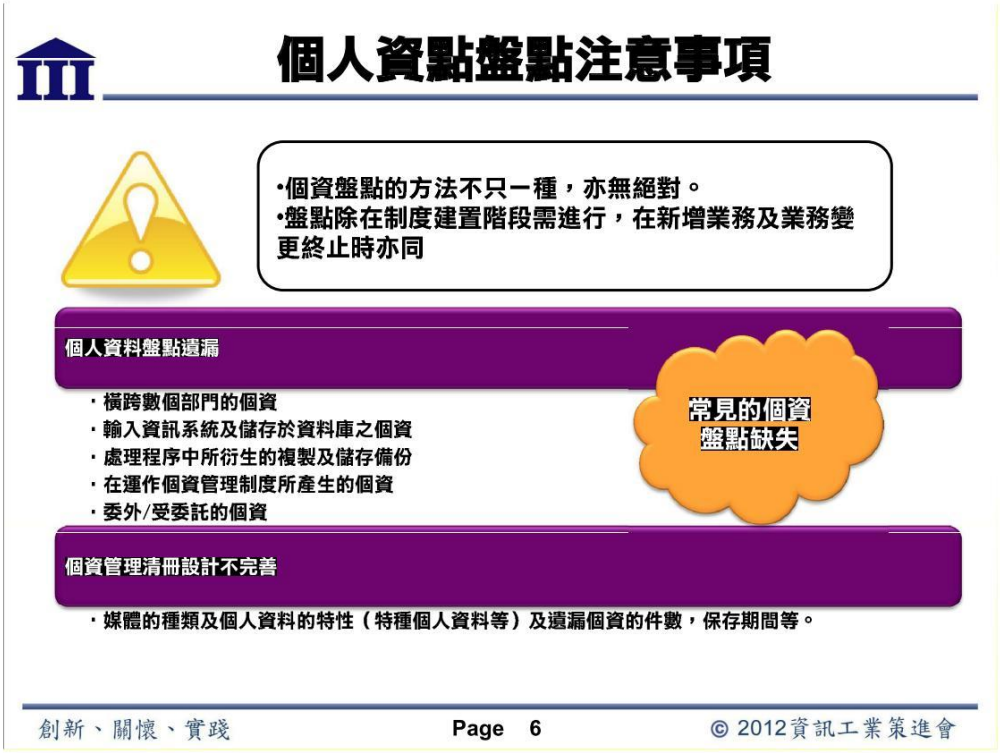
■ 個人資料盤點及風險分析

（個資管理架構與運作的基礎）



 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部



本報告之智慧財產權歸屬於法務部

風險評估注意事項

•風險評估方法亦有多種，應依自身需求選擇。
•個資上的風險評估應配合個資的生命週期逐項討論。
•風險的評估的目的係為風險對策。

對風險的認識不夠充分

- 風險內容不夠具體
- 作業情境遺漏，例如：編輯
- 風險情境遺漏，不要只考慮到洩漏、毀損、滅失。

無風險對策產出或風險對策不足

對剩餘風險的理解及掌握不夠充分

常見的風險缺失

© 2012資訊工業策進會

- 個人資料盤點與風險評估的意義
- 個人資料盤點與風險評估注意事項
- 個人資料盤點方法與執行
- 風險評估方法與執行
- 總結

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個資盤點方法

個資檔案普查 → 作業流程普查 → 個資作業流程圖繪製

個資清冊設計 → 個資清冊製作 → 個資清冊彙整

排除不納入管理的個資檔案 → 確認與個資相關的作業流程 → 找出遺漏的個資檔案

 © 2012資訊工業策進會

個人資料檔案普查1/2

供機關使用的所有個人資料原則上都是盤點的對象

- 提供行政服務等業務上所處理的個人資料
- 公務人員晉用及人事管理所處理的個人資料
- 運作個資管理制度所處理的個人資料

具體實例

提供行政服務等業務上所處理的個人資料	公務人員晉用及人事管理所處理的個人資料	運作個資管理制度所處理的個人資料
	・履歷表 ・健康檢查表 ・人事清冊、人事考核表 ・薪資明細清冊、薪資匯款申請書、薪資明細表等等 ・其他公務人員考、用、退、撫、考銓等人事晉用作業表單	・人員監督：保密契約、保密切結書 ・當事人權利行使：查閱、訂正、停止利用等申請書 ・人員教育訓練：學員名單、隨堂考試等測驗 ・安全管理措施：入出機房紀錄、生物辨識紀錄、資訊系統存取紀錄等

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個人資料檔案普查2/2

例外可不用列入盤點表單盤點清冊管理製個人資料。

即使不納入個資盤點清冊，機關仍應依其他規範進行管理。

- 名片(非檔案化)
- 簽呈、會議紀錄(非以蒐集個資為目的)
- 主管行程表、會議簽到表(個資種類少)
- 報價單(專為業務聯絡用而委由業管人員處理)
- 便當訂購表、下午茶訂購表(重要性極低)

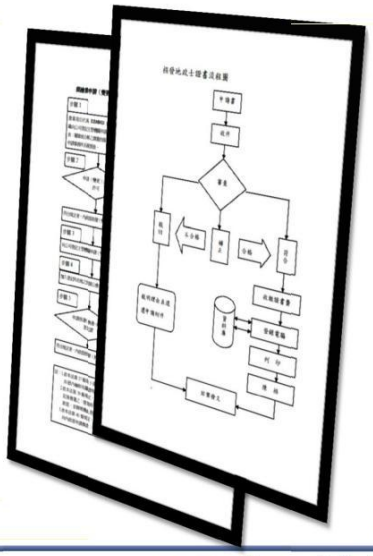
 © 2012資訊工業策進會

作業流程普查

根據機關本身所執掌業務統整所有流程

將個資有關的流程找出

與個資檔案普查出的表單做歸納，分類



 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個資作業流程圖繪製

當事人 | 蒐集 | 處理 | 利用 | 委外

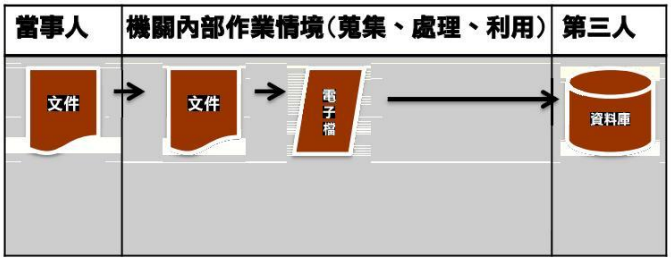
劃分由個資當事人所取得的個人資料（原始資料），與將所蒐集的個人資料輸入資訊系統處理後的作業結果及儲存資料（加工資料），繪出各個種類的個人資料。

因個人資料的記錄媒體（紙本、外接記錄媒體）不同，作業處理上就有所不同，流程圖上劃分為不同種類的個人資料較佳。例如：將紙本掃瞄成PDF檔儲存於資料庫或電腦硬碟中，其記錄媒體就有紙本、資料庫及硬碟電子檔的不同

 © 2012資訊工業策進會

Case Study

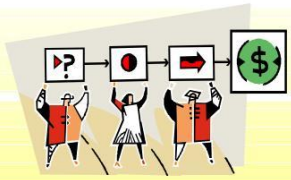
■ 請選擇與業務相關之流程繪製個資作業流程圖



個資陳情作業流程圖參考

檢察司

行政執行署



 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個資清冊

法務部「各單位內部保有及管理個人資料之項目彙整表」

項目 單位名稱	個人資料檔案名稱	法律依據	特定目的	個人資料類別	個人資料之範圍	有否特種資料？何種特種資料？	有無監督管理之非公務機關及其名稱

Case Study

■ 請依法務部公布之「各單位內部保有及管理個人資料之項目彙整表」設計其單位內部之個人資料盤點清冊

個資陳情作業流程盤點清冊參考

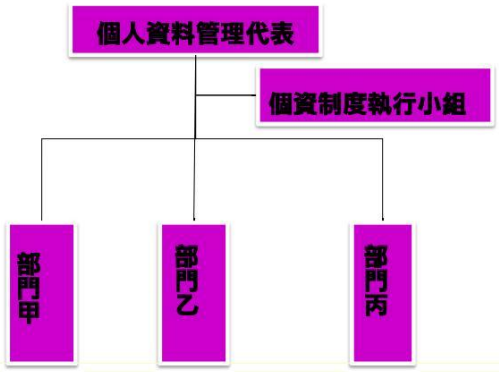
檢察司

行政執行署

本報告之智慧財產權歸屬於法務部

執行個人資料盤點1/4

- 盤點個人資料人員：以業務部門主管及業管人員為中心，與個資管理執行小組合作盤點個資。

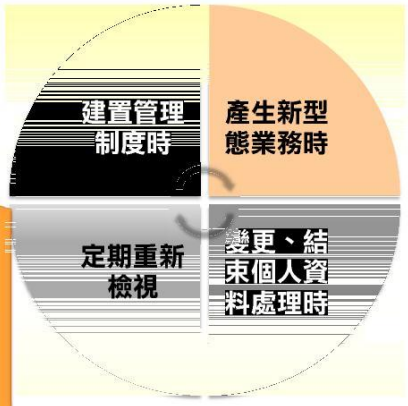


業務劃分	負責盤點個人資料人員
部門的固定業務（於該部門就可結束的業務）	負責該業務的部門主管與業管人員
橫跨複數部門的業務	各個相關部門的主管與業管人員
運作個資管理制度	個資管理制度執行小組

© 2012資訊工業策進會

執行個人資料盤點2/4

盤點個人資料時點：



定期（至少一年一次以上）重新檢視盤點的個人資料有無變化。有發生變化時，根據上述程序處理。定期檢視是為防止處理個人資料有遺漏及變化。

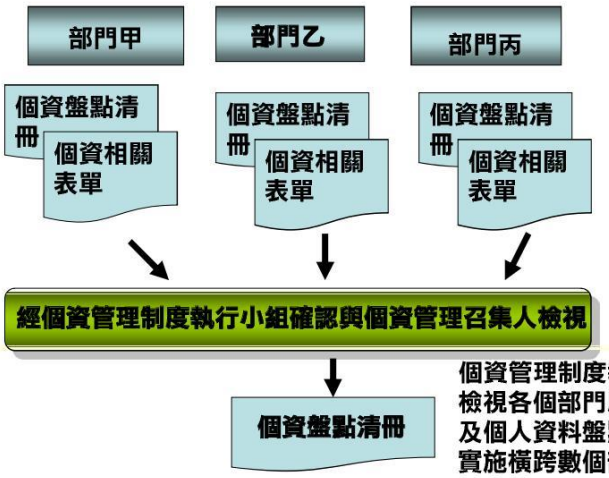
應重新檢視事項
- 變更個人資料作業的負責人、執行人
- 變更紀錄媒體、蒐集態樣
- 變更委託對象及委託業務內容
- 變更保存處所、期間
- 終止處理個人資料等情形

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

執行個人資料盤點3/4

匯整盤點後的個人資料



個資管理制度執行小組應從全機關的角度檢視各個部門所提出個人資料作業申請書及個人資料盤點清冊。特別是一種業務的實施橫跨數個部門時，要確認每個部門的整合性。

 © 2012資訊工業策進會

執行個人資料盤點4/4

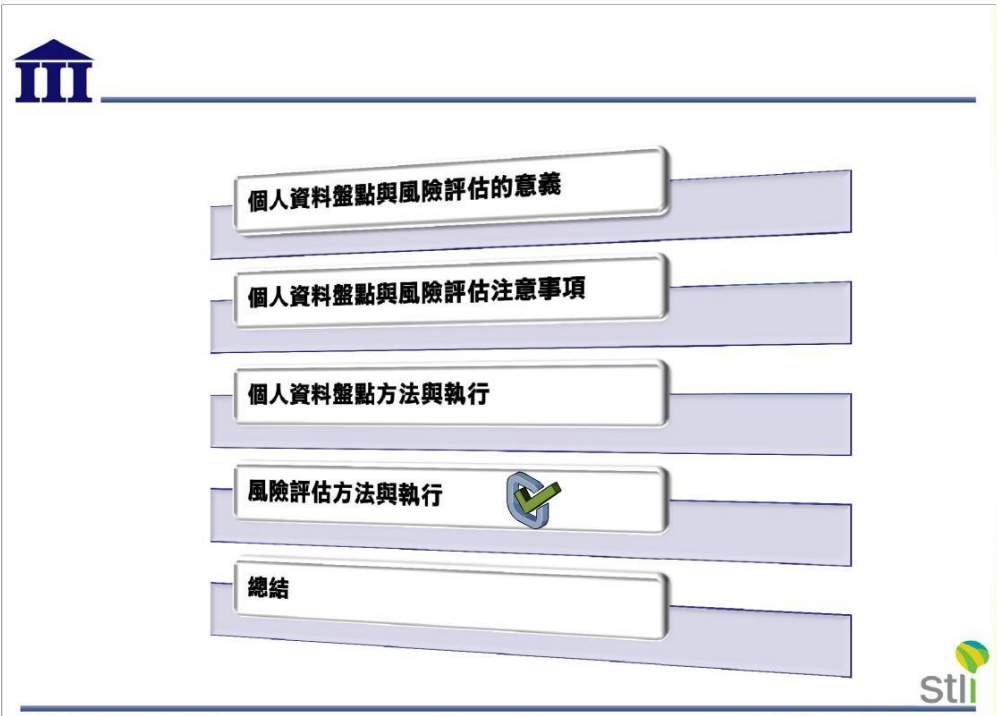
檢視盤點後的個人資料：

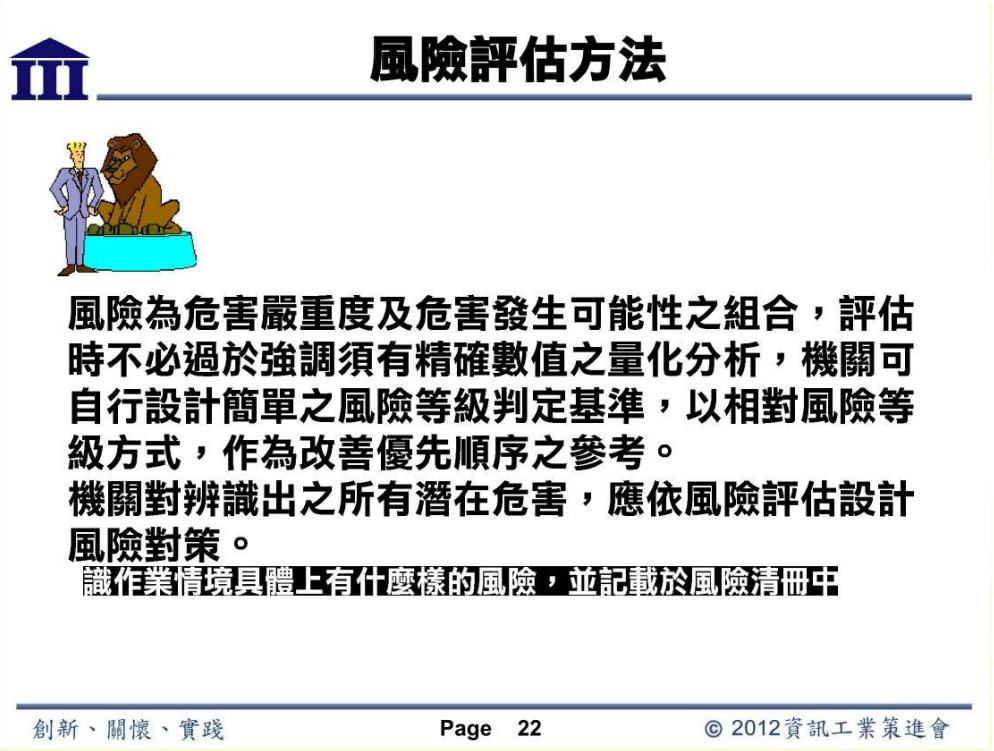
由部門主管或個資管理制度執行小組依下列觀點，檢查處理個人資料的適當性。如果有不完備的事項，由部門主管定期限處理。

- 應以機關最後以何種目的利用個人資料，具體、個別地就利用目的進行檢視。並只在達成利用目的的必要範圍內取得個人資料。不取得非必要的個人資訊。
- 不蒐集特種個人資料。有蒐集、處理、利用之必要時，應先確認有無個資法其他相關法令規範之但書規定。
- 以合法、正當的手段取得個人資料。不得以欺騙、虛偽等不法手段取得。
- 於蒐集、處理、利用、委外時，應符合機關個資管理制度中有關蒐集同意、告知事項、適用但書的規定。
- 個人資料作業的負責人、業管人員要明確及適當。
- 個人資料的保存期間應按法令及利用目的訂定保存期間。

 © 2012資訊工業策進會

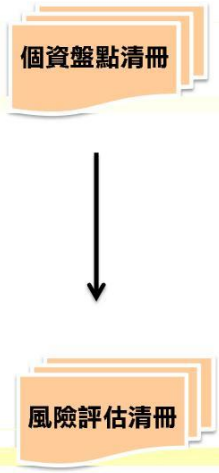
本報告之智慧財產權歸屬於法務部





本報告之智慧財產權歸屬於法務部

執行風險評估1/6



風險評估流程

- 明確個人資料作業情境、作業內容、作業人員
- 認識處理作業情境上的風險
- 訂定風險對策
- 反映到相關內部規範
- 掌握剩餘風險

 © 2012資訊工業策進會

執行風險評估2/6

風險評估時點

管理制度建置時的風險評估：制度建置時應配合個資盤點進行風險分析，針對風險分析擬定對策，設計管理規範。

發生新型態業務時的風險評估：發生新型態業務時、或是業務內容變更產生新種類的個人資料時，要與盤點個人資料連結，共同實施風險評估。

重新檢討風險：除處理的個人資料變更、環境變遷、事件事故的發生外，應定期重新檢討風險

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

執行風險評估3/6

認識處理作業情境上的風險(建議)

洩漏(對外洩漏)	滅失(遺失)	損毀(損壞、資料不正確)
違反相關法令、上級機關訂定的指引及其他規範	造成經濟上的損失、損壞機關聲譽	對當事人的影響

認識作業情境具體上有什麼樣的風險，並記載於風險清冊中

 © 2012資訊工業策進會

執行風險評估4/6

訂定風險對策：將所認識到的風險，根據定性評估的結果，訂定合理的風險對策，並記載於風險評估表。所訂定的對策應考量機關的資安政策、預算、技術等客觀因素後的最佳對策。

- **訂定風險對策**
  - **訂定風險對策時的參考資料**
    - 各目的機關主管機關所擬定的指引．行政規則
  - **風險對策舉例**

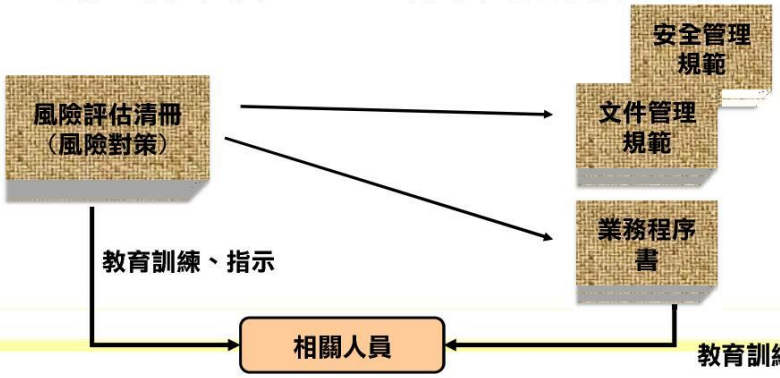
預估風險：人事部門把應徵者資訊存到USB記憶體帶回家，但家中電腦裝了P2P軟體，感染了曝露型病毒，洩漏應徵開缺者資訊。風險對策：①禁止在自己家中作業。②對在家作業採許可制。許可時，工作使用的電腦沒有裝載P2P軟體。③不得已許可在家作業的情況，僅能使用公司所配給的筆記型電腦，將硬碟加密的同時，也定期檢查電腦是否有安裝點對點傳輸軟體（ P2P ）。

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

執行風險評估5/6

■ 反映到相關內部規範：所訂定的風險對策，必須徹底讓相關部門負責人瞭解。除將風險對策反應在相關內部規範或作業程序書，使相關業管人員可以隨時參照外，也必須加以教育訓練與指示。

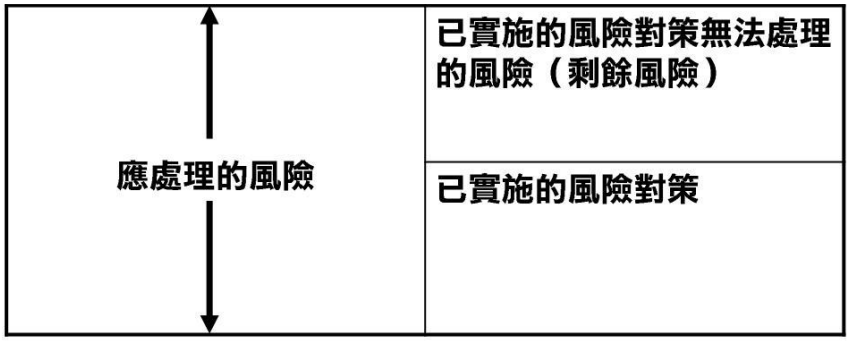


 © 2012資訊工業策進會

執行風險評估6/6

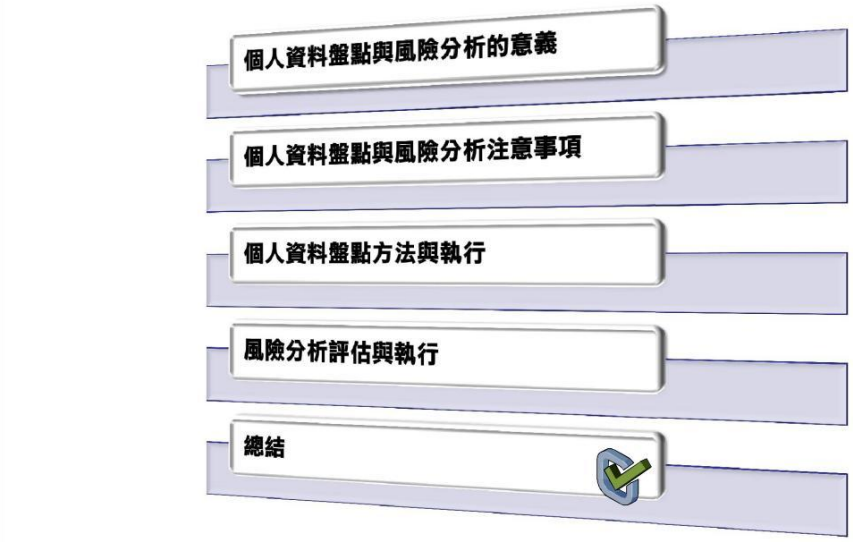
掌握剩餘風險：對剩餘風險的思考

（ ※剩餘風險有必要以稽核或運作的方式來確認是否已凸顯。 ）



 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部



總結

- 掌控業務流程與個人資料處理狀態
- 建議的個人資料盤點與風險分析實施方法
  - 透過適合機關作業情境之清冊格式
  - 由管理制度執行小組以面詢方式確認盤點與風險的內容。
- 預設風險與風險對策的參考資料
  - 各個目的機關主管機關訂定的指引、行政規則
- 盤點個人資料與風險評估是為了保護個人資料的手段，並非目的。最終目的是要採取必要且適當的風險對策保護個人資料。

本報告之智慧財產權歸屬於法務部

資料來源: 資策會科法所

本報告之智慧財產權歸屬於法務部

事件通報管理程序

施叔良
財團法人資訊工業策進會

© 2012資訊工業策進會

個資法施行細則草案預告版第九條

適當安全維護措施

一、成立管理組織，配置相當資源
二、界定個人資料之範圍
三、個人資料之風險評估及管理機制
四、事故之預防、通報及應變機制
五、個人資料蒐集、處理及利用之內部管理程序
六、資料安全管理及人員管理
七、認知宣導及教育訓練
八、設備安全管理
九、資料安全稽核機制
十、必要之使用紀錄、軌跡資料及證據之保存
十一、個人資料安全維護之整體持續改善

第一項必要措施,以所須支出費用與所欲達成之個人資力料保護目的符合適當比例者為限

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

應涵蓋範圍

 © 2012資訊工業策進會

個資法

12條

- 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

施行細則草案預告版

8條

外洩通知

- 受託人僅得於委託人指示之範圍內，蒐集處理，或利用個人資料，受託人認委託人之指示有違反本法或基於本法所發佈之命令規定之情事應立即通知委託人。

 © 2012資訊工業策進會

個資法

30條

軌跡保存

- 損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。

 © 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

罰則

民事責任：§28~40

- 賠償 (500-2億)

刑事責任：§41~46

- 刑責(2年-5年以下,或罰金20萬,意圖營利:100萬)

行政責任：§25、47~50

- 罰鍰

© 2012資訊工業策進會

ISO27001-A13資訊安全事故管理

事件通報處理

- A13.2.1 責任與程序
  - 控制措施
    - 應建立管理責任與程序，以確保對資訊安全事故做迅速，有效及依序的回應
- A13.2.2 從資訊安全事故中學習
  - 控制措施
    - 應有各項適當的機制，對資訊安全事故的型式、數量及形成能加以量化與監視
- A13.2.3 證據的收集
  - 控制措施
    - 在涉及法律行動(民事或刑事)的資訊安全事故後，對人員或組織的跟催措施，應收集、保存及呈現證據，以符合在相關審判時提出證據的規則

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

TPIPAS

4.4.7 事故之緊急應變

為避免事故可能產生之不利益及影響，事業應訂定事故緊急應變措施。

相關措施應至少包括：

(1) 使當事人知悉事故發生之方式，並提供後續查詢與處理管道。

(2) 防止事業所受損害擴大之方法。

(3) 避免類似事件再次發生之方法。

(4) 將事故通報授證機關，並於查明後告知當事人。

© 2012資訊工業策進會

BS10012

4.13.6管理安全事件

a. 評估和管理涉及個資的安全事件，包括減緩損害之程序

b. 記錄每個安全事件，包括事件如何發生的評估，採取的矯正行動，以及可以從事件學習到的教訓

c. 決定是否將安全事件轉由相關管制機關處理(例如:資訊委員會或主管機關)，或通知當事人

d. 紀錄任何已核發的轉介及通知

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

BS10012

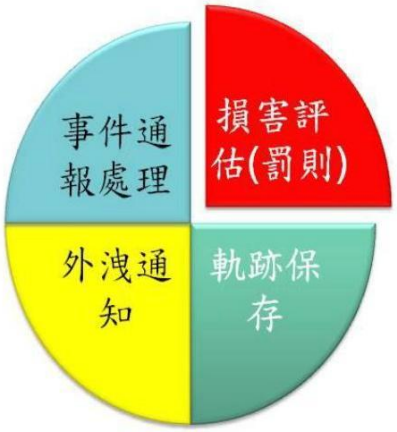
4.12.2申訴、抱怨與向上呈報

- PIMS應包含申訴、抱怨程序，確保組織正確處理有關個人資訊處理的訴怨，應包括當事人對於他們的訴怨被處理的方式考量及向上呈報的程序

© 2012資訊工業策進會

Workshop

- 請思考設計個資事件通報單應有欄位



© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

個資法

監督(主管機關)

22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。

個資法

監督(主管機關)

22條(續)

- 中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。

本報告之智慧財產權歸屬於法務部

個資法

監督(主管機關)

23條

- 對於前條第二項扣留物或複製物，應加封緘或其他標識，並為適當之處置；其不便搬運或保管者，得命人看守或交由所有人或其他適當之人保管。
- 扣留物或複製物已無留存之必要，或決定不予處罰或未為沒入之裁處者，應發還之。但應沒入或為調查他案應留存者，不在此限。

© 2012資訊工業策進會

- 個資事件法律處理

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

資料來源: 資策會科法所

本報告之智慧財產權歸屬於法務部

個人資料保護委外管理程序

施叔良
財團法人資訊工業策進會

© 2012資訊工業策進會

個資法施行細則草案預告版第八條

委託他人蒐集、處理或利用個人資料之全部或一部時，委託人應對受託人為適當之監督。
前項監督至少應包含下列事項：

一、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。
二、受託人就第九條第二項應採取之必要措施。
三、有複委託者，其約定之受託人。
四、受託人或其受僱人違反個人資料保護法規或委託契約條款時，應向委託人通知之事項及採行之補救措施。
五、委託人對受託人保留指示之事項。
六、委託關係終止或解除時，個人資料載體之返還，及儲存於受人持有個人資料之刪除。

第一項之監督，委託人應定期確認受託人執行之狀況，並將確認結果記錄之。

受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

BS10012規範

4.16

目標:確保代表組織的另一個組織處理個資時受到管理，以符合資料保護法律及優良實務。

說明:如資訊是由代表組織的其他組織處理時，PIMS應建立程序，確保：

a. 其它組織能夠提供充份的技術，實體及組織安全措施，以達到組織個資安全要求

b. 在與另一個組織約定之前，進行適當安全性的評估，作為盡責調查的行動之一，且如果因為將處理的個人資訊之本質或處理的特殊狀況所需要，組織在締結合約之前應對其它組織的安全措施安排進行稽核

© 2012資訊工業策進會

BS10012規範

4.16(續)

c. 一旦挑選了其它組織，組織應備妥書面協議來提供具體指明的服務，並要求其它組織提供處理個資的安全措施

d. 合約應規定，在擁有個資存取權的期間，其合約有義務要先獲得組織對此等意圖的許可

e. 如其它組織意圖使用轉包商來處理個資，其合約有義務要先獲得組織對此等意圖的許可

f. 合約應要求轉包商至少要遵循與其它組織相同的安全和其它規定，以及

g. 與其它組織締結的合約(向下延伸到任何轉包商)應具體指明在合約終止時，相關個人資訊應銷毀，交還組織或交給組織指定的另一個組織

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

委外應遵循之依據

- 個資法施行細則草案預告版第八條
- 個資施行細則第九條草案預告版"適當安全維護措施“
- 組織安全規範

© 2012資訊工業策進會

Workshop

- 請思考依據TPIPAS及BS10012的要求，會建議組織至少應產生哪些文件
- 請訂定委外管理流程(流程圖)
- 請訂定合約書應包括事項

© 2012資訊工業策進會

本報告之智慧財產權歸屬於法務部

產出

- 委外管理程序
- 受託廠商自評表
- 個人及公司保密切結書
- 合約書(或獨立資訊安全同意書)
- 資訊委外安全規範
- 監控記錄單

創新、關懷、實踐 © 2012資訊工業策進會

創新、關懷、實踐 © 2012資訊工業策進會

資料來源: 資策會科法所

本報告之智慧財產權歸屬於法務部

8.試行機關導入演練課程簽到表

（1）內政部地政司地政資訊作業科

（2）內政部警政署刑事警察局預防科 165 反詐騙諮詢專線

（3）法務部行政執行署與法務部檢察司

因簽到表內含有參與人員之個人資料，故在此予以移除，詳細簽到資料已附於呈繳法務部之「統計個資保護執行與成果報告」)。

9.試行機關導入演練課程照片

（1） 內政部警政署 165 專線

資料來源：資策會科法所拍攝

圖 5：內政部警政署學員出席狀況踴躍，排隊簽到及領取課程講義

本報告之智慧財產權歸屬於法務部

資料來源：資策會科法所拍攝

圖 6：內政部警政署學員出席狀況踴躍

資料來源：資策會科法所拍攝

圖 7：資策會顧振豪組長為學員說明本次教育訓練活動的舉行目的

本報告之智慧財產權歸屬於法務部

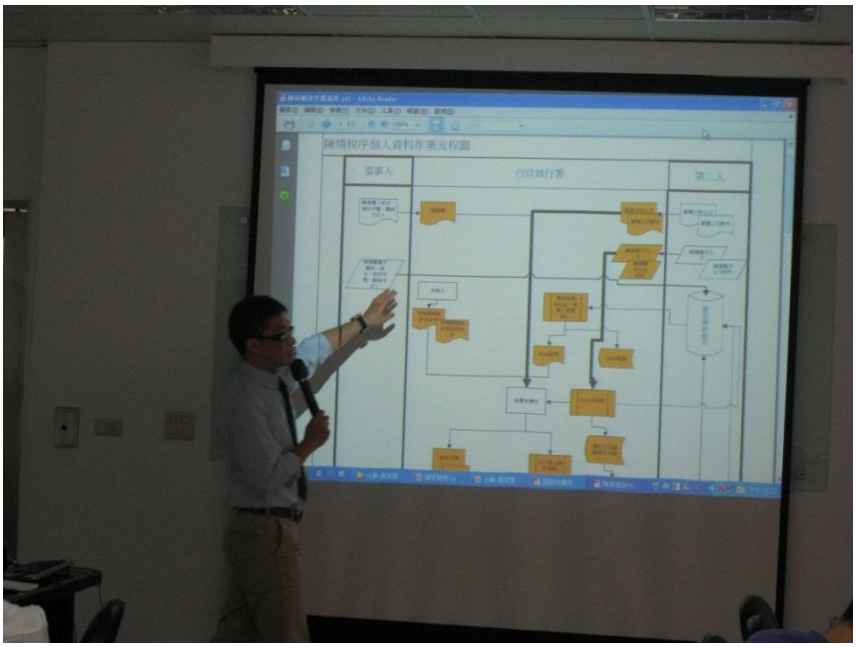
資料來源：資策會科法所拍攝

圖 8：資策會廖淑君研究員講授「個人資料保護法介紹」

資料來源：資策會科法所拍攝

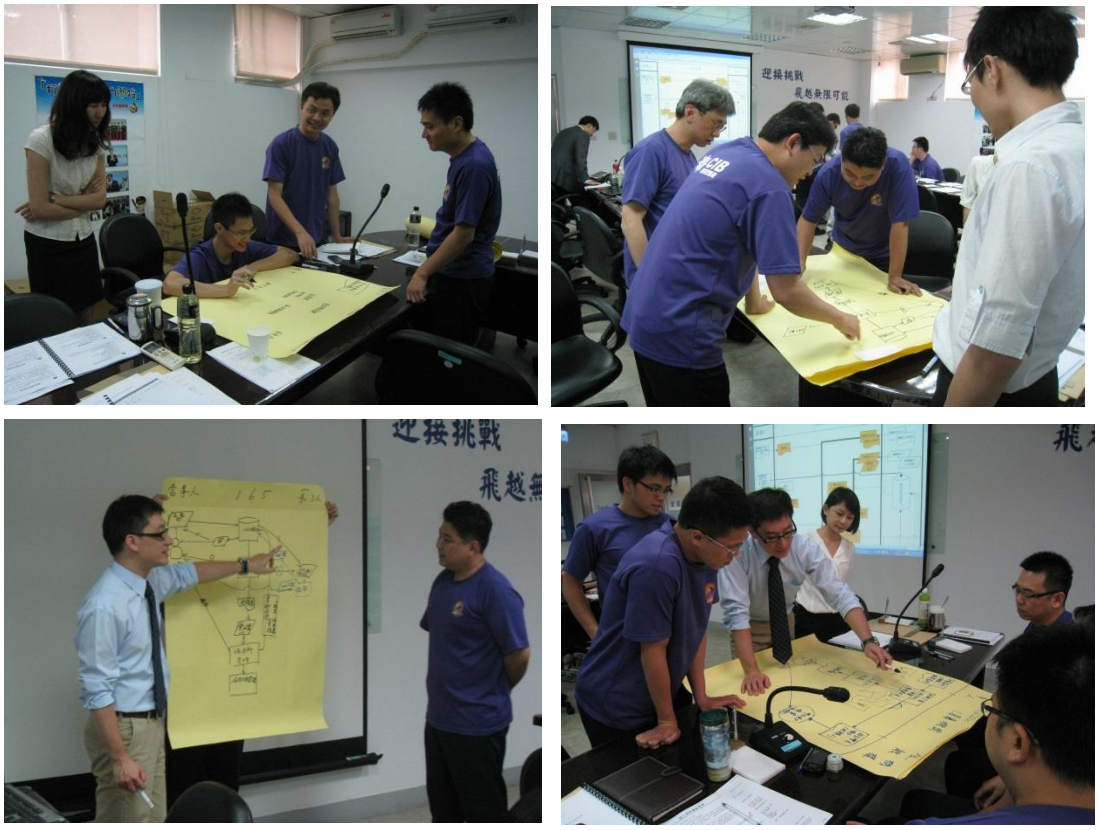
圖 9：資策會陳秭璇律師負責講授「考核作業手冊」

本報告之智慧財產權歸屬於法務部



資料來源：資策會科法所拍攝

圖 10：楊光華研究員負責講授「個資盤點、作業流檢視與風險評鑑」，教學員辨識單位中的個資檔案



資料來源：資策會科法所拍攝

圖 11：透過實例演練，讓學員自行思考並繪製個資流程圖，提升學學習成效

本報告之智慧財產權歸屬於法務部

資料來源：資策會科法所拍攝

圖 12：資策會施叔良顧問講授「委外與事件通報」，讓學員瞭解為何要建立事件通報機制

（2）內政部地政司

資料來源：資策會科法所拍攝

圖 13：資策會顧振豪組長講授「個人資料保護法介紹」及「考核作業手冊」

本報告之智慧財產權歸屬於法務部

資料來源：資策會科法所拍攝

圖 14：內政部地政司學員參與的狀況非常踴躍

資料來源：資策會科法所拍攝

圖 15：資策會張曉芸研究員負責講授「個資盤點與風險評估」

本報告之智慧財產權歸屬於法務部

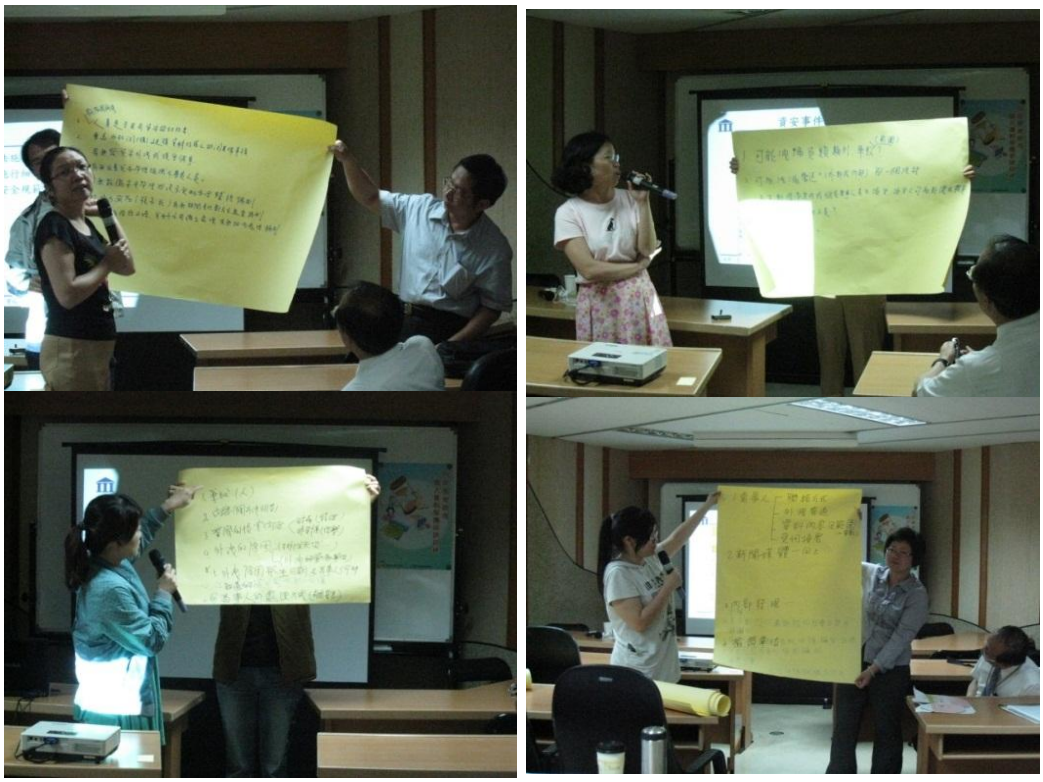
資料來源：資策會科法所拍攝

圖 16：內政部地政司學員討論熱烈

資料來源：資策會科法所拍攝

圖 17：資策會施叔良顧問負責講授「個人資料保護委外管理程序」

本報告之智慧財產權歸屬於法務部



資料來源：資策會科法所拍攝

圖 18：各組學員上台發表委外管理之實作結果

（3）法務部行政執行署與法務部檢察司

資料來源：資策會科法所拍攝

圖 19：資策會顧振豪組長負責講授「個人資料保護法介紹」

本報告之智慧財產權歸屬於法務部

資料來源：資策會科法所拍攝

圖 20：資策會陳秭璇律師負責講授「考核作業手冊」

資料來源：資策會科法所拍攝

圖 21：資策會張曉芸研究員負責講授「個人資料盤點與風險評估」

本報告之智慧財產權歸屬於法務部

資料來源：資策會科法所拍攝

圖 22：各組學員分享實例演練

資料來源：資策會科法所拍攝

圖 23：資策會施叔良顧問負責講授「委外與事件通報」

本報告之智慧財產權歸屬於法務部

資料來源：資策會科法所拍攝

圖 24：各組學員發表委外管理之實作結果

10.試行機關導入演練課程意見回饋表統計

（1）內政部警政署 165 專線

內政部警政署 165 反詐騙諮詢專線個人資料保護培訓教育訓練課程總共有 13 人報名，總共發放 13 份意見回饋表，回收 13 份，回收率為 100%。

有關對於當日課程的整體看法，很滿意佔 43.42%，滿意佔 47.37%，普通佔 9.21%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 90.79%。

有關對於財團法人資訊工業策進會廖淑君研究員表現的看法，很滿意佔 52.31%，滿意佔 47.69%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例

本報告之智慧財產權歸屬於法務部

證，講師的授課態度、敬業精神以及整體表現的滿意度為 100%。

有關對於財團法人資訊工業策進會陳秭璇律師表現的看法，很滿意佔 40%，滿意佔 56.92%，普通佔 3.08%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 96.92%。

有關對於財團法人資訊工業策進會楊光華研究員表現的看法，很滿意佔 61.54%，滿意佔 38.46%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 100%。

有關對於財團法人資訊工業策進會施叔良資深業務經理表現的看法，很滿意佔 55.38%，滿意佔 41.54%，普通佔 3.08%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 96.92%。

有關對於行政服務的看法，很滿意佔 61.54%，滿意佔 34.62%，普通佔 3.85%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 96.15%。

表 20：內政部警政署 165 專線意見回饋表統計結果(課程、講師、行政)

個人資料保護培訓教育訓練活動意見回饋表統計結果	很滿意	滿意	普通	不滿意	很不滿意
對今日課程的整體看法	43.42%	47.37%	9.21%	0.00%	0.00%
對講師表現的看法(廖淑君研究員)	52.31%	47.69%	0.00%	0.00%	0.00%
對講師表現的看法(陳秭璇律師)	40.00%	56.92%	3.08%	0.00%	0.00%
對講師表現的看法(楊光華研究員)	61.54%	38.46%	0.00%	0.00%	0.00%

本報告之智慧財產權歸屬於法務部

對講師表現的看法 (施叔良資深業務經理)	55.38%	41.54%	3.08%	0.00%	0.00%
對行政服務	61.54%	34.62%	3.85%	0.00%	0.00%

資料來源：本計畫活動產出

表 21：內政部警政署 165 專線培訓教育訓練活動意見回饋表統計結果(教學方式)

內政部警政署 165 反詐騙諮詢專線個人資料保護培訓教育訓練活動意見回饋表統計結果	過多	剛好	過少	不適用
此教育訓練課程使用之教學方式	3.64%	87.27%	7.27%	1.82%

資料來源：本計畫活動產出

（2）內政部地政司

內政部地政司個人資料保護培訓訓練課程總共有 25 人報名，總共發放 21 份意見回饋表，回收 17 份，回收率為 80.95%。

有關對於當日課程的整體看法，很滿意佔 22.55%，滿意佔 70.59%，普通佔 6.86%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 93.14%。

有關對於財團法人資訊工業策進會顧振豪組長表現的看法，很滿意佔 50.59%，滿意佔 42.35%，普通佔 7.06%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 92.94%。

有關對於財團法人資訊工業策進會顧振豪組長表現的看法，很滿意佔 48.24%，滿意佔 44.71%，普通佔 7.06%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 92.94%。

本報告之智慧財產權歸屬於法務部

有關對於財團法人資訊工業策進會張曉芸研究員表現的看法，很滿意佔 35.29%，滿意佔 60%，普通佔 4.71%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 95.29%。

有關對於財團法人資訊工業策進會施叔良資深業務經理表現的看法，很滿意佔 40%，滿意佔 56.25%，普通佔 3.75%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 96.25%。

有關對於行政服務的看法，很滿意佔 43.75%，滿意佔 53.13%，普通佔 3.13%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 96.87%。

表 22：內政部地政司培訓教育訓練活動意見回饋表統計結果(課程、講師、行政)

內政部地政司培訓教育訓練活動意見回饋表統計結果	很滿意	滿意	普通	不滿意	很不滿意
對今日課程的整體看法	22.55%	70.59%	6.86%	0.00%	0.00%
對講師表現的看法(顧振豪組長)	50.59%	42.35%	7.06%	0.00%	0.00%
對講師表現的看法(顧振豪組長)	48.24%	44.71%	7.06%	0.00%	0.00%
對講師表現的看法(張曉芸研究員)	35.29%	60.00%	4.71%	0.00%	0.00%
對講師表現的看法(施叔良資深業務經理)	40.00%	56.25%	3.75%	0.00%	0.00%
對行政服務	43.75%	53.13%	3.13%	0.00%	0.00%

資料來源：本計畫活動產出

本報告之智慧財產權歸屬於法務部

表 23：內政部地政司培訓教育訓練活動意見回饋表統計結果(教學方式)

內政部地政司個人資料保護培訓教育訓練活動意見回饋表統計結果	過多	剛好	過少	不適用
此教育訓練課程使用之教學方式	6.25%	80.00%	13.75%	0.00%

資料來源：本計畫活動產出

（3）法務部行政執行署與法務部檢察司

法務部行政執行署與法務部檢察司培訓教育訓練課程總共有 27 人報名，總共發放 27 份意見回饋表，回收 19 份，回收率為 70.37%。

有關對於當日課程的整體看法，很滿意佔 15.79%，滿意佔 72.81%，普通佔 11.40%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 88.60%。

有關對於財團法人資訊工業策進會顧振豪組長表現的看法，很滿意佔 21.05%，滿意佔 73.68%，普通佔 5.26%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 94.74%。

有關對於財團法人資訊工業策進會陳秭璇律師表現的看法，很滿意佔 21.05%，滿意佔 60%，普通佔 18.95%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 81.05%。

有關對於財團法人資訊工業策進會張曉芸研究員表現的看法，很滿意佔 21.05%，滿意佔 74.74%，普通佔 4.21%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方

本報告之智慧財產權歸屬於法務部

面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 95.79%。

有關對於財團法人資訊工業策進會施叔良資深業務經理表現的看法，很滿意佔 23.33%，滿意佔 75.56%，普通佔 1.11%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 98.89%。

有關對於行政服務的看法，很滿意佔 16.67%，滿意佔 80.56%，普通佔 2.78%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 97.22%。

表 24：法務部行政執行署與法務部檢察司培訓教育訓練活動意見回饋表統計結果(課程、講師、行政)

法務部行政執行署與法務部檢察司培訓教育訓練活動意見回饋表統計結果	很滿意	滿意	普通	不滿意	很不滿意
對今日課程的整體看法	15.79%	72.81%	11.40%	0.00%	0.00%
對講師表現的看法(廖淑君研究員)	21.05%	73.68%	5.26%	0.00%	0.00%
對講師表現的看法(陳秭璇律師)	21.05%	60.00%	18.95%	0.00%	0.00%
對講師表現的看法(楊光華研究員)	21.05%	74.74%	4.21%	0.00%	0.00%
對講師表現的看法(施叔良資深業務經理)	23.33%	75.56%	1.11%	0.00%	0.00%
對行政服務	16.67%	80.56%	2.78%	0.00%	0.00%

資料來源：本計畫活動產出

本報告之智慧財產權歸屬於法務部

表 25：法務部行政執行署與法務部檢察司培訓教育訓練活動意見回饋表統計結果(教學方式)

法務部行政執行署與法務部檢察司培訓教育訓練活動意見回饋表統計結果	過多	剛好	過少	不適用
此教育訓練課程使用之教學方式	0.00%	96.67%	3.33%	0.00%

資料來源：本計畫活動產出

11.試行機關導入演練課程意見彙整

（1）建議針對特定產業，如仲介業，目的事業主管機關業者之稽核及管理等事項提供相關課程

（2）建議提供講義電子檔供學員下載。

（3）建議將課程應增為兩天，才有足夠的時間研討及分享

（4）建議應多提供案例討論。

本報告之智慧財產權歸屬於法務部

肆、公務機關個人資料保護執行程序暨考核作業研究

一、個資執行暨考核作業程序及系統分析報告

（一）前言

財團法人資訊工業策進會(以下簡稱資策會)依據法務部之「99年度公務機關個人資料保護方案委辦計畫」(以下簡稱本計畫)，負責執行「個人資料保護執行程序暨考核作業手冊」相關工作。本報告為本計畫需求項目3、編定各公務機關「個人資料保護執行(管理)暨考核作業手冊程序及系統建置分析報告」之交付文件。

（二）目的

本報告主要目的係依據法務部個人資料保護法業務推動執行之需要，針對公務機關個資自評管理系統作業及個資教育訓練兩項業務推動，分別協助設計程序書及系統功能書，以作為相關工作之執行準則及後續法務部相關系統委外開發工作。

（三）適用對象

適用於本部及各公務機關人員參考。

（四）名詞定義

1.個資自評：各公務機關依據個資法的要求，依特定基準表，自我評量符合度。

2.個資教育訓練：公務機關依據100年10月間預告之個資法施行細則修正草案第十二條之安全維護措施要求，對組織同仁安排之教育訓練課程。

（五）程序書內容

本報告之智慧財產權歸屬於法務部

1.公務機關個資自評管理系統作業程序

（1）目的

為建立本部及各公務機關人員之公務機關個資自評管理業務，特訂定本作業程序，規範從單位申請系統使用帳號至機關個資現況成熟度登錄之實施管理活動，以便各公務機關本部進行公務機關法令符合度的有效監督要求。

（2）適用範圍

各機關之機關成熟度現況資訊皆為本系統管理的範圍。

（3）權責

A. 系統管理者

a.由本部資訊人員擔任

b.負責系統角色權限設定

c.負責人員權限設定

d.負責公務機關代碼維護

B. 業務管理者

a.負責自評作業功能管理

b.負責各類管理報表管理

c.負責自評領域維護

d.負責評估細項維護功能

本報告之智慧財產權歸屬於法務部

C. 機關管理者

負責維護機關個資保護現況

（4）名詞定義

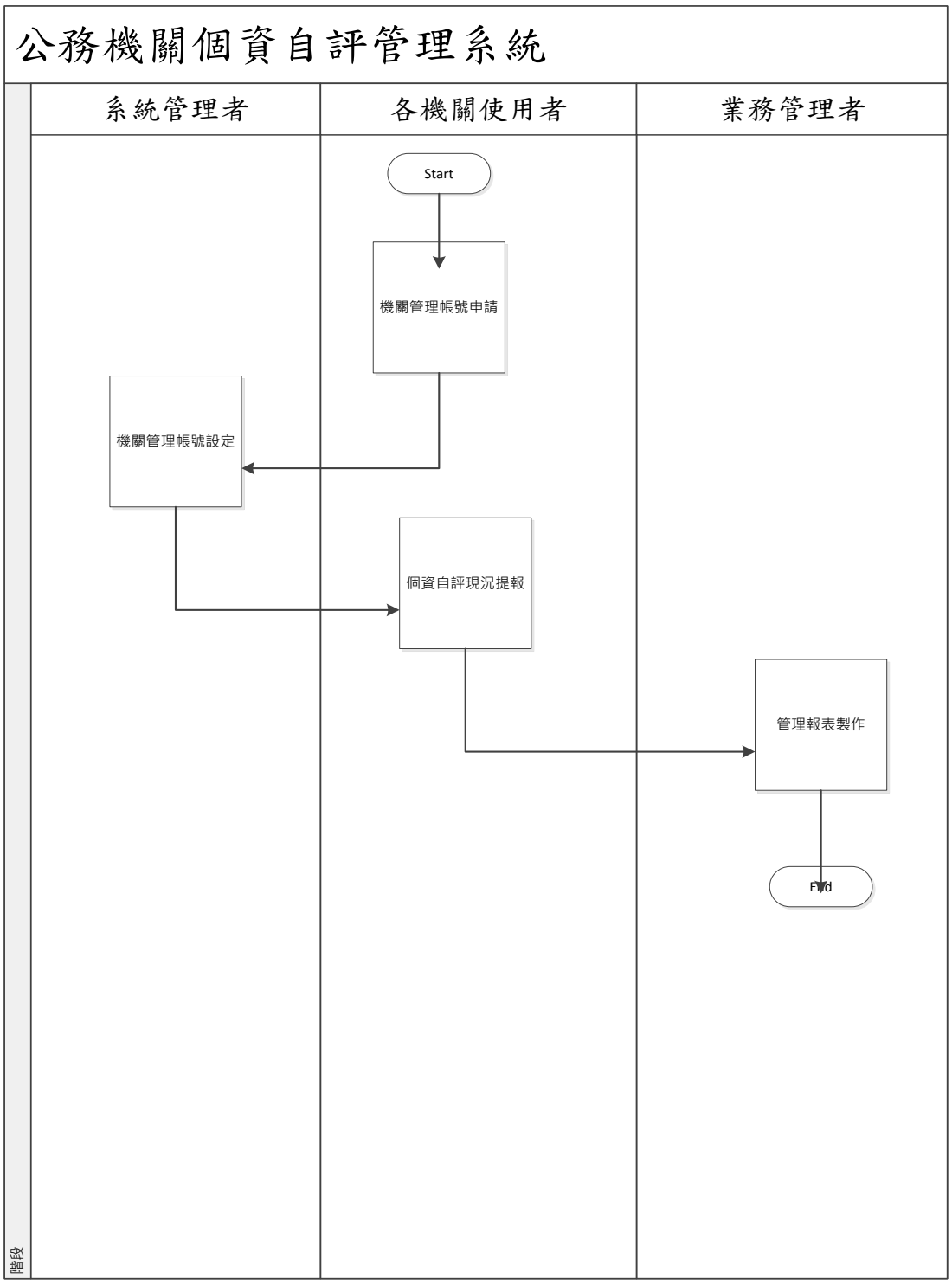
公務機關個資自評管理系統：由法務部開發管理維護，提供各機關維護組織個人資料保護成熟度現況。

（5）相關文件

無

本報告之智慧財產權歸屬於法務部

（6）流程圖



資料來源:本計畫整理

圖 25：公務機關個資自評管理系統流程圖

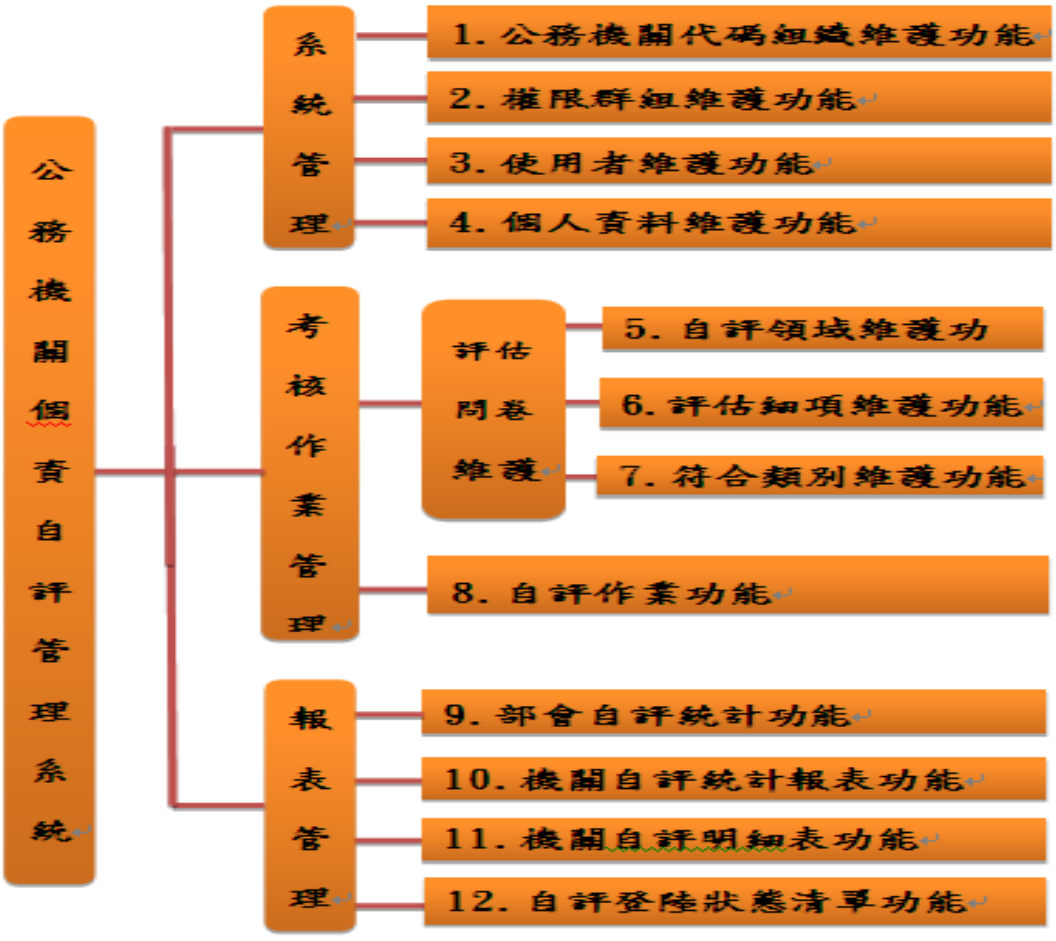
本報告之智慧財產權歸屬於法務部

2.公務機關個資自評管理系統功能

（1）目的

為建立法務部（以下簡稱本部）之公務機關個資自評管理業務，特訂定本作業程序，規範從單位申請系統使用帳號至機關個資現況成熟度登錄之實施管理活動，以便各公務機關本部，進行公務機關法令符合度的有效監督要求。

（2）功能架構圖



資料來源：本計畫整理

圖 26：公務機關個資自評管理系統架構圖

本報告之智慧財產權歸屬於法務部

（3）功能說明

系統登入必須先判斷是否為系統預設帳號，若為預設帳號則強制至「D.個人資料維護功能」進行密碼變更。

使用者登入系統後，至「G.權限群組維護功能」相關資料庫檢視可使用之功能才 Enable。

提供使用者忘記密碼，系統自動重新預設密碼，透過 e-mail 傳送至當事人之功能

A. 公務機關代碼組織維護功能

a.目的：依行政院人事行政總處異動進度維護正確資訊。
(註：若人事行政總處代碼無法提供”業務系統”之機關所屬層級，則須另增加機關層級維護功能)

b.功能說明：

I.系統管理者之角色方可以使用本功能。

II.提供查詢”、”變更”、”新增”及”註記刪除”功能。

B. 權限群組維護功能

a.目的：提供本系統之角色權限設定功能

b.功能說明：

I.系統管理者之角色方可以使用本功能。

II.預設功能權限對照表：

表 26：角色權限對照表(公務機關個資自評管理系統)

	1	2.1	2.2	2.3	2.4	3	4	5	6	7	8	9
業務管理者	X	X	X	X	X	X	X	X				X
系統管理者									X	X	X	X

本報告之智慧財產權歸屬於法務部

機關使用者	X		X	X	X							X

資料來源：本計畫整理

C. 使用者維護功能

a.目的：提供維護人員帳號及密碼維護功能。

b.功能說明：

I.系統管理者之角色方可以使用本功能

II.提供新增帳號密碼預設機制

III.提供人員帳號、密碼及所屬角色之維護功能，密碼資料庫內必須遮蔽，螢幕以代號顯示。

D. 個人資料維護功能

a.目的：提供所有使用者可以自行變更密碼。

b.功能說明：

I.所有使用者均可以使用本功能

II.密碼長度至少八碼

E. 自評領域維護功能

a.目的：提供系統管理者維護各領域資訊及其在所有領域所佔之分數權重。

b.功能說明：

I.業務管理者之角色方可以使用本功能。

II.提供”查詢”、”變更”、”新增”及”刪除”功能。

c.邏輯：

I.所有領域之分數權重總和不得超過 100%。

本報告之智慧財產權歸屬於法務部

II.“評估細項”之資料檔存有對應領域者不得刪除。

F. 評估細項維護功能

a.目的：提供維護各評估細項資訊及權重。

b.功能說明：

I.業務管理者之角色方可以使用本功能。

II.提供系統管理者維護各評估細項資訊及其在所有領域及在該領域所佔之分數權重。

c.邏輯：

各領域內評估細項之分數權重總和不得超過100%。

G. 符合類別維護功能

a.目的：提供業務管理者維護符合類別所對應之分數。

b.功能說明：

I.業務管理者之角色方可以使用本功能。

II.預設:符合=100%;部份符合=50%;未符合=%;不適用=100%。

H. 自評作業功能

a.目的：提供各單位填寫機關內個人資料管理符合現況

b.功能說明：

I.使用者依 ID 判斷所屬機關濾過讀取資料庫，預設查詢該機關資料庫主檔，選出符合條件之紀錄後展現於系統畫面，展現內容請參考，請參考表 5-2、表 5-3。

II.提供”查詢”、”變更”、”新增”、”刪除”功能，查詢：各

本報告之智慧財產權歸屬於法務部

機關可以查詢本機關資料庫內容,上級機關可以查詢下屬機關資料庫內容; 變更:進行更新時,更新前資料要記錄於歷史記錄檔,並標注更新人員 ID、日期及變更時間; 新增:系統登入後,若無法自資料主檔查無符合本機關條件之資料檔,此功能方啟動(enable),以提供新增一筆本機關之個資自評資訊;刪除:各機關只能刪除本機關之紀錄,刪除前之原資料要記錄於歷史資料檔。

I. 部會自評統計功能

a.目的:提供法務部掌握各部會(含所屬機關)之個資保護自評資訊報告。

b.功能說明:

I.本功能僅提供法務部"業務管理者"使用。

II.列印以部會及"自評總分數"為分類欄位,同時以直條圖呈現。

III.綜整再平均各部會及所屬機關的自評分數後,展現於報表,尚未填寫之機關不納入。

IV.提供查詢及列印功能。

c.邏輯:

I.單一機關之自評總分數。

II.部會機關總分數:已登錄所屬機關自評總分數之總和/已登錄所屬機關數。

J. 機關自評統計功能

a.目的:提供各主管機關掌握所屬機關之個資自評資訊。

b.功能說明:

本報告之智慧財產權歸屬於法務部

I.系統依使用者 ID 判斷是否有所屬機關，若有則呈現所屬機關代碼及機關名稱供使用者勾選查詢列印之機關。

II.提供可依業務系統(ex：檢察系統)或個別機關勾選需要查詢列印的資訊。

III.各主管機關列印所屬機關以”機關名稱”及各”領域”之自評分數及為座標，及各機關”自評總分數”。

IV.依機關代碼排序。

V.提供直條圖呈現各機關之領各領域自評分數。

VI.提供查詢及列印功能。

c.邏輯：

I.領域分數：單一機關各所屬領域分數=(“評估細項分數”*”符合類別”分數*該”評估細項”在所屬領域”分數權重”)之分數總合*該領域所佔分數權重。

II.自評總分數：該機關”領域分數權重”*”領域分數”之總合。

K. 機關自評明細報表功能

a.目的：提供各主管機關掌握所屬機關之個資自評詳細資訊。

b.功能說明：

I.系統依使用者 ID 判斷是否有所屬機關，若有則呈現所屬機關代碼及機關名稱供使用者勾選查詢列印之機關。

II.提供可依業務系統(ex：檢察系統)或個別機關勾選需要查詢列印的資訊。

III.以機關別分別呈現所有自評詳細內容。

IV.提供查詢及列印功能。

本報告之智慧財產權歸屬於法務部

L. 自評登錄狀態清單

a.目的：提供各主管掌握所屬機關系統提報狀況。

b.功能說明：

I.系統依使用者 ID 判斷是否有所屬機關，有下屬機關者方可執行此功能。

II.可選擇列印已登錄或未於系統登錄自評資料之清單。

III.以圓餅圖呈現已登錄及未登錄之統計資訊。

IV.提供查詢及列印功能。

（4）開發環境說明

A. 開發工具：ASP.net

B. OS：MS-Windows 2008 以上

C. Web Server：IIS

D. DB：MS-SQL

本報告之智慧財產權歸屬於法務部

（5）個資管理整體自評分析細項表

表 27：個資管理整體自評分析細項表

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
1	組織	機關是否已指派單位內負責個人資料管理的人員？					
2	組織	機關是否已組成個人資料保護組織，同時可清楚說明維護機關內部個人資料之管理作業權責？					
3	組織	承上題，上述要求是否已有文件化，載明成立個人資料保護管理組織及角色，並配置相當資源？					
4	組織	單位是否指派專人進行個人資料檔之管理及維護？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
5	組織	機關是否已清楚了解機關內有關個人資料之蒐集、處理、利用之範圍？					
6	組織	機關是否已辨識單位個資與個人資料保護法之適法性？					
7	組織	單位是否訂定經首長或其授權之人核准之員工及非員工個人資料如何與何時被蒐集、利用、以及保護之個人資料管理政策？					
8	告知	機關直接蒐集個人資料是否已取得當事人書面、電話、傳真或電子方式同意？（法令授權免通知者除外）					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
9	告知	機關是否設置網站供公眾查閱個人資料檔案名稱、機關名稱、聯絡方式、資料檔案保有依據及特定目的、個人資料類別等？(公務機關)					
10	告知	機關依法向當事人直接蒐集個資時，是否明確說明蒐集個人資料的機關名稱,目的,個資類別,期間,地區,對象,處理方式/當事人行使權利及方式/不提供之影響？					
11	告知	機關是否提供清楚與明顯的說明予組織內或組織外人員，有關個人資料的安全維護方式？					
12	告知	機關是否提供清楚與明顯的說明予組織內或組織外人員，有關當事人如何查詢或存取其個人資料？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
13	告知	機關是否提供清楚與明顯的說明予組織內或組織外人員，有關當事人如何更正或刪除其個人資料？					
14	告知	機關內間接蒐集之個人資料是否已規劃告知當事人？					
15	告知	機關是否設計提供當事人申訴程序與管道？					
16	蒐集處理利用	機關是否有盤點組織內所有的個人資料，並建立清冊以利管理？					
17	蒐集處理利用	機關內是否針對各項個人資料之蒐集、處理、利用及銷毀建立資料流程圖以掌握資料流向及管理方式？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
18	蒐集處理利用	機關進行個人資料蒐集時是否遵循所屬主管機關的法規或公約（例如 金融、保險、社會安全、健康照護等）？					
19	蒐集處理利用	機關內是否識別間接蒐集之個人資料之適法性及特定目的之合理性？					
20	蒐集處理利用	機關是否針對特種個資（醫療、基因、性生活、健康檢查、犯罪前科）進行蒐集、利用及處理？					
21	蒐集處理	機關若有蒐集特種資料是否取得法令依據？					
22	蒐集處理	機關若有蒐集特種資料是否清楚了解機關內有關特種資料之用途？					
23	蒐集處理	機關若有蒐集特種資料，是否有適當之安全維護計畫？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
24	蒐集處理利用	機關之個人資料管理是否有建立必要之使用紀錄、軌跡資料（Log Files）及證據之保存措施？					
25	蒐集處理利用	機關內是否有針為個人資料分級進行衝擊分析及風險評鑑？（含備份檔案及軌跡檔案）					
26	蒐集處理利用	機關內是否有針為個人資料不同等級處理進行安控措施？（含備份檔案及軌跡檔案）					
27	蒐集處理利用	機關是否執行資料安全管理？					
28	蒐集處理利用	機關是否執行人員安全管理？					
29	蒐集處理利用	機關否執行設備安全管理？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
30	蒐集處理利用	機關內是否有針對個人資料顯示進行適當的去識別化？					
31	蒐集處理利用	機關與其它單位個人資料交換是否已識別個人資料之適法性及特定目的利用之合理性？					
32	蒐集處理利用	機關與其它單位個人資料交換是否已採取適當保護措施？					
33	蒐集處理利用	對於個資(紙本及數位資料)之存取及利用是否保有完整的紀錄、軌跡資料					
34	蒐集處理利用	機關是否已針對受委託處理個資案件之單位，於契約上訂有個資保護法令及機關內部個資相關規定要求？					
35	蒐集處理利用	機關是否已針對受委託單位，於契約上訂有明確的監督要求?並執行監督?					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
36	蒐集處理利用	機關是否有將資料傳送於境外，該境外地區是否有個資保護法令(規範)，且已取得中央目的主管機關同意?					
37	訓練	機關是否已進行有效的個人資料保護全面性（含新人）人員宣導及教育訓練？					
38	訓練	機關是否針對負責管理及維護個人資料檔案之專人進行有效的專業教育訓練？					
39	程序	機關是否已建立個人資料內部管理程序或規則，以確保單位內個人資料蒐集、處理、利用、刪除及傳輸符合特定目的要求？					
40	程序	機關是否有設計當事人查詢、變更、刪除資料之程序？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
41	程序	機關是否有設計當發生個人資料被竊取、洩漏、竄改或其它侵害事件之主動通知程序?					
42	程序	機關是否有設計風險評估及管理程序？					
43	程序	機關內是否有設計個資事故通報程序？					
44	程序	機關內是否有設計個資事故應變處理程序？					
45	程序	機關內是否有設計內部稽核程序？					
46	程序	機關是否有設計文件管理程序？					
47	程序	機關是否有設計當個人資料蒐集目的消失或屆滿之資料刪除程序？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
48	程序	是否訂有個人資料檔案維護計畫及業務終止後個人資料處理方法等相關事項之辦法(中央目的主管機關)					
49	程序	是否訂有個人資料檔案維護計畫					
50	程序	是否訂有業務終止後個人資料處理方法					
51	程序	是否訂有申訴程序					
52	程序	是否訂有証據保存程序					
53	程序	是否訂有維護資料正確性程序					
54	程序	是否有盤點單維護機制					
55	PDCA	機關對於個資之蒐集、處理與利用之流程，是否進行內部稽核？					
56	PDCA	機關是否定期檢視個資政策及個資保護					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
		執行結果？					
57	PDCA	機關是否有實施個人資料安全維護之整體持續改善規劃？					
58	其它	機關是否取得品質管理系統(ISO9000)認證（請說明認證範圍）？					
59	其它	機關是否取得資訊安全管理系統(ISO27001)認證（請說明認證範圍）？					

資料來源：本計畫整理

本報告之智慧財產權歸屬於法務部

（6）個資環境設備安全評估自評項目表

表 28：個資環境設備安全評估自評項目表

序號	安全評估項目	問題	說明
1	存取控制實施(AC-3)	多少系統、帳號權限是否有作？	
2	最小權限(AC-6)	多少系統、帳號權限是否有作？	
3	職責分工(AC-5)	資料庫、系統開發、作業系統是否有分工？	
4	遠端存取(AC-17)	是否有提供、如何管制、加密機制？	
5	稽核事件(AU-2)	如何管理監視日誌(Log)？	
6	稽核紀錄的檢視、分析及報告(AU-6)	是否有定期檢視？	
7	識別與驗證(鑑別/Authentication)	是否有識別帳號(ID)、密碼(PW)的控管？	

本報告之智慧財產權歸屬於法務部

序號	安全評估項目	問題	說明
	(機關使用者)(IA-2)		
8	行動裝置的存取控制(AC-19)	是否有針對隨插即用存取裝置(USB)控管？	
9	媒體存取(MP-2)	是否有針對隨插即用存取裝置(USB)控管？	
10	媒體標記(MP-3)	儲存媒體(硬碟、光碟片、USB…等)的分類、分級、標示與管理？	
11	媒體儲存(MP-4)	儲存媒體的分類、分級、標示與管理？	
12	媒體傳輸(MP-5)	儲存媒體的分類、分級、標示與管理？	
13	媒體淨化(MP-6)	媒體如何刪除、銷毀或再使用？	
14	傳輸機密性(SC-9)	機敏性資料如何傳送？	
15	靜態資訊的保護(SC-28)	非經常使用個人資料或機敏性文件、資料、檔案如何儲存管理？	

本報告之智慧財產權歸屬於法務部

序號	安全評估項目	問題	說明
16	資訊系統監視(SI-4)	如何識別、監控對個人資料的存取活動？	

資料來源：本計畫整理

本報告之智慧財產權歸屬於法務部

3.公務機關個資保護教育訓練管理系統作業程序書

（1）目的

為建立法務部（以下簡稱本部）之全國個資保護專業教育訓練之管理業務，特訂定本作業程序，規範從單位帳號申請至教育訓練紀錄登錄之實施管理活動，以便各公務機關同仁皆能有效遵循管理之要求 。

（2）適用範圍

各機關之個資保護教育訓練資訊皆為本系統管理的範圍。

（3）權責

A. 系統管理者

a.由本部資訊人員擔任

b.負責系統角色權限設定

c.負責人員權限設定

d.負責系統資料轉入公務人員學習網

B. 業務管理者

a.負責個資訓練課程管理

b.負責各類管理報表管理

c.負責個資訓練類別管理

d.負責個資訓練保護課程管理

e.負責公務機關代碼維護

C. 各機關管理者

本報告之智慧財產權歸屬於法務部

a.負責機關內管理報表列印

b.負責個資訓練課程名稱維護

D. 一般同仁

參加各類個資保護訓練課程

（4）名詞定義

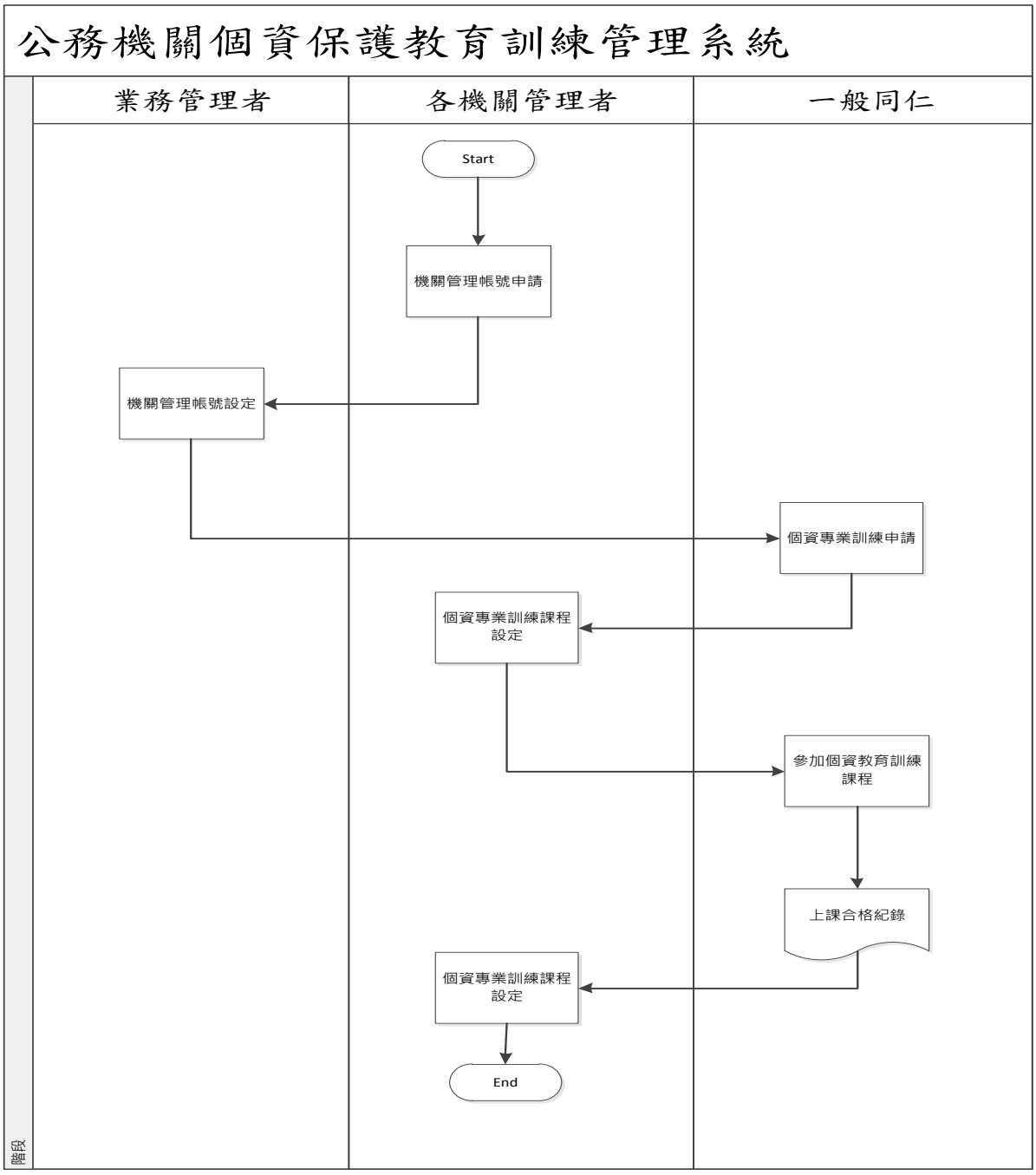
公務機關個資保護教育訓練管理系統:由法務部開發管理維護，提供各機關維護個人資料保護專業訓練紀錄。

（5）相關文件

無

本報告之智慧財產權歸屬於法務部

（6）流程圖



資料來源:本計畫整理

圖 27：公務機關個資保護教育訓練管理系統流程圖

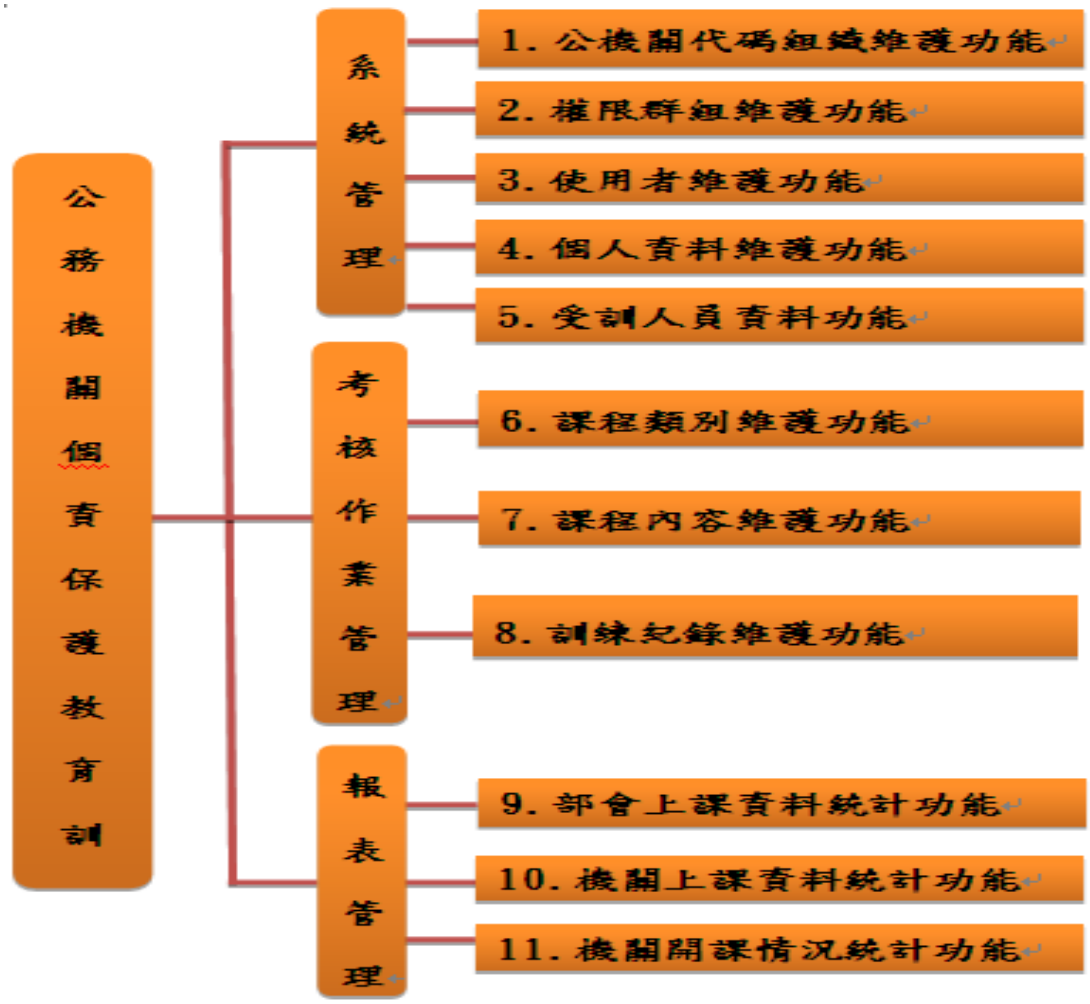
本報告之智慧財產權歸屬於法務部

4.公務機關個資保護教育訓練管理系統分析文件

（1）目的

為建立法務部之公務機關個資自評管理業務，特訂定本作業程序，規範從單位申請系統使用帳號至機關個資現況成熟度登錄之實施管理活動，以便各公務機關本部進行公務機關法令符合度的有效監督要求。

（2）功能架構圖



資料來源：本計畫整理

圖 28：公務機關個資保護教育訓練管理系統架構圖

（3）功能說明

本報告之智慧財產權歸屬於法務部

系統登入必須先判斷是否為系統預設帳號，若為預設帳號則強制至「D.個人資料維護功能」進行密碼變更。

使用者登入系統後，至「C.使用者維護功能」相關資料庫檢視可使用之功能才 Enable。

提供使用者忘記密碼，系統自動重新預設密碼，透過 e-mail 傳送至當事人之功能。

A. 公務機關代碼組織維護功能

a.目的：依行政院人事行政總處異動進度維護正確資訊。
(註：若人事行政總處代碼無法提供”業務系統”之機關所屬層級，則須另增加機關層級維護功能)

b.功能說明：

I.系統管理者之角色方可以使用本功能。

II.提供查詢”、”變更”、”新增”及”註記刪除”功能。

B. 權限群組維護功能

a.目的：提供本系統之角色權限設定功能

b.功能說明：

I.系統管理者之角色方可以使用本功能。

II.預設功能權限對照表：

表 29：角色權限對照表(公務機關個資自評管理系統)

	1	2.1	2.2	2.3	2.4	3	4	5	6	7	8	9
業務管理者	X	X	X	X	X	X	X	X				X
系統管理者									X	X	X	X
機關使用者	X		X	X	X							X

資料來源：本計畫整理

本報告之智慧財產權歸屬於法務部

C. 使用者維護功能

a.目的：提供維護人員帳號及密碼維護功能。

b.功能說明：

I.系統管理者之角色方可以使用本功能

II.提供新增帳號密碼預設機制

III.提供人員帳號、密碼及所屬角色之維護功能，密碼資料庫內必須遮蔽，螢幕以代號顯示。

D. 個人資料維護功能

a.目的：提供所有使用者可以自行變更密碼。

b.功能說明：

I.所有使用者均可以使用本功能

II.密碼長度至少八碼

III.訓練資料轉入”公務人員學習網”介面

E. 受訓人員資料功能

a.目的：提供機關查看及維護該機關受訓人員資料以及調閱該人員的上課紀錄。

b.功能說明：

I.查看該機關受訓人員資料

II.維護該機關受訓人員資料

III.調閱該人員的上課紀錄

F. 課程類別維護功能

a.目的：提供系統管理者維護訓練課程類別。

b.功能說明：

本報告之智慧財產權歸屬於法務部

I.系統管理者之角色方可以使用本功能。

II.提供”查詢”、”變更” 、”新增”及”刪除”功能。

III.個資保護訓練類別: 例如”法令類”、”管理類”、”資安類”及”技術類”

G. 課程內容維護功能

a.目的：提供各機關維護所屬機關之個資教育訓練課程。

b.功能說明：

I.各機關管理者之角色方可以使用本功能。

II.由各機關管理者自行維護機關內課程名稱及課程類別相關資訊。

III.維護內容至少包括:”年度”、”機關代碼”、”機關名稱”、”個資保護訓練類別”、”個資保護課程名稱”、”課程時數”。

H. 訓練紀錄維護功能

a.目的：提供各單位填寫機關內個人資料管理符合現況

b.功能說明：

I.使用者依 ID 判斷所屬機關濾過讀取資料庫，預設查詢該機關、該年度資料庫主檔，選出符合條件之記錄後展現於系統畫面，展現內容至少包括年度、個資訓練類別、個資保護課程名稱、上課時數、受訓人員身分証字號、受訓人員姓名、受訓時間。

II.提供”查詢”、”變更”、”新增”、”刪除”功能，查詢： 各機關可以查詢本機關資料庫內容; 變更：進行更新時，更新前資料要記錄於歷史記錄檔，並標注更新人員 ID、日期及變更時間變更; 新增: 選擇此一功能後，使用者可以依特定課程逐筆新增個人受訓記錄，新增欄位至少包括機關名稱(依登錄 ID 辨識預定)、年度(預設當年度)、個資訓練類別(下拉選單，讀取課程類別資料檔) 、

本報告之智慧財產權歸屬於法務部

個資保護課程名稱(下拉選單，以機關為過濾條件，顯現功能 4 課程資料檔之課程名稱) 、課程時數(由功能 4 課程資料檔預設，可修改)、上課日期、上課人員身分証字號、上課人員姓名、資料登錄人員及資料登錄日期(斜體字欄位不須顯示於畫面)。

III.單一課程可以同時多筆登錄上課人員資料

I. 部會上課資料統計功能

a.目的：提供法務部掌握各部會(含所屬機關)之個資保護報告上課資訊。

b.功能說明：

I.本功能僅提供法務部”業務管理者”使用。

II.列印以”部會”及”個資保護類別”為分類欄位，年度預設為當年度，同時以直條圖呈現。

III.依各項個資保護類別分別統計各部會(含所屬機關)的上課人數合計，展現於報表。

IV.提供查詢及列印功能。

J. 機關上課資料統計功能

a.目的：提供各主管機關掌握所屬機關之年度個資保護類別訓練人員受訓總數。

b.功能說明：

I.系統依使用者 ID 判斷是否有所屬機關，若有則呈現所屬機關代碼及機關名稱供使用者勾選查詢列印之機關或全部。

II.提供可依年度業務系統(ex：檢察系統)或個別機關勾選需要查詢列印的資訊。

III.顯現資料以所屬機關為範圍

IV.以機關代碼排序以”機關名稱”及各”個資訓練類別”為

本報告之智慧財產權歸屬於法務部

座標，分別統計該機關之個資訓練類別之總受訓人數 。

K. 機關開課情況統計功能

a.目的：提供機關管理者統計該機關的上課紀錄。

b.功能說明：

提供以年度方式查詢上課時數統計與開課情況統計。

（4）開發環境說明

A. 開發工具：ASP.net

B. OS：MS-Windows 2008 以上

C. Web Server：IIS

D. DB：MS-SQL

（六）參考文獻

法務部，個人資料保護執行（管理）暨考核作業手冊，2011 年 12 月 30 日。

本報告之智慧財產權歸屬於法務部

二、公務機關個人資料保護執行程序暨考核作業手冊

（一）前言

法務部為因應「個人資料保護法」之通過，使公務機關建立個人資料保護及管理標準作業化流程，同時加強機關內部考核程序及導入外部監督機制，特研擬本作業手冊以供公務機關參考。觀察國內目前各公務機關之做法，現行考核程序中並未納入個人資料保護法之應有稽核程序，亦未建立獨立監督之角色要求，為協助各公務機關執行業務，能建立相關個資保護程序，以保障人民隱私權益。本部委託財團法人資訊工業策進會（以下簡稱資策會）執行 99 年度「公務機關個人資料保護方案計畫」(以下簡稱本計畫)，編定公務機關「個人資料保護執行程序暨考核作業手冊」(以下簡稱本手冊)。本手冊為本計畫需求項目：三、編定各公務機關「個人資料保護執行程序暨考核作業手冊」之交付文件，提供各公務機關參考使用。

1.目的

本手冊主要以「個人資料保護法」(以下簡稱個資法）為基礎，並參考國際個人資料保護相關標準（NIST SP800-122、BS10012 等，但不以此為限)，將提供公務機關執行個資保護之參考。本手冊提供公務機關一般共通性個人資料保護之建議，而如何將本手冊之觀念與方法，有效並適切地導入各公務機關，須依各公務機關施政目標（計畫)、運作模式、業務屬性、機關文化及其他因素之影響而調整。因此，各公務機關可參考本手冊，就機關規模、目標、作業模式及業務需求或特性加以彈性運用，並參酌業務運作時之設定政策目標、規劃及建置架構、執行與操作、監督審查與矯正預防及改善等作業，修正成符合各公務機關特性之版本，並據以針對所屬之資產與資訊系統進行個資保護之建置程序，以符合個人資料保護法與相關施行細則、資訊安全管理要點之要求；本手冊即為提供這些作業之實務概況。

有關個人資料保護法所提及之個人資料蒐集、處理、利用及傳輸等態樣與相關施行細則、資訊安全管理要點之各項要求及實務作業，

本報告之智慧財產權歸屬於法務部

本手冊將於個資保護管理執行作業及相關流程中說明其管理重點與作業流程。

2.章節架構

本手冊共分成前言、個人資料保護相關規範、個人資料保護政策與架構、個人資料保護管理執行作業、個資保護管理建置流程、資訊安全管理制度（ISMS）與個資保護導入作業、考核監督作業、結論等進行撰述，重點摘錄如下：

第一章說明本手冊之目的、手冊章節架構介紹。

第二章說明與本手冊相關之依據探討，包括有我國個資相關規範及說明個資法修法重點、對公務機關之衝擊與應注意事項。

第三章說明個人資料保護政策、架構、目標與個人資料保護執行管理之作業項目與其作業內容。

第四章介紹建置個人資料保護管理流程之四個階段，分別為「計畫」、「執行」、「檢視」及「持續改善」。

第五章說明針對已通過 ISO 27001 資訊安全管理系統驗證的公務機關，建議其於個資保護系統的導入過程中，納入對機關現行資訊安全管理系統。另外，說明個資管理需求的補強措施建議與整合注意事項，以提供公務機關進行個資管理導入作業時的參考個人資料保護政策。

第六章說明因應個資管理之考核及監督作業說明。

第七章說明本手冊之結論。

3.使用建議

公務機關如欲瞭解我國個資法修正重點與公布後應注意事項，可參閱第二章個人資料保護相關規範。

本手冊主要內容為探討個人資料保護執行管理之作業項目與其作業內容、個資保護管理建置流程及持續改善之考核監督作業，提供

本報告之智慧財產權歸屬於法務部

公務機關於執行個人資料保護作業之參考，以便快速檢視各階段作業或所擬之文件內容，在執行方面是否仍有疏漏，適時予以補強。

本手冊希望期提供公務機關個人資料保護正確觀念及實務運用，建議公務機關將個人資料保護與日常運作模式相互結合，即將個人資料保護管理機制整合至公務機關各作業流程，善用 PDCA（Plan→Do→Check→Action，簡稱 PDCA）管理循環模式，以有效建立公務機關之個人資料保護能量，順利推動並落實個人資料保護法。

（二）個人資料保護相關規範

隨著科技與網際網路的快速發展，各種資訊與網路應用服務如雨後春筍般出現，如社群網站、電子商務網站、網路拍賣網站及網路銀行等，這些應用服務多帶有個人資料在其中，一旦安全控制措施不夠完備，容易造成個人隱私資料遭受侵害，因此，國際組織如經濟合作暨發展組織（OECD）、亞太經濟合作組織（APEC）等，均制訂相關規範，以提供其會員國對於涉及個人隱私資料保護問題之處理原則。此外，國際上亦有許多提供個人資料隱私衝擊保護、個資管理制度及個資安全控制保護措施之標準，可於實作時之參考，如 ISO 29100、ISO 22307、BS10012 及 NIST SP800-122 等等。

我國亦於民國 99 年 5 月 26 日公布「個人資料保護法」（尚未施行）條文，藉以規範公務和非公務機關對於許多敏感性個人資料的蒐集、處理及利用，以下將針對我國人資料保護的規範、標準及法令和個人資料保護政策、架構與目標進行說明。

民國 84 年 8 月 11 日公布施行「電腦處理個人資料保護法」，以非公務機關為例，電腦處理個人資料保護法之適用主體有行業類別之限制，僅限於徵信業、醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業等八行業，其餘一般行業與個人均不受規範，保護之客體亦只限於經電腦處理之個資，不包括非經電腦處理之個資，對於保護個資隱私權益之規範顯有不足，故法務部自民國 90 年起即積極進行相關修法工作，於整理國內學界與實務界之修法意見，並參酌各國個資保護之立法例，經召開多次公聽會與研討會後，研擬「電腦處理個人資料保護法修正草案」，報請行政院審查，行政

本報告之智慧財產權歸屬於法務部

院院會業於民國 93 年 9 月 8 日通過，並函送立法院審議。

民國 99 年 5 月 26 日修正公布個人資料保護法後，使個資法在保障個人隱私資料，並兼顧新聞自由平衡下邁向新的里程碑，個資法強化了個資揭露、查詢及更正等的自主控制，同時也將「亞太經濟合作論壇（APEC）隱私保護綱領」所揭示的預防損害、告知及蒐集限制等 9 項原則納入規範，以迎接個資保護全球化時代的來臨，以下針對新修正之個資法進行說明。

1.個人資料的定義與範圍

與電腦處理個人資料保護法不同的是，電腦處理個人資料保護法保護對象只限於經電腦處理之個人資料，因此，若非經電腦處理之個人資料，則不在該法適用範圍內，此將造成個人資料保護之漏洞，有失平衡。因此，為落實對個資之保護，本次修法將保護客體予以擴大，不再以經電腦處理之個資為限，將紙本資料併予納入。另外在保護範圍增列護照號碼、醫療、基因、性生活、健康檢查、犯罪前科及聯絡方式等得以直接或間接識別該個人之資料。

個資法對於個人資料之定義係指，自然人之姓名、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、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

為了充分保護當事人，個資法另外規範五種特種個人資料，包括醫療、基因、性生活、健康檢查及犯罪前科等個人資料。原則上，特種個資不得蒐集、處理或利用，除非符合第 6 條第 1 項之規定之例外規定，始可為之。

2.個資法及 100 年 10 月間預告之個資法施行細則修正草案內容之簡介

（1）個資法相關規範之簡介

新修正之個資法（尚未施行）將個人資料之範圍擴大，亦不再限制行業別。另外，針對行為規範也予以增修，並且強化行政

本報告之智慧財產權歸屬於法務部

機關監督非公務機關之職權，賦予中央目的事業主管機關或直轄縣市政府，於合乎比例原則之範圍內，得派員攜帶執行職務證明文件進入檢查。另外，為了強化個資當事人之權益以及降低當事人之訴訟成本，個資法新增符合規定之財團法人或公益社團法人得提起團體訴訟之規定。除此之外，個資法提高基於同一原因事實當事人可請求之賠償總額，以新台幣二億元為限。

以下以公務機關之角度為出發點，闡述公務機關適用個資法之重點。

如前所述，個資法刪除電腦處理個人資料法非公務機關行業別之限制，即凡持有個人資料之任何自然人、法人或其他團體，除「為單純個人或家庭活動之目的，而蒐集、處理或利用之個人資料」及「公開場合蒐集、處理、利用之未與其他個人資料結合之影音資料」外，皆須適用個資法。

個資法第 2 條定義公務機關之範圍，公務機關係指行使公權力之中央、地方機關或行政法人。所謂行政法人之定義，則依行政法人法第 2 條規定，為國家及地方自治團體以外，由中央目的事業主管機關，為執行特定公共事務，依法律設立之公法人。

除此之外，在中華民國領域外對中華民國人民蒐集、處理或利用個資者，亦有個資法之適用。

蒐集個人資料時，不論是直接或間接蒐集之型態，除符合得免告知情形者外，均須明確告知當事人公務機關名稱、蒐集目的、資料類別、利用地區、期間、對象及方式、當事人得行使權利之方式、當事人得自由選擇提供個人資料時，不提供將對其權益之影響，若為間接蒐集則還需另外告知資料來源。

另外，公務機關對於個人資料之蒐集、處理應具備特定目的以及特定情形。特定情形依個資法第 15 條之規定包含執行法定職務之必要範圍、經當事人書面同意以及對當事人權益無侵害。公務機關對個人資料之利用，依第 16 條規定，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。例外符合但書七種情形時，得為特定目的外利用。前述之七種情形分別為：法律

本報告之智慧財產權歸屬於法務部

明文規定；為維護國家安全或增進公共利益；為免除當事人之生命、身體、自由或財產上之危險；為防止他人權益之重大危害；基於公共利益而進行學術研究，且資料經處理後已無從識別當事人；有利於當事人權益；經當事人書面同意。

關於書面同意之要件，根據個資法第 7 條之規定，須經蒐集者告知個資法所定應告知事項後，所為允許之書面意思表示。如係特定目的外利用個人資料需當事人書面同意者，不得以概括方式取得其同意，而應另以單獨書面同意方式為之，以確保當事人之權益。

此外，公務機關就其蒐集之個人資料，應賦予當事人特定之權利行使管道。個資法第 10 條規定，公務機關應依當事人之請求，答覆查詢、提供閱覽或製給複製本。而針對前述該當事人權利行使的回覆時限，則根據個資法第 13 條規定，公務機關應於 15 日內，為准駁之決定；必要時，得予延長，延長之期間不得超過 15 日。若延長超過十五日，機關必須將其原因以書面通知請求之當事人。對於查詢或請求閱覽個人資料或製給複製本者，依據個資法第 14 條之規定，公務機關得酌收必要之成本費用。

公務機關依個資法第 11 條規定，應主動或依當事人之請求，更正或補充當事人之個人資料，以維護個人資料之正確。因未為更正或補充致造成不正確者，如係可歸責於該公務機關之事由，應於更正或補充後，通知曾提供利用之對象，使該資料能即時更新，避免當事人權益受損。

公務機關就其所保有之個人資料檔案，依個資法第 17 條之規定，應將檔案名稱、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公開於電腦網站，或以其他適當方式供公眾查閱，其有變更者亦同。

另外，個資法第 18 條規定，公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

個資法第 12 條規定，公務機關於違反個資法之規定而導致

本報告之智慧財產權歸屬於法務部

個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人，因此，公務機關應建立內部之事故應變及通報程序，以符合個資法之規範。

為加強個人資料之保護，中央目的事業主管機關或直轄市、縣（市）政府，發現非公務機關違反個資法規定或認有必要時，得派員攜帶執行職務證明文件，進入檢查，如發現有違法情事，並得採取必要處分。

個資法於第 28 條規定公務機關違反本法規定，而導致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，須負損害賠償責任，但損害因天災、事變或其他不可抗力所致者，不在此限。

刑罰之規範須詳見個資法第 41 條至第 46 條，值得一提的是，個資法針對公務員違法有加重之規定，第 44 條規定，公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。

關於個資法之施行期程，依據個資法第五十六條本法施行日期，由行政院定之。故其施行日期將俟法務部完成施行細則修訂後，由行政院頒布施行。

（2）100 年 10 月間預告之個資法施行細則修正草案內容之簡介

100 年 10 月間法務部預告之施行細則修正草案之內容主要針對間接識別、特種資料（病歷、基因、性生活、健康檢查、犯罪前科）及個人資料檔案之定義、委託監督項目、安全維護措施之內容、當事人自行公開之定義、告知通知之方式、團體訴訟中對於公益團體之定義等進行說明。本手冊將 100 年 10 月間預告之個資法施行細則修正草案總說明中的修正要點，摘要說明如下：

A. 100 年 10 月間預告之個資法施行細則修正草案第 3 條規定，所謂間接方式識別係指僅依該資料不能識別，須與其他資料對照、組合、聯結等，始能識別該特定個人者。但

本報告之智慧財產權歸屬於法務部

查詢困難、需耗費過鉅或耗時過久始能特定者，不在此限。

B. 關於病歷、醫療、基因、性生活、健康檢查以及犯罪前科之定義，規定於 100 年 10 月間預告之個資法施行細則修正草案第 4 條。

C. 100 年 10 月間預告之個資法施行細則修正草案第 7 條規定，受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。當事人行使本法之權利應向委託機關為之。亦即包含當事人請求查詢、閱覽、製給複製本、補充、更正、停止處理利用、刪除或請求損害賠償等權利時，應以委託機關為對象。此外，100 年 10 月間預告之個資法施行細則修正草案第 8 條規定，就委託他人蒐集、處理、利用之機關增訂委託人之適當監督義務規定。

D. 所謂的安全維護事項，根據 100 年 10 月間預告之施行細則修正草案第 9 條第 2 項之規定，包含下述 11 項必要事項：

a.成立管理組織，配置相當資源

b.界定個人資料之範圍

c.個人資料之風險評估及管理機制。

d.事故之預防、通報及應變機制。

e.個人資料蒐集、處理及利用之內部管理程序。

f.資料安全管理及人員管理。

g.認知宣導及教育訓練。

h.設備安全管理。

i.資料安全稽核機制

j.必要之使用紀錄、軌跡資料及證據之保存。

本報告之智慧財產權歸屬於法務部

k.個人資料安全維護之整體持續改善。

E. 100 年 10 月間預告之個資法施行細則修正草案第 10、17 條釐清當事人自行公開、已合法公開之個人資料、資料經過處理後或依其揭露方式無從識別特定當事人等概念。

F. 100 年 10 月間預告之個資法施行細則修正草案第 11、12 條增訂當事人自行公開、書面意思表示之方式及單獨所為之書面意思表示之意涵。

G. 100 年 10 月間預告之個資法施行細則修正草案第 13、18、19 條增/修訂個資法規定告知、通知以及公務機關以其他方式供公眾查閱之方式。

H. 公務機關依據本法，應指定專人辦理安全維護事項，所謂專人，根據 100 年 10 月間預告之施行細則修正草案第 21 條規定，係指具有管理及維護個人資料檔案之專業能力，且足以擔任機關檔案資料安全維護經常性工作之人員。公務機關應針對該人員辦理相關專業之教育訓練。

施行細則尚未正式公布，其施行日期日後將由行政院以命令定之。

（3）對公務機關之衝擊

面對個資法之施行，公務機關即將面對的主要衝擊如下：

A. 保護客體範圍擴大

個人資料之範圍不限於舊法所規範的電腦處理個資，包括直接、間接識別之個資或人工資料（書面文件）皆屬於新版個資法所規範之範圍。

B. 作業流程調整需求

本報告之智慧財產權歸屬於法務部

針對個人資料之蒐集、處理及利用之作業流內各階段活動，包括主動告知的實踐與責任、當事人權利行使時之回應與處理、委外作業權責定義與合約監督管理、個資事故流程之管理與檢討等階段，都必須重新檢視。

為因應個資法之要求，保有個人資料之公務機關須訂定機關內部適用之個人資料檔案安全維護規定。機關可參考法務部已對外公告「法務部個人資料保護管理要點草案」，該管理要點訂定以下內容，各機關可參酌本要點，依其機關以及職掌等現況，訂定之。草案內容如下：

a.總則：明定機關個人資料保護管理執行小組設置之目的、執行小組之任務、執行小組召集人、執行祕書及委員之組成及幕僚工作之負責單位、執行小組會議召開之期間、主持人及得邀請出列席之人員、指定專人及其辦理事項、設置個人資料保護聯絡窗口及其辦理事項。

b.個人資料範圍：明定本部保有特種資料之個人資料檔案名稱、本部保有個人資料特定目的之項目以本部依適當方式公開者為限，有變更者亦同。

c.個人資料之蒐集、處理及利用：明定個人資料之蒐集；處理或利用之正當法律程序；告知義務之程序；個人資料補充或更正之程序、資料正確性有爭議之處理程序；刪除、停止處理或利用個人資料之程序；個人資料遭到竊取、洩漏、竄改或遭其他方式侵害之通知處理程序。

d.當事人行使權利之處理：明定當事人請求之查詢答覆、提供閱覽、製給複製本、更正、補充、停止蒐集、處理、利用或刪除個人資料之處理程序，請求查詢、閱覽或製給個人資料複製本適用「法務部及所屬機關提供政府資訊收費標準」之規定並依「法務部受理申請提供政府資訊及閱覽卷宗須知」辦理，明定本部保有之個人資料檔案仍適用政府資訊公開法或相關法律規定，限制公開或不予提供。

本報告之智慧財產權歸屬於法務部

e.個人資料檔案安全維護：明定專人應依本要點及相關法令規定辦理個人資料檔案安全維護事項；針對個人資料檔案應建立管理制度及人員安全管理規範；明定個人資料檔案安全稽核之機關及程序；個人資料檔案發生非法入侵情事之緊急應變與通報程序；個人資料檔案安全維護工作應符合法務部個人資料保護管理要點、行政院及法務部訂定之相關資訊作業安全與機密維護規範。

C. 舉證與處罰之預防

透過建立個人資料保護政策與規範、定義適當個資管理機關及人員權責、提升安全控制措施至合適等級、保存重要個資之管理紀錄、軌跡紀錄與文件紀錄，以及持續進行人員認知與訓練等做法，確保機關面臨未來可能出現之訴訟風險可妥善處理，並且得以提出令法院願意採信之相關證據。

除此之外，公務機關必須建立持續改善機制，以確保機關內部所建置之個人資料保護系統符合個資法相關規範之要求，避免可能產生之相關風險。

（4）公務機關應注意事項

個資法對公務機關處理人員而言，須特別注意之規範內容如下：

A. 蒐集與處理

公務機關對個人資料之蒐集或處理，除第 6 條第 1 項所規定之特種資料外，應有特定目的，並符合特定情形，包含執行法定職務必要範圍內；經當事人書面同意或對當事人權益無侵害。另外，依個資法之規定，公務機關非向資料本人蒐集或處理個人資料時，必須依個資法第 8 條履行告知義務。

特種資料之蒐集、處理、利用，依第 6 條之規定，原則上禁止，只有於符合但書情形時，始得為之。

本報告之智慧財產權歸屬於法務部

另外，依個資法第八條之規定，下列情形得免告知，直接向當事人進行資料蒐集，包含依法律規定得免告知；個人資料之蒐集係公務機關執行法定職務；告知將妨害公務機關執行法定職務；告知將妨害第三人之重大利益；當事人明知應告知之內容。

B. 利用

公務機關利用個人資料時，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。但有下列情形之一者，得為特定目的外之利用，包含法律明文規定；為維護國家安全或增進公共利益；為免除當事人之生命、身體、自由或財產上之危險；為防止他人權益之重大危害；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；包含有利於當事人權益；經當事人書面同意等情形。

C. 當事人權利行使

公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同。相關事項包含個人資料檔案名稱；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。公開之程序以及做法除了依個資法之規範外，可參考政府資訊公開法之相關規定。

個資法第 11 條規定，個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

機關若違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。另外，因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

本報告之智慧財產權歸屬於法務部

而就損害賠償責任之認知部分，公務機關違反個資法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。於損害賠償之規定部分，公務機關適用國家賠償法之規定。

D. 個人資料之保存、維護與委外

個資法要求公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

公務機關須特別注意委外監督之相關法律規範，由於公務機關透過委外專案執行業務之情形相當普遍，若受委託方進行相關個人資料蒐集、處理及利用個人資料之行為時，依個資法第 4 條之規定，於個資法之適用範圍內，視同委託機關。再依 100 年 10 月間預告之個資法施行細則修正草案第 7 條規定，當事人行使本法之權利，應向委託機關為之，包含當事人可主張之權利以及損害賠償之權利，皆須向委託機關行使。故，若機關委託之法人、自然人或團體違反個資法之規定而造成當事人之損害時，個資當事人直接向公務機關提起國家賠償訴訟。據此，基於個資法之要求，公務機關必須妥善監督其委託廠商是否妥善管理所蒐集、處理及利用之個資，以杜絕日後遭國家賠償訴訟之風險。

（5）公務機關應立即研辦事項

各公務機關應立即研辦事項主要包括：

A. 各中央目的事業主管機關會同法務部訂定

公務機關或學術研究機構基於醫療、衛生、犯罪預防之目的而蒐集、處理或利用特種個人資料之範圍、程序及其他應遵循事項之辦法。

本報告之智慧財產權歸屬於法務部

B. 各中央目的事業主管機關訂定

a.非公務機關個人資料檔案安全維護計畫或業務終止後個人資料處理方法之標準。

b.訂定機關內部之個人資料管理要點

c.應訂定機關進行行政檢查之處理要點

C. 公開下列事項於電腦網站上，提供公眾查閱

a.個人資料檔案名稱。

b.保有機關名稱及聯絡方式。

c.個人資料檔案保有之依據及特定目的。

d.個人資料之類別。

D. 指定專人辦理個人資料檔案安全維護事項

有鑑於公務機關在個人資料保護與管理上事權統一之重要，公務機關應設立個人資料保護管理執行小組之任務編組，並指派小組召集人、執行秘書、委員及幕僚工作之負責單位等人員所組成，以利有效推動個人資料保護相關事務。

以法務部公布之法務部個人資料保護管理要點草案為例，法務部個人資料保護管理執行小組置召集人及執行秘書各一人，由部長指定之；委員十一人由各單位指派專人（科長以上）一人擔任。本小組幕僚工作由法務部法律事務司辦理；為強化幕僚功能，協助辦理幕僚工作，並得邀請法務部各單位人員參與幕僚作業。

本報告之智慧財產權歸屬於法務部

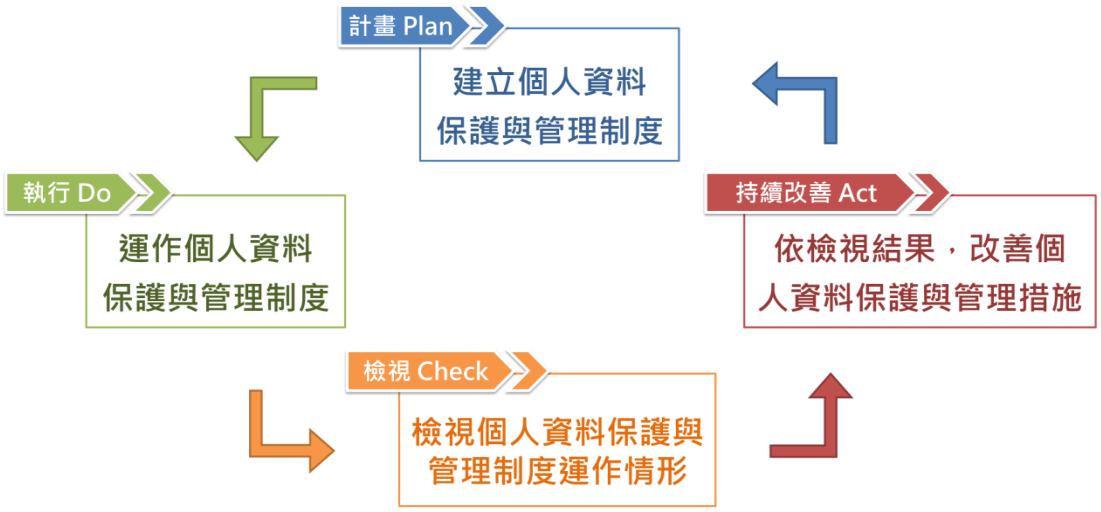
（三）個人資料保護政策與架構

1.個人資料保護之目標

個人資料保護管理的推動可以協助公務機關改善績效並提供更好的服務、資源的更有效使用並鼓勵創新。相反的，缺乏個人資料保護管理，人民與企業可能因公共服務不當而受傷害，公務機關的聲望可能因服務無法符合社會大眾的期望而受損。是故，個人資料保護管理的核心價值不僅在於降低威脅，更是追求機關創新機會與公眾價值。

2.個人資料保護流程之方法論

依我國個資法之背景觀之，個資法要求公務機關及非公務機關須以 PDCA 之方法論建置內部之個人資料保護制度，以確實保護內部所保有之個人資料。PDCA（Plan/Do/Check/Act）之內容主要為計畫、執行、檢視以及改善四個步驟，因此，公務機關建置內部之個人資料制度時，必須以此方法論建置之，本手冊第 4 章亦以此方法論安排章節以說明之個人資料保護制度之建置流程。參考下列對於 PDCA 流程圖之說明圖：



資料來源：本計畫自行繪製

圖 29：PDCA 流程圖

本報告之智慧財產權歸屬於法務部

3.個人資料保護政策

個人資料保護管理政策在於建立公務機關個人資料保護管理整體發展方向與基本原則。政策將確定公務機關的個人資料保護管理責任歸屬與績效的要求。它代表公務機關對促進良好個人資料保護管理的正式承諾，尤以機關首長的承諾為然。

公務機關應制定經機關首長核定的個人資料保護管理政策，明白陳述機關整體個人資料保護管理目標與改善機關個人資料保護管理績效之承諾。該政策宜包含：

（1）依機關的業務屬性與風險特性，將合法適當蒐集、處理以及利用個人資料；

（2）包括遵守個資法相關法令、規章與其它要求之承諾；

（3）管理措施文件化、實施與維持；

（4）與機關所有員工充份溝通，並確認所有員工均瞭解其個人肩負的責任；

（5）因應申訴以及諮詢之相關程序；

（6）定期審查，以確保管理政策的適宜性；

（7）持續改善個人資料保護管理制度 。

通常，個人資料保護管理政策說明由機關首長簽署。個人資料保護管理政策應與機關整體政策、施政目標及內部管理辦法一致，以達到融入機關文化之目的。在建立機關個人資料保護管理政策上，機關首長及高層主管應考量：

（1）機關整體施政目標及計畫所面臨的個人資料保護管理風險；

（2）法令與其他規章對個人資料保護管理要求；

（3）機關已往與目前的個人資料保護管理作為；

（4）其他利害相關者要求；

（5）持續改善的機會與需求；

本報告之智慧財產權歸屬於法務部

（6）個人資料保護管理所需資源；

（7）對機關同仁、民眾與其它機關的影響

為了促使機關個人資料保護管理有效執行，政策應予文件化，定期檢討制度的適切性，並視需要修訂。

機關同仁的參與及承諾對於建置完善的個人資料保護管理制度至為重要。機關同仁需瞭解個人資料保護管理於本身工作環境及品質之責任與義務，並應鼓勵機關同仁主動參與機關個人資料保護管理工作。公務機關須與機關同仁清楚溝通個人資料保護管理目標，使他們可以評估他們自己在個人資料保護管理績效上的貢獻。同時因法令的改變、社會期待的提昇是無法避免的，因此，公務機關的個人資料保護管理政策與管理制度，均需定期或不定期審查以確保它們的適切性與有效性。如有任何調整，則應儘速與利害相關者溝通。

4.個人資料保護管理執行作業

依照法務部於民國 100 年 10 月間預告之個資法施行細則修正草案，第 9 條對於母法所指之「適當安全維護措施、安全維護事項或適當之安全措施」進行定義。所謂適當安全維護措施係指以下 11 項內容：

（1）成立管理機關，配置相當資源資源。

（2）界定個人資料之範圍。

（3）個人資料之風險評估及管理機制。

（4）事故之預防、通報及應變機制。

（5）個人資料蒐集、處理及利用之內部管理程序。

（6）資料安全管理及人員管理。

（7）認知宣導及教育訓練。

（8）設備安全管理。

（9）資料安全稽核機制。

本報告之智慧財產權歸屬於法務部

（10）必要之使用紀錄、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。

實際執行操作，請參照本手冊第四章，以下就十一項必要措施，以單獨或整合方式，說明個資擁有者或管理人應如何準備相關管理規範與防護事項：

（1）成立管理機關，配置相當資源

為確保個人資料保護管理有效的執行,須界定機關之個人資料保護管理架構、予以文件化並溝通相關人員的角色、責任與權限，並提供充分的資源以利個人資料保護管理工作之推動。另外，針對可能影響機關個人資料保護管理的執行、人員職掌角色、責任和權限，均應明確化並文件化、充份溝通，以利個人資料保護管理作業執行。

機關首長負有個人資料保護管理之最終責任。首長應指派執行者（專人）負起特定責任，以確認機關適切地實施個人資料保護管理作業，並在機關中所有運作的階層與範圍，皆能執行相關的要求事項。管理階層應提供執行、管制與改善的必要資源。

而個人資料保護管理執行者（專人）應具有界定之角色、權限及責任以進行下列任務：

A. 確認機關個人資料保護管理的各項要求，係根據相關個資法令建立、實施及維持機關所建立之個人資料保護制度。

B. 定期向機關首長報告機關個人資料保護管理的績效以供審查，並作為改進之依據。

面對個資法，為展現機關對個資保護的承諾與決心，首要動作應先成立管理與推動機關，即專人、專責機關負責個資保護相關事宜並由各部門代表參與；再依據機關的需求與特性，規劃後續進行個資管理活動所需之功能性機關架構,及架構中相關人員的角色職責，並明確訂定權責與角色分配，俾能順利推動各項因應個資法之措施，以利溝通協調運作。

本報告之智慧財產權歸屬於法務部

機關內要有高階支持指導承諾之個資管理政策與要點,作為後續執行個資管理活動的最高指導原則,並告訴機關內部要重視且不違反個資法,形成管理政策。機關必須包括高階主管、部門主管及實際承辦人員在內,同時,機關內部須配置適當資源,如教育訓練、時間及預算去實施技術及管理上的相關安全措施。建議管理機關應配合現行機關已運行之管理架構,避免疊床架屋,造成權責不明狀況。舉例來說,機關若已有稽核小組或資安小組,應結合其功能性調整其職掌,以符合資源最佳運用狀態。

(2) 界定個人資料之範圍

機關須界定最主要的個資在什麼部分,將這些個資鑑別出來,納入管理範疇;進一步言,機關須進行法規盤點、作業流程分析及個資盤點,並且必須知道誰使用那些資料並且存放在什麼位置,另外,包括紙本和電子個資皆為須盤點的範圍。

界定個人資料之範圍,須透過分析個人資料生命週期活動之方式,尋找出個人資料之所在。

A. 盤點機關內部業務或服務作業流程,包括所有委外作業是否包括個人資料。

B. 法規盤點,盤點機關所須遵循之個資法相關規範。如有受委託之情形時,必須了解委託機關所應遵循之個資相關法規。

C. 個人檔案基本資訊,包括現行保有部門(含委外機關)、檔案類型(數位或紙本)、保有依據及蒐集目的。

D. 個人資料生命週期活動,包括盤點蒐集方式、蒐集者、蒐集介面、儲存位置(複本、備份/援地點)、檔案或軌跡資料之法定或自訂保存期限、連結或內部傳送對象與方式、刪除或銷毀方式,及國際傳輸對象與方式。

(3) 個人資料之風險評估及管理機制

本報告之智慧財產權歸屬於法務部

即隱私權衝擊分析，簡單而言，即萬一個資外洩或被不法利用，將對機關帶來多大衝擊。例如，是否帶來機關財務、信譽損失或造成當事人尊嚴名譽損害，若有風險便要思考並檢視內部之管理機制。

關於風險評估之相關做法與概念，其方法論建議參考研考會所出版之風險管理及危機處理作業手冊。該手冊針對如何進行風險辨識、風險分析、風險評量、風險處理以及風險之管理監督皆有詳細說明。

一般而言，辨識性強的個資之風險相對較高，如銀行帳號、信用卡號；除此之外，數量龐大的個資風險亦相當高，如資料庫風險通常也比紙本高；此外，醫療、基因、性生活、健康檢查或犯罪前科等，被個資法第 6 條列為特種個資類型之個人資料，其敏感程度高者也屬高風險個資。

所以，機關應針對個人資料進行風險評估，並提供相關管理機制。藉由適當的衝擊評估、分析與風險管理活動，瞭解個資項目或處理大量個資之應用系統，所可能面臨之個資洩露的弱點與威脅，及可能造成機關的衝擊與損失，以便及早採取可行之防範對策或行動方案，避免個資洩露事故之發生。

個人資料管理機制強度與應實施何種風險管理機制，可視機關衝擊分析與風險評鑑結果訂定。舉例而言，機關若擁有大量個資或是持有特種個資者，均應影響管理機制建置之強度與深度。機關可訂定風險評估分析準則，區分不同風險等級。以下提供簡要評估準則：

A. 依個資類別，區分一般個資與特種個資（醫療、基因、性生活、健康檢查及犯罪前科）。

B. 依個資數量，以個資數量若外洩時，對機關影響之大小。

C. 依個資之機密性、完整性及可用性被破壞時，會對機關、資產或人員造成傷害之影響等級。

（4）事故之預防、通報及應變機制

本報告之智慧財產權歸屬於法務部

簡言之，即為個資事故發生後的通報應變流程。可結合現有事件之既有通報及處理程序，整合為機關單一之事件通報處理程序；另外，應考量個資法之要求，定期演練以測試應變機制之有效性;同時亦應確認所有委外作業合約中對於個資事故通報處理之要求，要求內部與外部之事件通報程序之一致性。

關於事故應變機制建議參考研考會所公布之風險管理及危機處理作業手冊，就危機處理部份，公務機關須了解危機之種類，並且擬訂危機處理。

建議可視機關之特性與需要，設計和調整內部預防、通報及應變程序。尤其是通報個資當事人，應於何時通知與何種方式通知，機關應先設計相關程序，以保護機關並避免造成個資當事人更進一步之損害。以下簡述之：

A. 準備階段：預防動作應結合軌跡資料，啟動必要之系統日誌，記錄個人資料存取時之活動，分析可疑事件。

B. 偵測與分析階段：必要證據之保管為現階段最重要之關鍵點，由機關內部或外部專家組成應變及處理團隊，判斷風險發生之來源及可能影響範圍。

C. 減緩與復原階段：避免個資事故擴大，同時確認經個資事故與後續處理程序後，個人資料之完整性。

D. 事後處置階段：持續觀測是否需要進一步鑑識分析，並提出個資事故報告。

通報方式可以採用電子郵件、書函或其他可使當事人知悉的方式，但成本過高或有一定難度者，亦可採用公告、媒體等方式，建議可運用多種方式搭配補強，使當事人瞭解事實及處理狀況，不應隱藏事實或導致當事人進一步的損害。建議機關可提早規畫預防及聲明方式，除了盡通知義務外，最好能加入已採取的因應措施，這才是關鍵。

（5）個人資料蒐集、處理及利用之內部管理程序

本報告之智慧財產權歸屬於法務部

機關內部要有作業辦法或程序書，以建立明確個資蒐集、處理及利用時的具體規定，一般之作法為制定個資保護相關的執行程序與標準作業流程。機關若已建置資訊安全管理系統，則可針對現行資訊安全管理程序及作業進行調整，以符合個資保護作業。另一方面則可從現行管理規範中，檢視是否具備以下管理程序與作業要點。內部管理程序主要包含但不限於以下幾項內容：

A. 規定盤點相關法令、上級機關所訂之法令規範

B. 規定有關盤點個人資料的程序

C. 規定有關個人資料風險評估、分析及風險對策的程序

D. 規定機關各部門及各層級有關保護個人資料的權限及責任

E. 規定對發生緊急情況（個人資料外洩、滅失或毀損）的準備及對應的程序

F. 規定有關蒐集、處理、利用個人資料的程序

G. 規定有關安全、適當管理個人資料的措施及程序

H. 規定有關對應當事人權利行使的程序

I. 有關機關內部人員教育訓練的規定

J. 規定有關個人資料保護制度文件紀錄管理程序

K. 規定有關訂對應處理個人資料申訴及諮詢時的程序

L. 有關機關內部檢查、稽核的規定

M.規定有關管理制度矯正預防措施之程序

N. 規定有關機關代表人持續改善制度之程序

O. 規定有關違反內部規定的罰則

P. 委外監督程序之規定

機關內部管理要點與程序書者主要為個資擁有/管理人，可依循相關程序辦理與適切維護個人資料，日後亦可借助相關程序

本報告之智慧財產權歸屬於法務部

之落實度，驗證機關無故意或過失之責任。

（6）資料安全管理及人員管理

機關內應建立資訊安全制度，並說明對個資應該採取何種資訊科技與系統進行保護、人員存取個資的權限管制等，如設定帳號密碼，定期更換，不可共用、資料備份、使用後登出等基本要求。

人員管理則包括背景查核、教育訓練及監督等措施，若有委外業務，亦必須包括委外人員的管理。由於有些公務機關已於其內部導入資訊安全管理制度（ISMS），因此，此類公務機關可參考本手冊第五章對於 ISMS 與個人資料管理制度結合之建議。

（7）認知宣導及教育訓練

機關對於內部同仁應施行適當的個資宣導與教育訓練，並以內部宣導方式讓員工知道新個資法相關規定，要求員工確實瞭解並遵守個資蒐集、處理及利用時的具體規定。

由於個資擁有者或管理人須具備辦理安全維護事項之能力，因此，除要求個資專責人員資格外，亦應針對專責人員之職務內容，訂定相關教育訓練作業程序，包括資訊安全、隱私保護等課程。同時機關應指派教育訓練專責人員規劃與執行年度個資教育訓練，提升機關不同屬性人員之個資保護專業能力。

（8）設備安全管理

即針對各種保存個資的載具或系統，應定期的維護與更新。包括電腦等個資處理設備，只要含有個資的設備就要考慮安全與否，所有設備須有專人控管，並設有備援機制，更新或維護電腦設備時要有專人在場。除此之外，應確保在設備或媒體報廢時，安全清除或銷毀個人資料。

（9）資料安全稽核機制

本報告之智慧財產權歸屬於法務部

如前所述，個人資料管理制度係基於 PDCA 之方法論而建立。因此，於建立內部管理流程後，機關必須建立檢視機制（check）考核內部制度執行之情況。因此，機關應建立資料安全稽核機制，由機關內部之監督代表或者上級單位進行稽核。稽核之內容包含存放個資的資訊系統、業務流程以及個人資料管理內部程序之執行成效。

（10）必要之使用紀錄、軌跡資料及證據之保存

資訊設備或者紙本資料個資存取控制的紀錄、日誌檔（Log）等，都必須完整保留，這些都可能是未來於訴訟上舉證之相關資料。所以，應針對系統或各種類型的個資（如紙本、電子檔）的使用狀況建立存取紀錄及證據，例如存取個資檔案者之紀錄等。為使機關依規定適當保存相關資料，內部必須建立使用紀錄機制，包含何人、何物、何時、數量多寡、提供何部門做何用途使用等內容，以有利於管理追蹤及未來舉證之用。

（11）個人資料安全維護之整體持續改善

機關應建立 PDCA 機制，訂定個資安全目標或關鍵績效指標（KPI），透過矯正及預防措施，改善任何個資安全管理的異常或弱點。除此之外，針對個資保護不足之處，應持續更新改善。由於個人資料保護管理是一個『持續改善』的反覆過程或循環過程，故機關應順應機關內外部時勢，建置個人資料保護管理之『持續改善』機制，包括計畫、執行、檢視及持續改善等流程。如果機關執行個人資料保護管理作業資源充沛，可包括績效評估與監督，對已建立個人資料保護管理的機關而言，藉由個人資料保護管理目標的規劃與實際結果比較，評估對個人資料保護管理所投入之資源是否充足。

（四）個資保護管理建置流程

建置個資保護管理流程之目的，在於發展一套個資管理制度使公務機關可因應個資法之要求。首先，個資管理制度須符合我國個

本報告之智慧財產權歸屬於法務部

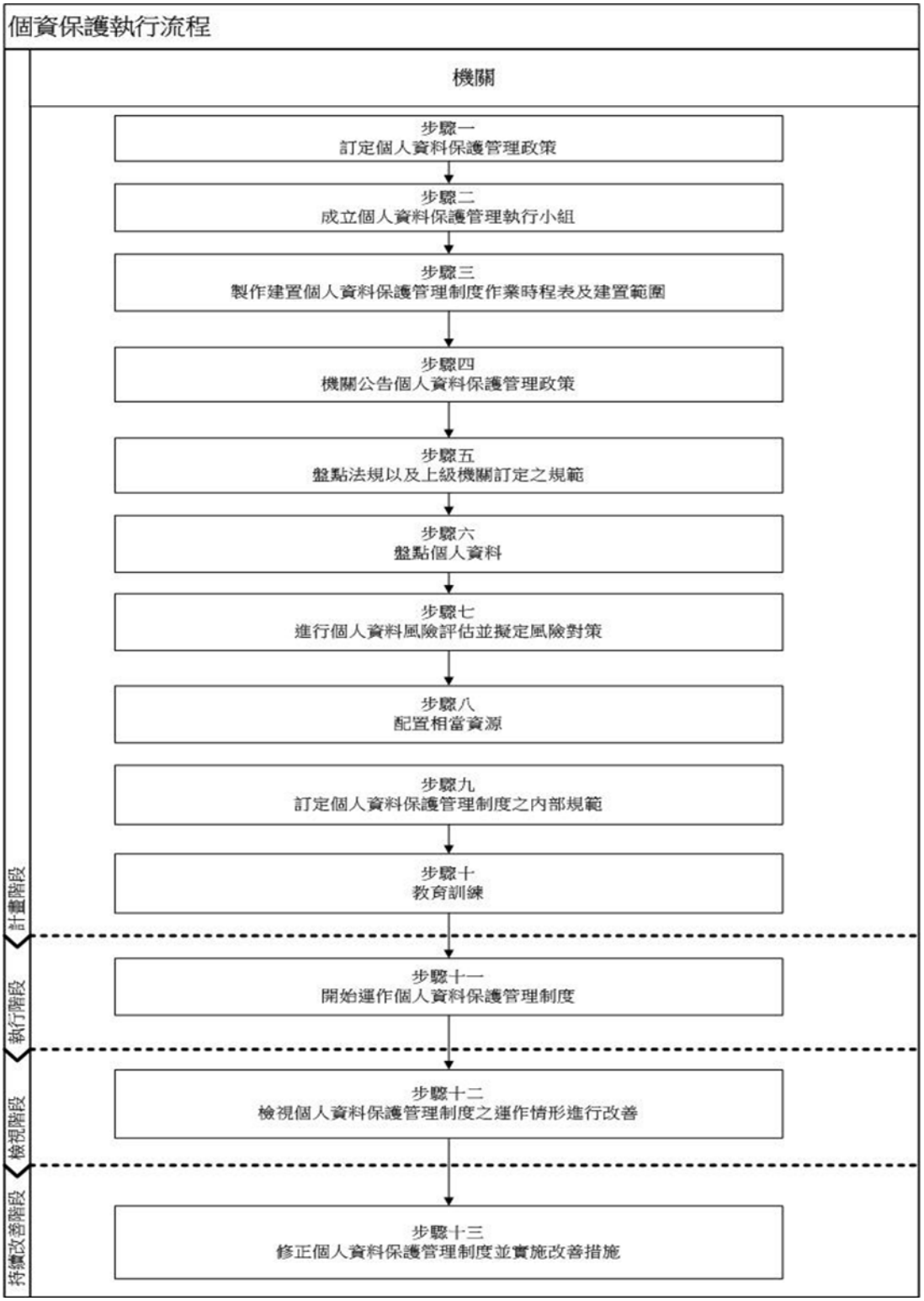
資法與其施行細則之法規命令要求，同時須能夠與國際隱私保護相關發展趨勢、標準等接軌，據此發展相關建置流程，協助政府機關建置個資管理系統並持續提升個資保護管理之成效。

個資保護管理建置流程分為計畫、執行、檢視及持續改善 4 個階段，每個階段皆有不同的任務（Task）需要執行，而過程中可能需要各種不同資訊的提供，再輔以各種執行手法與相關工具，完成該項任務，任務如有產出將可能成為其他任務或活動執行時所需參考之資訊。

另外，研考會亦訂定「個人資料保護參考指引」供政府機關關於執行個人資料保護之程序作業參考指引，該指引亦以 100 年 10 月間預告之個資法施行細則 11 項安全維護措施之角度，提供程序上之作法。以下表一亦表列該指引與本手冊之對照關係，各機關於執行個資保護時，於遵循法規要求之前提下，可相互參照本手冊以及該指引之內容，以建立其內部之個人資料保護與管理程序。

個資保護管理建置流程之各步驟如下頁圖：

本報告之智慧財產權歸屬於法務部



資料來源：本報告自行繪製

圖 30：個資保護管理建置流程圖

本報告之智慧財產權歸屬於法務部

個人資料保護管理流程與 100 年 10 月間預告之個資法施行細則草案第 9 條內容之對應關係表如下：

表 30：個資保護流程與 100 年 10 月間預告之個資法施行細則修正草案對應表

個資保護執行流程	本考核手冊所建議之管理步驟	個人資料保護參考指引	對應100年10月間預告之個資法施行細則修正草案第9條11項安全維護措施之內容
計畫階段（Plan）	步驟一 訂定個人資料保護管理政策	3.1.1 個資管理組織架構 －定義個資管理組織 －建立個資管理政策與要點 －發布個資管理組織架構	成立管理組織
計畫階段（Plan）	步驟二 成立個人資料保護管理執行小組		成立管理組織
計畫階段（Plan）	步驟三 製作建置個人資料保護管理制度作業時程表及建置範圍		成立管理組織
計畫階段（Plan）	步驟四 機關公告個人資料保護管理政策		成立管理組織
計畫階段（Plan）	步驟五 盤點法規以及上級機關訂定之	3.1.2 外部環境分析 －瞭解個資管	界定個人資料範圍

本報告之智慧財產權歸屬於法務部

個資保護執行流程	本考核手冊所建議之管理步驟	個人資料保護參考指引	對應100年10月間預告之個資法施行細則修正草案第9條11項安全維護措施之內容
	規範	理相關法規命令之遵循需求 －瞭解個資管理相關國際標準、原則等之遵循需求	
計畫階段（Plan）	步驟六 盤點個人資料	3.1.4 作業流程分析 －定義和個資相關之流程與應用系統範圍 3.1.6 個資項目盤點	界定個人資料之範圍
計畫階段（Plan）	步驟七 進行個人資料風險評估並擬定風險對策	3.1.7 個資衝擊分析 3.1.8 個資風險評估 3.2.2 建立個資管理程序	個人資料之風險評估及管理機制
計畫階段（Plan）	步驟八 配置相當資源	3.1.9 安全控制措施規劃 －評估所需資源	配置相當資源
計畫階段（Plan）	步驟九 訂定個人資料保	3.1.9 安全控制措施規劃	個人資料蒐集、處理及利用之內部管理程序/

本報告之智慧財產權歸屬於法務部

個資保護執行流程	本考核手冊所建議之管理步驟	個人資料保護參考指引	對應100年10月間預告之個資法施行細則修正草案第9條11項安全維護措施之內容
	護管理制度之內部規範	3.2.1 確立人員權責角色 3.2.2 建立個資管理程序 3.2.3 建立安全控制措施	資料安全管理及人員管理
計畫階段（Plan）	步驟十 教育訓練	3.2.5 宣導與教育訓練	認知宣導及教育訓練
執行階段（Do）	步驟十一 開始運作個人資料保護管理制度	3.2.2 建立個資管理程序	運作 11 項安全維護措施程序
檢視階段（Check）	步驟十二 檢視個資保護管理制度之運作情形進行改善	3.3.2 個資管理稽核活動	檢視前述程序運作情形
持續改善階段（Act）	步驟十三 修正個人資料保護管理制度並實施改善措施	3.4.2 個資管理改善計畫	個人資料安全維護之整體持續改善

資料來源：本報告自行繪製

本報告之智慧財產權歸屬於法務部

1.計劃

（1）步驟一：訂定個人資料保護管理政策

本步驟依據 100 年 10 月間預告之個資法施行細則修正草案第 9 條第 2 項第 1 款「成立管理組織」而來，機關的代表人必須訂定有關個人資料蒐集、處理、利用、刪除等保護政策，作為機關擬定個人資料保護制度的基本方向。個人資料保護政策中必須包含下列內容：

A. 機關推動個人資料保護管理作業之理由

亦即機關對於採取個人資料保護的態度與基本的想法，並且宣示機關將遵守個資法之要求。機關所採取個人資料保護的基本理念主要與機關的行政事項內容會有所關聯，因此政策內必須表明機關之主要職務以及相關工作內容。

B. 機關個人資料保護管理上所必須採取之作法

必須包含下列事項：

a.遵守個人資料保護相關法令、上級機關所訂定的各項法令規範。行政機關所訂定之內部規範若與個資法之要求相衝突時，優先適用個資法及其相關規範。

b.機關將建置個人資料保護管理制度及訂定內部相關規範並定期檢視、持續改善之。另外，機關亦注意將個人資料維持於最新以及正確之狀態。

c.機關將建置安全維護事項避免個人資料遭竊取、毀損、竄改、滅失或洩漏

d.機關將建置因應當事人申訴、諮詢之措施及當事人權利行使程序個人資料保護管理政策中所敘述內容，將具體化於機關之內部管理程序。

- 建議產出項目：個人資料保護管理政策一式。範例可參考附件一之個人資料保護管理政策。

本報告之智慧財產權歸屬於法務部

（2）步驟二：成立個人資料保護管理執行小組

本步驟依據 100 年 10 月間預告之個資法施行細則修正草案第 9 條第 2 項第 1 款「成立管理組織」而來，機關的代表人應透過由各部門主管及業管人員進行任務編組，以成立個人資料保護管理執行小組（以下稱執行小組）。機關代表人應準備個人資料保護管理制度計劃、執行、檢視及持續改善等所需之必要資源。而機關代表人之職責為制定及維護個人資料保護管理政策、準備個人資料保護管理制度執行所需之資源、任命個人資料保護管理執行小組、稽核小組並且須改善修正個人資料保護管理制度。

該執行小組須根據個人資料保護管理政策之內容，建置個人資料保護管理制度，並由機關代表人指定召集人領導執行小組並指示機關所屬各業務單位協助執行小組。

參考法務部所定之個人資料保護管理要點草案，其執行小組置召集人及執行祕書各一人，由部長指定之；委員十一人由各單位指派專人（科長以上）一人擔任。幕僚作業由特定單位辦理，但為強化幕僚功能，得邀請本部各單位人員參與幕僚作業。

- 建議產出項目：個人資料保護組織規定，範例可參考附件二之個人資料保護組織規定。

（3）步驟三:製作建置個人資料保護管理制度作業時程表及建置範圍

本步驟依據 100 年 10 月間預告之個資法施行細則修正草案第 9 條第 2 項第 1 款「成立管理組織」而來。執行小組應於訂定建置作業時程表後，通知相關業務人員並請求協助。建置作業時程表提出時應包含下列步驟四至步驟十三。

劃定建置範圍時，應考慮以下幾點：機關對於管理制度之期望、機關設定之目標以及應遵守之義務、機關可接受之風險、機關應適用之相關法令、利害關係人之利益。

- 建議產出項目：建置個人資料保護管理制度作業時程計畫表一式。範例可參考附件三之個人資料保護管理制度作業計畫表。

（4）步驟四：機關公告個人資料保護管理政策

本報告之智慧財產權歸屬於法務部

本步驟依據 100 年 10 月間預告之個資法施行細則修正草案第 9 條第 2 項第 1 款「成立管理組織」而來。執行小組應將機關代表人所訂定的個人資料保護管理政策，向機關內部全體從業人員公告周知並宣導，使其全體人員知悉遵守。由機關代表人公告周知個人資料保護管理政策之用意在於，除了可以提升全體人員理解對個人資料保護管理政策重要性，亦可增進各部門主管、業務管理人員與執行小組合作上的認識。

此外，為了要使一般民眾都可以容易取得機關之個人資料保護管理政策文件，採取如登載於機關的網頁與印刷於手冊或廣宣品的方法，及在機關內部宣導使機關全體人員徹底明瞭。

步驟四所稱在機關內之全體人員，指的是在機關裏直接或間接受到機關的指揮監督，及從事業務之人員，包括但不限於正職、約聘人員及其他機關之派遣人員等。

（5）步驟五：盤點法令以及上級機關訂定之規範

本步驟依據 100 年 10 月間預告之個資法施行細則修正草案第 9 條第 2 項第 1 款「成立管理組織」而來。機關須先確認本身有無關於蒐集、處理、利用個人資料相關之法令與上級機關所訂定之相關法令規範。

若機關在蒐集、處理個人資料方面，已有相關法令及上級機關所訂定之法規時，必須優先考慮適用該法規範。

舉例而言，若機關依法規命令蒐集當事人之個人資料時，依個資法第 8 條第 2 項之規定得免告知義務。據此，盤點法規命令除了檢視機關是否合理適法利用個資外，也可減免機關對於法規遵循之負擔。

- 建議產出項目：法規盤點清冊一式、法規盤點程序文件一式。法規盤點程序可參考附件四之法規盤點程序。

（6）步驟六：盤點個人資料

本步驟依據 100 年 10 月間預告之個資法施行細則修正草案第 9 條第 2 項第 1 款「界定個人資料之範圍」而來。各部門主管

本報告之智慧財產權歸屬於法務部

與業務負責人員應協助執行小組盤點機關內部所蒐集、處理及利用之個人資料。盤點個人資料之範圍為機關執行職務所利用之個人資料。

盤點個人資料之目標在於明確並毫無疏漏地找出機關所要保護之個人資料。盤點個人資料之方法，主要有（a）業務流程圖法：亦即從業務流程尋找出個人資料；(b）表單盤點法：亦即從保存的申請表單、儲存的資料，尋找出個人資料，機關可自行調整之。

盤點個人資料時，須建立盤點清冊。盤點清冊建議至少包括下列項目：流水編號、個人資料檔案名稱、作業流名稱、特定目的、個人資料項目（姓名、地址等）、個人資料類別、個人資料件數、紀錄之媒體型態（紙本或電子檔）、蒐集方法（直接蒐集或者間接蒐集）、處理部門主管及承辦人職級、有無告知當事人、有無提供第三人（或機關）、有無委託情形、儲存期間與儲存場所、刪除及銷毀之方法等項目。於編纂個人資料盤點清冊後，即可執行步驟七的個人資料風險評估，因此，做法上有利於檢討分析風險對策。

**注意要點：個人資料保護管理制度是以風險管理為核心。因此，盤點之首先要務為找出風險管理的對象。
**注意要點：初次進行時，主要有兩種情形「機關依職務提供行政事項業務時所處理的個人資料」、「人事管理時所處理的個人資料」，盤點後將出現「運用個人資料保護管理制度時所處理的個人資料」情形。

- 建議產出項目：特定業務之個人資料作業流程圖一式、個人資料盤點清冊一式、個人資料盤點程序規範一式。個人資料盤點程序可參考附件一之個人資料保護管理政策。

（7）步驟七：進行個人資料風險評估並擬定風險對策

本步驟依據 100 年 10 月間預告之個資法施行細則修正草案第 9 條第二項第三款「個人資料風險評估及管理機制」而來。

於完成步驟六盤點個人資料之作業後，執行小組已可掌握業務內容以及與業務內容有關之個人資料處理流程，並明確列出個

本報告之智慧財產權歸屬於法務部

人資料從進入機關內部起到離開為止的循環週期，亦即所謂個人資料的生命週期，依其循環週期的各個情境（例如：蒐集、輸入、編輯/更正、儲存、複製、內部傳送、連結、利用、輸出、刪除）尋找出可能產生之各種風險。

可能產生之風險之類型至少應包含下列項目：被竊取、竄改、毀損、滅失、洩漏、違反相關法令、上級機關所訂定之規範等。針對風險之類型，可參考研考會於 98 年 1 月所發佈之風險管理及危機處理作業手冊。

風險不一定是正在發生或過往已發生的，對於預測可能發生之風險也必須加以評估。風險之高低由執行小組判斷，須注意的是，若執行小組僅記載「有洩漏或遺失的風險」，係不夠具體的，而且並不足以作為檢討風險對策的對象。建議記載時，必須將風險發生之原因一併寫明，以便於日後尋找出風險對策訂定之方向。

另外，只從如何保護機關內部的資訊資產的觀點來評估風險、分析及建立風險對策係不夠充份的。機關於蒐集、處理、利用個人資料之各種情境下，主要產生蒐集當事人個人資料欠缺特定目的、特定情形、未對當事人履行告知義務或者告知事項不充分之情形，除此之外，機關內若未建置當事人權利行使機制，亦屬於風險之一，這些都是單從保護資訊資產的觀點出發所認識不到的風險。同時，保護個人資料，不僅是單純做到「保護」而已，還必須適當地處理個人資料，這些也不是為維護資訊資產完整性、可用性、機密性所能達成的。

關於已尋找出來並已認識的風險，則必須分析並評估風險的根本原因、發生的可能性以及發生後的影響，以設定風險等級。針對風險發生的結果及等級研擬合理的風險對策。所謂的「合理的風險對策」，就是能明確辨識、分析、評估處理個人資料時的風險，並針對該風險採取各種可能預防措施。機關於思考預防措施時，須考量機關預算及須耗費之成本，機關必須確認其所研擬之風險政策係可執行的。例如機關想引進可以把所有資料自動加密的資訊系統，但是因機關本身預算不足，目前只能由每個業管人員自行加密，此也為有效之風險政策之做法。

本報告之智慧財產權歸屬於法務部

必須建立風險評估暨管理機制清冊以管理風險評估之結果與風險對策，從個資生命週期之觀點建立風險與風險對策的關連性。由於風險之變動性，因此執行小組必須定期且依其需要隨時進行修正。據此，如果不把風險與風險對策的關連性明確記載在清冊中，機關就無法隨著與外在、內在環境變化修正各個行政事項業務內容。

再者，就算對所有認識到的風險都採取了風險對策也不表示所有風險就不會發生，有的風險的發生並不是機關所能掌控，例如地震、海嘯等自然災害的發生，或是目前的對策並不能完全消弭風險的發生，例如就算進行徹底的人員教育訓練仍不免發生人員因疏失而致外洩的情形。因此對現狀盡最大可能的提出風險對策後，若仍有未對應部分，須掌控並管理「剩餘風險」。

執行小組把提出的風險對策反映在機關內部的相關規定（例如出勤管理規定或資訊系統管理規定等安全管理措施規定、業務作業程序書等）中，並將相關規定記載於風險評估暨管理機制清冊中與風險作連結，便於相關人員能夠隨時查閱。

落實步驟七將所建立的風險對策歸納並落實於內部管理規範後，即完成機關內部有關安全管理措施的程序。

對於風險評估以及建立風險對策之方法可參考研考會 98 年 1 月所出版之風險管理及危機處理作業手冊。

***注意要點：步驟五至七是個人資料保護管理制度的基礎。因此，於建置管理制度過程中必須落實以下步驟並且確實執行。

- 建議產出項目：風險評估暨管理機制清冊一式、風險評估程序一式。風險評估程序之範例可參考附件六之風險評估程序。

（8）步驟八：配置相當資源

本步驟依據 100 年 10 月間預告之個資法施行細則修正草案第 9 條第 2 項第 1 款「配置相當資源」而來。進行步驟七風險評估程序時，執行小組即須判斷建置個人資料保護管理制度所必須之經營資源（人力、物力、金錢、資訊）。根據機關所掌握之資源，機關計畫建置各部門及各階層個人資料保護管理機制，並向

本報告之智慧財產權歸屬於法務部

機關代表人提案。另外，在確保資源的階段，會發生修正計畫的情形，這也是對於風險對策的一種反饋。機關代表人根據機制建置計畫，分配資源並調整人事等。

何謂相當資源？舉例而言，可視機關對於資訊安全事項所編列之預算以及資安人員與業務人員之比例而定。

（9）步驟九：訂定個人資料保護管理制度之內部規範

本步驟依據 100 年 10 月間預告之個資法施行細則修正草案第 9 條第 2 項第 5 款「個人資料蒐集、處理及利用之內部管理程序」而來。本步驟作業的目的是將步驟一到步驟八的程序中經過決定執行的事項歸納成為內部規範。個人資料保護管理制度是機關按自身情形所建立的管理制度，因此必須確保與機關種類、規模與其他現存的管理制度間之整合性，使之具備實效性並且貼合機關需要。訂定內部規定時，只要機構容易操作即可，不求訂定出繁複之程序。

在執行實施個人資料保護管理制度時，最少要有下列內部規定才足以落實。為了讓機關全體人員遵守內部規定進而實現個人資料保護，內部規定必須詳細地訂出具體執行的程序、方法等，如：

A. 規定盤點相關法令、上級機關所訂之法令規範

B. 規定有關盤點個人資料的程序

C. 規定有關個人資料風險評估、分析及風險對策的程序

D. 規定機關各部門及各層級有關保護個人資料的權限及責任

E. 規定對發生緊急情況（個人資料外洩、滅失或毀損）的準備及對應的程序

F. 規定有關蒐集、處理、利用個人資料的程序

G. 規定有關安全、適當管理個人資料的措施及程序

H. 規定有關對應當事人權利行使的程序

I. 有關機關內部人員教育訓練的規定

J. 規定有關個人資料保護制度文件紀錄管理程序

本報告之智慧財產權歸屬於法務部

K. 規定有關訂對應處理個人資料申訴及諮詢時的程序

L. 有關機關內部檢查、稽核的規定

M.規定有關管理制度矯正預防措施之程序

N. 規定有關機關代表人持續改善制度之程序

O. 規定有關違反內部規定的罰則

P. 委外監督程序之規定

執行小組制定規範時，就內部規範應包含各機關內各部門共同適用之部分，另外，針對機關內各部門之業務，依業務屬性可再制定詳細之處理程序。

訂定內部規定時，必須經由機關內部中具決定權人也就是機關代表人之核決與承認。內部程序包含以下內容：

A. 規定盤點相關法令、上級機關所訂之法令規範

盤點與機關本身規範時，不僅是訂定內部規則時須盤點，若相關法令有修改或者更新之情形，亦必須與時俱進加以修改機關之內部規則。

盤點法規命令程序的目的在於，個人資料法令、上級機關訂定的指引及其他規範若有增修改訂、廢止之情形時，必須反映在個人資料保護管理制度中。

- 建議產出項目：如步驟五。

B. 規定有關盤點個人資料的程序

盤點個人資料的詳細程序之執行作法請參考步驟六的執行程序，同時也必須規定程序，使得在盤點新蒐集的個人資料時沒有疏漏。另外，必須建立程序使得執掌個人資料保護管理的專人定期或不定期檢察個人資料範圍之最新狀況。

- 建議產出項目：如步驟六。

C. 規定有關個人資料風險評估、分析及風險對策的程序

將步驟七實執行的程序文件化足以完成風險評估、分析及

本報告之智慧財產權歸屬於法務部

風險對策的程序。訂定有關個人資料風險評估、分析及風險對策的程序內部規定時，應注意風險是依照環境的變化與技術的發展而經常變動，因此必須在程序中規定須定期或必要時應隨時修訂的程序，並將程序文件化。另外由於某個部門已經實際發生的風險，未來也可能會出現在其他部門單位，因此，必須實施全體機關的風險評估、分析及風險對策修訂程序。

- 建議產出項目：如步驟七。

D. 規定機關各部門及各層級有關保護個人資料的權限及責任

細則規定中必須明確規定在機關內部個人資料保護專人、機關各個部門層級負責處理個人資料的部門管理專人、權限及責任。如果機關在全國各地設有分支機關、辦公室時，也必須按層級訂定相同之內部規定。

- 建議產出項目：如步驟二。

E. 規定對發生緊急情況（個人資料遭竊取、洩漏或遭竄改等情形）的準備及對應的程序

為防止緊急情況，必須訂定機關緊急應變的程序，將機關內部的連絡程序、緊急情況時的清查程序、掌握受害程度與影響層面、防止受害擴大的程序等必要事項予以文件化。在何種情形將可能發生緊急狀況，只要落實執行步驟七風險評估、分析及風險對策程序，就可以明確了解緊急情況的發生原因。

另外為了將緊急情況發生而產生之損害控制在最低程度，必須訂定緊急應變程序。緊急應變程序規定之內容包含緊急狀況發生時，對當事人（民眾）、對上級機關以及對媒體等的應對等。

- 建議產出項目：緊急應變程序。緊急應變程序範例可參看附件七緊急應變程序。

F. 規定有關蒐集、處理、利用個人資料的程序

規定相關部門對於蒐集、處理及利用個人資料之細部程序。

本報告之智慧財產權歸屬於法務部

有關蒐集個人資料的作法應詳細規定，將蒐集方法區分為直接蒐集與間接蒐集的情形，直接向當事人蒐集個人資料時，機關須明確告知個資法所要求之相關資訊。而若是為間接蒐集當事人個人資料的情形，必須將個資法所要求之告知事項明確告知被蒐集個人資料之當事人。

- 建議產出項目：個人資料作業管理規定一式、個人資料作業申請書一式、利用、提供個人資料申請書。個人資料作業管理規定之範本可參考附件八之個人資料作業管理規定。

G. 規定有關安全、適當管理個人資料的措施及程序

有關適切、安全地管理個人資料的內部規定之內容，也包含確保有關正確性與安全性的規定。

有關確保正確性的內部規定中，必須規定利用資料處理系統、更新程序、確認處理結果，防止因負責處理個人資料業管人員的過失所致錯誤之程序等規定。

有關確保安全性的規定中，需規定有關合理性安全對策。關於安全措施的內容等，首先應先就個人資料處理流程相關人員權限設定權限管理，以確保個人資料僅在必要之人員範圍內進行處理，針對個人資料處理權限管制，參照行政院研究發展考核委員會「個人資料保護參考指引」之「個資項目與個資管理角色對應表」，填具各個相關人員及廠商權限劃分即可；另外針對物理、技術之安全管理措施，只要把步驟七風險評估、檢討分析風險對策中所採取的風險對策直接文件化應該就足夠。一般而言，參照「行政院及所屬各機關資訊安全管理規範」（行政院研究發展考核委員會八十八年十一月十六日八八會訊字第○五七八七號函）相關的資訊安全措施，按機關的業務內容與規模的合理性安全對策將之規範化之外，還包含下列規定：

a.規定進出辦公室的管理、防止個人資料失竊等的措施

b.規定控管有關個人資料及處理個人資料資訊系統存取、違法軟體之規定，以及監視資訊系統等措施

本報告之智慧財產權歸屬於法務部

c.規定有關個人資料儲存、保管、廢棄、備份等個人資料管理規定

d.規定有關委託處理個人資料之受委託方選擇標準以及契約條款之要求等相關監督個人資料處理受委託方的規定

建議產出項目：個人資料維護程序一式、安全管理措施一式、委外管理程序一式、委外作業選擇廠商標準一式、委外廠商一覽表、委外廠商個人資料保護檢查報告書一式。個人資料維護程序可參考附件九之委外管理規定；另外，表單五以及表單六提供委外廠商選擇評鑑表以及委外廠商管理一覽表之範例供參考。

H. 規定有關對應當事人權利行使的程序

由於個資法賦予個資當事人請求更正、複製或閱覽等相關權利，因此機關必須建立相關程序以妥善處理當事人行使權利之程序。

另外，對應當事人權利行使時，同時也有發生偽裝詐欺成當事人行使權利導致當事人個人資料外洩的危險，必須切記妥善實施確認當事人的程序。

- 建議產出項目：當事人權利行使規定一式、當事人權利行使申請書一式。當事人權利行使規定可參考附件十之當事人權利行使程序，另外，關於當事人權利行使申請書以及當事人權利行使紀錄表可參考表單七、八。

I. 有關機關內部人員教育訓練的規定

機關不只是要將個人資料保護管理制度相關事項廣為宣導、徹底實施教育訓練外，還必須讓業管人員學習如何適當地去運用個人資料保護管理制度的能力。有關人員教育訓練中應規定的內容有下列事項：

a.目的

b.時期、期間、對象（包含全體人員）

本報告之智慧財產權歸屬於法務部

c.內容、方法、場所

d.機關（負責主管）

e.通知程序

f.管理受教育訓練講習人員的方法（確認人員出缺席與對缺席者實施補課）

g.確認教育訓練效果的方法

h.實施教育訓練紀錄的內容、保管方法等

- 建議產出項目：個人資料保護教育訓練規定一式、全年個人資料保護教育訓練計畫書一式、各部門個人資料保護教育訓練計畫、執行教育訓練紀錄一式。個人資料保護教育訓練規定可參考附件十一教育訓練計畫之範例，另外，個人資料保護教育訓練計畫書可參考表單十四之範例。

J. 規定有關個人資料保護制度文件紀錄管理程序

機關必須訂定妥善管理規範個人資料保護管理制度文件、以及因運作個人資料保護管理制度作所產生的紀錄類資料之程序。至少必須將個人資料保護管理政策、內部規定、計畫書及紀錄等作為構成個人資料保護管理制度的文件加以管理。一旦開始運作個人資料保護管理制度之後，就必須在各種時間點落實執行紀錄。落實執行紀錄的另一個意義就是確保日後可供稽核之證據。有關於文件紀錄管理的程序，機關內部若已有類似的文件紀錄管理規定的話，準用該規定即可。

- 建議產出項目：文件紀錄管理規定一式、文件紀錄一覽表一式。文件紀錄管理規定可參考附件十二之範例；文件紀錄一覽表之格式可參考表單一、二、三之範例。

K. 規定有關對應處理個人資料申訴程序

機關對於當事人提出有關個人資料的申訴及諮詢應迅速回應。與當事人權利行使的回應相同，不適當及不確實的處理

本報告之智慧財產權歸屬於法務部

方式將是使原來單純的申訴變得更難處理。因此，必須妥善建立處理個人資料申訴之案件。

另外，當事人的申訴反應有時也會使機關再度檢視其內部個人資料保護管理制度之漏洞，就算不至成為不符合的情形，也會是在修正個人資料保護管理制度時的寶貴意見。因此，按照當事人申訴之重要程度，在內部規定中有必要訂定向機關代表人報告之程序及要件。

- 建議產出項目：申訴程序一式、申訴紀錄表一式。申訴程序可參考附件十三之程序範例；

L. 有關機關內部檢查、稽核的規定

機關除了建立內部之個人資料管理制度外，也必須建立其內部之稽核制度，亦即建構考核制度，透過考核制度，機關才能了解機關成員之實際表現與法規遵循落實之程度。

關於內部考核之細部作法，請參見本手冊陸、考核監督作業部份。另外，機關內部自評時，評估之細項請參考表單十八之個資管理整體自評分析細項表。

- 建議產出項目：例行檢查、稽核程序一式、例行檢查表一式、全年稽核計畫書一式、各部門稽核計畫及稽核查檢表一式、稽核報告書一式。稽核程序可參考附件十四之稽核程序規定範例；全年內部稽核計畫書、個別部門內部稽核計畫、個別部門內部稽核糾正事項確認表之範例可參考表單九、十以及十一。

M.規定有關管理制度矯正預防措施之程序

不符合事項是指透過外部驗認證機構的糾正、緊急狀況的發生、例行檢查及稽核的結果、外部的申訴等所發現的應修正事項。對於不符合事項，必須在內部規定中訂定矯正措施以及預防措施的程序。矯正措施是對於已發生的不符合之處進行修正，預防措施則是從已發生不符合事項的經驗記取教訓，確認是否類似不符合現象也發生在其他部門之可能性，應採取事前預防性措施。矯正措施與預防措施是為防止不符合事項再度發

本報告之智慧財產權歸屬於法務部

生，必須訂定包含下述各項程序：

a.確認不符合事項的內容

b.清查不符合事項的原因，建立矯正處置及預防措施

c.定出期限實施所建置的處置與措施

d.紀錄所實施的矯正處置及預防措施的結果

e.重複檢查所實施的矯正處置及預防措施的有效性

- 建議產出項目：矯正預防措施程序一式、矯正預防措施報告書一式。針對矯正預防程序，可參考附件十五之範例;而矯正預防措施報告書之範例可參考表單十六。

N. 規定有關機關代表人持續改善制度之程序

只改善不符合事項之處並不能算是經過機關代表人之持續改善制度。為使個人資料保護管理制度成為更好的管理制度,按情形必須將現行的個人資料保護管理制度架構做根本之修正改善。因此為修正改善個人資料保護管理制度，必須在內部規定訂出程序。

如有修正個人資料保護管理制度時，應斟酌下列事項：

a.有關稽核報告及個人資料保護管理制度運作情況的例行檢查報告

b.包含申訴等外部意見

c.對前次矯正預防及修正結果的後續追蹤

d.個人資料保護等相關法令、上級機關所訂定之指引及其他規範的增刪修訂情形

e.社會情勢的變化、民眾認知的變化、技術進步等各種環境變化

f.機關行政事項領域的變化

g.為改善個人資料保護管理制度由機關內、外部所蒐集之提案

本報告之智慧財產權歸屬於法務部

- 建議產出項目：機關之持續改善程序，機關持續改善程序之範例可參考附件十六之持續改善規定。

O. 規定有關違反內部規定的罰則

規定違反個人資料保護管理制度內部規定時的措施就是在機關內部人員服務規定中訂定相關獎懲規定。實際的罰則規定可適用服務規則中既有之規範，但必須在本規定中明確表示所適用之所有規定。

- 建議產出項目：個人資料保護管理制度獎懲規定一式。

P. 委外監督之規定

委外監督係依據個資法有關委外管理之相關規定，有（1）個資法第 4 條中，法律明定將受託機關於受託蒐集、處理及利用個人資料時，視同於委託機關。（2）100 年 10 月間預告之個資法施行細則修正草案第 8 條，明確委託人對於受託人「適當監督」之義務。（3）100 年 10 月間預告之個資法施行細則修正草案第 7 條，規定關於受託機關應遵循之個資法規，依委託機關應適用之規範為之。

為此，公務機關於有關個人資料業務有一部或全部委外時，應根據個資法相關規定對受委託機關執行相關管理措施。其相關管理措施又可區分為委託業務前的事前評鑑及委託業務後之事後監督考核。就事前評鑑作業而言，公務機關應訂定一套個人資料委外作業評鑑標準，並依該標準製作委外評鑑表，於個人資料委外作業委託前，對可能受委託之機關、法人、廠商或個人進行個人資料委外評鑑；對於個人資料保護管理未達委外評鑑標準的機關、法人、廠商或個人即應排除於受託委外作業之對象範圍。

對於已達委外評鑑標準的機關、法人、廠商或個人簽訂委外作業契約時，其契約條款內應針對個人資料保護管理事項，如委託機關與委外單位間之責任劃分、個人資料安全管理、複委託、對委託機關進行個人資料委外作業情況報告之內容與次

本報告之智慧財產權歸屬於法務部

數、違反個人資料保護條款契約責任及發生個人資料事故時應通報委託機關等進行規範。

委託機關並應依本手冊陸之二委外作業考核監督進行事後監督考核，以維持委外作業之受委託機關、法人、廠商或個人能維持一定之個人資料保護管理水準，相關程序內容可參考本手冊陸、考核監督作業章節對於委外作業監督考核機制之說明。

- 建議產出項目：表單五委外廠商評鑑表、表單六委外廠商一覽表

Q. 步驟十：實施個人資料保護管理制度教育訓練

機關應由教育訓練小組實施依部門或者職掌為區分進行教育訓練。教育訓練小組根據教育訓練計畫，於得到執行小組的協助後，實施教育訓練後，必須再度確認教育訓練效果，確認教育訓練效果之方法包含以考試或者撰寫心得報告之方式檢驗效果，同時，也應留下教育訓練之紀錄，供日後參考並符合個資法規之要求。

- 建議產出項目：個別部門教育訓練計畫、執行紀錄，其範例可參考表單十五。

2.執行

步驟十一：開始運作個人資料保護管理制度

機關依前述步驟建立計畫，規定執行程序，配置相當資源，規定各部門各層級負責人的責任、權限，並依其責任、權限及訓練，經機關代表人核可後，開始運作個人資料保護管理制度。

運作制度時，執行小組須持續維運該制度，包含進行有效性量測、確認目標達成度以及緊急應變措施之演練等作為。執行小組須注意，執行時即須注意個人資料保護管理制度運作之情形。

3.檢視

步驟十二：檢視個人資料保護管理制度之運作情形進行改善

本報告之智慧財產權歸屬於法務部

稽核小組，在個人資料保護管理制度開始運作後經過一定期間後，必須檢查個人資料保護制度運作狀況並給予適當的評價。稽核的目的是為了確認在管理制度運作後，管理制度架構是否能有效地運作以及確認是否落實考核手冊所訂定之事項。稽核小組必須將評價的結果總結成稽核報告書，並向機關代表人報告。

執行小組必須在機關代表人收到稽核報告後做出修正的指示時，按機關代表人之指示，進行改善個人資料保護管理制度。在進行必要的改善措施後，執行小組也要修改個人資料保護管理制度文件，以反映改善之內容。除此之外，執行小組須紀錄改善的內容、改善日期，並登載於改善紀錄中。

稽核之重點在於機關對於所設定之目標完成度，亦即是否落實機關所定之個人資料保護政策。

稽核自評之內容可見表單十八。

4.持續改善

步驟十三：實施修正個人資料保護管理制度

本步驟依據100年10月間預告之個資法施行細則修正草案第9條第二項第十一款「個人資料安全維護之整體持續改善」而來。經過機關代表人修正規定所訂程序，檢討現行個人資料保護管理制度是否適當，並依必要實施改善措施。於持續改善階段必須注意法規修正情形以及根據檢視後之評估情形調整個人資料保護管理制度之相關措施及作法。另外，針對個人資料保護管理制度持續改善之作法必須注意矯正預防措施之實施。舉例而言，執行效果好之部份須水平擴散，然而執行效果須改善並且修正之部份必須進行矯正預防措施，進行矯正預防措施時必須注意採取替代方案以確保個人資料保護管理制度之有效運行。

（五）資訊安全管理制度（ISMS）與個人資料管理制度作業

由於政府推行資訊安全管理系統之政策已行之有年，很多機關皆已建立資訊安全管理系統（以下簡稱ISMS）並取得ISO/IEC 27001驗證，而ISMS是推動個人資料管理保護工作的良好基礎，將個資保護融入現行資訊安全管理系統（ISMS）中，不僅避免管理制度上的

本報告之智慧財產權歸屬於法務部

多頭馬車，還能藉由 PDCA 循環強化個資保護工作。若是尚未導入資訊安全管理系統之機關，也可以參考本手冊，規劃建立具有架構的個人資訊管理制度。除了本手冊外，研考會所公布之「個人資料保護參考指引」之 3.5 部分亦說明資訊安全管理制度(ISMS)與個人資料保護管理制度之相互整合作法，已導入資訊安全管理系統 ISMS 之各機關可參考之。

以個資法的角度來看，個人資料的防護係從開始蒐集個資即納入法律規範，而 ISMS 則是控管機關所保有之資訊的處理與利用作業。個資與資訊安全管理之整合上，首先可將涵蓋機關內相關的個資流程納入現行 ISMS 實作的範圍中，整合過程包括有：建立、執行個資盤點與風險評鑑作業；ISMS 之安全控制措施（著重資料的「處理」之資訊安全層面）中，增加個人資料「蒐集」、「利用」活動的管控；並在現行 ISMS 管理流程中，強化對於個資事故處理與回應的完整性等。

從實作面的角度來看，以資料、資產盤點為例，不同於 ISMS 是由資訊部門主導，個資盤點需由各權責部門執行才能夠完善，同樣地，個資風險回應計畫與補救措施也應由各權責部門來提出。換言之，資訊部門提供個資防護技術面的作法，管理面則需透過各部門的參與(例如建立整合各部門之個資防護管理機關)，如此資訊安全管理制度（ISMS）與個人資料管理制度才能提供有效作業且合理之控制措施，並能貫徹持續改進之精神。

環顧過去因應政策要求而導入 ISO 27001:2005 資訊安全管理系統 （ISMS） 的機構，如今應該在既有 ISMS 架構上，檢視個人資料管控深度並予以強化，進而設計一套兼顧資安管理制度與法令遵循之控管措施。因此在相關施行細則尚未正式公告前，機關能預先準備的，即是重新檢視作業程序，找到其中之差異點，並審視個資管理與 ISMS 中之各項程序，是否有需修正之處或保留下來。

個資法會針對個資蒐集前，進行告知、特定目的及書面同意進行規範，而 ISMS 就不會涵蓋這些重點。但是 ISMS 所強調的安全防護控制措施，剛好可以提供有關個資在處理及利用階段所需之資訊安全防護。

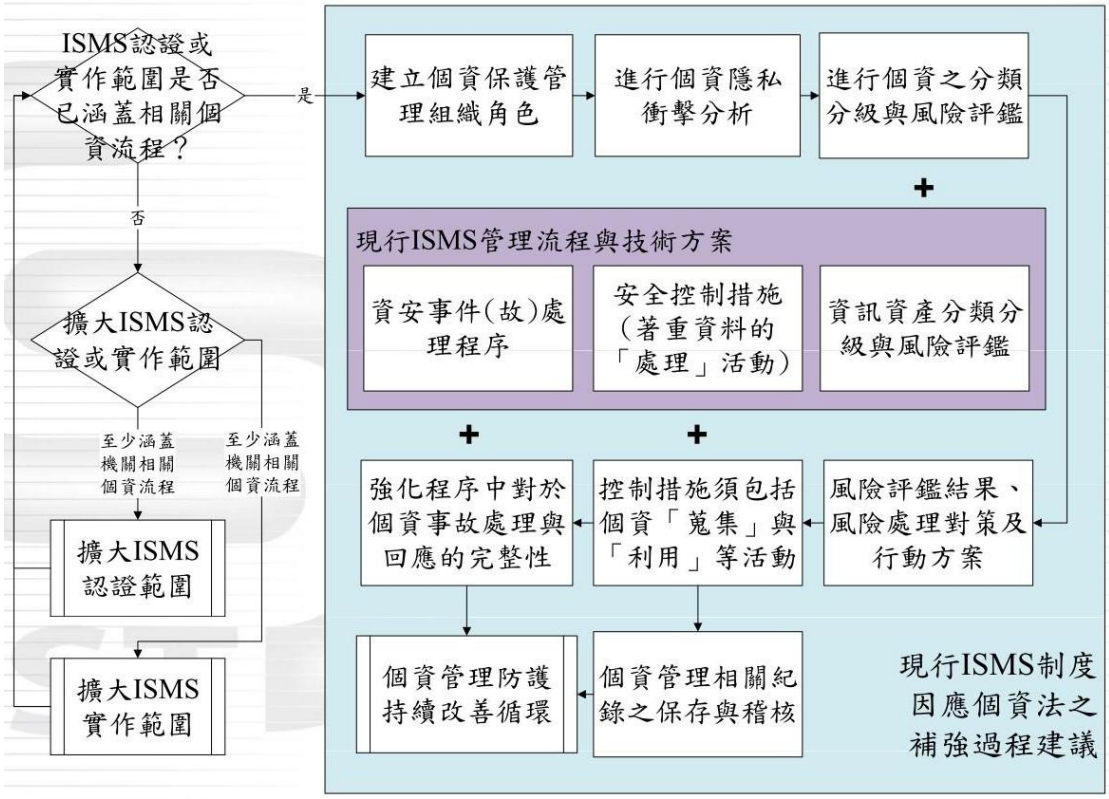
因此，已實施或已通過 ISO/IEC 27001 驗證的機關而言，依照

本報告之智慧財產權歸屬於法務部

ISO/IEC 27001 標準所要求的 11 項領域、133 項控制措施，進行個人資料的安全評估，並藉由強化既有資訊安全管理制度基礎，來達到制度整合且發揮管理綜效，讓各部門都能依循著相同作業流程，是必須思索考量的重要課題。

而將個資保護整併至 ISMS 的第一步，就是檢視現行 ISMS 認證或實作範圍，確認其是否涵蓋機關內的個資相關流程。目前 ISMS 導入範圍多以資訊部門為主，但個資相關的作業或流程與很多部門有關，像是業務單位、人事單位及總務會計等單位，因此，整併第一步就是進行業務流程普查，將握有個資的部門或相關作業流程納入 ISMS 範圍內。

而機關進行個資管理與資訊安全管理系統之整合建議流程，詳見下圖。



資料來源： 行政院研究發展考核委員會之「個人資料保護參考指引」

圖 31：個資管理與資訊安全管理系統之整合建議

個資法與 ISO/IEC 27001 標準有以下幾個共同之重點，值得考量如何進行整併或解決衝突。

本報告之智慧財產權歸屬於法務部

1.資產（個資）盤點之實作

ISMS 的經驗告訴我們，要做到安全，一定要先知道機關內保有哪些需要保護、值得保護的資產，對應到個資的保護，當然首要的就是找出機關內究竟有那些個人資料存在於那些部門、系統主機、個人電腦，甚至是文件檔案。亦即如何確認與盤點所有機關內之個人資料。基於個資法的要求，機關應採行個人資料的辨識，例如在資料庫、訓練紀錄、業務持續計畫、合約及檔案室中，個人資料都極可能包括在內，而如何符合 ISO 27001 與個資法的第一步，皆是從資產（個資）盤點及資產清冊開始。相較來說，個資法的目標明確，是針對資產清冊內之個人資料進行規範動作；即如何確認與盤點所有機關內之個人資料。基於個資法的要求，機關應採行個人資料的辨識，例如在資料庫、訓練紀錄、業務持續計畫、合約及檔案室中，個人資料都極可能包括在內。而如何符合 ISO 27001 與個資法的第一步，皆是從資產（個資）盤點及資產清冊開始。相較來說，個資法的目標明確，是針對資產清冊內之個人資料進行規範動作。

而機關資產（個資）盤點一般會先找出涉及之作業流程或服務，再進一步分析資產細節，也就是利用 4W1H 分析：What（資產盤點）、Where（來源）、Why（目的）、Who（利害關係人）、How（流程），藉此找出資產(個資)項目。相較來說，個資法的目標明確，是針對資產清冊內之個人資料進行規範動作而 ISMS 偏重個資的處理，較不重視資料從何而來或流向何處以及行為規範動作。

2.個資保護管理負責人指派

如何在資料的合理利用及當事人人格權不受侵害間取得平衡，在個資法通過後，組織必須指派具有相當決策層級之人員擔任全組織之個資保護管理負責，對組織個資運用擔負最高決策責任。例如，對於特種個資的運用，原則上是不可以蒐集、處理及利用。但在符合但書情形之下，例外地可以蒐集、處理、利用。此時，在管理制度之下，該蒐集、處理、利用之行為必須經由個資保護管理負責人授權同意，而未來若發生爭議時，該負責人必須對個資之使用負起全部之管理責任。

3.儲存、備份及存取管理

本報告之智慧財產權歸屬於法務部

即如何確保資料的生命週期已妥善定義與管理，以及資料之存取管理如何加強。

資訊備份：資訊應保留多久才是最佳時機呢？對資訊擁有者或管理者而言，若沒有規範應該留存多久，就等同「永久保留」之意。個資法通過之後，機關除考量資訊備份之機制安全外，亦應加入留存期間之規範，避免個人資料洩漏之風險。

資訊處置程序：考量部分資訊之「遮蔽機制」，不全然揭露所有資訊。例如：身分證字號，遮蔽幾碼不顯示，改以星號***替代；資料加密機制，以確保資料外洩時，無法被輕易解密。

交換協議：個人資料交換時，應建置適切之管理程序、責任及技術標準。

監控系統的使用：使用監控工具監控網路使用者時，應考量個人之隱私，同時基於個資法規之要求，能否取得當事人之書面同意接受監控，亦屬一大難題。

存取控制：當事人要求查詢或請求閱覽時，如何控制其相關權限？是否開放當事人依權限存取？或是提供不同的作法。

4.資訊安全事故管理

如何整合事故通報與處置程序，當發生資訊安全事故或是個人資料外洩時，機關常先採取保護自己的作法，最保險的方法是封鎖消息，通盤否認，或將矛頭指向是委外廠商的錯誤。另個資法要求機關若查明確屬於內部管控不當，導致資料外洩，得通知當事人。因此上述作法在個資法實施後可能不被允許；建議的作法是，個人資料外洩，可以視同機關之安全事件，依程序應變處置，同時為因應個資事故通報與後續處理回應之實務需要，與對於個資事故之數位證據與數位鑑識處理上的需求，建議可整合個資事故通報流程。

5.其他遵循性

此部分之 ISO 27001 條文明確指出要通過 ISO 27001 標準之驗證，得識別機關適用之法條與應確保個人資訊的資料保護與隱私。個資法亦要求指定專人（data protection officer），由此專人對管理者、使用者和服務提供者，提供其各自的責任及應遵照的特定程序。

本報告之智慧財產權歸屬於法務部

因此，個資法的通過對已取得 ISO 27001 的驗證者，具有加乘之效。針對涉及個人資料部分可以加強其管理之效度，同時檢視相關之技術配套措施是否足夠。

基於法律規範要求，機關必須將個資全面性納入管理，因此若機關現行 ISMS 認證或實作範圍並未涵蓋全機關，建議首先可對現行 ISMS 認證或實作的範圍進行擴大，以能涵蓋機關內的相關個資流程為主。接著再開始建立個資保護管理機關步驟，此外，可將 ISMS 中與個資有關之類別（通常為文件與資訊大類），依據個資屬性新增對應的次分類，例如加入包含一般個資或特種個資內容的文件或資訊類別，同時在 ISMS 的風險評鑑與風險處理等項目中，建議可加入與個資相關之弱點/威脅評估及個資保護技術性安全控制，即可整合 ISMS 與個資項目之風險評鑑作業，也利於機關採一致化的風險評鑑產出結果，進行風險處理對策之研擬與行動方案的規劃。

對於個資管理行動方案的實作，不論是管理制度或是技術控制措施，必須注意的是通常 ISMS 的管控較著重在個資實際的處理流程上，但從個資法的角度與規範要求，對於個資的蒐集或利用等活動的管理也同樣重要，因此在既有的 ISMS 安全控制措施基礎以上，必須補強個資項目在其他相關生命週期活動中的安全控制措施需求。有關個資蒐集、處理或利用等活動的流程管理制度與技術控制措施實作建議，參見行政院研究發展考核委員會「個人資料保護參考指引」之 3.2.2 建立個資管理程序與 3.1.9 安全控制措施規劃等章節內容。

6.檢視控制措施

對於尚未通過 CNS/ISO/IEC 27001 驗證的機關而言，藉由本手冊及研考會「個人資料保護參考指引」之個資保護管理建置流程進行個資管理，可為機關建立部分資訊安全管理制度的應用基礎，未來當機關開始導入資訊安全管理系統時，亦方便機關將已建立的個資管理程序與活動整合其中。同時，可以先從以下四大層面，檢視機關重要的控制措施是否已經落實。

（1）實體環境安全

評估辦公區域、資訊機房和資訊設備，是否已受到良好的安全防護，重點項目包括：

本報告之智慧財產權歸屬於法務部

A. 是否已確保辦公室與機房的環境安全？例如使用不易受到破壞的門與鎖；在重要的區域進行門禁管制或安裝監視系統，訪客要求需配載識別證，並且僅限於在特定處所活動；定期檢查消防設施和人員的逃生設備是否足夠？

B. 是否可預防有人從外部可以窺探辦公處所的電腦設備或螢幕資訊？有些機關在機房、會議室，喜歡採用透明玻璃，因此需要評估人員在操作資訊設備或進行會議時，是否會造成不當的資訊外洩。

C. 含有個人資料的資訊設備與文件，是否存放於安全地點？例如筆記型電腦等可攜式的設備，還有包括硬碟、磁帶、光碟、USB 隨身碟等儲存媒體，採取適當的安全防護以避免遺失；紙本文件存放在管制或上鎖的區域，使用碎紙機、大量文件水銷等方式確保廢棄的文件不會再被還原。

（2）機關安全

評估機關針對個人資料是否制定了一體適用的安全政策，以及相關的作業程序以便人員可以遵守，重點項目包括：

A. 機關是否指定專人負責個人資料的管理？是否已制訂個人資料保護全政策，並提供適當的人力與經費，由高階主管來支持個人資料安全管理和保護工作的落實。

B. 機關是否已有和個人資料安全有關的作業程序，可供員工操作並且遵守？例如密碼的使用與設定要符合安全原則；人員離開辦公處所時應讓桌面淨空，不遺留文件在未經監管的地點；電腦螢幕設定一定時間自動啟用螢幕保護程式等。

C. 機關是否已建立跨部門溝通與協調機制？例如由各部門推派一位個資管理代表或聯絡人；成立一個跨部門的個人資料保護執行小組，並定期召開個資保護協調會議等。

D. 機關是否定期實施教育訓練，並確認員工已充分了解其應盡的個資保護與安全責任？例如依據人員不同的工作職掌，實施認知、管理或技術的教育訓練，並透過內部稽核的實施，確認教育訓練的有效性與成果。

本報告之智慧財產權歸屬於法務部

E. 機關若發生個人資料外洩事件，是否有相關的處理程序，並進行事後的調查與檢討？例如在個人資料受到竊取、洩漏或不當侵害時，由專人來負責通知當事人；制訂個資事件的證據收集與保存程序，或是尋求外部的支援。

F. 是否有人可從機關外部來存取資料？個人資料是否需要和外部進行傳遞或交換？實施了哪些安全措施來控制、保護與監控這些行為？例如清查有哪些資料是可供外部存取的，並針對資料的傳遞或交換，依法定程序執行或建立內部的作業規範；對於資訊委外處理的服務廠商，要求相對應的個人資料保護措施等。

（3）資訊系統安全

評估資訊系統的建置、營運與服務，是否已有適當的安全措施，重點項目包括：

A. 資訊系統的日常操作，是否有文件化的作業程序？例如設備的異動維護，皆已經過授權並留下紀錄。

B. 含有個人資料的主機，是否需要更高的安全防護，並執行嚴格的存取管理？例如主機實施實體隔離與監控，採用生物辨識方式，進行存取控制。

C. 資訊系統是否有備援機制？針對儲存個人資料的設備，採用不斷電系統以持續維運；將資料備份存放在不同的地點；確保還原機制夠完善，定期執行演練與測試等。

D. 資訊系統與應用軟體的弱點是否能被發現，並且定期更新修補？例如透過定期的弱點掃瞄或滲透測試，以及制訂適當的修補程序來進行控管。

E. 是否已經強化網際網路與電子郵件的使用安全？例如有能力偵測或防止惡意程式下載至電腦系統；防毒機制可定期更新；郵件主機實施適當防護；資訊設備和系統的紀錄檔（log）集中留存並可防止竄改等。

（4）人員安全

本報告之智慧財產權歸屬於法務部

評估職務角色適任與分工代理是否適當，重要項目包括：

A. 與個資有關的人員聘用，是否進行適當的徵信或資格審查？例如針對背景和學歷資格的確認，確認前項工作的離職原因；進行適當的職務分工代理等。

B. 是否額外註明對於個人資料保護的相關要求？例如在聘僱合約中加以說明，並要求簽署保密協定；在新進員工訓練或員工手冊中說明機關對於個資法的政策與個資處理的要求等。

C. 是否清楚告知員工機關資訊設備的使用注意事項？例如不得將個人帳號密碼透露給第三人、避免瀏覽惡意網站、不使用機關電腦收發個人郵件、不使用個人郵件寄送業務相關資料等。

以上簡要的評估方法，可作為有心強化個資防護的機關參考。

（六）考核監督作業

機關需要一套完整的個人資料管理的考核監督制度,即內部稽核作業以針對機關成員進行遵循性考核考核,藉由考核制度機關才能了解機關成員的實際表現和遵循落實程度。

個人資料管理的內部稽核制度是機關內部一種獨立的評估功能，檢查及評估機關的各項活動，而對機關提供服務。其內部稽核之目的為在於檢查、評估內部控制制度之缺失及衡量營運之效率，適時提供改進建議，以確保該制度得以持續有效實施，並協助機關管理階層確實履行其責任。而內部稽核之範圍為檢查現有制度，以確保重大政策、計畫、程序、法令及規章之遵循以確定其結果是否與既定目的及目標一致，以及是否照原定計畫進行。

因此，內部稽核在管理上的目的包括：1.協助機關管理階層達到最有效之管理，俾能按既訂之作業程序或政策計畫達成任務。2.確定各項個人資料管理作業及各項業務處理程序正確無訛。3.揭發並建議改正不健全之記錄及作業制度。4.維護個人資料之安全及合理運用。5.加強個人資料管理績效評估與管制考核。6. 強調其持續不斷之持續性監督。

本報告之智慧財產權歸屬於法務部

1.個資管理內部考核監督作業

本機制由機關內遴聘內部具稽核專長之人員擔任召集人，並由稽核召集人推薦具專長之同仁若干人經機關首長同意後任命成立稽核小組，推動內部稽核業務；而稽核人員應秉持超然獨立之精神，以客觀公正之立場，確實執行其職務，並定期向機關首長報告稽核業務。

（1）查核之範圍、目的與適用對象

A. 範圍：

a.個人資料保護作業遵循相關法規的符合性之審查。

b.個人資料保護作業達成目標的程度之審查。

c.達成個人資料保護作業政策與目標的方法與程序有之效性與適切性之審查。

B. 目的：

a.督促本單位所屬各機關加強個人資料保護，落實個人資料保護安全工作。

b.督促本單位所屬機關辦理年度個人資料保護稽核計畫及查核事項。

c.督促本單位所屬機關提昇個人資料保護業務之內部控制及風險控管效能。

d.督促本單位所屬機關辦理本部或上級機關交辦重要個人資料保護業務。

C. 適用對象：

本單位暨所屬機關個人資料處理及使用單位。

（2）查核之責任

A. 查核應對受稽單位業務之使用者負責。

B. 查核應以內部稽核為基礎，進行風險評鑑。

本報告之智慧財產權歸屬於法務部

C. 查核人員應由最後結果的驗證著手，對內部控制及業務流程進行測試及查核，以獲得足夠的證據，證實最後結果的妥適性及正確性。

（3）查核機關分工說明

實施查核機關成員由相關上級主管機關或監督機關單位最高主官主導指派相關人員組成，並依查核需要得洽請專家、學者或專業機關提供顧問諮詢服務或加入查核機關。成立外部查核小組時，應依受查核單位之機關規模規劃查核人力，並應遴選一人擔任主任查核員；查核成員分工如下：

A. 主任查核員的責任

a.查核之文書審查、工作分配。

b.規劃與管理所有查核階段。

c.彙整文書審查結果。

d.控制和處理困難問題。

e.主持查核單位與受查核單位間的會議。

f.稽核議題之裁決。

g.即時反映重大問題。

h.提報查核結果。

B. 查核員的責任

a.完成分派的查核工作。

b.配合主任查核支援其他查核工作。

c.紀錄和報告所有的查核發現。

d.即時向受查核單位提出相關查核情況。

e.妥善保存所有查核相關文件及遵守保密規定。

f.查核過程須維持獨立客觀及專業水準。

g.追蹤矯正預防及改善措施的有效執行。

本報告之智慧財產權歸屬於法務部

（4）查核之規劃

A. 查核之規劃與執行

規劃查核時可包含一項或多項查核計畫，這些查核計畫可以有不同目標，且可採取合併查核或聯合查核方式進行。

B. 規劃查核時應涵蓋查核的型態、次數、所需資源、查核時程等。外部查核計畫之規劃與執行流程如下：

a.取得授權：機關最高管理階層應授權規劃外部查核。

b.擬訂查核計畫：應規劃查核計畫之目的、範圍、所需資源、時程等，以指導查核之規劃與執行。

c.執行查核計畫：依據核計畫，評估查核人員、挑選查核小組成員、管理查核活動之進行及提出查核紀錄及報告。

d.查核計畫及報告之審查：稽核計畫執行前及完成查核後之查核報告均應予審查，對於查核報告中所列受查核單位應矯正預防及改善之事項則應予列管。

C. 查核工作計畫應依下列原則擬訂：

a.瞭解受查核單位的機關規模、業務範圍、業務複雜度、潛在風險及機關文化等。

b.決定查核目標、查核時間和所需資源。

c.選擇查核成員及協調查核時程。

d.研擬查核工作計畫及準備檢核表等相關資料。

e.外部查核工作計畫應涵蓋業務之主要控制項目。

D. 查核檢核表之功能：

a.查核檢核表須於辦理外部查核前提供受稽單位填報並據以準備受查核事宜。

b.查核檢核表是一種確保查核深度和持續性的重要輔助工具。

本報告之智慧財產權歸屬於法務部

c.查核檢核表可以界定查核的範圍。

d.查核檢核表可以協助瞭解查核的運作和流程。

e.查核檢核表可以作為查核及受稽單位間之備忘錄。

E. 查核程序

查核階段區分如下：

a.文件審查階段：審查受稽單位機關、業務、工作說明及各項業務執行紀錄文件。目的在於為擬訂外部查核工作計畫提供規劃的重點，以及瞭解達成業務目標的策略和背景脈絡。文件審查的主要項目包括：

I.業務管理及風險控管架構

II.業務活動範圍

III.達成業務目標之策略與執行計畫

IV.執行業務時發生事件的處理文件

V.業務執行成果相關文件

b.實施實地查核階段：驗證受稽單位對機關本身的策略、目的和程序的遵循程度。實施外部查核的主要項目包括：

I.訪談受稽業務相關的管理者與使用者。

II.瞭解受稽業務內部控制與內部查核之管理規章。

III.審閱受稽業務辦理內部控制與內部查核之書面報告。

IV.審閱受稽業務辦理內部查核建議事項執行成果之書面報告。

F. 查核執行程序

a.機關查核小組

I.指派主任查核員。

II.界定查核目標、範圍及準則。

本報告之智慧財產權歸屬於法務部

III.評估查核之可行性。

IV.準備查核工作計畫及工作文件。

V.挑選查核小組成員，並指派工作。

VI.與受查核單位人員建立初步聯繫。

b.文件審查及執行現場查核活動

I.舉行啟始會議。

II.查核中與受查人員之溝通。

III.引導查核人員與受稽人員。

IV.蒐集與查核相關資訊。

V.記錄查核發現。

VI.研提查核建議與結論。

VII.舉行結束會議。

c.研擬查核報告

I.研擬查核報告。

II.簽報核准後分發查核報告予受查核單位。

d.執行查核後列管追蹤

G. 查核之執行

a.首次會議

I.介紹查核背景及預期達成的目標。

II.確認查核目的與範圍。

III.查核工作計畫之確認。

IV.查核小組的任務分配及受稽單位引導人員之分配。

V.查核方法的溝通。

VI.查核報告大綱說明。

本報告之智慧財產權歸屬於法務部

VII.確認查核的抽、複核方法。

VIII.查核的保密承諾。

IX.查核的執行限制與問題澄清。

b.參加人員

I.查核小組

i. 查核小組組長及成員。

ii. 見習查核員及主任查核員。

iii. 見證人。

II.受查核單位

i. 部門主管及員工。

ii. 見習人員。

H. 實地查核之進行

a.進入查核區域。

b.受查核單位介紹受查核業務。

c.查核小組說明查核需求。

d.進行必要查核調查。

e.依據查核查核表循序執行查核。

I. 查核之溝通技巧

a.營造融洽氣氛，問題詢問力求簡要。

b.當問題不瞭解時，應讓受稽單位明確知道。

c.表現正面態度，並給受稽單位適當正面的肯定。

d.顯示耐心與理解力，避免打斷受稽單位之發言。

e.詢問應使受稽單位感到自在。

f.問題應針對與受稽單位之業務相關。

本報告之智慧財產權歸屬於法務部

J. 查核之提問要領

a.盡量採開放式諮詢；非僅”是”或”不是”。

b.引導受稽單位瞭解提問，以迅速獲得所需答案。

c.查核時可考量以調查結果、長官意見、假設狀況等方式提問。

d.完成提問時，應總結問題的發現及表達感謝配合。

K. 查核紀錄要項

a.記錄客觀的證據；可接受的陳述。

b.針對查核時所有適當的資訊做紀錄，包括：

I.對受查核稽單位人員訪談之發現摘要。

II.引用看見的文件、紀錄或法規。

c.記錄不符合規定事項：

I.清楚記錄不符合事項及其發現依據。

II.清楚記錄發現的事實；不要誇大發現。

III.清楚說明不符合的理由。

IV.清楚記錄發現不符合事項時的在場人員。

V.記錄不符合事項發生的可能性說明。

VI.記錄不符合事項持續錯誤可能產生的後果。

L. 查核的事實確認程序

a.取得受稽單位的協助。

b.針對查核所關心的問題進行討論。

c.共同驗證所發現的結果。

d.記錄所有的證據。

e.註明相關資料之屬性如文件編號、人員姓名、職稱、時間、

本報告之智慧財產權歸屬於法務部

部門等。

M. 查核應注意事項

a. 查核報告應具建設性、專業性，並對受稽業務有所助益。

b. 查核過程須定期檢討進度與發現。

c. 排除負面資訊，並與受查核單位建立良好互動。

d. 對於證據不足的資訊，必須做出對受查核單位有利的判斷。

e. 重視與疏通被查核方的反應。

N. 查核小組會議

a. 依據查核工作計畫表中的排程舉行。

b. 僅限查核小組成員出席。

c. 由主任查核員主持。

d. 檢討查核工作的有效性。

e. 提報查核事項書面報告。

f. 評審各項查核書面報告。

g. 規劃外部查核之結束會議。

h. 主任查核員準備總結報告。

O. 查核總結內容

a. 業務管理的內部控制系統是否有效。

b. 內部控制系統有無任何缺失。

c. 有無對特定事項須特別注意的說明。

d. 管理階層是否承諾對有缺失的內部控制持續改善。

P. 查核結束會議

a. 主任查核員須準備和控制會議議程。

本報告之智慧財產權歸屬於法務部

b.決定會議出席者。

c.報告查核目標與範圍。

d.報告受稽業務。

e.報告查核過程的工作限制。

f.報告查核所獲機密性資料的保密處理。

g.查核總結報告。

h.查核相關之協議、建議及問題之澄清說明。

Q. 查核報告

查核報告重點：

a.查核發現的摘要。

b.查核的範圍。

c.內部控制符合相關法規及管理要求之說明。

d.內部控制不符合事項之說明。

e.相關的觀察及受查核單位、業務等之記載。

f.清楚記錄不符內部控制事項，讓受查核單位明確瞭解。

g.清楚說明查核報告事項的事實根據。

R. 查核報告之確認與管考

a.查核報告須經外部查核結束會議相關出席人員確認。

b.查核報告應函送受稽單位。

c.受查核單位應依查核建議制定改善計畫，並提供外部查核單位備查。

d.受查核單位應依據改善計畫實施，並評估改善措施之有效性。

e.外部查核單位應評估改善計畫，若必要，須導引受查核單位修訂改善措施。

f.受查核單位應將改善成果提供外部查核單位驗證實施情

本報告之智慧財產權歸屬於法務部

形及其有效性。

S. 個資管理查核作業流程設計及執行

依據受查核單位之個資作業流程、作業程序書(蒐集、處理及傳輸)及事故通報與作業程序文件，訂定合宜之個資外部查核作業執行程序，或於現行稽核作業程序中，檢討調整個資檢核項目，並定期至少一年需執行一次查核作業或依實際狀況執行不定期之查核作業。

2.委外作業監督考核機制

關於委外管理之相關規定，依個資法第 4 條中，法律明定將受託機關於受託蒐集、處理及利用個人資料時，視同於委託機關；且 100 年 10 月間預告之個資法施行細則修正草案第 8 條，就委託人對於受託人「適當監督」之義務加以明確化。另 100 年 10 月間預告之個資法施行細則修正草案第 7 條，規定關於受託機關應遵循之個資法規，依委託機關應適用之規範為之；且當事人行使個資法上權利，亦應向委託機關行使之。依目前法令，就受託機關管理之適當監督措施至少應包括如下：(1)對於受託人之蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間；(2)受託人之適當安全維護措施；(3)受託人有複委託時，其約定之受託人；(4)違反個資保護法規或委託契約條款時，受託人應向委託人通知之事項及採行之補救措施；(5)委託人對受託人保留指示之事項；(6)委託關係終止或解除時，受託人就個人資料載體之返還，及儲存於受託人持有個人資料之刪除。且委託人應定期確認受託人執行之狀況、紀錄確認結果，受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。如受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。

關於委外管理措施之問題，實際上就在於上述委託機關管理監督受託機關之項目是否完整、是否制訂相關確認機制、選任受託機關時是否盡相關注意義務等事宜。例如，實務上企業經常有使用人力派遣公司之情形，須注意於選擇派遣公司時，是否經過確認該派遣公司存在個資保護之相關環境設備、制度之程序、該派遣公司是否要求其人員配合個資法令相關之告知義務等等事宜，如未盡相關檢視工作，即可能存在法律上之風險。

本報告之智慧財產權歸屬於法務部

個資管理實務上涉及人員管理、委外人員之管理項目十分繁雜，然根本之道則須先確認人員於從事個資相關業務處理之作業流程，以了解人員在作業過程中可能存在的風險環節，嗣後再配合相關的風險環節的作業加強、人員聘雇合約、委託合約等契約之合理設計、以及落實個資管控及稽核措施與加強教育訓練與認知宣導。

委外管理之所以重要，是因為不論公務機關或非公務機關個人資料蒐集、處理及利用等程序委外皆有相當高的機會與比例，委外管理不可不慎。稽核要點如下：

A. 是否於合約中載明應遵循機關之個人資料保護管理原則？

B. 是否具備對個資事項之稽核權？確認機關是否派員執行稽核、稽核頻率及稽核紀錄等。

C. 是否確認委託機關之防護要求等級應與機關相同，以確保風險發生之可能性。

D. 委外機關管理受委託之個人資料是否與機關之管理等級相同？

E. 挑選委外廠商或合作夥伴（受託人）時是否充分考量其資安管理能力?

F. 是否確認所委託蒐集處理利用之個資範圍、類別、特定目的及其期間。

G. 是否確認受託人採取必要之個人資料檔案安全維護措施。

H. 有複委託者，是否確認其複委託之對象及確認複委託對象蒐集處理利用之個人資料之範圍、類別、特定目的及其期間。

I. 受託人或其受僱人違反個資保護法令或委託契約時，是否有向委託人通知之程序及確實通知。

J. 委託關係中止或解除時，是否要求受託人返還或銷毀因委託事項所交付之個資儲存媒體或紙本，及確認因委託事項所儲存於受託人處之個資確已刪除。

K. 是否以適當方式確認受託人具體執行要求之程序，並留存相關紀錄以供查驗。

本報告之智慧財產權歸屬於法務部

L. 受託人之事故通報程序是否建立且留存相關紀錄。

（七）結論

個資法在 99 年 5 月 26 日修正公布，在保障個人隱私資料並兼顧新聞自由平衡下邁向新的里程碑。個資法強化了個資揭露、查詢及更正等自主控制，同時也參考「亞太經濟合作論壇（APEC）隱私保護綱領」所揭示的預防損害、告知及蒐集限制等原則並納入規範，以迎接個資保護全球化時代的來臨。

個資法的通過，除使我國與國際接軌的程度更加緊密結合外，同時也保障個人資料不被濫用，所以，個資法對於民眾的個人資料保護，將有一定的成效。對於政府機關而言，則應審慎評估與個資法相關規定，包括訂定機關之個人資料保護管理要點、指定「專人」辦理個人資料安全維護事項、設置「個資保護聯絡窗口」及指定「召集人」等。同時考量與機關已導入之資訊安全管理制度互相結合，以利統一執行管理審查相關作業，在對機關衝擊最小的情況下，順利完成個資法的防護要求。

因此，本手冊發展之主要目的為協助政府機關執行個人資料保護作業，藉由個資保護管理建置流程，包括計畫、執行、檢視以及持續改善四個階段，循序漸進完成個資保護管理制度，以執行法定必要之個資保護安全措施-即成立管理機關，配置相當資源；界定個人資料之範圍；個人資料之風險評估及管理機制；事故之預防、通報及應變機制；個人資料蒐集、處理及利用之內部管理程序；資料安全管理及人員管理；認知宣導及教育訓練；設備安全管理；資料安全稽核機制；必要之使用紀錄、軌跡資料及證據之保存；個人資料安全維護之整體持續改善，以展現機關保護個資之良善管理 。

政府機關於完成個資保護建置流程後，檢視各項程序的執行情形，同時加強個資稽核作業，確保個資管理措施已落實於日常業務中。

（八）參考文獻目錄

1.行政院研究發展考核委員會，個人資料保護參考指引，101 年。

2.行政院研究發展考核委員會，風險管理與危機處理作業手冊，98 年。

本報告之智慧財產權歸屬於法務部

3.行政院國家資通安全會報，個資保護規劃與實作建議報告，100 年。

4.個人資料保護法，99 年。

5.行政院國家資通安全會報，資訊系統分類分級與鑑別機制，99 年。

6.行政院國家資通安全會報，資訊系統風險評鑑，99 年。

7.行政院國家資通安全會報，公務機密資料防護研究期末報告，98 年。

8.Organization for Economic Cooperation and Development （OECD）, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980-09-23.

本報告之智慧財產權歸屬於法務部

伍、跨境隱私保護之國際合作機制

一、國際合作及爭議案例處理研究報告

（一）前言

由於資訊科技以及全球商務型態之發展，將所蒐集到之個人資料流通於各國間之情形相當普遍。各國不同之個人資料保護法制已經變成阻撓個人資料自由流動之原因。而且，與自由貿易以及環境保護議題相比，各國對於跨境個人資料保護尚無法取得全球性之共識。因此應加強雙邊以及多邊等國際協商，以促進個人資料國際傳輸之效率，並且得以保護個人資料。

個人資料之跨境傳輸係相當容易以及快速的。無論是商業交易、就診紀錄、工作面試、甚至網路搜尋紀錄都能夠使用為辨別特定當事人之方法，以及記錄當事人之隱私生活。再因資料係屬可流動的，故跨境傳輸個人資料係屬相當常見的，包含不同國家政府機關內傳輸、為委託他國公司處理個人資料而傳輸，又或者不同國家之公司為了達成與當事人簽訂之契約內容而為之跨境傳輸，皆為目前常見之跨國傳輸個人資料之類型。

資料流動相當容易，但資料流動於兩國甚至多國之間，適用何國之個人資料保護法律具有不確定性，主要原因就在於各國對於跨境資料傳輸之相關法規皆有差異。另外，各國對於個人資料保護之法規以及制度亦有差異，以英國為例，英國設有資訊委員辦公室（Information Commissioner’s Office）以維護公眾資訊權而設立之獨立政府機關，該政府機關致力於提倡政府資訊公開及個人資料與隱私保護，然而日本並無類似之組織設計，光是尋找主管機關恐怕即造成相當阻礙。

跨境資訊傳輸產生了法律適用之不確定性，原因在於如何適用各國對於跨境資料傳輸之相關法規，就資料管理者係相當不確定的。以跨國企業經營之情形為例，跨國企業為了有效利用資源以及業務發展之需求，企業內之各國分公司傳輸個人資料之情形實屬常見。然而，由於各國個資保護法之規範內容互有差異，法規遵循之議題成為跨國企業之關注重點，例如位於澳洲之子公司傳輸個人資料予美國之子公司時，分公司間應遵循何國之個資法？如何調和因法規遵循所產生之差異情形成為尚待解決的議題。

本報告之智慧財產權歸屬於法務部

再以不同國家間之公部門傳輸個人資料之情形為例，為了執行公務或者依法執行等目標，國家間可能發生個人資料跨國傳輸情形。例如，由於空運旅客紀錄交換具有犯罪調查層面上的重要意義，因此國際間針對空運旅客紀錄（Passenger Name Record, PNR）訂有特殊協議，除了 PNR 外，美國與歐盟訂有安全港協議[64]，建立國際合作機制。然而，此類型之個人資料跨國傳輸涉及國家主權以及各國之國內個資法規不同如何適用等爭議，如何衡量個人資料保護與國家利益孰重孰輕之問題，仍值得觀察。

除了不同政府公務機關間個人資料傳輸可能產生之問題外，另外，為了節省經營成本，許多企業將其所擁有之個人資料庫委外交由其他國家之資料中心處理（data center），因此，企業必須利用跨國傳輸個人資料之方式，將個人資料傳輸給他國之資料中心或他國之雲端業者手中。但由於各國之個人資料保護法規內容可能不盡相同，各國如何確保他國之資料中心已採取妥善之措施保護個人資料之安全？是否於各國之個人資料法規中，制訂相關要件或義務規定？而各國企業是否透過訂定契約義務之方式，要求他國之資料中心採取妥善措施保護個人資料？目前國際間尚無定論。

然而，跨境資料傳輸其實是具有相當利益的。只是，在不同國家、區域之概念裡，對於何種資料可適用於跨境傳輸可能產生不同之意見。例如，歐盟法認為，航空公司之旅客資料係屬不可跨國傳輸之類型，但美國基於國家安全之利益而認為，航空公司之旅客資料係屬可以跨國傳輸之類型。不過，經過美國與歐洲簽訂之臨時協定後，執法機關以及維安機關可跨國獲得信用卡交易資料、跨國飛行資料以及網站瀏覽紀錄等資料。

基於政治以及經濟上利益，各國國際組織以及國內法皆致力推動於調和國際間個人資料保護原則。特別值得一提的是，歐盟所建立的跨國個人資料傳輸規範較為嚴格，嚴格之標準也造成了個人資料傳輸

[64] 目前參加安全港協議之前提為，必須是依公權力行使調查或者維護市場公平競爭。然而，目前受歐盟認可之交流類型主要為貿易行為以及與航空相關之紀錄。因此，只有符合以上之情形，才可以適用安全港協議，金融、電子商務等都還不能使用安全港協議。Miriam Wugmeister , Karin Retzer , Cynthia Rich , Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules, 38GEOJIL 449,469(2007)。安全港之優點在於，具有一致性、減少相關時間勞力費用之負擔、符合美國法體系並且亦達成歐盟個人資料保護指令之要求。但缺點主要有可用性程度受限（並非所有產業皆可適用）、個人資料隱私主管機關必須執行而且不見得可以減少負擔，原因在於組織必須每年重新進行認證，以確認符合安全港之要求。

本報告之智慧財產權歸屬於法務部

之困難，目前正面臨相當大之挑戰[65]。因此，歐盟採納了個人資料跨境傳輸時所需遵守之標準契約條款，以及具有拘束力之合作規則，以克服個人資料難以自由流動之困難。而國際社會也亟須一個可行並具有影響力之全球性跨境傳輸原則，以確保個人資料於跨境傳輸時之安全。

對於個人資料跨境傳輸機制之設計，也牽涉區域以及各國之立法精神以及文化背景。以歐盟為例，跨境傳輸個人資料首重隱私權之保護，此係其重視人權之必然結果。然而，從 APEC 之個人資料保護指令之內容觀之，重視個人資料之原因在於希望可促進區域內電子商務活動之發展。因此，適用不同之個資法規定或機制時，必須了解其背後之考量因素[66]。

（二）個人資料跨境傳輸之國際合作機制分析

1.歐盟

（1）歐盟個人資料保護指令

歐盟個人資料保護指令參照歐盟理事會公約，建立一套非常類似的個人資料跨境傳輸系統。歐盟同時在此保護指令中，確立個人資料保護以及個人資料跨境傳輸之原則。依據歐盟個人資料保護指令之說明，因為經濟以及社會環境之改變，跨境傳輸個人資料情形相當蓬勃，同時，會員國間不同的個人資料保護法制造成跨國傳輸個人資料之困難，而此現象可能阻礙了歐盟內之經濟發展。因此，於個人資料保護指令中，歐盟對於個人資料跨境傳輸提供一套最低標準、嘗試消除障礙之原則，希冀能促進會員國間之個人資料流通。

歐盟保護指令要求受移轉之人者必須採取「合適的保護措施」（adequate protection），以確保受移轉之個人資料之安全性；原則上，除非該非歐盟會員國之第三國已採取適當之個人資料安全保護措施，否則歐盟之會員國不得將個人資料跨境移轉予第三

[65] Lingjie Kong, Data Protection and Transborder Data Flow in the European and Global Context, European Journal of International Law, May 2010, page 441.
[66] Christopher Kuner, Regulation of Transborder Data Flows under Data Protection and Privacy Law,OECD Digital Economy Papers No.187,page 7 .

本報告之智慧財產權歸屬於法務部

國[67]，至於是否已採行合適之措施保護個人資料，必須個案認定第三國之個人資料法制實施狀況，歐盟雖然透過以上之標準要求會員國於跨境傳輸個人資料至第三國時，必須遵守以上原則。但，依歐盟個人資料保護指令之內容，若第三國未採取完善之個人資料保護法制時，於以下所述之情形時，歐盟會員國仍可將個人資料傳輸至第三國[68]：

A. 獲得當事人同意[69]

B. 為了履行當事人與資料控制者間的契約或者訂約前之預備行為

C. 為了實現資料管理者與第三人間對於資料當事人有利之契約

D. 基於法律要求或者實現重大公共利益，或者為了建立、實施法律聲明及防禦之目的

E. 為了保護資料當事人之重大利益

F. 為了提供一筆依法須提供予公眾的資訊、或是由具有法律上利益之人所查詢的資料。

若未具備歐盟保護指令第 26 條第 1 項之例外條件時，歐盟會員國仍有操作個人資料跨境傳輸之作法。依據歐盟保護指令第二項之規定，資料控制者依契約要求第三國之機關採取充分保護個人資料之措施以保護個人隱私權與其他人格權時，會員國仍可授權境內之機關傳輸個人資料至第三國[70]。

如此的制度考量，的確保護了歐盟會員國人民之個人資料，但由於事實上，大部分之非歐盟會員國並未具備歐盟認定的「合適的保護措施」，此時將造成非會員國與會員國間傳輸個人資料之阻礙。基本上，依據歐盟個人資料保護指令之內容，採取合適的保護措施是原則，指令第 26 條所指的情形是例外。綜上，當會員國與非會員國間跨國傳輸個人資料時，有三項法律要件必須

[67] EU Directive 95/46/EC of The European Parliament and of The Council of 24 October 1005, Chapter Ⅳ Article 26.
[68] EU Directive 95/46/EC of The European Parliament and of The Council of 24 October 1005, Chapter Ⅳ Article 26 1.
[69] Elizabeth H.Johnson, Data Protection Law in the European Union, 54-SEP FEDERLAW 44,46(2007)
[70] 可參考 2001/497/EC,2002/16/EC,以及 2004/915/EC 之歐盟跨境隱私契約範本。

本報告之智慧財產權歸屬於法務部

加以了解，其一為該非會員國必須符合歐盟認定具有合適個人資料保護制度，其二為符合指令第 26 條第一項所指出的例外情形，第三項為必須依指令第 26 條第二項採取有效的安全防衛措施以保護個人資料。

但，指令中所指的合適之保護措施（Adequacy）為何？歐盟執行委員會（EU Commission）提出相關標準以供評價移轉個人資料之第三國是否具有合適的個人資料保護制度。透過歐盟執委會提出之標準，可避免因各國各自評價所造成標準不一的問題，而標準一致的標準亦可供第三國參考，依歐盟保護指令第 26 條第 6 項之規定，如何認定第三國已經採取充足的個人資料保護措施必須依循以下要件進行認定是否已經充分保護資料當事人之個人資料以及其他相關基本人權，包含該國之國內法、加入國際條約的情形、與他國針對個資保護之協商情形。

然而，事實上對於第三國是否已經採取合適的個人資料保護措施之評價係相當困難的。首先，設定有個人資料保護法制的國家並不普遍，而依據歐盟個人資料保護指令訂其國內法之非歐盟會員國更是少見。除此之外，以美國、加拿大以及澳洲為例，這些國家採取聯邦法律系統，故其國內各州對於個人資料保護法制之規範具有相當大的差異。另外，評價他國是否具有合適的個人資料保護措施其實是涉及政治性議題，非常敏感。有些國家認為，歐盟評價他國法制之行為係挑釁或者歧視的行為。對此，歐盟採取正面評價，而非負面列舉的方式，彈性的評價第三國之法制環境。除此之外，歐盟也將評價第三國法制環境之過程視為繼續發成之程序，而非以作出具體列表為目標。

如前所述，若接受個人資料之地區不被認定為具有合適之保護措施時，亦可依指令所提供之有效安全保護措施為之，主要包含標準契約範本之使用以及共同約束條款兩項機制。以下分別就標準契約條款以及共同約束條款兩項機制分析：

A. 標準契約範本

歐盟執委會依歐盟個人資料保護指令第 26 條第 4 項提出標準契約範本（the Contractual Model and Standard Contractual

本報告之智慧財產權歸屬於法務部

Clauses）以供各會員國於跨境傳輸時使用。標準契約範本之起草精神為，會員國簽訂標準契約後，即可不需徵求該國個人資料保護機關之准許，增進個人資料跨國傳輸之效率以及速度。

雖然該標準契約範本仍有發展空間，但國際上已有相當多國家利用該標準契約處理個人資料跨境傳輸。目前歐盟發展三套標準契約範本供會員國於跨境傳輸個人資料時參考，分別是2001/497/EC、2004/915/EC 及 2010/87/EU 之標準契約附錄。契約範本將資料傳送者以及資料進口者之義務分別規範。將個人資料傳輸至第三國時，縱使個人資料接收國已經採取合適的個人資料保護措施，個人資料的傳輸國仍必須採取額外的個人資料保護措施，2001/497/EC 以及 2004/915/EC 主要針對會員國之資料管理者將個人資料傳輸至非會員國之資料管理者，而2010/87/EU 廢除 2002/16/EC 契約範本，除了針對會員國之資料管理者將個人資料傳輸至設立於非會員國之資料處理者之情形外，賦予當事人更廣泛之契約求償權利，亦即個人資料受侵害之當事人可採取法律行動先向個人資料輸出者請求損害賠償，若個人資料輸出者無資力或發生逃避損害賠償責任之情形時，當事人可以向受個人資料進口者委託者（sub-processor）要求就其責任範圍負責。

根據以上所提之標準契約之性質以及應用範圍，歐盟執委會對於如何評價第三國之安全保護措施係採取嚴格之態度。換句話說，標準契約內容以及執行措施必須被檢驗，事實上歐盟所提供的標準契約被視為契約化的歐盟個人資料保護指令，要件規定上相當嚴格。

於標準契約條款中，於第三人利益條款中，關於責任原則之訂立，歐盟對於出口個人資料之會員國課予較高責任，另外Decision2001/497/EC 之附錄亦使個人資料輸出者以及進口者對於資料當事人負連帶責任，此責任制度之規定使得當事人更容易實行其權利。而 2004/915/EC 考量到連帶責任可能使傳輸與接受個人資料之雙方負過大之責任，故採取實質審查標準，認為個人資料之輸出者（exporter）以及進口者（importer）分別就其義務違反部分負損害賠償責任。個人資料輸出者對其未

本報告之智慧財產權歸屬於法務部

慎選個人資料進口者而事後產生之損害需負其責任，亦即個人資料輸出者必須注意個人資料進口者所在之國家是否已採取合適的措施保護個人資料，否則若因為個人資料進口者之疏失而造成當事人之損害時，個人資料輸出者必須負損害賠償責任。因此，若資料當事人因個人資料進口者之疏失而受損害時，當事人應先向個人資料輸出者要求採取適合的防護措施以保護其權利；若個人資料輸出者並未採取措施保護個人資料時，當事人可向個人資料進口者主張其權利。資料當事人同時亦得向做出錯誤選擇(選了未採取適合的個人資料保護措施之資料管理人)的個人資料輸出者主張損害賠償。此種責任規定在實務操作上非常重要，賦予個人資料輸出者必須審核個人資料進口者之背景(個人資料進口者所在之國家是否已採取適合的個人資料保護法制)，也更強化了個人資料於跨境傳輸時之保護措施。

另外，依據歐盟隱私權保護小組之建議，為了使資料當事人得以伸張其權利，歐盟標準契約條款賦予當事人利益第三人的地位。第三人利益契約對於當事人主張其權利時是相當重要之依據，尤其是許多歐盟境內之企業基於成本等考量，多將其所蒐集的個人資料交由歐盟外其他國家之機構處理個人資料，在這樣的情形下，個人資料在何處被處理，有時是難以確定的，透過賦予當事人第三人利益契約之方式，使當事人得以主張契約上之權利。然而利益第三人條款於實際操作上可能會遭遇困難，原因在於歐盟會員國之國內法中，並非所有歐盟會員國之契約法皆有利益第三人之概念[71]。

若要透過個人資料進口者與輸出者所定之契約監督雙方執行個人資料傳輸契約成果，事實上是有困難的，原因在於，訂定契約之精神即在於雙方之意願，外部監督機關很難針對契約實行本身進行審核、調查以及制裁。另外，對於設立在非會員國之個資進口者，監督機關很難進行有效的控管。據此，歐盟於標準契約建立契約監督機制，監督機關主要為各國監督機關。各國監督機關在以下三種情形時，可禁止個人資料之跨國

[71] Lingjie Kong, Data Protection and Transborder Data Flow in the European and Global Context, 21EURJIL 441,452.

本報告之智慧財產權歸屬於法務部

傳輸（1）個人資料之跨國傳輸係為了規避其國內法之規定（2）當違反契約之證據存在時（3）預期違約情形出現時。除了外部監督機制，歐盟亦在標準契約中規範和解機制。根據2001/497/EC 附錄之契約文字中指出，若資料當事人無法透過利益第三人契約解決爭議之情形時，可交付獨立第三人解決，例如個人資料保護機關；另外，亦可在個人資料移轉者所在地之法院提起訴訟；除此之外，亦可交由仲裁機關解決[72]。

標準契約範本作法提出後，於 2006 年，歐盟執委會提出標準契約之運用報告。歐盟執委會指出，先前之所以無法順利獲得標準契約運用報告係因為各國個資監督主管機關未適當的監督個人資料傳輸之情形。這也點出事實上，歐盟執委所面臨的兩難情況為，應如何有效監督個人資料跨境傳輸之情形。表面上雖然歐盟執委會建立了完善的制度保護了歐盟境內公民個個人資料，但實際情形卻是制度難以操作、甚至不可行的。標準契約之內容形成其實就是將歐盟隱私保護原則契約化，要件過於嚴格又缺乏彈性，標準契約條款增加個人資料跨境傳輸之行政費用負擔[73]，故傳輸以及接收個人資料之雙方不願意以標準契約條款作為其約定之內容。對於跨國傳輸個人資料之跨國企業而言，標準契約條款缺乏彈性，原因在於，實務上企業跨國傳輸個人資料時，不見得設立完整傳輸系統，時常運用郵件交換、內部資料庫查詢以及內部網路等工具跨國傳輸個人資料，此時，標準契約條款無法因應現況而調整，而產生難以適用之情形[74]。

B. 共同約束條款（Binding Corporate Rules）

如前所述，歐盟執委會已體認到模範契約範本適用上之問題。考量到企業營運之利益增加了共同約束條款（Binding Corporate Rule, BCR）機制。BCR 為歐盟工作小組依循歐盟個人資料保護指令之精神所提出，使跨國企業、團體以及國際組

[72] Commission Decision 2001/497/EC Standard Contractual Clauses Clause7; Decision 2002/16/EC Standard Contractual Clauses Clause7

[73] Miriam Wugmeister , Karin Retzer , Cynthia Rich , Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules, 38GEOJIL 449,467(2007).

[74] Miriam Wugmeister , Karin Retzer , Cynthia Rich , Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules, 38GEOJIL 449,467(2007).

本報告之智慧財產權歸屬於法務部

織跨境傳輸個人資料至其分公司、子機構位於其他未設有妥善個人資料保護法制制度之國家時，可遵循之規則，因此，當歐盟境內之企業選擇跨境傳輸個人資料時，可考慮選擇安全港協議[75]、BCR 以及標準契約條款其一為之。BCR 建立之宗旨在於，讓跨國組織減低簽署契約條款之行政負擔支出，可更有效率的於其團內跨境傳輸個人資料。但，BCR 僅適用在組織內部跨境移轉個人資料之情形，若是不同公司、企業或組織跨國傳輸個人資料情形時，則不適用 BCR。

BCR 之內容需被各國之個人資料保護主管機關所准許，於 BCR 架構下，歐盟創造了相互承認機制，當一方會員國之主管機關支持 BCR 之內容時，另外一方會員國之主管機關基本上不再要求修訂 BCR 之內容。但，BCR 之內容仍遵守歐盟個人資料保護指令所設定之原則。不同於標準契約條款，BCR 為跨國企業的運作規則，於符合特定情形時，BCR 會被用於保護跨國個人資料傳輸之情形。有些跨國公司本身架構不複雜，但是於全球設有許多分部，而分公司間之個人資料傳輸情形中，常理上並不使用協定，以避免增加企業營運之成本。此時，依循個人資料保護指令第 26 條第 2 項，於企業內個人資料跨境傳輸之情形發生時，BCR 將介入要求企業採取適當的個人資料保護措施。簡單來說，BCR 為具有企業內部自我拘束之效力。不同於標準契約條的是，BCR 屬於單方面之規範，故並未規範雙方之權利義務。除此之外，BCR 並非為行為法，其不能代替個人資料保護法，而且 BCR 之內容必須遵守個人資料保護原則為之。BCR 之內容主要有隱私保護原則（透明性、資訊品質原則、安全管理措施等原則）、有效措施（審核、教育訓練、申訴處理系統等）以及證明 BCR 具有拘束力之相關元素[76]。

實務上，歐盟境內的跨國企業利用 BCR 傳輸個人資料至歐盟境外子公司之案例並沒有很多，多數歐盟會員國對於 BCR 的運用仍存有疑慮。原因在於，BCR 缺乏簡化性程序，

[75] 但安全港協議僅適用於傳輸至美國境內，並符合特定產業種類時，始得為之。

[76] http://ec.europa.eu/justice/policies/privacy/binding_rules/procedure_en.htm ,最後瀏覽日 100 年 10 月 24 日。

本報告之智慧財產權歸屬於法務部

於多國參與情形下，為了符合不同的法律特別規範，對於 BCR 將產生更為狹窄之解釋，降低企業利用 BCR 之意願。

值得一提的是，歐盟議會於 2008 年實施犯罪偵查合作對於個人資料傳輸之保護框架（Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters），針對因犯罪偵查需求而須傳輸個人資料至境外之情形，進行相關規範，例如，必須確認接受個人資料之國家具有良好之個人資料保護機制等要件[77]，其後續發展須進一步追蹤。

（2）歐盟一般資料保護規則草案

歐盟隱私保護指令自 1995 年公布以來，已經歷經 17 年之光陰，於此十幾年之光陰中，全球科技、資料共享以及資料蒐集規模之急遽增加，使得修改隱私保護指令之呼聲漸高。因此，歐盟理事會於 2012 年 1 月 25 日提出歐盟一般資料保護規則草案 (Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data, General Data Protection Regulation)。

本草案針對個人資料跨境傳輸之相關規定在第五章第 40 條以下，原則上必須符合歐盟執委會所認定之「已提供適當保護措施」。何謂已提供適當保護措施？評估時，考量該國、地區之個人資料保護法制；具備個人資料保護獨立機關等因素。若該國或該組織無法獲得相關認可，於第三國提供適當之保障措施時，亦可進行個人資料跨境傳輸。歐盟認定之適當保障措施，包含共同約束條款（Binding Corporate Rules）以及標準契約條款，針對共同約束條款之要求事項以及契約條款之內容皆訂於本規則草案中。當然，於資料當事人表示同意時，亦符合本草案之內容。

2.歐盟與美國所簽訂之安全港協議

[77] Article 13 of the Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters

本報告之智慧財產權歸屬於法務部

為了犯罪偵查機關執行公務之目的，政府間時有合作跨傳輸個人資料之需求。以美國與歐盟為例，為打擊恐怖犯罪之目的，對於旅客資料跨境傳輸簽署旅客姓名傳輸協議(Agreement between the European Union and the United States of America on the Processing and transfer of Passenger Name Record Data by Air Carriers to the United States Department of Homeland Security)。另外，對於金融資料之跨境傳輸亦簽訂協議（Council of the European Union, Council Decision on the Conclusion of the Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for Purposes of the Terrorist Finance Tracking Program,24 June 2010.)。歐盟與美國間成立高度密切聯絡小組(the High Level Contact Group)以統合處理歐盟會員國與美國政府機關就協議事項之協調事宜。同時，亦設定個人資料跨境傳輸保護之相關標準，以供歐盟及美國政府遵循之。

由於美國採取分散式之之法律規範模式以保障個人資料，與歐盟各會員國之作法不同，又因為美國並未被歐盟執委會認定為具備充分（adequate）之保護措施地區，因此於個人資料跨境傳輸時，依歐盟個人資料保護指令，歐盟內之個人資料似不能傳輸至美國，除非符合其他例外情形。對此，為了弭平兩區域間因個資法規範不同所造成個資無法跨國傳輸之情形，美國商務部與歐盟執委會協議採取安全港架構。[78]該安全港架構提供欲跨境傳輸個人資料之組織可自行評估並決定是否加入安全港架構。

安全港協議列出七項原則，包含通知（Notice）、選擇（Choice）、轉讓個人資料予第三方（Onward Transfer, Transfers to Third Parties）、存取（Access）、安全（Security）、資料完整性（Data Integrity）、執行（Enforcement）。各原則之內容如下：

（1）通知

當組織蒐集並利用當事人之個人資料時，必須通知資料當事人。此外，必須通知當事人聯絡窗口之訊息，使資料當事人於申訴或者提出任何請求時有可聯絡之管道。除與組織之聯絡方式

[78] 張乃文，解析個人資料國際傳輸之法規範趨勢，萬國法律，第 181 期，2012 年 2 月。

本報告之智慧財產權歸屬於法務部

外，包含向第三方揭露資訊之方式以及限制其使用及揭露之手段及方法。

（2）選擇

將當事人之個人資料提供與第三方前或者用於不符合當初蒐集目的之情形時，必須使當事人有機會選擇是否同意該行為。

（3）轉讓個人資料予第三方

當組織將個人資料轉讓與第三方時，組織必須符合通知以及以及選擇原則之要求。組織必須確保第三方同樣遵守安全港架構下之隱私保護原則，例如可透過訂定契約之方式，要求第三方亦須遵守安全港之架構。

（4）存取

當事人對於組織所擁有之個人資料可要求其保持正確，並有要求其刪除、修改或者進行更正之權利。僅在該行為將產生和個人隱私不相稱之風險或侵犯到其他人之權利時，當事人才不能行使相關權利。

（5）安全

組織必須採取合理之安全預防措施以避免個人資料洩漏、受濫用、非法存取、非法修改以及毀損之情形。

（6）資料完整性

使用個人資料時，必須於其蒐集個人資料之目的具關聯性。組織必須採行適當措施確認個人資料對於其使用之意圖、個人資料內容之準確性、完整性等內容。

（7）執行

為了確認組織是否依循安全港所要求之原則跨境傳輸個人資料，必須建立獨立申訴機制；確認組織承諾遵守安全港原則之程序已被實施；未遵守原則時，組織應矯正其傳輸行為。組織必

本報告之智慧財產權歸屬於法務部

須提出年度自我檢視文件。

安全港架構主要透過非公務機關組織自律之方式運行。除了自律訂定隱私計畫之方式以遵守安全港架構之要求外，組織本身也可以制定相關監管之隱私政策，以符合美國與歐盟之安全港架構。

此外，除了符合安全港原則外，組織亦必須建立損害賠償措施，並且建立相關爭端解決管道，以符合美國政府以及歐盟會員國個人資料主管機關之要求。

3.APEC 亞太經濟合作組織跨境隱私規則運作機制

2004 年 11 月，亞太經濟合作會議（Asia-Pacific Economic Cooperation, 以下簡稱 APEC）訂立隱私保護綱領，綱領之制定主要係以會員經濟體之經濟利益為出發點，相較於歐盟隱私保護指令，有認為 APEC 隱私保護綱領是目前世界組織對於個人資料保護規範中，規範強度稍低之公約。縱使規範強度不若歐盟，但 APEC 隱私保護綱領之重要性仍不容小覷，以 APEC 會員國之涵蓋範圍而言，亞太經合會涵蓋美國、加拿大、墨西哥、祕魯、智利、俄羅斯、澳洲以及中國等共 21 個國家，其經濟圈遍及世界四大洲，故隱私保護綱領於全球性個人資料保護法制中，絕對佔有舉足輕重之角色。

APEC 透過亞太經濟合作組織資訊隱私開路者合作計畫（APEC Data Privacy Pathfinder Projects）建立多邊隱私保護認證機制。開路者計劃之內容包含了自我評估[79]、承諾審查[80]、互相承認與接受[81]、爭議解決與執行[82]等九項子計畫[83]。開路者計劃之目標主要在於符合 APEC 隱私保護綱領之原則下，推動 APEC 跨境隱私保護規則（Cross-Border Privacy Rules, CBPRs）。開路者計劃透過設計一連串的制度，提供企業經營者得以建立其內部之跨境資料傳輸規則，並且透過認證機制[84]

[79] 商業組織自我評估之綱領
[80] 信賴標章以及跨境隱私規則之審查程序之綱領
[81] 通過認證、審查合格之機構名冊
[82] 個人資料保護主管機關或者隱私權聯絡辦公室名冊、合作協議範例、跨境申訴處理機制範例、針對跨境隱私規則系統之反應機制、跨境隱私規則國際執行領航者計劃。
[83] APEC Data Privacy Pathfinder Projects Implementation Work Plan
[84] 公證認證機制必須具備兩項基本功能，其一為認證企業已依 APEC 隱私保護綱領建立其內部之跨境隱私規則，其二為該機制必須提供爭端解決並且供消費者可投訴其個人資料受侵害情事之管道。公正認證機制不限制各國個人隱私主管機關，亦包含已於會員經濟體內建立良好信譽

本報告之智慧財產權歸屬於法務部

（Accountability Agents）之建立，使企業得以提供消費者可信之標章。

開路者計劃透過五項核心文件，推動 CBPRs 之發展，核心文件之內容包含申請認證組織自我評估之評量表、對於認證組織根據隱私綱領九項原則所訂定的要求給予企業認證、審核認證組織之資格、跨境隱私合作協議、共同監督者（Joint Oversight Panel）之章程等。

以下介紹 APEC 跨境隱私規則運作之相關機制：

（1）APEC 跨境隱私保護規則（Cross-Border Privacy Rules，以下簡稱 CBPRs）

電子商務指導小組（ECSG）致力於發展 CBPRs 系統以建立消費者與企業間之互信基礎。2010 年六月，建立 APEC 跨國隱私執行文件，多邊協議提供會員經濟體針對個人資料跨境分享與互助之機制。該協議文件進一步實現 APEC 隱私保護綱領之宗旨，以及提供更有效之機制促進個人資料之跨境流動。

CBPRs 主要基於 APRC 隱私保護綱領以及各經濟體之國內法所編寫。CBPR 系統並非硬性法，只是提供相關原則供有需要使用之組織參考，各組織可依其本身之情形彈性制定其內部之跨境個資隱私規則。CBPRs 系統並不取代會員國之國內法。如果國內法之要求高於 CBPRs 系統時，則企業所定之跨境隱私規則仍須遵循國內法之要求，但若該會員經濟體並無個人資料保護之國內法時，則 CBPR 則為最低之保護標準。APEC 將認證機構分為公部門以及私部門，於細部之原則規範有所不同，但兩者仍須遵循共通之原則[85]（Accountability Agent Recognition Criteria）。

基本上，CBPRs 系統僅供於 APEC 會員國向其他 APEC 會員經濟體跨境蒐集或接受個人資料時使用。CBPRs 要求組織發展其跨國隱私保護之企業內部規則，該規則必須透過公正第三人（Accountability Agent）認證其符合 CBPRs 之最低要求後，始可跨國傳輸個人資料。一旦企業內部所制定之跨境傳輸規則被認證後，將會約束企業本身，同時，該會員經濟體國內之管理者，例

之隱私標章系統，以及符合其業務執行類政府單位（政府機關、消費者保護機構、隱私標章發放機構）。資料來源：APEC Data Privacy Pathfinder Projects Implementation Work Plan.

[85] 獨立性、程序要求、驗證程序、申訴處理機制、

本報告之智慧財產權歸屬於法務部

如隱私主管機關，也將要求企業執行該項隱私政策。

CBPRs 強調責任原則，認為企業必須為其向顧客所作之承諾負責任，另外責任原則為企業處理個人資料時，必須遵循之最高宗旨。除此之外，必須於 CBPRs 內建立有效的執行制度，以落實保護個人資料、促進個人資料流通之原則，綜上所述，CBPR 必須以企業、顧客、立法者以及政府之角度加以考量，而 CBPRs 制定過程中，主要以各經濟體內之立法者以及政府機關為關鍵之地位。

企業建立其內部之跨境隱私規則時，需進行以下四個步驟：自我評量（Self-Assessment）、檢視是否遵守隱私保護綱領（Compliance review）、識別/採納（Recognition/Acceptance）、爭端解決機制與執行（dispute resolution/Enforcement）。首先，企業必須透過 APEC 根據隱私保護綱領所提供之[51]個問題86進行內部之自我評量。然後，由公正第三方之認證機構（Accountability Agent）針對企業所提供之自我評量表進行評估。認證機構也必須確認企業本身執行隱私政策之確切情形，申請者將依公正第三人所提出之程序性要求，執行自我評量表所提及之相關施行程序。一旦企業通過認證機構之檢視後，公司隱私權政策將被 APEC 所認證，並將經由公告之方式，宣告企業已建立其內部之跨境隱私規則。於企業建立其內部跨境隱私規則後，透過內部之爭端解決機制以及外部規範之方式，確保企業內部跨境規則之確實執行情形。

以下說明 CBPRs 四項步驟之內容:

A. 企業之自我評估

APEC 將由適合的認證機構提供自我評估表給企業進行自我評估程序。該評估表之問題內容將會以 apec 所定之相關文件為最低標準（跨境協議文件、跨境隱私共同監督者之章程等）;其實企業透過自我評估表,可以檢視其內部隱私政策之內容，更進一步可以建立公司之隱私政策。基本上，目前有五十

[86] 51 個問題可依隱私綱領分為通知、選擇、當事人查閱修正權利等符合 APEC 隱私保護原則之類別。

本報告之智慧財產權歸屬於法務部

一個問題，但各國之認證組織仍可視其需求，增加自我評估表之問題。當企業依 CBPRs 系統之要求而完成相關程序後，認證組織將會將認證結果公佈於公開頁面上供他人查詢，

B. 確認是否遵循 APEC 隱私綱領

首先必須確立認證組織之資格。如何確立認證組織之資格呢？由各會員經濟體之隱私執行機關所推派的共同監督小組將會確認認證組織已經符合相關要求。當共同監督小組認可認證組織之資格時，將會做出結論，使會員經濟體得以判斷該認證組織適格與否。若通過相關資格檢驗後，將視為 ECSG 所認可之認證組織。目前有相關標準認定認證組織是否適格，包含程序性要求、爭端解決機制、利益迴避政策等。另外，認證組織必須定期統計申訴案件之數據以及相關案件（匿名化）。申訴處理將是 CBPRs 的重點，原因在於妥善申訴機制之建立，將使 CBPRs 更透明化，並且得以符合隱私保護綱領之要求。再者，將可根據申訴修正並供更進一步之措施，改善跨境隱私規則之內容。最重要的是，妥善的申訴機制將使得消費者對於跨國隱私保護機制更具信心，而可促進個人隱私跨境流通。

認證機構將依企業所遞交的自我評量表，評估企業之隱私政策是否符合 CBPRs 程序性之要求。相關程序性要求係依據各會員經濟體之情形訂定之，故為最低之要求。

當認證機構欲以其本身設計之內部評估表取代 APEC 所認證的自我評估表，認證機構應該以符合會員經濟體法制以及 APEC 認證內容為基本概念為設計出發點。

C. 認證

會員經濟體應建立已認證之企業以及認證機構之相關資訊，包含聯絡資訊等，提供消費者使用。

D. 執行

透過認證機構以及各國隱私保護主管機構執行 CBPRs 系統。

本報告之智慧財產權歸屬於法務部

CBPRs 之架構為 APEC 的會員經濟體得推薦公正的「認證機構」（Accountability agents）認證其國內公司遵守 APEC 隱私保護綱領所制定之原則。由於 APEC 各會員經濟體於該國之個人資料保護之機制並不相同，有些國家透過消費者保護之主管機關、隱私保護專責機構，有會員國亦利用私人機構之方式，例如隱私權標章認證機構，以上組織皆符合 CBPRs 架構中之認證機制[87]。認證機構之重要任務在於，必須能夠有效處理申訴事件。由於各國之法制不同之問題，透過 CBPRs 系統之協助，使不同國家之認證機構得跨境合作解決申訴案件或者可請求他國之認證機構協助，以保護消費者之利益。除了申訴案件之解決外，認證機構必須監控企業是否遵循 CBPRs 系統之規範，以及企業所訂的跨境隱私規則是否符合 APEC 隱私保護綱領之要求。CBPRs 系統非常重視認證組織之功能，若某會員國內之唯一認證機構退出或者停止認證業務時，該會員經濟體內之企業申請認證事宜皆須停止。除此之外，若該會員經濟體出現了新的認證組織時，以前申請過的企業必須重新向新的認證組織提出申請，以確保受認證之組織所定之跨境隱私規則持續有效。

認證組織之監督者為共同監督小組（the Joint Oversight Panel，以下簡稱 JOP）。根據 APEC 之制度設計，將從參與 CBPRs 系統之會員經濟體中，選出三個會員經濟體之代表，以組成共同監督小組 JOP。2011 年於舊金山召開的會議更要求共同監督小組 JOP 必須報告申請加入之會員經濟體參加 CBPRs 要件之狀況。

JOP 應如何組成？依 section 6.2 of the Joint Oversight Panel 之內容，JOP 由三個會員經濟體之代表所組成。JOP 必須依循 ECSG 之要求以及加入 CBPRs 成員之需求，協助執行 CBPRs。若 JOP 之成員之一也為會員經濟體之認證機構（政府機構）時，DPS 將會指定其他 APEC 會員經濟體暫代 JOP 成員之職務。JOP 也將建立工作小組協助 APEC 會員經濟體以及 APEC 秘書處之相關任務。JOP 之主席在每次 DPS 開會前一個月必須提出報告說明 JOP 之任務執行狀況。

JOP 的工作內容包含以下幾項：

[87] APEC,Project 8: Scope and Governance of a Cross- Border Privacy Rules System, http://aimp.apec.org/ Documents/2010/ECSG/DPS1/10_ecsg_dps1_012.doc

本報告之智慧財產權歸屬於法務部

A. 依 CBPRs 系統之設計，推薦會員經濟體選定認證機構（Accountability Agent）之標準。

B. 認證並且有權利終止認證機構之認證資格。另外，JOP 亦蒐集認證機構所認證之案例，確認認證過程符合 APEC 認證標準原則，並且將確認結果向會員經濟體公布。

C. 蒐集認證機構所接獲之申訴案件。

D. 當認證機構針對企業所提出之申請進行認證，而可能發生利益衝突之情形時，JOP 必須建議認證機構停止並退出認證程序。

E. 查核認證機構是否依認證原則（the Accountability Agent Recognition Criteria）審核企業之申請。

F. 當認證機構本身之經營權、內部結構以及政策將影響法規遵循時，JOP 必須重新檢視認證機構進行認證之適格性。

G. 當必須與會員經濟體合作時，JOP 於必要時，將幫助會員經濟體審視並且編輯相關文件之內容。

H. 執行 CBPRs 系統所訂之任務。

如前所述，根據 APEC 之制度設計，加入 CBPRs 之會員經濟體經受認證已符合 APEC 隱私保護綱領原則後，即被視為以符合各會員經濟體之國內法，而可進行個人資料跨境傳輸行為。2011 年於舊金山召開的會議更要求共同監督小組必須報告申請加入之會員經濟體符合參加要件之狀況，故 APEC 並未採取同儕評量之方式。目前可知已採取 CBPRs 之會員經濟體為澳洲、紐西蘭、加拿大、香港以及韓國（法制沒有採取 CBPRs 所要求的企業認證要件之國家）。但有認為參與 CBPRs 之企業，仍無法免除需要冗長的申請程序以及行政負擔，而上述缺點正是當初 APEC 想要極力避免的[88]。

值得一提的是，國際商會（International Chamber of Commerce, ICC）亦提出了可多項溝通之草案，該草案更進一步說明當美國

88 https://www.privacyinternational.org/article/apec-cross-border-privacy-rules-ready-party-will-anyone-come，最後瀏覽日 2011 年 10 月 25 日。

本報告之智慧財產權歸屬於法務部

金融業已經達成了其國內之個資法要求後，可認證其亦符合APEC 隱私保護綱領之要求，不需要再透過 CBPRs 之架構進行認證程序，此草案將會影響共同監督小組評價其他法規系統之設置目的，已經有會員經濟體對此草案表示參與之意願，但國際商會所提出之草案仍有品質管控以及透明性不足等疑慮，其發展之動態值得觀察。

（2）APEC 跨境隱私執行機制（APEC Cross-Border Privacy Enforcement Arrangement, CPEA）

為了達成 APEC 隱私保護綱領鼓勵個人資料跨境傳輸之精神，APEC 於 2010 年六月提出了可供雙邊、或多邊協議之跨境隱私執行機制並提出文件範本[89]，提供會員國間進行犯罪調查、隱私權執行案等跨國資料傳輸時利用。另外，透過此文件之建立，使會員經濟體間可交流分享國際傳輸之經驗。

本跨境隱私合作協議機制是 APEC 開路者機制（Pathfinder）為達成隱私保護綱領之要求所建立。本跨境隱私執行機制主要希望促進 APEC 會員經濟體內之個人隱私執法機關之合作；建立個資隱私保護機關的合作機制，包含調查、執行之合作；推動跨境隱私規則 CBPRs 之利用；除了 APEC 會員經濟體外，本跨境隱私執行機制也鼓勵非會員國分享與交流個人資料跨境執行與調查行動。

跨境隱私執行機制在於建立實用之多邊合作機制，APEC 希望其所有之會員經濟體皆可參與本跨境隱私執行機制。本跨境隱私執行機制內容包含合作協議之起源、定義與法律限制、管理者機關、加入與退出機制、跨國合作、保密協定、資訊交流機制、其他事項（人員交換、爭端解決、檢視），除此之外，本跨境隱私執行機制亦附上標準表格，提供跨國個人資料傳輸所需利用之表格。

關於 APEC 內的合作事宜管理者，APEC 跨境隱私執行機制交由電子商務指導小組（ECSG）指定 APEC 秘書處、會員經濟體之隱私執行機關（獲得其同意）或者 APEC 秘書處與國家隱私

[89] 簽署之國家包含澳洲、加拿大、香港、中國、紐西蘭以及美國。

本報告之智慧財產權歸屬於法務部

執行機關共同（獲得其同意）管理。管理者主要之任務為，接受參加、退出之通知，列出使用跨境個人資料傳輸機制者之名單，並且編列各會員經濟體完整的聯絡方式以供參閱。除此之外，其亦負責公告會員經濟體內相關合作協議，並促進各會員經濟體利用跨國合作模式之意願。

跨境隱私執行機制之內容，須符合 APEC 隱私綱領之內容，但跨境隱私執行機制並非以限制各會員國之國內法為宗旨。另外，會員經濟體亦可針對個人資料跨國傳輸之活動另外訂定協議或公約，並不侷限於使用跨境隱私執行機制之內容。會員經濟體若有意加入跨境隱私執行機制，可向管理者申請，並採取合理措施通知其他已參與之會員國，例如於官方網頁上公佈已加入或退出跨境隱私執行機制之訊息。跨境合作時，以將資源利用最大化為目標，參與者應排列不同優先順序事務以處理，請求協助者於請求時提供特定理由，另外，若合作事宜係與執行跨境隱私規則（CBPRs）有關者，參與者必須以執行跨境隱私規則（CBPRs）為優先。

（3）目前 APEC 之發展

2011 年 11 月 APEC 於夏威夷所召開之會議指出，著眼於保護個人隱私，將加強區域性以及國際性之個人資料保護機制。透過整合區域以及國際間之個人資料保護機制，加強個人資料跨境傳輸機制之運作。

2011 年 12 月，日本國內共 15 個機關加入 APEC 跨境隱私執行機制（CEPA）。目前已加入跨境隱私機制之會員國包含澳洲、加拿大、香港、紐西蘭以及美國。如前所述，跨境隱私執行機制主要促進會員經濟體間對於個人資料之跨境傳送更為流通，並且希冀透過跨境隱私執行機制調合各國間因個資法保護要件不同，而產生扞格之情形。加入本跨境隱私執行機制之各國個人資料保護主管機關可相互合作執行跨境個人資料保護事宜。APEC 已開始思考除了亞太地區之個人資料跨境機制之加強外，也思考如何與其他區域之跨境隱私機制進行合作或者整合，以歐盟為例，APEC 思考如何將 CBPRs 機制與歐盟之共同約束條款作調和，以促進全球間之個人資料跨境傳輸。

本報告之智慧財產權歸屬於法務部

2012 年，APEC 將依透明化、流通化、以及低成本化之目標建置更為完善之跨境傳輸個人資料制度。除了加強區域內各國對於跨境隱私系統之認識外，也希望區域內之會員經濟體可踴躍參與跨境隱私機制。

4.經濟合作與發展組織（Organization for Economic Co-operation and Development, OECD）之個人資料跨境傳輸機制建議

如前所述，各國對於其國內個人資料保護法要求之差異，可能造成個人資料跨境傳輸時之障礙。例如有些行業，例如金融業以及保險業對於跨境個人資料傳輸有極大需求，但卻因為各國法制不同，而產生個人資料無法有效傳輸之情形。因此，解決個人資料跨境傳輸之問題，成為各國所共同面臨之議題，承上，經濟合作與發展組織會員國認為須制訂區域性之個人資料保護機制以避免個人隱私權被侵害、個人資料被濫用等情形，同時可幫助調和各國之個人資料保護法制，並且在提升人權保護以及避免妨礙個人資料國際傳輸間尋求平衡點[90]。據此，OECD 制定隱私保護與個人資料跨境流通之指導原則。

該指導原則係於 1980 年 9 月 23 日被 OECD 所接受，該指導原則整合國際間對於個人資料蒐集以及管理制度之共識。由於指導原則係 OECD 於 1980 年提出第一個全球性的隱私保護原則，因此該指導原則對於美國早期建立「公平資訊實務」具有深遠影響，除了美國之外，OECD 指導原則亦被各國接受為個人資料保護原則，因此指導原則亦為各組織、各國所建立之個人資料保護原則之基本架構。

OECD 於 1980 年公佈「個人資料保護準則以及跨國資訊傳輸準則」（Recommendations of the Council Concerning Guidelines Government the Protection of Privacy and Trans-Border Flows of Personal Data），列出七項原則；一、通知（Notice）：當個資被收集時，應通知當事人。二、目的（Purpose）：資料僅得以說明之目的為使用，不得作為其他目的之使用。三、同意（Consent）：未獲得當事人之同意時，不得揭露當事人之資訊。四、安全保障（Security）：需保障被蒐集之資料被濫用。五、揭露（Disclosure）：當事人應被告知誰在蒐集他們的資料。六、

[90] OECD 網站，http://www.oecd.org/document/20/0,3746,en_2649_34255_15589524_1_1_1_1,00.html，最後瀏覽日 2011 年 9 月 28 日。

本報告之智慧財產權歸屬於法務部

查閱（access）：當事人應可查閱其個人資料並且可改正任何不精確之個人資料。七、責任原則（Accountability）：當事人須被通知須負起個人資料蒐集使用以及管理責任者為何人。透過個人資料保護準則以及跨國資訊傳輸準則表達各國整合個人資料保護原則之共識，亦可了解OECD各會員國對於消除各國間對於個人資料保護差異以及建立更有效率之跨國個人資料傳輸制度有一致想法。

除了個人資料保護準則以及跨國資訊傳輸準則外，OECD隱私保護與個人資料跨境流通指導原則主要也包含八項原則，包含限制蒐集原則（The Collection Limitation Principle）、資料品質原則（The Data Quality Principle）、目的明確化原則（The Purpose Specification Principle）、限制使用原則（The Use Limitation Principle）、安全保護原則（The Security Safeguards Principle）、公開原則（The Openness Principle）、個人參與原則（Individual Participation Principle）、責任義務原則（Accountability Principle）。指導原則中，最重要的兩個基本思想為，保護個人隱私以及個人自由、促進各國間個人資料傳輸之流動，故為嘗試平衡保護個人隱私以及促進流動之兩項目標，於限制個人資料流動同時，同時亦強化推廣個人資料自由跨境流動之概念。

雖然OECD之指導原則希望能建立共通原則以消除各會員國國內法之差異，但OECD之指導原則係無拘束力的，例如，簽署OECD指導原則之美國並無將指導原則訂入其國內法內，故關於個人資料保護之法律於各會員國間仍互有異同。

OECD於2007年提出關於跨境合作傳輸個人資料法律機制之建議（Recommendation of the Council on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy）。內容建議會員國須採取以下措施以促進個人資料跨境傳輸機制建立。包含：

（1）各國之個人資料保護主管機關須改善其國內之個資法體系以使該國於執行跨境個人資料保護體系可更為完善並有效率與他國之執行機關合作。

（2）發展有效率之國際間跨境傳輸個人資料之機制以促進跨境隱私機制之完善。

（3）與其他會員國發展雙邊合作機制，以確保個人資料保護機制完善。包含通知、申訴處理、事件調查之協助、資訊分享等措施。

本報告之智慧財產權歸屬於法務部

（4）與其他會員國以發展跨境個人資料保護機制為目標進行討論以及相關措施之研析。

雖然 OECD 原則上不禁止個人資料國際傳輸，但仍明列特定三種情形，禁止個人資料之國際傳輸行為。包含其他會員國顯然未遵守此指導原則；從其他會員國再輸出資料是為了規避本國隱私保護相關規範；對於在本國內受隱私保護程度較高之資料種類，該他國未提供同等程度保護等三種情形。

事實上，OECD 了解個人資料跨境傳輸並非僅牽涉區域內之利益，因此必須注意其他國際組織之作法，以達成整合並有效運作之機制。OECD 藉由了解 APEC 之作法，與 APEC 合作將其運作模式建立於 OECD 之機制內。舉例而言，APEC 建立會員國名冊，以便有效處理個人資料案件爭議之相關申訴，該會員國名冊亦透過合作方式提供與 OECD，可建立個人資料跨傳輸有效之區域合作機制。

與歐盟隱私保護指令不同，OECD 對於個人資料跨境傳輸行為基本上係不禁止的，但仍容有主管機關依法禁止個人資料跨境傳輸行為之空間。

（三）國際個資保護之爭議案例分析

1.飛航旅客紀錄（the Passenger Name Record）

由於 911 恐怖攻擊造成美國國土安全之疑慮，美國於 2001 年 11 月通過法律要求通過美國領土或者由美國領土起飛之飛機必須提供旅客名單予美國國土安全部，以作為紀錄或追蹤之用。進一步言，紀錄飛航旅客之目的主要作為犯罪偵查之用。

飛航旅客紀錄之內容包含 34 個欄位，例如姓名、住址、電話號碼、電子郵件信箱、帳戶及信用卡資料，甚至連旅客於飛機上之點餐紀錄都列入須提供之範圍。

然而，由於歐盟隱私保護指令之規範，原則上，唯有第三國被歐盟執委會認定具有適當保護措施之情況時，歐盟始同意將個資傳輸至第三國。因此，兩國間之法律規範內容即產生衝突。了解此情形後，歐盟執委會開啟與美國國土安全部（the US Department of Homeland

本報告之智慧財產權歸屬於法務部

Security, DHS）之協議，並於 2004 年達成共識，雙方並簽訂協議。[91]

飛航旅客協議之內容不以通則性為規範模式，而是透過不同之案例分析以尋求共同原則。以下簡介協議內容所提及之原則：

（1）傳輸旅客資料並加以利用時，必須合於傳輸旅客資料之目的。

（2）傳輸旅客資料時以必要為原則，不應該毫無限制地將個資內容全部傳輸。

（3）僅於特殊之例外情形下，始可使用敏感性資料。

（4）為了使個人資料保持完整及安全，必須採取適當之措施。

（5）必須由政府主管機關進行監督跨境傳輸個人資料之事宜。

（6）當旅客之個人資料傳輸至第三國時，必須通知旅客當事人。

（7）旅客有權利查閱其個人資料之內容。

（8）旅客資料保存期間僅能以傳輸旅客資料之目的內為之。

2.Google Buzz 之和解案

Google 於 2010 年發佈了 Google Buzz 之服務，該服務類似社交網站"twitter"，透過 Buzz，使用者可用簡單之介面，輕鬆發佈訊息、照片。但，美國聯邦貿易委員會（the U.S. Federal Trade Commission, FTC）指出 Google 違背 FTC 法第 5 條之內容[92]以及 Google 所公布之隱私權政策，於未獲得使用者同意之情形下，違法蒐集使用者之個人資料。除此之外，Google 也違反了安全港協議(U.S.-EU)對於個資當事人之資料進行跨境傳輸時，應盡之通知以及提供當事人選擇權之義務[93]。

Google 於事後進行檢討其作法，除了立即關閉此服務外，並對於侵犯使用者個人隱私之行為道歉，同時與 FTC 達成和解。

2011 年 5 月 30 日所公布之和解內容主要有幾項值得注意之重點。

---

[91] Maria Tzanou, Data Protection in EU Law: An Analysis of the EU Legal Framework and the ECJ Jurisprudence, in TITLE OF Personal Data Privacy and Protection in a Surveillance Era: Technology and Practices, Beginning Page 273,Page290(2011)

[92] 違反之內容包含沒有讓當事人行使同意權；未遵守公司本身對於使用者所承諾之隱私權政策；採取誤導使用者之作法違法蒐及使用者之個人資料。

[93] http://www.infolawgroup.com/2011/04/articles/enforcement/ftc-takes-a-big-step-in-privacy-enforcement-with-google-buzz-settlement/，最後造訪日期：2012 年 5 月 12 日。

本報告之智慧財產權歸屬於法務部

第一，FTC 首度要求企業執行較為明確及精密之隱私之政策以保護使用者之隱私。第二，FTC 首度對於美國與歐盟簽署之安全港協議表示明確執法之態度，FTC 要求 Google 依安全港協議之內容提供最新之安全港聲明，以確保 Google 跨境傳輸個人資料之行為合於協議之範圍。

3.歐洲推行被遺忘之權利（the right to be forgotten）

所謂被遺忘之權利主要係指若個人資料當事人發現自己之個人資料被存取於網路或者是公司之資料庫內時，可要求網站經營者或者是企業刪除其個人資料，以下以 Google 於 2008 年引發之爭議為案例說明。

Google 被發現於 2008 年 3 月至 2010 年 5 月間，透過其街道定位服務，違法蒐集位於荷蘭 360 萬個無線路由器（Wi-Fi routers）之資料。Google 因其違法蒐集資料之行為，面臨 140 萬歐元之罰款[94]。

由於荷蘭相當重視隱私保護之概念，因此 Google 之作法引起社會之爭議，在荷蘭社會反彈之壓力下，Google 於 11 月 15 日宣布，同意提供民眾將其住家地點或公司行號之無線路由器識別碼資料退出 Google 資料庫之機制，亦即供民眾行使被遺忘之權利。路由器之擁有者亦可透過更改服務設定識別碼（Service Set Identifier, SSID）之方式，退出 Google 定位服務之資料庫。荷蘭個人資料保護主管機關首長 Jacob Kohnstamm 認為，Google 所提出之改善措施對於消費者隱私之保護具有正面之幫助。

歐洲各國對於 Google 所蒐集之無線存取資料皆有隱私保護之疑慮，因此，除了荷蘭外，目前 Google 也在法國公告提供此項退出機制，未來將進一步於全球實施。

針對被遺忘之權利，目前歐洲各國有諸多討論，歐盟法正考慮將被遺忘之權利於其法律中進行規範，但由於相關規定將立即增加網路相關企業經營者之負擔，因此仍須進一步觀察其後續發展。

[94] Google 所提供的定位服務主要是透過所蒐集之資訊，提供其開發的 Android 手機定位服務，利用所蒐集的定位資料使行動電話或者行動裝置之用戶得以定位其所在之位置，並且提供用戶當地氣象以及地圖資訊。除此之外，定位服務也增加 Google 對鄰近商號之廣告收益。Google 實施退出資料庫之機制後，其必須另外以 GPS 系統進行定位，定位服務可能將發生不精確之情形，另外，也將使得行動裝置因需搜尋衛星訊號而耗費較多電力。Google 全球隱私顧問 Peter Fleischer 指出，事實上 Google 的定位服務無法辨識個人資料，但 Google 認為提供退出資料庫機制更增進對於個人隱私之保護。

本報告之智慧財產權歸屬於法務部

4.Facebook 之和解案

社群網站對於隱私權保護之侵害疑慮，進幾年來已多受討論，但是隨著社群網站融入人們之社會活動越深，其對於隱私權保護之重視也應順應加強以符合各國或各國際組織之規範。

從臉書設立之初，其對於隱私權保護之政策即成為各界檢視之重要對象。2011 年美國聯邦貿易委員會（the U.S. Federal Trade Commission，FTC）認為臉書並未完善執行使用者個人資料及隱私之保護措施，並且於未獲得當事人同意之情形下，將使用者之個人資料傳輸給應用程式之開發商，此舉已嚴重侵害使用者對其個人資料之控制權，對此，FTC 要求臉書進行改善並且於未來 20 年內，每兩年必須執行內部隱私保護措施之稽核程序。

本爭議其實也暴露美國對於個人資料保護法制之不足，對此，美國政府以及國會正推動多項網路安全法案，希望得以規範由於網路時代興盛而導致之相關問題。[95]

5.雲端科技所引發之個人資料跨境傳輸議題

雲端科技發展後，個人資料跨境傳輸之議題愈發重要，國際間對於如何管理雲端上之個人資料亦有多項討論。澳洲研究上指出，使用雲端服務者中，70%之使用者皆不清楚其個人資料存放之位置。

以澳洲為例，雲端服務之提供者促請澳洲政府對於個人資料存放於雲端議題進行解釋以及相關立法規範，主要原因在於，若服務提供者無法信賴其所使用之雲端服務的隱私權保護作法，那麼即有可能降低其使用雲端服務之意願，為了加強雲端產業之利用，政府應針對相關議題訂定規範，以確保使用者之個人資料受妥善之保護，亦能對雲端服務之使用具信心[96]。

再以蘋果推出之雲端服務(icloud)為例，由於蘋果產品熱賣，搭配 iphone、ipad 之使用，蘋果也於去年開始提供 icloud 雲端服務。隨著

95 http://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html，最後造訪日期：2012 年 5 月 12 日

96 http://www.cso.com.au/article/422490/australian_concerned_about_personal_data_drifting_offshore_/?fp=4&fpid=959105 ,最後造訪日期:2012 年 5 月 12 日。

本報告之智慧財產權歸屬於法務部

雲端服務使用之人數增加，個人資料保護議題也隨之受到各界關注。主要受到疑慮之處在於，資料當事人對於其個人資料之掌控度不足，服務提供者所採取之相關措施透明度也不高。此違反歐盟隱私保護指令之透明以及當事人資料自主權之原則。對於使用者而言，了解資料處理者如何處理、將資料傳送至何處以及資料儲存地等內容係相當重要的。以歐洲之使用者為例，當其使用蘋果之雲端服務時，其存放於雲端資料庫之個人資料即可能發生跨境傳輸之情形。對此，蘋果必須妥善掌控資料流動過程並且僅能將個人資料傳輸至歐盟執委會認為具備妥善個人資料保護措施之地。[97]

對於雲端產業個人資料保護議題也為近來頗受矚目之焦點，不只是國外，包含我國之相關業者也呼籲政府提出相對應之法規範，使產業界可遵循，亦使使用者對雲端服務更具信心[98]。因此，各國以及國際組織對其法規範發展，仍有待吾人持續觀察，以促進雲端產業之發展。

（四）建議政府可採取之方式及作法

1.規範時須考量社會、科技發展以及企業可遵循之程度

國際組織雖對於跨境傳輸個人資料之機制皆有所著墨，但其建立之目標並不在削減各國政府建構個人資料保護法之權利。只是，隨著全球經濟以及犯罪偵查活動等機制之發展，個人資料跨境傳輸之情形只會越來越普遍。國內法規範個人資料跨境傳輸之作法也必須隨著當時之社會、科技背景而作調整。以雲端產業之發展為例，政府近來鼓勵雲端產業之發展，但雲端科技涉及個人資料跨境傳輸之部分，產業界必須倚靠國內政府以及國際組織所提出之明確規範為之，以遵循相關法令規範。另外，訂定跨境傳輸之相關法規範時，也必須考量中小企業可遵循之程度，以免造成企業負擔過大成本之壓力[99]。

2.制定跨境傳輸之法規範時，須要求當事人注意其跨境傳輸法規範之透明

97 http://www.businesscomputingworld.co.uk/combating-the-legal-data-protection-risks-of-apples-icloud/ , 最後造訪日期:2012 年 5 月 12 日。

98 詳見台灣雲端運算產業協會向行政院提出產業發展建言「建構台灣雲端運算產業良好環境之建言芻議」http://www.twcloud.org.tw/Cloud/news2.do?id=2011041312f4ce53bc9178f&place=1

99 Christopher K Christopher Kuner, Regulation of Transborder Data Flows under Data Protection and Privacy Law,OECD Digital Economy Papers No.187,page 8

本報告之智慧財產權歸屬於法務部

性要求以及提供同意權行使之管道，並設立窗口。

政府制定個人資料跨境傳輸之相關法規範時，必須注意其透明性，所謂透明性係指個人資料保護之主管機關須設立窗口供資料當事人申訴或者表達意見之用，除此之外，當個人資料被傳輸至國外，政府應要求資料管理者公布個人資料儲存地以及接受個人資料組織之相關資料供資料當事人查詢。

關於當事人同意機制之作法，政府必須考量其實際施行之情形。由於網際網路使用之普遍，雖然許多網站於傳輸個人資料前會以網頁勾選之方式獲得當事人之同意，但此作法實有須進一步檢討之空間。尤其我國政府目前將發展雲端科技視為國家科技政策重要之一環時，對於個人資料之保護更是應該多予注重。當事人使用雲端科技時，其個人資料即可能發生跨境傳輸之情形，縱使當事人已經於使用雲端服務前同意將個人資料跨境傳輸，也可能發生事實上當事人對於其個人資料之儲存地、接受者為何亦無法掌握，因此，除了獲得當事人之同意外，網路服務提供者也必須將相關資訊公布予使用服務之人了解，以確保當事人可確實行使其同意權。

除了資料當事人不知如何行使其個人之權利外，對於個人資料受跨境傳輸之個人而言，一旦其個人資料遭受外洩而發生相關權利受損情形時，當事人並不了解應以何法條主張其權利，另外，當事人也不知道應該向哪一主管機關聯絡。對此，建議我國政府於思考跨境傳輸個人資料之相關法制度時，應秉持透明公開原則使人民知道如何行使其權利。

另外，由於科技以及國際組織對於個人資料跨境傳輸之作法可能隨著時間作出不同之修正及改變，建議政府於訂定相關跨境資料傳輸規定後，應定期檢視法規範之內容是否符合當時科技之要求。此外建議各中央目的事業主管機關須設立窗口並且對外公告，使資料當事人對於跨境傳輸其個人資料有相關申訴或者請求時，知道可尋求哪個單位之協助。

3.加強國際合作機制

事實上，隨著個人資料跨境傳輸之情形越來越普遍，以地理上或者國家領土作為規制之界限已越發模糊，因此，政府於思考個人資料

本報告之智慧財產權歸屬於法務部

跨境傳輸議題時，必須考量國際組織之作法，不可儘將眼光鎖定於國內法規制範圍，以增進個人資料國際傳輸機制之完善，如此始能有效運作個人資料跨境傳輸機制。

各國際組織與國家雖然對於個人資料跨境傳輸訂有相關規定以及機制，但各國政府間對於個人資料跨境傳輸之作法以及管制措施皆有不同。有些主管機關要求國內之業者或機關於跨境傳輸個人資料前，必須向主管機關登記。另以加拿大個資法為例，其係要求傳輸個人資料者須採取相關措施確認，並無須向主管機關登記之要求。

對此，國際上已有相當聲音希望建構全球性之個人資料跨境傳輸機制。2009 年，馬德里決議（the Madrid Resolution）[100]提出個人資料及隱私保護國際標準（International Standards on the Protection of Personal Data and Privacy)希望透過本標準建立全球性之個人資料隱私保護以及跨境傳輸之標準。標準內指出將個人資料跨境傳輸時，個人資料之接受者必須採取適當之保護措施以確保個人資料受妥善管理。另外，馬德里決議也接受個人資料接受者可採取歐盟之共同約束條款（the Binding Corporate Rules)或者簽訂標準契約(Contractual Clauses)之方式，作為個人資料保護之措施。除此之外，馬德里協議也建議各國之個人資料保護主管機關可於個人資料跨境傳輸前，須經由主管機關核可使得為之。

4.政府應建立跨部會之組織或者設立相關人才與資源以確實執行跨境傳輸制度

雖然國際間對於個人資料跨境傳輸之議題多所討論，但，事實上，許多國家之個人資料保護主管機關並無資源以及人員可以執行跨境傳輸個人資料之機制。歐盟曾經於其會員國間進行調查，27 個會員國間，有 11 個會員國之個人資料保護主管機關表示，國內並無相關資源以及人才可以確實執行個人資料跨境傳輸之機制。據此，若要配合我國對於個人資料國際傳輸之法規範以及國際組織之作法，中央目的事業主

[100] 馬德里決議於 2009 年 11 月作成，該決議主要係於第 31 屆個資保護以及隱私專責機構國際會議（the 31st International Conference of Data Protection and Privacy Commissioner in Madrid）所作成。超過 50 個國家支持馬德里決議就國際隱私保護標準之內容，希望能夠達成整合國際隱私法制規定之目標。除了各國之專責機構參與該會議外，Google 以及 Facebook 等大型網站業者亦參與此會議，因此該會議充分蒐集各國政府專責機關以及業者之意見，使結論具有代表性。

本報告之智慧財產權歸屬於法務部

管機關必須培養相關人才得以掌握國際間對於個人資料跨境傳輸之作法，以求得確實執行跨境傳輸之機制。

5.我國個資法目前對於國際傳輸之規範以及國際規範模式

我國個資法對於企業之個人資料國際傳輸之規定僅見於新修正之個資法第 21 條[101]。第 21 條僅規範四種中央目的事業主管機關得限制之情形，包含涉及國家重大利益、國際條約或協定有特別規定、接受國對於個人資料之保護為有完善之法規致有損當事人權益之虞、以及以迂迴方法向第三國（地區）傳輸個人資料規避本法等四種情形。

至於公務機關跨境傳輸個人資料之規範，於尚未施行之新修正個資法規定內並無說明。以現行之電腦處理個人資料保護法第 9 條之規定為例，公務機關對於個人資料之國際傳遞及利用，應依相關法令為之，觀諸修正理由之說明，新修正之個資法未沿用電腦處理個人資料保護法之規定理由在於公務機關執行法定職務，將個人資料作跨國（境）之處理或利用，本即依相關法規辦理，無庸特別規定。

對於跨境隱私之規範模式，觀察國際趨勢後大致可分為兩種類型。第一種類型接近我國目前之立法模式，即是原則上同意機構可進行個人資料之跨境傳輸，但於例外情形時則限制個人資料傳輸行為[102]。另外一種規範模式則是設立許多法規範要件，於進行個人資料跨境傳輸行為前，須符合相關要件始可為之，兩種規範模式都有其利弊。

以第一種規範模式為例，為使跨境傳輸個人資料之行為不侵犯當事人之隱私權及個人資料，必須於該機制中鼓勵建立相關自律性措施，並且須要對於跨境傳輸所引起之損害事件於法規範中明確訂定相關之損害賠償規範。而對於第二種之規範模式而言，由於嚴格之法規範要求往往於執行上產生無效率、行政成本過高之情形，因此，建議於我國政府於法規範要求上不要有過多之行政登記要求，並且應鼓勵須跨境傳輸個人資料之非公務機關採取機構式之跨境傳輸機制（organizationally-based data transfer mechanisms），例如歐盟之共同約

[101] 新修正之個資法尚未實施，其實施日期有待行政院指定。

[102]以 NCC 通訊傳播委員會日前所發佈之行政函釋為例，通傳會於 2011 年 9 月 21 日預告訂定「限制非公務機關國際傳遞個人資料之命令」，預告將規範通訊傳播事業於國際傳遞即利用個人資料時，應考量接受國家及地區對個人資料有完善之保護法令，而其經衡酌大陸地區之個人資料保護法令尚未完備，故限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區。

本報告之智慧財產權歸屬於法務部

束條款或者 AEPC 跨境隱私規則之作法等，採取機構自律之方式，以收個人資料保護之效果。

6.建議我國政府應採取之方式

如前所述，我國於個資法中已針對個人資料之國際傳輸進行規範。亦加入 APEC 跨境隱私規則機制之實驗小組內，希望能透過國際參與之方式，推動個人資料跨境傳輸活動，並符合國際組織之隱私保護要求。由於我國並未被歐盟執委會認定為具有合適個人資料保護措施之地區，因此，若我國之組織欲從歐盟會員國之地區接收個人資料時，必須注意其他之機制包含與資料傳輸者簽訂模範契約條款之方式或者是採取共同約束條款之方式。另外，亦可比照美國與歐盟間所建立之安全港模式，與歐盟會員國簽訂安全港協議，以符合歐盟隱私權保護指令之要求。

除了持續參加 APEC 所建立之跨境傳輸機制外，對於非 APEC 會員經濟體之地區，建議透過雙邊擬定安全港架構或者簽訂合作備忘錄之方式，建立與他國間之個人資料傳輸跨境合作。透過安全港架構以及合作備忘錄之簽訂，可確保雙邊之合作內容、擬定跨境傳輸之必要注意原則、建立聯絡窗口等相關機制之健全，亦可使國內須要進行個人資料跨境傳輸之企業、組織以及個人有明確之法規範可依循。

（五）跨境傳輸個人資料之契約範本

依歐盟目前之作法為例，位於歐盟會員國內之資料傳輸者於跨境傳輸個人資料時，為了確保資料當事人之權益，以及要求資料接受者依歐盟隱私保護指令處理以及利用所接收之當事人資料，歐盟公布三個模範契約條款。以下所見之契約條款主要係引自歐盟 2010 年 2 月 5 日所公布之模範契約條款(on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under Directive 95/46/EC of the Ruropean Parliament and of the Council)。目前，我國政府並未提供相關契約範本供參考，藉由參考歐盟之作法，可給與吾人一些思考之方向。以下提供歐盟之標準契約條款以及其中譯內容。

本報告之智慧財產權歸屬於法務部

Clause 1
Definitions

For the purposes of the Clauses:

(a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ;

(b) ‘the data exporter’ means the controller who transfers the personal data;

(c) ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive95/46/ec

(d) ‘the sub-processor’ means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) ‘the applicable data protection law’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) ‘technical and organisational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

第一條
定義
以下定義相關名詞：
（a）個人資料、特種個人資料、處理、資料控制者、個資處理者、資料當事人以及監督機關之定義與歐盟個人資料隱私保護指令相同。
（b）資料輸出者，係指傳輸個人資料之資料控制者。
（c）資料進口者，係指同意接收個資者，且其位處之地區並不被歐盟認為具有適當個人資料保護措施之地區。
（d）受委託之處理者，係指於個資傳輸過程中受資料進口者委託或者依資料輸出者委託處理者皆屬之。
（e）可適用之資料保護法係指資料輸出者所位處之會員國內與保護基本人權、自由以及與隱私保護相關之法律。
（f）技術以及組織之安全措施，係指採取該措施之目的在於防止不法侵害、個人資料外洩、遭更改、無權揭露或者查詢個人資料等行為。特別是利用網

本報告之智慧財產權歸屬於法務部

路傳輸個人資料時，而必須採取之相關措施。

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

第二條
傳輸之細節
關於特種個資之傳輸規定將於附加條款中進行規定。

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

第三條
第三方利益條款
1.資料當事人得依照本契約條款、第 4 條（b）至（i），第 5 條（a）至（e）以及（g）至（j），第 6 條（1）至（2），第 7 條，第 8 條（2）以及第 9 條至第 12 條向資料輸出者行使第三人利益契約之請求權。
2.萬一資料當事人無法向資料輸出者行使第三人利益契約之契約上請求權時，資料當事人得依照本契約條款，第 5 條（a）至（e）以及（g），第 6 條，第 7 條，第 8 條（2）以及第 9 條至第 12 條向資料進口者行使第三人利益契約之請求權。
3.萬一資料當事人無法向資料輸出者以及資料進口者行使第三人利益契約之契約上請求權時，可依本條款，第 5 條（a）至（e）以及（g），第 6 條，第 7 條，第 8 條（2）以及第 9 至第 12 條。

本報告之智慧財產權歸屬於法務部

4.於資料當事人同意以及該國之訴訟法允許時，資料當事人可提起團體訴訟。

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses; EN 12.2.2010 Official Journal of the European Union L 39/11

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

第四條

本報告之智慧財產權歸屬於法務部

資料輸出者之義務

資料輸出者同意並且保証以下事項：

（a）處理個人資料，包含傳輸行為，將遵守會員國以及歐盟所有關於個人資料保護之相關法律規範。

（b）於個人資料傳輸之期間，資料輸出者將指導並要求資料出口者遵守有關於處理個人資料之相關法律規範。

（c）資料輸出者保證採取技術以及組織上之安全措施。

（d）於衡量法規範之要求後，將採取適當之技術以及組織上之作法以避免個人資料因意外滅失、毀損、遭竄改、未經授權之揭露或查詢。特別是透過網路傳輸個人資料時，將採取相關資訊安全措施以保護資料之安全以及完整性。

（e）遵守其所欲採取之安全維護措施。

（f）若跨境傳輸之內容包含特種個人資料時，必須於傳輸時、傳輸前或者於傳輸後盡速通知資料當事人，通知內容必須包含告知當事人其將把當事人之個人資料傳輸至未具有適當安全措施之區域。

（g）當受委託處理個人資料之機構依第 5 條（b）以及第 8 條（3）通知資料輸出者相關事項時，資料輸出者作出繼續傳輸或者停止監督之決定時，資料輸出者將相關內容同時通知該國之個人資料保護專責機構。

（h）資料當事人可以向資料傳輸者要求本契約之條款之複印本，其並可要求資料傳輸者說明其所採取之技術以及組織上之安全措施。若契約中含有其他與個資無關之商業協議，資料輸出者可予以刪除並提出之。

（i）若有委託他人處理個人資料之情形時，確認受委託者亦採取相同程度之保護措施。

（j）將會遵守第 4 條（a）至（i）之規定。

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

本報告之智慧財產權歸屬於法務部

i.any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

ii.any accidental or unauthorised access; and

iii.any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

第五條

資料進口者之義務

資料進口者同意並且保証以下事項：

（a）遵守資料輸出者之要求以及本契約條款之約定。若資料進口者因任何理由無法提供相同規格之措施時，將通知資料輸出者其無法達成之原因，以便資料輸出者作出是否繼續進行跨境傳輸之決定。

（b）如果資料進口者之國家修改相關個人資料保護法之法規而使資料進口者可免除本條款之要求或者資料輸出者之要求時，須通知資料輸出者相關訊息，以利資料輸出者作出是否繼續傳輸個人資料或者終止本傳輸契約之決定。

（c）資料進口者將於資料傳輸前，於其組織內部採取技術以及組織上之安全措施。

（d）於以下情形發生時，將立即通知資料輸出者：

i.依法向法律執行機關揭露當事人個資之情形。

ii.個資外洩事故以及未經授權之存取行為發生時。

iii.對於個資當事人之要求未及時回覆時。

（e）對於資料輸出者之個資專責機關之要求會立即且適當處理之。

（f）將依本契約條款接受由資料傳輸者對於資料進口者或由資料輸出者或者輸

本報告之智慧財產權歸屬於法務部

出者國家之個人資料專責機關所挑選出之獨立稽核機構之稽核要求。
（g）資料當事人可向資料進口者要求其與傳輸者間、其與受委託處理個人資料者間之契約複本，但若契約內容含有與個人資料傳輸無關之商業機密條款時，資料進口者可予以刪除。
（h）若發生委託處理個人資料之情形時，資料進口者應先取得資料輸出者之書面同意。
（i）受委託處理個人資料者進行個人資料處理之服務將依循第 11 條之規定。
（j）若與受其委託處理個人資料者達成相關協議時，將依循與個資傳輸者之契約約定盡速傳送條款內容予資料傳輸者。

Clause 6
Liability

The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses. EN 12.2.2010 Official Journal of the European Union L 39/13

第六條
契約責任
1.若資料當事人因第 3 條或者第 11 條所提及之原因或者因受委託處理個資者之不當行為而遭受損害時，雙方同意由資料傳輸者負損害賠償責任。
2.若個資當事人依前項向個資輸出者請求損害賠償，卻發生因資料傳輸者無資力而無法賠償個資當事人之情形時，資料進口者同意個資當事人可向其主張損害賠償責任。

本報告之智慧財產權歸屬於法務部

個資出口者不得以係受委託處理個人資料者之問題予以抗辯，進而逃避損害賠償責任。
3.若因資料輸出者以及資料進口者無資力，使個資當事人無法依前兩項之條款向個資輸出者以及個資進口者獲得損害賠償時，個資當事人可向受委託處理個人資料者請求損害賠償責任。

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

第七條
和解、調解與管轄權條款
1.於個資當事人依法或依本契約條款請求損害賠償時，資料進口者將接受個資當事人所提之條件。
（a）與調解有關之衝突，可透過仲裁或者個資專責機關予以解決。
（b）個資輸出者國家之法院具有審判權。
2.契約當事人同意不侵害個資當事人依國家或者國際組織之條款可請求之程序以及實質上之損害賠償責任。

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

第 8 條

本報告之智慧財產權歸屬於法務部

與個資專責機關之合作

1.若相關法律要求資料輸出者將契約複本存放於個資專責機關時，資料輸出者同意將契約複本存放於個資專責機關。

2.契約雙方同意個資專責機關有權對資料進口者以及受委託處理個人資料者進行稽查。

3.若有相關免於稽查之法規或者約定時，資料進口者必須立即通知資料輸出者相關規定，使資料輸出者可以作出是否繼續傳輸個人資料之決定。

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established,
namely .....
.....

第 9 條

準據法

本契約條款之準據法依循資料輸出國所在地之法律。

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

第 10 條

契約變更

雙方同意不更改契約條款。但只要在不與本契約條款發生衝突之情形下，雙方可增加與業務有關之條款約定。

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses . Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent

本報告之智慧財產權歸屬於法務部

and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely.....

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

第 11 條

委託處理個人資料

1.於未獲得資料輸出者之書面同意前，資料進口者不得轉包個人資料之處理程序予他人。於資料進口者同意後，受委託者必須於資料輸出者之同意範圍內，依循個人資料進口者依本契約所應盡之保護義務。若受委託者未於資料輸出者之同意範圍內完成相關之要求時，資料進口者應對資料輸出者負全部之法律責任。

2.資料進口者與受委託處理個人資料者間所簽定之契約亦應包含利益第三人條款，以避免個資當事人因資料輸出者無資力而無法請求損害賠償之情形，受委託處理個資者之責任僅限於其所經手處理之程序為限。

3.受委託處理個人資料者應依個資輸入者所應遵守之個人資料法規。

4.資料輸出者應依循第 5 條（j）之說明，於資料進口者通知個人資料委託是向後，保留受委託協議之複本至少一年。相關複本應可被資料輸出者國內之個人資料專責機關所調閱。

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

第 12 條

個人資料處理服務中止後之義務

1.除非有其他法律規定之情形，雙方同意於資料處理服務終止後，資料進口者與受委託處理個人資料者應依資料輸出者之要求採取返還所有傳輸之個人資料以及相關複本或返還、銷毀所有傳輸個資之措施。

2.資料進口者以及委託處理個人資料者承諾於資料輸出國及其國內之個人資料

本報告之智慧財產權歸屬於法務部

保護專責機關要求後，將其所採取之措施交由資料輸出者以及個資專責機關進行檢視。

二、APEC 跨境隱私國際執行合作文件

（一）前言

本跨境執行文件與撰寫主要依循亞太經濟合作組織（Asia-Pacific Economic Cooperation，以下簡稱 APEC）目前所提供之相關文件為之。APEC 目前透過跨境隱私規則(Cross Border Privacy Rules，以下簡稱 CBPRs)推動個人資料跨境隱私事宜。透過設計一連串的制度，提供企業經營者得以建立其內部之跨境資料傳輸規則，並且透過認證機制[103]（主要為公正第三人之專責機構 Accountability Agents）之建立，使企業得以提供消費者可信之標章。

CBPRs 系統僅供於 APEC 會員國向其他 APEC 會員經濟體跨境蒐集或接受個人資料時使用。CBPRs 要求組織發展其跨國隱私保護之企業內部規則，該規則必須透過公正第三人（Accountability Agent）認證其符合 CBPRs 之最低要求後，始可跨國傳輸個人資料。一旦企業內部所制定之跨境傳輸規則被認證後，將會約束企業本身，同時，該會員經濟體國內之管理者，例如隱私主管機關，也將要求企業執行該項隱私政策。

為了達成 APEC 隱私保護綱領鼓勵個人資料跨境傳輸之精神，APEC 於 2010 年六月提出了可供雙邊、或多邊協議之跨境隱私合作執行文件範本（APEC Cross-Border Privacy Enforcement Arrangement）[104]，提供會員國間為犯罪調查、隱私權執行案等跨國資料傳輸個人資料之用。另外，透過制式表格之填寫，使會員經濟體間可執行有效率之個人資料跨境傳輸活動。

跨境隱私合作執行文件是 APEC 開路者機制（pathfinder）為達成隱私保護綱領之要求所研究之產出，另外，開路者機制亦利用跨境隱私規則之建立，增進個人資料國際傳輸之應用。故，本跨境隱私合

[103] 公證認證機制必須具備兩項基本功能，其一為認證企業已依 APEC 隱私保護綱領建立其內部之跨境隱私規則，其二為該機制必須提供爭端解決並且供消費者可投訴其個人資料受侵害情事之管道。公正認證機制不限制各國個人隱私主管機關，亦包含已於會員經濟體內建立良好信譽之隱私標章系統，以及符合其業務執行類政府單位（政府機關、消費者保護機構、隱私標章發放機構）。資料來源：APEC Data Privacy Pathfinder Projects Implementation Work Plan.

[104] 簽署之國家包含澳洲、加拿大、香港、中國、紐西蘭以及美國。

本報告之智慧財產權歸屬於法務部

作執行文件主要希望促進以下目的：

1.APEC 會員經濟體內之個人隱私執法機關之合作

2.建立個資隱私保護機關的合作機制，包含調查、執行之合作

3.推動跨境隱私規則 CBPRs 之利用

4.除了 APEC 會員經濟體外，本跨境隱私合作協議也鼓勵非會員國分享與交流個人資料跨境執行與調查行動。

跨境隱私執行文件目的在於建立實用之多邊合作機制，APEC 希望其所有之會員經濟體皆可參與本跨境隱私執行機制，該機制於文件後附上標準表格，提供跨國個人資料傳輸所需利用之表格，本報告將於後分別說明之。

依目前 APEC 對於個人資料跨境隱私機制之設計，事實上，為了有效率地促進各國間對於個人資料跨境傳輸之行為，APEC 於跨境隱私機制之設計上並不要求各會員經濟體以分別訂定雙邊或多邊協議之方式為之。基本上，根據 CBPRs 機制之設計，只要各會員經濟體以該機制之設計具備相關要件後，即可進行個人資料跨境傳輸行為。不過，APEC 開路者計畫亦鼓勵會員經濟體間以合作協議文件之方式，對於兩國間之跨境傳輸行為進行合作，本報告亦於後面章節草擬 APEC 跨境隱私國際執行合作備忘錄草稿供參。

（二）APEC 跨境合作備忘錄（Memorandum of Understanding）

1.簽署合作備忘錄之主體

（1）本合作協議係成立於中華民國行政院經濟部商業司（例）與_____間

（2）中華民國行政院經濟部商業司係其業管行業之中央目的事業主管機關，依中華民國個人資料保護法之設計，掌管業管行業遵循個資法要求之相關事務。

（3）（說明簽署備忘錄他方機關之性質以及遵循之法令為何）

2.本合作備忘錄之目的

（1）增加雙方對於個人資料保護以及傳輸事宜之活動

本報告之智慧財產權歸屬於法務部

（2）促進犯罪偵查以及執行之跨境傳輸活動

（3）協助雙方針對相關事宜進行教育訓練、經驗分享以及政策制定之合作

（4）符合 APEC 隱私保護框架之要求

（5）符合 OECD 對於跨境傳輸個人資料之相關規範

3.本合作備忘錄之效力

（1）本合作備忘錄以不違反國際條約及雙方國內之個人資料保護法為前提。

（2）本合作備忘錄若有定有相關附件，並不包含於合作備忘錄所協議之範圍內。

4.本合作備忘錄之期限

（1）於本合作備忘錄簽署後兩年內，雙方應執行相關協議內容

（2）若其中一方欲終止本合作備忘錄，應通知他方。

（3）於雙方同意之情形下，可延長本合作備忘錄之期限。

5.本合作備忘錄遵循之國際組織對於隱私保護之原則

本合作備忘錄遵守 OECD 隱私保護以及跨境傳輸個人資料指令、APEC 隱私保護框架。除此之外，本合作備忘錄將持續關注國際間對於跨境個人資料傳輸機制之相關發展。

6.本合作備忘錄之連繫窗口

（1）將定期召開雙邊會議，以共同協商擬定合作方針。

（2）召開雙邊會議時，建議邀請專家與會提供跨境個人資料傳輸之專業意見，並進行意見分享。

7.資訊共享

（1）針對跨境個人資料傳輸之共同議題、重大爭議事件等，雙方皆應進行資訊分享，除此之外，資訊分享之內容建議包含政策研究、

本報告之智慧財產權歸屬於法務部

隱私議題研究、教育訓練機制研究與經驗、執行方向、自評及外部稽核機制、共同進行犯罪偵查事項、重大隱私政策議題、資訊安全問題及技術、國內個資法修正報告以及個資法規範執行經驗等。

（2）為促進雙方之資訊分享機制，雙方應共同成立小組並且設立聯絡窗口。

8.犯罪偵查以及執行之跨境合作

為犯罪偵查及執行事項而須進行跨境傳輸個人資料時，必須提供申訴窗口供資料當事人主張。除此之外，必須建立申訴處理機制以迅速並有效處理資料當事人之意見。

9.定期稽核與自我檢視機制

針對隱私保護機制所設計之外部稽核、內部稽核以及隱私衝擊評鑑等機制與方法論，雙方應提供對方參考。

10.以符合雙方國內之個人資料保護相關法制為前提，簽署本合作備忘錄

為符合雙方之國內法規範，雙方可限縮本合作備忘錄之協議範圍。針對有爭議之偵查或執行案件，協商時，應以雙方之最大利益為之。

11.人員交換及訓練之派遣機制

為加強雙邊合作，雙方應派遣其相關主管機關之人員至他方進行經驗交流、分享以及教育訓練。

12.費用

（1）支出費用若係為符合本合作備忘錄之內容，由雙方自行負擔。

（2）若係請求他方協助傳輸個人資料時，應協調以分擔或移轉所花費之費用。

13.保密協定

本報告之智慧財產權歸屬於法務部

請求他方傳輸個人資料後，應符合請求協助之目的以利用所接收之個人資料。

14.爭端解決機制

雙方應成立爭端解決小組以處理爭議案件。

15.啟動修改本合作備忘錄之要件

（1）雙方於任何時間都可要求修改本合作備忘錄。

（2）於本合作備忘錄生效 18 個月後，雙方可各自指派代表共同檢視本合作備忘錄，並於適當之情形下，合意修改本備忘錄。

雙方代表簽名：

（三）關於請求他國政府協助之表格（Request for Assistance Forum）

Data of the request:

1.Case Name 案例名稱

2.Authority Contact Details 主管機關之聯絡窗口

From:

表 31：請求他國政府協助之表格 1

Requesting Authority, Economy 請求協助之會員經濟體	
Contact Person, Title 連絡負責人	
Telephone 電話	
Email Address 電子郵件信箱	
Postal Address 郵遞區號及地址	

資料來源：資策會科法所自行製作

本報告之智慧財產權歸屬於法務部

To:

表 32：請求他國政府協助之表格 2

Receiving Authority, Economy 接收協助請求之會員經濟體	
Contact Person, Title 連絡窗口	
Telephone 電話	
Email Address 電子郵件信箱	
Postal Address 郵遞區號及地址	

資料來源：資策會科法所自行製作

3.Confidentiality Requirements 請求事項之保密項目

4.Assistance Requested 請求協助內容

5.Time and Manner of Response 回應請求時間及其方式

6.Organization(s) Involved 相關組織

表 33：相關組織表

Name 組織名稱	
Address/URL 地址	
Contact Person, Title 連絡窗口及職稱	
Telephone/Email Address 電話及電子郵件信箱	

本報告之智慧財產權歸屬於法務部

Principal Activities 組織活動內容	
Any Additional Background Information:其他備註事項	

資料來源：資策會科法所自行製作

7.Individual(s) Involved 相關資料當事人

表 34：相關資料當事人表

Name 姓名	
Address/URL 地址	
Contact Person, Title 連絡人	
Telephone/Email Address 電話	
Principal Activities 相關活動註明	
Any Additional Background Information:其他備註事項	

資料來源：資策會科法所自行製作

8.Background and Status of the Investigation 調查事項之背景

9.Type of Privacy Principles at Issue 自我檢視是否可能違反 APEC 所有之隱私保護原則

Include All APEC Privacy Principles (Preventing harm/Notice/Collection Limitation/Uses of Personal Information/Choice/Integrity of Personal Information/Security Safeguards/Access and Correction/Accountability/)

本報告之智慧財產權歸屬於法務部

10.Possible law violations, potential sanctions, on-going proceedings and contemplated proceedings 可能違反之相關法規範說明

11.Other Relevant Information 其他相關資訊

（四）我國政府聯絡窗口表格（Contact Point Designation Form）

Contact Point Designation Form

Economy Name 會員經濟體名稱: Date 日期:

Contact Point

表 35：我國政府聯絡窗口表

Privacy Enforcement Authority 隱私主管機關	
Name 機關名稱	
Title/Position 頭銜/職稱	
Address 地址	
Telephone 電話	
Fax 傳真	
E-mail 電子信箱	
Website Address 網址	

資料來源：資策會科法所自行製作

本報告之智慧財產權歸屬於法務部

（五）我國之個人資料保護執行機關與個資保護措施及相關政策之說明

Summary statement of Privacy Enforcement Authority enforcement practices, policies and activities 簡述個資保護執行機關之執行狀況、政策以及行動

This form seeks to capture in summary form the enforcement jurisdiction and policies of each Participant in the APEC Cooperation Arrangement for Cross-Border Privacy Enforcement. The information will usually be posted on the relevant Participant's website and, when available, at a central reference point maintained by the Administrator.本文件主要簡述並歸納參與跨境隱私規則制度之執行機關政策作法。相關資訊必須公布於個資保護執行機關之官方網站上，並且得以使公眾查詢之。

Privacy Enforcement Authority name 隱私主管機關:

Economy 會員經濟體:

Website address 網址:

Key law(s) enforced by your authority 國內所使用之個人資料法制:

(Consider including a link to the relevant legislation)請附上相關法律之連結

General sectors/jurisdictions regulated by your authority 相關隱私保護機關:

(Public sector, private sector, a particular industry sector? Do you operate in a particular geographical jurisdiction such as a state or

本報告之智慧財產權歸屬於法務部

province?)公部門?私部門?相關部門是否以地理作為管轄劃分之標準?

Approach to investigation / resolution of enforcement matters 調查及執行事項之內容:

(What are your key enforcement activities or roles? For example, do you receive complaints, grant approvals, investigate, mediate or make determinations on matters? Broadly speaking, what are your investigation processes? What are your enforcement powers?) 主要執行活動之內容為何?舉例而言，組織是否處理抱怨、准許、調查或者調解相關爭議？廣泛而言，調查之內容為何？

Prioritization policies 隱私主管機關所提供之相關執行要點說明:

(Does your authority have a policy on the prioritization of enforcement matters it is willing to handle? If so, please provide a link to your current policy)對於執行事項，組織是否有優先處理之情形？若有，請提供相關政策之連結。

Other relevant information 其他相關事項:

(Are there any restrictions on how your agency can cooperate on enforcement? Are there any circumstances in which your agency may be required by law to provide information obtained under the Cooperation Arrangement to a third party?)對於執行事項是否有相關限制，是否具有依合作協議提供個人資料予第三方之情況？

（六）結論

國內於 2010 年 5 月 26 日修正公布之新版「個人資料保護法」，為協助企業因應法制遵循的壓力，提升隱私保護能力，政府機關積極參與國際相關組織(如 APEC 亞太經濟合作組織)，希冀遵循跨境隱私要求及相關機制以與國際之要求接軌，並降低產業跨境資料傳輸之風險，提升我國產業之國際形象。

本報告之智慧財產權歸屬於法務部

APEC 電子商務指導小組暨跨境隱私之次級小組會議，了解目前國際組織跨境隱私相關機制之推行現況，同時掌握國際隱私保護最新發展趨勢，足資作為個人資料管理制度建置與推行之參考。我國已於 2011 年向 APEC 成員進行介紹我國目前對於個人資料保護制度之相關發展情形，使 APEC 會員國了解台灣對於個人資料保護之重視程度，相信有助於後續制度包含跨國相互承認的推動。

由於 2011 年所召開之 APEC 會議已通過針對跨境隱私保護所推動之資料隱私開路者倡議計畫之所有文件，並經各會員經濟體討論與承認。雖然 APEC 會員經濟體採認 CBPRs 制度，不必然表示經濟體有參與 CBPRs 制度之義務，惟未來跨境隱私議題發生時，國內之公務機關與非公務機關，仍將面臨來自 APEC 及會員經濟體之國際壓力。故如何使個人資料管理制度符合國內個人資料保護法規之要求，並進一步契合 APEC 等國際組織之最新發展，將是後續國內在隱私保護推動上，所須正視的重要課題。

本報告之智慧財產權歸屬於法務部

陸、資料隱私及資訊透明國際研討會

一、前言

我國前年（民國 99 年）三讀通過新版個人資料保護法（以下稱個資法），未來將全面規範全台約 123 萬家企業以及 2,300 萬民眾。法務部已於 10 月 27 日預告新版個資法施行細則草案，新版個資法適用的對象將涵蓋所有類型的組織與企業，面臨這即將到來的個人資料保護適法性之衝擊，企業是否做到了完善的應對，降低因個資法造成的影響與衝擊，已成為目前企業經營最重要的議題。

面臨國際化、全球化及多元化，國際上針對隱私保護之規範已行之多年，我國就保護個人資料之政策與規範，應以符合國際組織及各國對隱私權保護之要求，並尊重本土化之資訊隱私保護措施，才能順應國際趨勢，達成國際合作的目標。

為使我國個資法之實行及後續修正更臻縝密，法務部在行政院科技顧問組支持下，與經濟部國貿局及經濟部商業司為因應個資法之修正通過，欲使公務機關個人資料保護方案更加完善，故委託資策會科技法律研究所執行「99 年度公務機關個人資料保護方案」，並舉辦「個資保護無國界-隱私保護與個資管理跨境合作國際研討會」，邀請國際個資保護標竿國家之專家學者及官方代表，針對各國個人資料保護規範與推動政策，以及跨境合作等議題，進行相關經驗之分享與交流，並借鏡他國對其個人資料保護之經驗，作為我國推行個人資料保護制度之參考。統計總出席人數高達 528 人。

表 36：講習活動統計

活動日期	地點	實際出席人數
100 年 11 月 2 日	福華文教會館卓越堂（台北市新生南路三段 30 號 2 樓）	338
100 年 11 月 3 日		190
總計		528

資料來源：資策會科法所自行製作

二、活動記錄

本報告之智慧財產權歸屬於法務部

本計畫已於 100 年 11 月 2 日及 100 年 11 月 3 日順利舉辦「個資保護無國界-隱私保護與個資管理跨境合作國際研討會」，一般民眾、業界及公務人員出席非常踴躍。

（一）議程

表 37：議程

2011/11/02 （三）國際個資保護規範與推動政策概況		
09:30-10:00	報到	
10:00-10:30	開幕式貴賓致詞	法務部曾勇夫部長 行政院科技顧問組陳炳煇執行秘書 經濟部商業司李錁副司長 資訊工業策進會李世光執行長
10:30-11:00	我國個資保護法制與相關推動政策	法務部法律事務司鍾瑞蘭副司長
11:00-11:20	TEA BREAK	
11:20-12:10	美國商務部個資隱私保護政策概況	美國商務部科技與電子商務司 Joshua Harris 副司長
12:10-13:30	午餐	
13:30-14:20	澳洲隱私保護與資訊自由政策	澳洲資訊委員會政策部 Rachael Spalding 政策助理委員
14:20-15:10	日本個人資料保護法制	日本亞細亞大學法學院 加藤隆之副教授
15:10-15:30	TEA BREAK	
15:30-16:20	APEC 跨境隱私規則	APEC 資料隱私次級工作小組 Joshua Harris 副主席
16:20-17:00	綜合座談	主持人：王郁琦 副教授 世新大學智慧財產權研究所 與談人 美國商務部科技與電子商務司 Joshua Harris 副司長

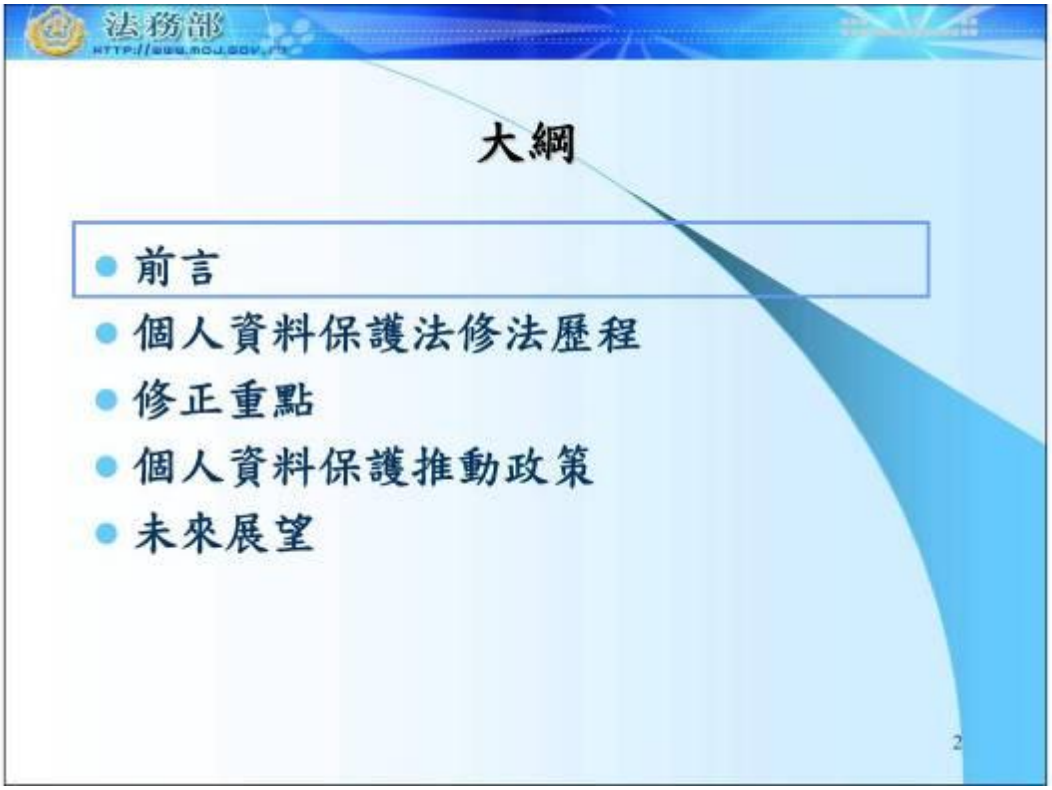
本報告之智慧財產權歸屬於法務部

		澳洲資訊委員會政策部 Rachael Spalding 政策助理委員
16:20-17:00	綜合座談	日本亞細亞大學法學院 加藤隆之副教授 JIPDEC 隱私標章推動中心 関本貢副中心長
2011/11/03 （四）個資保護與管理制度		
09:30-10:00	報到	
10:00-10:10	長官致詞	經濟部商業司李鎂副司長
10:10-10:50	臺灣個人資料保護與管理制度	資訊工業策進會科技法律研究所　邱映曦主任
10:50-11:10	Tea Break	
11:10-11:50	日本個資管理制度分享	JIPDEC 隱私標章推動中心 関本貢副中心長
11:50-12:00	閉幕致詞	資訊工業策進會科技法律研究所 戴豪君所長

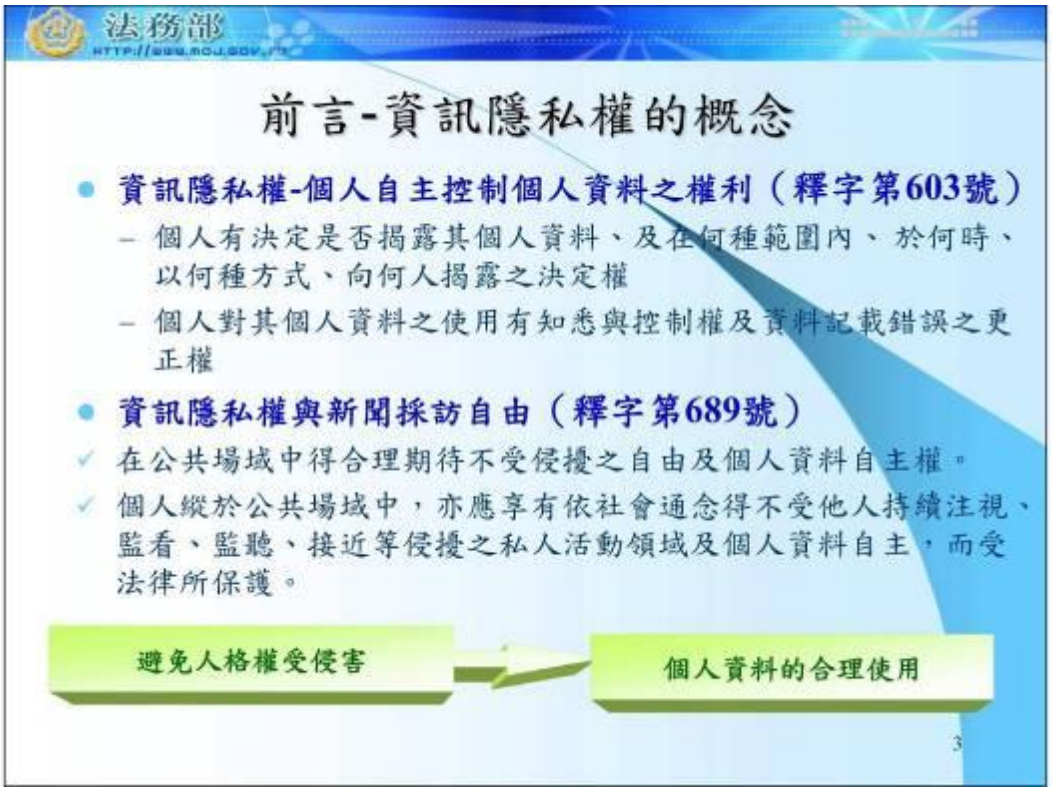
資料來源：資策會科法所自行製作

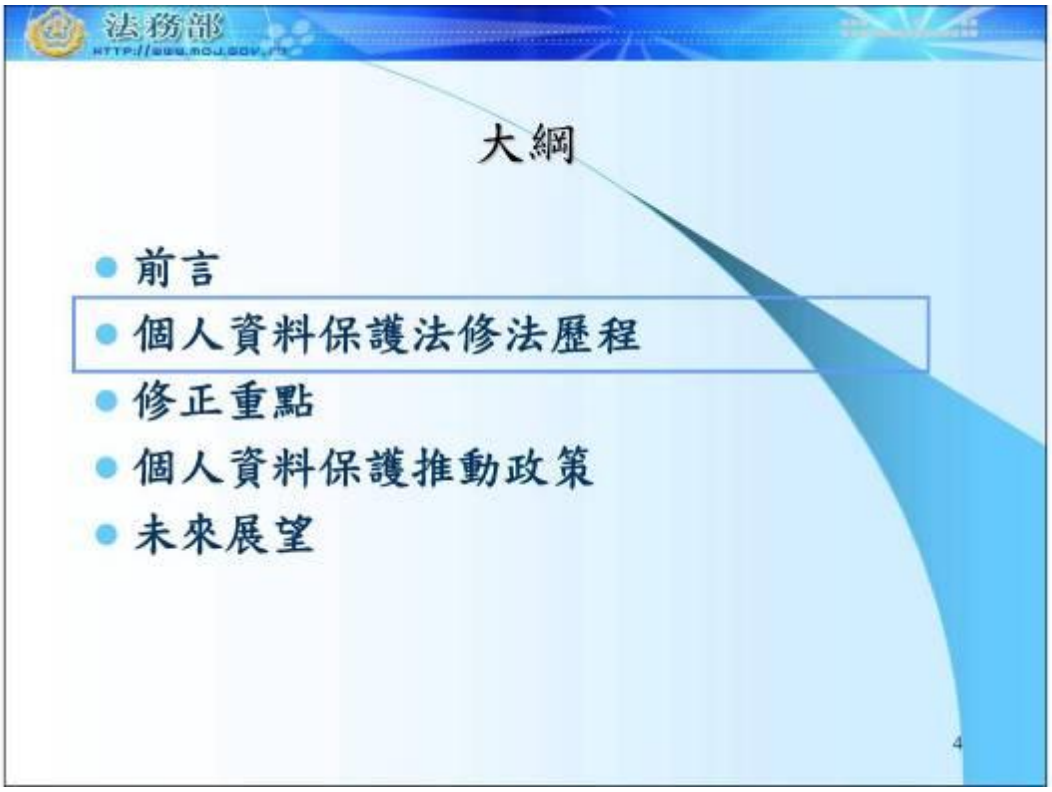
本報告之智慧財產權歸屬於法務部

（二）會議簡報



本報告之智慧財產權歸屬於法務部





本報告之智慧財產權歸屬於法務部

法務部

修法歷程

- 鑒於電腦科技日新月異，利用電腦蒐集、處理、利用個人資料之情形日漸普遍，再加上各類型商務行銷廣泛大量蒐集個人資料，對於個人隱私權之保護造成莫大威脅。
- 法務部自2001年起成立修法專案小組，2004年完成修正草案後，即陳報行政院轉請立法院審議，立法院終於去（2010）年4月27日完成三讀程序，並於同年5月26日公布（目前尚未施行）。

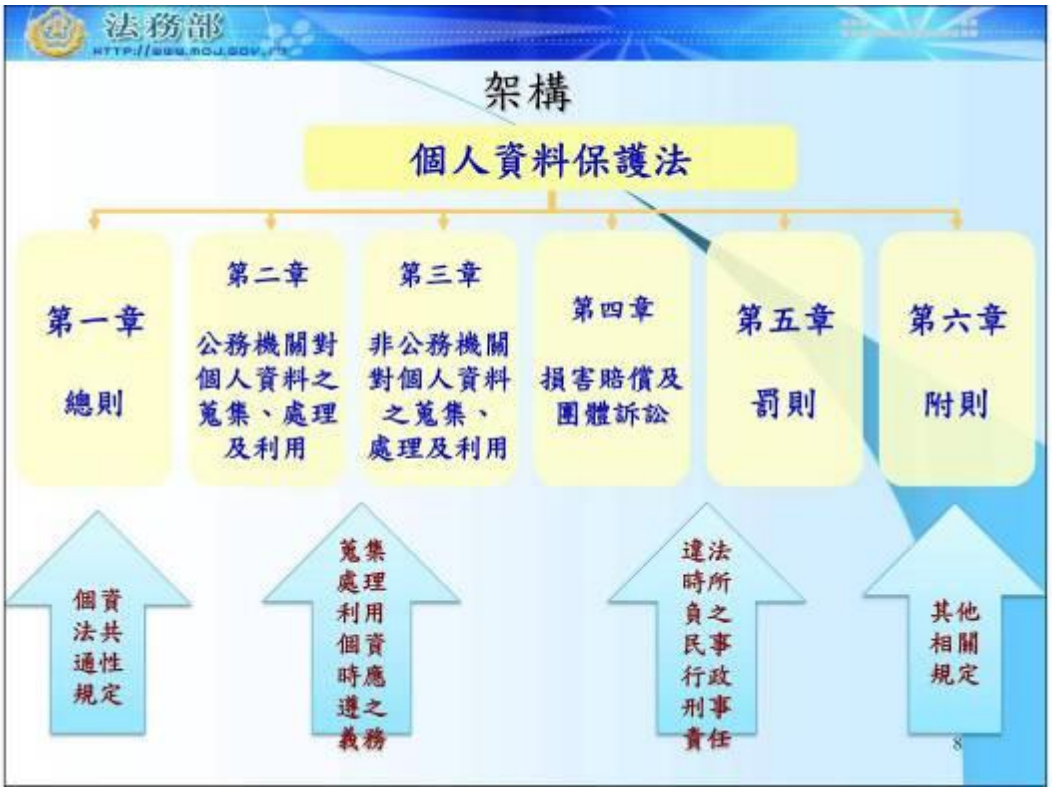
5

法務部

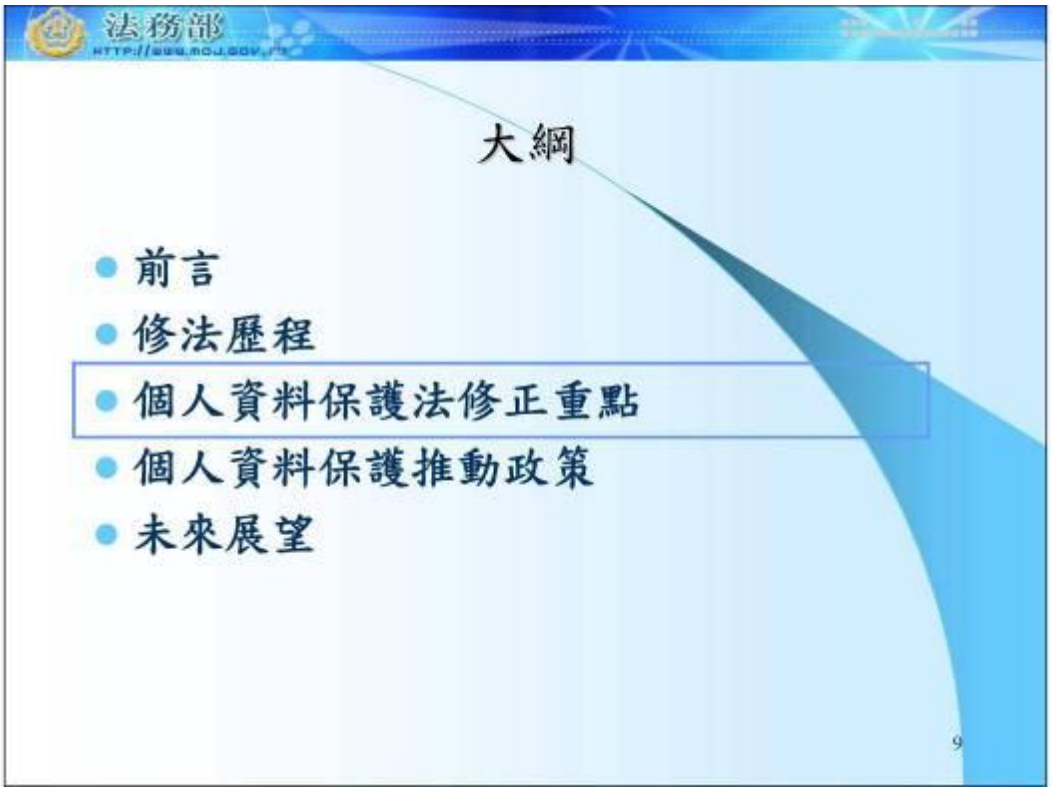
個人資料保護法修法歷程

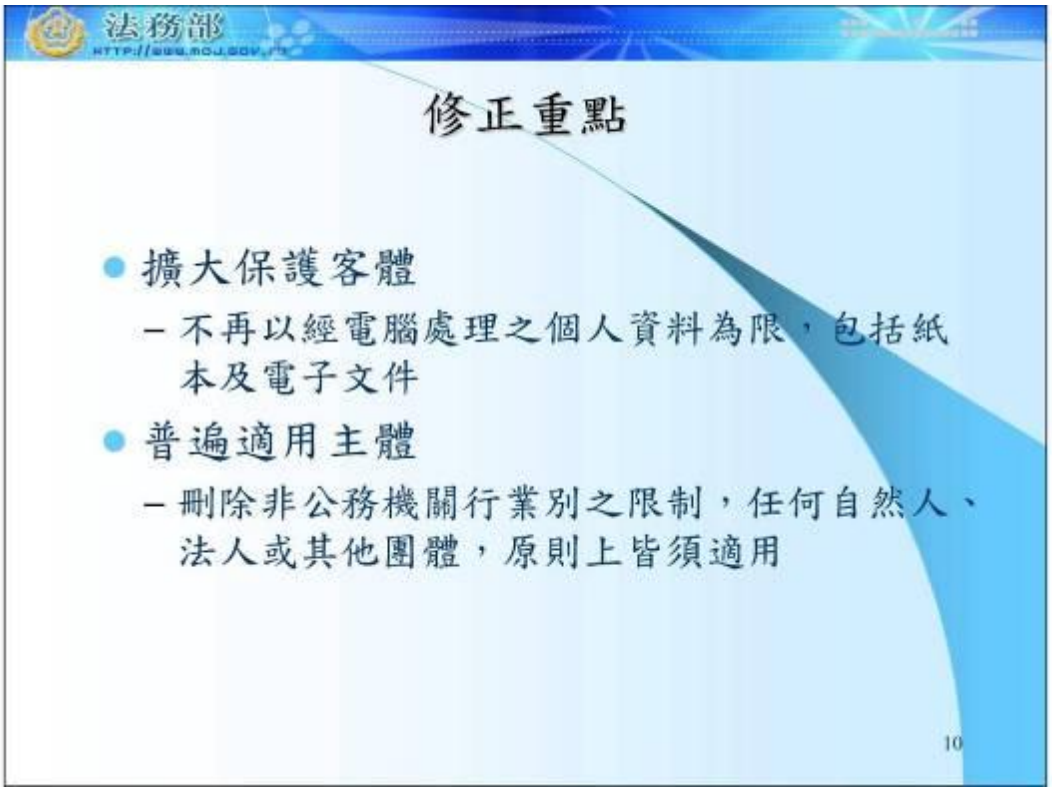
6

本報告之智慧財產權歸屬於法務部



本報告之智慧財產權歸屬於法務部





本報告之智慧財產權歸屬於法務部

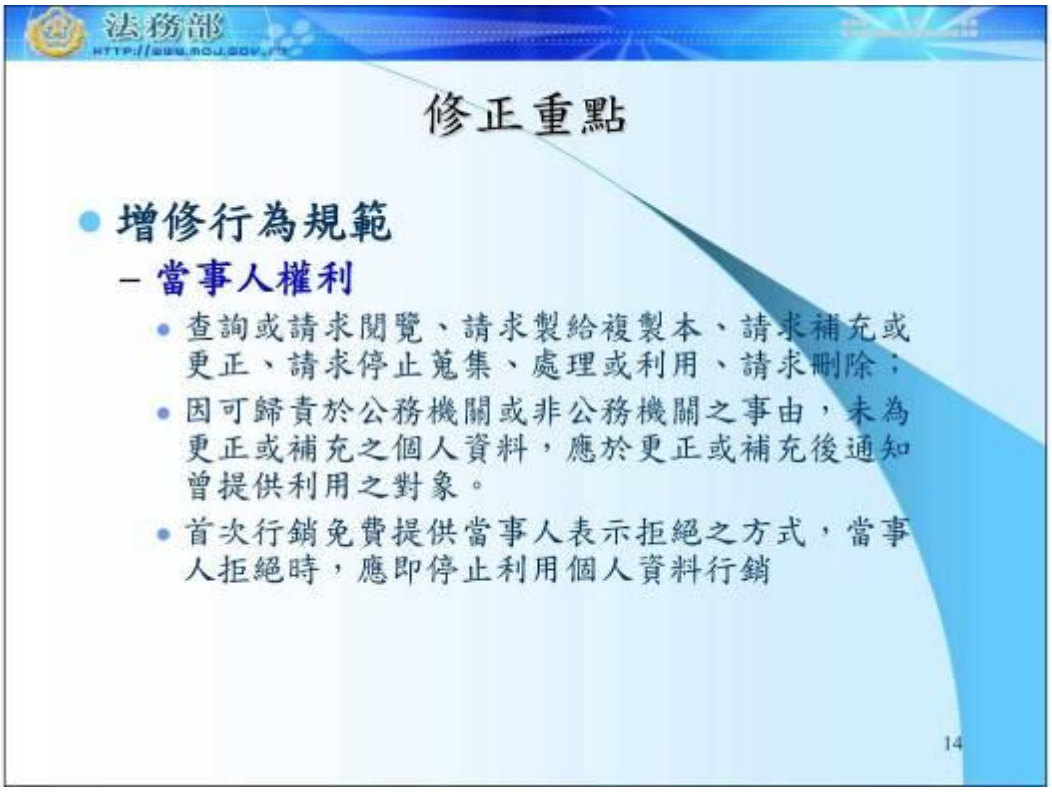
	修正前	修正後
公務機關	中央或地方機關 （第3條第6款）	中央或地方機關 或行政法人 （第2條第7款）
非公務機關	1.徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。 2.醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。 3.其他經法務部會同中央目的事業主管機關指定之事業、團體或個人 （第3條第7款）	公務機關以外之 自然人、法人或其他團體 （第2條第8款）

法務部

依現行法經法務部會同中央目的事業主管機關指定之事業、團體或個人

1) 期貨業
2) 臺北市產物、人壽保險商業同業公會
3) 中華民國產物保險商業同業公會及中華民國人壽保險商業同業公會
4) 臺灣更生保護會
5) 財團法人犯罪被害人保護協會
6) 利用電腦網路開放個人資料登錄之就業服務業
7) 百貨公司業及零售式量販業(資本額1000萬元以上之股份有限公司型態，且採會員制為行銷方式)
8) 不動產經紀業
9) 文理類補習班(除語文類科外)
10) 無店面零售業(以網際網路及型錄方式零售商品之公司行號)(99.7.1)
11) 錄影節目帶出租業(99.7.1)
12) 無店面零售業(電視購物頻道供應者)(99.7.1)
13) 運動場館業(99.11.1)

本報告之智慧財產權歸屬於法務部



本報告之智慧財產權歸屬於法務部

修正重點

- 強化行政監督
  - 中央目的事業主管機關或直轄縣市政府，得派員攜帶執行職務證明文件進行行政檢查
- 促進民眾參與
  - 增訂符合規定之財團法人或公益社團法人得提起團體訴訟
- 調整責任內涵
  - 提高基於同一原因事實應對當事人負損害賠償責任之總額上限為二億元
  - 提高對非公務機關所課之罰鍰額度

15

個人資料保護法 vs. OECD隱私權保護指導綱領 vs. 歐盟個人資料保護指令

16

本報告之智慧財產權歸屬於法務部

法務部

大綱

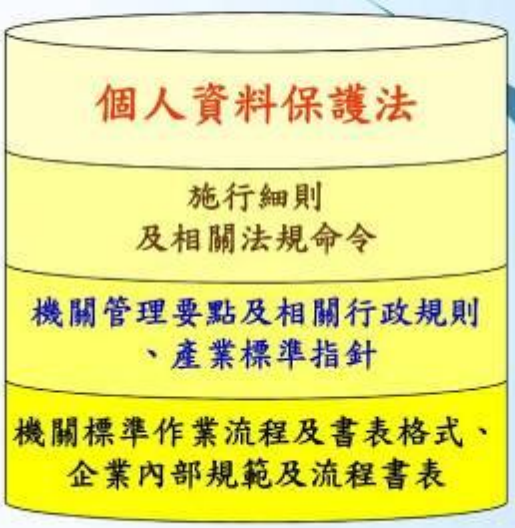
- 前言
- 修法歷程
- 個人資料保護法修正重點
- 個人資料保護推動政策
- 未來展望

17

法務部

建置個資保護制度之體系

個人資料保護



資訊安全

18

本報告之智慧財產權歸屬於法務部

本報告之智慧財產權歸屬於法務部

本報告之智慧財產權歸屬於法務部

法務部

相關子法修訂

項目	主辦機關
研修「個人資料保護法施行細則」修正草案	法務部
訂定「個人資料保護法」第6條第2項法規命令 ●特種資料蒐集、處理或利用之範圍、程序及其他應遵循事項之辦法	各機關
訂定「個人資料保護法」 第27條第3項法規命令 ●個人資料檔案安全維護計畫及處理方法之標準等相關事項之辦法	各目的事業主管機關
修訂個人資料之特定目的及個人資料類別	各機關

23

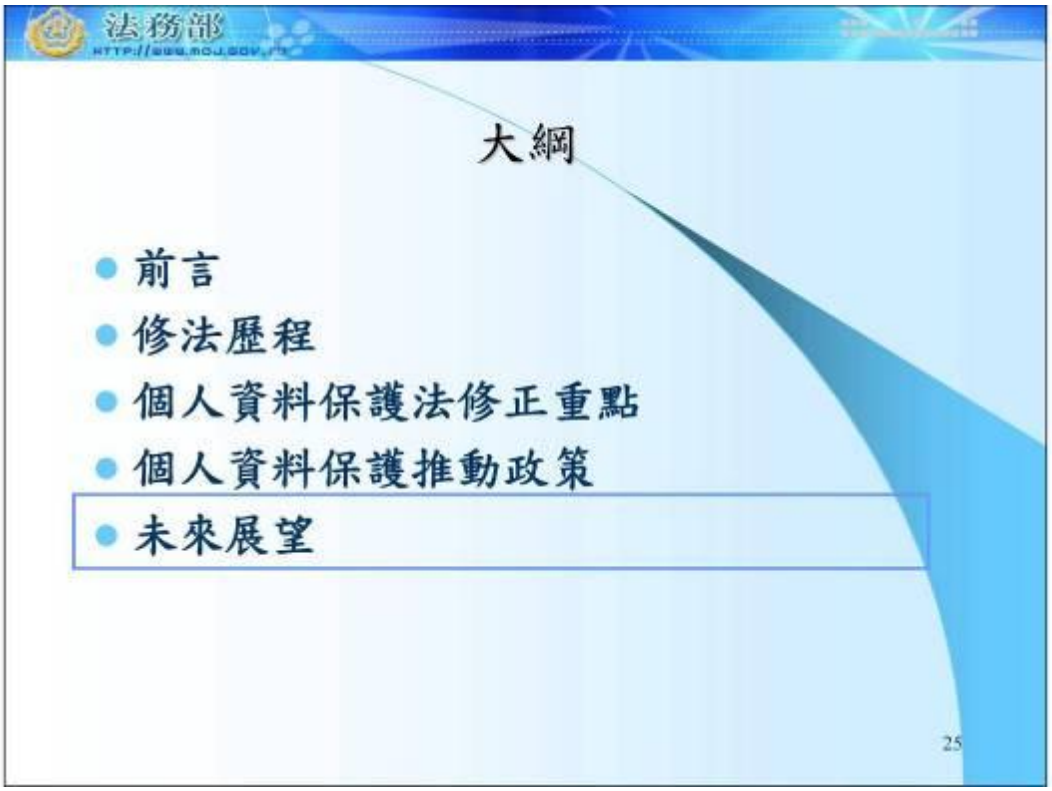
法務部

配套措施

項目	主辦機關	協辦機關
各機關設置專人及個人資料保護聯絡窗口	各機關	法務部
訂定公務機關個人資料保護管理要點	各機關	法務部
「個人資料保護專區」 網頁規劃	各機關	法務部
協助推動零售業「隱私權認證標章」 制度	經濟部	法務部
協助行政院發展數位鑑識技術與扶植產業	行政院	法務部
建立院級跨部會協調聯繫機制	法務部	各機關
公務機關專責人員培訓及宣導	法務部	各機關

24

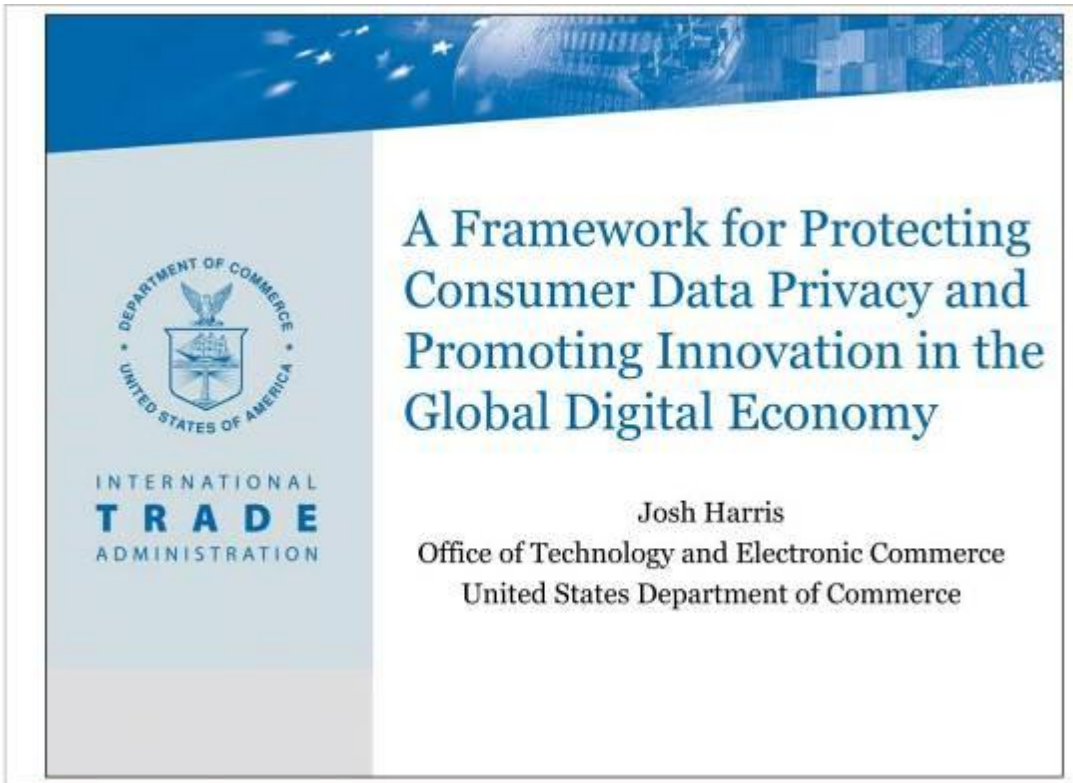
本報告之智慧財產權歸屬於法務部

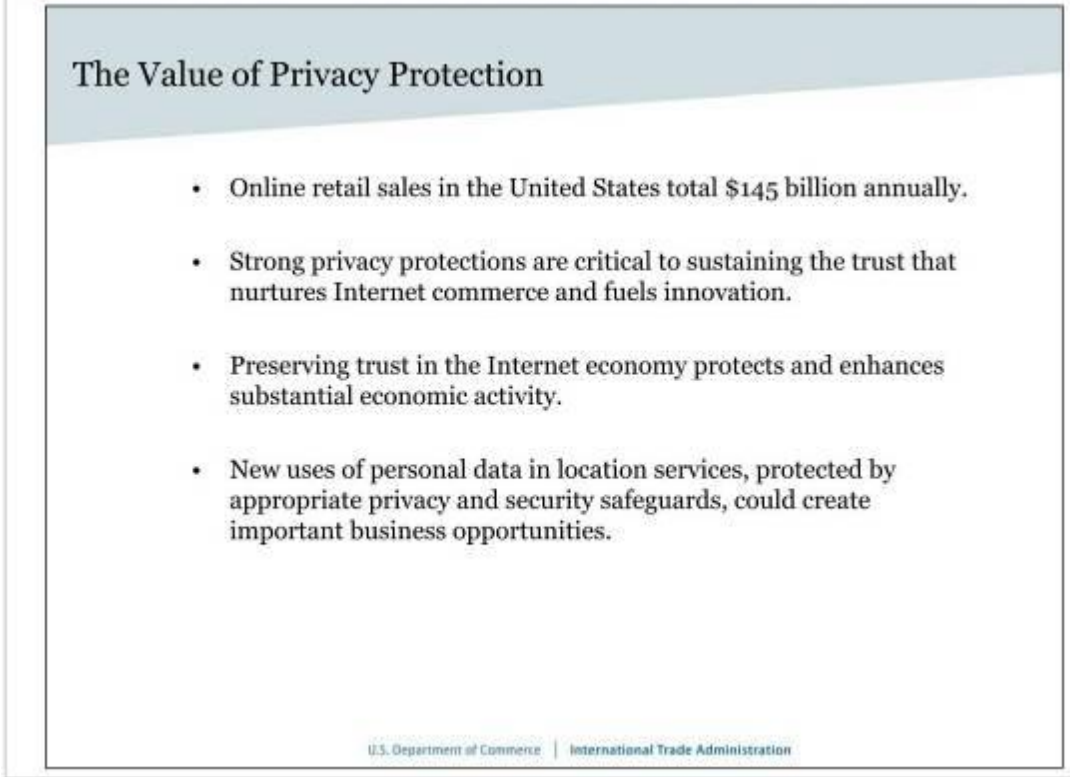


本報告之智慧財產權歸屬於法務部

資料來源：本簡報由法務部提供

本報告之智慧財產權歸屬於法務部





本報告之智慧財產權歸屬於法務部

Privacy Protection in the U.S. Federal Government

- The United States government plays a critical role in promoting data privacy protections in the public and private spheres.
- In some cases, agencies consider privacy issues in response to specific Congressional mandates.
- In others, agencies integrate privacy into initiatives that advance their core missions.

The Current U.S. Consumer Data Privacy Framework

- The consumer data privacy framework in the United States is flexible and effectively addresses some consumer data privacy challenges in the digital age.
- This framework consists of:

  a) Industry best practices;
  b) FTC enforcement, and;
  c) A network of chief privacy officers and other privacy professionals.

本報告之智慧財產權歸屬於法務部

Policy Formulation: The U.S. Commerce Department Green and White Papers

I. Green Paper:

- 8 month consultation with industry, consumer advocates and academic stakeholders, approximately 70 comments submitted and reviewed
- Released December, 2010
- Green Paper available at www.tinyurl.com/42S3KEJ

II. White Paper:

- 11 Months of additional consultation, approximately 100 comments submitted and reviewed
- Released November, 2011

Building on the Strength of the U.S. Consumer Data Privacy Framework

- Most Federal data privacy statutes apply only to specific sectors.
- The White Paper recommends filling the gaps in the existing framework to promote more consistent responses to privacy concerns.
- The White Paper calls for legislation to supplement the existing framework by creating a baseline standard of protection to the sectors that existing Federal statutes do not cover.

本報告之智慧財產權歸屬於法務部

The Consumer Privacy Bill of Rights

I. Individual Control

II. Transparency

III. Respect for Context

IV. Security

V. Access and Accuracy

VI. Focused Collection

VII. Accountability

U.S. Department of Commerce | International Trade Administration

I. Individual Control

"Consumers have a right to exercise control over what personal data organizations collect from them and how they use it."

U.S. Department of Commerce | International Trade Administration

本報告之智慧財產權歸屬於法務部

II. Transparency

"Consumers have a right to easily understandable and accessible information about privacy and security practices."

U.S. Department of Commerce | International Trade Administration

III. Respect for Context

"Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with their relationships with consumers."

U.S. Department of Commerce | International Trade Administration

本報告之智慧財產權歸屬於法務部

IV. Security

"Consumers have a right to secure and responsible handling of personal data."

U.S. Department of Commerce | International Trade Administration

V. Access and Accuracy

"Consumers have a right to access personal data in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to the consumer if the data is inaccurate."

U.S. Department of Commerce | International Trade Administration

本報告之智慧財產權歸屬於法務部

VI. Focused Collection

"Consumers have a right to reasonable limits on the personal data that organizations collect and retain."

U.S. Department of Commerce | International Trade Administration

VII. Accountability

"Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights."

U.S. Department of Commerce | International Trade Administration

本報告之智慧財產權歸屬於法務部

Implementing the Consumer Privacy Bill of Rights

- Implementing these principles across the wide range of innovative uses of personal data requires a process to establish more specific practices.
- The White Paper encourages companies, industry groups, privacy advocates, consumer groups, academics, and other relevant groups to participate in multistakeholder processes to develop codes of conduct that implement these general principles.
- The White Paper also seeks the participation our international partners in these multistakeholder processes.

A Multistakeholder Process for Consumer Data Privacy

- The White Paper calls on the Department of Commerce's National Telecommunications and Information Administration (NTIA) to convene stakeholders in a deliberative process to develop codes of conduct as technologies and market conditions change.

本報告之智慧財產權歸屬於法務部

Promoting International Interoperability

- Mutual recognition of commercial data privacy frameworks is a means to achieve meaningful global data protection.
- Two principles should determine whether the conditions for mutual recognition exist:
  1. effective enforcement; and
  2. mechanisms that allow organizations to demonstrate accountability.

Conclusion

- The **Consumer Privacy Bill of Rights** should be the legal baseline that governs consumer data privacy in the United States.
- The Department of Commerce will convene multistakeholder processes to encourage the development of **enforceable codes of conduct**.
- We will engage with our international partners to facilitate the **interoperability** of our respective consumer data privacy frameworks.
- Finally, this framework is a call for the ongoing participation of **private-sector stakeholders**.

本報告之智慧財產權歸屬於法務部

資料來源：本簡報由 Joshua Harris 提供

本報告之智慧財產權歸屬於法務部

本報告之智慧財產權歸屬於法務部

Office of the Australian Information Commissioner (OAIC)

- Privacy, FOI and information management policy
- Former Office of the Privacy Commissioner integrated into OAIC
- Extensive range of functions – complaints, monitoring compliance, legislative review, advice to government and business
- Privacy functions drawn from the *Privacy Act 1988*

The Privacy Act – a snapshot

- Covers:
  - Australian Government agencies (includes the Australian Capital Territory and Norfolk Island, but not other States or Territories)
  - Credit providers and reporters
  - All private health service providers
  - Businesses with turnover of more than $3 million
  - Some other small businesses (e.g. who trade in personal information)

本報告之智慧財產權歸屬於法務部

Scope of Australian privacy regulation

- Privacy Act focuses on information privacy protection
- Does not cover bodily or territorial privacy
- Regulates the handling of 'personal information' – information which identifies you or could identify you
- Stricter rules apply to 'sensitive information'

Privacy Principles

- Privacy Principles regulate how personal information is handled
- Information Privacy Principles (IPPs) apply to Australian and some Territory Government Agencies
- National Privacy Principles (NPPs) apply to private sector organisations
- The principles are not prescriptive - each agency or organisation needs to apply the principles to its own situation

本報告之智慧財產權歸屬於法務部

Privacy law reform in Australia

- ALRC Report 108 – 'For Your Information: Privacy Law and Practice' (May 2008)
  - 295 recommendations
- Government's First Stage Response – *'Enhancing National Privacy Protections'* (October 2009)
  - Responds to 197 recommendations
- Exposure draft legislation prepared and referred to Senate Committee for inquiry and report
- Public comment on exposure draft legislation

First Stage Response

Outlines the Government's position on:

- developing a single set of Privacy Principles
- redrafting & updating the structure of the Privacy Act
- addressing the privacy impact of new technology
- strengthening the Privacy Commissioner's powers and functions
- introduction of comprehensive credit reporting and enhanced protections for credit reporting information
- enhancing and clarifying the protections around the sharing of health information and the ability to use personal information to facilitate research in the public interest.

本報告之智慧財產權歸屬於法務部

Australian Privacy Principles (APPs)

- Exposure draft of 13 APPs
  - Released June 2010
  - Will apply to both the private and public sector
  - Unifies and replaces the IPPs (public sector) and the NPPs (private sector)
  - Structured to reflect the flow of information, from collection, through to use and disclosure and access and correction

Senate Committee Report - APPs

- The Senate Committee's final report:
  - Recommends simplifying the draft APPs, and the production of guidance material to aid interpretation
  - Avoids re-examining Government's policy positions on which the draft APPs were based

本報告之智慧財產權歸屬於法務部

Privacy complaints

- One of OAIC's key responsibilities is to investigate and manage privacy complaints
- Complaints are generally resolved on a case by case basis through conciliation
- If parties cannot reach an agreement, the OAIC has the power to make a determination
- The OAIC also has the power to investigate matters on its own motion

Data breaches

- Privacy Act does not contain data breach notification obligations
- Privacy Act does require that agencies and organisations take reasonable steps to maintain security of personal information they hold
- OAIC recommends data breach notification as 'best-practice'
- The OAIC has begun publishing the results of investigations to encourage organisations to follow best practice

本報告之智慧財產權歸屬於法務部

Proposed new enforcement powers

- Government proposes new powers for the OAIC so that it can:
  - make an enforceable determination on an own motion investigation
  - accept and enforce undertakings from agencies or organisations
  - seek civil penalties for serious or repeated offences.
- The OAIC's current limited enforcement powers has led to a reliance on co-operative forms of regulation

Regulation of international transfer of information in Australia

- NPP 9 - private sector can only transfer personal information of Australians to foreign countries if it satisfies one of several conditions, e.g. where the individual consents
- Draft APP 8 – agencies and organisations will remain accountable for any disclosure of personal information outside Australia

本報告之智慧財產權歸屬於法務部

International co-operation

- International co-operation is becoming increasingly important
  - More organisations operate on a global level leading to privacy issues across many countries
- Technological developments have created privacy challenges
  - Breaches occur in increased number of ways
  - Increase in potential scale of breaches
  - Uncertainty as to how the Privacy Act applies to data submitted via the internet by individuals in Australia to an overseas organisation

OAIC international involvement

- Asia Pacific Economic Cooperation (APEC)
  - Cross-border Privacy Enforcement Arrangement (CPEA)
- Global Privacy Enforcement Network (GPEN)
- Asia Pacific Privacy Authorities (APPA)

本報告之智慧財產權歸屬於法務部

Examples of international co-operation

- The OAIC relies on useful mechanisms such as international co-operation for privacy issues concerning multi nationals
- Some examples of international co-operation

OAIC resources and materials

- Website – www.oaic.gov.au
- Publications on our website:
  - Fact sheets
  - Guidelines
  - Privacy Impact Assessment Guide
  - Frequently Asked Questions
  - Links to Privacy law

本報告之智慧財產權歸屬於法務部

資料來源：本簡報由 Rachael Spalding 提供

本報告之智慧財產權歸屬於法務部

Personal Information Protection Legislative Development in Japan

Associate Professor of Law, Asia University, Japan
Takayuki KATO
katot@asia-u.ac.jp

Development of the Acts

1988 The Act on Protection of Personal Information Retained by Administrative Organs was enacted.

By 2005 The related acts were fully enforced.

- The Act on the Protection of Personal Information
- Cabinet Order for the Enforcement of the Act on the Protection of Personal Information
- Basic Policy for the Act on the Protection of Personal Information

Meets OECD 8 principles

本報告之智慧財產權歸屬於法務部

Outline of the Acts

Basic Policy	The Act on the Protection of Personal Information	any entity
Details	The Act on the Protection of Personal Information	civil sector
Details	The Act for the Protection of Personal Information Retained by Administrative Organs	public sector
Details	The Act for the Protection of Personal Information Retained by Incorporated Administrative Agencies, etc.	incorporated administrative agencies
Details	Municipal Ordinance	local government
More Details	Guidelines Established by Each Competent Minister	

Characteristics

Technology and public attitude toward the protection of personal is changing.

And

Basic Policy hasn't changed much.

Although Guidelines made by Ministers are not law, their roles are important and they are working well!!

As of March 2003, 40 Guidelines have been issued.

本報告之智慧財產權歸屬於法務部

Competent Ministry

The Act on the Protection of Personal Information	Consumer Affairs Agency
The Act for the Protection of Personal Information Retained by Administrative Organs	Ministry of General Affairs
The Act for the Protection of Personal Information Retained by Incorporated Administrative Agencies, etc.	Ministry of General Affairs
Municipal Ordinance	Municipalities
Guidelines Established by Each Competent Minister	Ministry

Role of Each Ministry

Consumer Affairs Agency

⇒big role in the past for the enactment of the Law coordination and research role now

Each Ministry

⇒ needs modification of its guideline constantly

本報告之智慧財產權歸屬於法務部

Current Institutional Problems

Role of Consumer Affairs Agency

- International conferences
- Across the board research
- No superseding power to the other ministries

Guidelines consistency

- Could be time-consuming
- Focusing on its interest
- No interest in an institutional issue

Solution

Adopting a Commissioner system, or creating a sole third party organization?

Research done and planned by Consumer Affairs Agency

(last year) Roles and systems of Commissioners
⇒focusing on the criteria and idea of independency
(U.S., U.K., Germany, France, Sweden, Ireland)
(this year) Administration of Commissioners
(Planned)

本報告之智慧財產權歸屬於法務部

Maybe a Try?

National Numbering System
(Mutual Number System) will be adopted soon.

At the same time,

A Third Independent Body to observe privacy issues will be established.

Administrative Problems

1. Effectiveness of Enforcement
   No Punishment case, but many leakage cases (over 400 cases every year) still exists.

2. Passing personal data to a third party
   Always needs consent?

本報告之智慧財產權歸屬於法務部

Waseda University Case

(Facts)

1.Waseda University, one of the major universities, planned to hold a discussion meeting with the President of China.

2. The Police asked the University to pass the list of the attendance which includes the names and their addresses.
3. Without the consent of the attendance, the University passed the personal information to the Police.

Waseda University Case

(Supreme Court ruling, 3 to 2)

1.The University should have obtained the consent, but didn't.

2. Omitting the necessary process is illegal and should pay about 50 dollars to each attendance.

(Dissent)

1.Passing the information is highly required for the security reasons.

2. Although omitting the consent is a problem, it is hard to say the act of the University is illegal.

本報告之智慧財產權歸屬於法務部

Issues

1. Is attendance to a University event a personal or social act?
2. Who judge the necessity and the significance of the security? Always entities handling personal information?
   -----One of the provisions says,
   Entities handing personal information MAY pass the formation without consent if cases in which it is necessary for cooperating with a State organ.
3. If they misjudge it, they have to reimburse the whole attendance for the damages?
   - 3 students filed suit, but the attendance was 1400.
   - 3 other students filed suit in the same case and were admitted about 100 dollars each.

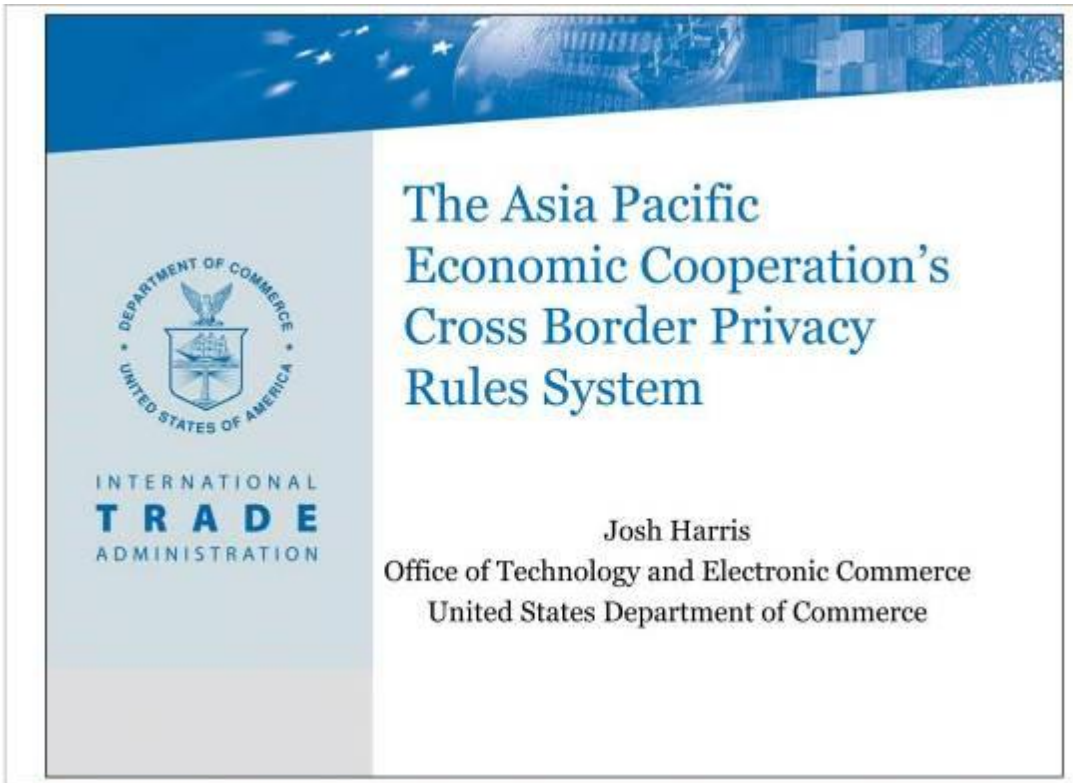
Reluctant to pass personal data
Impediment to free flow of information

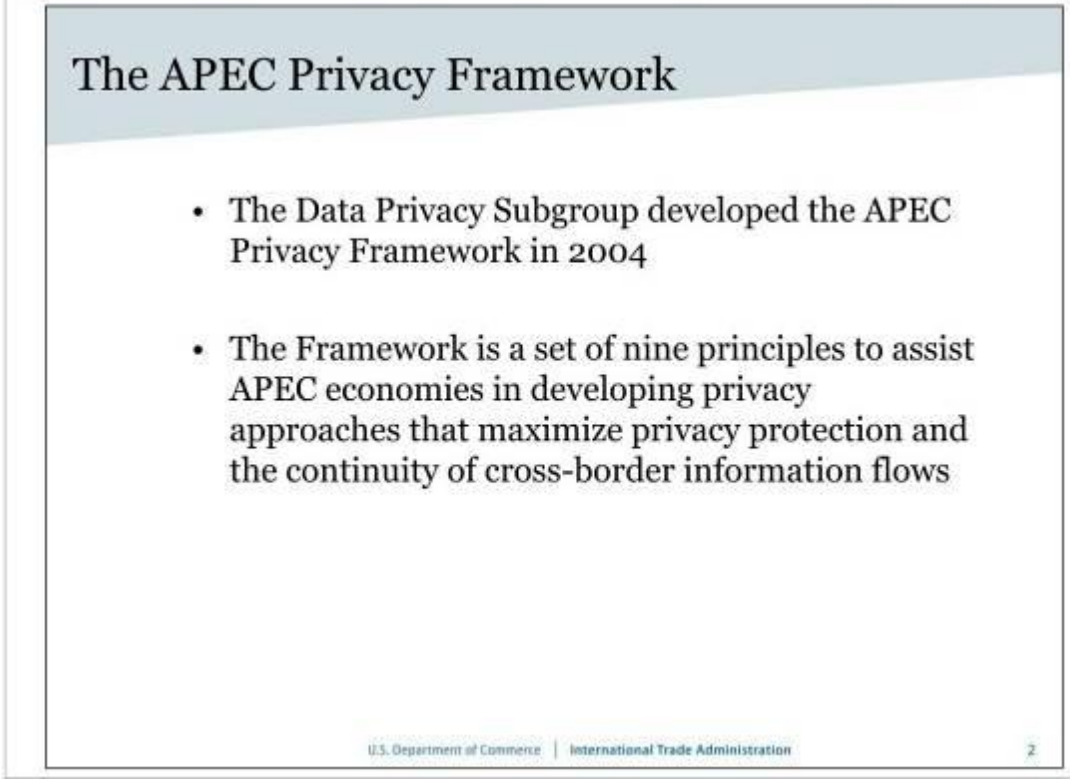
Thank you very much for listening to my speech!

If you have further questions, please don't hesitate to ask me anything.

資料來源：本簡報由加藤隆之提供

本報告之智慧財產權歸屬於法務部





本報告之智慧財產權歸屬於法務部

The APEC Privacy Principles

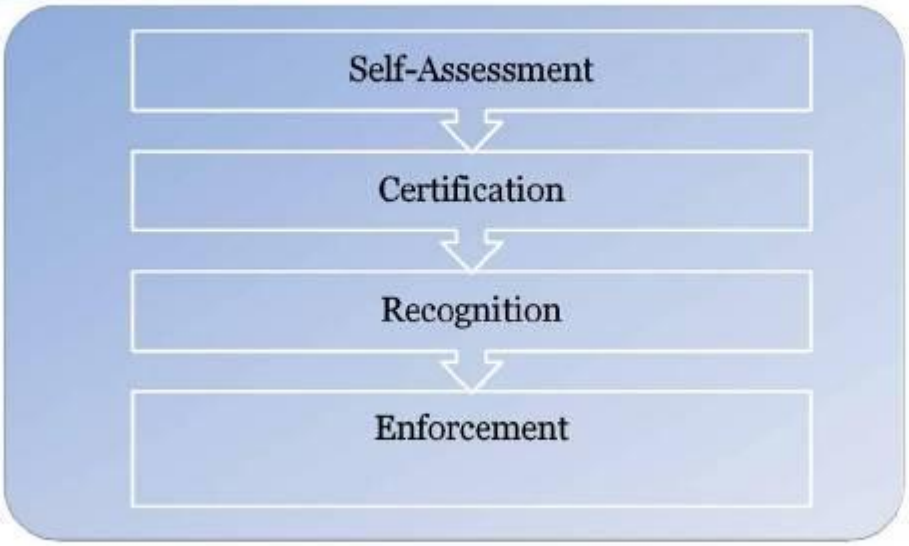
1) Preventing Harm
2) Notice
3) Use
4) Collection Limitation
5) Choice
6) Security Safeguards
7) Integrity
8) Access and Correction
9) Accountability

The Role of Cross Border Privacy Rules

- The Framework states that international implementation of these principles may be achieved through Cross Border Privacy Rules (CBPRs)
- CBPRs are a set of voluntary rules developed by an organization based upon the APEC Privacy Principles
- The organization then commits to apply these rules to its activities involving transfers of personal information across borders

本報告之智慧財產權歸屬於法務部

CBPRs In Practice: A Four Step Approach



How Are CBPRs Certified?

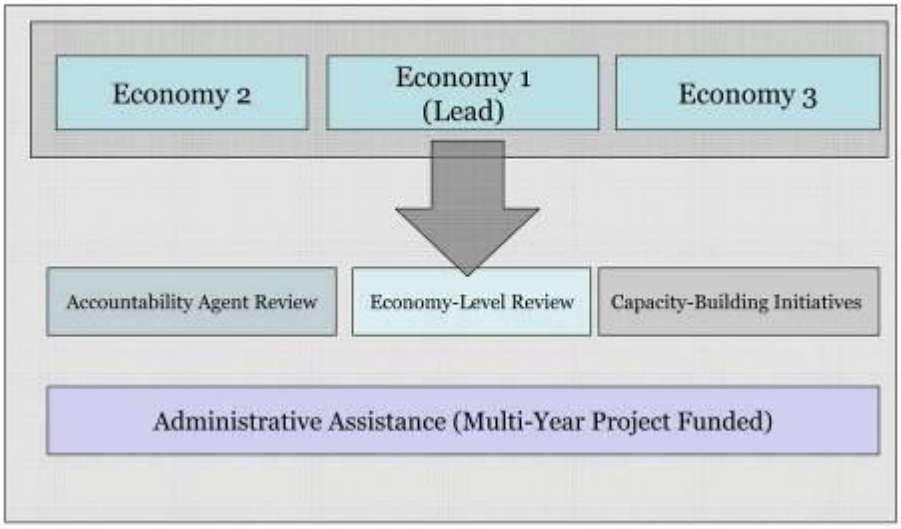
- In order to receive APEC certification, every applicant's self-assessment must be verified by a third party, also known as an Accountability Agent
- Participating Accountability Agents will make use of a baseline guidance document to assess the answers provided by the applicant
- Upon successful review, an applicant's privacy policy is deemed compliant with the Cross Border Privacy Rules System

本報告之智慧財產權歸屬於法務部

How Are CBPRs Enforced?

- In order to participate in this system, an APEC member economy must participate in the Cross Border Privacy Enforcement Arrangement
- Must be supported by a letter of confirmation from the economy's ECSG delegation, which identifies:
  1) The Relevant Privacy Enforcement Authority: any public body responsible for enforcing Privacy Law
  2) The Applicable Privacy Law: laws that have the effect of protecting personal information consistent with the APEC Privacy Framework
- In addition, the economy must demonstrate its enforcement ability to the CBPR Joint Oversight Panel.

Structure of the CBPR Joint Oversight Panel



本報告之智慧財產權歸屬於法務部

資料來源：本簡報由 Joshua Harris 提供

本報告之智慧財產權歸屬於法務部

本報告之智慧財產權歸屬於法務部

本報告之智慧財產權歸屬於法務部

本報告之智慧財產權歸屬於法務部

臺灣個人資料保護轉型之契機

法制面

個人資料保護法通過

國際組織APEC要求

企業與消費者

電子商務跨國貿易蓬勃，營造企業形象與聲譽

詐騙事件頻傳，消費者隱私保護意識抬頭

經濟部提出「電子商務個人資料管理制度建置計畫」，建立「臺灣個人資料保護與管理制度（Taiwan Personal Information Protection and Administration System, TPIPAS），並依循制度預備推行「資料隱私保護標章（Data Privacy Protection Mark, DP Mark）」

data privacy protection mark

stli 7

TPIPAS 架構鳥瞰

TPIPAS 規範綜覽

制度簡介

TPIPAS 導入流程

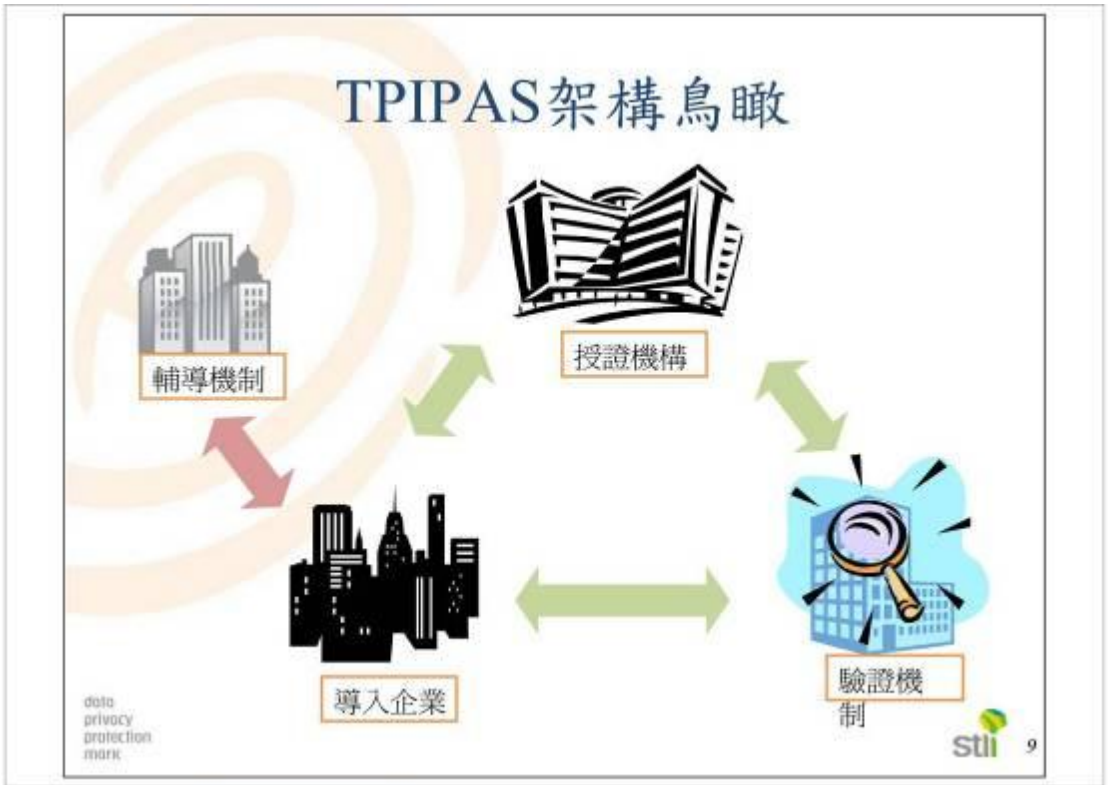
TPIPAS 特色

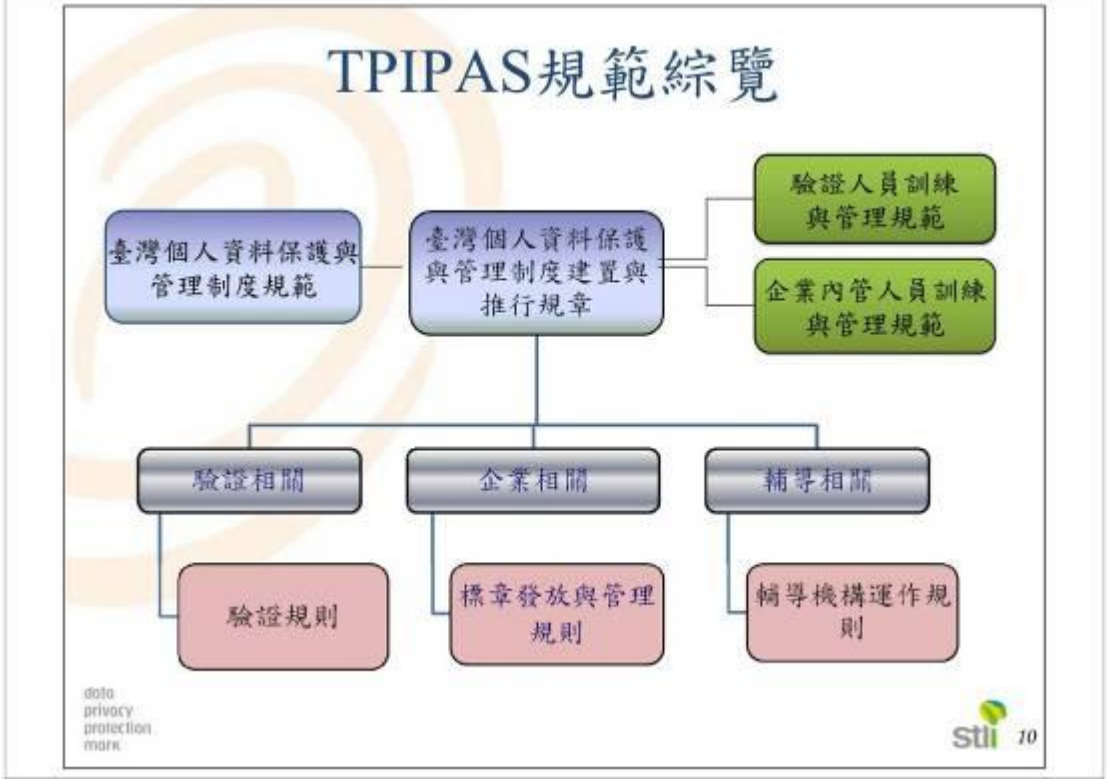
TPIPAS V.S 個人資料保護法

data privacy protection mark

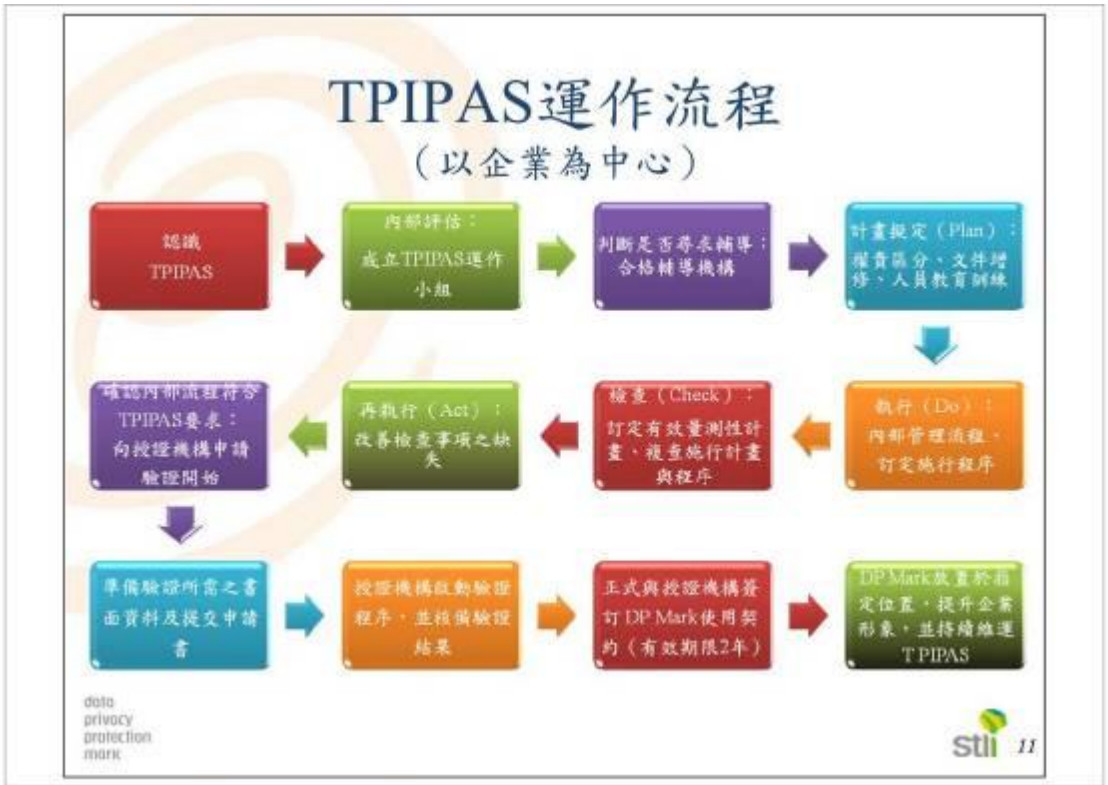
stli 8

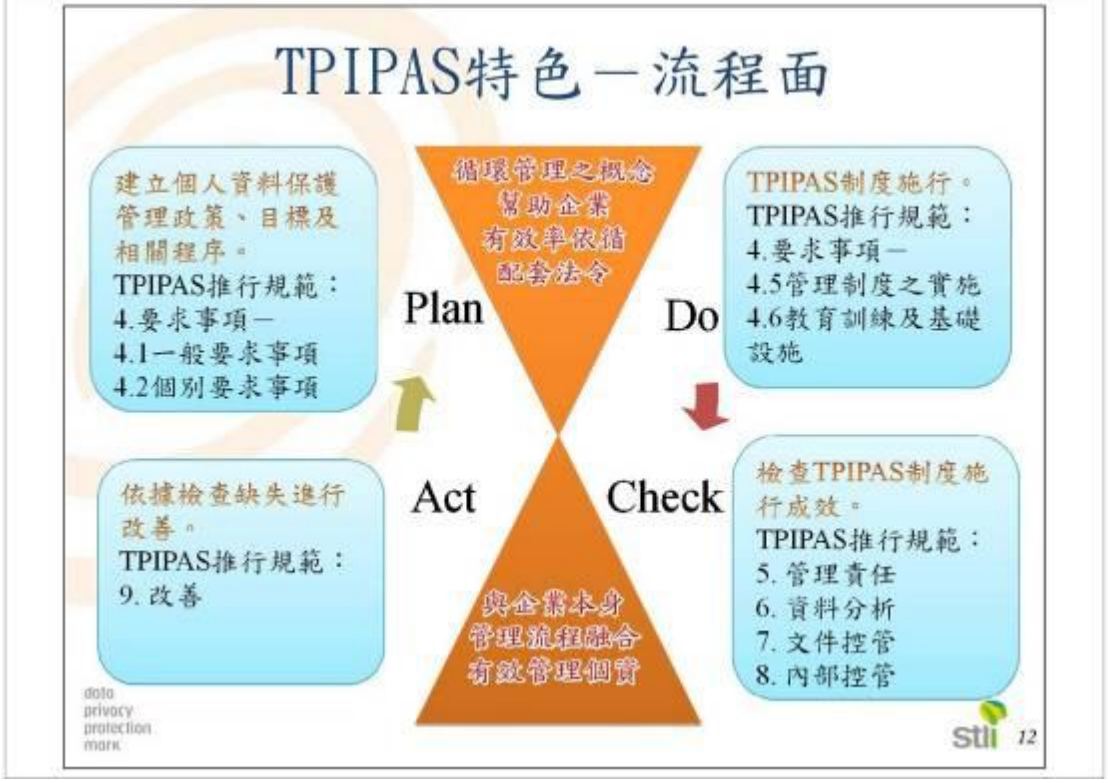
本報告之智慧財產權歸屬於法務部



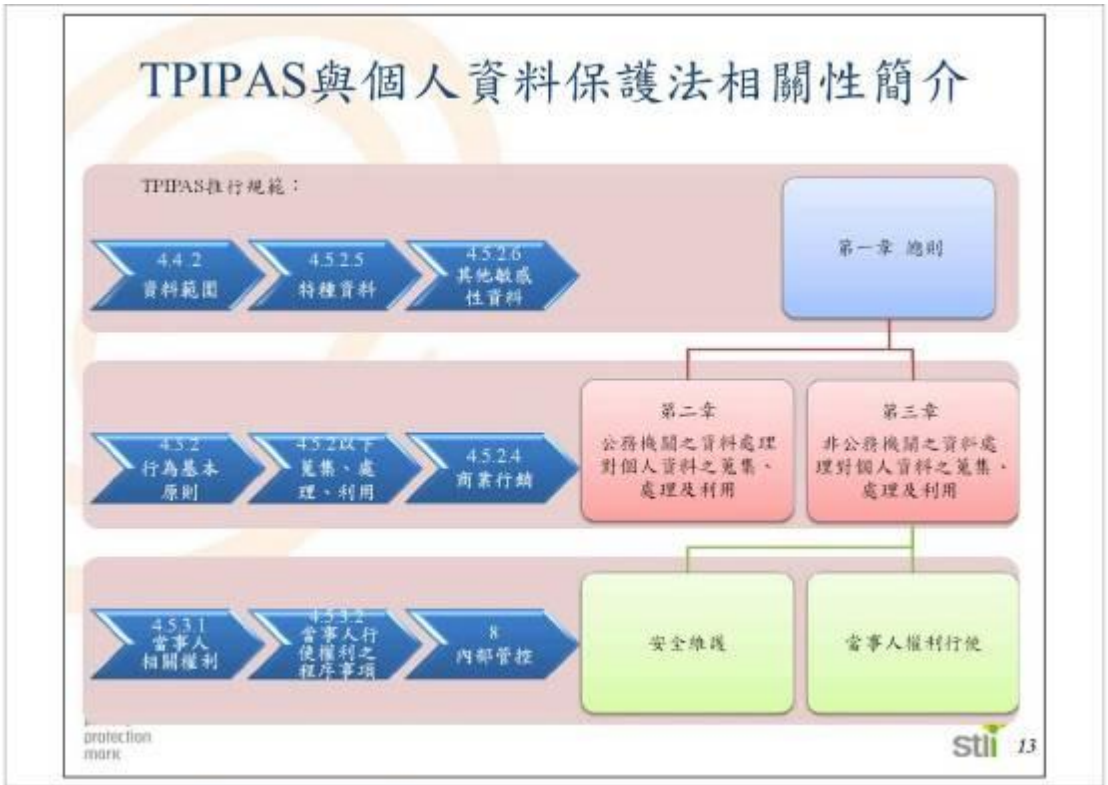


本報告之智慧財產權歸屬於法務部



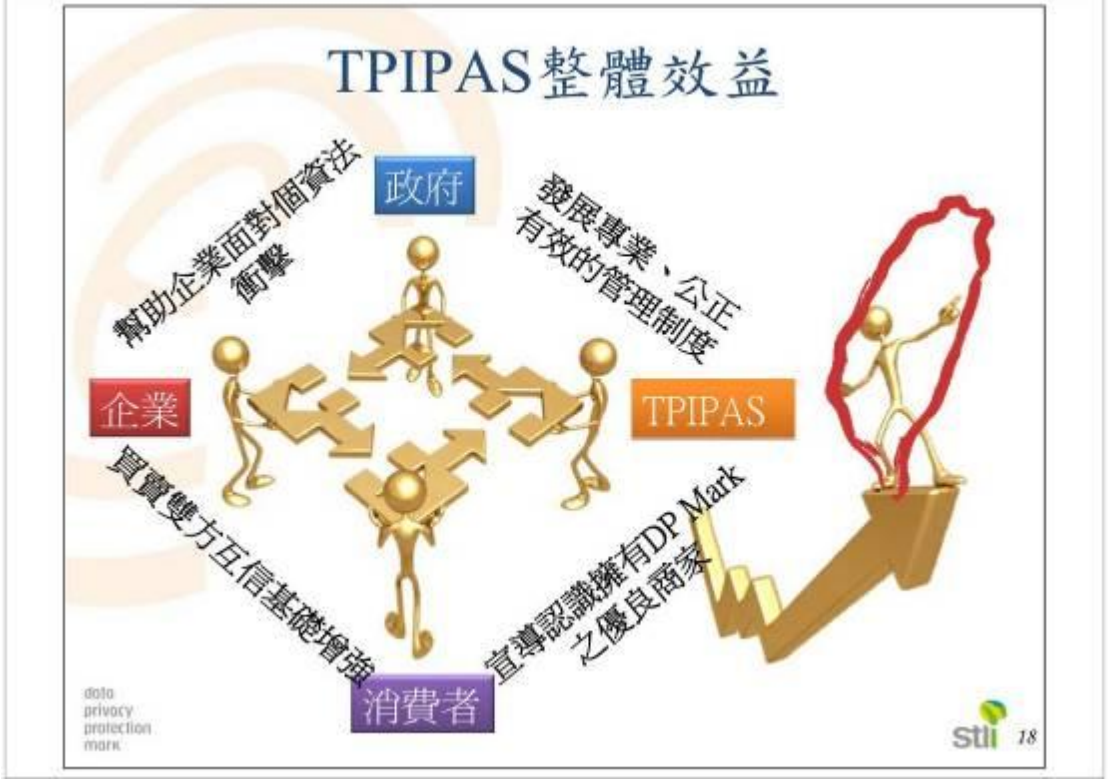


本報告之智慧財產權歸屬於法務部

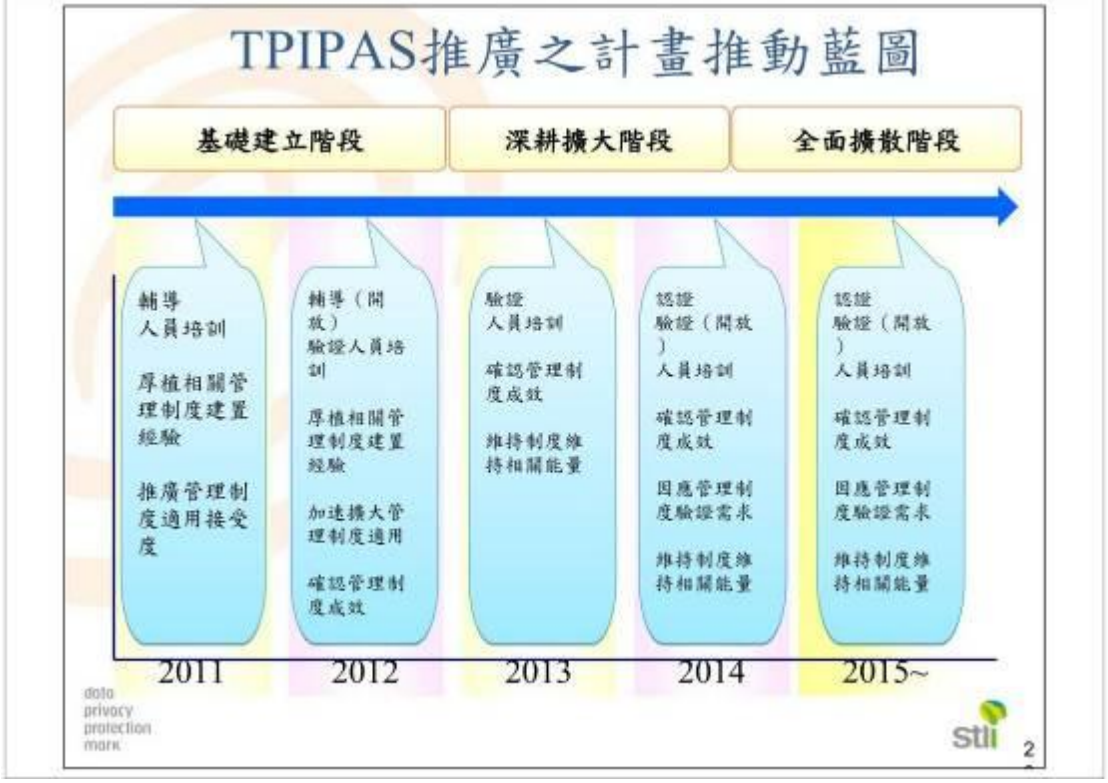


本報告之智慧財產權歸屬於法務部

本報告之智慧財產權歸屬於法務部



本報告之智慧財產權歸屬於法務部



本報告之智慧財產權歸屬於法務部

TPIPAS推廣現況之試辦導入

以試辦導入以及人才培訓
經驗持續完善制度規範

data privacy protection mark

stli 21

TPIPAS推廣現況之自我評量結果

六場宣導說明會發遞500份問卷，回收230份，
有效問卷127份。

有效問卷中，就新個資法所要求重要事項已均有對應程序並有相關紀錄者則只有約6.3%。

上述數據只考慮事業是否有對應方針，尚未評估事業所採取之方針之品質良窳，且尚未計入事業是否投入必要資源、掌握個資管理基本資訊等關於個資制度本身之數據，顯然在修正通過之個資法正式施行前，事業為遵循個資法要求、強化自身個資管理仍有許多努力空間。

data privacy protection mark

stli 22

本報告之智慧財產權歸屬於法務部

資料來源：本簡報由資策會科法所製作

本報告之智慧財產權歸屬於法務部

The PrivacyMark® System

System, Quality Control, Transparency & Mutual programs

Nov. 3, 2011

JIPDEC

Profile of the PrivacyMark® System

About JIPDEC

http://privacymark.org/

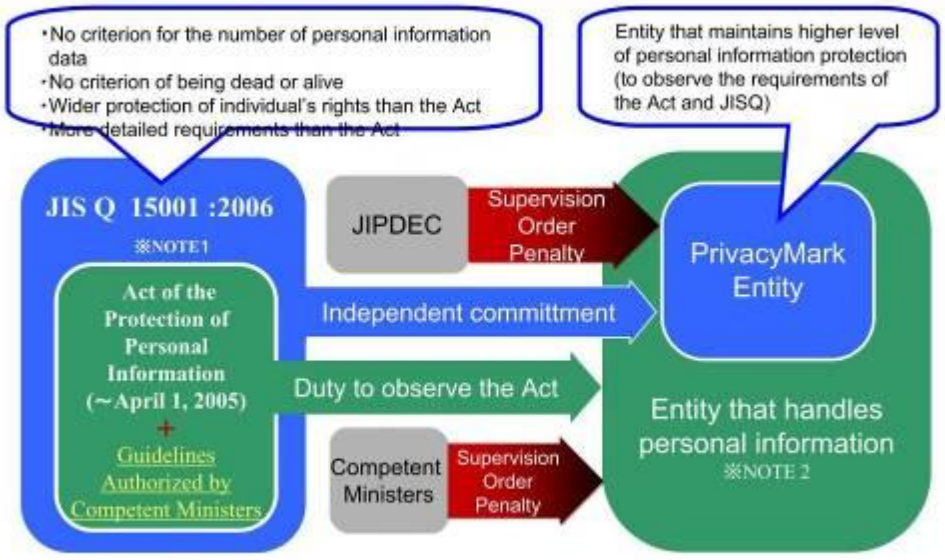
- ➢**Establishment** December 20, 1967
- ➢**Annual budget** 3 billion yen (fiscal year 2011)
- ➢**Number of Staff** 139 (as of April 1, 2011)
- ➢**Directors President** Tsutomu MAKINO
- ➢**Main Business**
  - Operation of the PrivacyMark® System ➢**Number of Staff: about 50**
  - Operation of the Information Security Management System (ISMS) Conformity Assessment System
  - Development and Promotion of Digital Information Uses
  - Promotion of Electronic Commerce and Electronic Data Interchange

(as of April 1, 2011)

Copyright© 2011 JIPDEC All rights reserved

本報告之智慧財產權歸屬於法務部

The Japanese Act and The PrivacyMark® System



NOTE 1: JIS Q15001 is the standards based on Industrial Standardization Law in Japan.

NOTE 2: It's total number of the personal information identified that makes up personal information databases, etc. used for its business not exceeding 5,000 on any given day in the last six months.

Copyright© 2011 JIPDEC All rights reserved

Profile of The PrivacyMark® System

1. Objectives:

- ➢ to enhance consumers' awareness of personal information protection
- ➢ to provide entities with an incentive to win social trust from consumers and business partners

2. Date of Commencement : April 1, 1998

3. Promotion Body: JIPDEC

4. Criterion: JIS Q 15001:2006 "Personal information protection Management Systems – Requirements"

Japanese Industrial Standard

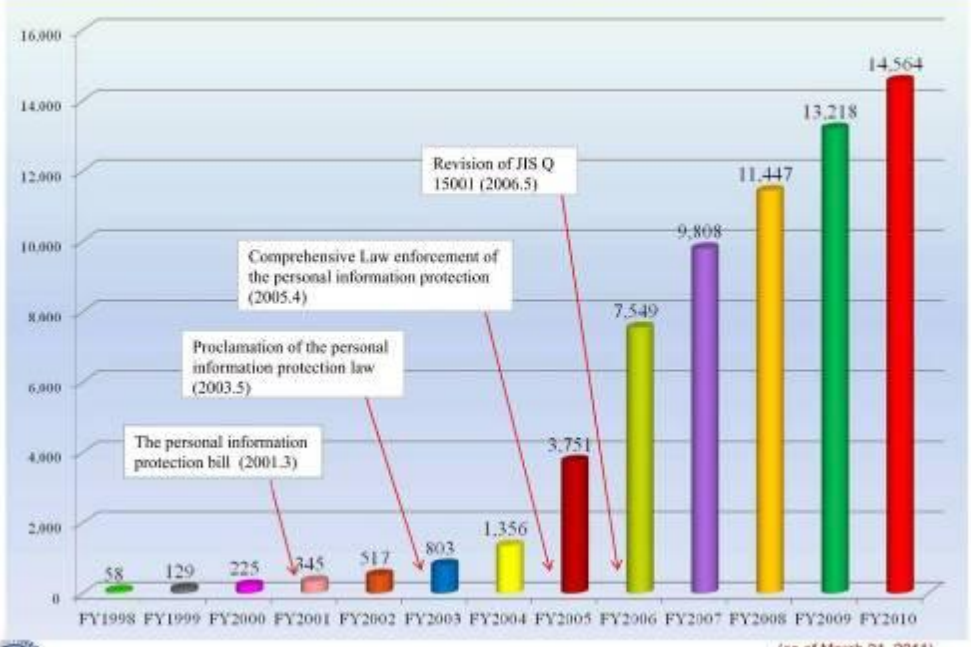
The PrivacyMark® System has adopted JISQ15001 as its assessment criterion since 1999 when the first edition was developed, encompassing the eight principles of OECD and extracting most of the concept of the EU Directive.

The second edition was made public in 2006.

Copyright© 2011 JIPDEC All rights reserved

本報告之智慧財產權歸屬於法務部

The accumulated number of PrivacyMark® entities

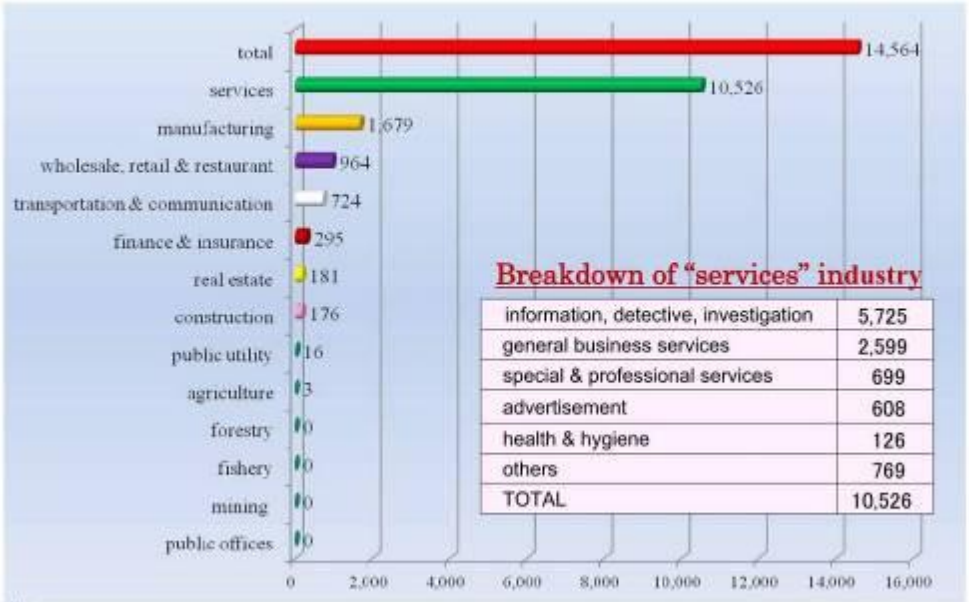


(as of March 31, 2011)

Copyright© 2011 JIPDEC All rights reserved

JIPDEC 4

The number of PrivacyMark® entities by industry



Breakdown of "services" industry

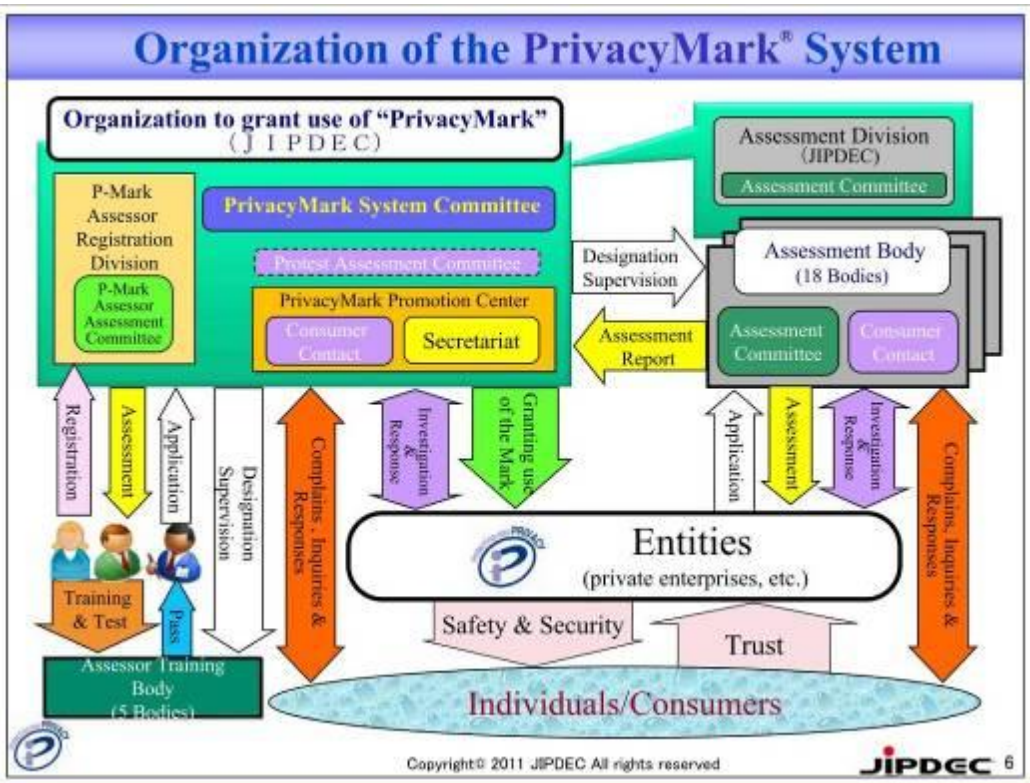
information, detective, investigation	5,725
general business services	2,599
special & professional services	699
advertisement	608
health & hygiene	126
others	769
TOTAL	10,526

(as of March 31, 2011)

Copyright© 2011 JIPDEC All rights reserved

JIPDEC 5

本報告之智慧財產權歸屬於法務部



The PrivacyMark® System

(1) The PrivacyMark® System Committee

■ **Committee Members:**

- **designate experts on personal information protection matters from the outside**
- **Members: Professors, Representatives of business groups, Representatives of consumers, Lawyers, etc.**

■ **Roles & Responsibilities:**

- **establishment and revision of rules and regulations of the System**
- **designation and cancellation of Assessment Body**
- **cancellation or suspension of the PrivacyMark® entities that violated PrivacyMark® System Rules and Regulations**
- **Operation of the System etc.**

Copyright© 2011 JIPDEC All rights reserved

本報告之智慧財產權歸屬於法務部

The PrivacyMark® System

(2) The Assessment Body

■JIPDEC and 18 Bodies:

・JIPDEC: Assessment Division

・18 Bodies: 12 industry-specific bodies and 6 regional bodies

■Roles & Responsibility:

・operating assessment business such as document assessment and on-site assessment, and assessment of whether applicants meet the requirements of JIS Q 15001:2006

・making final decisions referring to the Assessor's report at Assessment Committees

・reporting the results of the Assessment Committee to the PrivacyMark® System Committee

■ Assessment Committee

・Members : designated experts from the outside

➢experts of personal information protection,

➢professors,

➢representatives of business groups and consumers, lawyers, etc.

Copyright© 2011 JIPDEC All rights reserved

The PrivacyMark® System

(3) The PrivacyMark® Assessor Training Body

・5 Designated Bodies (as of March 31, 2011)

・operate a 5-day Course for new entries (Assistant Assessor) and a half-day Follow-up Course for all Assessors

(4) The PrivacyMark® Assessor Registration Division

■ operates registration of the PrivacyMark® Assessors

■ the number of Assessors registered

(Totaled 1,189 Assessors as of Sep 30, 2011)

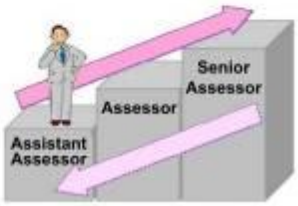
➢Senior Assessor : 280

➢Assessor : 278

➢Assistant Assessor : 631

■Assessor Assessment Committee

➢assesses whether or not the applicants have competence for the concerned qualification



Copyright© 2011 JIPDEC All rights reserved

本報告之智慧財產權歸屬於法務部

The PrivacyMark® System

(5) The PrivacyMark® Consumer Contact

- set up in JIPDEC and in each Assessment Body
- handles inquiries and complaints on personal information issues free of charge
- investigates cases and provides results with the perso including entities' remedial actions, if any.
- The contact of JIPDEC is composed of four regular consultants and a part-time consultant in addition to a manager and an assistant.
- The number of the cases handled in FY2010 was 379.

Copyright© 2011 JIPDEC All rights reserved

The PrivacyMark® System

(6) The Protest Assessment Committee (ad-hoc committee)

In the case of a protest or complaint about the matters below filed by any PrivacyMark® entity, applicant for a PrivacyMark® entity or Assessor position, person who took a course for Assessors, and consumers, the Protest Assessment Committee shall be temporarily set up in the PrivacyMark® System Committee.

- ➢ on the result of new entry or renewal assessment for use of the PrivacyMark®, Assessment Boby, Assessor Training Body from the applicants concerned
- ➢ on the result of assessment by Assessor Training Body from the applicants
- ➢ any related complain on the System, each Body, etc. from consumers, etc.

and the like

Copyright© 2011 JIPDEC All rights reserved

本報告之智慧財產權歸屬於法務部

The PrivacyMark® System

Procedure

Entity(Applicant) shapes its PMS which is in compliance with JISQ15001:2006.

↓

Application officially accepted by JIPDEC※1

↓

PMS documents assessment by JIPDEC※1

↓

Operation review by an on-site assessment of JIPDEC※1&2

↓

Assessment report reviewed & assessed by Assessment Committee

↓

Notification of the result (Approved or Not Approved)

↓

Granting use of PrivacyMark and announcing the entity on the HP

about four to six months

※NOTE: 1. by JIPDEC or the Assessment Body received an application from an entity(applicant)
2. in general, an on-site assessment conducted by an unit of two assessors for a day (in case of a large size business operator, for two or three days) and if needed, an instruction for improvement issued to the entity concerned

Copyright© 2011 JIPDEC All rights reserved

The PrivacyMark® System

➢The concept of JISQ15001 is continuous improvement based on by the PDCA Cycle.

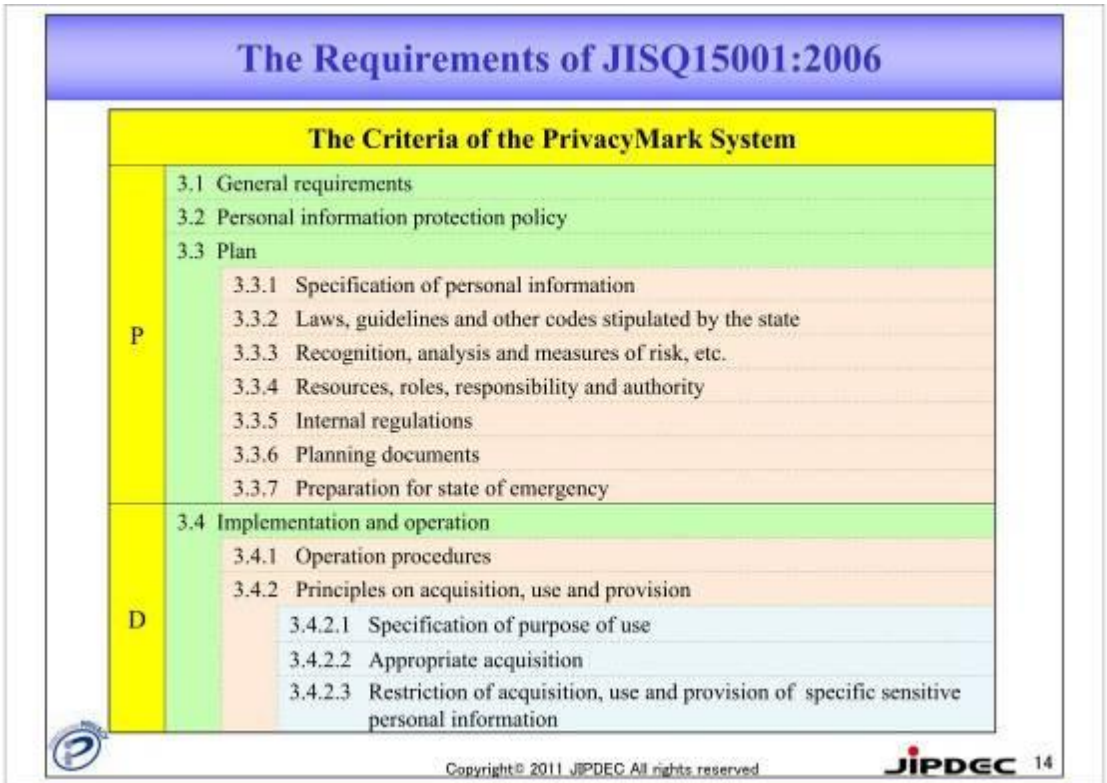
➢The System assesses whether or not applicants' PMS※ adequately manage risks on handling of personal information.

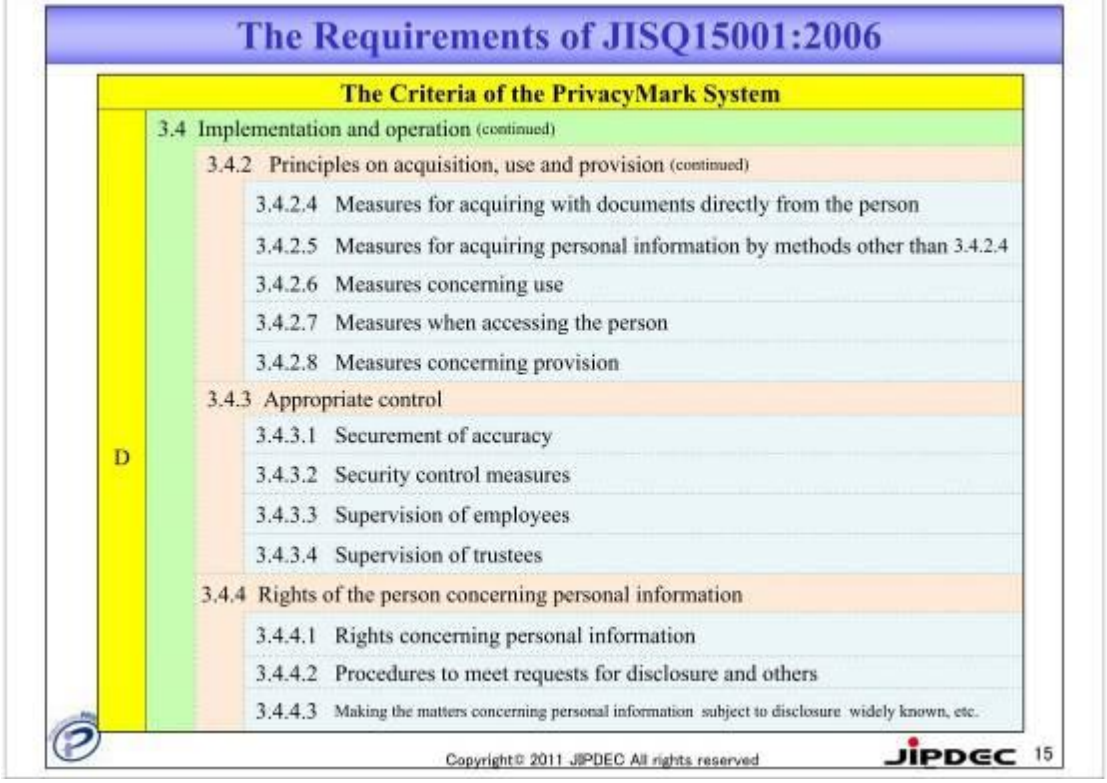
※PMS: Personal information protection Management System

➢ Refer to page 7-8 for the two stages of the assessments.

Copyright© 2011 JIPDEC All rights reserved

本報告之智慧財產權歸屬於法務部





本報告之智慧財產權歸屬於法務部

The Requirements of JISQ15001:2006

The Criteria of the PrivacyMark System	
D	3.4 Implementation and operation (continued)
	3.4.4 Rights of the person concerning personal information (continued)
	3.4.4.4 Notification of purpose of use of personal information subject to disclosure
	3.4.4.5 Disclosure of personal information subject to disclosure
	3.4.4.6 Correction, addition or deletion of personal information subject to disclosure
	3.4.4.7 Veto of use or provision of personal information subject to disclosure
	3.4.5 Education
	3.5 Personal information protection management system documents
	3.5.1 Range of documents
	3.5.2 Document control
	3.5.3 Record control
	3.6 Response to complaints and consultations
C	3.7 Inspection
	3.7.1 Confirmation of operations
	3.7.2 Audits
A	3.8 Corrective actions and preventive actions
	3.9 Review by the representative of the business entity

Copyright© 2011 JIPDEC All rights reserved

The PrivacyMark® System

Major Assessment Items of the PrivacyMark® System

1. Document Assessment : 122 items

- It should announce its privacy policy (personal information protection policy).
- It should establish its PMS.
- It should establish the procedures to implement the PMS.
  - how to acquire, use and provide personal information
  - how to response to the inquiries from the persons concerned (disclosure, correction, deletion, etc.)
  - education, inspection(confirmation & audit), corrective and preventive action, review of PMS, etc.

2. On-site Assessment: Operations / Security Safeguards 52 items / 41 items

- It should implement, maintain, review and correct its PMS.
- It should specify all kinds of personal information and recognize risks on the handling of the personal information.
- It should analyze the risks and take appropriate security control measures.
- It should handle the information in accordance with the procedures.
- It should provide all of managements and employees with education on the personal information protection.
- It should implement audit process.
- It should implement corrective and review process.

Copyright© 2011 JIPDEC All rights reserved

本報告之智慧財產權歸屬於法務部

The Fee Structure of the PrivacyMark® System

UNIT:1,000JPY (Tax included)

Category	New Application			Renewal		
Scale	Small	Medium	Large	Small	Medium	Large
Application Fee	50	50	50	50	50	50
Screening Fee	200	450	950	120	300	650
Mark Use Fee	50	100	200	50	100	200
Total	300	600	1,200	220	450	900

- The effective period of the mark use fee is for **2 years**.
- Business scale

Large: Business operators on a scale exceeding that of medium scale business operators

Small: Business operators with a number of full-time employees of 20 or less. In the case for wholesalers, retailers (including food outlets) and services, with a number of the employees of 5 or less

Medium:

	Manufacturers and Others	Wholesalers	Retailers	Services
Capital	300 million or less	100 million or less	50 million or less	50 million or less
Persons※	300 or less	100 or less	50 or less	100 or less

※NOTE: the number of the persons who belong to the entity such as employees, directors and the like

Copyright© 2011 JIPDEC All rights reserved

The PrivacyMark® System

Mutual Recognition Programs by JIPDEC

1. with DSIA (Dalian Software Industry Association), China

Since June 2008

http://www.pipa.gov.cn/Default.asp

- DSIA comprehensively introduced the PMS based on JIS Q 15001: 2006 with full cooperation of JIPDEC.
- DSIA implements the same operations as PrivacyMark System so that it may allow Japanese entities to outsource their business to PIPA-Mark entities without much efforts on investigating foreign trustees.

Copyright© 2011 JIPDEC All rights reserved

本報告之智慧財產權歸屬於法務部

The PrivacyMark® System

Mutual Recognition Programs by JIPDEC

(continued)

2. with KAIT (Korea Association of Information and Telecommunication)

Since September 2002

➢ The mutual recognition program with KAIT is for online environment.

Copyright© 2011 JIPDEC All rights reserved

The PrivacyMark® System

Mutual Recognition Programs by JIPDEC

(continued)

3. with Triple I (Institute for Information Industry), Taiwan

MOU : in July 2010

➢ Triple I has been developing , what we call, the Taiwan version of the PrivacyMark System entrusted by Taiwan Government since the proclamation of comprehensive personal information protection law in Taiwan.

➢ JIPDEC provides know-how of the System with Triple I based on the MOU made in July 2010 in order to commence the pilot test in June 2011 and the mutual recognition program in the future.

Copyright© 2011 JIPDEC All rights reserved

本報告之智慧財產權歸屬於法務部

資料來源：本簡報由關本貢提供

本報告之智慧財產權歸屬於法務部

（三）綜合座談摘要記錄

1.問：現在公司常跨國經營或委外，各位專家對台灣此跨境傳輸趨勢有何建議?

答：

（1）JIPDEC 隱私標章推動中心関本貢副中心長：

以日本國內情形而言，日本的隱私標章無法在外國做驗證，且對象也只限日本企業，雖然外國人資料在日本國內時會受保護，但移出國外的部分就有賴與 APEC 的日後合作。

（2）Rachael Spalding 政策助理委員：

在澳洲，委外時仍必須遵守澳洲法，私部門其實也願意配合，因符合其利益。

（3）Joshua Harris 副主席：

這可以透過契約約定來實行,但這不意謂簽約後委託人即免責，相反地，委託人仍須監督受託人，另一方面可用問卷來使相關廠商確認其符合相關原則，或者可以另有白名單列出合格廠商。

（4）加藤隆之副教授：

我認為這部份有賴國際間彼此合作,當然國內法的進展與此是可一同併進的。

2.問：各國對雲端產業跨境傳輸的個資保護有無特別做法？

答：

本報告之智慧財產權歸屬於法務部

（1）Joshua Harris 副主席：

美國並無特別法規，SLA 等都必須考慮相關的原則，我們並不想制訂一個特別的要求，重要的是不要讓廠商因為特別的法規，為規避責任而轉移資料中心設置地點。

（2）Rachael Spalding 政策助理委員：

法律是科技中立的，如果去規範特定技術，就會不得不一直修法，所以原則規定較佳。

（3）加藤隆之副教授：

日本也無相關法律規範，雲端的環境有時不知道相關的資料是放在何地域，很難以特定法律來規制。

（4）JIPDEC 隱私標章推動中心関本貢副中心長

日本法規確實未能直接針對雲端做規範，唯一相近的只有利用契約來做，但其實一般人還不太了解雲端，也許了解更多後就可以反應在法規中。

3.問：各國政府間可能也會有跨境傳輸，目前有何協定來做這個部份，又如何判斷其適用界線?

答：

（1）Joshua Harris 副主席：

在美國有一個規範，但因為業務關係，我本人不甚清楚這部份，我後續可以再請教我的同事再回覆您。

（2）Rachael Spalding 政策助理委員：

本報告之智慧財產權歸屬於法務部

澳洲有不同領域的特別法規定,因此如有其他法律以進行相關規範，即可據以處理。

4.問：是否請各位外賓就網路、網站的跨國境傳輸個資保護最新狀況提供分享？

答：

（1）Joshua Harris 副主席：

以 APEC 的運作方式為例，是以資料蒐集點在何處區分，例如資料若蒐集在越南,那越南就可以來處理,當然這只是開始點，實際情況很複雜。

（2）Rachael Spalding 政策助理委員：

一般來說,網站都有很多條款,教育消費者有自保概念也很重要。

（3）加藤隆之副教授：

資料存取前應先經過同意，目前這還不夠，例如現在我們 google 自己的名字，會得到很多資訊，但 Google 並沒有先取得我們的同意，目前日本尚不知如何解決。

本報告之智慧財產權歸屬於法務部

Privacy in Australia

2 November 2011

Presenter: Rachael Spalding
Assistant Commissioner Policy
Office of the Australian information Commissioner
www.oaic.gov.au

Foreword

This article hopes to give you a general overview of The Office of the Australian Information Commissioner(OAIC)¸Australian privacy regulation at the national level, and the privacy law reform in Australia. The article will also briefly discuss privacy issues arising from:

1. How the OAIC handles complaints and investigate potential breaches of privacy
2. How Australia regulates the transfer of information overseas
3. The OAIC's experience, as a privacy regulator, with international privacy co-operation.

The role of the OAIC

The OAIC is an independent Government agency. The OAIC's aim is to protect information rights and advance information policy.

The OAIC was formed on 1 November 2010 following reforms which brought together, for the first time in one agency, functions relating to the regulation of privacy and freedom of Information (or FOI), as well as functions relating to Government information policy and management.

The former Office of the Privacy Commissioner (OPC), which was the national privacy regulator, was integrated into the OAIC. The establishment of a single agency responsible for privacy, FOI and information policy contributes to the Australian Government's overarching objective to deliver consistent information policy across government.

本報告之智慧財產權歸屬於法務部

The OAIC has three commissioners – the Information Commissioner, the Privacy Commissioner and the FOI Commissioner. The Commissioners are appointed by the Australian Government. The introduction of an Australian Information Commissioner as well as a FOI Commissioner has resulted in a more cohesive approach to Government information handling and release.

The Information Commissioner has a broad function to report on the Federal Government's policy and practice regarding the handling and accessibility of information held by the Government. This significantly assists in promoting a culture of coordinated and responsible information handling and management. The Information Commissioner is also vested with the FOI and Privacy functions, which can generally be delegated to the Privacy Commissioner or the FOI Commissioner.

The OAIC also relies on advisory bodies such as the newly formed Information Advisory Committee (IAC).The aim of the IAC is to assist and advise the Australian Information Commissioner in matters relating to the performance of the Information Commissioner functions. Other than the Information Commissioner, the inaugural IAC members were appointed in September 2011.

The OAIC also receives strategic advice and support from the Privacy Advisory Committee (PAC). The PAC consists of no more than six members who advise the Information Commissioner on privacy matters relating to his or her field of expertise, recommend materials for inclusion into guidelines that are issued by the Commissioner and engage in and promote community education and consultation in relation to the protection of individual privacy.

The OAIC's extensive range of functions include:

1. handling complaints about privacy and FOI
2. merit review of FOI decisions
3. monitoring compliance with privacy and FOI laws
4. legislative review of those laws
5. providing privacy, FOI and information policy advice to government and business, and promoting and encouraging the adoption of privacy standards in the community.

The Privacy Commissioner's functions and powers remain unchanged, although a new aspect of his role is that he can also carry out the OAIC's FOI functions if needed. The legislative basis of the OAIC's privacy functions is drawn primarily from the *Privacy Act 1988*.

本報告之智慧財產權歸屬於法務部

Privacy regulation in Australia

The Privacy Act provides protection for personal information that is handled by:

1. Australian Government agencies (including the Australian Capital Territory and Norfolk Island but does not include other States or Territories who generally have their own privacy regimes)
2. Credit providers and reporters
3. All private health service providers
4. Businesses with an annual turnover of more than $3 million
5. Not-for-profit organisations across Australia
6. Some other small businesses (e.g. who trade in personal information).

The Privacy Act creates a single, nationally consistent framework for protecting privacy. However, for constitutional reasons, a number of states and territories within Australia also have their own system of privacy regulation. State privacy laws tend to regulate the State public sector (including the public health system). Where there are inconsistencies with State or Territory laws, national legislation prevails. This overlapping system can create complexity and difficulties for business, such as healthcare providers. The Australian Government has indicated that working towards a nationally consistent privacy framework is an important priority – this is an issue I will cover later in my presentation.

As a way to share information and promote consistent privacy practice within Australia, Privacy Authorities Australia (or PAA) was established in April 2008. PAA membership includes privacy representatives from all states and territories as well as the Australian Privacy Commissioner. PAA meets on a regular basis to promote best practice and consistency of privacy policies and laws.

In Australia, federal privacy legislation is primarily concerned with information privacy. That is, it regulates the manner in which individuals' personal information is handled by the private and public sector.

'Privacy' I am referring to the protection of personal information or 'data'. I am not referring to related concepts like bodily or territorial privacy, which lie outside the scope of the Privacy Act.

So, what is personal information?Under Australian law, personal Information is information that identifies you or could identify you. There are some obvious examples of personal information, such as your name or address. Personal information can also include medical records, bank account details, photos, videos,

本報告之智慧財產權歸屬於法務部

and even information about what you like, your opinions and where you work - basically, any information where you are reasonably identifiable. Information does not have to include your name to be personal information. For example, in some cases, your date of birth may be enough to identify you.

The Privacy Act does not cover de-identified statistical data, where individuals cannot reasonably be re-identified. The de-identification of personal information highlights the issue of government openness and transparency and how this interacts with individual privacy. It is important that governments continue to make available to the public as much information as possible. As a great amount of information held by government likely relates to individuals, the de-identification (also known as anonymisation) of personal and sensitive information becomes more important.

In the Australian context, most public information which is released is specifically understood not to include personal information. However, some information released will include personal information. Also, technological developments may mean that there is scope for such data to become de-anonymised in the future. It is the role of organisations such as the OAIC, which has functions relating both to government transparency and the protection of personal information, to ensure that an appropriate balance is struck between these two competing interests.

Another important category of personal information in the Privacy Act is sensitive information. Sensitive information is a subset of personal information. It includes health information as well as information about an individual's religion, race, sexual preferences or criminal record. The Privacy Act imposes stricter rules about when sensitive information can be collected and how it should be handled. Usually, sensitive information can only be collected with the individual's consent and there are tighter restrictions on how this type of information can be used and disclosed.

The Privacy Act has two sets of principles which regulate the collection, use, disclosure and security of personal information:

1. 11 Information Privacy Principles (IPPs) – which apply to Federal and some territory government agencies (specifically the Australian Capital Territory and Norfolk Island). As I noted earlier, other state and territory governments do not fall under the jurisdiction of the Privacy Act
2. 10 National Privacy Principles (NPPs) - which regulate the way private sector organisations collect, use disclose and store personal information.

The IPPs and the NPPs are similar, though not identical. For example, the NPPs (unlike the IPPs) provide obligations which cover the international transfer of data

本報告之智慧財產權歸屬於法務部

(which we call transborder dataflows), and provide specific regulation for sensitive information. Both sets of Privacy Principles contained in the Privacy Act are not prescriptive and are technology neutral. That is, they don't tell agencies and organisations what they must do in each situation or how to apply specific technologies. Instead, they offer principles about the way in which personal information should be handled, and each agency or organisation needs to apply those principles to its own situation.

Organisations or industries may also apply to the Commissioner for approval of a privacy code. If approved, the code can replace the NPPs for organisations bound by it. The obligations in any privacy code must be at least equivalent to those in the NPPs. The advantage of the code is that a particular sector can agree on how the principles will be applied by that sector. Some organisations (such as small businesses – meaning businesses with an annual turnover of less than $AU3 million) and some acts or practices (such as those of journalists and political parties) are also exempted from the Privacy Act.

Having two sets of principles is not ideal. Privacy law reform is firmly on the agenda in Australia and consolidation of the two sets of privacy principles to a single set is a likely outcome.

Privacy law reform in Australia

In addition to all the activity around the establishment of the OAIC, it has also been monitoring a range of privacy-related reforms at the national level.

In 2006, the Australian Attorney-General asked the Australian Law Reform Commission (ALRC) to begin a review of privacy law in Australia. The ALRC is a Government agency that reviews Australia's laws. The ALRC conducts inquiries into areas of law at the request of the Attorney-General of Australia. Although the ALRC cannot initiate its own inquiries, it is independent of government. The ALRC makes recommendations to government so that government can make informed decisions about law reform, but the ALRC's recommendations do not automatically become law.

After a 2 year enquiry the ALRC released a report on its review of Australian privacy law in May 2008 (known as Report 108 – 'For Your Information: Privacy Law and Practice'). The ALRC's report contains 295 recommendations, relating to:

1. Simplifying and streamlining the Privacy Act

本報告之智慧財產權歸屬於法務部

2. Uniform privacy principles that apply to both the private and public sector
3. National consistency
4. Regulating trans-border data flows
5. Reconsideration of exemptions and exceptions
6. Improved complaint handling and stronger penalties
7. More comprehensive credit reporting (also known as positive credit reporting)
8. Health privacy
9. Data breach notification, and
10. A cause of action for a serious invasion of privacy

The Australian Government indicated that it would respond to the ALRC's recommendations in two stages. The Government's First Stage Response to the ALRC Report – 'Enhancing National Privacy Protections' - was released in October 2009. It responds to 197 of the 295 recommendations. It focuses on the following areas which will establish the foundations for ongoing reform:

1. A new, single set of privacy principles called the Australian Privacy Principles or APPs
2. Reform of credit reporting regulation
3. Enhanced powers for the OAIC, and
4. Reform of the health and research provisions of the Privacy Act.

The Australian Government is approaching these reforms by preparing exposure draft legislation in relation to each area. So far, the Government has released exposure draft legislation relating to the APPs, and also for the credit reporting provisions.

Each piece of exposure draft legislation has been referred to a Senate Committee for inquiry and report. The Senate Committee has invited public comment on that legislation.

The Government's first stage response outlined the Government's position on:

1. The development a single set of Privacy Principles
2. The redrafting and updating of the structure of the Privacy Act
3. Measures proposed to address the privacy impact of new technology
4. Amendments to the Privacy Act to strengthen and clarify the powers and functions of the Privacy Commissioner
5. The introduction of comprehensive credit reporting and enhanced protections for credit reporting information, and
6. Enhancing and clarifying the protections around the sharing of health information and the ability to use personal information to facilitate research in the public interest.

本報告之智慧財產權歸屬於法務部

The Government's response also addresses national consistency. It notes that the transition to a single set of Privacy Principles will mark a significant step toward consistent privacy laws in Australia. For the first time, a single privacy regime will apply across both the private sector and the Commonwealth public sector. The Government's response also notes that the proposed reforms will create a platform from which it can pursue national harmonisation through discussion with the states and territories. However, for now, State privacy laws will continue to regulate the State public sector (including the public health system). Ultimately, the goal is consistent set of privacy standards for the Commonwealth, state and territory public sectors, as well as the private sector.

In June 2010, the Government released an exposure draft of the Australian Privacy Principles (APPs). The draft APPs are a single set of principles that unify and replace the IPPs and the NPPs, and will apply to both the private and public sector. The draft APPs are a response to the ALRC's recommendation that the Privacy Act be restructured around a unified set of principles, rather than applying different principles to the public and private sectors. The ALRC thought that this would clarify and simplify obligations, and promote national consistency in privacy regulation.

The draft Australian Privacy Principles (as the name implies) are principles-based law and will continue to regulate agencies and organisations in a flexible way, and be as technology neutral as possible. There are 13 draft APPs which are structured to reflect the flow of information—from collection, through to use and disclosure and access and correction.

The APPs will represent a significant change for Australian Government agencies, particularly as many of the APPs are based on the National Privacy Principles which currently regulate the private sector. This Australian model for a single set of privacy principles reflecting the flow of information may be of interest to other jurisdictions including here in Taiwan. It is the OAIC's view that consistency and simplicity of regulation will also empower individuals to understand and exercise their privacy rights.

The Australian Government released an exposure draft of the Australian Privacy Principles in June this year (2011). It was referred to the Australian Senate's Finance and Public Administration Committee for inquiry and report. The Senate Committee invited public comment on the draft legislation.

本報告之智慧財產權歸屬於法務部

The Senate Committee received submissions from businesses, government and a number of public interest groups. This reflects the interest that the privacy reforms have attracted in Australia.

The OAIC also made a substantial submission aimed at maximising this opportunity to improve the Act. The OAIC also made a submission in relation to the exposure draft of the credit reporting provisions of the Act, and intends to do the same in relation to subsequent exposure drafts, once that legislation is released.

The Senate Committee's final Report into the draft APPs was tabled in the Australian Parliament on 15 June 2011. The committee recommended simplifying the draft APPs in a number of areas, and also the production of various guidance material to aid interpretation. The committee's recommendations generally avoid re-examining the Government's policy positions on which the draft APPs were based. Further privacy reform activity in relation to online privacy, health and credit reporting, is continuing.

Key responsibilities of the OAIC

I turn to one of the key responsibilities of the OAIC – complaint handling. I will focus on the current powers of the OAIC in relation to complaint handling, as well as proposals for new powers as part of the current privacy law reform process.

Under the current Privacy Act, individuals who believe that their privacy may have been interfered with by an agency or organisation are able to lodge a complaint with the OAIC. The OAIC may then undertake preliminary inquiries of the respondent to determine whether there are grounds, and whether the Privacy Commissioner has jurisdiction, to formally open an investigation into the complaint.

Under the Privacy Act, the OAIC is generally required to investigate a breach of privacy where an individual has complained to the OAIC. Where a breach of privacy has occurred, the OAIC generally tries to resolve the complaint on a case by case basis through conciliation. If the parties cannot reach an agreement, the OAIC has the power to make a determination that there has been a breach of privacy and that the respondent should, for example, provide compensation. However, we see this as a last resort and encourage parties to resolve the complaint through conciliation. We find that this generally provides the most satisfying outcome for the complainant.

The Commissioners have the power to investigate matters on their own motion about potential interferences with privacy without first receiving a complaint from an

本報告之智慧財產權歸屬於法務部

individual. However, under the current Privacy Act, the OAIC is unable to impose a penalty on an agency or organisation when the Commissioner has initiated an investigation on his own motion, without a complainant. Instead, in cases where we have investigated matters using the own motion power, the OAIC works closely with the agency or organisation to ensure ongoing compliance and better privacy practice. For example, in recent investigations, such as one involving Google Street View, we have settled upon agreed undertakings with the organisation.

Other recent own motion investigations have included:

1. unauthorised persons accessing the personal information of a corporation's customers in Australia and overseas, including individuals' names, addresses and credit card details
2. a mailing list error by a large company resulted in thousands of letters with incorrect addresses being mailed out which may have caused the 'personal information' (including names and telephone details) of some of its customers to be improperly disclosed.

The OAIC generally commences an investigation on its own motion when it becomes aware of data breaches – that is, instances where personal information held by agencies or organisations has been compromised.

The Privacy Act does not impose an obligation on agencies or organisations to notify individuals whose personal information has been compromised – often referred to as data breach notification. However, the Privacy Act does require that agencies and organisations take reasonable steps to maintain the security of the personal information they hold. Failure to do so constitutes a breach of our current laws.

Also, the OAIC recommends notification to affected individuals, and in certain cases, to the OAIC, as one of the steps in our best-practice guide to data breach handling, which is available on our website. The OAIC has also recently begun publishing the results of investigations that we have initiated on our own motion. Our experience has been that this encourages organisations to follow best practice when it comes to handling data breaches – that is, to respond quickly and mitigate the impact on individuals, including by notifying individuals and/or the OAIC of the fact that personal information has been compromised.

The Australian Government has indicated that it will introduce new laws to strengthen the powers of the OAIC. The Government has not yet released exposure draft legislation in this area, but it has stated that it intends to make amendments so that the Information Commissioner can:

本報告之智慧財產權歸屬於法務部

1. make an enforceable determination on an own motion investigation
2. accept undertakings from agencies or organisations and, if necessary, enforce those (through a court), and
3. seek (through a court) a civil penalty for serious or repeated offences.

The OAIC would rather not have to use such powers. Our recent experience in relation to our own motion investigations, such as Google Street View, show how agreed undertakings can operate successfully. Nevertheless, overseas experience has indicated that regulators with the power to pursue large penalties will often do so, and the OAIC may, in appropriate cases, do the same.

In the OAIC's view, the greatest benefit of additional powers for the Information Commissioner would be that they provide added credibility for enforcement of privacy law, reinforce the significance of privacy compliance, and give everyone an even greater incentive to take privacy more seriously.

It should also be noted that the OAIC's ability to rely on alternative enforcement mechanisms are also indicative of Australia's stable political landscape which has enabled the Government to rely on informal, co-operative and flexible forms of regulation. For this reason, the Australian private sector is generally receptive to good privacy practice proposals from Government or the OAIC, in instances where Australian privacy law prescribes no obligations, such as data breach notification.

The OAIC doesn't just handle complaints and respond to privacy breaches. Importantly, we also have an educative role – to encourage the adoption of privacy standards more broadly across our community. The OAIC also has an advising role – to give advice to federal and some other agencies, as well as the private sector, as to how privacy can be promoted in their functions and activities. The OAIC's approach has always been to place great emphasis on the policy development and policy advising role of the Office. Our experience has been that it is easier and more productive to influence the development of policies and initiatives in the formative stage rather than trying to add privacy considerations on at the end. It is a much better public policy outcome to have privacy 'built in' rather than 'bolted on'.

Regulation of international transfer of information in Australia

A significant privacy challenge faced by Australia and other countries is the increasing transfer of information overseas. In brief, National Privacy Principle 9 (NPP 9) states that an Australian private sector organisation can only transfer personal

本報告之智慧財產權歸屬於法務部

information of Australians to foreign countries, if it satisfies one of several listed conditions. This includes where the individual consents; or where the organisation reasonably believes that the foreign recipient is subject to a law, binding scheme or contract that imposes substantially similar principles to those of the NPPs. The aim of NPP 9 is to ensure that Privacy Act obligations cannot be avoided by sending personal information offshore.

The Australian Government is looking to introduce new Australian Privacy Principles which will apply to both the public and private sectors. Proposed Australian Privacy Principle 8 (APP 8) deals with cross-border disclosures of personal information. APP 8 states that before an organisation or Australian Government agency discloses personal information to an overseas recipient, generally it must take reasonable steps to ensure the overseas recipient does not breach the APPs in handling that information. The organisation or agency will also retain accountability for the overseas recipient's handling of the information. While it is based on NPP 9, the new principle uses the concept of 'accountability' as the basis for organisations to be responsible for the protection of the personal information of their customers. This is more consistent with the approach adopted in international regimes, such as the APEC Privacy Principles, in particular the 'accountability principle'.

International Cooperation

Following on from my point about NPP 9 and draft APP 8, the OAIC is conscious of the importance of international cooperation in regulating the international transfer of information and the investigation of breaches. International cooperation and coordination is increasing in importance as more organisations operate on a global level, and technologies increase the ability to collect and transfer information. The Internet, for example, means that information is easy to access and publish; it is searchable, downloadable and reusable and can remain in circulation indefinitely. Personal information released online can be difficult to recoup, delete or control.

These technological developments have created privacy challenges in relation to the protection of information privacy. Privacy breaches can now occur in an increased number of ways and the potential scale of breaches has increased as has the potential impact of and damage caused by such breaches.

In addition, in Australia there is uncertainty as to how the Privacy Act applies to personal information submitted via the Internet by individuals in Australia to an overseas organisation.

本報告之智慧財產權歸屬於法務部

Recognising the constantly changing global environment and the increasing information flows around the Asia-Pacific region and the world, the OAIC is involved in a number of forums for international cooperation, policy development and knowledge sharing. The OAIC has actively participated in recent work done to strengthen international cooperation on privacy regulation, such as the APEC Cross-border Privacy Enforcement Arrangement (CPEA) which came into operation in July 2010. The CPEA sets out a framework for voluntary cooperation and assistance between participating authorities on privacy enforcement related activities. The OAIC is a co-administrator of the Arrangement, and was closely involved in its development.

The OAIC is also a member of the Global Privacy Enforcement Network (GPEN) of privacy enforcement authorities, which was launched in March 2010. The GPEN is an inclusive network of privacy enforcement authorities established to:

1. discuss the practical aspects of privacy law enforcement co-operation
2. share best practices in addressing cross border challenges
3. work to develop shared enforcement priorities
4. support joint enforcement initiatives and awareness campaigns.

The OAIC also participates in the Asia Pacific Privacy Authorities (APPA) forum, along with privacy regulators from New Zealand, Hong Kong, Korea, Canada's federal regulator and British Columbia, together with the Australian State and territory privacy regulators. APPA is the principal forum for privacy authorities in the Asia Pacific Region to form partnerships and exchange ideas about privacy regulation, new technologies and the management of privacy enquires and complaints.

The OAIC's limited powers under the Privacy Act, and the uncertainty about jurisdiction in relation to personal information submitted by the internet, has meant that the OAIC has had to rely on other useful mechanisms – such as international cooperation – for privacy investigations concerning multi-nationals. I will highlight some examples from the OAIC's experience where the development of coordinated international approaches has resulted in positive outcomes.

In April 2011 the OAIC commenced an "own motion" investigation into a report from Sony Computer Entertainment Europe Limited (SCE Europe) that its database had been hacked and that the personal details of up to 77 million customers may have been compromised.

Within Australia, the OAIC sought information from Sony Computer Entertainment Australia (SCE Australia), a related company. The investigation involved a review

本報告之智慧財產權歸屬於法務部

of the acts and practices of both SCE Australia and its related companies. As the incident occurred outside of Australia, our Privacy Act will only apply where the requirements of the extraterritorial provisions of the Act are met.

While the incident did not constitute a breach of our Privacy Act, during the course of the investigation the Privacy Commissioner obtained information on the inter-relationship of the various Sony entities involved in this matter. This information demonstrated the potential challenges for agencies, such as the OAIC, that regulate the flow of personal information where large global companies undertake different functions relating to the provision of services and products, including the collection of personal information, while operating out of different jurisdictions. In recognition of this the Privacy Commissioner provided a copy of his investigation report to privacy regulators in the APEC member economies, for their consideration.

In May 2010, Google identified that it may have inadvertently collected personal information as part of its Street View mapping, when it collected open (non-password protected) WiFi network locations. At the same time Google notified the OAIC in Australia of this issue, it also notified 28 other jurisdictions in relation to the same issue. In considering Google's advice and commencing an investigation, the OAIC worked informally with some of its APPA partners to share information and discuss a range of common issues. While this did not formally invoke the CPEA arrangements, OAIC liaised closely with several of its counterparts. This informal liaison would not have been possible without the CPEA mechanisms in place. Each jurisdiction came to a similar conclusion about Google's collection of personal information and the remedies adopted in each jurisdiction were similar.

本報告之智慧財產權歸屬於法務部

The Asia Pacific Economic Cooperation's Cross Border Privacy Rules System

2 November 2011

Presenter: Joshua Harris
Associate Director, Office of Technology and Electronic Commerce
U.S. Department of Commerce &
Vice Chair
APEC Data Privacy Subgroup

The APEC Privacy Framework

The Data Privacy Subgroup developed the APEC Privacy Framework in 2004. The Framework is a set of nine principles to assist APEC economies in developing privacy approaches that maximize privacy protection and the continuity of cross-border information flows.

The APEC Privacy Principles

1. Preventing Harm
   Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

2. Notice
   Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include:
   (1) the fact that personal information is being collected;
   (2) the purposes for which personal information is collected;
   (3) the types of persons or organizations to whom personal information might be disclosed;
   (4) the identity and location of the personal information controller,

本報告之智慧財產權歸屬於法務部

including information on how to contact them about their practices and handling of personal information;

(5) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.

3. Use

Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except:

(1) with the consent of the individual whose personal information is collected;

(2) when necessary to provide a service or product requested by the individual; or,

(3) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

4. Collection Limitation

The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

5. Choice

Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.

6. Security Safeguards

Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

7. Integrity

Personal information should be accurate, complete and kept up-to-date to the

本報告之智慧財產權歸屬於法務部

extent necessary for the purposes of use.

8. Access and Correction

Individuals should be able to:

(1) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;

(2) have communicated to them, after having provided sufficient proof of their identity, personal information about them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; in a form that is generally understandable; and challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.

The individual should be provided with reasons why and be able to challenge such denial. Such access and opportunity for correction should be provided except where:

(1) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question;

(2) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or

(3) the information privacy of persons other than the individual would be violated.

9. Accountability

A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

The Role of Cross Border Privacy Rules

The Framework states that international implementation of these principles may be achieved through Cross Border Privacy Rules (CBPRs). CBPRs are a set of voluntary

本報告之智慧財產權歸屬於法務部

rules developed by an organization based upon the APEC Privacy Principles. The organization then commits to apply these rules to its activities involving transfers of personal information across borders

Source: Author Joshua Harris

圖 32：CBPRs In Practice: A Four Step Approach

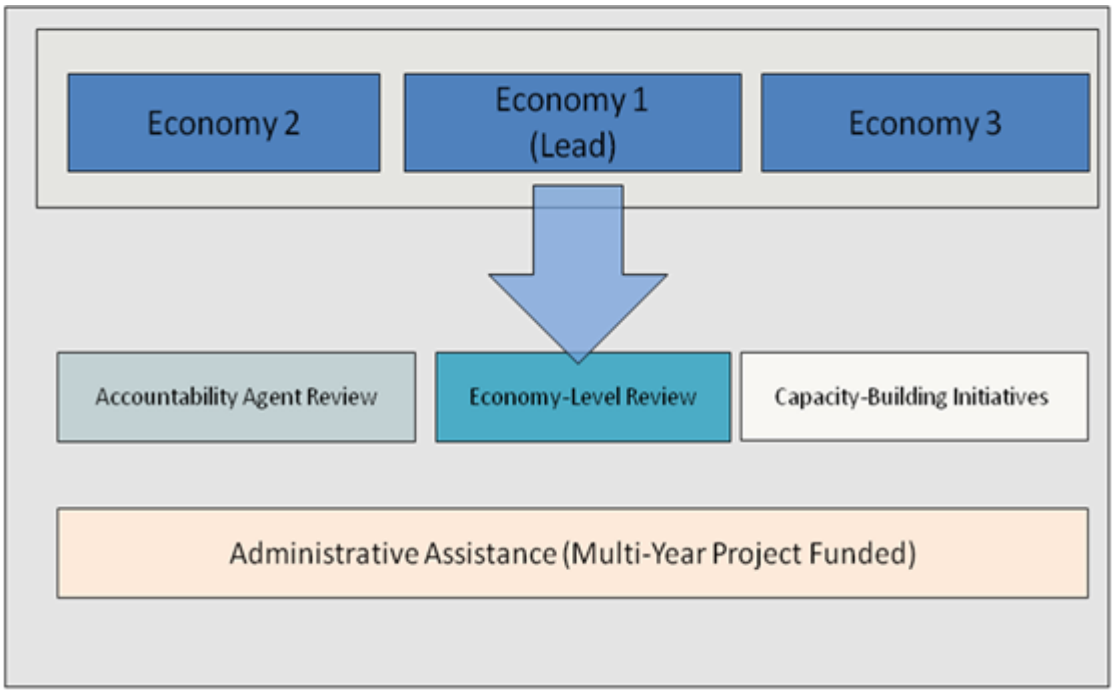
How Are CBPRs Certified?

In order to receive APEC certification, every applicant's self-assessment must be verified by a third party, also known as an Accountability Agent. Participating Accountability Agents will make use of a baseline guidance document to assess the answers provided by the applicant. Upon successful review, an applicant's privacy policy is deemed compliant with the Cross Border Privacy Rules System.

How Are CBPRs Enforced?

In order to participate in this system, an APEC member economy must participate in the Cross Border Privacy Enforcement Arrangement. It must be supported by a letter of confirmation from the economy's ECSG delegation, which identifies the relevant privacy enforcement authority: any public body responsible for enforcing privacy law and the applicable privacy law - laws that have the effect of protecting personal information consistent with the APEC Privacy Framework. In addition, the economy must demonstrate its enforcement ability to the CBPR Joint Oversight Panel.

本報告之智慧財產權歸屬於法務部



Source: Author Joshua Harris

圖 33：Structure of the CBPR Joint Oversight Panel

International Implementation of the Framework: 2005-2012

In 2005, APEC member economies formed a Cross Border Privacy Rules Study Group to study this approach. The Data Privacy Pathfinder is introduced in 2007. A work plan detailing nine voluntary projects necessary to implement the Pathfinder is introduced and endorsed in 2008 and one year later, in 2009, a CBPR Test Pilot is conducted across four economies. In 2010, six of the nine projects are completed and endorsed. All the projects are completed in 2011. The Cross Border Privacy Rules System is expected to go live and projected in 2012.

本報告之智慧財產權歸屬於法務部

Personal Information Protection Legislative Development in Japan

2 November 2011

Presenter: Takayuki KATO
Associate Professor of Law
Asia University, Japan

Development of the Acts in Japan

The Act on Protection of Personal Information Retained by Administrative Organs was enacted back in 1988. By 2005, the related acts were fully enforced, including:

1. The Act on the Protection of Personal Information, etc.;
2. Cabinet Order for the Enforcement of the Act on the Protection of Personal Information; and
3. Basic Policy for the Act on the Protection of Personal Information.

All of the relevant regulations are enacted and enforced to meet the OECD 8 principles:

1. Collection Limitation Principle
   There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle
   Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle
   The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle
   Personal data should not be disclosed, made available or otherwise used for

本報告之智慧財產權歸屬於法務部

purposes other than those specified in accordance with the Purpose Specification Principle except with the consent of the data subject or by the authority of law.

5. Security Safeguards Principle
   Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness Principle
   There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle
   An individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; to be given reasons if a request made is denied, and to be able to challenge such denial; and to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle
   A data controller should be accountable for complying with measures which give effect to the principles stated above.

本報告之智慧財產權歸屬於法務部

表 38：Scope of the Acts

Basic Policy	The Act on the Protection of Personal Information	any entity
Details	The Act on the Protection of Personal Information	civil sector
Details	The Act on the Protection of Personal Information Retained by Administrative Organs	national public sector (the government)
Details	The Act on the Protection of Personal Information Retained by Incorporated Administrative Agencies, etc.	incorporated administrative agencies
Details	Municipal Ordinance	local government
More Details	Guidelines Established by Each Competent Ministry	civil sector

Source: Author Takayuki KATO

Characteristics

Although the basic policy for the protection of personal data has not changed much, because of technology advancements, public attitude toward the protection of personal data is changing constantly. The amendment of the Act on the Protection of Personal Information is unnecessary; however, the government needs to set more detailed rules. As of March 2003, 40 Guidelines have been issued. The role of "guidelines" made by Ministries is important and practically they are working well. But theoretically they are not law.

本報告之智慧財產權歸屬於法務部

表 39：Competent Ministry

The Act on the Protection of Personal Information	Consumer Affairs Agency
The Act on the Protection of Personal Information Retained by Administrative Organs	Ministry of General Affairs
The Act on the Protection of Personal Information Retained by Incorporated Administrative Agencies, etc.	Ministry of General Affairs
Municipal Ordinance	Municipalities
Guidelines Established by Each Competent Ministry	each Ministry

Source: Author Takayuki KATO

Role of Each Ministry and Current Institutional Problem

Consumer Affairs Agency used to play a big and important role in the past for the enactment of the Law, but now it mainly plays coordination and research role. Consumer Affairs Agency still participates in international conferences; however, it has no superseding power to other ministries.

Ministry of General Affairs also plays an important role for the protection of personal data retained by the state.

Each ministry issues its guidelines and modifies them constantly. However, each ministry focuses only on its own interests instead of the overall interests.

Solution to the Institutional Problem

Is adopting a Commissioner system, or creating a sole independent or third party organization a solution?

The Consumer Affairs Agency of Japan has done the relevant research and has made a plan to form the commission system. The expected roles and systems of Commissioners focus on the criteria and idea of independency (like in the U.S., U.K., Germany, France, Sweden and Ireland).

Maybe a Try?

National Numbering System (Mutual Number System) will be adopted soon. At the same tim**e**, a Third Independent Body to observe privacy issues incurred by this system will also be established.

Current Administrative Problems

本報告之智慧財產權歸屬於法務部

The effectiveness of enforcement is one of the current problems that Japan faces in personal information protection. There is no punishment case so far. But many leakage cases (over 400 cases every year) still exist.

In the situation of passing personal data to a third party, the question raised is whether consent is always needed. Difficulty in balancing between police power and the protection of personal data.

Waseda University Case

Waseda University, one of the major universities, planned to hold a discussion meeting with the President of China. The Police asked the University to pass the list of the attendance which includes the names and their addresses. Although the University had plenty of time to ask the attendance for the consent, the University passed the personal information to the Police without their consent. Three students disturbed the meeting and were arrested by the police. They sued the University for this mistreatment of their personal data.

The issues involved in the Waseda case include:

1. Is attendance to a University event a personal or social act?
2. Who judge the necessity and the significance of the security? Always entities handling personal information? One of the provisions says that entities handing personal information MAY pass the information without consent if cases in which it is necessary for cooperating with a state organ.
3. If they misjudge it, they have to reimburse the whole attendance for the damages? 3 students filed suit, but the attendance was about 1400. The other 3 students filed suit in the same case and were admitted about 100 dollars each.

In 2003, the Supreme Court ruled 3-2 in this case. The majority opinion indicated that the University should have obtained the consent but it did not even try to do so. Omitting the necessary process for the consent is illegal. Because the University failed to obtain the required consent, it should pay about 50 dollars to each attendance.

The dissent argued that, in this case, passing the information is highly required for the security reasons. Although omitting the consent is a problem, it is hard to say the act of the University is illegal.

三、意見調查統計

（一）100 年 11 月 2 日 回收有效問卷數 53 份，參加總人數 338 人

表 40：100 年 11 月 2 日 意見調查表統計

整體看法	議題符合性	書面資料合適性	時數分配之適當性	環境之配合度
分數	4.4	4.2	4.3	4.4
總分(平均)	4.3			

講師表現的看法	Joshua Harris	Rachael Spalding	加藤隆之	Joshua Harris(APEC)

本報告之智慧財產權歸屬於法務部

議題之專業知識	4.4	4.5	4.4	4.6
講授態度及敬業精神	4.4	4.5	4.4	4.6
講解方式及表達能力	4.3	4.5	4.1	4.5
講師之整體表現	4.3	4.5	4.2	4.6
總　分(平均)	4.4	4.5	4.3	4.5

其他行政服務的看法	活動事前之各項服務	活動現場之各項服務
分數	4.5	4.4
總分(平均)	4.4	

訊息管道	科技法律研究所電子報	科技法律透析期刊廣告	來自網站訊息或電子報	活動宣傳海報或 DM	其他管道
總計（份）	17	0	7	5	23

資料來源：由資策會科法所製作

（二）100 年 11 月 3 日 回收有效問卷數 58 份，參加總人數 190 人

表 41：100 年 11 月 3 日 意見調查表統計

整體看法	議題符合性	書面資料合適性	時數分配之適當性	環境之配合度
分數	4.4	4.4	4.4	4.5
總分(平均)	4.4			

講師表現的看法	邱映曦	關本貢
議題之專業知識	4.5	4.5
講授態度及敬業精神	4.6	4.5
講解方式及表達能力	4.5	4.4
講師之整體表現	4.5	4.5
總　分(平均)	4.5	4.5

其他行政服務的看法	活動事前之各項服務	活動現場之各項服務
分數	4.6	4.5
總分(平均)	4.5	

訊息管道	科技法律研究所電子報	科技法律透析期刊廣告	來自網站訊息或電子報	活動宣傳海報或 DM	其他管道
總計（份）	20	1	10	9	24

資料來源：由資策會科法所製作

本報告之智慧財產權歸屬於法務部

（三）意見及回覆

1.意見：因沒有上網留意議程，前一天接到電話才知道改時間，且沒有收到報名成功 Email 通知；建議可以參考中華經濟研究院的報名系統及通知方式。

答覆：將轉知 MIS 此訊息，以利納入架設新版報名系統之考量。

2.意見：應全面提供優惠停車位。問題三：應全面提供優惠停車位。

答覆：受限於經費，無法全面提供優惠停車券，於活動報名網頁　注意事項已進行說明。

3.意見：建議增加歐盟國家的制度分享課程及邀請中國學者來台。

答覆：納入未來舉辦個資法國際研討會邀請外賓之考量。

4.意見：日語翻譯人員專業能力不足，漏翻譯一大段；同步翻譯機器在研討會過程中有發生斷訊的情形。

答覆：將轉知本次合作廠商-統一翻譯社，若未來有日文即時口譯合作，將嚴格要求翻譯人員專業程度；設備若有故障，當日現場均有備品可以更換。

四、效益分析

個資法修正通過後，對公務機關推動業務及民間企業之營運都帶來相當衝擊，有關個資隱私的跨境保護也成為各國政府持續推動個資與隱私保護下一個重大議題。APEC 透過資訊隱私開路者合作計畫（APEC Data Privacy Pathfinder Projects）的跨境隱私規則（Cross- Border Privacy Rules，以下簡稱 CBPRs），提供企業經營者得以建立其內部之跨境資料傳輸規則，並且透過認證機制 （Accountability Agents），使企業得以提供消費者可信之標章。認證機構審核企業符合 CBPRs 之最低要求後，即認為該企業符合跨國傳輸個人資料之要求。一旦企業內部所制定之跨境傳輸規則被認證後，將會約束企業本身。同時，該會員經濟體國內之管理者，例如隱私主管機關，也將要求企業執行該項隱私政策。而加入 CBPRs 系統之會員經濟體，必須參加共同監督小組（the Joint Oversight Panel）之選任過程。

本報告之智慧財產權歸屬於法務部

由於我國為 APEC 之會員國，並且積極參與跨境隱私規則（Cross- Border Privacy Rules，以下簡稱 CBPRs）之制度之實驗計畫，透過國際研討會與專家學者經驗之交流與分享，更進一部了解各國在 APEC 現行跨境隱私規則的框架下，對於跨境隱私與個人資料的保護與管理，與執行經驗的分享與實作，提供我國積極參與 CBPRs 計畫參考。

同時，在與會專家的積極討論下，相關之建議將成為我國對於個人資料保護與跨境傳輸之參考。未來各目的事業主管機關，也應思考如何在 APEC 跨境隱私規則的架構下，訂定相關參考規範，以與國際個人資料保護發展之脈動接軌，建立我國於國際間之個人資料保護聲譽，增加我國於國際活動之能見度。

五、結語

由於全球化的影響與資通訊科技之發達，使資訊儲存媒介益發多元，個人資料與資訊也隨著網際網路而流通快速，相對的個人資料與資訊的蒐集、儲存，與利用也日益複雜。受 OECD、APEC 等國際組織，以其個資保護與管理發達的國家，各國也陸續推陳強化個資隱私保護的規範與機制，本次國際研討會的舉辦提供我國與外國專家學者，針對個人資料與隱私的保護與管理進行交流與分享，了解個資保護與管理發達的國家對於個資保護與管理的實作經驗，以及如何透國國際合作，管理與保護無所不在的個人資料。

六、簽到表

（因簽到表內含有參與人員之個人資料，故在此予以移除，詳細簽到資料已附於呈繳法務部之「資料隱私及資訊透明國際研討會－研討會成果報告」）。

本報告之智慧財產權歸屬於法務部

七、活動照片

資料來源：由資策會科法所自行拍攝

圖 34：外賓及長官合照

資料來源：由資策會科法所自行拍攝

圖 35：法務部　曾勇夫　部長

本報告之智慧財產權歸屬於法務部

資料來源：由資策會科法所自行拍攝

圖 36：行政院科技顧問組　陳炳煇　執行秘書

資料來源：由資策會科法所自行拍攝

圖 37：資訊工業策進會　李世光　執行長

本報告之智慧財產權歸屬於法務部

資料來源：由資策會科法所自行拍攝

圖 38：經濟部商業司　李錏　副司長

資料來源：由資策會科法所自行拍攝

圖 39：法務部法律事務司　鍾瑞蘭　副司長

本報告之智慧財產權歸屬於法務部

資料來源：由資策會科法所自行拍攝

圖 40：美國商務部科技與電子商務司副司長暨 APEC 資料隱私次級工作小組副主席　Mr. Joshua Harris

資料來源：由資策會科法所自行拍攝

圖 41：澳洲資訊委員會政策部政策助理委員 Ms. Rachael Spalding

本報告之智慧財產權歸屬於法務部

資料來源：由資策會科法所自行拍攝

圖 42：日本亞細亞大學法學院　加藤隆之　副教授

資料來源：由資策會科法所自行拍攝

圖 43：資訊工業策進會科技法律研究所　邱映曦　主任

本報告之智慧財產權歸屬於法務部

資料來源：由資策會科法所自行拍攝

圖 44：JIPDEC 隱私標章推動中心　関本貢　副中心長

資料來源：由資策會科法所自行拍攝

圖 45：綜合座談

本報告之智慧財產權歸屬於法務部

資料來源：由資策會科法所自行拍攝

圖 46：資訊工業策進會科技法律研究所　戴豪君　所長

資料來源：由資策會科法所自行拍攝

圖 47：參與人數踴躍

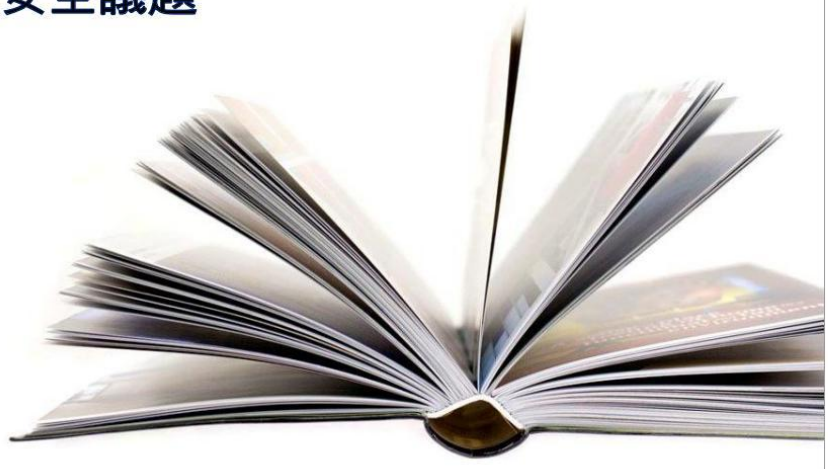
本報告之智慧財產權歸屬於法務部

柒、公務機關個人資料保護專責人員培訓教育訓練

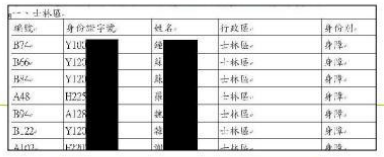
一、初階公務機關個資保護專責人員培訓教材

本報告之智慧財產權歸屬於法務部

個人資料安全議題



個人資料安全議題 (1/10)



■水利署外洩個資 跨機關資料調閱問題大

個資事件類型	個資安全措施	資料來源	資安人 2011/01/19

日前民眾向立委及市議員爆料指出，經濟部水利署網站傳出將民眾個人資料外洩事件。任何人只要下載「台北市99年度水災保全計畫」，就可看到台北市士林、北投文山區部份易發生水災地區的住戶個人資料，包括姓名、地址、出生年月日、身分證字號、聯絡電話等個資，約400多筆。

對應個人資料保護法…

■第18條-
■公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

■第27條第2項-
■中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

事件學習

■資料調閱應明定資料蒐集目的及保管權責，取得資料後亦需善盡保管責任。
■個人資料管理者應妥善保護個人資料之安全，並定期檢視和重新評估該些保護措施。

4

本報告之智慧財產權歸屬於法務部

個人資料安全議題 (2/10)

■國科會、內政部 政府單位個資外洩頻傳

個資事件類型	個資安全措施	資料來源	資安人 2009/06/29

根據網友提供消息，內政部某單位將含有20多筆民眾身分證字號、地址等個資的Excel檔放在網路上供存取，經本刊通報後，該單位資訊管理室人員表示，當初是使用微軟Index server做檢索，卻沒做好資料夾設定，將該檔案放在網路目錄下瀏覽，以為僅供內部網路存取，沒想到卻被Google扒走。此類錯誤許多單位都曾犯過，但值得警惕的是，該單位於去年底清查時以為移除該檔案就沒事，尚未通報Google移除頁庫存檔內容，因此被網友發現。

對應個人資料保護法…

■第18條-
■公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

■第28條第1項-
■公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。

事件學習

■個人資料管理者應妥善保管個資，並設定個資存取的權限控管等保護機制，以確保個人資料的安全，並定期檢視和重新評估該些保護措施與紀錄。

5

個人資料安全議題 (3/10)

■國中基測的委外單位涉販賣基測個資

個資事件類型	個資委外事件	資料來源	聯合新聞網

台灣某補習班業者涉嫌販售國中基測個資，經民眾檢舉並由地檢署偵查後，將該公司的負責人以涉嫌違反背信及電腦處理個人資料保護法起訴。該公司是負責辦理 97 年國中基測的委外單位負責受理考生報名，並建立考生基本資料電子檔，以利後續相關基測報名的相關事務。該業者的負責人二度指示職員竊取學生個資並依據縣市區域燒錄至光碟，交予國內各地補習班或私立高中，獲取不法利益 480 萬元，對此地檢署對該公司負責人求刑 10 年。

對應個人資料保護法…

■第4條-
■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，於本法適用範圍內，視同委託機關。

■第18條-
■公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

事件學習

■針對涉及個資的委外作業，應重新審閱委外合約，對委外廠商的資訊安全管理應有相當的要求與管控，並應在契約條款轉嫁風險。

6

本報告之智慧財產權歸屬於法務部

個人資料安全議題 (4/10)

■洩個資! 少校、警員、監理都有份

個資事件類型	個資安全措施	資料來源	聯合報 2011/02/15

數家徵信業者透過管道向軍警等人員購買他人通聯、戶籍、前科等資料一千多筆，檢警等單位昨天查獲掛鉤的四名警員、一名少校、一名監理人員及三名「白手套」正擴大偵辦。 檢警指出，徵信業者對個資的需求殷切，不惜以高價誘使公務員鋌而走險。雙向通聯紀錄，八年前一筆的行情約二千五百元，近來漲到二萬五千元到四萬元，贓款透過白手套進入公務人員口袋。 檢警估計，兩年來，至少有三家徵信業者透過管道非法取得逾千筆個資。

對應個人資料保護法...

■第42條-
■意圖為自己或第三人不法之利益或損害他人之利益，...足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。

■第44條-
■公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。

事件學習

■個人資料管理者應妥善保管個資，並設定個資存取的權限控管等保護機制，以確保個人資料的安全，並定期檢視和重新評估該些保護措施與紀錄。

7

個人資料安全議題 (5/10)

■千筆中X局客戶個資丟馬路

個資事件類型	個資安全措施	資料來源	蘋果日報2010/06/20

銀行竟將民眾重要個資丟棄在路邊，真是太離譜！北縣八里鄉西濱快速道路一處路段，前天被人發現上千張前中X局開戶申請的文件散落一地，部分還掉落下方涵洞，單據上除了姓名、電話，還有身分證號及銀行帳戶等重要個資。

對應個人資料保護法...

■第27條第1項-非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
■第27條第2項-中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。
■第27條第3項-前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之

事件學習

■個人資料管理者應妥善保護個人資料之安全，並定期檢視和重新評估該些保護措施。

8

本報告之智慧財產權歸屬於法務部

個人資料安全議題 (6/10)

■韓國農協銀行遭入侵 委外廠商員工筆電惹的禍

個資事件類型	個資安全措施	資料來源	資安人 2011/05/16

上個月的攻擊讓韓國農業協同銀行的服務停擺數天之久，約3千萬用戶受到影響，同時有部分信用卡客戶資料遭到刪除。根據韓國媒體報導，檢方追蹤後發現此次發動攻擊....但值得注意的是，追蹤後發現農協被發動攻擊的根源來自委外廠商IBM某位員工所使用的筆記型電腦。....該台筆電在這7個月以來，管理者密碼都沒有變更，也有明顯管理上的疏失。

對應個人資料保護法...

- ■第27條第1項-非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- ■第27條第2項-中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。
- ■第27條第3項-前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之

事件學習

■個人資料管理者應妥善保護個人資料之安全，並定期檢視和重新評估該些保護措施。

9

個人資料安全議題 (7/10)

■民眾至萬芳醫院 志工給的便條紙背後竟藏他人就醫資訊

個資事件類型	個資安全措施	資料來源	中時電子報 2011/08/04

台北市立萬芳醫院，爆發有民眾就醫時，到服務台詢問就醫資訊，結果當時志工提供的便條紙，居然發現是另外一名病患的就醫資料，包括姓名、年齡、體重、還有就醫科別，全部被看光光。...院方也進一步調查，發現是門診醫師，將病患的病歷列印出來發現有錯誤，應該會放到銷毀處，卻誤回收成便條紙再利用。

對應個人資料保護法...

- ■第27條第1項-非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- ■第27條第2項-中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。
- ■第27條第3項-前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之

事件學習

■個人資料管理者應妥善保護個人資料之安全，並定期檢視和重新評估該些保護措施。

10

本報告之智慧財產權歸屬於法務部

個人資料安全議題 (8/10)

■史上最大個資外洩案, SONY真的該Sorry

個資事件類型	個資安全措施	資料來源	聯合新聞網2011/06/03

SONY的遊戲主機PS3網路平台PSN，在四月十九日遭到駭客入侵，高達六十個國家七千七百萬用戶個資外洩。可能外洩的個資包括姓名、住址、電話號碼、電郵信箱信用卡資料、性別及生日等。SONY不但沒有在第一時間告知PSN用戶還試圖掩飾，第一份通告於被駭十天後才寄出。駭客攻擊中受害的SONY網路用戶已超過一億人。

對應個人資料保護法…

■第28條第4項-對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。
■第29條-非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。
■第12條-公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或 其他侵害者，應查明後以適當方式通知當事人。

事件學習

■個人資料管理者應妥善保護個人資料之安全，並在個資外洩事件發生後查明真相並據實告知當事人。

11

個人資料安全議題 (9/10)

■燦坤電腦遭駭客入侵　上百會員險被詐騙

個資事件類型	個資安全措施	資料來源	東森新聞 2010/6/27

最近有不少到燦坤3C門市購物的消費者抱怨接到了詐騙電話，燦坤也發現確實是電腦資料庫被駭客入侵、盜竊會員資料。接到詐騙電話的會員至少上百人，燦坤發言人羅瑞誠表示已報警處理，同時發了60萬通電話簡訊提醒會員。
據警方統計，從4月份到現在，至少有上百位燦坤的會員接到類似電話，消費者也質疑賣場電腦控管有疏失。燦坤發言人羅瑞誠承認，經查後發現確實是被駭客入侵，他們也立即「將防火牆更加強，並向刑事局報案，傳了將近60萬通防詐騙電話(簡訊)提醒消費者千萬不要受騙上當。」羅瑞誠強調，目前已在網站首頁發表緊急通知，用醒目的紅色字眼，請會員留意詐騙電話。消基會則表示，燦坤必須舉證當時有為電腦資料庫設立完整防火牆，否則被騙的消費者有權向燦坤求償。

對應個人資料保護法…

■第28條第4項-對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。
■第29條-非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。

事件學習

■組織宜加強網路存取之控管，隨時監控網路之異常流量，並留存所有防護機制之稽核證據(Log)，以作為證明組織盡良善管理責任之證據。

12

本報告之智慧財產權歸屬於法務部

個人資料安全議題 (10/10)

■457筆人事行政主管個資 網路曝光

個資事件類型	個資安全措施	資料來源	公視新聞 2010/10/10

行政院人事行政局地方行政研習中心的網站突然出現大量身分證字號。有公務員反映被「外洩」的公務員身分證字號十八萬筆，擔心個資外流、遭人濫用。
人事局表示該資料為6年前某專案所開放的資料，但結束後人員未刪除資料，導致Google連結主機輕易找到資料，目前已刪除相關紀錄。

對應個人資料保護法…

■第28條第1項-公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。

■第28條第4項-對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。

事件學習

■組織宜針對網路上存在之組織內部個人資料進行清查，如發現遺留於網路上之內部資料，應立即進行清除，並應建立組織內部個人資料之存取控制機制，妥善保護個資。

13

個人資料保護法簡介

本報告之智慧財產權歸屬於法務部

新版《個人資料保護法》的修法緣由及進程

為什麼要修法？ 1. 起訴成功率低 2. 出事單位不在列管範圍 3. APEC 人權要求銜接 4. 扼止詐騙

修法進度？

- 1995：08/11 公布電腦處理個人資料保護法
- 2010：04/20 新版個人資料保護法二讀通過
  - 04/27 新版個人資料保護法三讀通過
  - 05/26 總統公布新版個人資料保護法

還有多少時間準備？

個資法施行細則研修七大方向 (1/3)

七大方向	內容說明
訂資料保護基本方針	■先由法務部擬定基本方針。 ■再由各目的事業主管機關以法務部發布的基本方針為基礎，依據不同產業的資料特性，來訂定監管產業的個人資料保護標準指針（Guidelines）。 ■產業再依照各目的事業主管機關所發布的標準指針，來研訂企業內個人資料保護政策及應該遵守的相關法令要求。
不確定法律概念的具體化	■不確定法律概念的具體化有2個作法，包括定義性的規定與建立次標準。 ◆ 定義性的規定 ➢ 概念明確化 • 如什麼樣的個人資料才可資識別、刪除和銷燬如何界定，聯絡方式如電子郵件有哪些行為是否可資識別等 ➢ 範圍界定 • 例如特種資料適用範圍，什麼是病歷，什麼是醫療性資料，哪些特種資料有哪些例外情形可蒐集 ➢ 程序性定義 • 例如書面同意、國際傳輸、行政檢查或團體訴訟等 ◆ 建立次標準 ➢ 例如公共利益，這會因為個案而有不同的內涵呈現，判斷標準也不同，回歸司法審查的個案判斷，因此只能提出標準性的建議。

本報告之智慧財產權歸屬於法務部

個資法施行細則研修七大方向 (2/3)

七大方向	內容說明
釐清責任歸屬	■包括委託關係、民事責任、刑事責任，行政責任的認定，如何區分委託者與受託者的權利義務關係，企業或機關如何與內部員工、公務員區分彼此的責任義務，都將在細則中規定。 ■企業必須建立個人資料保護的標準、個資保管流程、資訊安全管理的流程，透過這些流程來認定哪些是屬於員工個人行為，而哪些部分才是企業應負的責任。這可用來認定真正外洩行為人的責任，區分民事、刑事與行政責任的切割。
個人資料保護團體的認定	■未來每個企業和公家機關都將面臨大量的個人資料的查詢請求，或是查詢個資在企業或機關內部是否有達到適當保管和適當安全維護，這些查詢需要法令諮詢，例如企業如何龐大群眾的法令諮詢、訴訟、損害賠償如何執行等。 ■法務部將在施行細則中訂定個人資料保護團體的許可認定方式，由各目的事業主管機關提供這類許可，讓第三人保護團體提供訴訟服務或提供其他業務諮詢。
確定執行個資保護事項的協調聯繫機制	■確定執行個資保護事項的協調聯繫機制是為了解決公務機關執行個資法時，若發生了重大爭議時的協調聯繫機制。 ■其可作為公務機關間彼此溝通業務的管道、民間企業與公務機關的協調溝通機制，以及國際傳輸的協調溝通機制。

17

個資法施行細則研修七大方向 (3/3)

七大方向	內容說明
明定目的事業主管機關的認定程序	■因為主管機關要負責行政檢查、裁處罰鍰等，故必須確定產業的主管機關。 ■施行細則中將建立一套認定程序來決定誰是主要的目的事業主管機關，這正是協調聯繫機制中的一環，若無法決定，再由行政院協調指派。
公開和報告的義務	■在細則中將明定各機關公開資訊的期限，至少在新法施行前，希望每個機關都清查所擁有的個人資料檔案，並對外公開法定項目的資訊。 ■將來還會有報告的義務，法務部會視預算，發行年刊或年鑑，來記錄每一個公務機關或非公務機關的個人資料保護執行成效，並進行執行成效的統計分析，希望透過這些公開和報告的義務，讓大家更重視個資保護，減少後續賠償問題。 ■施行細則還會訂定一些共同辦理事項與配套措施，包括修正特定目的的範圍，採取分類編號的方式，建立共通性的總類特定目的，以及依業務別區分的個別性特定目的，做為主管機關監督管理的工具，未來行政檢用來判斷企業是否合法蒐集、使用和處理個資，就是以特定目的作為認定依據。特定目的是每一個蒐集者都需要注意的事。

18

本報告之智慧財產權歸屬於法務部

個人資料保護法的重要立法意旨

新版個人資料保護法

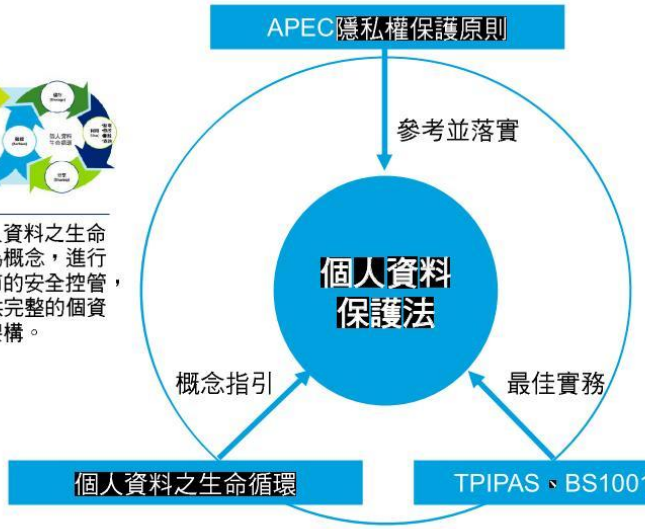
1. 擴大保護客體：	納入人工與其他類型資料 解決以往資料外洩只要不及於電腦（或自動化設備）處理，即不適用之怪現象，且納入直接與間接識別
2. 普遍適用主體：	刪除行業別之限制，我國自然人/公私機構一體適用 解決以往只有列入受管理的政府機關與8種民間產業的不合理情況
3. 增修行為規範：	限制蒐集特種資料、規範書面同意方式、增課告知義務(當事人依規定得行使之權利及外洩之告知)、放寬查詢權利、限制任意行銷，不遵守行為規範的行政裁罰
4. 強化行政監督：	中央目的事業主管機關或地方政府得行政檢查、處分或處罰
5. 節省訴訟成本：	增訂團體訴訟裁判費減免規定 為鼓勵隱私權益遭侵害之當事人透過團體訴訟進行民事或行政救濟，本法增訂團體訴訟裁判費減免之規定。
6. 調整責任內涵：	加重刑事責任及擴大適用範圍、提高民事損害賠償總額限制、提高行政罰鍰並課以負責人（代表人、管理人）監督責任 舉證責任倒置

19

我國個人資料保護法與實作概觀

- APEC隱私保護原則為亞太地區經濟體間及其貿易夥伴間對於隱私保護的遵循原則。
- 個資法修正內容內，亦已將APEC隱私保護原則的9項原則落實於條文內容之中。

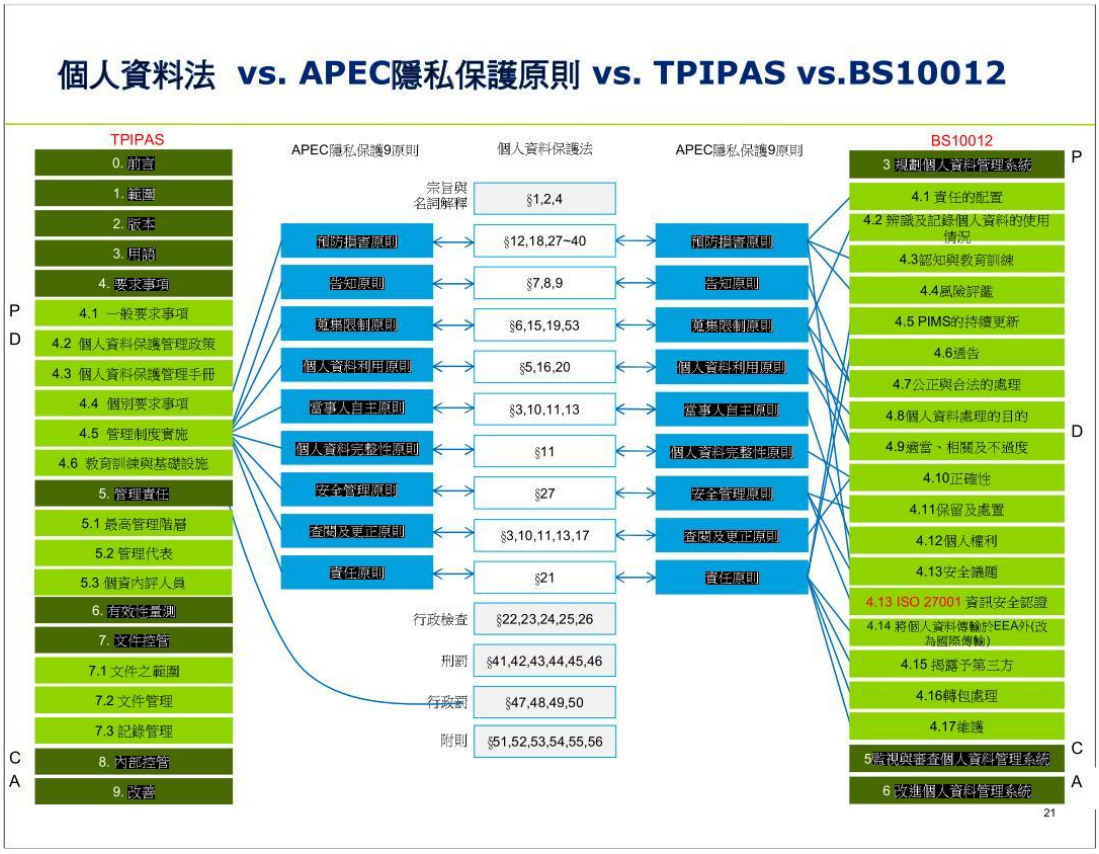
依個人資料之生命循環為概念，進行各環節的安全控管，以提供完整的個資保護架構。

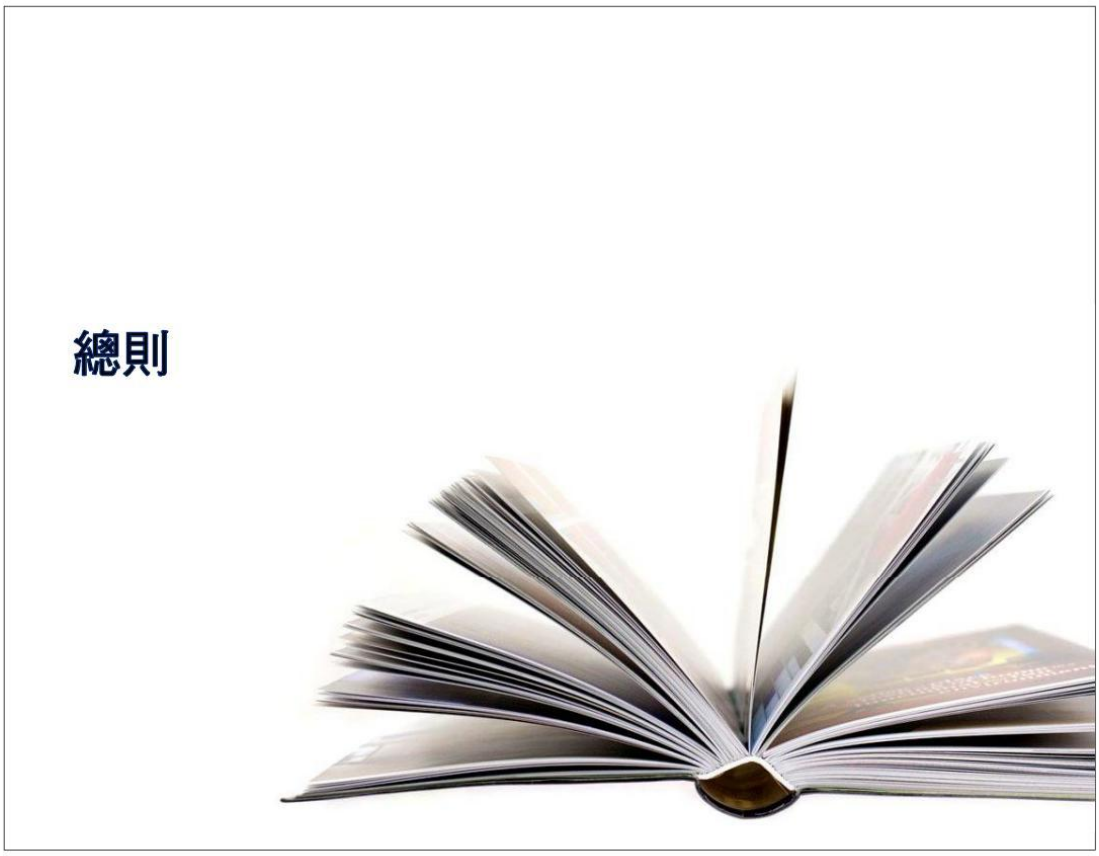


個人資料保護標準的目的在建立個人資料保護的最佳實務與協助組織符合個人資料保護法的規範。

20

本報告之智慧財產權歸屬於法務部





本報告之智慧財產權歸屬於法務部

個資之蒐集、處理或利用須有為特定目的

第5條
第53條

■ 第5條-個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

電腦處理個人資料保護法之特定目的
(法務部法85法令字第19745號令)

代號	特定目的項目
002	人事行政管理
⋮	⋮
095	其他司法行政業務
096	其他地方政府事務
097	其他合於營業登記項目或章程所定業務之需要
098	其他金融業務管理
099	其他財政收入
100	其他財政服務
101	其他諮詢與顧問服務。

■第53條-本法所定特定目的及個人資料類別，由法務部會同中央目的事業主管機關指定之。

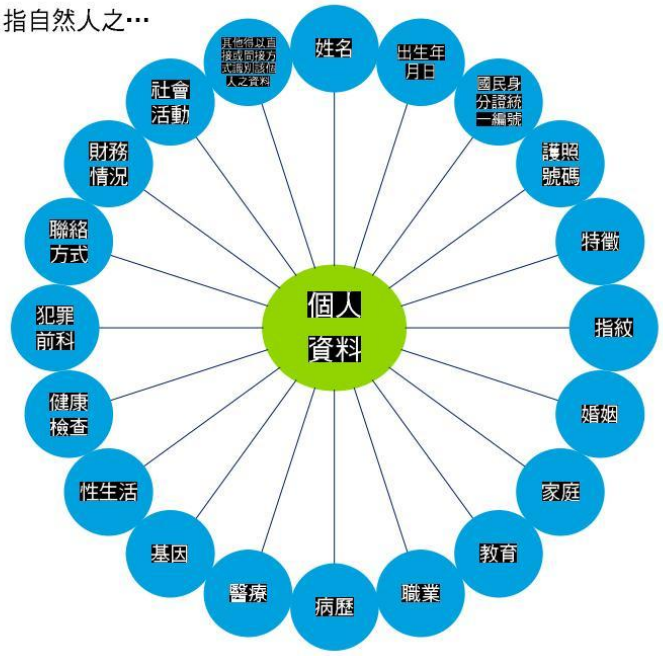
■本專案仍採用目前在電腦處理個人資料保護法中訂定的101項特定目的為參考來源。

23

個人資料之定義與活動

第2條

指自然人之…



■本專案仍採用目前在電腦處理個人資料保護法中訂定的個人資料類別為參考來源。

與個人資料相關的活動

蒐集	指以任何方式取得個人資料(包含直接或間接)
處理	指為建立或利用個人資料檔案[註]所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送
利用	指將蒐集之個人資料為處理以外之使用
國際傳輸	指將個人資料作跨國(境)之處理或利用

註：個人資料檔案指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

24

本報告之智慧財產權歸屬於法務部

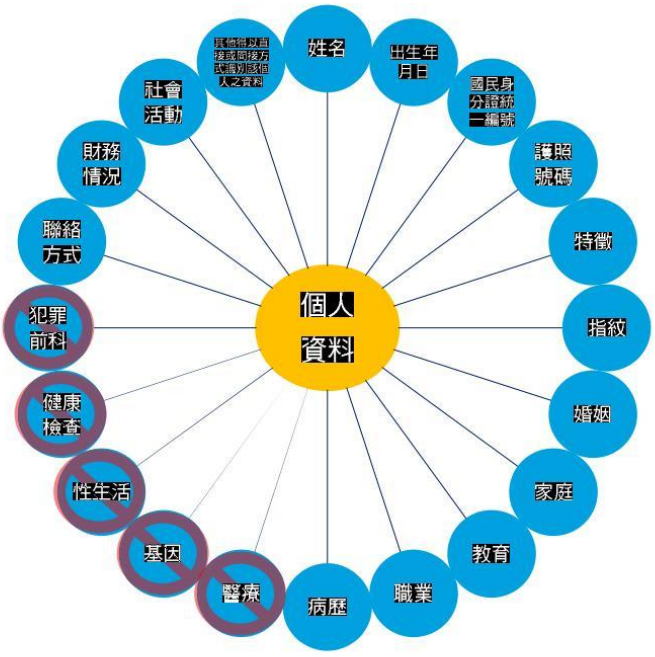
第6條

特殊個人資料之限制

■第6條-有關**醫療**、**基因**、**性生活**、**健康檢查**及**犯罪前科**之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

1. 法律明文規定。
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，且有適當安全維護措施。
3. 當事人自行公開或其他已合法公開之個人資料。
4. 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，且經一定程序所為蒐集、處理或利用之個人資料*。

*個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之。



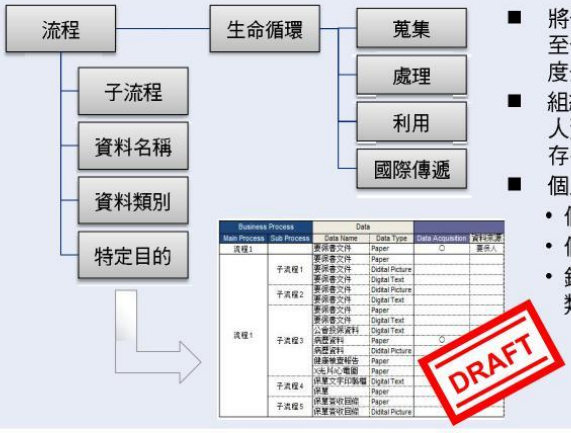
25

個人資料之定義與活動-對應措施

■ 盤點需要保護的個人資料

◆ 識別需要保護的個人資料：本專案仍採用目前在電腦處理個人資料保護法中訂定的個人資料類別為參考來源。

◆ 依個人資料的生命循環識別資料流



■ 將個人資料、與其相關的軟硬體與使用者彙整至個人資料清冊內，藉以作為後續個資管理制度分析、設計、管理之依據。

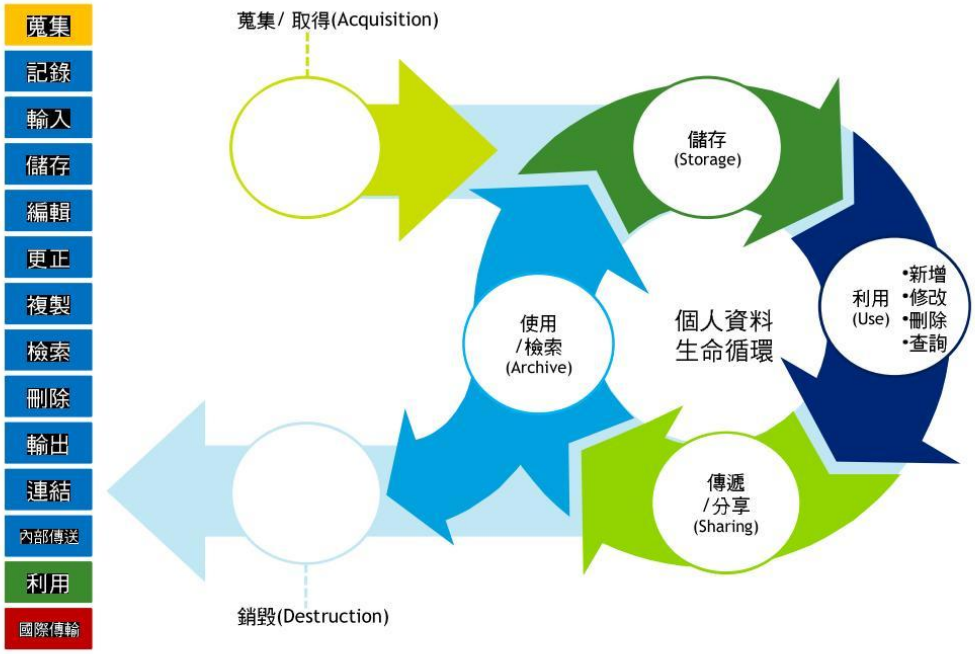
■ 組織可透過個人資料清冊達成法令規定辨識個人資料類型之要求，並確認資料後方能對資料存在的環境施予控管。

■ 個人資料清冊應記錄下列項目
- 個人資料的使用目的
- 個人資料在組織中的流向
- 鑑別與描述組織中具高處理風險之個人資料類別

26

本報告之智慧財產權歸屬於法務部

[Ref.]個人資料之生命循環



27

個人資料保護法規範主體及當事人權利

第2條 第3條 第4條

第2條

■當事人

指個人資料之本人。

(僅指生存之自然人，死亡者不算)

■公務機關

指依法行使公權力之中央或地方機關或行政法人。

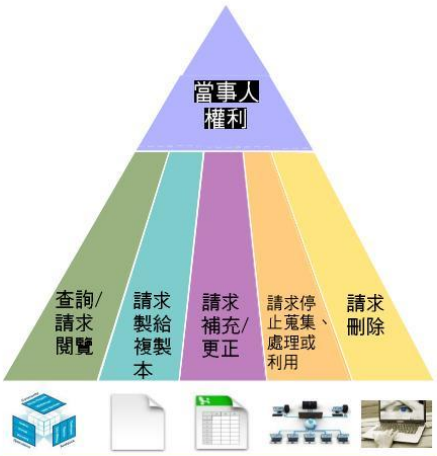
■非公務機關

指公務機關以外之自然人、法人或其他團體。

第4條

■委託機關

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，於本法適用範圍內，視同委託機關。



第3條-當事人就其個人資料依本法規定行使之權利，不得預先拋棄或以特約限制之。

28

本報告之智慧財產權歸屬於法務部

個人資料保護法規範主體及當事人權利-對應措施

- 確認所有委託機構具有同等級的個資保護措施
  - ◆盤點委託機構
  - ◆調整委託契約
  - ◆第三方稽核權利或報告
  - ◆個資保護措施檢核表

- 為了滿足當事人權利的行使，須改變現有的個人資料作業流程，包括
  - ◆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（特殊情況下機關有權拒絕使用者的刪除要求）

  以上所新增或調整之流程皆須有正式的紀錄留存，以便為日後舉證之所須。

29

個人資料蒐集之告知事項

第8條
第9條

向當事人直接蒐集者……

■第8條第1項-公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

1. 公務機關或非公務機關名稱。
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*第三條*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，不提供將對其權益之影響。

■第8條第2項-但有下列情形之一者，得免為告知：

1. 依法律規定得免告知。
2. 個人資料之蒐集係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。

(機關可以透過各種方式告知，電子郵件、簡訊、電話等方式，而且告知不需要對方回應，只要有紀錄能事後舉證，證明企業確實有告知即可。)

非由向當事人直接蒐集者……

■第9條第1項-公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及第18條第1項之1~5款所列事項。(得於首次對當事人為利用時併同為之)

■第9條第2項-有下列情形之一者，得免為前項之告知：

1.有*第8條第2項*所列各款情形之一。
2.當事人自行公開或其他已合法公開之個人資料。
3.不能向當事人或其法定代理人為告知。
4.基於**公共利益**為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。
5.大眾傳播業者基於新聞報導之**公益目的**而蒐集個人資料。

30

本報告之智慧財產權歸屬於法務部

查詢或請求閱覽個人資料或製給複製本

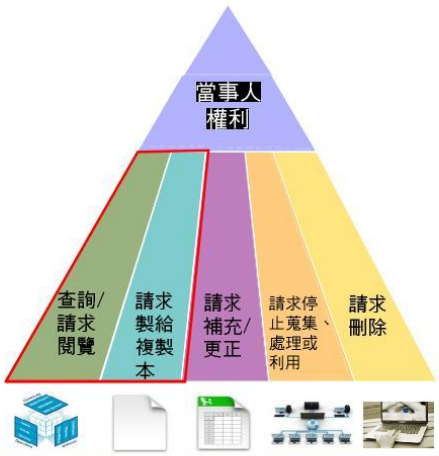
第14條 第10條 第13條

■第10條-公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：

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。

第13條-公務機關或非公務機關受理當事人依第10條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

第14條-公務機關或非公務機關得酌收必要成本費用



第3條-當事人就其個人資料依本法規定行使之權利，不得預先拋棄或以特約限制之。

31

更正或補充、停止蒐集處理或利用、刪除個人資料

第11條 第13條

■第11條第1項-公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。
(須定期檢視個人資料檔案及追蹤紀錄機制)

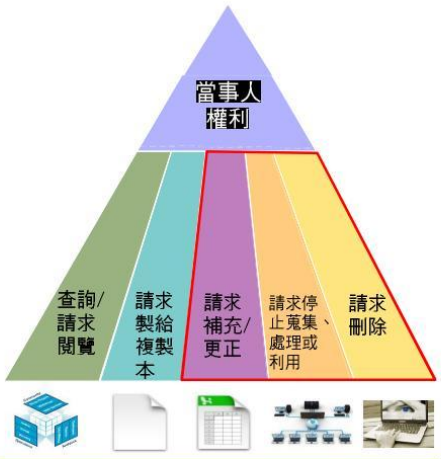
■第11條第2項-個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須並註明其爭議或經當事人書面同意者，不在此限。

■第11條第3項-個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

■第11條第4項-違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。

■第11條第5項-因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

第13條-公務機關或非公務機關受理當事人依第11條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。



第3條-當事人就其個人資料依本法規定行使之權利，不得預先拋棄或以特約限制之。

32

本報告之智慧財產權歸屬於法務部

第12條

違反本法的通知

■第12條-公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

因應措施：

1. 設計個資保護組織。
2. 設計通報機制。
3. 釐清責任權責。

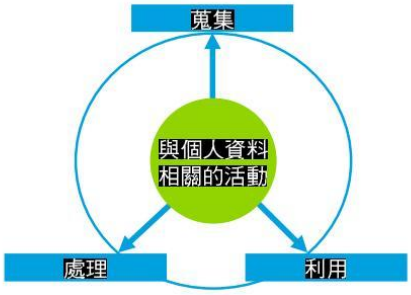
33

公務機關對個人資料之蒐集、處理及利用

本報告之智慧財產權歸屬於法務部

個人資料之蒐集、處理及利用

第7條 | 第16條
第15條 | 第18條



第18條-公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

特定目的內……

■第15條-公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

1. 執行法定職務必要範圍內。
2. 經當事人書面同意[註1]。
3. 對當事人權益無侵害。

特定目的外……

■第16條-公務機關對個人資料之利用，除第六條第一項所規定資料外，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。但有下列情形之一者，得為特定目的外之利用：

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，且資料經過處理後或依其揭露方式無從識別特定當事人。
6. 有利於當事人權益。
7. 經當事人書面同意[註2]。

註1：第7條-指當事人經蒐集者告知本法所定應告知事項後，所為允許之書面意思表示。

註2：第7條-指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之書面意思表示。

35

個人資料之蒐集、處理或利用-對應措施

■ 書面同意
◆有關書面同意之方式，依民法及電子簽章法規定為之。

■ 單獨所為之書面意思表示
◆上述書面同意內涵之明確化並須單獨為之，應避免列入定型化契約之約定條款而作概括同意。

36

本報告之智慧財產權歸屬於法務部

[Ref.]個資外洩檢舉窗口 法務部6月底對外公告

■針對個資法修正三讀後，各方熱烈討論該怎麼做?該做什麼才是對個資善盡管理防止保護之責? 法務部在後續的行動方案中，已經依據個資法第18條完成指定專人辦理個人資料安全維護事項與職責上，做出了個資管理代表之明確定位、職責的定義說明。此外，包含各機關應設置個資保護聯絡窗口，提供一個個資保護上的暢通管道以及統籌專責人員之訓練需求。

■法務部法律事務司表示，自去年就已行文各機關要求設立個資專職窗口，部分機關已確實設立並回報，將來如果民眾遇到疑似個資外洩事件，就可以向該事業目的主管機關的窗口檢舉。此外，在12月底前各機關也必須完成單位內的個人資料保護管理計畫。同時身為非公務機關之主管機關者也需制定管理要點以便於產業遵循。無店面零售業主管機關商業司，正在研擬隱私標章制度，將來取得標章的單位，若疑似個資外洩，就能提出善盡管理責任的證明。或者走法律訴訟一途。

■關於專責人員職責部分，亦提出利用PDCA之方法對個資保護管理制度之計畫、執行、檢查與行動階段做出細部工作內容，提供各界目前討論之方向以及參考依循。

資安人 http://www.informationsecurity.com.tw/article/article_detail.aspx?tv=11&aid=5744

37

第17條

提供公眾查閱

■第17條-公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同：

1. 個人資料檔案名稱。
2. 保有機關名稱及聯絡方式。
3. 個人資料檔案保有之依據及特定目的。
4. 個人資料之類別。

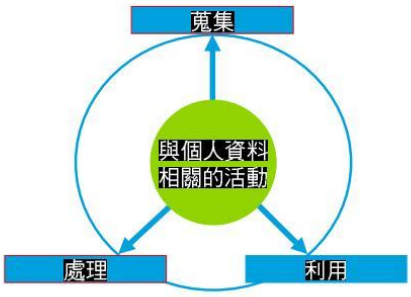
38

本報告之智慧財產權歸屬於法務部

非公務機關對個人資料之蒐集、處理及利用

個人資料之蒐集與處理

第7條
第19條



特定目的內……

■第19條第1項-非公務機關對個人資料之**蒐集或處理**，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

1. 法律明文規定。
2. 與當事人有契約或類似契約之關係。
3. 當事人自行公開或其他已合法公開之個人資料。
4. 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過處理後或依其揭露方式無從識別特定當事人。
5. 經當事人書面同意[註]。
6. 與公共利益有關。
7. 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

■第19條第2項-蒐集或處理者知悉或經當事人通知依第19條第1項第7款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

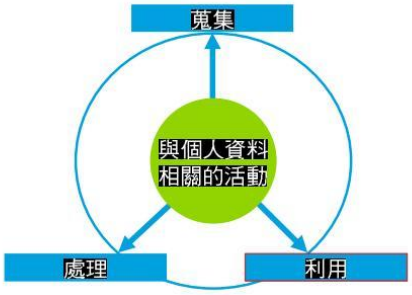
註：第7條-指當事人經蒐集者告知本法所定應告知事項後，所為允許之書面意思表示。
(書面同意：有關書面同意之方式，依民法及電子簽章法規定為之。)

40

本報告之智慧財產權歸屬於法務部

個人資料之利用

第7條
第20條



特定目的外……

■第20條第1項-非公務機關對個人資料之利用，除第六條第一項所規定資料外，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。但有下列情形之一者，得為特定目的外之利用：

1. 法律明文規定。
2. 為增進公共利益。
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，且資料經過處理後或依其揭露方式無從識別特定當事人。
6. 經當事人書面同意[註]。

■第20條第2項-非公務機關依第1項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。

■第20條第3項-非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

註：第7條-指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之書面意思表示。

（上述書面同意內涵之明確化並須單獨為之，應避免列入定型化契約之約定條款而作概括同意。）

41

個人資料之蒐集、處理或利用-對應措施

■ 契約或類似契約關係

◆ 這項要件不限形式，只要符合契約的法定規範，透過網頁同意按鈕的使用者條款也可以成立。

■ 當事人自行公開或其他已合法公開之個人資料

◆ 對於個人自行公開的個資，或是其他合法公開的個人資料，企業就可以自行運用，不需要取得書面同意，也不用與當事人建立契約關係。

◆ 若是第三方公開的個人資料，企業必須確認這些公開資料的合法性後才能利用。

■ 一般可得來源

◆ 如從網際網路蒐集來的個人資料，因為無法查證資料是否合法，個資法則將這類行為視為合法蒐集，但「機關若後來發現這些資料不合法，或者使用者要求企業禁用時，企業就必須刪除或停止使用。」

42

本報告之智慧財產權歸屬於法務部

第21條

國際傳輸個人資料

■第21條-非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：

1. 涉及國家重大利益。
2. 國際條約或協定有特別規定。
3. 接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。
4. 以迂迴方法向第三國(地區)傳輸個人資料規避本法。

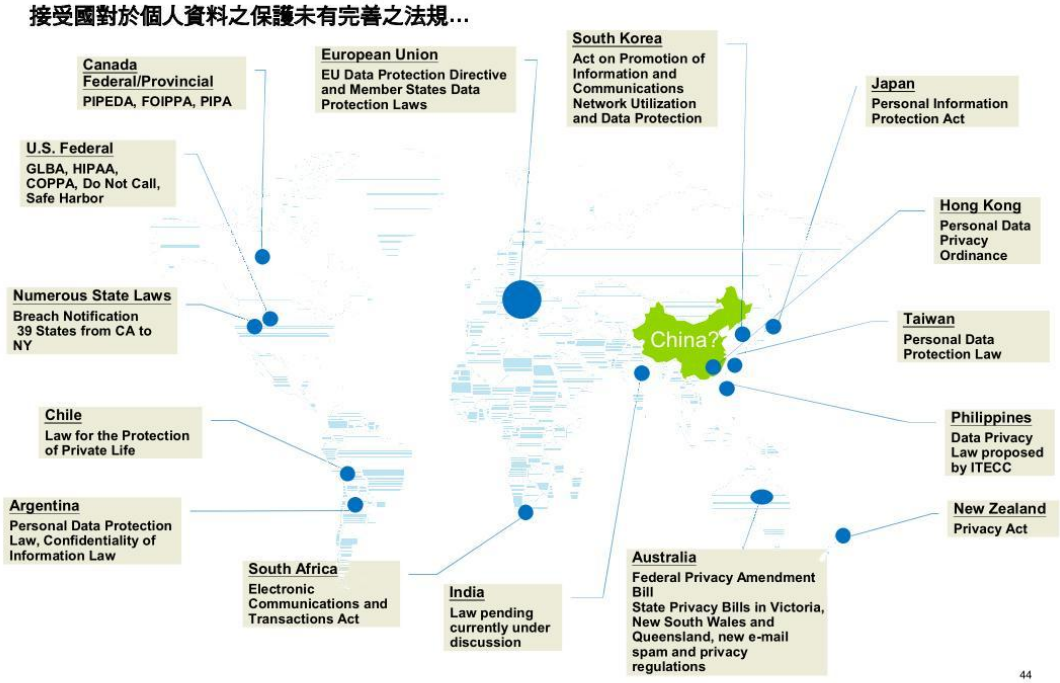
注意：

1. 應確保第三人會採取一致的措施，以維護資料隱私的安全。
2. 將個資傳輸予未訂個資保護相關法令國家時，應特別注意。
3. 外商銀行於台灣執行個資的蒐集、處理及利用亦須符合我國個資法。

43

國際傳輸個人資料

接受國對於個人資料之保護未有完善之法規…



44

本報告之智慧財產權歸屬於法務部

強化行政監督(1/2)

第22條
第26條

■第22條第1項-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。

(第26條)中央目的事業主管機關或直轄市、縣（市）政府檢查後，未發現有違反本法規定之情事者，經該非公務機關同意後，得公布檢查結果。

■第22條第3項-中央目的事業主管機關或直轄市、縣（市）政府為第一項檢查時，得率同資訊、電信或法律等專業人員共同為之。
■第22條第4項-對於第1項及第2項之進入、檢查或處分，非公務機關及其相關人員不得規避、妨礙或拒絕。
■第22條第5項-參與檢查之人員，因檢查而知悉他人資料者，負保密義務。

■第22條第2項-中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。

強化行政監督(2/2)

第23條
第24條

■第23條第1項-對於第22條第2項扣留物或複製物，應加封緘或其他標識，並為適當之處置；其不便搬運或保管者，得命人看守或交由所有人或其他適當之人保管。
■第23條第2項-扣留物或複製物已無留存之必要，或決定不予處罰或未為沒入之裁處者，應發還之。但應沒入或為調查他案應留存者，不在此限。

■第24條第1項-非公務機關、物之所有人、持有人、保管人或利害關係人對第22條及第23條之要求、強制、扣留或複製行為不服者，得向中央目的事業主管機關或直轄市、縣(市)政府聲明異議。

■第24條第2項-第24條第1項聲明異議，中央目的事業主管機關或直轄市、縣(市)政府認為有理由者，應立即停止或變更其行為；認為無理由者，得繼續執行。經該聲明異議之人請求時，應將聲明異議之理由製作紀錄交付之。

■第24條第3項-對於中央目的事業主管機關或直轄市、縣(市)政府第24條第2項決定不服者，僅得於對該案件之實體決定聲明不服時一併聲明之。但第24條第1項之人依法不得對該案件之實體決定聲明不服時，得單獨對第24條第1項之行為逕行提起行政訴訟。

本報告之智慧財產權歸屬於法務部

第25條

違規處理

■第25條第1項-非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣(市)政府除依本法規定裁處罰鍰外，並得為下列處分：

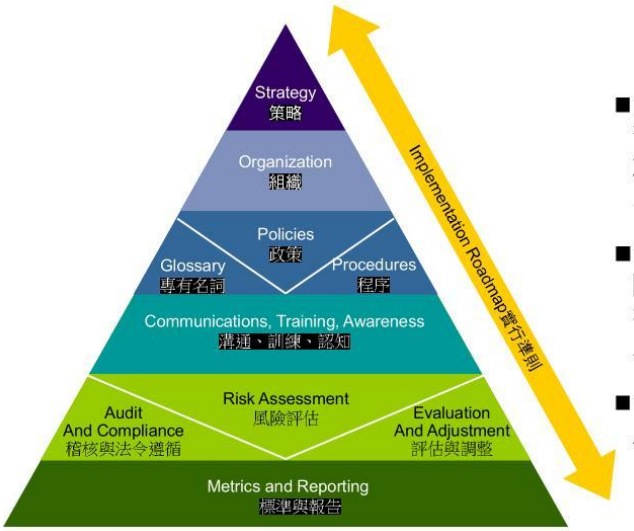
1. 禁止蒐集、處理或利用個人資料。
2. 命令刪除經處理之個人資料檔案。
3. 沒入或命銷燬違法蒐集之個人資料。
4. 公布非公務機關之違法情形，及其姓名或名稱與負責人。

■第25條第2項-中央目的事業主管機關或直轄市、縣(市)政府為前項處分時，應於防制違反本法規定情事之必要範圍內，採取對該非公務機關權益損害最少之方法為之。

47

第27條

實施個資保護安全措施



■第27條第1項-非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

■第27條第2項-中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

■第27條第3項-前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。

48

本報告之智慧財產權歸屬於法務部

損害賠償及團體訴訟

損害賠償

第28條

- 第1項-公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。(無過失損害賠償責任)
- 第2項-被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。
- 第3項-依前2項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。
- 第4項-對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。
- 第5項-同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第3項所定每人每一事件最低賠償金額新臺幣五百元之限制。
- 第6項-第2項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

50

本報告之智慧財產權歸屬於法務部

損害賠償

第29條

- 第1項-非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。(舉證責任倒置之過失責任)
- 第2項-依前項規定請求賠償者，適用第28條第1項至第6項規定。

第30條

- 損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。

第31條

- 損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，非公務機關適用民法之規定。

51

團體訴訟

第32條

- 依本章規定提起訴訟之財團法人或公益社團法人，應符合下列要件：
  1.財團法人之登記財產總額達新臺幣一千萬元或社團法人之社員人數達一百人。
  2.保護個人資料事項於其章程所定目的範圍內。
  3.許可設立三年以上。

第33條

- 第1項-依本法規定對於公務機關提起損害賠償訴訟者，專屬該機關所在地之地方法院管轄。對於非公務機關提起者，專屬其主事務所、主營業所或住所地之地方法院管轄。
- 第2項-前項非公務機關為自然人，而其在中華民國現無住所或住所不明者，以其在中華民國之居所，視為其住所；無居所或居所不明者，以其在中華民國最後之住所，視為其住所；無最後住所者，專屬中央政府所在地之地方法院管轄。
- 第3項-第1項非公務機關為自然人以外之法人或其他團體，而其在中華民國現無主事務所、主營業所或主事務所、主營業所不明者，專屬中央政府所在地之地方法院管轄。

52

本報告之智慧財產權歸屬於法務部

團體訴訟

第34條
- 第1項-對於同一原因事實造成多數當事人權利受侵害之事件，財團法人或公益社團法人經受有損害之當事人二十人以上以書面授與訴訟實施權者，得以自己之名義，提起損害賠償訴訟。當事人得於言詞辯論終結前以書面撤回訴訟實施權之授與，並通知法院。
- 第2項-前項訴訟，法院得依聲請或依職權公告曉示其他因同一原因事實受有損害之當事人，得於一定期間內向前項起訴之財團法人或公益社團法人授與訴訟實施權，由該財團法人或公益社團法人於第一審言詞辯論終結前，擴張應受判決事項之聲明。
- 第3項-其他因同一原因事實受有損害之當事人未依前項規定授與訴訟實施權者，亦得於法院公告曉示之一定期間內起訴，由法院併案審理。
- 第4項-其他因同一原因事實受有損害之當事人，亦得聲請法院為前項之公告。
- 第5項-前2項公告，應揭示於法院公告處、資訊網路及其他適當處所；法院認為必要時，並得命登載於公報或新聞紙，或用其他方法公告之，其費用由國庫墊付。
- 第6項-依第1項規定提起訴訟之財團法人或公益社團法人，其標的價額超過新臺幣六十萬元者，超過部分暫免徵裁判費。

第35條
- 第1項-當事人依第34條第1項規定撤回訴訟實施權之授與者，該部分訴訟程序當然停止，該當事人應即聲明承受訴訟，法院亦得依職權命該當事人承受訴訟。
- 第2項-財團法人或公益社團法人依前條規定起訴後，因部分當事人撤回訴訟實施權之授與，致其餘部分不足二十人者，仍得就其餘部分繼續進行訴訟。

53

團體訴訟

第36條
- 各當事人於第34條第1項及第2項之損害賠償請求權，其時效應分別計算。

第37條
- 第1項-財團法人或公益社團法人就當事人授與訴訟實施權之事件，有為一切訴訟行為之權。但當事人得限制其為捨棄、撤回或和解。
- 第2項-前項當事人中一人所為之限制，其效力不及於其他當事人。
- 第3項-第1項之限制，應於第34條第1項之文書內表明，或以書狀提出於法院。

第38條
- 第1項-當事人對於第34條訴訟之判決不服者，得於財團法人或公益社團法人上訴期間屆滿前，撤回訴訟實施權之授與，依法提起上訴。
- 第2項-財團法人或公益社團法人於收受判決書正本後，應即將其結果通知當事人，並應於七日內將是否提起上訴之意旨以書面通知當事人。

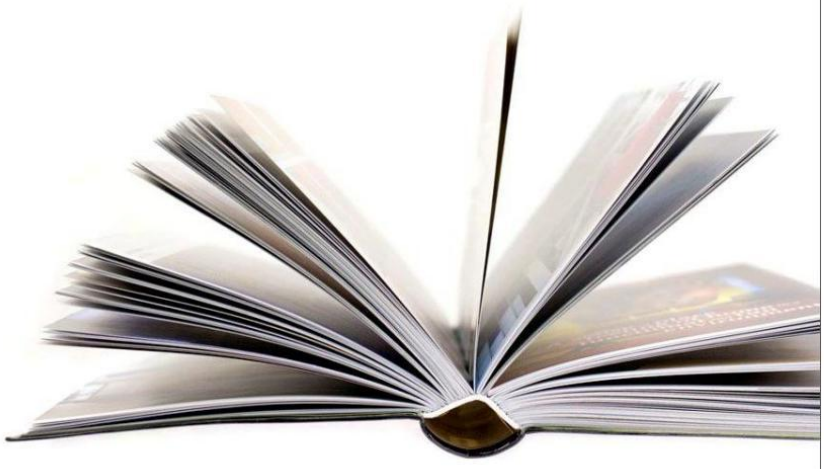
第39條
- 第1項-財團法人或公益社團法人應將第34條訴訟結果所得之賠償，扣除訴訟必要費用後，分別交付授與訴訟實施權之當事人。
- 第2項-提起第34條第1項訴訟之財團法人或公益社團法人，均不得請求報酬。

第40條
- 依本章規定提起訴訟之財團法人或公益社團法人，應委任律師代理訴訟。

54

本報告之智慧財產權歸屬於法務部

罰則



刑罰

第41條

違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分

意圖營利

(非告訴乃論)

足生損害於他人者

第1項

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

第2項

處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金

第42條

意圖為自己或第三人不法之利益或損害他人之利益

對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確

足生損害於他人者

處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰

56

本報告之智慧財產權歸屬於法務部

處罰對象及告訴乃論

- 處罰對象
  - 第43條-中華民國人民在中華民國領域外對中華民國人民犯第41及42條之罪者，亦適用之。
  - 第44條-公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。
- 告訴乃論
  - 第45條-本章之罪，須告訴乃論。但犯第41條第2項之罪者，或對公務機關犯第42條之罪者，不在此限。
- 第46條-犯本章之罪，其他法律有較重處罰規定者，從其規定。

57

行政罰

針對非公務機關…

第47條

1. 違反第6條第1項規定。
2. 違反第19條規定。
3. 違反第20條第1項規定。
4. 違反中央目的事業主管機關依第21條規定限制國際傳輸之命令或處分。

→ 中央目的事業主管機關或直轄市、縣（市）政府 → 處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正 → 屆期未改正者，按次處罰之

非公務機關之代表人、管理人或其他有代表權人，不能證明已盡防止義務者外

第48條

1. 違反第8條或第9條規定。
2. 違反第10條、第11條、第12條或第13條規定。
3. 違反第20條第2項或第3項規定。
4. 違反第27條第1項或未依第2項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

→ 中央目的事業主管機關或直轄市、縣（市）政府 → 限期改正 → 屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰

58

本報告之智慧財產權歸屬於法務部

行政罰

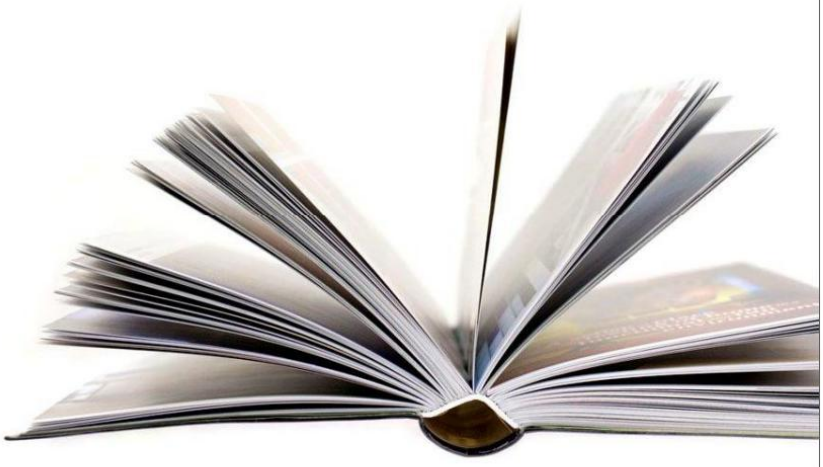
第49條

無正當理由違反第22條第4項規定者 → 中央目的事業主管機關或直轄市、縣（市）政府 → 處新臺幣二萬元以上二十萬元以下罰鍰

非公務機關之代表人、管理人或其他有代表權人，不能證明已盡防止義務者外

59

附則



本報告之智慧財產權歸屬於法務部

附則

第51條

- 第1項-有下列情形之一者，不適用本法規定：
  1.自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。
  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。
- 第2項-公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。

第52條

- 第1項-第22條至第26條規定由中央目的事業主管機關或直轄市、縣（市）政府執行之權限，得委任所屬機關、委託其他機關或公益團體辦理；其成員因執行委任或委託事務所知悉之資訊，負保密義務。
- 第2項-前項之公益團體，不得依第34條第1項規定接受當事人授與訴訟實施權，以自己之名義提起損害賠償訴訟。

第54條

- 本法修正施行前非由當事人提供之個人資料，依第9條規定應於處理或利用前向當事人為告知者，應自本法修正施行之日起一年內完成告知，逾期未告知而處理或利用者，以違反第9條規定論處。

61

資訊安全影片欣賞與案例探討

本報告之智慧財產權歸屬於法務部

動畫短片欣賞－維護個資鬥陣行

影片內容探討

- 劇情描述
  - ◆由影片中的劇情可以瞭解，阿郎以公司同仁的帳號密碼取得了客戶的資料，同時，也在網路上以P2P程式蒐集並下載被害人的個人資料，再轉賣給不肖份子，以獲取個人的利益。

- 影片中的「阿郎」，違反個人資料保護法中的哪一項條款？
  - ◆阿郎賣出個人資料的行為，因為有別於「蒐集」及「處理」的定義，應該屬於個資法規範內的「利用」行為。阿郎將個人資料賣出給不肖份子，顯然並非當初蒐集之特定目的的必要範圍之內，也沒有「法律明文規定」、「經當事人書面同意」等情形，因此違反個資法第20條第1項。

  - ◆除此之外，阿郎在網路上以P2P程式蒐集並下載被害人的個人資料，構成個資法所規範的「蒐集」行為，而阿郎在進行個人資料的蒐集時，顯也違反個資法第19條有關於蒐集的規定。

64

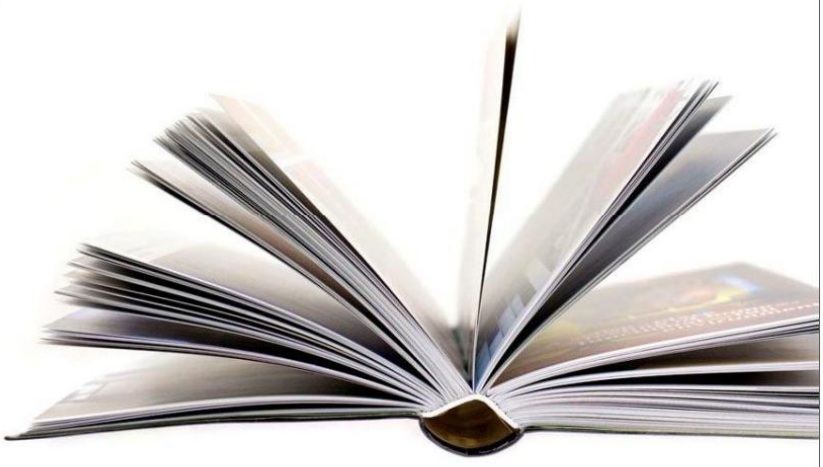
本報告之智慧財產權歸屬於法務部

影片內容探討

- 影片中的「阿郎」，可能面臨的罰則為何？
  - ◆依據個資法第41條，阿郎違反第19條及第20條第一項的項目，且足生損害於他人，可以處2年以下有期徒刑、拘役或科或併科新臺幣20萬元以下罰金。
  - ◆又阿郎心想藉由賣出個資等重要資訊以致富，顯然在犯前述之罪時懷有營利之意圖，故依據個資法第41條第二項，可提高懲處至5年以下有期徒刑，並得併科新臺幣100萬元以下罰金。
- 面對影片中的「阿郎」，我們該如何進行防範?
  - ◆不使用P2P軟體
  - ◆個人帳戶資料勿隨意給予他人
  - ◆時常更新防毒軟體病毒碼
  - ◆不下載非法軟體

65

判例探討



本報告之智慧財產權歸屬於法務部

違反電腦處理個人資料保護法之案例(1/5)

■非公務機關意圖營利致生損害於他人案

受審法院	台灣高等法院	判決字號	94年上易字第980號

案例摘要

被告：丙○○、乙○○

1) 丙○○：
於92年2月間成立「誠立電腦資訊工作室」（未經商業登記），明知該工作室未經設立登記，且**未依規定向目的事業主管機關即交通部電信總局申請許可、登記並領得「徵信業電腦處理個人資料許可執照」，依法不得為個人資料之蒐集、電腦處理或國際傳遞及利用**，竟基於意圖營利之犯意，自92年2月間起，多次向真實姓名不詳之蕭姓男子等人購買而蒐集各類個人或工商私密資料共計2千多萬筆，並在各大報紙刊登「千禧年新商名單」之廣告，以每筆新台幣0.6至0.8元不等之價格販賣給乙○○及綽號小謝、小張及房屋仲介業、幼教業等不特定人，並應各該購買資料客戶之需求，以電腦編排資料，或將個人資料列印於報表、標籤上，或燒錄於光碟內，而進行電腦處理後，再交付各該買主使用於拓展業務或轉賣營利使用。

67

違反電腦處理個人資料保護法之案例(1/5)

■非公務機關意圖營利致生損害於他人案

受審法院	台灣高等法院	判決字號	94年上易字第980號

案例摘要

2) 乙○○：
「瑟菲思股份有限公司」及「東榆顧問股份有限公司」之實際負責人，**未依規定向目的事業主管機關**即交通部電信總局申請許可、登記並領得「徵信業電腦處理個人資料許可執照」，**依法不得為個人資料之蒐集、電腦處理或國際傳遞及利用**，竟基於意圖營利之犯意，自91年間起，因其客戶需要寄件名單，遂多次自丙○○、萬士通資訊有限公司優力國際行銷有限公司唐○○購得而蒐集各類個人或工商私密資料共計24萬7千多筆，並自行寄發印有「行銷尖兵2004年最新工商名單」之廣告，以每筆資料0.5至1元不等之價格，販賣予蔡○○、李○○等保險公司、銀行業之業務人員及補教業等不特定公司行號或個人，且依客戶需求印製成個人資料電腦連續報表或姓名、地址名條貼紙。

3) 丙○○、乙○○販售前述個人及工商企業私密資料予不特定客戶後，致使個人資料之所有人均因個人私密資料遭外洩利用，屢接獲產品行銷或展業電話、廣告文宣及簡訊，**不勝困擾，造成生活不便，足認已生損害**於上開人等。

4) **法院判決**：違反《電腦處理個人資料保護法》第19條第1項，而犯同法第33條意圖營利違反前項規定之罪。

68

本報告之智慧財產權歸屬於法務部

違反電腦處理個人資料保護法之案例(1/5)

■非公務機關意圖營利致生損害於他人案

受審法院	台灣高等法院	判決字號	94年上易字第980號

案例重點

舊法《電腦處理個人資料保護法》將非公務機關定義為特定行業，但新修正《個人資料保護法》**已經沒有產業的分別了。任何人都可能會觸犯《個資法》**，應謹慎！
尤其是新《個資法》的**第19條**、**第20條**，現在任何人都需要注意是否有觸犯！

只要他人的個人資料因為您的行為而洩漏，導致他們遭到任何方式的騷擾、不便，都足以構成損害，也可能足以讓您依照《個人資料保護法》遭罰！

參考法條

舊法	新法
電腦處理個人資料保護法第19條 非公務機關未經目的事業主管機關依本法登記並發給執照者，不得為個人資料之蒐集、電腦處理或國際傳遞及利用。徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人，應經目的事業主管機關許可並經登記及發給執照。前二項之登記程序、許可要件及收費標準，由中央目的事業主管機關定之。	**(已刪除)**

69

違反電腦處理個人資料保護法之案例(1/5)

■非公務機關意圖營利致生損害於他人案

受審法院	台灣高等法院	判決字號	94年上易字第980號

參考法條

舊法	新法
電腦處理個人資料保護法第18條 非公務機關對個人資料之蒐集或電腦處理非有特定目的，並符合左列情形之一者，不得為之： 一、經當事人書面同意者。 二、與當事人有契約或類似契約之關係而對當事人權益無侵害之虞者。 三、已公開之資料且無害於當事人之重大利益者。 四、為學術研究而有必要且無害於當事人之重大利益者。 五、依本法第3條第7款第2目有關之法規及其他法律有特別規定者。	**個人資料保護法第19條** 非公務機關對個人資料之蒐集或處理，除第6條第1項所規定資料外，應有特定目的，並符合下列情形之一者： 一、法律明文規定。 二、與當事人有契約或類似契約之關係。 三、當事人自行公開或其他已合法公開之個人資料。 四、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。 五、經當事人書面同意。 六、與公共利益有關。 七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。 蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

70

本報告之智慧財產權歸屬於法務部

違反電腦處理個人資料保護法之案例(1/5)

■非公務機關意圖營利致生損害於他人案

受審法院	台灣高等法院	判決字號	94年上易字第980號
參考法條			
舊法		新法	
電腦處理個人資料保護法第23條 非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之。但有左列情形之一者，得為特定目的外之利用： 一、為增進公共利益者。 二、為免除當事人之生命、身體、自由或財產上之急迫危險者。 三、為防止他人權益之重大危害而有必要者。 四、經當事人書面同意者。		**個人資料保護法第20條** 非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為增進公共利益。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、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。 六、經當事人書面同意。 非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。 非公務機關於首次 行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。	

71

違反電腦處理個人資料保護法之案例(1/5)

■非公務機關意圖營利致生損害於他人案

受審法院	台灣高等法院	判決字號	94年上易字第980號
參考法條			
舊法		新法	
電腦處理個人資料保護法第33條 意圖營利違反第7條、第8條、第18條、第19條第1項、第2項、第23條之規定或依第24條所發布之限制命令，致生損害於他人者，處2年以下有期徒刑、拘役或科或併科新臺幣4萬元以下罰金。		**個人資料保護法第41條** 違反第6條第1項、第15條、第16條、第19條、第20條第1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2年以下有期徒刑、拘役或科或併科新臺幣20萬元以下罰金。 意圖營利犯前項之罪者，處5年以下有期徒刑，得併科新臺幣100萬元以下罰金。	

72

本報告之智慧財產權歸屬於法務部

違反電腦處理個人資料保護法之案例(2/5)

■侵入住宅竊聽個人資料案

受審法院	台灣高等法院	判決字號	86年上易字第1265號

案例摘要

被告：郭○○、蕭○○

1) 郭○○係「聯合」徵信社負責人，接受一姓名、年籍不詳之成年男子客戶之委託，共同意圖營利，並基於概括之犯意之聯絡推由蕭○○以鐵條撥開大門，並在大門電門開關處裝置觸控器，無故侵入陳○○所居住該棟公寓住宅樓梯間，在二、三樓之間屬於陳○○所使用之第九四四一九五五五號電話之分線盤鐵盒架內，未經居於四樓當事人陳○○之書面同意或與當事人陳○○有契約或類似契約之關係，**私自架設錄音設備，用以竊聽蒐集陳○○之家庭、職業、財物狀況及社會活動等個人資料致生損害於陳○○**，並每日前往該處，以鐵器撥動觸控器打開大門，更換錄音帶，攜回上開徵信社交予郭○○再由郭○○轉交予該不詳名之男子。

2) **法院判決**：違反《電腦處理個人資料保護法》第18條第1款、第2款，致生損害於陳○○，故犯同法第33條。

73

違反電腦處理個人資料保護法之案例(2/5)

■侵入住宅竊聽個人資料案

受審法院	台灣高等法院	判決字號	86年上易字第1265號

案例重點

任何形式的蒐集個人資料，都須依法行之。即便沒有直接接觸到當事人，也沒有從他人得到當事人的個人資料，也有可能觸犯個資法的規定！

參考法條

舊法	新法
電腦處理個人資料保護法第18條第1款、第2款 非公務機關對個人資料之蒐集或電腦處理非有特定目的，並符合左列情形之一者，不得為之： 一、經當事人書面同意者。 二、與當事人有契約或類似契約之關係而對當事人權益無侵害之虞者。	**個人資料保護法第19條** 非公務機關對個人資料之蒐集或處理，除第6條第1項所規定資料外，應有特定目的並符合下列情形之一者： 一、法律明文規定。 二、與當事人有契約或類似契約之關係。 五、經當事人書面同意。

74

本報告之智慧財產權歸屬於法務部

違反電腦處理個人資料保護法之案例(2/5)

■侵入住宅竊聽個人資料案

受審法院	台灣高等法院	判決字號	86年上易字第1265號
參考法條			
舊法		新法	
電腦處理個人資料保護法第33條 意圖營利違反第7條、第8條、第18條、第19條第1項、第2項、第23條之規定或依第24條所發布之限制命令，致生損害於他人者，處2年以下有期徒刑、拘役或科或併科新臺幣4萬元以下罰金。		**個人資料保護法第41條** 違反第6條第1項、第15條、第16條、第19條、第20條第1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2年以下有期徒刑、拘役或科或併科新臺幣20萬元以下罰金。 意圖營利犯前項之罪者，處5年以下有期徒刑，得併科新臺幣100萬元以下罰金。	

75

違反電腦處理個人資料保護法之案例(3/5)

■擅自開啟電話接線箱竊聽個人資料案

受審法院	台灣高等法院	判決字號	89年上更(一)字1054號
案例摘要			
被告：甲○○ 1) 甲○○：為「一統徵信有限公」之調查員，負責該公司受委託調查在宜蘭縣員山鄉榮民醫院工作之乙○○是否結交女友之資料蒐集，因跟蹤拍照無結果後，為求績效，竟自民國八十六年九月十二日晚上七、八時許起，**擅自開啟中華電信公司宜蘭營業處，轄有之編號ＹＳ－三０九０號電話接線箱，擅接小型錄音機一部**，竊聽上開醫院所承租（起訴書誤載為乙○○所承租）裝設於乙○○辦公室，由乙○○專用之０三－0000000電話**蒐集乙○○日常生活動態等個人資料致生損害於乙○○**，並每隔一、二天即收取更換錄音帶一次，攜回上開一統公司，交予不知情之該一統公司費姓經理。 2) **法院判決**：違反《電腦處理個人資料保護法》第18條第1款、第2款，致生損害於乙○○，故犯同法第33條。			

76

本報告之智慧財產權歸屬於法務部

違反電腦處理個人資料保護法之案例(3/5)

■擅自開啟電話接線箱竊聽個人資料案

受審法院	台灣高等法院	判決字號	89年上更(一)字1054號

案例重點

任何形式的蒐集個人資料，都須依法行之。即便沒有直接接觸到當事人，也沒有從他人得到當事人的個人資料，也有可能觸犯個資法的規定！

參考法條

舊法	新法
電腦處理個人資料保護法第18條第1款、第2款 非公務機關對個人資料之蒐集或電腦處理非有特定目的，並符合左列情形之一者，不得為之： 一、經當事人書面同意者。 二、與當事人有契約或類似契約之關係而對當事人權益無侵害之虞者。	**個人資料保護法第19條** 非公務機關對個人資料之蒐集或處理，除第6條第1項所規定資料外，應有特定目的並符合下列情形之一者： 一、法律明文規定。 二、與當事人有契約或類似契約之關係。 五、經當事人書面同意。

77

違反電腦處理個人資料保護法之案例(3/5)

■擅自開啟電話接線箱竊聽個人資料案

受審法院	台灣高等法院	判決字號	89年上更(一)字1054號

參考法條

舊法	新法
電腦處理個人資料保護法第33條 意圖營利違反第7條、第8條、第18條、第19條第1項、第2項、第23條之規定或依第24條所發布之限制命令，致生損害於他人者，處2年以下有期徒刑、拘役或科或併科新臺幣4萬元以下罰金。	**個人資料保護法第41條** 違反第6條第1項、第15條、第16條、第19條、第20條第1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2年以下有期徒刑、拘役或科或併科新臺幣20萬元以下罰金。 意圖營利犯前項之罪者，處5年以下有期徒刑，得併科新臺幣100萬元以下罰金。

78

本報告之智慧財產權歸屬於法務部

違反電腦處理個人資料保護法之案例(4/5)

■公務機關受友人之託查詢個人資料案

受審法院	台灣高等法院	判決字號	85年上易字第1527號

案例摘要

被告：陳○○

1) 陳○○：為警員，然並非處理BQ-六八八八號車禍警員，又未經受理報案，卻以其受友人傅○○之託，使用個人密碼啟動電腦端末機查詢車號ＢＱ-六八八八號自用小客車之車籍資料(含有個人資料如：姓名、身分證統一編號及地址等)，**查出車籍資料內的個人資料。傅○○在一旁窺視**。

2) **法院判決：**
法官認為，車籍資料含有個人資訊，公路監理機關作為公務機關，應防止其洩漏。陳○○非處理ＢＱ-六八八八號車禍警員，又未經受理報案，受朋友之託使用個人密碼輸入代號啟動電腦端末機查詢車籍資料。雖然沒有列印提供給友人，也沒有讓友人在一旁抄錄，但顯然有洩密故意。

79

違反電腦處理個人資料保護法之案例(4/5)

■公務機關受友人之託查詢個人資料案

受審法院	台灣高等法院	判決字號	85年上易字第1527號

案例重點

即便沒有列印個人資料、提供給他人當事人抄錄個人資料這些明顯違法的動作，只要可以推論有洩漏之故意，都有可能遭到個資法的制裁！

參考法條

舊法	新法
電腦處理個人資料保護法第17條 公務機關保有個人資料檔案者，應指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	**個人資料保護法第18條** 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

80

本報告之智慧財產權歸屬於法務部

違反電腦處理個人資料保護法之案例(5/5)

■賄賂警察換取個人資料案

受審法院	台灣高等法院	判決字號	94年上訴字第2203號

案例摘要

被告：黃○○、葉○○等人

1) 黃○○：為專門接受徵信業者委託以查取個人資料之**徵信管道業者**。黃○○知悉葉○○為警察人員，其為圖將上開資料出售與他人，**多次交付賄款以換取葉○○告知上開資料，之後再出售圖利**。黃○○另外還透過電話分別冒充警員名義，**多次憑葉○○洩漏之當月保密代號（碼）**，各向警政、戶政單位及監理機關查詢數人之全戶、年籍、車籍等資料。

2) 葉○○：為苗栗縣警察局保安隊巡佐，**是依據法令從事公務之人員**，且具有調查職務因偵辦案件所需，得向各警察局通報台或主管機關查詢案件關係人之入出境資料、前科車籍、口卡、全戶資料、電話查住址、行動電話、銀行帳戶等資料，**且依法不得洩漏之**。葉○○連續以本人或盜用同事魏○○警員之領用密碼登入警政電腦系統，查取特定被查人之出入境、前科、車籍、口卡、外籍護照等個人資料，並將**該等職務上應秘密之個人資料透過電話回報予被告黃○○**。

81

違反電腦處理個人資料保護法之案例(5/5)

■賄賂警察換取個人資料案

受審法院	台灣高等法院	判決字號	94年上訴字第2203號

案例摘要

3) **法院判決：**

黃○○：違反《電腦處理個人資料保護法》第23條之規定，應依同法第33條規定處斷。

葉○○：為苗栗縣警察局保安隊巡佐，係依據法令從事公務之人員，違反《電腦處理個人資料保護法》第 8條之規定，應依同法第 33條規定處斷。

案例重點

賄賂公務機關或以其他方式非法取得個人資料，除了違反個人資料保護法，還有可能受到違反刑法的規定！

身為公務機關，應謹慎保護當事人的個人資料，千萬不可以接受不肖分子的賄賂，也不可以提供給不肖分子竊取個人資料的方法！

82

本報告之智慧財產權歸屬於法務部

違反電腦處理個人資料保護法之案例(5/5)

■賄賂警察換取個人資料案

受審法院	台灣高等法院	判決字號	94年上訴字第2203號
參考法條			
舊法		新法	
電腦處理個人資料保護法第23條 非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之。但有左列情形之一者，得為特定目的外之利用： 一、為增進公共利益者。 二、為免除當事人之生命、身體、自由或財產上之急迫危險者。 三、為防止他人權益之重大危害而有必要者。 四、當事人書面同意者。		**個人資料保護法第20條** 非公務機關對個人資料之利用，除第6條第1項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為增進公共利益。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、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。 六、經當事人書面同意。 非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。 非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。	

83

違反電腦處理個人資料保護法之案例(5/5)

■賄賂警察換取個人資料案

受審法院	台灣高等法院	判決字號	94年上訴字第2203號
參考法條			
舊法		新法	
電腦處理個人資料保護法第33條 意圖營利違反第7條、第8條、第18條、第19條第1 項、第2項、第23條之規定或依第24條所發布之限制命令，致生損害於他人者，處2年以下有期徒刑、拘役或科或併科新臺幣4萬元以下罰金。		**個人資料保護法第41條** 違反第6條第1項、第15條、第16條、第19條、第20條第1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2年以下有期徒刑、拘役或科或併科新臺幣20萬元以下罰金。 意圖營利犯前項之罪者，處5年以下有期徒刑，得併科新臺幣100萬元以下罰金。	

84

本報告之智慧財產權歸屬於法務部

違反電腦處理個人資料保護法之案例(5/5)

■賄賂警察換取個人資料案

受審法院	台灣高等法院	判決字號	94年上訴字第2203號
參考法條			
舊法		新法	
電腦處理個人資料保護法第8條 公務機關對個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。但有左列情形之一者，得為特定目的外之利用： 一、法令明文規定者。 二、有正當理由而僅供內部使用者。 三、為維護國家安全者。 四、為增進公共利益者。 五、為免除當事人之生命、身體、自由或財產上之急迫危險者。 六、為防止他人權益之重大危害而有必要者。 七、為學術研究而有必要且無害於當事人之重大利益者。 八、有利於當事人權益者。 九、當事人書面同意者。		**個人資料保護法第16條** 公務機關對個人資料之利用，除第6條第1項所規定資料外，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。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為維護國家安全或增進公共利益。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、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。 六、有利於當事人權益。 七、經當事人書面同意。	

85

面對新版個人資料保護法，該如何因應？

本報告之智慧財產權歸屬於法務部

個資法疑義及說明 – 彙整說明

個資法的目的

- 為規範個人資料之蒐集、處理及利用，避免人格權受到侵害，並促進個人資料之合理利用，特制定本法。

個資法要求

- 除特種資料以外，並沒有規定哪些資料不能收。
- 它只強調，你想要蒐集或處理個資，必須符合規定，且要保護及留紀錄；否則就 不要拿、不要留；
- 它也沒不准你提供或傳輸個資，但是一樣就是要符合規定並且做好管控，否則，不要傳就沒事了!
- 重點是，這些過程都需要留下紀錄，以作為舉證之用！

87

怎麼做？

查法令

- 有沒有法令有較鬆的要求？

清個資

- 找出業務範圍內可能有個資的地方

設控管

- 針對有個人資料的部份進行管理的設計

做確實

- 以稽核或教育訓練等方式，確保大家都落實執行

88

本報告之智慧財產權歸屬於法務部

同仁現在開始要做什麼準備？

識別業務範圍的法令依據

- 請針對您所負責的業務，整理相關的法令依據及可能之個資檔案，包含：
  - 法令規範可以蒐集的資料(如：員工健康檢查)；
  - 法令規定可以給的資料(如：配合檢警調查)；
  - 法令規定不可刪除的資料(如：離職員工資料的保存年限要求)。

留意個資的流向與管理方式

- 請時時留意您身邊各種可能的個人資料，以及相關的管理方式是否適當，如：
  - 傳真機的資料是否隨時取回；
  - 包含個人資料的紙本是否有適當的銷燬而未被當成回收用紙使用。

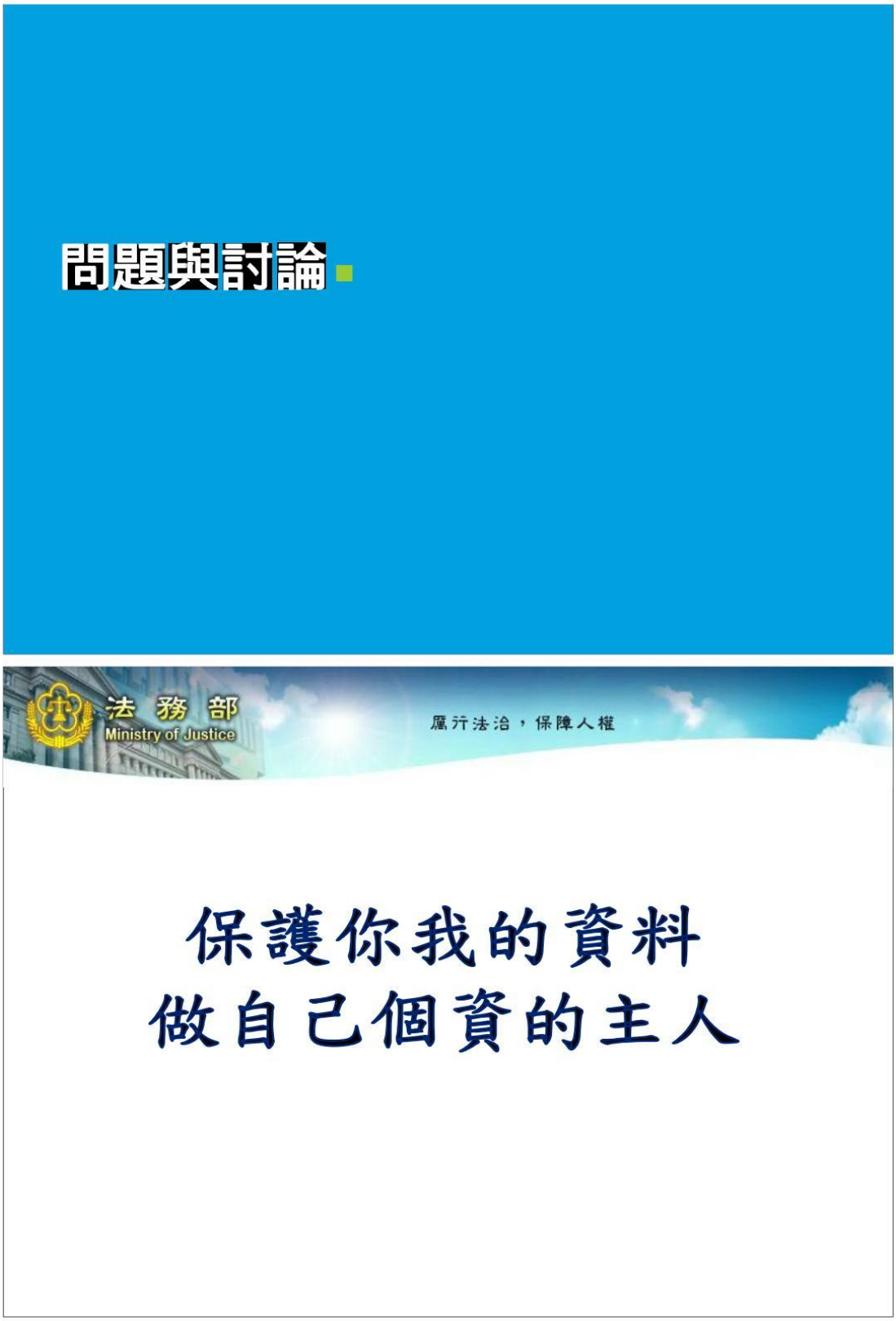
89

最後提醒事項

■ 經識別的個人資料，都必須評估其風險，並依其風險大小設置對應之安全控管機制，故個資留越多，部處所要花的控管成本將越高。故我們建議…

90

本報告之智慧財產權歸屬於法務部



資料來源：本計畫撰寫

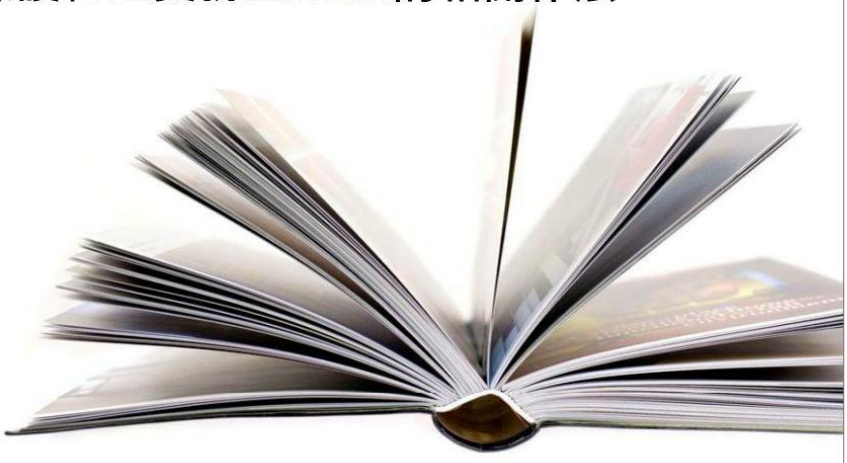
本報告之智慧財產權歸屬於法務部

二、中階公務機關個資保護專責人員培訓教材

（一）中階教材

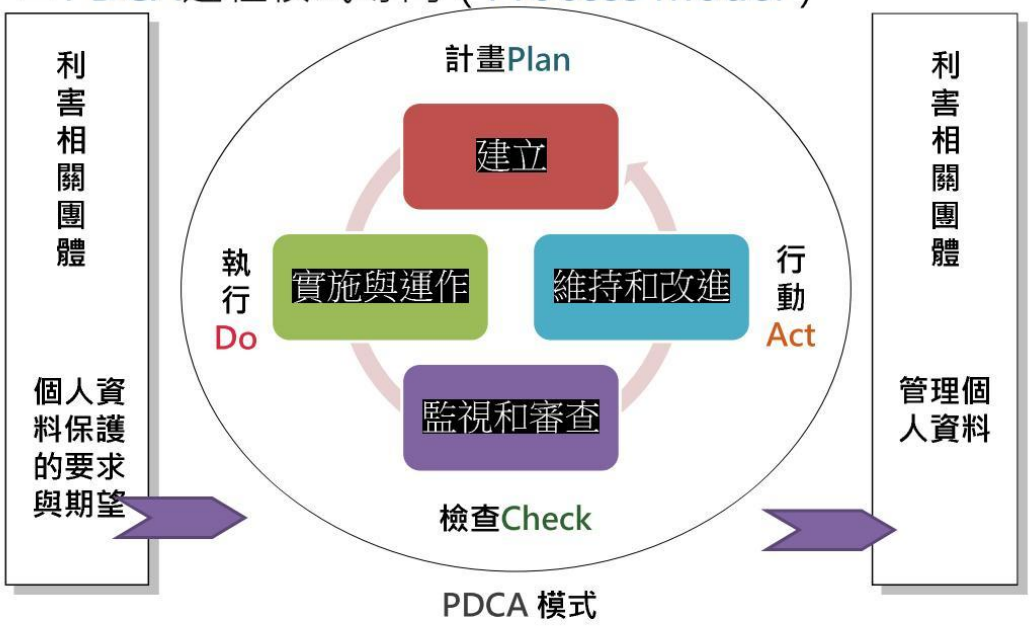
本報告之智慧財產權歸屬於法務部

個人資料保護管理實務上PDCA的相關作法與原則



個人資訊管理系統PDCA循環

■ PDCA過程模式導向（Process model）



4

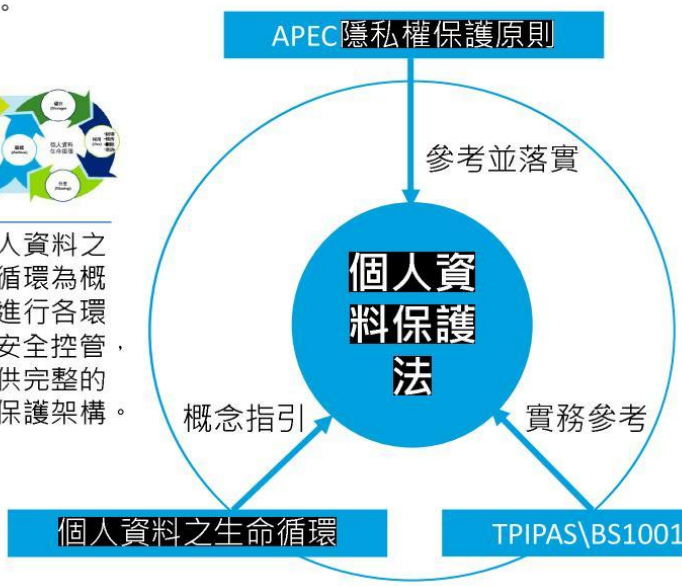
©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

我國個人資料保護法與實作概觀

- APEC隱私保護原則為亞太地區經濟體間及其貿易夥伴間對於隱私保護的遵循原則。
- 個資法修正內容內，亦已將APEC隱私保護原則的9項原則落實於條文內容之中。

依個人資料之生命循環為概念，進行各環節的安全控管，以提供完整的個資保護架構。

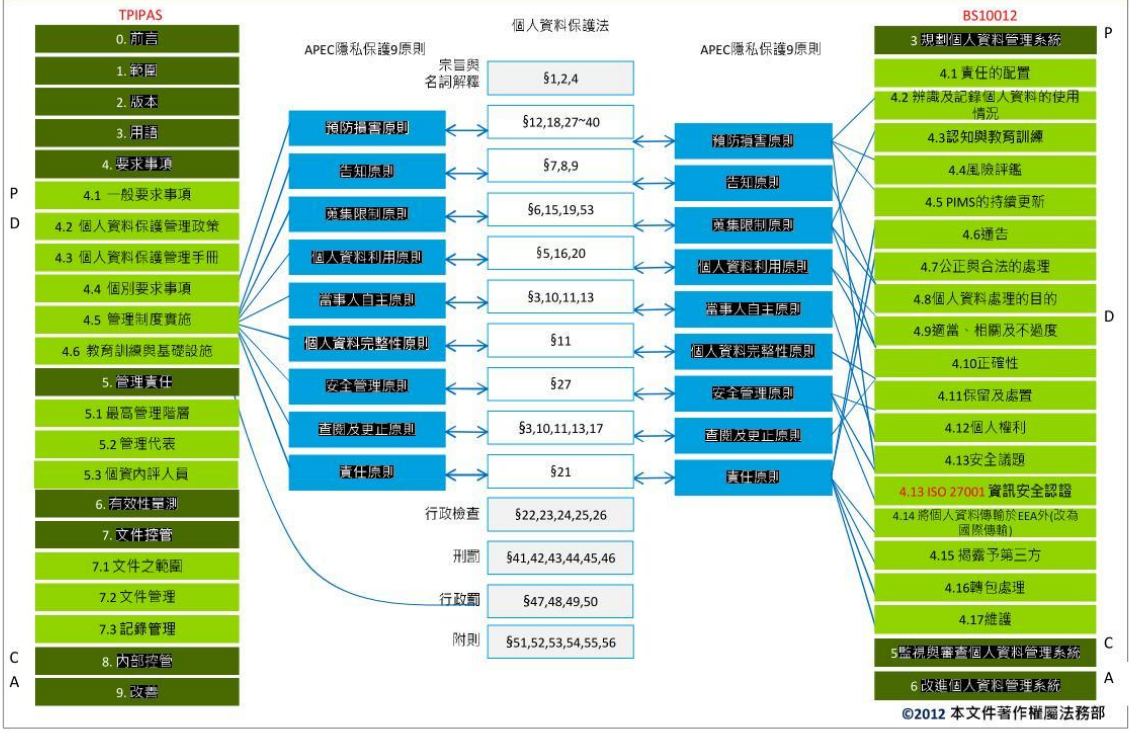


個人資料保護標準的目的在建立個人資料保護的最佳實務與協助組織符合個人資料保護法的規範。

5

©2012 本文件著作權屬法務部

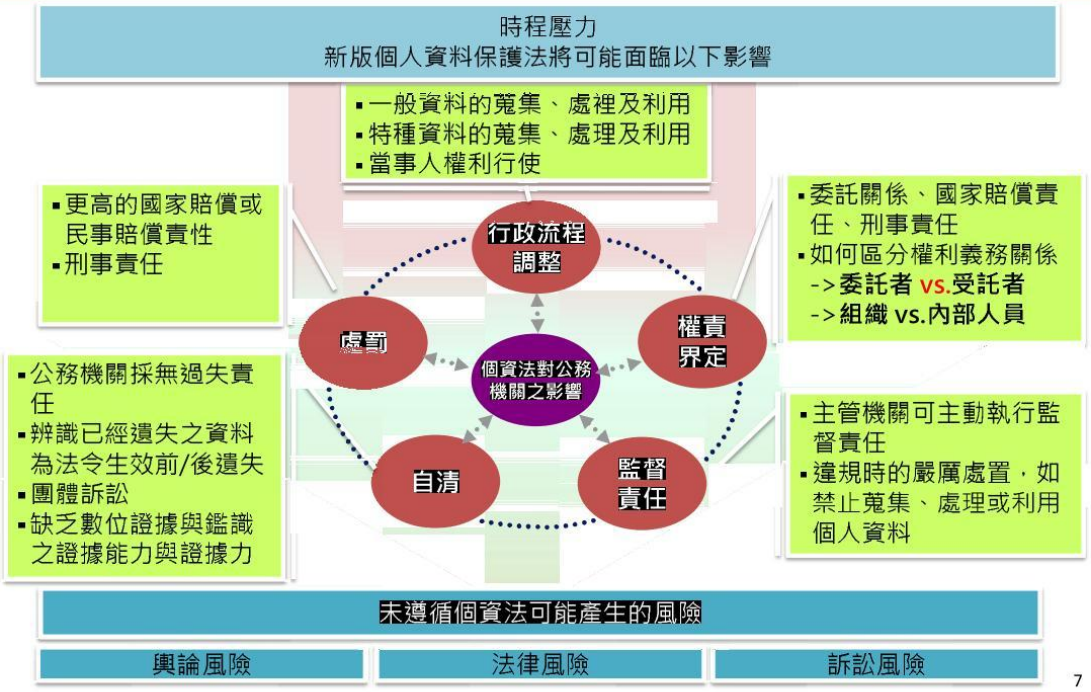
個人資料保護法 vs. APEC隱私保護原則 vs. TPIPAS vs.BS10012



©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

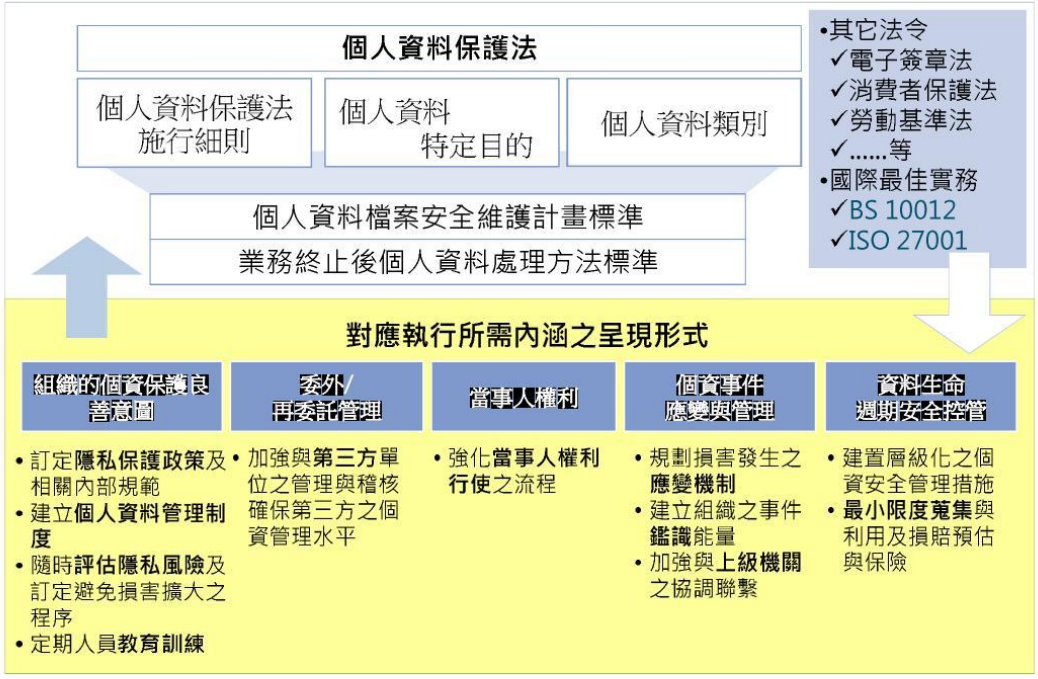
五大影響點與風險



7

©2012 本文件著作權屬法務部

What : 個人資料保護法概要與影響

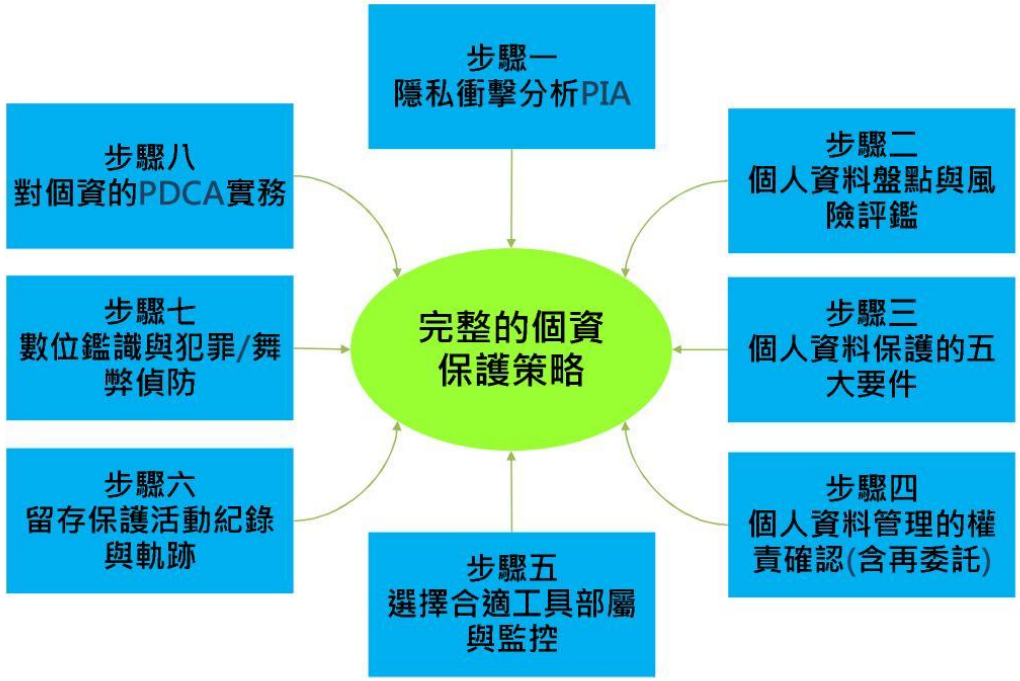


8

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

How：完整的個資保護策略



9

©2012 本文件著作權屬法務部

個資法的遵循-怎麼達成?

查法令

- 有沒有其他法令有相關的要求？

清個資

- 找出業務範圍內可能有個資的地方

設控管

- 針對有個人資料的部分進行管理的設計

做確實

- 以稽核或教育訓練等方式，確保大家都落實執行

10

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

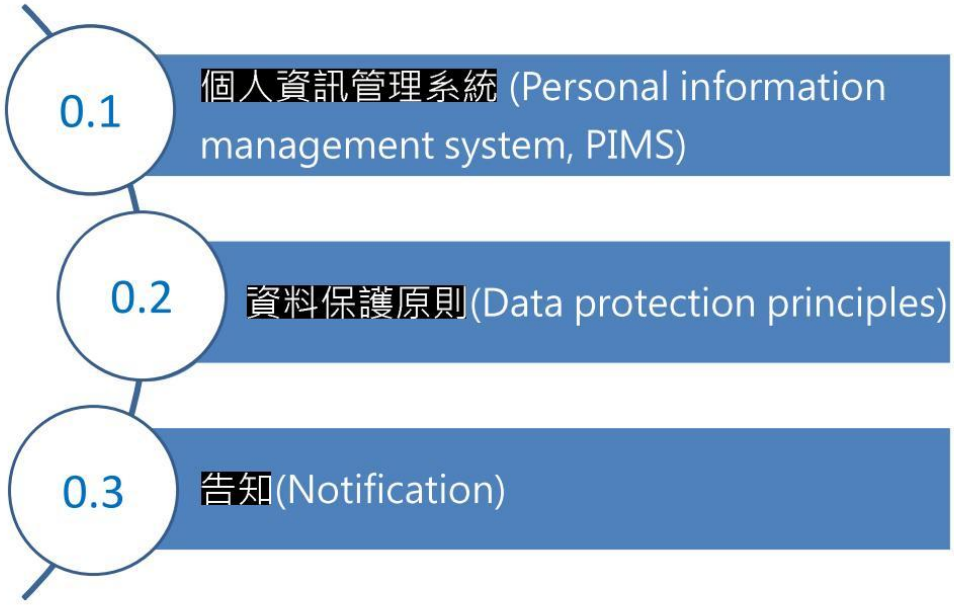
介紹「BS 10012：2009」個人資料管理系統

(資料來源：BSI英國標準協會)

0 簡介(Introduction)

本報告之智慧財產權歸屬於法務部

0 簡介



13

©2012 本文件著作權屬法務部

0.1 個人資訊管理系統(PIMS)

本標準的目的是

- 讓組織能夠備妥個人資訊管理系統(Personal Information Management System, PIMS)，作為整體資訊治理基礎設施的一部分

- 個人資訊管理系統(Personal Information Management System, PIMS)提供了一個架構，讓組織能維持和改善對資料保護相關法律及優良實務的遵循。
- 本標準使用英國用語「個人資訊 (Personal Data)」
- 為避免英文翻譯混淆，我國個人資料保護法用語為「個人資料(Personal Information) 」或「個人資料檔案(Personal Information File)」 。

14

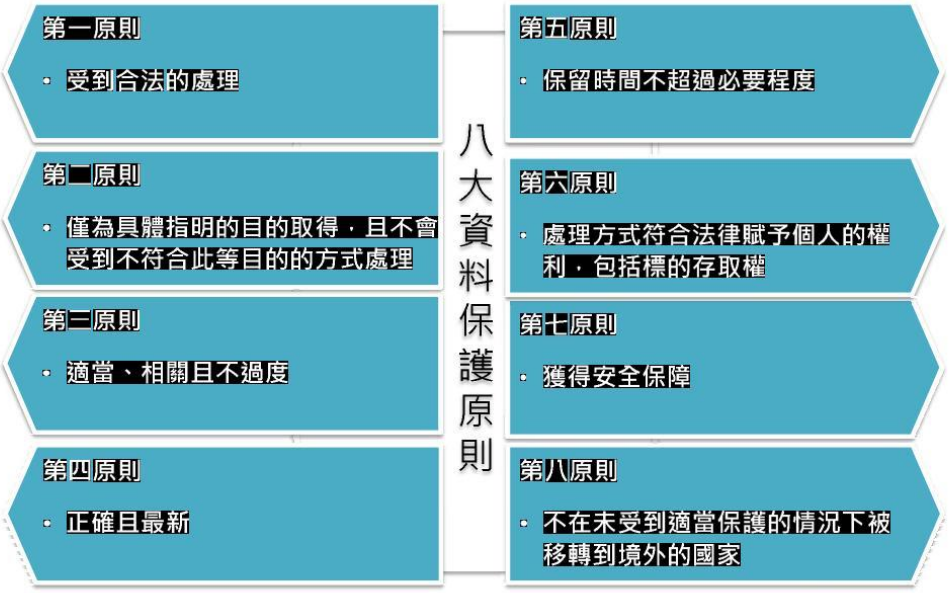
(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

0.2 資料保護原則

■ 「資料控制者」(Data Controller)必須遵循八大資料保護原則，其要求個人資料必須：



15

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

0.3 告知

■ 要求組織將處理過程告知資訊委員(ICO)，以確保透明公開，但免除告知義務的例外狀況不適用此規定。

- (我國目前並無資訊委員(ICO)，建議參考未來各中央目的事業主管機關推動施行之相關法規及行政規則)。

16

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

1 範圍(Scope)

1 範圍

- 本標準具體說明對個人資訊管理系統(PIMS)的各項要求。PIMS提供了一個架構，讓組織能對資料保護法律及優良實務的遵循。
- 本標準應用了**「計畫-執行-檢查-行動」(Plan-Do-Check-Act, PDCA)**循環。
- 本標準乃是為任何規模和部門的組織而設計。其目的是為個人資訊的管理提供一個共同的基礎，進而對個人資訊的管理產生信心，並讓內部和外部的評估人員有效評估組織遵循資料保護法律及優良實務的狀況。

18

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

2 名詞、定義與縮寫 (Terms, definitions and abbreviations)

2.1 名詞與定義

稽核 (audit)	• 有系統地檢查，以判定活動及相關結果是否符合規劃中的安排，且這些安排是否受到有效實行，適於達到組織的政策和目標。
當事人 (individual)	• 個人資訊所屬之人。
管理系統 (management system)	• 建立政策和目標以及達到這些目標的系統。
不符合事項 (nonconformity)	• 未實現某項要求之狀況。
組織 (organization)	• 處理資訊的法律實體。如：自然人、獨資商號、公司、合夥事業、法人團體、公共部門 、機構、志工協會及慈善團體。

20

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

2.1 名詞與定義

個人資訊 (personal information)	• 與可辨識之自然人有關的個人資料。
個人資訊管理政策 (personal information management policy)	• 組織為了維持和改善對資料保護法律及優良實務的遵循所制訂，並由管理高層正式核准的整體意圖與方向聲明。備註：下簡稱「政策」。
個人資訊管理系統(PIMS)	• 是建立、實行、運作、監督、審查、維持和改善個人資訊管理的整體管理架構之一部分。
程序 (procedure)	• 作某件事的一套正式或公認的行動方式，且已做成文件紀錄。

21

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

2.1 名詞與定義

流程 (process)	• 為達某種結果而採行的一連串行動。
處理 (processing)	• 取得、紀錄或持有個人資訊、或對個人資訊進行任何運作。(這包括蒐集、組織、改編、變更、揭露、分享、宣傳、比對、整合、凍結、清除或破壞個人資訊。)
系統 (system)	• 一套互有關係或相互影響的要素。
人員 (workers)	• 在組織控制下工作之人。 備註：這包括員工、臨時雇員、承包商、志工及顧問。

22

(資料來源：BS 10012: 2009，BSI英國標準協會)

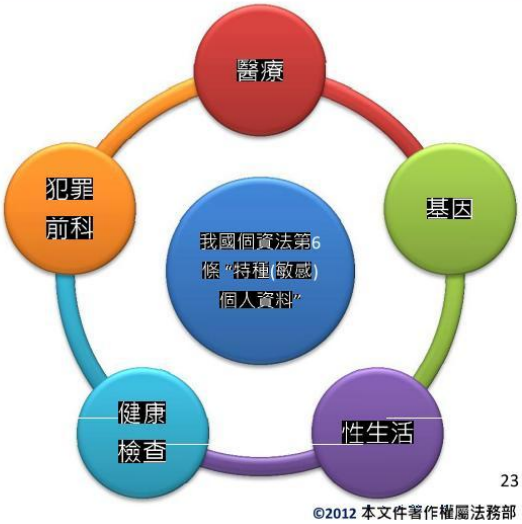
©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

2.1 名詞與定義

敏感個人資訊
(sensitive personal information)

- 請注意: BS 10012:2009 對於「敏感個人資訊」係依「英國個人資料保護法」規定所定義，與「我國個人資料保護法」對於「特種(敏感)個人資料 」之定義不同，避免混淆，特此說明



23

©2012 本文件著作權屬法務部

3 規劃個人資訊管理系統(PIMS)
(Planning for a personal information management system)

本報告之智慧財產權歸屬於法務部

3 規劃個人資訊管理系統(PIMS)

- 目標：規劃如何實行個人資料管理系統，使其可提供方向和支援，讓組織遵循資料保護法律及優良實務。

3.1	PIMS的建立與管理
3.2	PIMS的範圍與目標
3.3	個人資訊管理政策
3.4	政策內容 (Policy content)
3.5	職責與責任承擔
3.6	資源提供
3.7	將PIMS深植於組織文化

25

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

3 規劃個人資訊管理系統(PIMS)

- 3.1 PIMS的建立與管理
  - 組織應依據第3.2條到第3.7條之要求建立、實作、維護及持續改進PIMS。建立文件紀錄的個人資訊管理系統(PIMS)。
- 3.2 PIMS的範圍與目標(Scope and objectives)
  - 組織應考量以下事項，定義範圍，並制訂個人資訊管理的目標：

26

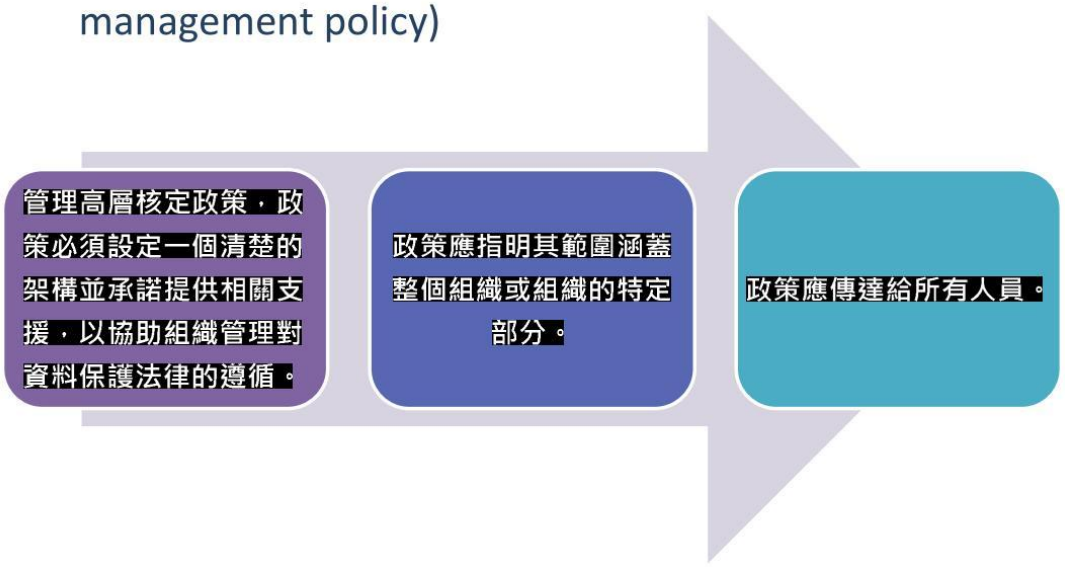
(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3 規劃個人資訊管理系統(PIMS)

■ 3.3 個人資訊管理政策(Personal information management policy)



27

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

3 規劃個人資訊管理系統(PIMS)

■ 3.4 政策內容 (Policy content) (1 of 2)

- 政策應指明組織致力於遵循資料保護法律及優良實務的承諾，包括：

編號	內容
a)	組織只會基於合法的組織目的，在確實**必要的範圍內**處理個人資訊
b)	僅基於**合法目的蒐集最少**的必要個人資訊，且不會處理多餘的個人資訊；
c)	**清楚告知**個人，何人會以何種方式使用他們的個人資訊；
d)	僅處理**相關且適當**的個人資訊；
e)	**公平合法**地處理個人資訊 (參照第 4.7條)；
f)	**維持**一份組織處理的個人資訊類別清單(參照第4.2條)；
g)	確保正確的個人資訊，在必要之處，維持正確且最新的個人資訊；
h)	僅基於法律或管制規定的要求或合法的組織目的來保留個人資訊；

28

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3 規劃個人資訊管理系統(PIMS)

■ 3.4 政策內容 (Policy content) (2 of 2)

- 政策應指明組織致力於遵循資料保護法律及優良實務的承諾，包括：

編號	內容
i)	尊重個人對他們個人資訊的相關權利，包含標的存取權；
j)	保障所有個人資訊的安全；
k)	僅在有**適當充分保護**的狀況下，將個人資訊移轉到國(境)外的地方；
l)	適用資料保護法所允許的各種例外狀況；
m)	發展和實行PIMS，讓政策落實；
n)	在適當之處，確認內部與外部的利害關係人，以及這些利害關係人涉及及組織PIMS治理的程度；
o)	確認對PIMS有特定職責且承擔責任 (參照第3.5條)的人員。

29

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

3 規劃個人資訊管理系統(PIMS)

■ 3.5 職責與責任承擔(Responsibility and accountability)

- **管理高層團隊應有一位成員負責組織內部的個人資訊管理**，才能證明組織對資料保護法律及優良實務的遵循狀況。

其責任應包括：

- 管理高層團隊核准政策；
- 依政策要求發展與實行PIMS；
- 與政策遵循有關的安全與風險管理。

- **組織應指派一位或以上適當資格或有經驗的人員**負責每日監督組織遵循政策的狀況。
- 所有人員均必須遵守政策，落實相關流程和程序，組織亦應備妥獎懲制度、適當的員工發展訓練，以及對任何不符合要求狀況的處理程序。

30

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3 規劃個人資訊管理系統(PIMS)

- 3.6 資源提供(Provision of resources)
  - 組織應提供資源，建立、實行、運作並維持PIMS。
- 3.7 將PIMS深植於組織文化(Embedding the PIMS in the organization's culture)
  - 為確保個資管理成為組織核心價值及有效管理的一部分，應：

• a)持續進行教育和意識提升計畫；	• b)建立評估PIMS意識傳達有效性的流程；	• c)將以下事項的有效性傳達給所有人員： • 1)達成PIMS的目標； • 2)遵守政策 • 3)持續改善政策	• d)確保所有人員知道PIMS目標及違反的後果。

31

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4 實行與運作PIMS (Implementing and operating the PIMS)

本報告之智慧財產權歸屬於法務部

4 實行與運作PIMS

■ 4.1 重要人員之指派(Key appointments)

目標

- 確保組織依照政策的要求，指派適當的承擔責任及負責執行職務之人員。

● 4.1.1 管理高層(Senior management)

- ➢ 組織應指定管理高層團隊中的一位成員擔任組織內部個人資訊管理的責任，如此才能證明組織對資料保護法律及優良實務的遵循狀況。
- ➢ 承擔責任的管理高層及負責日常遵循的人員可以是同一人。

33

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.1 重要人員指派

● 4.1.2 日常監督組織遵循政策狀況的責任

- ➢ **應指派一位或以上有適當資格或經驗的人員**，負責每日監督組織遵循政策的狀況。可全職或兼職負責這項職務。
- ➢ 被指派的人員應負責以下事項：

編號	內容
a)	遵循政策的整體責任/發展審查政策/確保政策落實/管理階層審查政策；
b)	對人員進行訓練及意識提升；
c)	個人資訊處理程序的核准，例如隱私權聲明的管理和傳達/個人資訊的蒐集與處理/申訴處理/安全事件的管理/委外管理。
d)	與組織內負責風險管理和安全問題的人聯繫；
e)	提供個人資料保護相關法規的專家建議和指引；/確保組織取得資料保護立法的相關更新法令及適當指引；/持續檢視並反映法律、實務和技術的變更；
f)	提供與資料分享專案有關的建議(包括資料攜出的安全問題)；
g)	依照適當情況，實施適用的產業規範中所載明的個人資訊處理相關實務。

34

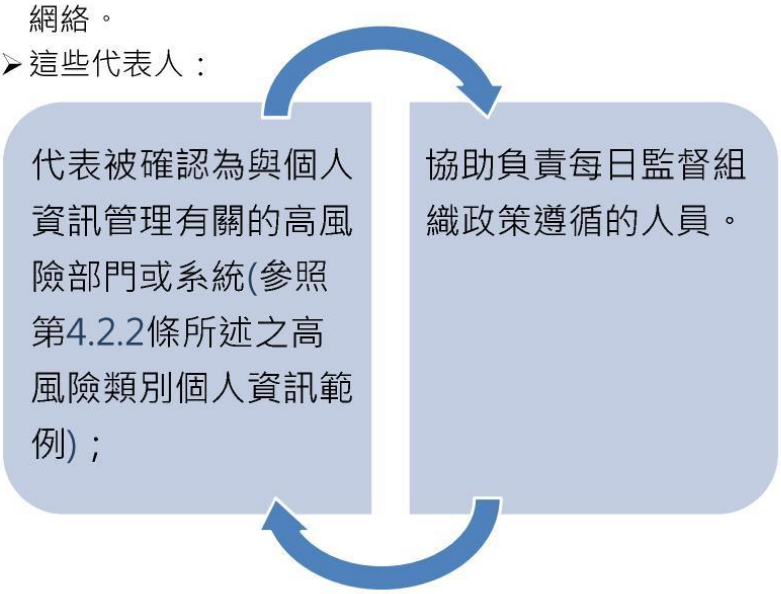
(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.1 重要人員指派

- 4.1.3 資料保護代表人(Data protection representatives)
  - 如處理個人資訊的部門或系統有多個，應建立資料保護代表人網絡。
  - 這些代表人：



35

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.2 識別並記錄個人資訊的用途

■ 4.2 識別並記錄個人資訊的用途(identifying and recording uses of personal information)

目標

- 確保組織了解其處理的個人資訊之類別，以及處理此等資訊的相關風險程度。

- 4.2.1 總論(General)
  - 應維持一份**個人資訊類別清單**，這份清單亦應載明使用每個個人資訊類別的**目的**。應紀錄個人資訊會歷經哪些**流程**。

36

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.2 識別並記錄個人資訊的用途

- 4.2.2 高風險個人資訊(High-risk personal information)
  - 個資類別清單應考量組織的高風險個資類別之明確識別及文件紀錄。(備註：在大量處理個人資訊的領域，風險程度可能增高)
  - 本標準係依英國個資法所認定高風險個資類別應包括：

    (備註: 本標準之敏感性資訊係依「英國個人資料保護法」所定義，與「我國個人資料保護法」之「特種(敏感)個人資料 」之定義不同，為避免混淆，特此說明)

37

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.4 風險評估

■ 4.4 風險評估(Risk assessment)

目標

- 確保組織了解處理特定類型個人資訊的任何相關風險。

評估風險

- 建立評估處理個人資訊對相關個人風險程度的流程(應包括其他組織所從事的資訊處理。)

管理風險

- 應妥善管理所評估確認的任何風險。

呈報及審查程序

- 建立程序，讓可能對個人造成的損害或痛苦的任何個人資訊處理能夠向上呈報，由負責個人資訊管理及相關責任的人員來審查。

38

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.3 訓練與意識

■ 4.3 訓練與意識(Training and awareness)

目標

- 確保**所有人員**在處理個人資訊時**知道自己的職務**。

- 應確保每日負責確認組織遵循資料保護法律及作業規範的人員，能夠證明他們確實**了解相關要求**及**如何實施**。
- 應確保此等人員在適當時與**外部機構聯絡**，以持續獲知與個人資訊管理有關的議題。
- 應能證明所有人員**了解責任**，並考量相關安全需求，以確保個人資訊是在符合程序下受到保護和處理。
- **所有人員均應接受訓練**，讓他們有能力依據程序處理個人資訊。訓練應適合每個人員在組織內的角色。

39

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.5 維持最新的個人資訊管理系統(PIMS)

■ 4.5 維持最新的個人資訊管理系統(PIMS)(Keeping PIMS up-to-date)

目標

- 評估PIMS是否能持續提供基礎設施，來維持和改善對資料保護法律及優良實務的遵循。

- 負責每日監督組織遵循政策的人員，應持續評估PIMS是否能證明組織遵循資料保護法律及優良實務，並能在**需要時**做出改變(變更)。
- 應於**組織要求或技術變更時**，進行PIMS的審查。

40

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.6 通知

■ 4.6 通知(Notification)

目標

- 確保組織依照個人資料保護相關法規的要求，將其處理個人資訊之細節告知資訊委員(ICO)
- (我國目前並無資訊委員(ICO)，建議參考未來各中央目的事業主管機關推動施行之相關法規及行政規則)。

● 應結合相關程序來落實告知(除非資料保護相關法律之告知例外要求)，並確保此等告知的內容是正確且最新的。

- ➢ 依據我國個資法第7、8、9...條：告知及書面同意等要求
- ➢ 通知方式：依施行細則及未來各中央目的事業主管機關之法規與行政規則

41

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.7 公平合法地處理

■ 4.7 公平合法地處理(Fair and lawful processing)

目標：確保個人資訊受到公正合法的處理，且在開始處理前已清楚確認處理個人資訊的法律基礎。

4.7.1	個人資訊的蒐集與處理
4.7.2	隱私權公告與聲明的紀錄
4.7.3	隱私權公告與聲明的時機
4.7.4	隱私權公告與聲明的可取得性
4.7.5	第三方

42

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.7 公平合法地處理

- 4.7.1 個人資訊的蒐集與處理(Collection and processing of personal information) (1 of 2)應建立程序，確保：

編號	內容
a)	**公平合法地**處理個人資訊；
b)	僅在個人資料保護相關法律確認為正當的目的及範圍內處理個人資訊及敏感個人資訊；
c)	提供個資給組織的任何人會獲得「隱私權公告」或線上隱私權聲明，提供的方式可能是全文呈現，也可能僅提供摘要和公告全文的連結或出處。此等隱私權公告或聲明應清楚傳達以下資訊： ✓ 組織的身份； ✓ 處理個資目的； ✓ 將個資揭露給第三方之相關資訊； ✓ 個人對個資存取權之相關資訊； ✓ 個資是否在無充分保護下被移轉國(境)外； ✓ 欲詢問個資處理相關問題，如何聯繫組織之細節； ✓ 在網站上蒐集個人資訊所使用之任何技術 (例如cookies) 之細節； ✓ 確保處理過程公平的任何其他資訊。

43

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.7 公平合法地處理

- 4.7.1 個人資訊的蒐集與處理(Collection and processing of personal information)(2 of 2)

編號	內容
d)	如為了行銷目的或未來可能用於行銷目的而蒐集個資，應建立程序確保向個人清楚解釋其**可拒絕此等行銷之方式**。
e)	如是根據個人的同意來處理資訊，而該**個人已撤銷其同意**，在此等情況，應建立程序，根據該同意所為的資訊處理將停止。
f)	如其他部門要求或法律規定行銷必須有明確的同意行為，應包含**取得此等同意**的程序。
g)	如組織為特定目的蒐集敏感個資，應建立程序，確保隱私權公告明確陳述敏感個資被使用或可能被使用之目的。
h)	應建立程序確保新的蒐集方法會由合格或有經驗的人員檢視並簽名核定，以確保此等方法是符合資料保護法律。

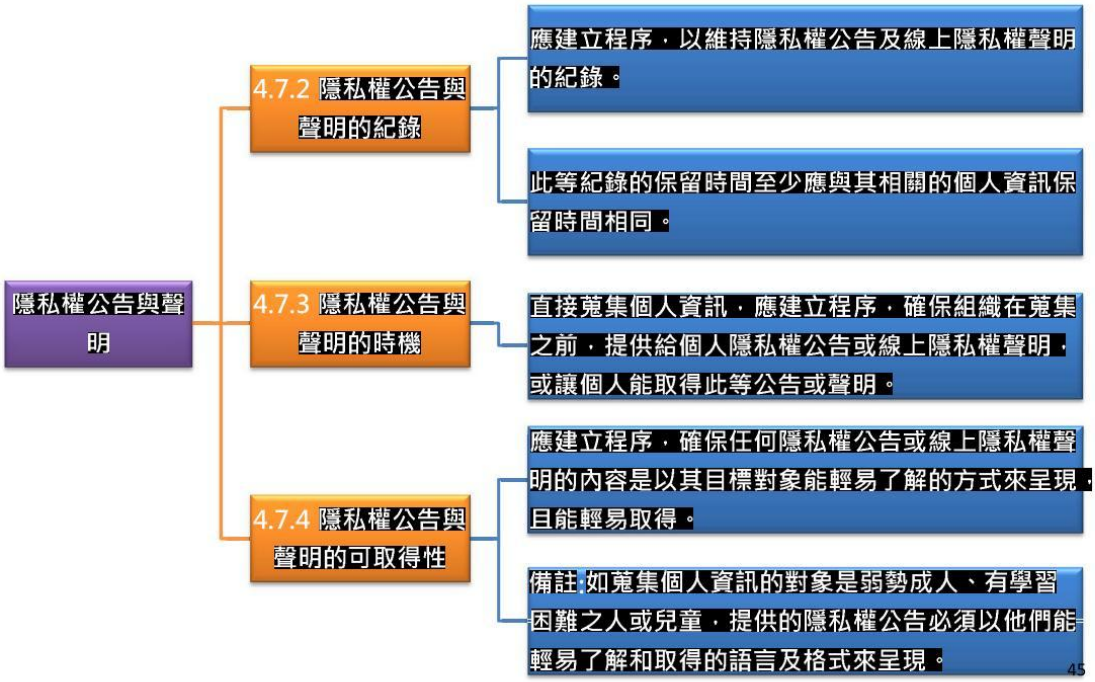
44

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.7 合法地處理



45

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.7 公平合法地處理

- 4.7.5 第三方(Third parties)
  - 應建立程序，確保個資是從第三方公平合法地蒐集。
  - 應建立程序，確保在需要之處對個人提供隱私權公告，且在適當之處提供線上隱私權聲明，但如果這麼做需要付出不相稱的努力，則不在此限。

備註：前文中的**「不相稱的努力」**不僅指「相當大的努力」，因為組織可能必須克服許多困難才能提供隱私權公告，並在需要之處提供線上隱私權聲明，而這樣的處理可能對個人造成不利影響。

46

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.8 為具體指明的目的處理個人資訊

■ 4.8 為具體指明的目的處理個人資訊(Processing personal information for specified purposes)

目標

- 確保組織僅為一個或以上具體指明的目的而取得個人資訊，且不會以任何不符合此等目的之方式對個人資訊做進一步的處理。

● 4.8.1 處理的基礎(Grounds for processing)應建立程序：

a)確保個人資訊不會以違反或可能違反任何法律義務之方式被處理，包括法律規定、習慣法或合約條款的義務。

b)確保為具體指明之目的所蒐集的個人資訊不會用於任何其他不相容的目的，但以下情況不在此限：

- 1)適用免除法律義務的情況；
- 2)如組織欲為特定目的外利用個人資訊，該個人資訊所屬之人已同意組織為特定目的外利用其個人資訊。

c)確保敏感個人資訊將用於相容的新目的時，組織在處理前已獲得個人之明確同意，但免除此等義務的情況不在此限。

47

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.8 為具體指明的目的處理個人資訊

● 4.8.2 取得當事人對於特定目的外利用之同意 (Consent to new purposes)

應建立程序：

- 確保個人同意組織為特定目的外利用其資訊，是在自由意識且資訊充分的情況下提供。
- 確保：

a)**獲取個人同意**組織為特定目的外利用其個人資訊的肯定表示；以及

b)維持為新目的獲得**同意的紀錄**。

48

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.8 為具體指明的目的處理個人資訊

● 4.8.3 資料分享(Data sharing)

應建立程序確保在組織與其他組織分享個資時，雙方當事人對於個資之責任已正式載明於書面協議或合約。

如其他組織將為自己的目的使用個人資訊，應建立程序確保：
a)書面協議或合約載明資訊可能被使用之目的，以及進一步為其他目的使用個資的任何限制或約束；
b)其他組織提供承諾或證據，來證明其不會以牴觸個人資料保護相關法律》的方式處理資訊。

應建立程序，確保涉及與第三方分享個人資訊處理符合告知程序，及提供給個人的隱私權公告或線上隱私權聲明的條款。

如不可能，組織應確保：
a)有合法資料分享基礎；
b)在受到要求時，取得個人對資料分享的同意。

當允許與第三方分享資料但不需個人同意的情況，應建立程序，確保該資料分享的協定與控制措施已做成可稽核的文件紀錄。

在必須與第三方分享資料的情況，例如法律規定，應建立程序，確保資料分享的協定與控制措施已做成文件記錄。

49

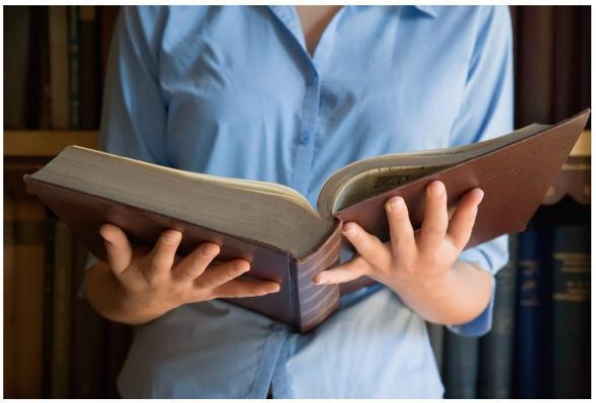
(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.8 為具體指明的目的處理個人資訊

● 4.8.4 資料比對(Data matching)

➢ 在將個人資料與其他個人資料比對，以達成某種目的之情況，例如進一步辨識個人的特徵，應建立程序，確保比對的個人資訊**已依照法律要求或已獲得同意，僅用於已告知且相容的目的**。



50

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.9 適當、相關且不過度

■ 4.9 適當、相關且不過度(Adequate、relevant and not excessive)

目標：確保個人資訊是適當、相關且不過度。

4.9 適當、相關且不過度	4.9.1 適當	應建立程序，確保蒐集個資的目的是適當的。
		應包含定期審查個人資訊處理相關技術和流程的程序，確保個人資訊處理的目的仍是適當的。
	4.9.2 相關且不過度	在合法目的所需要的範圍內，處理最少的個人資訊；
		不處理不相關或對明確陳述的目的而言是多餘的資訊，除非個人選擇提供此等資訊，且組織僅在個人同意下處理此等資訊
		審查個人資訊處理的相關新系統及流程，以確保處理之資訊是相關且不過度的。

如個人資訊對組織的目的而言是不相關或不需要的，PIMS應確保該個人資料不會被處理。

51

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.10 正確

■ 4.10 正確(Accuracy)(1 of 2)

目標

- 確保個資是正確的，且在需要之處維持最新的個資。應建立程序：

確保被處理之個人資訊維持完整和正確性。 → 若當事人資訊不正確且不能更正，例如歷史紀錄，應建立程序，指出該資訊不正確，並在適當之處提供正確的個人資訊。 → 確保人員被告知正確紀錄個人資訊的重要性，以及僅使用最新的個人資訊來做出有關個人的重要決定之重要性。 → 檢查當事人聲稱的不正確資訊是否真的不正確。

52

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.10 正確

■ 4.10 正確(Accuracy)(2 of 2)

●應建立程序，處理及審查與個人資料處理有關的新系統及流程：

處理	確認
• 如組織提供給任何第三方的個人資訊是不正確且過時的，應將該情況告知該第三方，並告知第三方此等資訊不應被用來做出有關該個人的決定； • 在需要之處將任何更正的個人資訊提供給第三方。	• 確保這些系統或流程能盡可能防止記錄不正確或過時的個人資訊； • 對不正確或過時的個人資訊做出更正。

53

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.11 保留與處置

■ 4.11 保留與處置(Retention and disposal)

目標：確保個人資訊保留的時間不超過必要程度。

應建立個資的保留時程表，該時程表應：

- 包含法律及組織要求的任何最低保留時間
- 對保留時間提供清楚的正當理由和基礎；以及
- 如保留個人資訊的時間超過載明的最低保留時間，例如可能為歷史及/或研究目的而保留，應載明任何可適用的正當理由。

應建立程序，以落實保留時程表，並將時程表傳達給所有相關人員。

應建立程序，確保組織依規定處置不再需要的個人資訊。

應建立處置程序，且該程序的管理應符合：

- 核准的流程；
- 具有符合個資敏感程度的安全保障程度；
- 組織的資訊安全風險評估。

備註：在某些案例，將個人資訊移往檔案館以便永久保存，此等處置方式可能是較適當的。

54

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.12 個人的權利

■ 4.12 個人的權利(Individuals' Rights)

目標：確保組織備妥適當的程序，讓個人的權利能夠受到尊重。

4.12.1 個人的權利(Rights of individuals)

- 應建立程序，確保當事人對其個人資訊的相關權利受到尊重且當個人請求行使此等權利時，組織會在任何法律規定的時間限制內處理此等請求。
- 備註：此等權利包括資訊存取權、反對處理權...。

4.12.2 申訴與向上呈報(Complaints and appeals)

- 應包含申訴程序，確保組織正確處理有關個人資訊處理的申訴。應包括當事人對於他們的申訴被處理的方式考量及向上呈報的程序。

55

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.13 安全議題

■ 4.13 安全議題(Security issues)

目標

- 實施適當的技術及安全措施，確保個資受到保護，不會遺失或受損，也不會受到未經授權或不合法的處理。

● 4.13.1 安全控制措施(Security controls)

➢ PIMS應考量以下方面，並具體指明安全控制措施：

a) 所處理個資類型；
b) 若資訊受到損害，對當事人的風險及衝擊。

✓ 備註：風險評估(參照第4.4條)將確立組織控制措施的適當程度。過度的安全要求與不夠具體的安全要求同樣是有害的。

➢ 如處理的個資屬於高風險個資，應確保具體指明和實行的安全措施對於已評估的風險來說是適當的，並確保安全措施隨著時間經過仍是適當的。

✓ 備註：在適當時，組織可考慮遵循BS ISO/IEC 27001標準。組織也可以選擇由外部機構進行BS ISO/IEC 2700標準的認證，以證明其遵循標準。

56

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.13 安全議題

- 4.13.2 儲存與處置(Storage and handling)
  - ➢ 應建立程序，確保個人資訊受到安全的儲存與處理，並備妥符合其機密性和敏感度的預防措施。
    - ✓ 備註：組織應特別注意個人資訊儲存在媒體及可攜式裝置的情況，例如備份媒體、可移除式USB磁碟、可移除式硬碟、筆記型電腦及手提裝置。
- 4.13.3 傳輸(Transmission)
  - ➢ 個人資訊在組織內部以電子或手動方式傳輸，或傳輸到其他組織時，應建立程序，確保此等傳輸的安全受到組織定義的適當方法所保障，進而保護傳輸期間的資訊安全。
- 4.13.4 存取控制措施(Access controls)

在允許人員存取個資的情況，應建立程序，確保只有在職務上需要存取之人員才能存取個資。

如存取權限是法律所賦予，應建立程序，確保人員清楚了解存取權限僅為工作目的而賦予，且人員僅能為合法目的存取資訊。

如處理的個人資訊屬於高風險個人資訊，應建立程序，確保存取權限的控制措施能反映該資訊的敏感度。

應建立程序，確保所有存取個人資訊的行為受到監督，且受到符合組織訊安全風險評估之評估。

57

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.13 安全議題

- 4.13.5 安全評估(Security assessments)
  - 應建立程序，確保組織定期進行安全評估。
  - 此等評估應確認現存的安全控制措施是否充足，並在需要之處提供改善的建議。
  - 此等評估應考量當安全事件發生時，對個人所受到之危害、損害的風險。
- 4.13.6 管理安全事件(Managing security incidents)

  應包含以下適當程序：
  - **評估和管理涉及個資的安全事件**，包含減緩損害之程序；
  - **記錄每個安全事件**，包括事件如何發生的評估、採取的矯正行動，以及可以從事件學習到的教訓；
  - **決定**是否將安全事件轉由相關管制機關處理(例如資訊委員會或主管機關)，或通知當事人；
  - **紀錄任何已核發的轉介及通知。**

58

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.14 將個人資訊移轉到國(境)外的地方

■ 4.14 將個人資訊移轉到國(境)外的地方

目標：確保個人資訊被移轉到國(境)外的地方被處理時，受到充分的保護。

應建立程序，確保個人的權利受到保護：				應建立程序，確保：		
在合約中納入保障條款，確保資訊及資訊的處理受到保護；	在移轉到美國的情況，確認個資將被移轉的目的地組織是否已證明其遵循美國聯邦貿易委員會的要求，且符合安全港原則；	確認目的地國家或地區是否已被中央目的事業主管機關(暫定)評估為能夠提供充足的保護；以及	若資訊是由另一個組織處理的情況，對該組織善盡監督之責。	遵循性保護人員(參照第4.1.2條)檢查所有涉及個人資訊移轉到國(境)外地方的行動。	檢查確認移轉已受到充分保護。	位在國(境)外的地方、代表組織處理個人資訊的轉包商，依照要求執行合約，確保個人資訊受到充分保護。

59

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.15 對第三方揭露資訊

■ 4.15 對第三方揭露資訊(Disclosure to third parties)

目標：確保對第三方揭露個人資訊之行為受到管理，以符合資料保護法律

a)應建立適當程序，確保第三方提供：

1)其具有個資存取權的證明；

2)在需要時，其身分之證明。

→ b)確保組織對第三方揭露任何資訊具有合法基礎。

c)組織應在需要的範圍內，對第三方揭露最少的個人資訊。

→ d)應維持個人資料揭露的記錄。此等記錄應能證明揭露是合法的，且應能讓組織持續追蹤個資在何處被揭露。

60

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

4.16 外包處理

■ 4.16 外包處理 (Sub-contracted processing)

目標：確保代表組織的另一個組織處理個資時受到管理，以符合資料保護法律及優良實務。

- 如資訊是由代表組織的其他組織處理時，應建立程序，確保：

編號	內容
a)	其他組織能提供充分的技術、實體及組織安全措施，以達到組織個資安全要求；
b)	在與另一個組織約定之前，進行適當安全性的評估，作為盡責調查的行動之一，且如果因為將處理的個人資訊之本質或處理的特殊狀況所需要，組織在締結合約之前應對其他組織的安全措施安排進行稽核；
c)	一旦挑選了其他組織，組織應備妥書面協議來提供具體指明的服務，並要求其他組織提供處理個資的安全措施；
d)	合約應規定，在擁有個資存取權的期間，其安全措施能定期受到稽核；
e)	如其他組織意圖使用轉包商來處理個資，其合約有義務先獲得組織對此等意圖的許可；
f)	合約應要求轉包商至少要遵循與其他組織相同的安全和其他規定；以及
g)	與其他組織締結的合約(向下延伸到任何轉包商)應具體指明在合約終止時，相關個人資訊應銷毀、交還組織或交給組織指定的另一個組織。

61

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

4.17 維護

■ 4.17 維護(Maintenance)

建立維護程序，確保各項程序及技術要素受到維護，並因此能正確且適當運作。

這些程序應能確保組織在頻繁排定的時間，規劃並執行此等維護。

62

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

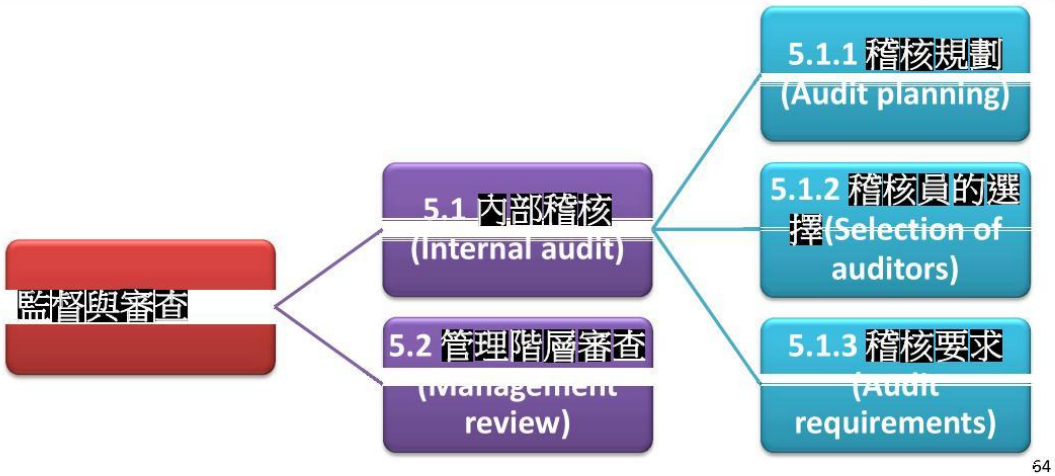
本報告之智慧財產權歸屬於法務部

5 監督與審查PIMS
(Monitoring and reviewing the PIMS)

5 監督與審查PIMS

目標

- 確保PIMS的有效性及效率受到監督和審查。



64

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

5 監督與審查PIMS

■ 5.1 內部稽核(Internal audit)

5.1.1 稽核規劃(Audit planning)

- 組織應考量政策要求，規劃、建立和維持稽核方案，以監督和審查組織處理個人資訊的有效性及效率。
- 稽核方案應明確包含任何高風險個人資訊之處理(參照第4.2.2條)，且應包含其它組織執行的個人資訊處理(參照第4.16條)。

5.1.2 稽核員的選擇(Selection of auditors)

- 組織應選擇適當的稽核員，且稽核員應盡責進行稽核，以確保稽核方案的客觀性及公正性。
- 備註：規模較大以及處理高風險個人資訊(參照第4.2.2條)的組織，應考量由外部當事人定期進行稽核。

65

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

5 監督與審查PIMS

■ 5.1 內部稽核(Internal audit)

5.1.3 稽核要求(Audit requirements)

- 稽核應在規劃的時間進行，以判定PIMS：
  - 運作是否符合政策及確立的程序；以及
  - 是否已根據技術要求來實行和維護。
- 在稽核後，如發現個人資訊的處理有任何重大偏離政策及/或確立程序的情況，應將詳述此等情況的稽核報告提供給管理階層。
- 稽核報告亦應確認可能影響組織遵循政策的技術或流程相關問題。

66

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

5 監督與審查PIMS

■ 5.2 管理階層審查(Management review)

- 組織應執行PIMS之管理審查，其執行頻率可為定期、於預先安管理階層應經常定期或在發生重大變化時審查PIMS，以確保系統維持適切性、充足性及有效性。
- 管理階層審查應根據以下事項來執行：
  - 來自PIMS使用者之回饋意見；
  - 人員發現並向上呈報的風險；
  - 稽核的結果；
  - 程序審查紀錄；
  - 技術升級及/或更換的結果；
  - 管理機關的正式評估請求；
  - 申訴處理；以及
  - 已發生的違反/安全事件。
- 管理階層審查應提供PIMS可能變更的相關詳細資訊，例如確認可能影響遵循的政策、程序及/或技術修正。
- 如PIMS實行重大變更，在實行後應儘快完成稽核。

67

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

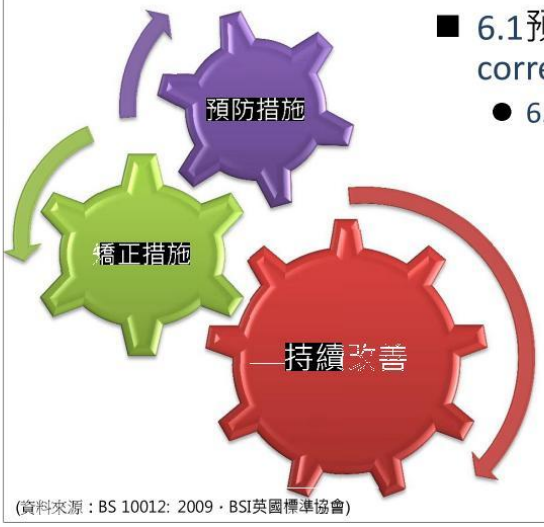
6 改善個人資訊管理系統(PIMS)
(Improving the PIMS)

本報告之智慧財產權歸屬於法務部

6 改善個人資訊管理系統(PIMS)

目標

- 實施矯正措施，以改善個人資訊管理系統(PIMS)的有效性和效率。



■ 6.1預防與矯正措施(Preventive and corrective actions)

- 6.1.1總論(General)
  - 組織應藉由實施預防與矯正措施來改善PIMS。
  - 所有提議的改變及/或改善應先評估在實行，以確保達成政策的各項要求。
  - 如變更可能影響證明組織遵循資料保護法律及優良實務的能力(例如將個人資訊轉換為新的儲存檔案格式)，此等變更應受到審查，以判定其是否確實對組織遵循造成影響。
  - 由預防及矯正措施所產生的變更應做成文件紀錄，並根據保留時程加以保留。

69

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

6 改善個人資訊管理系統(PIMS)

- 6.1.2 預防措施(Preventive actions)

組織應採取行動來監視潛在的不符合事項，以防止它們發生。

a)找出潛在的不符合事項及其原因；

b)決定與實行需要的預防措施；

c)記錄採取的行動並加以審查；

d)找出變化的風險；

e)確保所有需要知道的人員被告知潛在的不符合事項，以及備妥的預防措施。

70

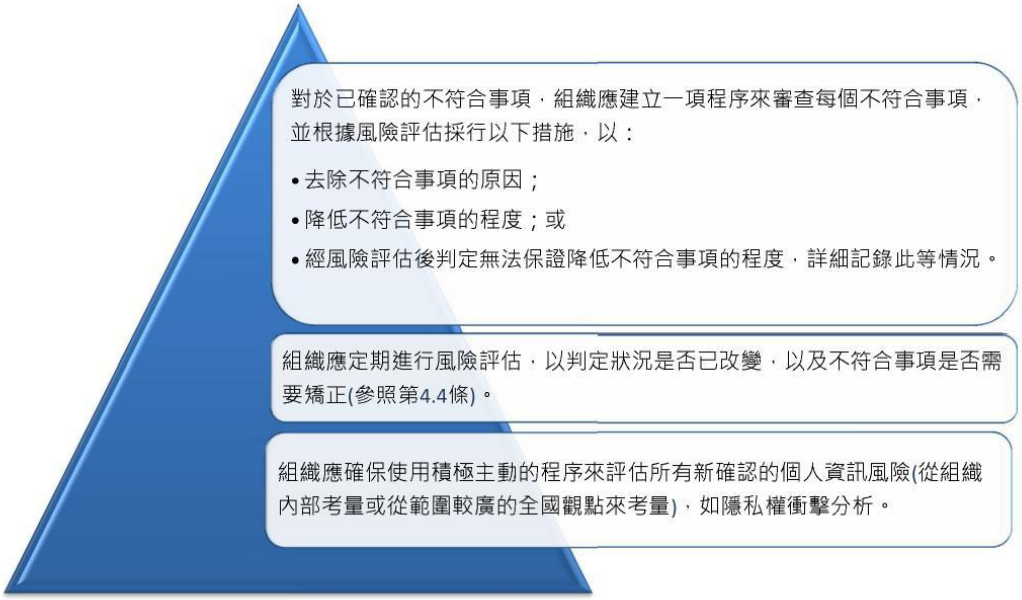
(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

6 改善個人資訊管理系統(PIMS)

● 6.1.3 矯正措施(Corrective actions)



71

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

6 改善個人資訊管理系統(PIMS)

■ 6.2 持續改善(Continual improvement)

組織應透過稽核結果、預防措施與矯正行動以及管理階層審查，持續改善個人資訊管理系統(PIMS)的有效性。

組織應運用申訴、資安事件、標的存取請求及其它議題，來協助改善個人資訊管理系統(PIMS)的有效性。

72

(資料來源：BS 10012: 2009，BSI英國標準協會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

介紹「JISQ-15001：2006」個人資料保護管理系統指引

(資料來源：JISQ日本工業標準調查會)

前言

本報告之智慧財產權歸屬於法務部

前言

- 此標準規範乃基於日本工業標準化法，通過日本工業標準調查會審議，並由日本經濟產業大臣(經濟部長)修正後公告實施。
- 此份文件乃根據JISQ 15001:1999進行修訂。爾後相關標準規範皆須依JISQ 15001:2006執行。

75

©2012 本文件著作權屬法務部

個人資料保護管理系統適用範圍

本報告之智慧財產權歸屬於法務部

個人資料保護管理系統適用範圍

- 此規範適用於任何在商業行為中會使用到個人資料的企業。不論企業種類及規模大小,於執行上述所列事項時,皆須依照此標準進行

77

(資料來源： JISQ 15001:2006 ，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

相關名詞解釋及其定義

本報告之智慧財產權歸屬於法務部

相關名詞解釋及其定義 (1/3)

個人資料 (Personal information)	• 含姓名、出生年月或其他可以明確識別特定之人的資料，亦包含參照其他資料後可容易識別個體之相關資料
當事人 (Person)	• 個人資料中可被具體識別之個人
營業單位 (Business Entity)	• 任何從事商業形式之法人、個人或團體

79

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

相關名詞解釋及其定義 (2/3)

個人資料保護之稽查員 (Personal Information Protection Auditor)	• 由營業單位代表所指派之人員，須為公平及客觀的角色，具責任及權力實施與回覆稽查之狀況
當事人的同意 (Consent of the Person)	• 在給定蒐集或利用有關個人資料之目的下，自當事人取得交付願意之許可，如為兒童，則須取得監護人之同意。
個人資料保護管理者 (Personal Information Protection Managers)	• 由營業單位所指派的管理者，負責個人資料保護管理系統的營運

80

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

相關名詞解釋及其定義 (3/3)

個人資料管理系統 (Personal information Management System)	• 管理系統包括策略、組織、規劃、實施、審查和稽核，用於保護企業內部使用個人資料的權利與利益以及考慮其個人資料的實用性
不符合事項 (Nonconformance)	• 未符合此規範內的某項要求
改正措施 (Corrective action)	• 檢討不符合事項之原因並加以改進之措施

81

(資料來源： JISQ 15001:2006 ，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

個人資料保護管理系統要求事項

本報告之智慧財產權歸屬於法務部

個人資料保護管理系統要求事項

- 一般要求事項
- 個人資料保護方針
- 個人資料保護計畫
- 個人資料保護計畫實施及其運用
- 個人資料保護教育
- 個人資料保護管理系統文件
- 申訴及諮詢
- 查核與驗證
- 矯正及預防措施
- 營業單位代表人之審查機制

83

©2012 本文件著作權屬法務部

3.1 一般要求事項

- 營業單位必須**建立**、**執行**、**維護**及**改善**個人資料保護管理系統。

84

(資料來源： JISQ 15001:2006・JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3.2 個人資料保護方針

營業單位在明確制定個人資料保護的理念下，下列個人資料保護政策，必須持續的改進：

a) 個人資料蒐集、揭露與利用的合適性，須考慮其個人資料內容與企業規模大小（包括為達某些特定目的，需將資料用於原範 圍外之事項），並採取相對應之措施。

b) 持續修正預防個人資料的洩露、遺失以及危害相關流程

c) 申訴與諮詢之回覆

d) 遵守個人資料的蒐集相關法令、準則以及其他相關規範

e) 持續改善個人資料管理系統

f) 代表者的姓名

- 營業單位代表在紀錄個人資料時，須包含以上所述之方針（以電子文件、磁帶或一般人無法用感官方式辨識之方法，以下皆同），並應採取適當之措施，使一般民眾及受雇員工皆能充分瞭解其內容。

85

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

3.3 個人資料保護計畫(1/5)

項目	內容
➢ 3.3.1 個人資料之範疇	✓ 營業單位必須建立與維持相關的程序來識別企業內所有用於商業行為上之個人資料
➢ 3.3.2 法令、準則與其他相關的規範	✓ 營業單位必須建立與維護相關的流程，並遵循法令、準則與基於蒐集個人資料的其他相關規範
➢ 3.3.3 風險的認識、分析與對策	✓ 如個人資料範疇所定義：營業單位為預防將個人資料使用在非預期之目的，必須建立與維護相關流程來採取必要之措施 ✓ 如個人資料範疇所定義：在持有個人資料的部分，營業單位必須建立與維護相關程序以識別及分析相關之風險（包括個人資料洩漏、遺失與危害的可能性、預期對經濟的不利、喪失社會地位等...）並採取相關必要的措施。

86

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3.3 個人資料保護計畫(2/5)

從內部指派可了解並實踐此規範之個人資料保護管理者。並賦予個人資料保護管理系統的執行與運作之責任與管理權限。此執行之管理權限須獨立運作於其他的責任，且須確保該系統可順利執行。

營業代表人須指派相關人員並賦予責任與權限，紀錄於文件內並告知員工。使個人資料保護管理系統能有效率的被執行

3.3.4 資源、職掌、責任與權限

營業單位之代表人須準備所需之資源以建立、實施、維護及改善個人資料保護管理系統

個人資料保護管理者需回報營業代表人其運行之個人資料保護管理系統狀態，包括基本的檢閱與相關的改善方法

87

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

3.3 個人資料保護計畫(3/5)

3.3.5 內部規則：經營單位代表人需具體化內部的規章，將其規章項目文件化，並維護此規章項目，其相關的項目如下列所示：

編號	內容
a)	說明個人資料的流程
b)	相關的規章於個人資料的流程與相關的規定
c)	個人資料風險的認識、分析與對策的流程與相關規定
d)	詳細說明於參考法令、準則與其他相關的規範
e)	個人資料蒐集、利用及提供之相關規定
f)	適切的個人資料保護管理相關規定
g)	本人表達（使用目的的通知與揭露、內容的修正、追加或者刪除、停止或消去使用、拒絕將資料提供給第三方等）相關要求規定
h)	申訴處理之相關規定
i)	個人資料保護之教育訓練規定
j)	個人資料保護之內部查核規定
k)	違反內部規章之相關處罰規定
l)	個人資料保護管理系統的文書管理之相關規定
m)	緊急事項準備及因應措施之相關規定
n)	來自於企業代表人之相關規定之增改

經營單位代表人須修正內部規章以便個人資料管理系統可以根據企業的運作流程正確的運行。

88

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3.3 個人資料保護計畫(4/5)

■ 3.3.6 計畫書

- 營業代表者需製作相關之**教育訓練**、**稽核計畫**並將其文件化以確保個人資料保護管理系統可正確的運行。

89

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

3.3 個人資料保護計畫(5/5)

3.3.7 緊急情事之應變

a) 取得一個方法來處理，當個人資料洩漏、遺失或損害的情況發生時，當事人能很快速地被通知其已洩漏的內容，又或者當事人能夠容易取得訊息內容的方式

b) 盡速公布事實經過、發生原因及因應措施，以避免第二次危害的發生

c) 迅速的回報其發生的案例以及分析相關的機關組織

準備事項於個人資料的洩漏、遺失或損害的部分，營業代表者需建立與維護流程來回應上述項目

營業單位代表者須建立與維護相關流程來詳細說明緊急事項發生時的應方式。營業代表者須建立及維護相關流程，以因應如個人資料的洩漏、遺失或損害而導致經濟損失、喪失社會地位等突發狀況，使企業損失達最小。

90

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3.4 個人資料保護計畫之實施及其運用

3.4.1 運用程序　營業單位代表者需闡明流程於確保個人資料保護管理系統之運作流程

3.4.2 蒐集、利用及提供原則

特定目的

3.4.2.1 蒐集個人資料時，須定義其使用目的，並盡可能僅於特定的範圍內使用。

合法蒐集

3.4.2.2 須使用合法且正當措施蒐集之個人資料

91

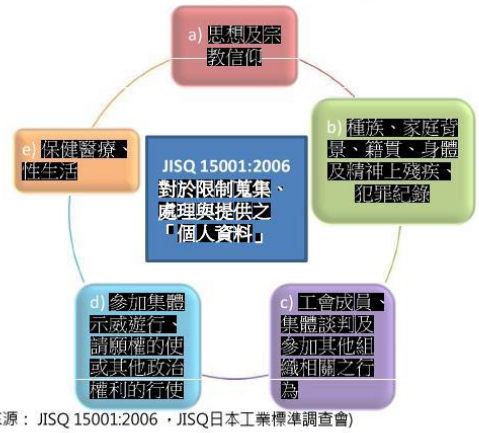
(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

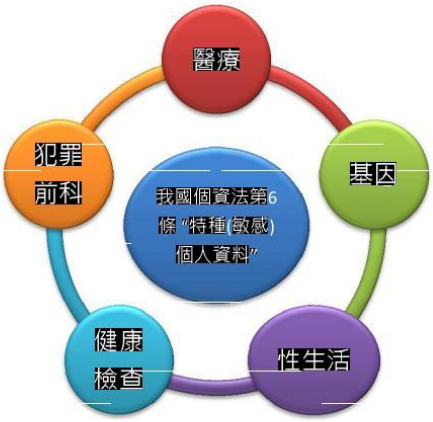
©2012 本文件著作權屬法務部

3.4 個人資料保護計畫之實施及其運用

■ 3.4.2.3 有限制的蒐集、使用以及提供詳細之個人資料

- 營業單位代表者在蒐集、利用或提供個人資料時應取得當事人的允許外，以下(a)～(e)的個人資料內容是不可蒐集、利用或提供的，但符合條款3.4.2.6者，不在此限。
- **(請注意: JISQ 15001:2006 對於限制蒐集、處理與提供之「個人資料」與「我國個人資料保護法」對於「特種(敏感)個人資料 」之定義不同，避免混淆，特此說明)**





92

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3.4 個人資料保護計畫之實施及其運用

3.4.2.4 以書面方式向本人取得個人資料之措施

透過本人書面文件（包括其他以電子文件、磁帶或其他無法透過人體感官識別之方式，以下皆同）蒐集個人資料時，於取得本人同意前，須至少明確告知下列事項。若為保護生命、身體或財產之緊急情況所需及符合條款3.4.2.5(a)～(d)所提及之情況，則無須明確告知及取得同意；若為3.4.2.6(a)～(d)之情況，則無須取得本人同意。

a) 營業單位名稱	b) 資料保護管理人（或代理人）姓名、稱謂、部門及連絡方式	c) 使用目的	d) 是否提供給第三者	e) 說明計畫委託使用個人資料之場合	f) 當3.4.4.4至3.4.4.7所提及之情況下須提供查詢連絡人資訊及回應之影響。	g) 說明提供個人資料或不願意提供個人資料之結果	h) 說明當個人資料蒐集的方式無法經易被辨識時的影響

- 提供給第三者之目的
- 提供的個人資料項目
- 提供的手段或方法
- 提供第三者的資訊或第三者組織種類和屬性
- 說明取得個人資料相關之契約

93

(資料來源：JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

3.4 個人資料保護計畫之實施及其運用

■ 3.4.2.5 以非書面方式向本人取得個人資料之措施

使用3.4.2.4以外之方式蒐集個人資料時，除使用目的已先行公佈及任何右列事項發生外，應立即告知當事人其使用目的或以公開方式進行。

- a) 當公開或告知當事人其使用目的時，可能造成生命財產或其他權利損害時，抑或有心人士或第三者可能對該使用的目的產生興趣時。
- b) 當公佈此使用目的後可能危害企業的權利或法律利益時。
- c) 當蒐集個人資料目的容易被察覺時
- d) 當公務機關或地方公共團體執行法定事務時需要配合之場合；如告知當事人或公開方式將使該事務在執行上有所不便時

94

(資料來源：JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3.4 個人資料保護計畫之實施及其運用

■ 3.4.2.6 利用的相關措施

- 須明確定義個人資料使用之範圍
- 當為達特定目的而超出原目的之範圍外時，除以下四項外，須至少告知3.4.2.4 (a)至(f)之項目及取得當事人之同意：

(a) 基於法律規定之個人資料提供

(b) 為保護個人生命財產，必須利用該個人資料或需耗費過鉅或耗時過久始能取得當事人同意時

(c) 當個人資料的蒐集為特殊需求，用以增進公共衛生與兒童健康成長，且需耗費過鉅或耗時過久始能取得當事人同意時

(d) 當需配合國家機關、地方公共團體或其他受委託單位執行法定事務及取得當事人之同意降造成執行之困難時。

95

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

3.4 個人資料保護計畫之實施及其運用

■ 3.4.2.7 當個人資料的使用接觸到當事人時，除下列情況外應取得當事人同意，且應對當事人告知至少3.4.2.4(a)～(f)所列事項及其蒐集管道與方法

如於蒐集個人資料時，已公布或告知3.4.2.4(a)～(f)所列事項或以上內容，且已取得本人同意時。

隨企業合併或其他原因而承繼之已提供的個人資料，仍使用於承繼前之特定目的範圍內。

當符合3.4.2.5的d)情況時，營業單位可未告知或公布其個人資料蒐集之使用目的而接觸當事人

當部分或全部之個人資料委託於該特定目的之使用範圍內時。

於特定之個人或企業間共用個人資料且當事人已被充分告知至少以下事項時：

- 共用之事項
- 共用之個人資料項目
- 共用者之使用範圍
- 共用者使用之特地目的
- 該負責個人資料管理者之名稱或姓名
- 取得之方法

當符合3.4.2.6 a)～d)所列之事項

96

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3.4 個人資料保護計畫之實施及其運用

- 3.4.2.8 提供的相關措施
- 當提供個人資料於第三者時，除符合以下所列符合以下所列事項外，須事先至少告知當事人3.4.2.4 (a)～(d)事項，且取得當事人之同意。

(a) 對3.4.2.4或3.4.2.7所規定之項目，已至明確告知當事人3.4.2.4 (a)～(d)之事項且取得本人同意時	
(b) 須廣散的提供大量個人資料，且在取得當事人同意上須耗費過鉅或耗時過久時，可以告知當事人或講授相同的替代方案之方式進行右列事項的告知：	•提供給第三者之利用目的 •提供給第三者之個人資料項目 •提供給第三者之管道與方法 •應本人要求刪除可識別當事人之個人資料時，停止提供第三者之相關事項 •取得方法
(c) 包括法人及其他團體幹部及股東相關資料之法人及其他團體資料，或者法定之個人資料，或者本人或法人及其他團體自行公開或提供公開資料時，須預先告知本人上述b)所提及之事項；或置於本人易知悉之狀態	
(d) 特定目的達成之必要範圍內，全部或部分之個人資料委託時	
(e) 隨企業合併或其他原因而繼承的已提供之個人資料，仍使用於繼承前之特定目的範圍內時	
(f) 於特定之個人或企業間共用個人資料且當事人已被充分告知至少右列事項時：	•共用之事項 •共用之個人資料項目 •共用者之使用範圍 •共用者使用之特地目的 •該負責個人資料管理者之名稱或姓名 •取得之方法
(g) 屬3.4.2.6 (a)～(d)所列事項時。	

97

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

3.4 個人資料保護計畫之實施及其運用

- 3.4.3 個人資料之妥善管理

3.4.3.1 正確性之確保
- 營業單位於特定目的達成之必要範圍內，為確保個人資料之正確性，須經常更新其管理方式。

3.4.3.2 安全管理措施
- 營業單位應預防所取得之個人資料遭到洩漏、遺失或毀損之風險，並使用適切之安全管理措施。

3.4.3.3 就業者之監督
- 營業單位對所取得之員工個人資料，須對這些資料做安全管理之風險評估，因此，就業者須對營業單位進行相關必要之監督。

3.4.3.4 委託之監督
- 營業單位委託處理全部或部分之個人資料時，為個人資料之安全管理所需，須對受委託者進行相關必要之監督。

營業單位須於保有個人資料期間，以書面保存個人資料相關之契約

98

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3.4 個人資料保護計畫之實施及其運用

■ 3.4.4 個人資料相關之當事人權利

- 營業單位可利用電腦檢索所建立並依特定之規則整理、分類、篇目、索引的個人資料庫，當事人可要求營業單位公開、內容之修正、增加或刪除、停止利用、刪除或提供於第三者之相關權限(以下稱"明確指示之個人資料")。當事人要求之使用目的告知、公開、內容之修正、增加或刪除、停止利用、刪除或提供於第三者(以下稱"公開相關")時，於3.4.4.4～3.4.4.7規定下，須立即採取相對應之措施。
- 然若有以下所列之情形，則不在此限。

a. • 當事人或第三者之生命財產將會因個人資料被公開而受到危害時。

b. • 公開個人資料將導致助長或誘發不法之行為時。

c. • 公開個人資料將損害國家利益或國與國間之互信關係或將導致國家於國際談判時處於不利之位置。

d. • 公開個人資料將導致在犯罪之預防、鎮壓或搜查等公共安全執行困難時。

99

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

3.4 個人資料保護計畫之實施及其運用

■ 3.4.4.2 公開或其他相關之應對程序

營業單位應將下列事項規範於程序內以處理公開相關事項：

a) 因應公開相關要求之提議

b) 建立要求公開之相關提交文件

c) 公開相關要求者本人或代理人身分確認之方法

d) 3.4.4.4及3.4.4.5情形之手續費(僅限特定場合)收取標準

營業單位須考慮當事人要求之公開相關事項所訂定之程序，避免對當事人負擔過重或造成不便。

營業單位於3.4.4.4及3.4.4.5之情況下因應當事人要求，應依實際情況收取合理之手續費，此手續費之金額並無相關規定。

100

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3.4 個人資料保護計畫之實施及其運用

■ 3.4.4.3 明確指示個人資料的一般認知

a)營業單位之姓名或名稱

b)管理者(或代理人)之姓名、職稱及其連絡方式

c)所有明確指示之個人資料之特定目的。[除3.4.2.5 a)～c)所提之事項外]

d)處理明確指示之個人資料相關之申訴事件

e)營業單位依據個人資料保護相關法律（平成15 年法律第57 号）第三十七條第一項授權者之對象為企業時相關之申訴事件，應諮詢該授權之個人資料保護團體。

f)3.4.4.2之既定手續

營業單位於取得已明確示之個人資料時，在易於接觸到當事人之條件下，應列出上列相關明確指示之事項 。

101

(資料來源： JISQ 15001:2006 ，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

3.4 個人資料保護計畫之實施及其運用

個人資料相關之當事人權益

3.4.4.5明確指示個人資料公開

當營業單位收到當事人自行要求公開可識別當事人之個人資料(包括可明確識別當事人之個人資料仍未存在時)時，應須立即向當事人以書面取得個人資料公開之同意(或其他可取得當事人同意之方法)。然有右列情形時，便無全部或部分公開之必要，且須立即向當事人說明此要旨及理由：

a) 當事人或第三者之生命財產或其他權益將受到損害時

b) 導致營業單位業務之合法性受到阻礙時

c) 違反相關法令時

102

(資料來源： JISQ 15001:2006 ，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3.4 個人資料保護計畫之實施及其運用

個人資料相關之當事人權益

3.4.4.4 明確指示之個人資料使用目的的通知

- 營業者於當事人要求告知對可識別當事人之個人資料的使用目的時，應立即處理。然如發生3.4.2.5所列之(a)～(c)中無須立即告知使用目的之情形時，仍須立即通知並說明當事人無須立即告知之理由。

3.4.4.6 明確指示之個人資料修正、增補及刪除

- 營業單位對於3.4.4.5所述之結果，欲以個人資料不實為由之個人資料修正、增補及刪除(以下稱「訂正事項」)時，在為達特定目的之範圍內，須立即進行必要之調查，並根據該調查結果，對該明確指示之個人資料訂正時及訂正後，須立即告知當事人理由及其影響(包含訂正事項之內容)。

3.4.4.7 明確指示個人資料的利用及提供之否決權

- 當事人可依此條要求營業單位對於可識別之明確指示個人資料利用的停止、刪除或停止提供給第三者(以下簡稱”利用停止等事項”)。並且，在解釋該措施後，須立即向當事人說明。然而於3.4.2.5 (a)～(c)所述之情形時，除無須停止利用亦須立即向當事人說明理由。

103

(資料來源：JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

3.4.5 個人資料保護教育

■ 營業單位須建立與維持對各部門及不同職務階層的所屬員工，依下列事項順序進行定期且適切之教育：

- a) 合適的個人資料保護管理系統之重要性與優點
- b) 為建立合適個人資料保護管理系統所需之職務及相關責任
- c) 違反個人資料保護管理系統時可能遭遇之結果

營業單位須制定、實施及維持教育訓練之計畫與實施、結案報告之審查、計畫之修訂及相關紀錄之保存責任與權限

104

(資料來源：JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

3.5 個人資料保護管理系統文件

3.5.1 文件範圍

營業單位須書面訂定以下個人資料保護管理系統基本及增訂之要點：

a)個人資料保護方針

b)內部規定

c)規格要求事項及營業單位對於個人資料保護管理系統實行上必要之判斷紀錄

d) 計劃書

3.5.2 文件管理

營業單位須訂定、執行及維持全部規格要求之文件管理程序。文件管理之程序須包含以下所列事項：

a) 文件之發行及修改相關事項

b) 確立文件修改訂定之內容、版本數及關連性。

c)有相關文件需求時，易於參照之相關事項 。

3.5.3 記錄管理

營業單位對於個人資料保護管理系統與其規格要求事項之合適性之驗證須製作及維持相關紀錄。

營業單位須訂定、執行及維持相關紀錄蒐集之程序。

105

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

3.6 申訴與諮詢

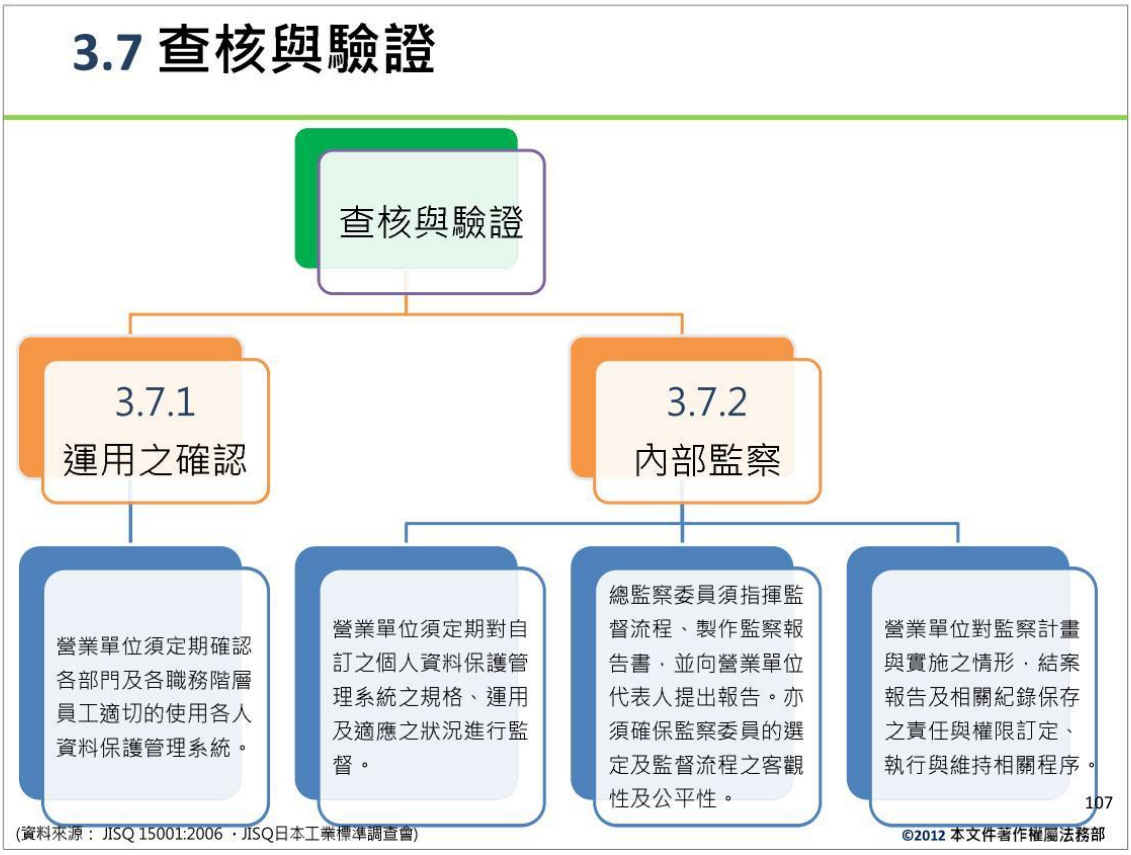
■ 營業單位**必須接受**對於當事人申訴或諮詢有關個人資料之蒐集及個人資料保護管理系統相關事項，並須**給予立即適切之回應**。

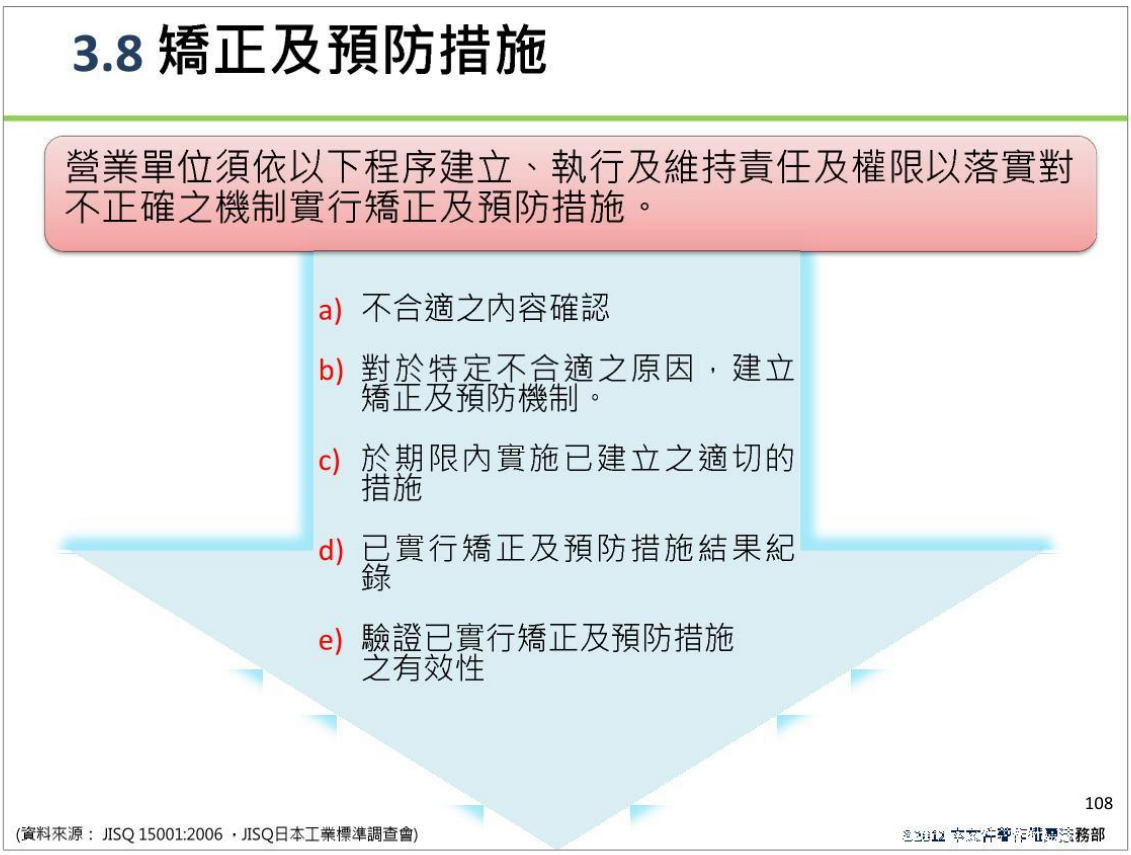
106

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部





本報告之智慧財產權歸屬於法務部

3.9 營業單位代表人之審查機制

營業單位代表人為維持個人資料之保護措施，須定期對個人資料保護管理系統進行評估。下列事項為定期評估之要點：

- a) 內部審查及個人資料保護管理系統運用現況之相關報告
- b) 包括申訴在內之外部意見
- c) 先前已結案之審查相關後續執行之貫徹結果
- d) 個人資料蒐集相關之法令、國家政策方針及其他相關規範修改之現況
- e) 社會情勢、一般認知、技術進步等環境變化
- f) 改善方法之提案

109

(資料來源： JISQ 15001:2006，JISQ日本工業標準調查會)

©2012 本文件著作權屬法務部

問題與討論

資料來源：本計畫撰寫

本報告之智慧財產權歸屬於法務部

（二）個人資料保護執行管理暨考核作業手冊介紹

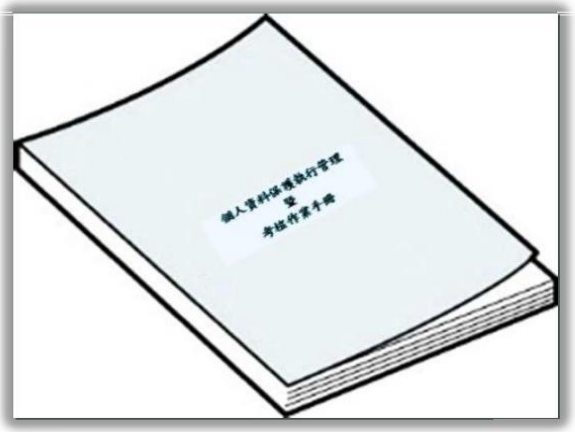
法務部
「99年度公務機關個人資料保護方案」
委辦計畫

個人資料保護執行管理暨考核作業手冊(草案)
介紹

財團法人資訊工業策進會
中華民國 101 年 01 月

大綱

- 目的
- 作業手冊介紹
- Q&A



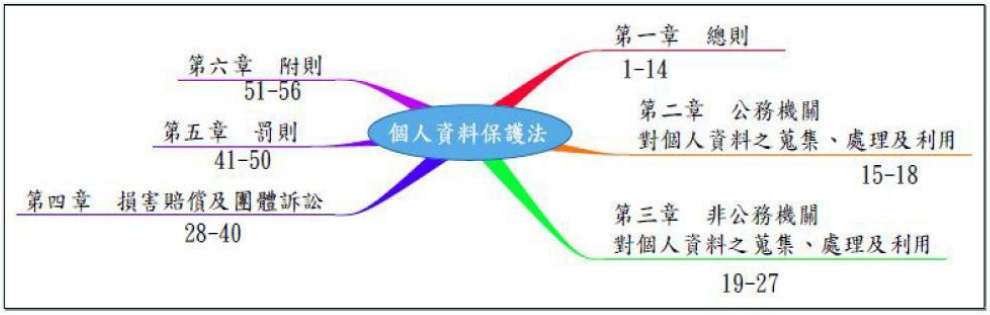
©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

目　　的

©2012 本文件著作權屬法務部

個人資料保護法



- 目的
  - 為規範個人資料之蒐集、處理及利用，
  - 以避免人格權受侵害，
  - 並促進個人資料之合理利用

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

新舊法條對照？(1/2)

	現況	即將面對
何謂個資	僅限電腦處理、足以識別個人的資料。	所有可直接或間接識別個人的任何形式資料。
規範對象	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，以及後來加入的無店面零售業。	所有蒐集、處理及利用個資的公務機關、企業、個人與團體。
個人權利	當事人可針對其個資，提出查詢及請求閱覽、製給複製本、補充或更正、停止電腦處理及利用、刪除等要求。	除左列項目外，亦可要求停止蒐集、處理或利用其個資。
受託者視同委託機關	受委託處理資料之團體或個人，其處理資料之人，視同委託機關之人。	受委託蒐集、處理或利用個人資料者，視同委託機關。
主動告知義務	無規範。	資料蒐集、處理、改變使用目的、異動，或個資遭竊取、洩漏、竄改及其他侵害時，應主動明確告知當事人。

©2012 本文件著作權屬法務部

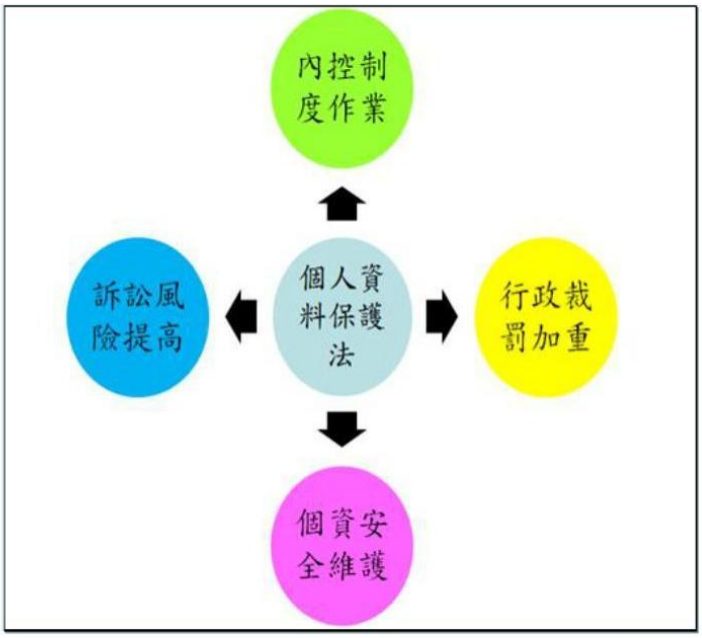
新舊法條對照？(2/2)

	現況	即將面對
團體訴訟	無規範。	符合規定的財團法人或公益社團法人，可為被害民眾提起團體訴訟。
損害賠償	同一事件的損害賠償最高總額為新台幣2,000萬元。	同一事件的損害賠償最高總額為新台幣2億元，若所涉利益超過2億元，則不受此限。
罰則	僅處罰意圖營利而侵害他人個資者。	因違反個資法規定而損害他人者，及意圖營利而侵害個資者，皆會受罰，且刑期與罰鍰增加。非公務機關的代表人、管理人或其他有代表權人，除能證明已盡防止義務，否則應接受相同罰鍰處罰。
無過失責任	公務機關違反本法規定，致當事人權益受損因天災、事變或其他不可抗力所致者，不在此限。	公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
溯及既往	無規範。	非由當事人直接提供的現有資料，必須在新法正式施行後一年內完成告知，逾期未告知而處理或利用者，將視為違法。

©2012 本文件著作權屬法務部

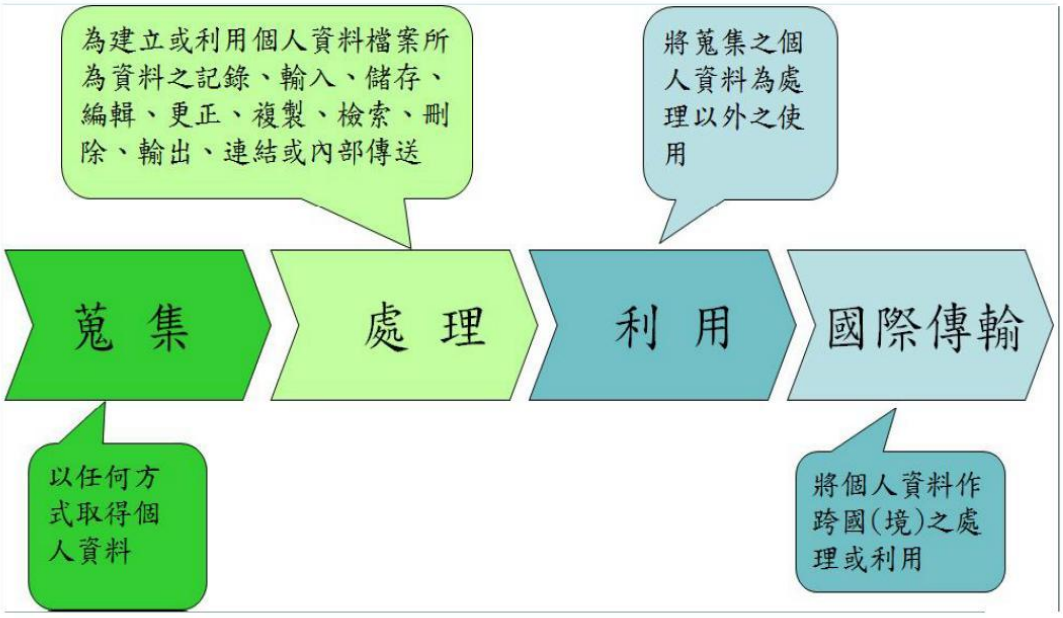
本報告之智慧財產權歸屬於法務部

個人資料保護法對組織之影響



©2012 本文件著作權屬法務部

個資法適用活動範圍



©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

個人資料活動管理重點

©2012 本文件著作權屬法務部

適當安全維護措施

- 成立管理組織，配置相當資源。
- 界定個人資料之範圍。
- 個人資料之風險評估及管理機制。
- 事故之預防、通報及應變機制。
- 個人資料蒐集、處理及利用之內部管理程序。
- 資料安全管理及人員管理。
- 認知宣導及教育訓練。
- 設備安全管理。
- 資料安全稽核機制。
- 必要之使用紀錄、軌跡資料及證據之保存。
- 個人資料安全維護之整體持續改善。

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

個資管理制度之五大挑戰

©2012 本文件著作權屬法務部

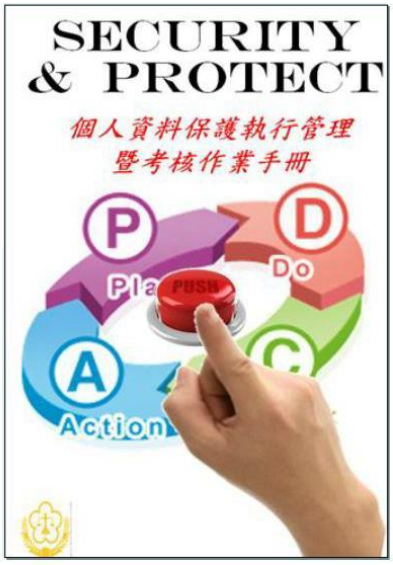
手冊之目的

- 落實憲法保障人民資訊隱私權、資訊科技政策及達到安全、安心與信賴的資訊環境。
- 參考國際上個人資料保護相關標準(BS10012、NIST SP800-122等，但非以此為限)，以系統化的方式說明建置個資保護管理制度之參考步驟。
- 提供政府機關訂定個資保護參考，手冊係屬建議性質，政府機關可參考本手冊，針對資訊系統與所屬資產所需個資保護，就組織特性、業務需求，修正組織所需版本，以符合資安管理要點、個人資料保護法與相關施行細則內容、國際隱私保護原則、個資管理標準之要求。

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

作 業 手 冊 介 紹



©2012 本文件著作權屬法務部

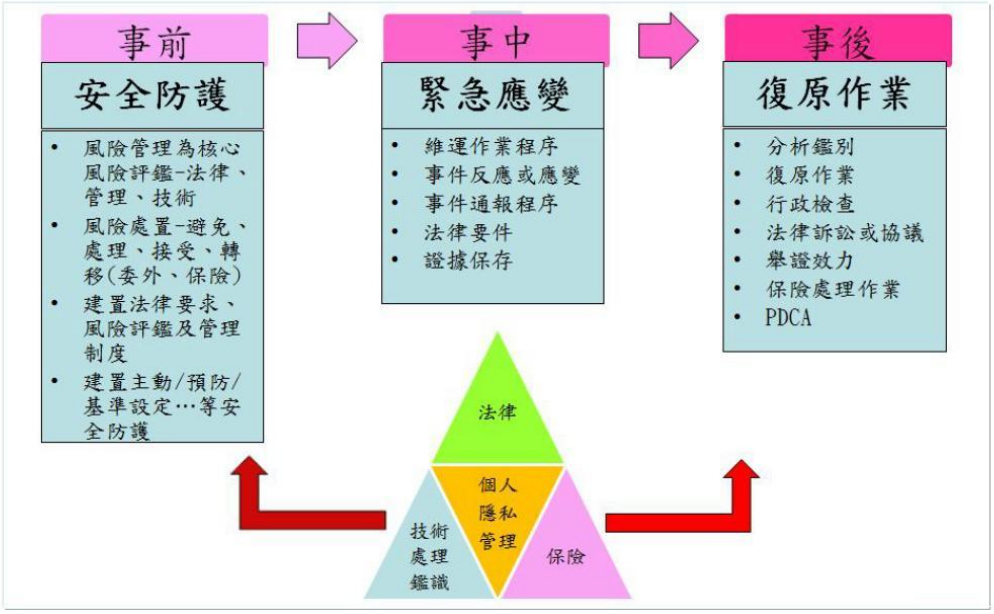
章節架構

- 前言
  - 目的、使用對象、章節架構及使用建議
- 文獻探討
  - 介紹國際上與個資保護相關規範或標準，如APEC隱私保護綱領、OECD隱私保護及個人資料之國際傳遞指導方針、BS 10012 及NIST SP800-122等。
- 個資保護管理建置流程
  - 以定義、規劃、執行及維護等四階段，說明各階段進行的活動(Activity) 項目，並輔以範例解說。
- 結論
- 附件
  - 個資保護系統檢核表、個人資料保護管理要點範本、個人資料保護與隱私政策範本、個資管理整體準備度評估問卷、個資項目衝擊分析檢核表、個資應用系統衝擊分析檢核表、資安事故通報與紀錄表、稽核計畫範本、稽核紀錄範本、個資項目技術安全控制措施基準值評估表、委外作業稽核計畫範本、委外作業稽核紀錄範本、個資認知宣導海報範本、預防與矯正行動方案範本。

©2012 本文件著作權屬法務部

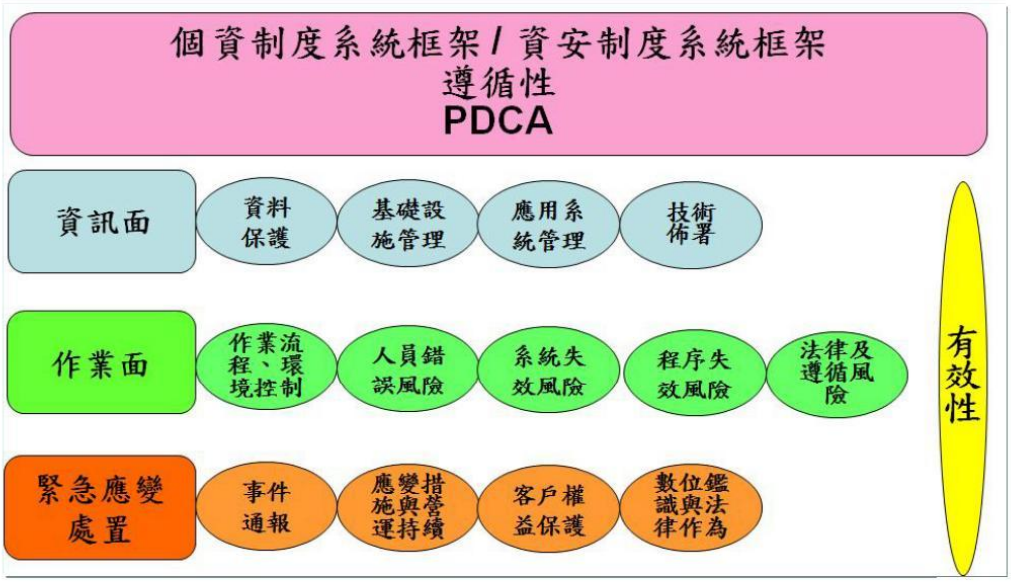
本報告之智慧財產權歸屬於法務部

個資保護管理架構



©2012 本文件著作權屬法務部

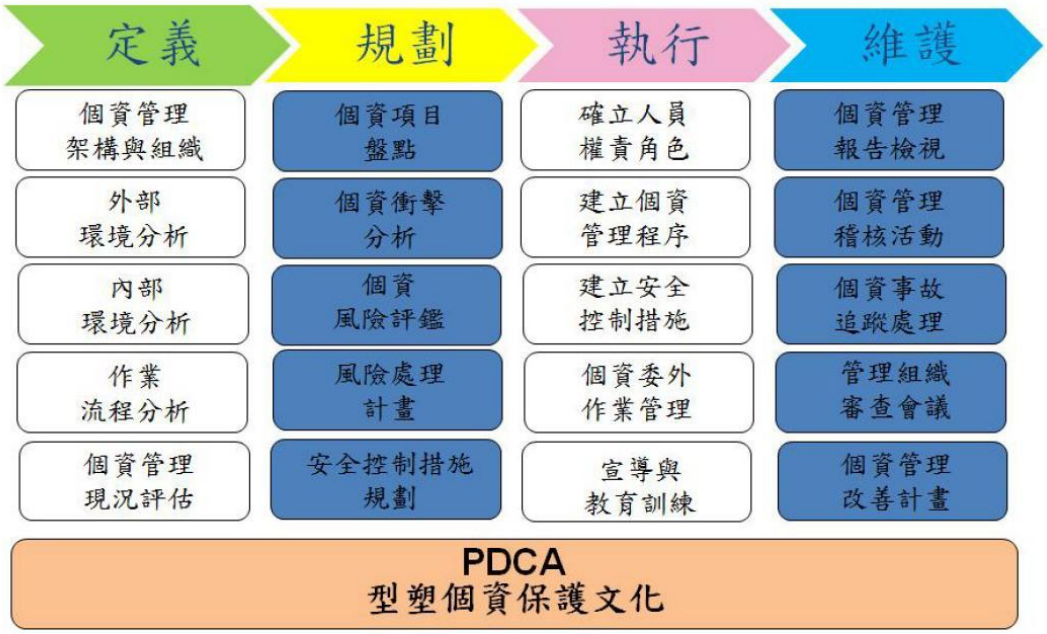
個資保護管理架構規劃



©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

個資保護管理建置流程



©2012 本文件著作權屬法務部

個資保護管理建置流程-定義

個資管理 架構與組織	• 功能性組織架構。 • 人員的角色職責。 • 個資管理政策與要點。
外部 環境分析	• 外部環境對於個資的相關需求。 • 有個資往來活動之外部利害關係人，例如客戶、供應商、委外廠商或人員、合作組織、策略聯盟等。
內部 環境分析	• 識別與分析現行和個資有關的管理制度內容、應用範圍、單位或人員等資訊。 • 彙整個資內外部環境與利害關係人之分析結果，作為各階段範圍的參考。
作業 流程分析	• 建置個資管理的範圍，進行相關作業流程的分析。 • 涵蓋了那些和個資有關之流程或應用系統。
個資管理 現況評估	• 本項為可選擇性之執行活動。 • 對個資管理的現況進行評估，以了解目前在個資管理各領域上準備度較為不足之處。 • 作為未來提比較之參考基準。

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

個資保護管理建置流程-規劃

個資項目盤點	• 盤點個資項目內容，包括個資項目的類別、目的、來源、欄位、數量、型態、相關週期活動、利害關係人等。
個資衝擊分析	• 瞭解個資項目或應用系統所可能面臨到之的弱點與威脅。 • 可能造成組織的衝擊與損失。
個資風險評鑑	• 針對個資項目的機密性、完整性及可用性等構面，進行個資風險評鑑作業。 • 彙整相關個資隱私衝擊分析結果，建立風險因應策略。
風險處理計畫	• 依據風險因應策略、個資風險評鑑報告內容、法令法規的要求、以及組織可運用之相關資源。 • 擬訂可行之個資管理風險處理計畫。 • 符合法令法規對相關個資管理措施的要求。
安全控制措施規劃	• 依據風險處理計畫。 • 個資項目技術控制措施基準值評估表。 • 規劃個資保護技術方案與/或控制方法。

©2012 本文件著作權屬法務部

個資保護管理建置流程-執行

確立人員權責角色	• 依據個資生命週期各階段活動，建立組織人員對應各階段活動的個資存取權責與角色。 • 個資管理程序和安全控制措施的運作基礎。
建立個資管理程序	• 建立組織之個資管理流程與程序，降低風險。
建立安全控制措施	• 建立組織相關個資管理安全控制措施，降低風險。
個資委外作業管理	• 針對個資委外作業，透過相關委外合約規範要求及稽核活動，確保委外作業建立必要的個資管理流程、程序及安全控制措施。
宣導與教育訓練	• 依據個資管理之目標與需求，建立並實施個資管理相關人員訓練計畫。

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

個資保護管理建置流程-維護

個資管理報告檢視	• 運用PDCA機制。 • 定期與不定期檢視個資管理活動與紀錄，或進行趨勢分析。 • 針對未達到目標之項目，適時提出行動方案提升管理成效。
個資管理稽核活動	• 規劃定期與不定期個資管理。 • 個資委外作業活動的稽核。 • 針對稽核發現提出矯正預防行動方案。
個資事故追蹤處理	• 因應個資事故通報與處理回應。 • 數位證據與數位鑑識處理上的需求等。 • 建立相關作業程序與人員職責角色分派，並與組織相關之資安事故程序予以整合運作。
管理組織審查會議	• 針對設定期間個資管理相關重要議題與績效，進行階段性審查，並與相關利害關係人溝通個資管理的成效。 • 對重大計畫或議題進行決策，提供管理活動所需相關資源。
個資管理改善計畫	• 運用PDCA機制，分析並彙整相關可提升個資管理活動的潛在機會點，提出個資管理改善計畫，追蹤檢視執行成果，持續改善提升組織的個資管理系統。

©2012 本文件著作權屬法務部

定義階段-活動與任務

活動與任務	
Activity 0.1: 個資管理組織架構	Task 0.1.1 瞭解組織現行架構(含單位別與功能性)和人員角色職責
	Task 0.1.2 定義個資管理功能性組織
	Task 0.1.3 定義個資管理組織人員角色職責
	Task 0.1.4 建立個資管理政策與要點
	Task 0.1.5 發布個資管理組織架構
Activity 0.2: 外部環境分析	Task 0.2.1 瞭解個資管理相關法令、規範、準則等之遵循需求
	Task 0.2.2 瞭解個資管理相關國際標準、原則等之遵循需求
	Task 0.2.3 外部利害關係人分析
Activity 0.3: 內部環境分析	Task 0.3.1 瞭解現有管理制度內容與應用範圍
	Task 0.3.2 內部利害關係人分析
	Task 0.3.3 分析個資管理涵蓋範圍
	Task 0.3.4 定義組織個資管理導入各階段範圍
Activity 0.4: 作業流程分析	Task 0.4.1 分析服務目錄與服務等級協議
	Task 0.4.2 分析業務作業流程
	Task 0.4.3 分析委外作業流程
	Task 0.4.4 定義和個資相關之流程與應用系統範圍
Activity 0.5: 個資管理現況評估	Task 0.5.1 進行組織個資管理現況評估
	Task 0.5.2 分析個資管理現況評估資料
	Task 0.5.3 產出組織個資管理現況評估分析結果

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

定義階段-相關產出(1/3)

• 個資管理組織與角色職責分工(範例)

組織架角色	人員	工作職掌	任期
管理代表(召集人)	主管或副主管	▪擔任個資與隱私保護之召集人，統籌決策及執行組織資訊安全與個資與隱私保護管理業務之資源整合運用	永久
個資保護專員	組長級以上由主管指派	▪協助管理代表(召集人)推行個資管理	依任命期限
個資保護工作組長	各組組長	▪協助管理代表(召集人)與個資保護專員推行執行個資管理活動	依任命期限
組織同仁	包括個資保護計畫推動範疇內相關同仁	▪落實個資與隱私保護相關作業規範 ▪配合執行或參加個資與隱私保護相關教育訓練	永久
委外廠商與人員	包括個資保護計畫推動範疇內相關委外人員及供應者	▪遵循組織制定之個資保護與隱私政策與相關作業規範 ▪配合組織辦理之個資與隱私保護管理稽核活動	依委外合約期限
稽核小組	由管理代表指派	▪研提年度個資與隱私保護管理稽核計畫 ▪配合年度稽核計畫執行相關稽核活動並提供改善建議事項予管理代表	依任命期限

©2012 本文件著作權屬法務部

定義階段-相關產出(2/3)

作業流程分析(範例)

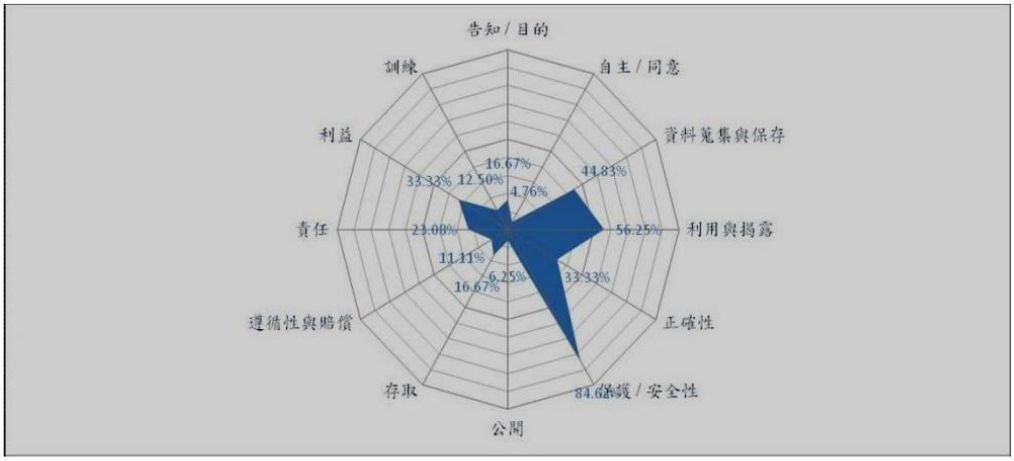
- 資安職能評量運作與題庫建立作業由相關專業人士分工進行，評量運作由資安職能評量小組負責執行，包含命題規範、命題審題及行政試務等業務。
- 命題規範、命題審題作業由資安專家組成團隊進行合作，以建立資安職能評量之題庫
- 辦理訓練之相關作業，包括：場地安排、會場規劃、人力規劃、招生報到作業、教材編印與執行紀錄等

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

定義階段-相關產出(3/3)

- 導入前個資管理整體準備度雷達圖(範例)



©2012 本文件著作權屬法務部

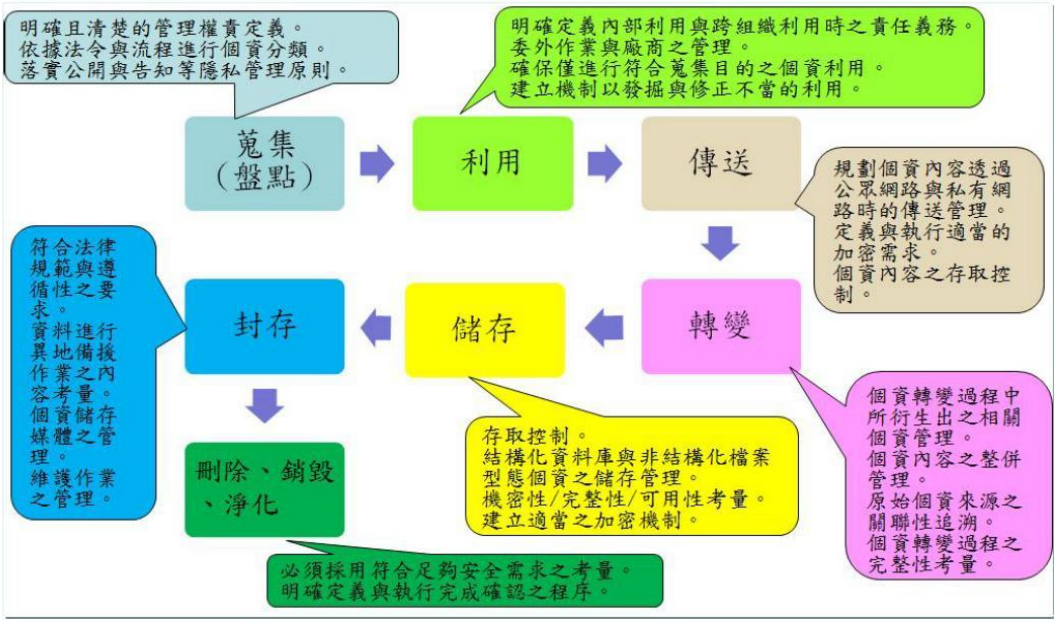
規劃階段-活動與任務

活動與任務	
Activity 1.1: 個資項目盤點	Task 1.1.1 識別不同作業流程之個資項目
	Task 1.1.2 識別個資項目之類別、依據及目的
	Task 1.1.3 識別個資項目相關生命週期活動
	Task 1.1.4 識別個資項目與外部利害關係人之介面
	Task 1.1.5 完成個資項目盤點
Activity 1.2: 隱私衝擊分析	Task 1.2.1 設計隱私衝擊分析檢核表
	Task 1.2.2 進行個資項目隱私衝擊分析
	Task 1.2.3 識別處理個資之關鍵應用系統
	Task 1.2.4 進行個資處理關鍵應用系統隱私衝擊分析
	Task 1.2.5 完成隱私衝擊分析
Activity 1.3: 個資風險評鑑	Task 1.3.1 分析個資項目之個資性與安全控制項目基準值
	Task 1.3.2 分析個資項目弱點與威脅內容
	Task 1.3.3 評估個資項目個資性、弱點及威脅之風險等級
	Task 1.3.4 計算個資項目風險值
	Task 1.3.5 完成個資風險評鑑
Activity 1.4: 風險處理計畫	Task 1.4.1 評估可接受個資項目風險值
	Task 1.4.2 評估風險處理計畫所需資源
	Task 1.4.3 確認可接受風險值
	Task 1.4.4 安排風險處理計畫所需資源
Activity 1.5: 安全控制措施規劃	Task 1.5.1 建立組織安全控制措施原則
	Task 1.5.2 規劃組織安全控制措施
	Task 1.5.3 確認組織安全控制措施規劃內容

©2012 本文件著作權屬法務部

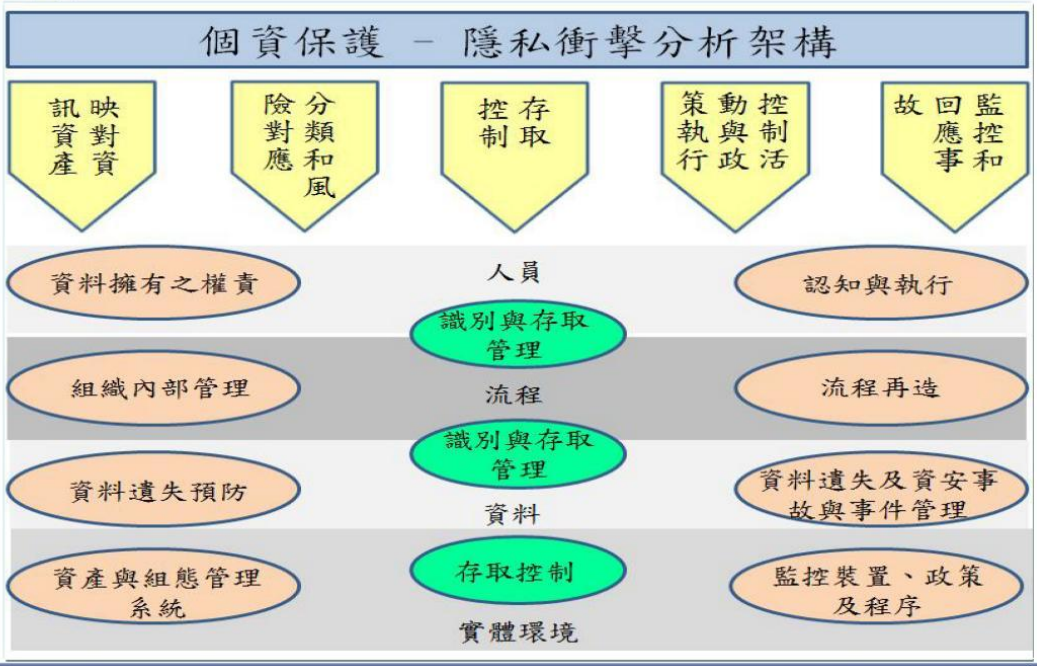
本報告之智慧財產權歸屬於法務部

個資生命週期各階段分類與管理重點



©2012 本文件著作權屬法務部

個資衝擊分析架構



©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

個資風險評鑑

- 瞭解個資項目/應用系統個資性風險等級，並彙整相關個資衝擊分析結果，做為後續擬訂安全控制措施之依據。
- 個資項目/應用系統之個資風險等級基準值
  - 含有個資之類別
    - 洩露不同類別與數量個資時的違法性風險
  - NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定
    - 為技術性控制措施，主要提供以風險為基礎的方法與指導方針，協助保護可識別之個人資料的機密性
  - 「資訊系統分類分級與鑑別機制」影響構面，與個資項目價值對應等級
    - 資訊資產之影響構面等級，進行對個資項目價值之對應
    - 六大影響構面：資料保護受到損害、影響業務運作、影響法律規章遵循、人員傷亡、損害組織信譽及其他

©2012 本文件著作權屬法務部

個資保護技術控制措施建議參考

- ISO 27001 資訊安全管理標準
- NIST SP800-122（個人可識別資訊機密性保護指引）
- NIST SP800-53（安全控制指引）
- 行政院研考會暨技術服務中心之相關資安參考指引

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

SP800-122技術控制措施（1/6）

- 存取控制實施(AC-3)
  - 組織能透過存取控制政策與存取實施機制(如存取控制清單)控制對PII(Personally Identifiable Information)的存取。
  - 實施的方式有很多種，其中之一為執行以角色為基礎(Role-Based)的存取控制並進行設定，如此，每位使用者僅能存取該使用者角色所需的片段資料。另一種作法為僅允許使用者透過應用程式限制使用者對PII的存取，而非允許使用者直接存取包括PII的資料庫或檔案。
  - 對儲存的資訊進行加密也是實施存取控制的選項之一。
  - OMB M-07-16明確指出聯邦機構必須"使用NIST驗證過的加密模組，所有帶有聯邦機構資料的可攜式電腦／設備，除非該資料經由副首長或資深人員以書面形式確認為非敏感級"。

    Office of Management and Budget ,OMB -行政管理和預算局

©2012 本文件著作權屬法務部

SP800-122技術控制措施（2/6）

- 職責分工(AC-5)
  - 組織對於存取PII應強制實施職責分工。例如，將PII資料去識別化的使用者不該也是扮演允許他們去存取需重新識別紀錄資訊。
- 最小權限(AC-6)
  - 組織應強制實施嚴格的權限/特權設定或由所需的使用者(與代表使用者的執行程序)進行存取，以完成指定之作業。關於PII，組織必須確保需存取PII的使用者僅能存取最小的PII數量，以及從事工作任務所需的特權(如讀、寫、執行）。
- 遠端存取(AC-17)
  - 組織可選擇禁止或嚴格限制遠端存取PII。如果允計遠端存取，組織應確保傳輸過程是經過加密。
- 使用者基礎的協同合作與資訊分享(AC-21)
  - 組織可提供自動化機制以協助使用者決定對PII的存取授權是否符合存取限制，例如合約基礎的限制。

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

SP800-122技術控制措施（3/6）

- 行動裝置的存取控制(AC-19)
  - 組織必須選擇禁止或嚴格限制來自於可攜式或行動裝置對PII的存取，如膝上型電腦、行動電話及個人數位助理（PDA），這些設備通常比非可攜式設備(如桌上型電腦)具有較高的風險。有些組織可能選擇限制對含有高衝擊性的PII進行遠端存取，如此，資訊就不會離開實體範圍。如果行動裝置被允許存取，組織需確保裝置被適當的保護，並定期掃描這些裝置以驗證其安全狀態(如使用最新的防惡意程式並啟動、作業系統完整更新）。
- 稽核事件(AU-2)
  - 組織能監控影響PII機密性的事件，如對PII的未授權存取。
- 稽核紀錄的檢視、分析及報告(AU-6)
  - 組織可定期檢視與分析資訊系統稽核紀錄，以發現影響PII的不當或不尋常活動的跡象；調查可疑的活動或可疑的違規；將發現報告給適合的主管並採取適當措施。

©2012 本文件著作權屬法務部

SP800-122技術控制措施（4/6）

- 識別與驗證(鑑別/Authentication)(機關使用者)(IA-2)
  - 使用者於存取PII之前，可被唯一識別與驗證。而驗證機制的強度需求一般而言應視系統與PII的衝擊等級而定。OMB-07-16規定聯邦機關必須”只有在使用雙因子驗證的情況下，始可允許遠端存取。其中一項驗證因子為所使用的設備需從獲得存取的電腦中隔離”。而且”對於遠端存取必項使用暫停功能(time-out)；行動裝置使用者在三十分鐘內沒有動作時，應重新驗證"。
- 媒體存取(MP-2)
  - 組織可限制對包含PII的資訊系統媒體之存取，例如數位媒體(如光碟片、USB隨身碟及磁帶等)與非數位媒體(如文件或縮微膠片)。這當中也包括具有儲存能力的可攜式或行動裝置。

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

SP800-122技術控制措施(5/6)

- 媒體標記(MP-3)
  - 組織可標記包含PII的資訊系統媒體與輸出，以指示該媒體與產出該如何被散佈與處理。只要該媒體或輸出被保存在安全的環境下，這些特定的媒體或輸出可免予標記。至於標記的範例包括標示於列印出來文件的封面或貼標籤於數位媒體上。
- 媒體儲存(MP-4)
  - 組織必須安全地儲存PII，不論是文件與數位媒體，直到該媒體經由適當的設備、技術及程序破壞或加工處理。例如，將儲存於可移動式媒體上的PII進行加密。
- 媒體傳輸(MP-5)
  - 組織對於包含PII的數位／非數位媒體與行動裝置，在組織控制區域之外進行傳輸時，必須加以保護。例如，加密儲存資訊與將媒體鎖定固定的容器內。

©2012 本文件著作權屬法務部

SP800-122技術控制措施(6/6)

- 媒體淨化(MP-6)
  - 組織對於包含PII的數位／非數位媒體於丟棄或釋出再使用之前，應先予以淨化處理。例如，硬碟的消磁處理－使用磁場方式讓硬碟無法使用。
- 傳輸機密性(SC-9)
  - 組織必須保護PII傳輸的機密性。最常使用的方式為通訊加密或傳輸前將資訊加密。
- 靜態資訊的保護(SC-28)
  - 組織必須保護靜態下的PII機密性，所謂靜態資訊意指存於於輔助儲存設備的資訊，如硬碟、磁帶。通常是藉由加密這些儲存資訊來完成。
- 資訊系統監視(SI-4)
  - 組織必須使用自動化工具以監視內部或網路邊界對PII的不尋常／可疑傳輸或事件。例如，使用資料遺失預防技術(DLP)。

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

規劃階段-相關產出(1/6)

- 個資盤點表(範例)

第一部分：流程利害關係人與支援流程分析							
服務目錄或作業流程名稱	利害關係人					支援流程名稱	是否為個資流程(若是則繼續進行第二、三部分)
	客戶/使用者	組織內部	委外	供應者	其他		
資安職能推廣與管理	OOO/政府機關	無	OOO	開發與維護組(開發"公務人員資安訓練管理系統")	無	基礎建設維護流程	資安職能訓練報名表 建立之學員檔案

第二部分：個資流程輸入/輸出與個資項目分析				
服務目錄或個資流程名稱	個資類別		流程輸入 (個資項目文件或檔案名稱)	流程輸出 (個資項目文件或檔案名稱)
	一般個資	特種個資		
資安職能推廣與管理	●		資安職能訓練計畫	資安職能訓練報名表

第三部分：個資流程生命週期管理活動分析							
服務目錄或個資流程名稱	生命週期活動 - 註明與個資項目(物)有關之人/事/時/地						
	蒐集	利用	傳送	轉變	儲存	封存	銷毀
資安職能推廣與管理	●	●	●	●	●	●	●

©2012 本文件著作權屬法務部

規劃階段-相關產出(2/6)

- 個人資料檔案項目彙總表(範例)

個人資料檔案	蒐集保有之特定目的	個人資料類別	個人資料檔案之保有期限	個人資料利用之範圍
資安職能訓練報名表	053教育或訓練行政/093其他中央政府/097其他合於營業登記項目或章程所定業務之需要	C001辨識個人者/C003政府資料中之辨識者	當事人自行維護	組織內/受委託機關
課程講師聯絡資料	053教育或訓練行政/093其他中央政府/097其他合於營業登記項目或章程所定業務之需要	C001辨識個人者/C003政府資料中之辨識者	當事人自行維護	組織內/受委託機關
資安推廣活動報名表	053教育或訓練行政/093其他中央政府/097其他合於營業登記項目或章程所定業務之需要	C001辨識個人者/C003政府資料中之辨識者	當事人自行維護	組織內/受委託機關
課程報名表	053教育或訓練行政/093其他中央政府/097其他合於營業登記項目或章程所定業務之需要	C001辨識個人者/C003政府資料中之辨識者	當事人自行維護	組織內/受委託機關

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

規劃階段-相關產出(3/6)

• 個資項目隱私衝擊分析(範例)

個資項目表單/系統名稱	每年處理之個資數量	每筆個資的欄位數量	資料管理者之角色	角色是否有正當的需求來運用個資	當事人是否要求具有進入其個資之權限	資料不正確時當事人是否能要求修改	個人資料是否定期依據法規檢核、刪除	是否有防制措施，避免個資之意外或不合法的損毀或遺失、修改..等	隱私權保護程序中是否涉及第三方處理？
資安職能訓練報名表	1-500	1-10	個資管控者，部分	不適用	不適用	不適用	否(永久保存，密級)	分享區管理	是(部分)
教育訓練機構建立之學員檔案	1-500	1-10	個資管控者，部分	不適用	不適用	不適用	否(永久保存，密級)	分享區管理	是(部分)
課程講師聯絡資料	1-500 (<20)	1-10	個資管控者，部分	否(被動回應)	不適用	不適用	否(永久保存，密級)	分享區管理	是(部分)
資安推廣活動報名表	500-5,000	1-10	個資管控者，部分	不適用	不適用	不適用	否(永久保存，密級)	分享區管理	是(部分)
課程報名表	500-5,000 (<1,000)	1-10	個資管控者，部分	不適用	不適用	不適用	否(永久保存，密級)	分享區管理	是(部分)

©2012 本文件著作權屬法務部

規劃階段-相關產出(4/6)

• 個資風險等級基準值建議表(範例)

參考項目	個資風險等級		
	普	中	高
含有個資類別	未具有任何個資，或僅含有姓名、公務電話、公務傳真、公務email等公務個資，且公務個資筆數不超過特定筆數(依機關需求自行訂定)	含有一般個資，如姓名、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、教育、職業等「個人資料保護法」定義之個人資料數量在特定筆數(依機關需求自行訂定)以下，或公務個資數量超過特定筆數(依機關需求自行訂定)(含)以上	含有特種個資，如有關醫療、基因、性生活、健康檢查及犯罪前科之個資，或含有一般個資之資料筆數超過特定筆數(依機關需求自行訂定)(含)以上
NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或人員造成有限的傷害(可能輕微影響本機關聲譽、但不會造成任何財務損失或遭受訴訟之情事)	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或人員造成傷害(可能會影響本機關聲譽、財務損失或遭受訴訟，但不至於對本機關業務之持續運作造成重大影響)	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或人員造成重大傷害(非常可能嚴重影響本機關聲譽、重大財務損失或重大訴訟，且可能造成本機關主要業務中止)
「資訊系統分類分級與鑑別機制影響構面與個資項目價值對應	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之安全等級皆為普或安全等級為中者不超過一項	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面的安全等級皆無高，且其中二項安全等級為中	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之安全等級皆為中，或「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之其中一項安全等級為高者

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

規劃階段-相關產出(5/6)

• 個資衝擊評鑑結果(範例)

項次	個資項目名稱	個資風險等級
1	資安職能訓練報名表	中
2	學員檔案	中
3	課程講師聯絡資料	中
4	資安推廣活動報名	中
5	課程報名表	中
6	研討會參與人員到課紀錄統計表(excel)	中
7	報名學生資料	中
8	網路報名資料excel	中
9	得獎者基本資料	中

©2012 本文件著作權屬法務部

規劃階段-相關產出(6/6)

• 個資保護技術性安全控制項目基準值建議(範例)

安全控制(NIST編號)	風險等級所對應之安全控制項目基準值建議		
	普	中	高
存取控制之執行(AC-3)	應建立個資處理授權表、亦應將加密應用於設備、檔案、紀錄、程式、網域等存取活動	依據風險評鑑結果與人員職責應開放必要之最小權限(除可執行之應用程式、系統功能外，亦包含可使用之通訊埠(port)、通訊協定(protocol)及服務(services))；或建議結合職責分工，採用以角色為基礎的存取控制(Role-based access control)機制	應採用DLP與DRM工具，若本項個資均為特種個資，必要時應側錄使用者存取行為，並由指定之高階主管審視或抽核是否有不符合機關資安規範之行為
職責分工(AC-5)	無建議	應依據獨立性原則採用職責分工(separation of duties)，譬如負責系統管理者(如administrator)不應同時負責管理系統日誌(log)	請參閱本控制項基準值為「中」之控制措施
最低限度存取(AC-6)	無建議	請參閱「職責分工(AC-5)」基準值為「中」之控制措施說明	請參閱本控制項基準值為「中」之控制措施
遠端存取(AC-17)	遠端存取管制範圍除與機關之外部連線外，亦包含使用者於機關非使用本機登入	遠端存取應使用加密線路以確保傳輸資料之機密性與完整性	請參閱本控制項基準值為「中」之控制措施
使用者資訊共享(AC-21)	無建議	個資不應儲存於共享資料夾	儲存於資料庫之密碼與機密/特種個資建議採用SHA-1雜湊演算法之輸出值儲存
可攜式行動裝置之存取控制(AC-19)	可攜式行動裝置包含外接儲存設備(如USB隨身碟、外接硬碟)、含有資料儲存功能之可攜式行動運算/通訊設備(如筆記型電腦、PDA、行動電話、數位相機、錄音筆等)	機關應限制可寫入與可攜式媒體之使用(僅授權人員得使用)	請參閱本控制項基準值為「中」之控制措施

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

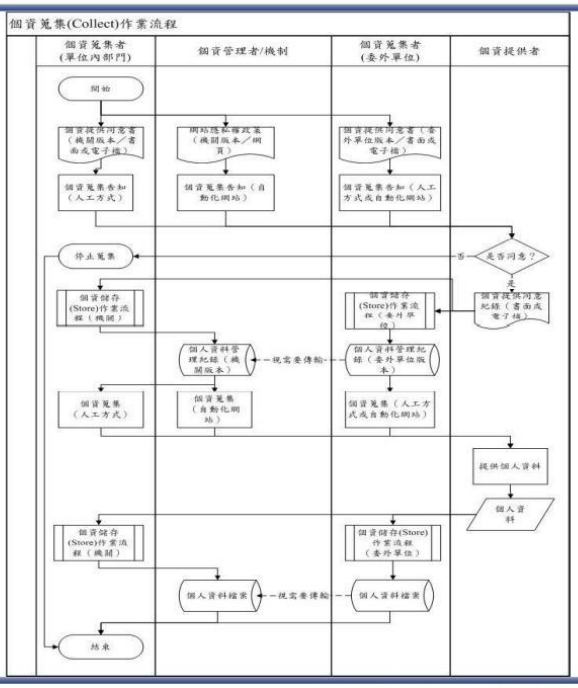
執行階段-活動與任務

活動與任務	
Activity 2.1: 確立人員權責角色	Task 2.1.1 識別個資管理相關人員或群組角色
	Task 2.1.2 建立個資項目生命週期活動與個資管理角色之對應表
	Task 2.1.3 識別對應表內個資管理角色細部權責定義需求
	Task 2.1.4 完成人員權責角色定義
	Task 2.1.5 轉換個資管理人員權責角色定義至相關應用系統權限定義
Activity 2.2: 建立個資管理程序	Task 2.2.1 設計個資蒐集作業流程
	Task 2.2.2 設計個資處理作業流程
	Task 2.2.3 設計個資傳輸作業流程
	Task 2.2.4 設計個資事故管理作業流程
	Task 2.2.5 設計個資管理稽核作業流程
	Task 2.2.6 修訂組織內部管理制度文件
Activity 2.3: 建立安全控制措施	Task 2.3.1 分析個資保護安全控制項目基準值需求
	Task 2.3.2 規劃個人資料生命週期保護構面控制項目行動方案
	Task 2.3.3 規劃整體環境身分識別與存取管理構面控制項目行動方案
	Task 2.3.4 規劃基礎設施網路安全管理構面控制項目行動方案
	Task 2.3.5 建置個資保護安全控制項目行動方案
Activity 2.4: 個資委外作業管理	Task 2.4.1 檢視個資委外作業合約與範圍
	Task 2.4.2 調整個資委外作業合約與工作計畫書內容
	Task 2.4.3 規劃個資委外作業稽核計畫
	Task 2.4.4 執行個資委外作業稽核
Activity 2.5: 宣導與教育訓練	Task 2.5.1 規劃個資認知宣導活動
	Task 2.5.2 規劃個資管理認知與教育訓練計畫
	Task 2.5.3 執行個資管理認知與教育訓練計畫

©2012 本文件著作權屬法務部

執行階段-相關產出(1/3)

- 建立個資管理程序
  -個資蒐集作業流程(範例)



©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

執行階段-相關產出(2/3)

- 個資項目技術控制措施基準值評估表(範例)

No	Checkbox			Level	Control	Note
	Yes	No	N/A			
技術控制措施類別(1)存取控制之執行						
1		V		普	是否已建立個資處理授權表	包括加密應用於設備、檔案、紀錄、程式、網域等存取活動
技術控制措施類別(2)職責分工						
10		V		中	是否已依據獨立性原則採用職責分工	例如負責系統管理者不應同時負責管理系統日誌(log)
技術控制措施類別(3)最低限度存取						
15		V		中	「職責分工」Level等級中之內容是否完全符合	
技術控制措施類別(4)遠端存取						
17			V	中	本機關是否已建立遠端存取之自動監控措施	確保從遠端連線至本機關資訊系統之活動，均符合本機關所訂定之遠端存取政策
技術控制措施類別(5)使用者資訊共享						
22	V			中	權限是否已依據個人、組別、組織等層級進行功能分類與授權	例如限制讀取、寫入、刪除、執行、列印等
技術控制措施類別(6)可攜式行動裝置之存取控制						
27	V			普	可攜式行動裝置，若連接至本機關內部網路與資訊系統時，是否已經過授權始可使用	可攜式行動裝置包含外接儲存設備(如USB隨身碟、外接硬碟)、含有資料儲存功能之可攜式行動運算/通訊設備(如筆記型電腦、PDA、行動電話、數位相機、錄音筆等)

©2012 本文件著作權屬法務部

執行階段-相關產出(3/3)

- 年度個資管理認知與訓練計畫表(範例)

課程類別	課程名稱	學分數	實施頻率	參加對象		
				主管人員	個資管理專責人員	一般同仁
認知	個資管理基礎認知課程	1.5	每年	O	O	O
認知	個資法令規範充電課程	1.5	每半年	O	O	O
一般訓練	個資(蒐集)生命週期作業流程說明	1	每年	O	O	O
一般訓練	個資(利用與處理)生命週期作業流程說明	1	每年	O	O	O
一般訓練	個資(蒐集)生命週期技術措施說明	1	每年		視需要	視需要
一般訓練	個資(利用與處理)生命週期技術措施說明	1	每年		視需要	視需要
專業訓練	個資流程與項目盤點實務課程	1	每年		O	
專業訓練	個資衝擊分析實務課程	1	每年		O	
專業訓練	個資衝擊評鑑實務課程	1	每年		O	
專業訓練	DLP(XX)技術課程	1	每年		視需要	

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

維護階段-活動與任務

活動與任務	
Activity 3.1: 個資管理報告檢視	Task 3.1.1 彙整前一檢視週期個資事故紀錄
	Task 3.1.2 彙整前一檢視週期個資流程管理紀錄
	Task 3.1.3 彙整前一檢視週期個資保護安全控制項目管理紀錄
	Task 3.1.4 彙整前一檢視週期個資管理認知與教育訓練計畫執行紀錄
	Task 3.1.5 進行個資管理預期目標與實值之差異分析
	Task 3.1.6 研擬差異項目之預防與矯正行動方案建議
Activity 3.2: 個資管理稽核活動	Task 3.2.1 安排個資管理內部稽核人員與職責分工
	Task 3.2.2 規劃個資管理內部稽核計畫
	Task 3.2.3 核可與通知個資管理內部稽核計畫
	Task 3.2.4 執行個資管理內部稽核
	Task 3.2.5 完成個資管理內部稽核報告
Activity 3.3: 個資事故追蹤處理	Task 3.3.1 個資事故識別與登錄
	Task 3.3.2 進行個資事故範圍控制與調查
	Task 3.3.3 進行個資事故通報
	Task 3.3.4 擬定個資管理新增控制措施建議
	Task 3.3.5 完成個資事故結案
Activity 3.4: 管理組織審查會議	Task 3.4.1 彙整外部最新個資相關法令規範內容
	Task 3.4.2 彙整個資管理預防與矯正行動方案
	Task 3.4.3 彙整個資事故追蹤處理結果
	Task 3.4.4 彙整內部與個資委外作業稽核結果
	Task 3.4.5 舉行管理組織審查會議
Activity 3.5: 個資管理改善計畫	Task 3.5.1 安排個資管理改善計畫相關人力與資源
	Task 3.5.2 執行個資管理改善計畫
	Task 3.5.3 檢視個資管理改善計畫執行結果

©2012 本文件著作權屬法務部

維護階段-相關產出(1/3)

- 稽核計畫(範例)

機關名稱	*{OO 機關}*				
考評單位名稱	*{OO 機關}*				
計 畫 名 稱	*{OOO 年度 第O次OOOO 個資考評作業稽核計畫}*				
擬 定 部 門		負責人		日 期	

1.稽核目的

為瞭解*{OO 機關}*對於*{考評機關名稱}*個人資料作業之保護與管理活動執行情形，依據本機關*{OO 外部查核作業程序規定}*執行查核，以確保*{OO 機關}*落實本機關對個人資料檔案相關保護措施之要求。本計畫將採獨立查核方式，判斷相關保護措施的控制目標、方法、流程及程序是否符合*{中華民國個人資料保護法}*、*{OO 機關個人資料管理規定}*、*{OOOOO 標準}*之要求。

2.作業方式

依據*{ OO 查核管理規定 }*，自*{日期}*至*{日期}*為止之書面或電子資料為本次稽核樣本之母體。本次稽核將採用書面與實地查核方式進行。

3.稽核依據

{中華民國個人資料保護法}、*{OO 機關個人資料管理規定}*、*{OOOOO 標準}*。

4.稽核範圍

本次執行之稽核範圍包含*{OO 機關所屬 OO 科、OO 室、OO 中心、OO 股...}*之個人資料蒐集、處理及利用等相關流程。

5.稽核時程規劃

詳見 7.稽核時程規劃表。

6.注意事項

{略...}。

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

維護階段-相關產出(2/3)

- 個資事故通報與紀錄表(範例)

機關名稱				表單編號	
提出單位		提出人員		提出日期	
處理單位		處理人員		處理日期	

處理過程紀錄

個資事故識別與紀錄
?個資事故發生與發現之日期與時間：
?遭受揭露之個資範圍與數量：
?遭受揭露個資之儲存媒體：
個資事故評鑑與分類
?影響範圍(包含系統、人員、組織)：
?可能影響之當事人範圍與人數：
個資事故通報與應變
?是否需(或已)通報主管機關、執法單位或媒體：
?是否需向社會大眾公告：
?通知個資事故當事人之通報對象、內容、方式及時機：
個資事故診斷與調查
?個資事故相關採證程序之紀錄、證據保存方式及負責人員：
?個資事故根因分析結果：

矯正與預防行動方案			
?個資事故之新增控制措施(以避免已遭受揭露之個資遭到再次揭露)：			
預計方案完成日期		負責人員	
實際方案完成日期		追蹤人員	
覆核主管		覆核日期	

©2012 本文件著作權屬法務部

維護階段-相關產出(3/3)

- 預防與矯正行動方案(範例)

機關名稱				表單編號	
提出單位		提出人員		提出日期	
處理單位		處理人員		處理日期	

說明

不符合事項/問題來源與說明
根本原因分析
矯正與預防措施說明

預計改善完成日期		負責人員	
實際改善完成日期		追蹤人員	
覆核主管		覆核日期	

©2012 本文件著作權屬法務部

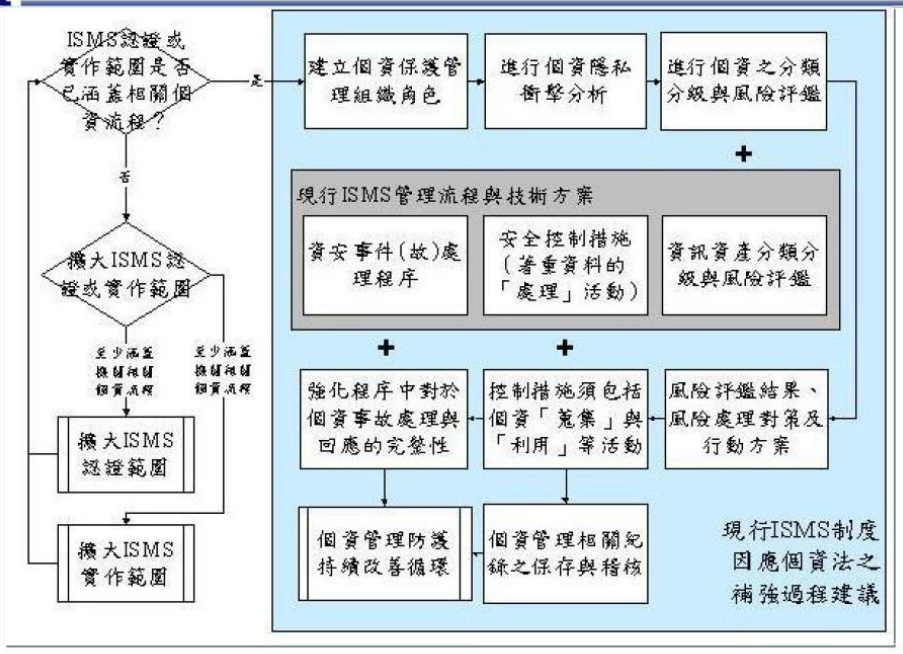
本報告之智慧財產權歸屬於法務部

個資保護管理建置-點線面

- 3點
  - 進行個資流程與個資項目盤點
  - 分析個資風險評鑑威脅與弱點
  - 設定流程技術控制措施基準點
- 2線
  - 內線：組織內部個資管理防線
  - 外線：作業委外個資管理防線
- 1面
  - 個資與資訊安全管理及PDCA合而為同一面

©2012 本文件著作權屬法務部

ISMS與個資保護導入之整合



©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

個資外洩處理原則

- 民眾
  - 建議，依個人資料保護法規定，可舉證損害具體求償，知悉後的兩年內聲請國賠。
  - 遇個人資料遭外洩處理方式
    - 保全證據
    - 舉證損害
    - 立即向外洩資料單位反映，並可請求損害賠償。
    - 若該單位未妥善處理，可透過司法途徑解決。
- 公務單位
  - 遭民眾抱怨申訴時或媒體揭露報導時，應該怎麼處理 ？
  - 媒體採訪時，應如何應對 ？

©2012 本文件著作權屬法務部

個資事件/故應變

- 結合現有國家資通安全應變機制、公務機關事件分級之通報與處理。
- 整合組織單一事件/故通報與處理程序
  - 如增列個資外洩類別
- 考量個資法之要求
  - 如查明後通知當事人之方式
- 定期演練測試
- 注意委外作業之通報與處理程序之一致性
- 處置態度
  - 危機處理

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

應變應有之步驟程序

事前	事中	事後
準備	偵測與分析 減緩與復原	事後處置
• 建立組織 • 建立通報與應變機制 • 建立應變程序 • 事件通知程序-當事人、媒體及內部人員 • 定期演練機制 • 結合軌跡資料之留存 • 啟動必要之系統日誌 • 記錄個資存取活動 • 分析可疑事件	• 評估、調查判斷發生來源 • 決定優先處理順序 • 判斷影響範圍 • 鑑識分析及證據留存 • 調查結果確認 • 避免個資事故擴大 • 確保個資事故與處理後，個資之完整性 • 依法通報個資當事人	• 持續觀測 • 提出個資事故報告 • 召開事件檢討會議 • 應變計畫維護 • PDCA • 準備後續可能法律程序

©2012 本文件著作權屬法務部

應變重點-溝通與協商

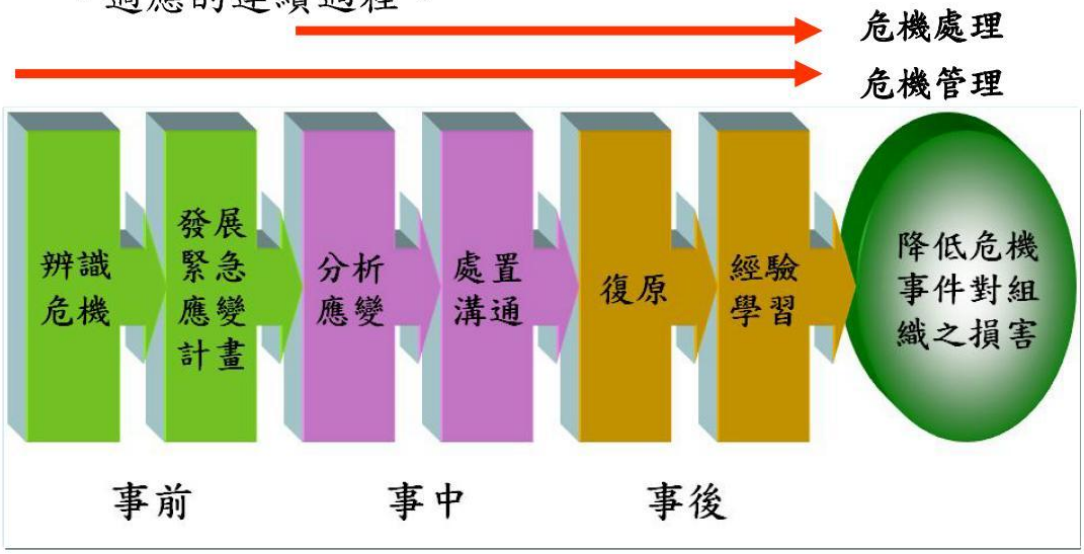
- 目的:
  提升對組織的信任
- 作法（對外溝通原則）:
  - 掌握溝通目的與底線
  - 了解溝通對象，慎訂溝通策略
  - 儘早、主動溝通
  - 善用多元溝通管道
  - 態度真誠、坦白與公開
  - 傾聽民眾關切的重點
  - 滿足媒體的需要
- 作法（對內溝通原則）:
  - 上對下要做個資政策的宣達
  - 下對上要做個資風險發現的報告
  - 單位之間要分享處理經驗

©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

危機管理

- 是組織從因應危機至危機解除、復原的一個不斷學習、適應的連續過程。



©2012 本文件著作權屬法務部

危機處理作業基準

- 「行政院所屬各機關風險管理及危機處理作業基準」--危機處理專章。

危機處理應與風險管理架構相呼應，並預為規劃預防、應變與復原措施。

應針對危機事件訂定緊急應變計畫，並透過測試演練，驗證有效性。

各部會應強化危機處理整體概念及內外部協調整合機制。

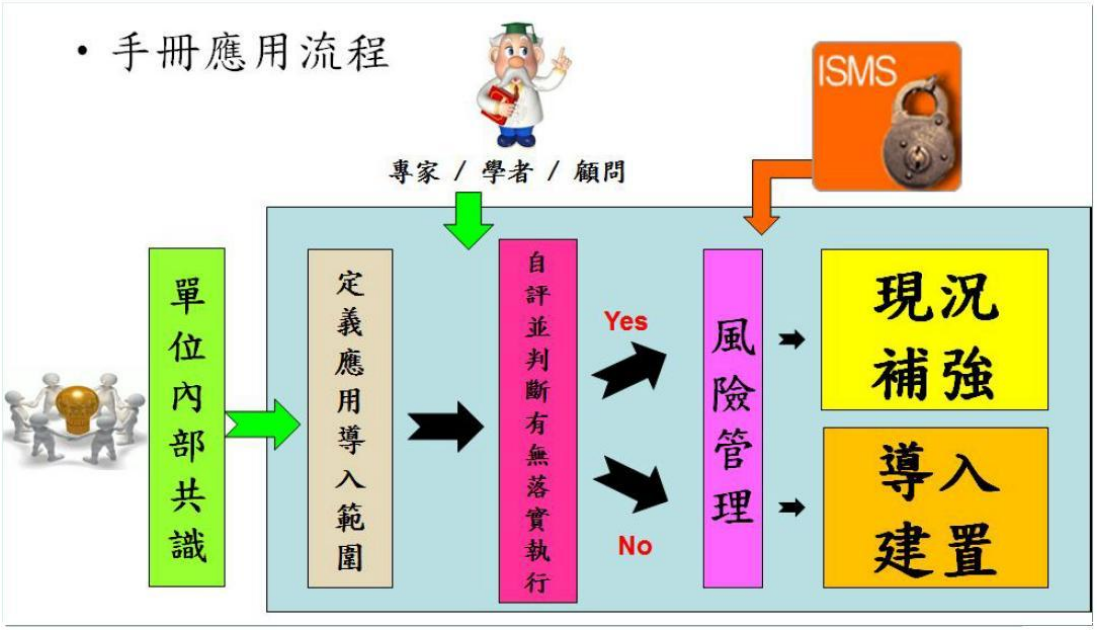
各部會應適時成立危機應變小組或陳報上級成立跨部會小組，爭取第一時間解決。

各部會應透過處理案例持續學習及檢討改進。

©2012 本文件著作權屬法務部

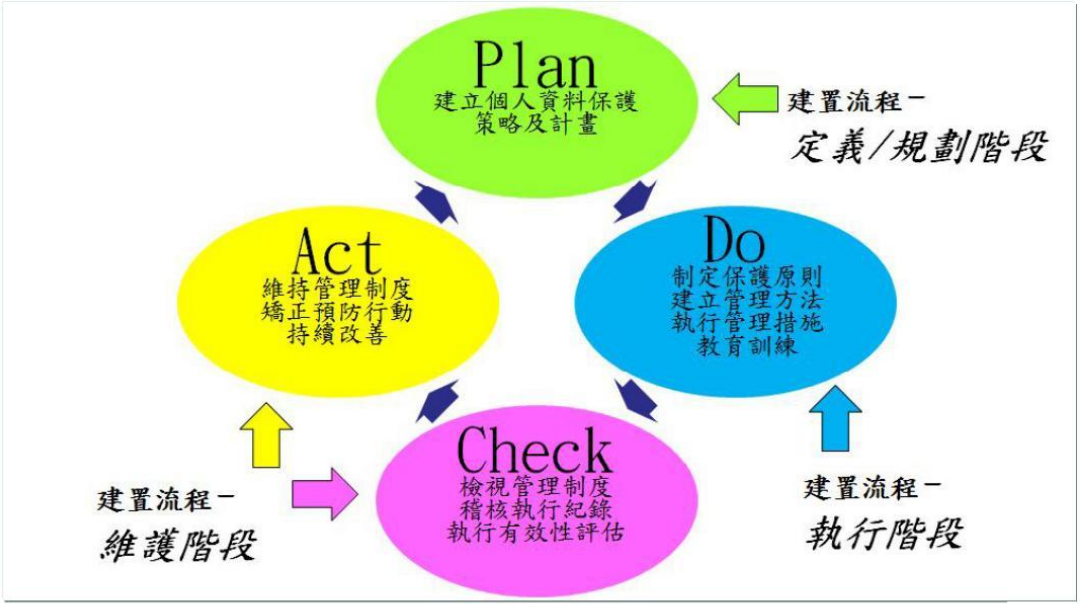
本報告之智慧財產權歸屬於法務部

個人資料保護管理制度



©2012 本文件著作權屬法務部

個人資料保護之PDCA架構



©2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

結論

- 個資保護管理建置流程
  - 提供組織於導入個資保護系統之參考，因而發展出一套適用於各組織面對個資法實施時，如何建立組織內個資管理機制之參考步驟。
- 個資保護管理建置流程分為定義、規劃、執行及維護等四個階段
  - 各階段分別有不同的活動(Activity)進行，例如個資管理組織架構、個資項目盤點、個資隱私衝擊分析與風險評鑑、個資管理流程及技術控制措施建立等。
  - 各項活動中又有許多任務(Task)需要執行。
  - 過程中可能需要各種不同資訊的提供，再輔以各種執行手法與相關工具，完成該項任務。
  - 任務如有產出將可能成為其他任務或活動執行時所需參考之資訊。

©2012 本文件著作權屬法務部

問題與討論

報告完畢

敬請指教

策進資訊科技之創新應用，協助發展知識經濟
推廣資訊技術有效應用，促進資訊社會之健全發展
建構數位經濟發展環境，帶動資訊產業之永續成長

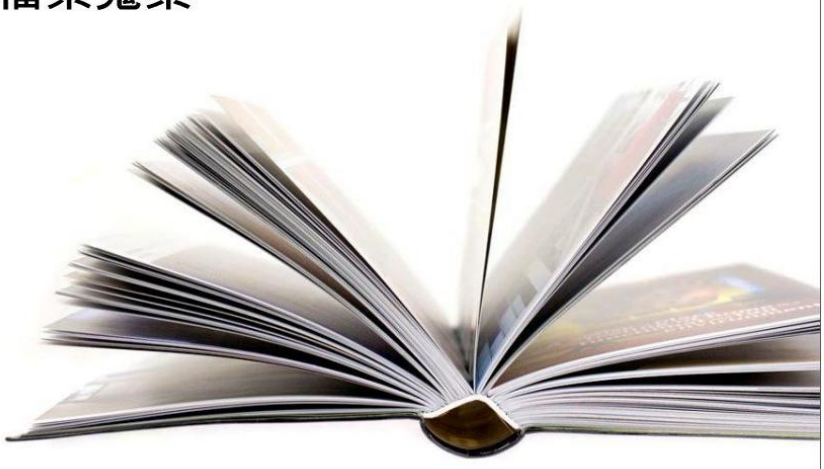
資料來源：本計畫撰寫

本報告之智慧財產權歸屬於法務部

三、進階公務機關個資保護專責人員培訓教材

本報告之智慧財產權歸屬於法務部

個人資料檔案蒐集



為何要蒐集「個人資料檔案清冊」

本報告之智慧財產權歸屬於法務部

那「個人資料檔案清冊」的概念從哪來？

- ISO27001資訊安全管理系統(資料來源：BSI英國標準協會)
  - A.7.1.1 資訊資產
    - 宜明確識別所有資產，並製作與維持所有重要資產的清冊。
- BS10012個人資訊管理系統(資料來源：BSI英國標準協會)
  - 4.2 辨識及記錄個人資訊的使用情況
    - 組織應維護一份個人資訊分類清冊。
    - 清冊亦應記錄各類個人資訊之使用目的。
    - 組織應記錄個人資訊在組織中之流向。
- TPIPAS臺灣個人資料保護與管理制度
  - 4.4.2 納入管理之個人資料範圍
    - 事業應識別其保有之個人資料，劃定其納入個人資料管理制度之範圍並建立清冊。
- JISQ15001個人情報保護(資料來源：JISQ日本工業標準調查會)
  - 3.3.1 特定的個人資料
    - 營業單位必須建立與維持相關的程序來識別企業內所有用於商業行為上之個人資料。

2012 本文件著作權屬法務部

個資法有說要做「個人資料檔案清冊」嗎？

- 當然沒有
- 那為什麼要做？
  - 雖然個資法沒講，但第18條有規定，讓盤點個人資料成為保護個資的第一步

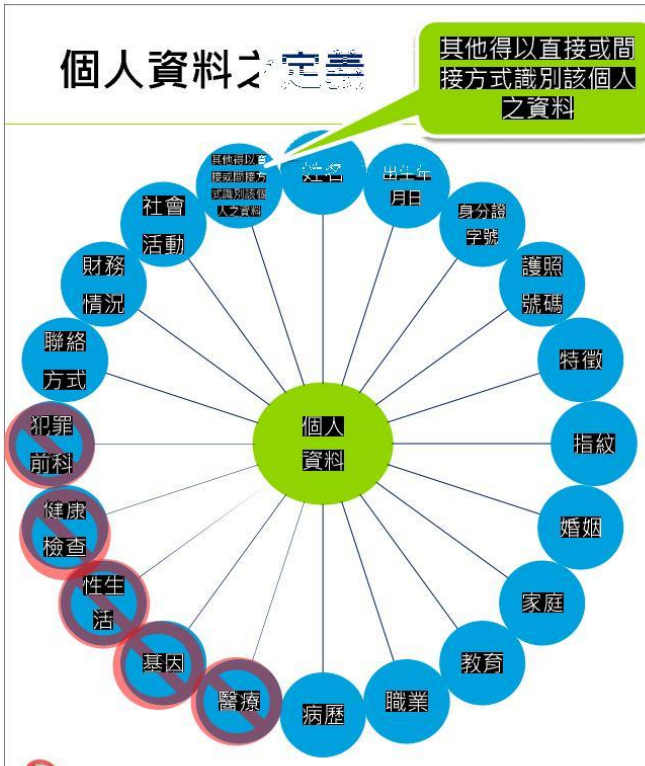
    §18 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- 不做會怎麼？
  - 沒識別到=沒管理
    - 造成個人資料控管實施的缺口
    - 可能無法於法定的規定時間內完整回覆行使權利的當事人

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

甚麼是「個人資料」

個人資料之定義



個資法第六條，原則上不得蒐集、處理、利用。

P.8

與個人資料相關的活動

- **蒐集**　指以任何方式取得個人資料(包含直接或間接)
- **處理**　指為建立或利用個人資料檔案[註]所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送
- **利用**　指將蒐集之個人資料為處理以外之使用
- **國際傳輸**　指將個人資料作跨國(境)之處理或利用

注意：個人資料檔案係指依系統建立之個人資料，指為一定期間持有目的，經有組織之整理，可分類檢索且為有意義集合之個人資料。

8

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

電腦處理個人資料保護法之個人資料類別說明

附件二

電腦處理個人資料保護法之個人資料類別

法務部　　中華民國八十五年八月七日法八五令字第一九七四五號
財政部　　台財稅字第八五二〇七八七二二號
經濟部　　經（八五）商字第八五〇二一六一五號
教育部　　台（八五）人（五）字第八五五一四九一〇號令發布
交通部　　交資八十五字第〇四八九八號
行政院新聞局　（八五）閩治字第一〇六九四號
行政院衛生署　衛署資訊字第八五〇五八九〇一號

代　號　識別類：
C〇〇一　辨識個人者。
例如：姓名、職稱、住址、工作地址、以前地址、住家電話號碼、相片、指紋、電子郵遞地址及其他任何可辨識資料本人者等。
C〇〇二　辨識財務者。
例如：銀行帳戶之號碼與姓名、信用卡或簽帳卡之號碼、個人之其他號碼或帳戶等。
C〇〇三　政府資料中之辨識者。
例如：身分證統一編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等。
代　號　特徵類：
C〇一一　個人描述。
例如：年齡、性別、出生年月日、出生地、國籍等。
C〇一二　身體描述。
例如：身高、體重、血型等。
C〇一三　習慣。
例如：抽煙、喝酒等。
C〇一四　個性。
例如：個性等之評述意見。
代　號　家庭情形：
C〇二一　家庭情形。
例如：結婚有無、配偶或同居人之姓名、前配偶或同居人之姓名、結婚之日期、子女之人數等。
C〇二二　婚姻之歷史。
例如：前次婚姻或同居、離婚或分居等細節及相關人之姓名等。
C〇二三　家庭其他成員之細節。
例如：子女、受扶養人、家庭其他成員或親屬、父母等。
C〇二四　其他社會關係。
例如：朋友、同事及其他除家庭以外之關係等。
代　號　社會情況：
C〇三一　住家及設施。
例如：住所地址、設備之種類、所有或承租、住用之期間、租金或稅率及其他花費在房屋上之支出、房屋之種類、價值及所有人之姓名等。
C〇三二　財產。
例如：所有或具有其他權利之動產或不動產等。
C〇三三　移民情形。
例如：護照、工作許可文件、住居或移行限制、入境之條件及其他相關細節等。
C〇三四　旅行及其他遷徙細節。
例如：過去之遷徙、旅行細節、外國護照及工作證照及工作證等相關細節等。
C〇三五　休閒活動及興趣。
例如：嗜好、運動及其他興趣等。
C〇三六　生活格調。
例如：使用消費品之種類及服務之細節、個人或家庭之消費模式等。
C〇三七　慈善機構或其他團體之會員資格。
例如：俱樂部或其他志願團體或持有參與者紀錄之單位等。
C〇三八　職業。
例如：學校校長、民意代表或其他各種職業等。
C〇三九　執照或其他許可。
例如：駕駛執照、行車執照、自衛槍枝使用執照、釣魚執照等。
C〇四〇　意外或其他事故及有關情形。

P.9　　2012 本文件著作權屬法務部

個人資料說明(1/2)

這些都是個人資料喔!

類別	內容
特徵	年齡、性別、出生地、國籍、身高、體重、血型、抽煙、喝酒等。
婚姻	婚姻之歷史：前次婚姻或同居、離婚或分居等細節及相關人之姓名等。
	家庭其他成員之細節：子女、受扶養人、家庭其他成員或親屬、父母等。
家庭	是否有結婚、配偶或同居人之姓名、前配偶或同居人之姓名、結婚之日期、子女之人數等。
教育	學校紀錄：大學、專科或其他學校等。
	學生紀錄：學習過程、相關資格、考試成績或其他學習紀錄等。
職業	現行之受僱情形、離職經過、工作經驗、工作紀錄。
病歷	依醫療法(第六十七條)所定之病歷應包括下列各款之資料： 一、醫師依醫師法執行業務所製作之病歷。 二、各項檢查、檢驗報告資料。 三、其他各類醫事人員執行業務所製作之紀錄。 (此部分尚未確定)
聯絡方式	傳統的聯絡方式：電話、地址。
	時尚的聯絡方式： Email、MSN、SKYPE、FaceBook、微博等。
	其他的聯絡方式：個人部落格、批踢踢(PTT)的帳號、Mobile01的帳號等。

P.10　　2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

個人資料說明(2/2)

這些都是個人資料喔!

類別	內容
財務情況	帳戶之號碼與姓名、信用卡或簽帳卡之號碼、收入、所得、資產、投資、銀行、負債、支出、信用評等、貸款、結匯紀錄、票據信用、津貼、福利、贈款等。
社會活動	移民情形、旅行及其他遷徙細節、休閒活動及興趣等。
醫療	指以治療、矯正或預防人體疾病、傷害、殘缺為目的 ，所為的診察、診斷及治療或基於診察、診斷結果，以治療為目的，所為的處方、用藥、施術或處置等行為全部或一部之總稱。(此部分尚未確定)
基因	指人體之染色體所儲存超過十萬對以上最基本而具有全部遺傳特質或特定生物功能DNA(去氧核醣核酸)之遺傳單位。
性生活	指所有與性行為有關之活動之總稱，如性傾向、性慣行等。
健康檢查	指以檢驗為目的所為一般性或遺傳性、傳染性、精神性等疾病檢查之健康資料之總稱，如健康檢查報告等。
犯罪前科	指經法院判定有罪確定者。

2012 本文件著作權屬法務部

一直有聽說個人資料的生命週期，那是什麼？

■ 就是...

■ 作什麼用？

- ◆ 檢視組織使用個資之業務流程
- ◆ 得以完整盤點個人資料檔案
- ◆ 作為安全管控設計基礎
- ◆ 作為舉證證物之一
- ◆ 便於行使當事人權益

明白什麼是蒐集了嗎？

明白什麼是處理了嗎？

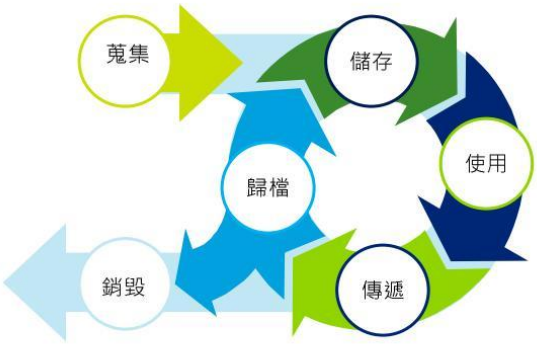
明白什麼是利用了嗎？

明白什麼是國際傳輸了嗎？

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

動腦時間1-蒐集



明白什麼是蒐集了嗎？

明白什麼是處理了嗎？

明白什麼是利用了嗎？

明白什麼是國際傳輸了嗎？

2012 本文件著作權屬法務部

動腦時間1-蒐集

1. 只成立在「為建立個資檔案」所為之蒐集
2. 直接蒐集、間接蒐集傻傻分不清楚嗎？還有不屬於蒐集的呢？

明白什麼是處理了嗎？

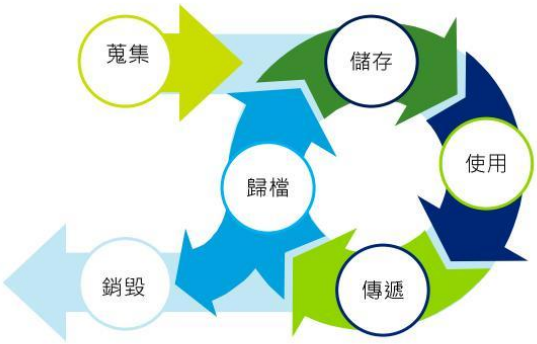
明白什麼是利用了嗎？

明白什麼是國際傳輸了嗎？

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

動腦時間2-處理



明白什麼是蒐集了嗎？

明白什麼是處理了嗎？

明白什麼是利用了嗎？

明白什麼是國際傳輸了嗎？

2012 本文件著作權屬法務部

動腦時間2-處理

明白什麼是蒐集了嗎？

為建立或利用個資檔案所為資料之記錄、輸入、儲存、 編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。(見個資法第二條第四款)

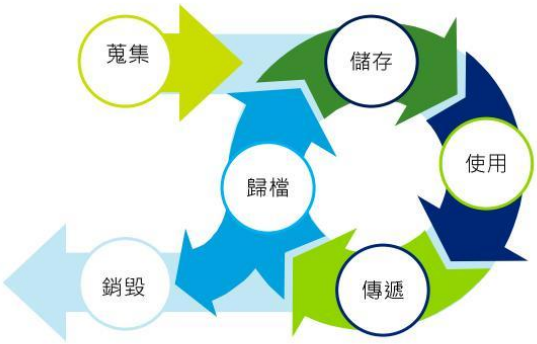
明白什麼是利用了嗎？

明白什麼是國際傳輸了嗎？

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

動腦時間3-利用



明白什麼是蒐集了嗎？

明白什麼是處理了嗎？

明白什麼是利用了嗎？

明白什麼是國際傳輸了嗎？

2012 本文件著作權屬法務部

動腦時間3-利用

明白什麼是蒐集了嗎？

明白什麼是處理了嗎？

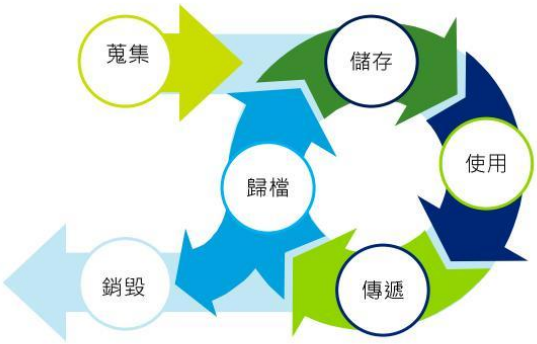
掃描文件？複製文件？下載文件？
上傳文件？審核文件？銷毀文件？
行銷作業？傳遞給第三方？
(不一定通通都是利用哦)

明白什麼是國際傳輸了嗎？

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

動腦時間4-國際傳輸



明白什麼是蒐集了嗎？

明白什麼是處理了嗎？

明白什麼是利用了嗎？

明白什麼是國際傳輸了嗎？

2012 本文件著作權屬法務部

動腦時間4-國際傳輸

明白什麼是蒐集了嗎？

明白什麼是處理了嗎？

明白什麼是利用了嗎？

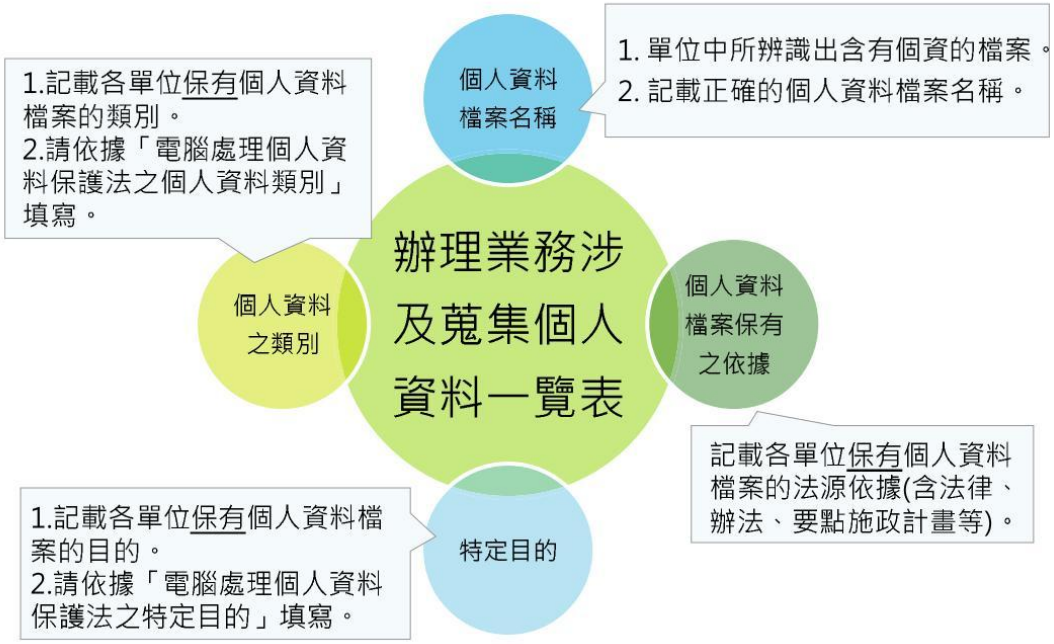
外交部將個資傳給國外的領事館或辦事處？

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

「個人資料檔案清冊」的架構

「個人資料檔案清冊」如何填？



P.22

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

辦理業務涉及蒐集個人資料一覽表

請填寫個人資料檔案的正確名稱

請填寫保有該個人資料檔案的法源依據

請依據「電腦處理個人資料保護法之特定目的」填寫

請依據「電腦處理個人資料保護法之個人資料類別」的填寫

個人資料檔案名稱	個人資料檔案保有之依據	特定目的	個人資料之類別
機關員工聯絡資訊	行政院及所屬機關人事資料統一管理要點	002 人事行政管理	**個人資料類別**：識別類（C001 識別個人者）；受僱情形（C061 現行之受僱情形）
差勤資料	公務人員請假規則	002 人事行政管理	**個人資料類別**：識別類（C001 識別個人者）；受僱情形（C061 現行之受僱情形）
福利資料（含婚、喪、生育及子女教育補助、急難救助、員工文康活動等資料）	行政院所屬各級人事機構人員設置管理要點、全國軍公教員工待遇支給要點、中央公教人員急難貸款實施要點、中央各機關學校員工文康活動實施要點	002 人事行政管理	**個人資料類別**：識別類（C001 識別個人者、C003 政府資料中之識別者）；家庭情形（C023 家庭其他成員之細節）；財務細節（C087 津貼、福利、贈款）

sample

說明：本表係擷取自行政院人事行政局所填列之「辦理業務涉及蒐集個人資料一覽表」，有關人事機構辦理人事業務涉及蒐集個人資料之共同性部分。

P.23

2012 本文件著作權屬法務部

電腦處理個人資料保護法之個人資料類別說明

代　號　識別類：

C〇〇一　辨識個人者。

例如：姓名、職稱、住址、工作地址、以前地址、住家電話號碼、相片、指紋、電子郵遞地址及其他任何可辨識資料本人者等。

C〇〇二　辨識財務者。

例如：銀行帳戶之號碼與姓名、信用卡或簽帳卡之號碼、個人之其他號碼或帳戶等。

C〇〇三　政府資料中之辨識者。

例如：身分證統一編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等。

代　號　特徵類：

C〇一一　個人描述。

例如：年齡、性別、出生年月日、出生地、國籍等。

C〇一二　身體描述。

例如：身高、體重、血型等。

P.24

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

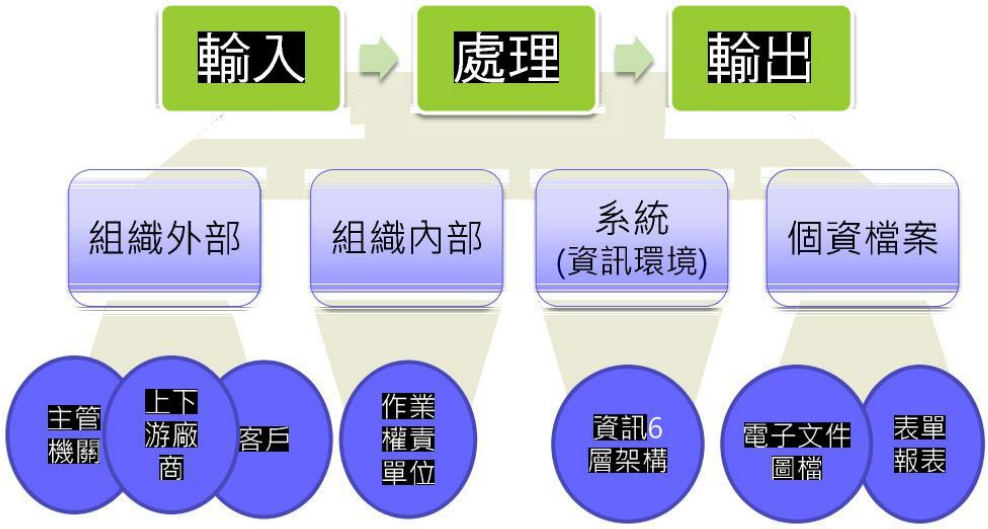
電腦處理個人資料保護法之特定目的說明

代號	特定目的項目
○○一	人身保險業務（依保險法令規定辦理之人身保險相關業務）
○○二	人事行政管理
○○三	土地行政
○○四	公立與私立慈善機構之目標
○○五	公共衛生
○○六	公共關係
○○七	火災預防與控制
○○八	戶政及戶口管理
○○九	不動產服務
○一○	公職人員財產申報業務
○一一	立法或立法諮詢
○一二	民政
○一三	代理與仲介之管理
○一四	犯罪預防、刑事偵查、執行、矯正、保護處分或更生保護事務
○一五	外匯管理
○一六	生態保育
○一七	合法性審計

2012 本文件著作權屬法務部

企業資訊流概覽圖的繪製概念-資訊處理流程

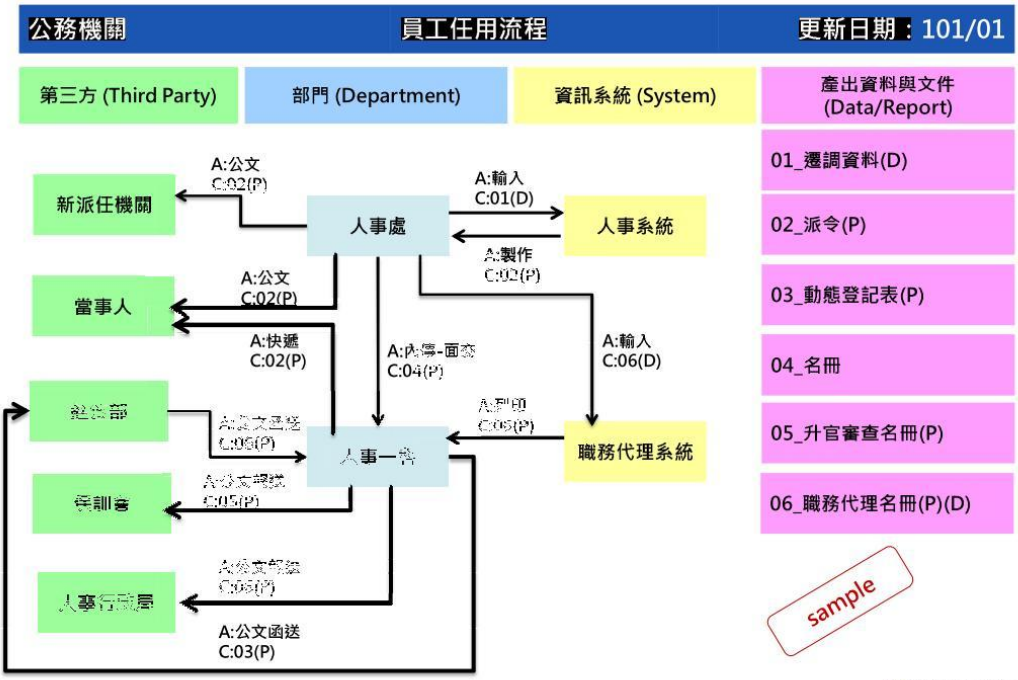
■ 如何找出個人資料檔案 - 以資訊處理的概念出發



2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

員工任用流程



練習時間

本報告之智慧財產權歸屬於法務部

本報告之智慧財產權歸屬於法務部

風險評鑑概論

風險評鑑執行之依據

■ 為什麼要作風險評鑑？

◆臺灣個人資料保護與管理制度(TPIPAS)

➢ 4.4.3 風險管理措施

- 事業應就納入管理範圍之資料，分析其可能面臨之風險與威脅，並訂定不同層級之管控措施。

◆BS 10012:2009(資料來源：BSI英國標準協會)

➢ 4.4 風險評鑑

- 目標:
  確保組織了解處理特定類型個人資訊的任何相關風險.

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

何謂風險評鑑？

- 風險管理(Risk Management)
  - 藉由協調各項活動以指導與控管組織之有關風險。
- 風險評鑑(Risk Assessment)
  - 「風險分析」與「風險評估」的整體過程。

風險分析	風險評估
• 系統性的使用資訊，以識別緣由與估計風險。	• 把預估的風險和已知的風險準則進行比較的過程，以決定風險的顯著性。

2012 本文件著作權屬法務部

弱點分析與威脅分析

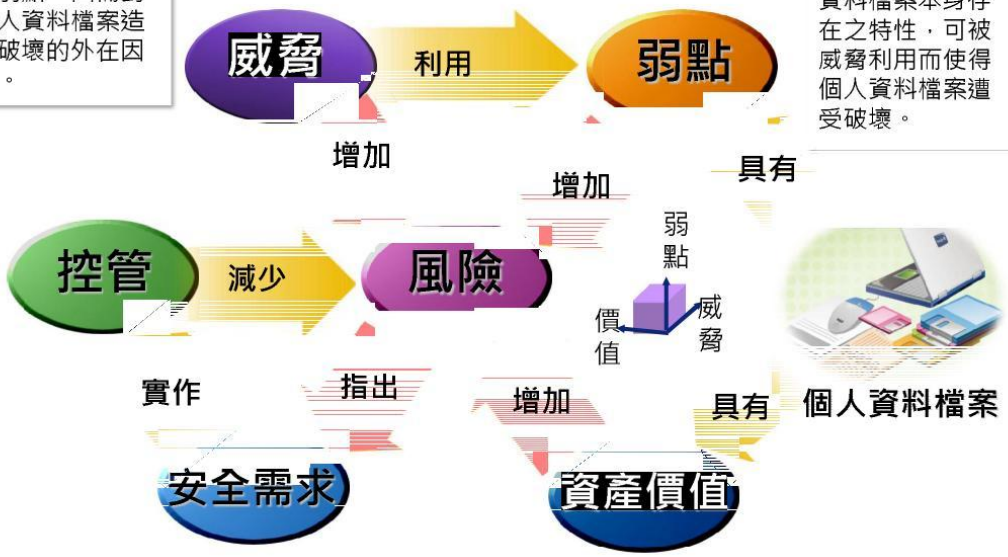
- 弱點分析
  - 弱點是個人資料檔案本身存在之特性，可被威脅利用而使得個人資料檔案遭受破壞。
  - 弱點值
    - 衡量目前公司控管之完整度
- 威脅分析
  - 威脅是可利用弱點，因而對個人資料檔案造成破壞的外在因素。各類弱點會因為不同威脅的發生而產生風險，故需考量威脅發生之重大性。
  - 威脅值
    - 考量現有控管或機制，威脅能利用弱點而造成的衝擊與可能性（機率）

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

風險評鑑元素

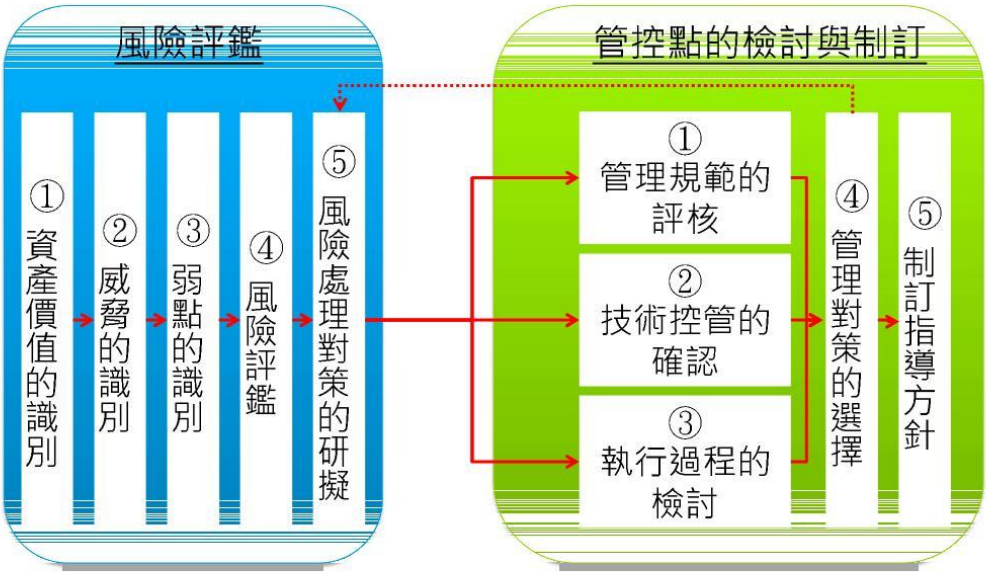
「威脅」是可利用弱點，因而對個人資料檔案造成破壞的外在因素。



「弱點」是個人資料檔案本身存在之特性，可被威脅利用而使得個人資料檔案遭受破壞。

2012 本文件著作權屬法務部

風險評鑑方法示意圖



2012 本文件著作權屬法務部

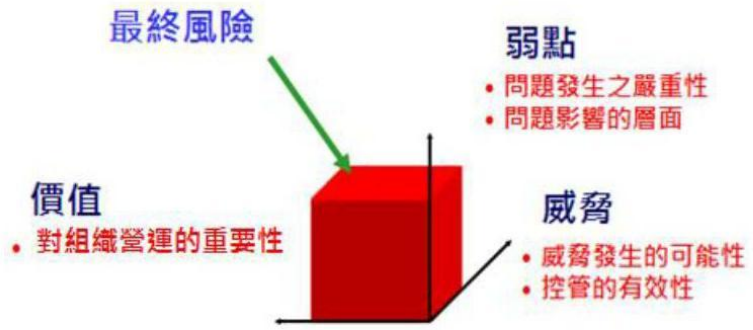
本報告之智慧財產權歸屬於法務部

風險評鑑的公式

白話的說法：
風險 = 出事以後影響有多大 x 保護程度好不好 x 會出事的可能性有多高

1 2 3

Risk = Value x Vulnerabilities x Threats
風險　資產價值　弱點值　威脅值



P.37

2012 本文件著作權屬法務部

可接受風險水準

控管措施

可接受風險水準：

由管理組織依所面臨之風險及所願意投入之資源，而決定風險可接受水準，以作為控管機制設計及建置之基準。

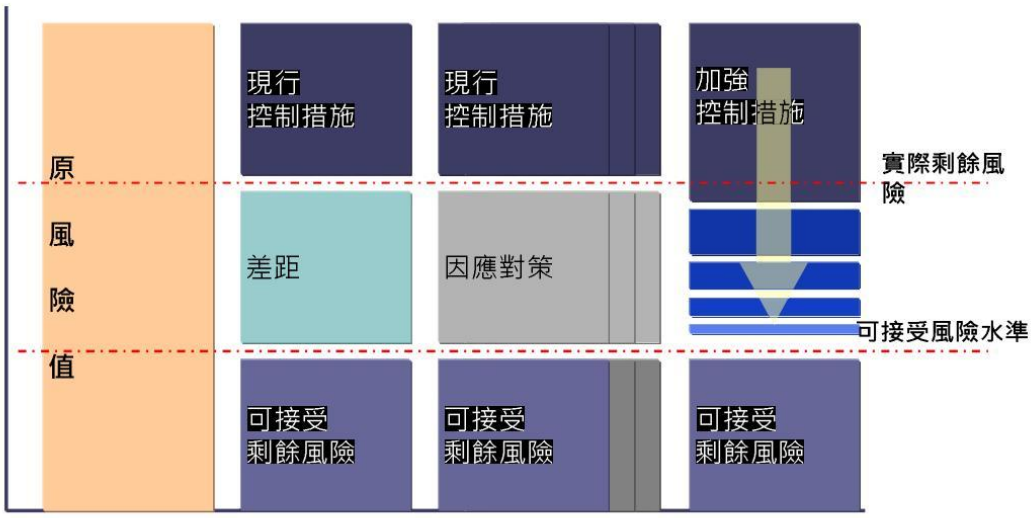
找到平衡點!

P.38

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

風險因應對策



2012 本文件著作權屬法務部

個人資料保護風險評鑑執行作業

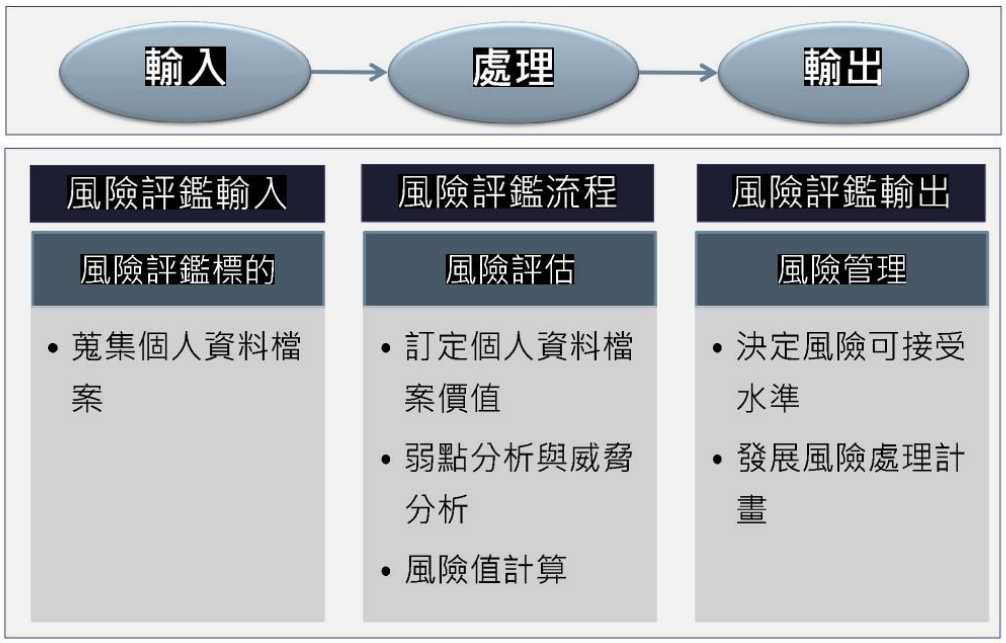
風險辨識	風險評估	風險處理
蒐集個人資料檔案與相關資產	判定個人資料檔案群組價值	擬定風險可接受水準
個人資料檔案及相關資產分類分群	判定個人資料檔案群組弱點值	擬定風險處理計畫
執行隱私衝擊分析	判定個人資料檔案群組威脅值	追蹤風險處理情形
	產出風險值	第二次風險評鑑

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

風險評鑑執行說明

執行風險評鑑及管理



2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

風險分析步驟

風險 = 出事以後影響有多大 x 保護程度好不好 x 會出事的可能性有多高
價值

辨識資產(個資清冊)

個人資料檔案名稱	個人資料檔案保有之依據	特定目的	個人資料之類別
公務人員履歷資料(含公務人員基本資料、現職、學歷、考試、訓練、家屬、經歷、考績、獎懲、銓審等人事21表資料)	人事管理條例、行政院暨所屬各機關人事行政資訊化統一發展要點、行政院及所屬各機關人事資料統一管理要點	002 人事行政管理	**個人資料類別**：識別類(C001 辨識個人者、C003 政府資料中之辨識者)、特徵類(C011 個人描述)、家庭情形(C021 家庭情形、C023 家庭其他成員之細節)、社會情況(C031 住家及設施、C038 職業、C039 執照或其他許可)、教育、技術或其他專業(C051 學校紀錄、C052 資格或技術、C054 職業專長)、受僱情形(C061 現行之受僱情形、C062

決定資產價值

資料類別	說明	價值
敏感個人資訊	含醫療、基因、性生活、健康檢查或犯罪前科之一個人資料檔案者。	3
一般直接識別個資	除敏感個人資訊以外，其檔案內含有可識別2的個人資料者。	2
難以識別個人	係指查詢困難、需耗費過鉅或耗時過久始能特定者，如加密或去識別化。	1

P.43

2012 本文件著作權屬法務部

風險分析步驟

風險 = 出事以後影響有多大 x 保護程度好不好 x 會出事的可能性有多高
弱點值

弱點分析

弱點是個人資料檔案本身存在之特性，可被威脅利用而使得個人資料檔案遭受破壞。

弱點值

衡量目前控管之完整度。

1. 以個資法、施行細則、個人資料檔案安全維護計畫及業務終止後處理方式、國內及國際最佳實務，定義其弱點項目。
2. 定義弱點值高低之判斷標準。

弱點值的設定

弱點項目	風險值	評斷原則
V02.缺乏對外部團體與資訊安全相關之規範	1	已與外部團體訂有資訊安全相關之權利與義務
	2	僅與部份外部團體訂定委任之權利義務契約
	3	尚無與外部團體訂定權利及義務契約之機制
V04.缺乏一般辦公環境的安全控管	1	已制定完善之辦公環境控管政策並妥為遵循
	2	已有辦公環境控管政策但未完備或未確實遵循
	3	尚未對辦公環境制定控管政策
V05.缺乏書面化操作程序之控管	1	已有詳盡的書面處理程序，即時更新，且妥為
	2	資料，或書
	3	尚無操作

弱點值為1~3，衡量目前控管之完整度

P.44

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

風險分析步驟

風險 = 出事以後影響有多大 x 保護程度好不好 x 會出事的可能性有多高
威脅值

威脅分析
威脅是可利用弱點，因而對個人資料檔案造成破壞的外在因素。各類弱點會因為不同威脅的發生而產生風險，故需考量威脅發生之重大性。
威脅值
考量現有控管或機制，威脅能利用弱點而造成的衝擊與可能性（機率）。

威脅值的設定

文件	洩漏 竊取 竄改 偽造 遺失 損毀 當事人權利損失 違法

1. 定義個人資料檔案可能產生之威脅。
2. 定義威脅值高低之判斷標準。

2012 本文件著作權屬法務部

風險評鑑結果 (範例)

風險值=資產價值x弱點值x威脅值

資產價	弱點項目	弱點值	威脅項目	威脅值	風險值	註記	控管編號
3	V 2.缺乏資料的安全管理	3	盜賣	2	18	[Q19]目前廠區進出不能開啟手機，唯無明確列示禁止物品攜入之項目，亦僅為人員口頭提示。	A.9.2.6
			洩漏	3	27		A.10.5.1
			竄改	2	18		A.10.7.3
			偽造	2	18		A.10.7.4
							A.12.4.2
							A.12.5.4

1 2 3

Risk = Value x Vulnerabilities x Threats
風險 資產價值 弱點值 威脅值

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

風險評鑑與衝擊分析之關係

名詞說明

個資管理衝擊分析(Privacy Impact Analysis; PIA)

- 本活動主要為識別組織對個人資料管理之現況，以瞭解其現行制度所可能產生的遵法風險，進一步辨識個人資料管理之可行強化項目。

風險評鑑 (Risk Assessment; RA)

- 本活動將依據個資衝擊與潛在風險分析結果，提出個資管理改善建議與因應對策之行動方案。

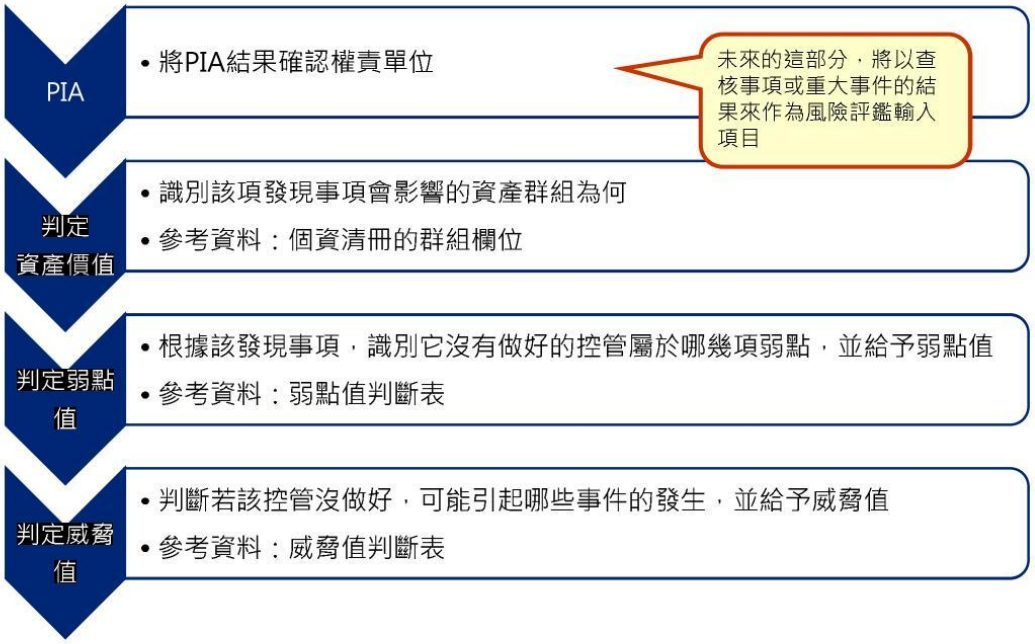
稽核作業 (Audit)

- 針對目前規範進行查核，以確認控管之落實度。

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

實際執行流程



2012 本文件著作權屬法務部

風險評鑑案例

- PIA發現事項

  帳號權限控管：
  部分應用系統未有定期覆核帳號權限之機制。

- Step1：找出受影響的個人資料檔案及其**資產價值**
- Step2：判定弱點值
  - ◆ 找出弱點項目，並確認資產類別所適用之弱點項目；再判定弱點值
- Step3：判定威脅值
  - ◆ 找出威脅項目，確認該弱點適用的威脅種類
- Step4：決定風險值

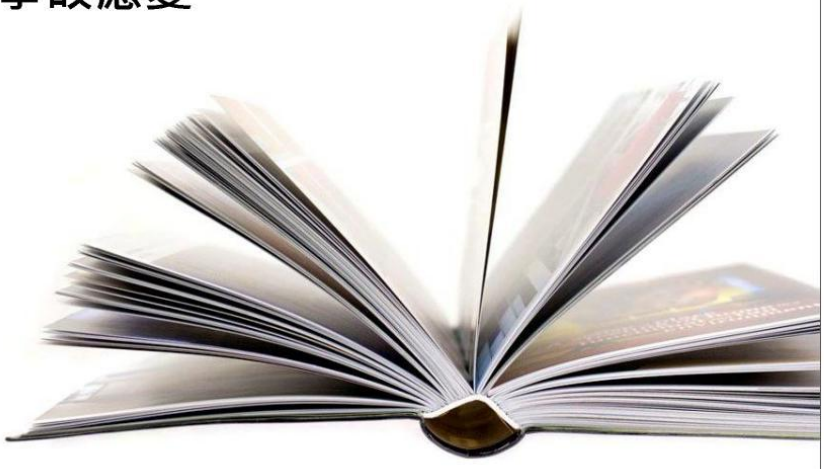
2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

風險評鑑實作

本報告之智慧財產權歸屬於法務部

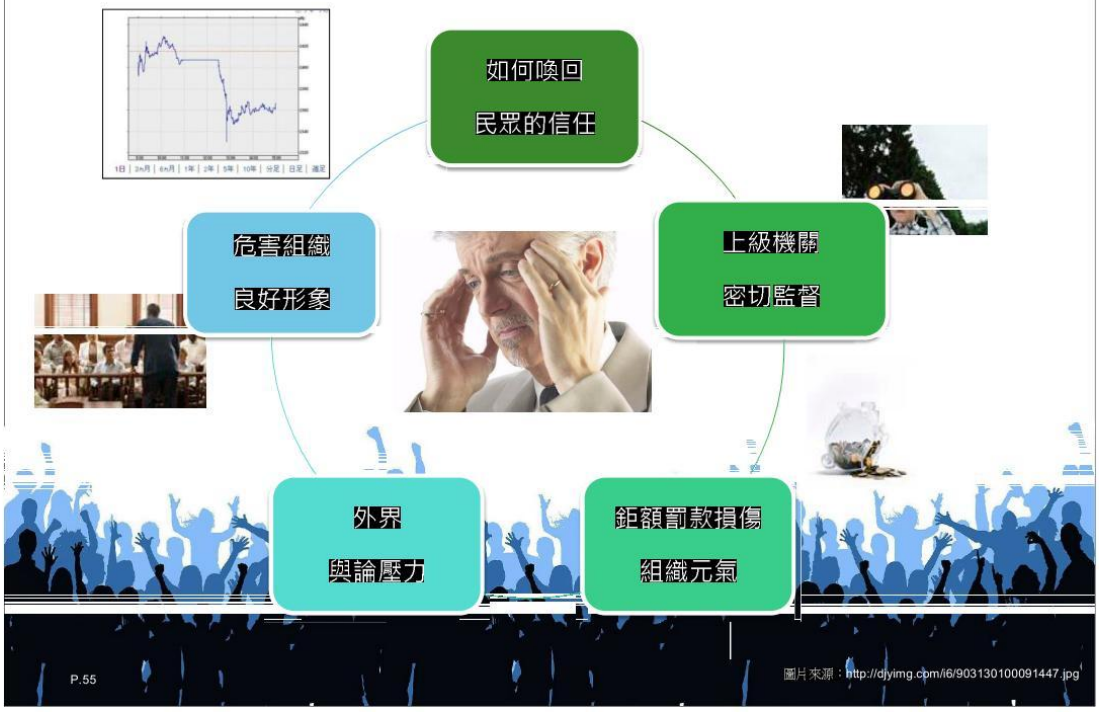
個資侵害事故應變



個資外洩與應變案例

本報告之智慧財產權歸屬於法務部

個資外洩後的結果...



資料外洩怎麼處理很重要!

個資事件類型	某市政府網站擺烏龍，民眾個資外洩	資料來源	華視 2008/11/17

某市政府法規會，也就是主管消費者保護的機關網站，把民眾申請國賠的資料，全部開放提供檢索，不但個人身分資料全都查得到，就連就醫紀錄都被貼在網站上。

當市民想申請國賠，而進入某市政府法規會網站時，在全文檢索中隨意輸入查詢字眼，就會出現一筆民眾的案例資料，不只是文字陳述，就連車禍照片與當事人就醫紀錄，全都一覽無疑，還有民眾的身分證就這樣顯示在網站上。

某市市議員質疑，主管消費者保護的法規會，竟然成了洩密個人資料的兇手。法規會則表示是外包資訊廠商，忘記把資料加密，才導致民眾的個人資料全都露，已經請廠商趕工補救。

P.56

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

公務機關有事件處理的流程跟方式嗎?
- 有! 國家資通安全應變機制【公務機關事件分級】

（一）4級事件
符合下列任一情形者，屬4級事件：
1. 國家機密資料遭洩漏。
2. 國家重要資訊基礎建設系統或資料遭竄改。
3. 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

（二）3級事件
符合下列任一情形者，屬3級事件：
1. 密級或敏感公務資料遭洩漏。
2. 核心業務系統或資料遭嚴重竄改。
3. 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

（三）2級事件
符合下列任一情形者，屬2級事件：
1. 非屬密級或敏感之核心業務資料遭洩漏。
2. 核心業務系統或資料遭輕微竄改。
3. 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

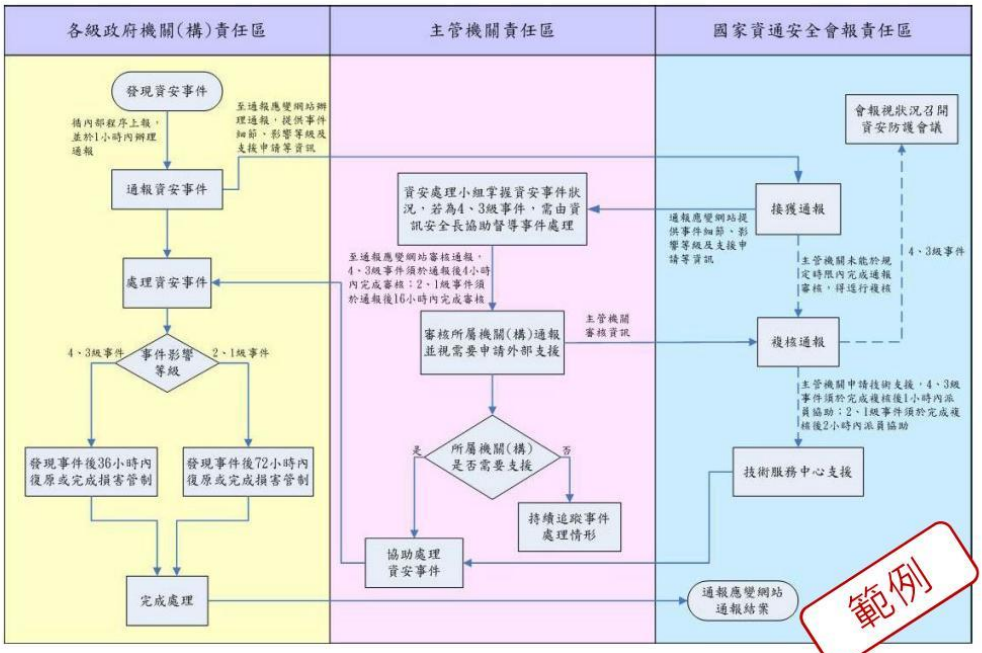
（四）1級事件
符合下列任一情形者，屬1級事件：
1. 非核心業務資料遭洩漏。
2. 非核心業務系統或資料遭竄改。
3. 非核心業務運作遭影響或短暫停頓。

個人資料之保護為資訊安全之一環，因此應若有個資外洩事件，應依國家資通安全應變機制進行通報與處理

P.S. 詳細應變流程請參閱【個人資料保護執行程序暨考核作業手冊要點】之說明

2012 本文件著作權屬法務部

公務機關有事件處理的流程跟方式嗎?
- 有!國家資通安全應變機制【公務機關事件應變流程】

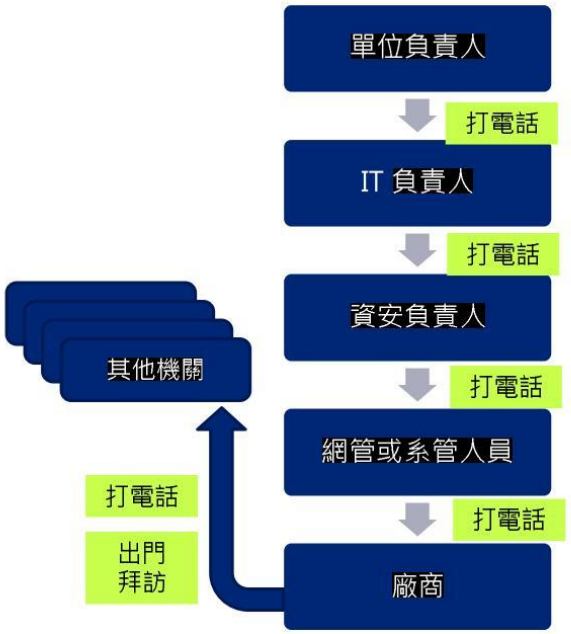


2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

個資侵害事故應變流程

傳統應變流程



2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

緊急應變應有之程序與框架

事件發生前

事件發生時

事件結束後

工作項目

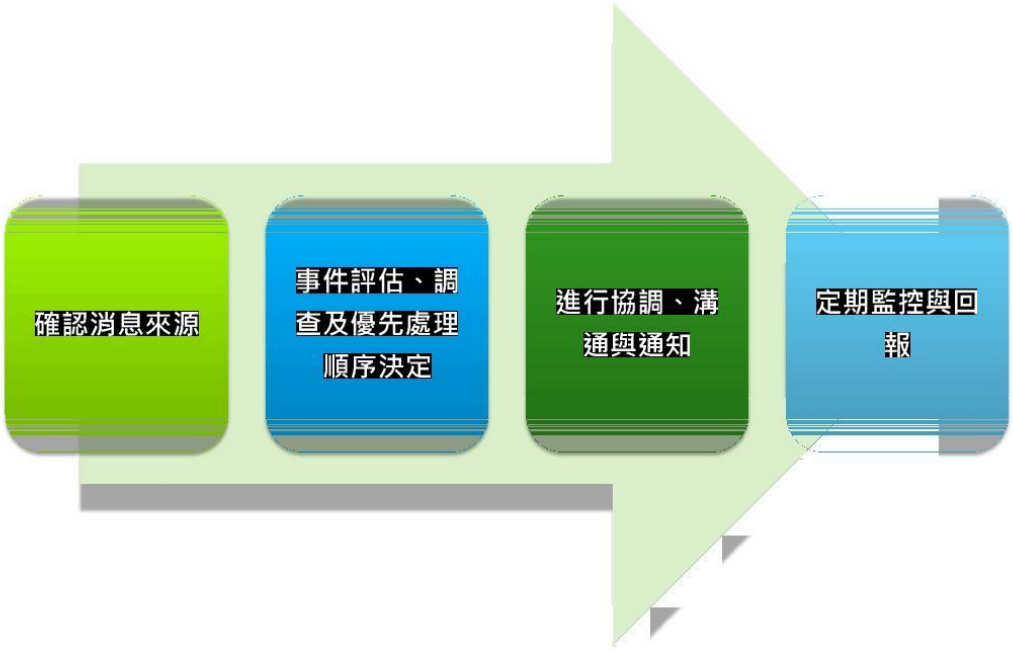
- **建立組織**
  - 建立個資侵害事件應變處理小組
- **事件通知程序**
  - 資料當事人、媒體及內部人員之通知程序擬定
  - 建立對外連繫清單
  - 聲明稿擬定
- **程序建立及定期演練機制**
  - 擬定事件應變程序並定期進行演練作業

- **情報確認階段**
- **事件被媒體公開或調查結果確認**
- **後續應變階段**

- **召開事件檢討會議**
- **應變計畫維護**

2012 本文件著作權屬法務部

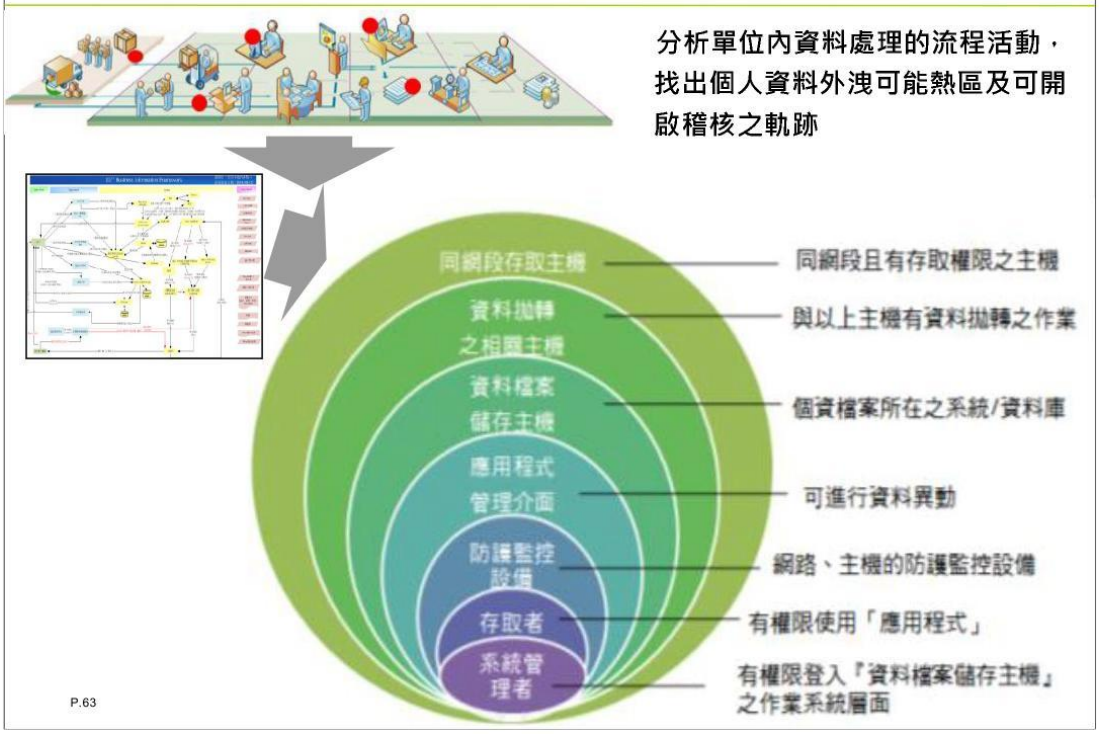
事件發生時之應變步驟



2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

事件鑑識示意圖


分析單位內資料處理的流程活動，找出個人資料外洩可能熱區及可開啟稽核之軌跡

P.63

建立對外聯繫清單及聲明稿擬定範本

一、聲明稿範本

適用時機：當發生個人資料外洩時，第一時間的回應稿

本單位深知個人資料保護之重要性，因此，一向致力於資訊處理過程之安全性，致力提升民眾服務品質及安全。

針對【日期】，所發生之【事件名稱】，【單位發言人姓名】提出以下幾點說明：

（一）所有個人資料保護，於處理過程中，皆受到嚴密的標準控管，除對於處理資料之系統設定安全性控管，且所有接觸資料人員，更受嚴格限制及作業監控。

（二）【其他說明項目】

（三）對於本次事件，本單位將收集相關資訊提供調查單位，並於調查過程中，竭盡全力配合，以協助上級機關、廠商與社會大眾盡速破獲狀況，以防其責。

sample

三、對外聯繫清單

（一）聯繫時機與負責單位

單位	XXX 負責單位	聯繫時機

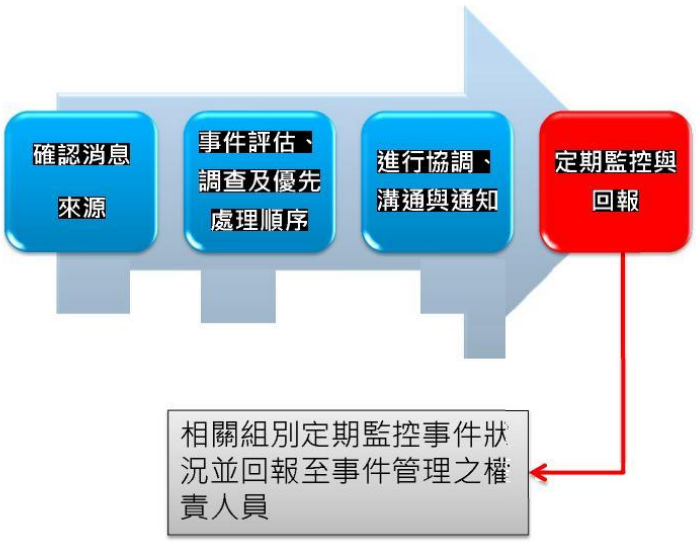
sample

P.64

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

定期監控與回報



2012 本文件著作權屬法務部

事件檢討會議

- 舉行事件檢討會議
  - 會議內容應包括以下:
    - 重述事件全貌
    - 相關人員參與個人資料外洩事件過程之應變能力說明
    - 是否有遵循文件要求之程序
    - 如何防止事件再次發生
    - 需額外採購之工具或資源
  - 個資外洩事件應變處理小組須考量過去發生的個人資料外洩事件紀錄，找出個人資料外洩事件發生的模式，並提出建議的改善機會，包括控管措施加強及個人資料外洩事件緊急應變計畫之改善。

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

我需要準備個資外洩的應變程序嗎?

- 錯誤的認知:
  - 認為個資雖有不當使用及未經授權的情形，但因未有立即而明顯的損害，所以不需立即應變
  - 評估應變作為的順序時，只考慮到現有資源，而未考慮到對當事人的衝擊及影響範圍。

我們應先問自己下列問題
• 個資外洩的民眾抱怨數量是否增加?
• 組織是否已經針對個人資料進行盤點及造冊?
• 個人資料的管理權責是否已經定義明確?
• 所屬單位是否有上級機關?上級機關是否有明定相關的義務及權責?
• 過去是否有發生個人資料誤用及不當存取的情形?後續處理?
• 是否曾發生儲存個人資料的手提電腦及儲存設備、媒體遺失的情況?後續處理?
• 一旦有個資外洩的情事，組織內部知不知道有那一些告知對象?

P.67

2012 本文件著作權屬法務部

程序建立及定期演練機制

- 應針對事件應變程序定期進行演練作業，演練方式可分為通報程序演練或鑑識調查程序之演練，於演練完成後，若發生重大問題或未達目標之要求時，應會同演練計畫執行時之細項結果舉行檢討會議。
- 請考慮書面模擬演練、情境模擬演練及實況演練

P.68

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

個人資料外洩事件緊急應變計畫

■ 更新過程

◆ 應定期檢討個人資料外洩事件緊急應變計畫，如有下列項目，應立即更新計畫內容。

- ➢ 新法或現行個人資料保護法修訂時，應立即針對該異動進行相關之修正。
- ➢ 內部組織架構重大之變更。
- ➢ 內部個人資料保護政策之修訂。

2012 本文件著作權屬法務部

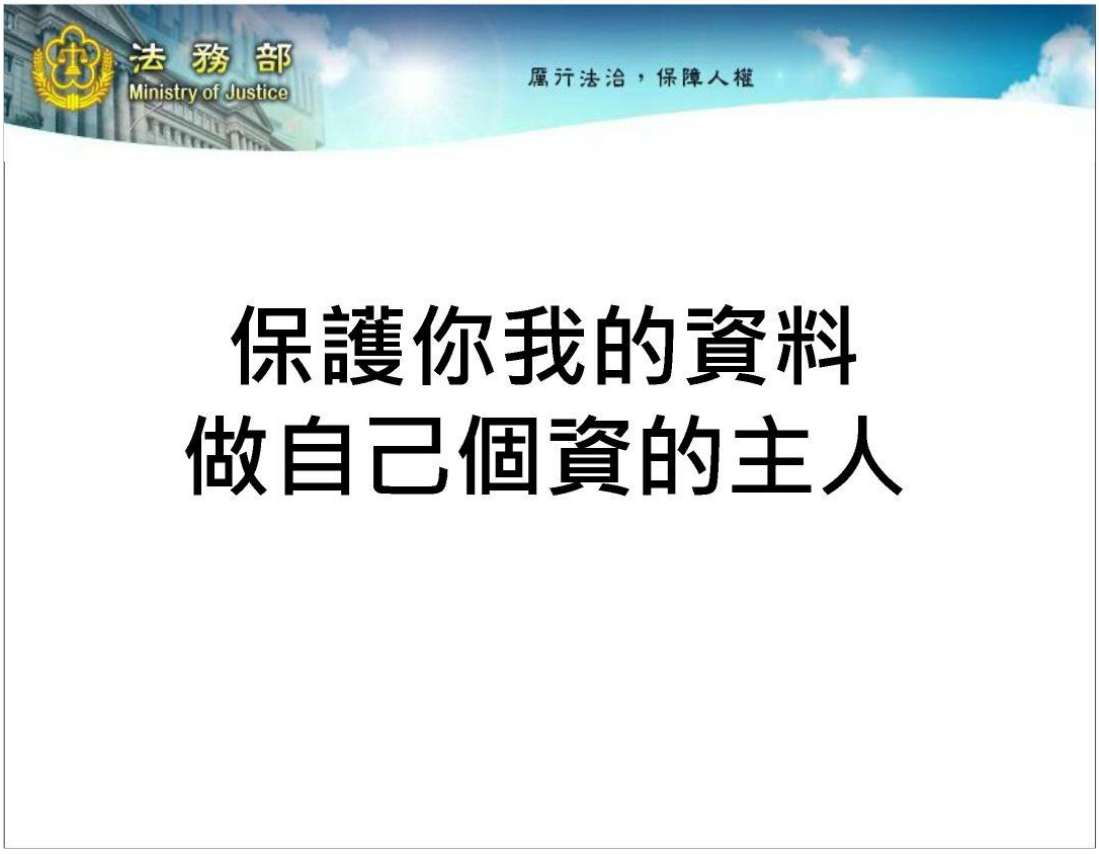
危機處理三要素

2012 本文件著作權屬法務部

本報告之智慧財產權歸屬於法務部

問題與討論

本報告之智慧財產權歸屬於法務部



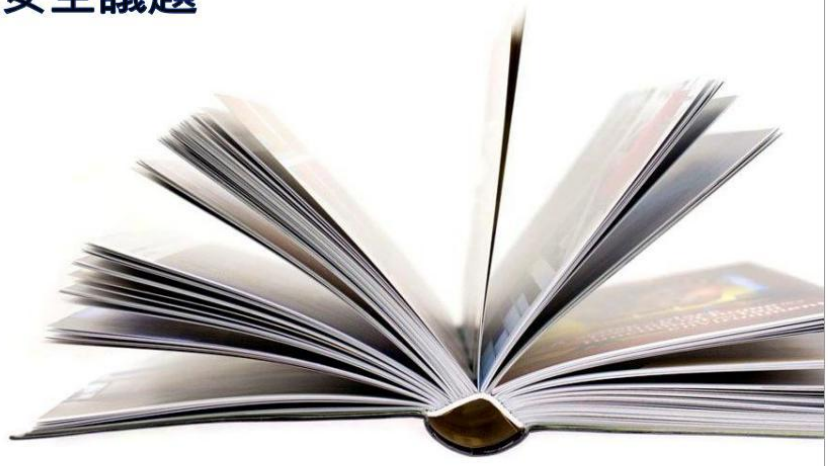
資料來源：本計畫撰寫

本報告之智慧財產權歸屬於法務部

四、公務人員及民眾認知宣導教材

本報告之智慧財產權歸屬於法務部

個人資料安全議題



個人資料安全議題 (1/3)

■史上最大個資外洩案，SONY真的該Sorry

個資事件類型	個資安全措施	資料來源	聯合新聞網 2011/06/03

SONY的遊戲主機PS3網路平台PSN，在四月十九日遭到駭客入侵，高達六十個國家、七千七百萬用戶個資外洩。可能外洩的個資包括姓名、住址、電話號碼、電郵信箱、信用卡資料、性別及生日等。SONY不但沒有在第一時間告知PSN用戶還試圖掩飾，第一份通告於被駭十天後才寄出。駭客攻擊中受害的SONY網路用戶已超過一億人。

對應個人資料保護法…

■第28條第4條-對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。

■第29條-非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。

事件學習

■個人資料管理者應妥善保護個人資料之安全，並在個資外洩事件發生後查明真相並據實告知當事人。

4

本報告之智慧財產權歸屬於法務部

個人資料安全議題 (2/3)

■千筆中X局客戶個資丟馬路

個資事件類型	個資安全措施	資料來源	蘋果日報2010/06/20

銀行竟將民眾重要個資丟棄在路邊，真是太離譜！北縣八里鄉西濱快速道路一處路段，前天被人發現上千張前中X局開戶申請的文件散落一地，部分還掉落下方涵洞，單據上除了姓名、電話，還有身分證號及銀行帳戶等重要個資。

對應個人資料保護法…

■第27條第1項-非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
■第27條第2項-中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。
■第27條第3項-前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之

事件學習

■個人資料管理者應妥善保護個人資料之安全，並定期檢視和重新評估該些保護措施。

5

個人資料安全議題 (3/3)

■民眾至萬芳醫院 志工給的便條紙背後竟藏他人就醫資訊

個資事件類型	個資安全措施	資料來源	中時電子報 2011/08/04

台北市立萬芳醫院，爆發有民眾就醫時，到服務台詢問就醫資訊，結果當時志工提供的便條紙，居然發現是另外一名病患的就醫資料，包括姓名、年齡、體重、還有就醫科別，全部被看光光。…院方也進一步調查，發現是門診醫師，將病患的病歷列印出來發現有錯誤，應該會放到銷毀處，卻誤回收成便條紙再利用。

對應個人資料保護法…

■第27條第1項-非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
■第27條第2項-中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。
■第27條第3項-前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之

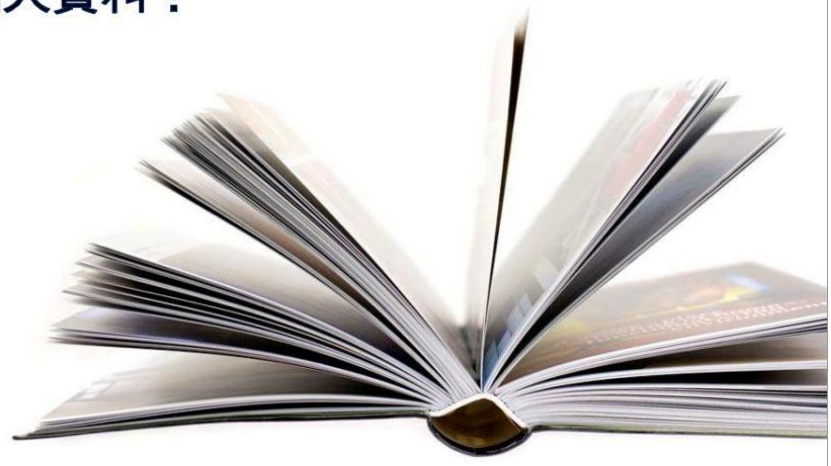
事件學習

■個人資料管理者應妥善保護個人資料之安全，並定期檢視和重新評估該些保護措施。

6

本報告之智慧財產權歸屬於法務部

什麼是個人資料？



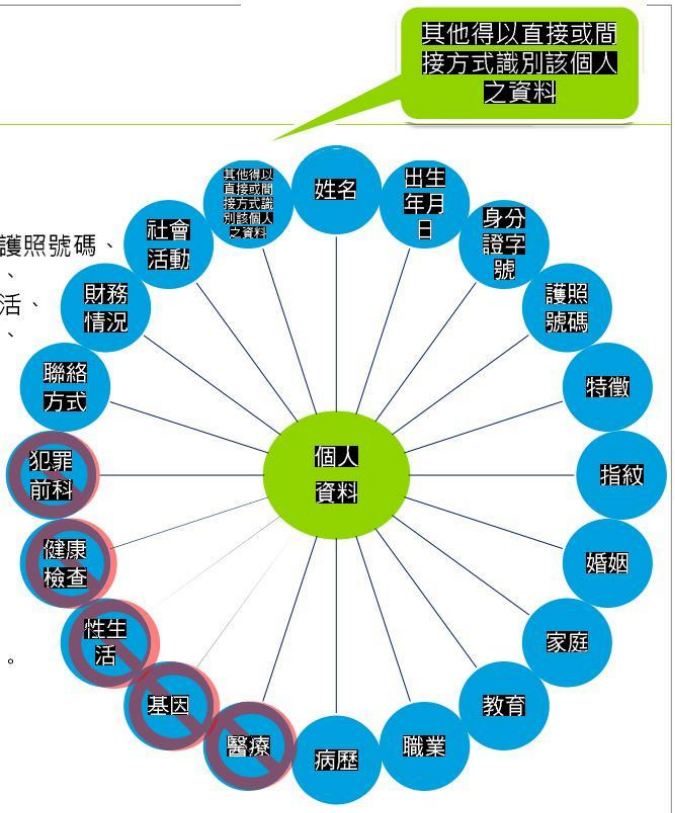
個人資料之定義

依據個人資料保護法第二條，
個人資料係指(生存)自然人之：

姓名、出生年月日、身份證號、護照號碼、
特徵、指紋、婚姻、家庭、教育、
職業、病歷、醫療、基因、性生活、
健康檢查、犯罪前科、聯絡方式、
財務情況、社會活動，
或其他可以直接或間接方式
識別個人的各種資料。

...

其中以紅色標示之項目，包含
醫療、基因、性生活、
健康檢查、犯罪前科
依據個人資料保護法第六條，
原則上不得蒐集、處理、或利用。



8

本報告之智慧財產權歸屬於法務部

個人資料說明

這些都是個人資料喔!

類別	內容
特徵	年齡、性別、出生地、國籍、身高、體重、血型、抽煙、喝酒等。
婚姻	婚姻之歷史：前次婚姻或同居、離婚或分居等細節及相關人之姓名等。
	家庭其他成員之細節：子女、受扶養人、家庭其他成員或親屬、父母等。
家庭	是否有結婚、配偶或同居人之姓名、前配偶或同居人之姓名、結婚之日期、子女之人數等。
教育	學校紀錄：大學、專科或其他學校等。
	學生紀錄：學習過程、相關資格、考試成績或其他學習紀錄等。
職業	現行之受僱情形、離職經過、工作經驗、工作紀錄。
病歷	過去、現在或未來、生理與心理的病患狀況紀錄，包括病患的個人資料，病程紀錄，藥物使用記錄，檢查資料與報告及影像診斷報告，過去病史、家族史及預防接種等。
聯絡方式	傳統的聯絡方式：電話、地址。
	時尚的聯絡方式： Email、MSN、SKYPE、FaceBook、微博等。
	其他的聯絡方式：個人部落格、批踢踢(PTT)的帳號、Mobile01的帳號等。

9

個人資料說明

這些都是個人資料喔!

類別	內容
聯絡方式	傳統的聯絡方式：電話、地址。
	時尚的聯絡方式： Email、MSN、SKYPE、FaceBook、微博等。
	其他的聯絡方式：個人部落格、批踢踢(PTT)的帳號、Mobile01的帳號等。
財務情況	帳戶之號碼與姓名、信用卡或簽帳卡之號碼、收入、所得、資產、投資、銀行、負債、支出、信用評等、貸款、結匯紀錄、票據信用、津貼、福利、贈款等。
社會活動	移民情形、旅行及其他遷徙細節、休閒活動及興趣等。
醫療	指以治療、矯正或預防人體疾病、傷害、殘缺為目的 ，所為的診察、診斷及治療；或基於診察、診斷結果，以治療為目的，所為的處方、用藥、施術或處置等行為全部或一部之總稱。
基因	指人體之染色體所儲存超過十萬對以上最基本而具有全部遺傳特質或特定生物功能DNA(去氧核醣核酸)之遺傳單位。
性生活	指所有與性行為有關之活動之總稱，如同性戀等。
健康檢查	指以檢驗為目的所為一般性或遺傳性、傳染性、精神性等疾病檢查之健康資料之總稱，如健康檢查檢查報告等。
犯罪前科	指構成犯罪之具有犯罪紀錄者而言，如良民證等。

本報告之智慧財產權歸屬於法務部

與個人資料相關的活動

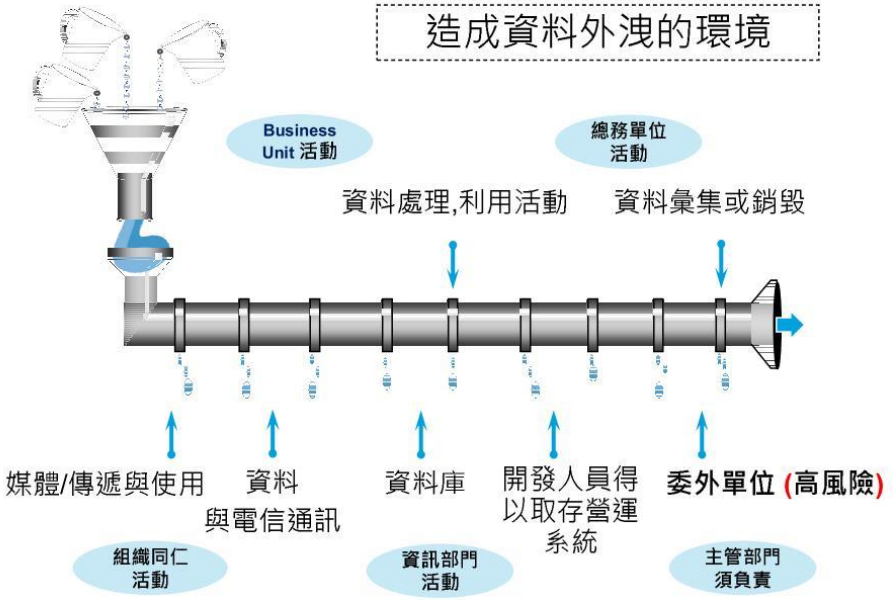
蒐集	指以任何方式取得個人資料(包含直接或間接)
處理	指為建立或利用個人資料檔案[註]所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送
利用	指將蒐集之個人資料為處理以外之使用
國際傳輸	指將個人資料作跨國(境)之處理或利用

註：個人資料檔案指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

11

個人資料外洩常發生的時機...

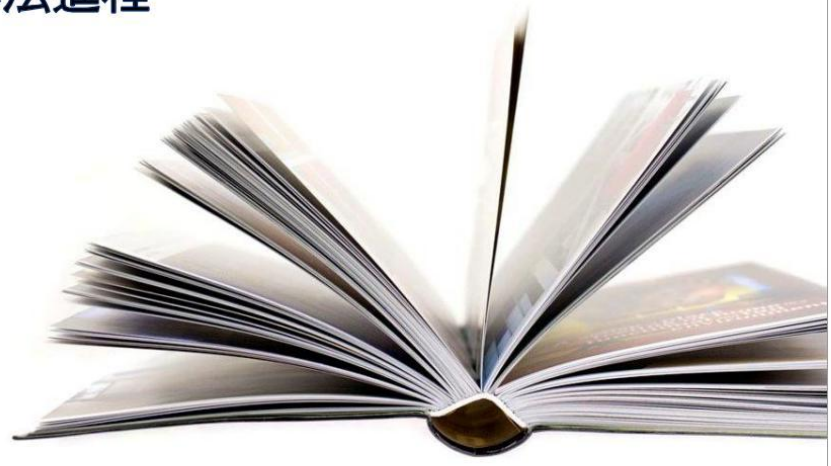
■在整體環境中，存在各式各樣資料外洩的可能性



12

本報告之智慧財產權歸屬於法務部

個資法修法進程



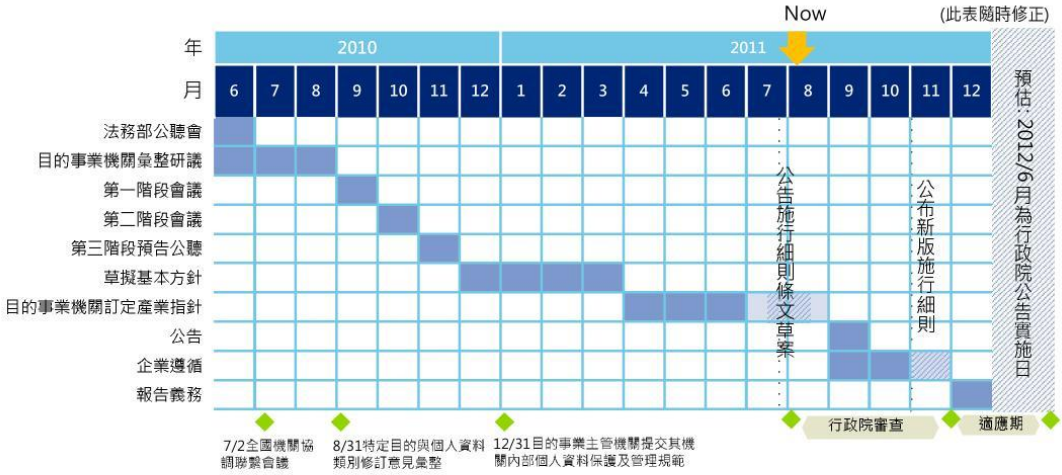
新版《個人資料保護法》的修法緣由及進程

為什麼要修法？ 1. 起訴成功率低 2. 出事單位不在列管範圍 3. APEC 人權要求銜街 4. 扼止詐騙

修法進度？

- 1995：08/11 公布電腦處理個人資料保護法
- 2010：04/20 新版個人資料保護法二讀通過
  - 04/27 新版個人資料保護法三讀通過
  - 05/26 總統公布新版個人資料保護法

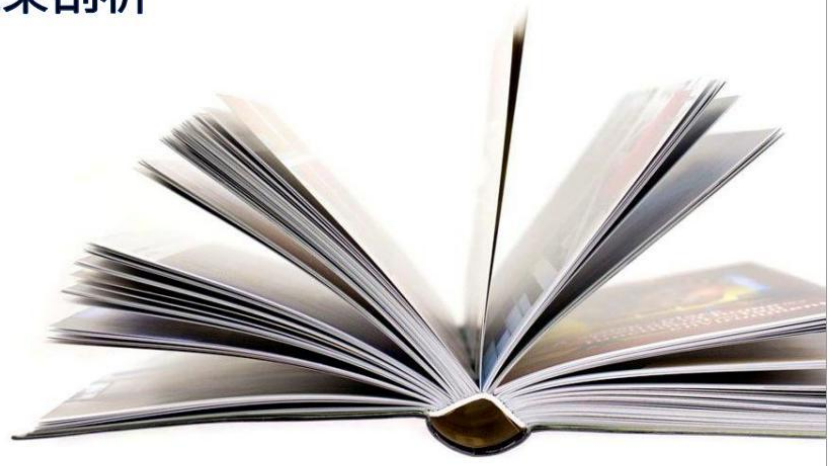
還有多少時間準備？



14

本報告之智慧財產權歸屬於法務部

個資法框架剖析



新版個資法修正的重要立法意旨

新版個人資料保護法

1. 擴大保護客體：	納入人工與其它類型資料 解決以往資料外洩只要不及於電腦（或自動化設備）處理，即不適用或無罪之怪現象，且納入直接與間接識別
2. 普遍適用主體：	刪除行業別之限制，我國自然人/公私機構一體適用 解決以往只有列入受管理的政府機關與8種民間產業的不合理情況
3. 增修行為規範：	限制蒐集特種資料、規範書面同意方式、增課告知義務（4項資料的權利與正確性及外洩之告知）、放寬查詢權利、限制任意行銷，不遵守行為規範的行政裁罰
4. 強化行政監督：	中央目的事業主管機關或地方政府得強制檢查、處分或處罰解決因為普遍適用主體後，管制單位的模糊，並將資料保護的查察措施，擴及非司法警察機構
5. 促進民眾參與：	建立團體訴訟機制 對於管理與求償或資料保護實務的進展，納入民間監督與求償，冀能提高全民重視與普及
6. 調整責任內涵：	加重刑事責任及擴大適用範圍、提高民事損害賠償總額限制、提高行政罰緩並課以負責人、代表人、管理人監督責任舉證責任倒置

16

本報告之智慧財產權歸屬於法務部

個人資料保護法架構

個人資料保護法

17 ©2011 動業眾信版權所有 保留一切權利

個人資料保護法通過後，可以保障我(當事人)的那些權益呢？

本報告之智慧財產權歸屬於法務部

Part1.個資蒐集之告知事項–直接蒐集時...

如果今天有業者打電話來詢問我的個人資料…

嘟~~！嘟~~！嘟~~！

(電話接起來)

對方：您好，我們是XXX公司，
想請您留下您的一些個人資料...

我們很常在電視新聞上看到民眾遭到偽裝成公司業者的不肖分子詐騙個人資料。有時即便是正當業者，也可能將我們的個人資料作不正當或非法的利用！

面對這種情形，
我們該如何保護自己呢？

■其實，不管是誰向我們蒐集個人資料時，原則上都應該明確告知以下事項：

① 對方機關名稱。
② 蒐集個人資料的目的。
③ 個人資料之種類或項目。
④ 個人資料利用之期間、地區、對象及方式。
⑤ 當事人依《個人資料保護法》第三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，不提供將對其權益之影響。

■ 如果對方沒有主動告知以上資訊，**我們可以要求對方先行告知喔！**

■ 當我們在業務上詢問民眾的個人資料時，也得告知民眾以上資訊喔！

19

Part1.個資蒐集之告知事項–直接蒐集時...

向當事人直接蒐集者……

■《第8條》第1項-公務機關或非公務機關依第15條或第19條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

1. 公務機關或非公務機關名稱。
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*第三條*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，不提供將對其權益之影響。

■《第8條》第2項-但有下列情形之一者，得免為告知：

1. 依法律規定得免告知。
2. 個人資料之蒐集係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。

注意事項：
1. **公務機關或非公務機關在直接蒐集資料時，可以透過任何方式告知當事人左列六點事項。**
2. **公務機關或非公務機關僅需告知當事人，不須要等當事人做任何回應。**

20

本報告之智慧財產權歸屬於法務部

Part2.個資蒐集之告知事項—間接蒐集時…

Q：什麼是間接蒐集呢？
A：就是當我們不是直接向當事人(如民眾、客戶)直接蒐集他們的個人資料，而是從第三人、其他公司或是中央及地方其他行政單位索取資料時…

(電話接起來)
對方：您好，我們從**你的朋友**那裏得到你的電話和職業等資訊…

不管是**我們**在業務上要利用
從第三方索取的民眾資料，

還是有**其他機構或業者**
透過我們的親朋好友或其他公司
拿到我們的個人資料，

在處理或利用這些資料之前
我們及對方都有義務告知如右的資訊喔！

■切記！在處理或利用並非由當事人提供之個人資料**之前**，原則上都有義務告知當事人以下事項：

① 個人資料來源。
② 自己(對方)機關名稱。
③ 蒐集個人資料的目的。
④ 個人資料之種類或項目。
⑤ 個人資料利用之期間、地區、對象及方式。
⑥ 當事人依《個人資料保護法》第三條規定得行使之權利及方式。

■ 當我們在業務上詢問民眾的個人資料時，**也得告知民眾以上資訊喔！**

■ 如果對方沒有主動告知以上資訊，我們可以要求對方先行告知喔！

21

Part2.個資蒐集之告知事項—間接蒐集時...

向非當事人間接蒐集時……

■《第9條》第1項-公務機關或非公務機關依第15條或第19條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知下列事項：

1. 個人資料來源。
2. 公務機關或非公務機關名稱。
3. 蒐集之目的。
4. 個人資料之類別。
5. 個人資料利用之期間、地區、對象及方式。
6. 當事人依第三條規定得行使之權利及方式。

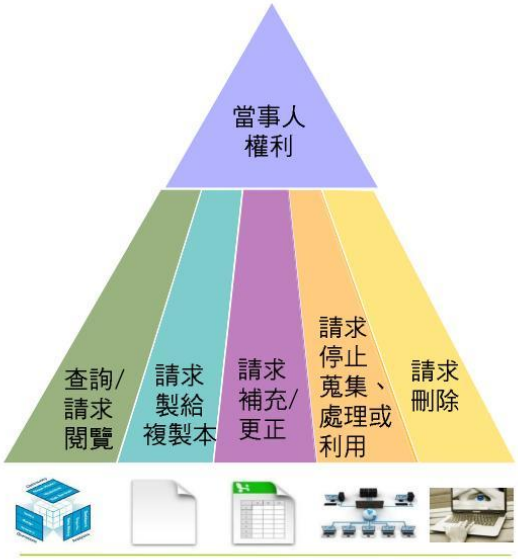
■《第9條》第2項-但有下列情形之一者，得免為告知：

1. 第8條第2項所列各款情形之一。
2. 當事人自行公開或其他已合法公開之個人資料。
3. 不能向當事人或其法定代理人為告知。
4. 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。
5. 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

22

本報告之智慧財產權歸屬於法務部

Part3.當事人有哪些權利可以行使呢？



- 新版個人資料保護法規範當事人擁有以下五項權利：
  - ◆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
- 《第3條》當事人就其個人資料依本法規定行使之權利，**不得預先拋棄或以特約限制之。**

別讓你的權利睡著了

23

Part4.公務機關個人資料之蒐集、處理及利用

當我們蒐集或處理別人的個人資料時，還有什麼要注意的嗎...？

有！

我們在**蒐集**或**處理**個人資料時應有特定目的，例如為了進行申報所得稅的業務目的，而非毫無理由直接向民眾蒐集！

另外，還需要符合：

1. **只在執行法定職務的必要範圍內！**
不做多餘或沒有必要的處理，如明明只是我們部門要進行的業務，還把民眾的個資轉給其他不相干部門使用...。

2. **經當事人書面同意！**
必須在告知當事人應告知事項後，對方以書面方式表示同意！不可以只有告訴對方而不取得其同意...

3. **對當事人權益無侵害。**

有沒有例外情形，
可以在特定目的之外**利用**個人資料？

有！但條件更嚴格：

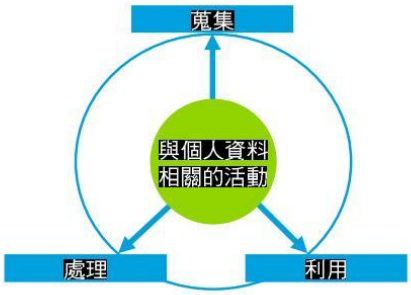
1. 法律明文規定。
2. 為維護國家安全或增進公共利益。
3. 為免除當事人之生命、身體、自由或財產上之危險。
4. 為防止他人權益之重大危害。
5. 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過處理後或依其揭露方式無從識別特定當事人。
6. 有利於當事人權益。
7. 經當事人書面同意。

可見原則上都只能在**特定目的之內**...

24

本報告之智慧財產權歸屬於法務部

Part4.公務機關個人資料之蒐集、處理及利用



第18條-公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

特定目的內……

■第15條-公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

1. 執行法定職務必要範圍內。
2. 經當事人書面同意[註1]。
3. 對當事人權益無侵害。

特定目的外……

■第16條-公務機關對個人資料之利用，除第六條第一項所規定資料外，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。但有下列情形之一者，得為特定目的外之利用：

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，且資料經過處理後或依其揭露方式無從識別特定當事人。
6. 有利於當事人權益。
7. 經當事人書面同意[註2]。

註1：第7條-指當事人經蒐集者告知本法所定應告知事項後，所為允許之書面意思表示。

註2：第7條-指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之書面意思表示。

25

沒遵守個人資料保護法，我以及我的公司會被罰則嗎？

本報告之智慧財產權歸屬於法務部

團體訴訟

恐怖的糾團力量...

- 為促進民眾參與個人資料保護事宜及損害發生後方便行使民事賠償權，新法特規定符合一定要件之財團法人或公益社團法人，得代替當事人提起團體訴訟，以節省勞費並保護民眾權益，並定有法院之專屬管轄。(第32-34條)

註：提起訴訟之財團法人或公益社團法人，應符合下列要件：

1.財團法人之登記財產總額達新臺幣一千萬元或社團法人之社員人數達一百人。

2.保護個人資料事項於其章程所定目的範圍內。

3.許可設立三年以上。

27

民事賠償

- 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。(第28條)

  (舉證責任倒置之過失責任)

- 損害賠償總額，以每人每一事件新臺幣五百元以上二萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。(第28條)

  (取決於公務機關對個資的蒐集程度 -> 最小限度蒐集與利用)

- 對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。 (第28條)

- 損害賠償，除依本法規定外，
- 公務機關適用國家賠償法之規定。(第31條)

28

本報告之智慧財產權歸屬於法務部

刑事罰則

第41條

非法蒐集特種資料、違反蒐集,處理,利用、國際傳輸之規定

→ 意圖營利 (非告訴乃論)

→ 足生損害於他人者
- → 2年有期徒刑 20萬元罰金
- → 5年有期徒刑 100萬元罰金

第42條

意圖為自己或第三人不法之利益或損害他人之利益

→ 對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確

→ 足生損害於他人者
- → 5年有期徒刑 100萬元罰金

第44條

公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。

意圖營利及為自己或第三人之利益而損害他人利益者，需負刑事責任，但要注意：就算沒有意圖營利或謀取自身利益，只要違反個資法且足以造成他人損害者，也有可能要負刑事責任喔！

29

我的公司違反個資法的罰則？

民事責任
- 每人每一事件五百元以上二萬元以下計算
- 合計最高可達新台幣兩億元。但因該原因事實所涉利益超過新台幣兩億元者，以該所涉利益為限

不同事件，另外計算！

萬一可證明損失超過兩億，就得賠償對方的損失金額！

行政責任
- 處罰鍰後改正：處新台幣五萬元以上五十萬元以下罰鍰
  - 1.特種個資
  - 2.蒐集或處理個資應有特定目的
  - 3.特定目的外之利用
  - 4.中央主管機關限制國際傳輸之命令或處分
- 限期改正未改正處罰鍰：處新台幣二萬元以上二十萬元以下罰鍰
  - 1.直接及間接蒐集應告知事項
  - 2.有關當事人權利行使之規定
  - 3.個資檔案安全維護計畫

雙罰：非公機關及其代表人、管理人或其他有代表權人

覆巢之下無完卵；老闆有事，大家都遭秧！
自己在職場上也要避免造成公司的違法！

30

本報告之智慧財產權歸屬於法務部

面對新版個人資料保護法，我該如何因應？

個資法疑議及說明 – 彙整說明

個資法的目的

- 為規範個人資料之蒐集、處理及利用，避免人格權受到侵害，並促進個人資料之合理利用，特制定本法。

個資法要求

- 除特種資料以外，並沒有規定哪些資料不能收。
- 它只強調，你想要蒐集或處理個資，就要保護、就要留紀錄；否則就不要拿、不要留；
- 它也沒不准你提供或傳輸個資，但是一樣就是要符合規定並且做好管控，否則，不要傳就沒事了!
- 重點是，這些過程都需要留下紀錄，以作為舉證之用！

32

本報告之智慧財產權歸屬於法務部

怎麼做？

查法令

- 有沒有法令有較鬆的要求？

清個資

- 找出業務範圍內可能有個資的地方

設控管

- 針對有個人資料的部份進行管理的設計

做確實

- 以稽核或教育訓練等方式，確保大家都落實執行

33

同仁現在開始要做什麼準備？

識別業務範圍的法令依據

- 請針對您所負責的業務，整理相關的法令依據及可能之個資檔案，包含：
  - 法令規範可以蒐集的資料(如：員工健康檢查)；
  - 法令規定可以給的資料(如：配合檢警調查)；
  - 法令規定不可刪除的資料(如：離職員工資料的保存年限要求)。

留意個資的流向與管理方式

- 請時時留意您身邊各種可能的個人資料，以及相關的管理方式是否適當，如：
  - 傳真機的資料是否隨時取回；
  - 包含個人資料的紙本是否有適當的銷毀而未被當成回收用紙使用。

34

本報告之智慧財產權歸屬於法務部

最後提醒事項

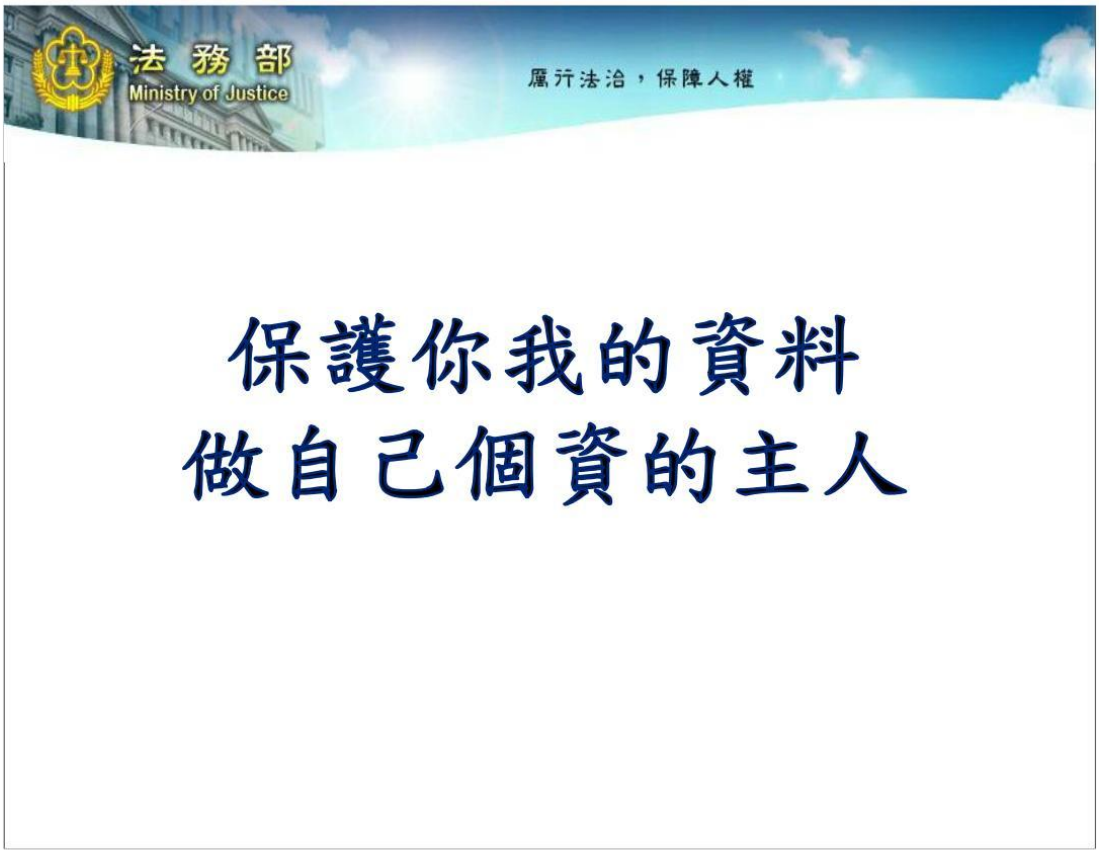
- 經識別的個人資料，都必須評估其風險，並依其風險大小設置對應之安全控管機制，故個資留越多，部處所要花的控管成本將越高。故我們建議...

35

問題與討論

36

本報告之智慧財產權歸屬於法務部



資料來源：本計畫撰寫

本報告之智慧財產權歸屬於法務部

五、民眾認知宣導摺頁

本報告之智慧財產權歸屬於法務部

個資防護多用心，
你我財產有保障！

新版《個人資料保護法》於2010年4月27日立法院院會中完成三讀程序，並於同年5月26日由總統公布。面對社會上層出不窮的個人資料外洩事件，讓更多人意識到個人資料保護的重要性，然而，個資外洩對被害人造成的傷害更是難以想像的，到底，我該如何保護自己的個人資料以免遭到侵害呢？

什麼是個人資料？

個人資料就像是我們申辦郵局帳戶、在網路上購物、或到醫院就診時，留下的諸如姓名、出生年月日、身分證字號等個人專屬資訊。依據《個人資料保護法》第2條，個人資料係指自然人之姓名、出生年月日、身份證號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、基因、性生活、健康檢查、犯罪前科、聯絡方式(如：Email、Facebook、即時通訊軟體帳號等)、財務情況、社會活動，或其他可以直接或間接方式識別個人的各種資料。

哪些個人資料是不得隨意蒐集、處理及利用的？

新版個資法規定，有關**醫療**、**基因**、**性生活**、**健康檢查**及**犯罪前科**這五種個人資料，原則上是不得蒐集、處理或利用的，除非有下列情形：

1.法律明文規定。

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，且有適當安全維護措施。

3.當事人自行公開或其他已合法公開之個人資料。

4.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，且經一定程序所為蒐集、處理或利用之個人資料。

僅有以上四種情形，公務機關或非公務機關才可以蒐集、處理或利用我們的個人資料喔!

個人資料外洩可能產生什麼樣的危害？

雖然個人資料並非像金錢一樣，遺失了會馬上造成財務上的損失，但是，個資外洩所造成的危害恐怕比金錢損失還要嚴重。如果讓不肖分子取得我們的個人資料，很可能會：

1.利用個人資料**仿冒身分**，對我們或我們的親友進行**詐騙及騷擾**。

2.利用個人資料裡的特定組合，進行如**成立人頭帳戶**、**盜取網路帳號密碼**、**公佈個人敏感資料**(如病歷、健康檢查)等不法行為。

3.無故掛失或變更如提款卡等**個人金融及交易工具**的狀態。

如何防範自己的個人資料外洩？

1.不要隨意向陌生的來電者透漏自己的個人資料！

2.如有需要提供自己的個人資料時，應謹慎小心，避免提供過多的資訊，提供資料之前，一定要明確的瞭解下列事項：

(1) 公務機關或非公務機關名稱。
(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) 當事人依第三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，不提供將對其權益之影響。

3.注意自己的錢包，避免遺失重要證件！如有發現不幸遺失證件的情形，應立刻報失！

4.鎖好住宅的信箱，防止信件被盜取，搬家時，也應及早變更寄件地址，避免信件落入不明人士手中！

5.不要為了換取贈品或優惠，而在不明網站上任意提供自己的個人資料！

6.含有個人資料的信件或文件，在使用完畢後，一定要撕碎或銷毀 (如：電費單、刷卡單、就醫資訊)！

資料來源：本計畫撰寫

圖 48：民眾認知宣導摺頁

本報告之智慧財產權歸屬於法務部

六、個人資料保護宣導摺頁說明手冊

公務機關個人資料保護法須知

公務機關個人資料保護原則

我國個資法第1條開宗明義揭示其立法精神為「避免人格權受侵害，並促進個人資料之合理使用」，公務機關基於依法行政及正當程序之要求，對於個人資料之蒐集、處理或利用，應恪遵本法，致力於隱私權保護及資料之合理使用；以下謹就公務機關進行個人資料之蒐集、處理或利用，提出相關重點方針。

關於整體規劃

一、訂定當事人行使權利之處理程序

（1）維護當事人之查詢、閱覽權利
請注意准駁之決定期間及書面通知方式（個資法第10條、第13條第1項）。

（2）維護當事人資料之正確性，並保障其請求更正、補充、停止處理或利用之權利
請注意准駁之決定期間及書面通知方式（個資法第11條、第13條第2項）。

（3）維護當事人請求刪除、停止蒐集、處理或利用該個人資料之權利（個資法第11條第3、4項）。

二、訂定個資蒐集、處理及利用之相關程序。

三、應將特定事項公開於電腦網站，供公眾查詢（個資法第17條）。

四、應指定專人辦理個人資料檔案安全維護事項（個資法第18條）。

公務機關個人資料保護法須知

關於個人資料之蒐集、處理及利用

一、告知義務及蒐集、處理和利用要件

	向當事人蒐集個人資料	個人資料非由當事人提供
告知義務	▲應明確告知當事人個資法第8條第1項。 △但有個資法第8條第2項情形之一者，得免為告知。	▲依個資法第9條第1項，應在「處理或利用前」向當事人告知或「得於首次對當事人為利用時」（個資法第9條第3項）併同對當事人告知： A、個人資料來源（個資法第9條第1項）。 B、個資法第8條第1項第1-5款。 △但有個資法第9條第2項情形之一者，得免為告知。
蒐集、處理要件	▲公務機關對個人資料之蒐集、處理應有「特定目的」（個資法第15條）。	
利用要件	▲公務機關對個人資料之利用，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（個資法第16條本文）。 △屬於個資法第16條但書情形之一者，得為特定目的外之利用。	

二、蒐集、處理和利用時應共同注意事項

（1）特種個人資料之蒐集、處理或利用

A、原則：不得蒐集、處理或利用（個資法第6條本文）
B、例外：個資法第6條但書。

（2）當個人資料蒐集之特定目的消失或期限屆滿時

A、原則：應主動或依當事人之請求，刪除、停止處理或利用該個人資料（個資法第11條第3項本文）。
B、例外：個資法第11條第3項但書。

公務機關違反個資法之告知義務

若致生個人資料被竊取、洩漏、竄改或其他侵害者，公務機關應查明後以適當方式通知當事人（個資法第12條）。

公務機關如何適用個資法
公務機關 個人資料保護法須知

法務部
MINISTRY OF JUSTICE

法務部：
10048 台北市重慶南路一段130號　電話：(02)2314-6871
第二辦公室：
10048 台北市貴陽街一段235號　電話：(02)2316-7000
法務部網站　http://www.moj.gov.tw

台北市敦化南路二段216號22樓
電話：(02) 6631-1000　FAX：(02) 6631-1001
科技法律研究所網站　http://stli.iii.org.tw/

公務機關如何適用個資法
公務機關 個人資料保護法須知

法務部編印

本報告之智慧財產權歸屬於法務部

資料來源：本計畫撰寫

圖 49：個人資料保護宣導摺頁說明手冊

本報告之智慧財產權歸屬於法務部

七、第一年度公務機關個人資料保護專責人員培訓教育之紀錄彙整及成果追踪報告

（一）前言

新版個人資料保護法（以下稱個資法）已於 99 年 4 月 27 日立法院三讀修正通過，並於同年 5 月 26 日由總統正式公布，為確保公務機關個人資料保護機制建置之順利推展，法務部特別委託財團法人資訊工業策進會科技法律研究所，針對公務人員舉辦「公務機關個人資料保護專責人員初階培訓教育訓練」課程，以奠定全國各公務機關個人資料保護專責人員對於個資保護的基礎概念。

本計畫透過教育訓練協助全國各行政單位提升對於個人資料隱私保護的認知及專責人員的能力，降低公務機關保有個人資料之安全風險，並培訓各機關種子講師，以因應機關人員及民眾之諮詢，進而達成因應未來新修正個資法的施行，並減少個資外洩及國家賠償責任發生。統計總培訓公務人員人數達 828 人。

表 42：培訓課程出席人數統計表

日期	場次	地點	培訓人數
10/12 (三)	高雄	國立科學工藝博物館演講廳	176 人
10/17 (一)	台北	台北市公務人力發展中心福華文教會館卓越堂	512 人
10/19 (三)	台中	台中市公務人力訓練中心簡報室	140 人
總計			828 人

資料來源：本計畫活動產出

（二）培訓課程說明

「公務機關個人資料保護專責人員初階培訓教育訓練」課程，主要向公務機關個人資料保護專責人員介紹個人資料保護法的相關規定及其對組織可能產生的衝擊。課程內容將包含個人資料外洩案例分析與個人資料保護法條文簡介，使專責人員瞭解法規之要求並

本報告之智慧財產權歸屬於法務部

具備個人資料保護基本認知。議題主要分為下數各項說明：

1.個人資料安全議題

藉由最近公務機關及非公務機關相關的個資外洩新聞事件的分析，使學員了解個人資料與資料安全與我們的工作與生活息息相關。

2.個人資料保護法簡介

說明新版「個人資料保護法」的修法緣由及進程、個資法施行細則研修方向，使學員清楚瞭解新舊法之間的差異性。

3.總則

說明個人資料的定義、與不得蒐集、處理或利用的資料類型、法律賦予當事人行使的權利、機關受理當事人請求的准駁回覆期限以及向當事人蒐集個人資料時，應明確告知當事人哪些事項等。

4.公務機關對個人資料之蒐集、處理及利用

說明公務機關對個人資料之蒐集、處理及利用在特定目的之內與目的外之規範，以及相關因應措施。

5.非公務機關對個人資料之蒐集、處理及利用

說明非公務機關對個人資料之蒐集、處理及利用在特定目的之內與目的外的規範、相關因應措施、國際傳輸的限制，以及說明中央目的事業主管機關或直轄市、縣（市）政府的行政監督權。

6.損害賠償及團體訴訟

說明舉證責任倒置原則、損害賠償及團體訴訟。

7.罰則

本報告之智慧財產權歸屬於法務部

說明刑罰以及行政罰。

8.附則

說明不適用個資法規定之特定情形（如：單純個人或家庭活動之目的）、間接蒐集資料的告知期限，及逾期未告知的罰則。

9.資訊安全影片欣賞與案例探討

使用行政院國家資通安全會報技術服務中心於 98 年舉辦的資安系列競賽資安動畫金像獎佳作「維護個資鬥陣行」，將個人資料外洩的案例以生動活潑的動畫方式呈現，透過案例的探討，讓學員將課堂上所學習到的個資法新知，應用在影片的情境中。

10.判例探討

以舊版「電腦處理個人資料保護法」法院判例進行探討，一方面幫助學員將個資法的知識學以致用，另一方面從判例中瞭解新舊法之間在判別上的差異性。

11.面對新版個人資料保護法，該如何因應？

分享新版「個人資料保護法」正式施行前，如何準備與因應新法。

12.Q & A 時間

提出個資相關議題與講師進行討論。

（三）活動內容

第一年度「公務機關個人資料保護專責人員培訓教育」已於 100 年 10 月 19 日前於高雄、台北與台中，完成每場 6 小時之培訓教育。

1.初階公務機關個人資料保護專責人員培訓教育「高雄場」

本報告之智慧財產權歸屬於法務部

（1）時間：100 年 10 月 12 日

（2）地點：國立科學工藝博物館演講廳

（3）議程：

表 43：初階高雄場議程

時　　間	議　　題
9:00 ~ 10:20	個人資料安全議題
	個人資料保護法簡介
	總則
10:40 ~ 12:00	公務機關對個人資料之蒐集、處理及利用
	非公務機關對個人資料之蒐集、處理及利用
	損害賠償及團體訴訟
13:00 ~ 14:20	罰則
	附則
	資訊安全影片欣賞與案例探討
14:40 ~ 15:40	判例探討
	面對新版個人資料保護法，該如何因應？
15:40 ~ 16:00	Q & A 時間

資料來源：本計畫活動產出

2.初階公務機關個人資料保護專責人員培訓教育「台北場」

（1）時間：100 年 10 月 17 日

（2）地點：台北市公務人員人力發展中心福華文教會館卓越堂

（3）議程：

表 44：初階台北場議程

時　　間	議　　題
9:00 ~ 10:20	個人資料安全議題
	個人資料保護法簡介
	總則
10:40 ~ 12:00	公務機關對個人資料之蒐集、處理及利用

本報告之智慧財產權歸屬於法務部

	非公務機關對個人資料之蒐集、處理及利用
	損害賠償及團體訴訟
13:00 ~ 14:20	罰則
	附則
	資訊安全影片欣賞與案例探討
14:40 ~ 15:40	判例探討
	面對新版個人資料保護法，該如何因應？
15:40 ~ 16:00	Q & A 時間

資料來源：本計畫活動產出

3.初階公務機關個人資料保護專責人員培訓教育「台中場」

（1）時間：100 年 10 月 19 日

（2）地點：台中市公務人員人力訓練中心簡報室

（3）議程：

表 45：初階台中場議程

時　　間	議　　題
9:00 ~ 10:20	個人資料安全議題
	個人資料保護法簡介
	總則
10:40 ~ 12:00	公務機關對個人資料之蒐集、處理及利用
	非公務機關對個人資料之蒐集、處理及利用
	損害賠償及團體訴訟
13:00 ~ 14:20	罰則
	附則
	資訊安全影片欣賞與案例探討
14:40 ~ 15:40	判例探討
	面對新版個人資料保護法，該如何因應？
15:40 ~ 16:00	Q&A 時間

資料來源：本計畫活動產出

（四）問題整理

本報告之智慧財產權歸屬於法務部

1.個資法法條解釋及名詞定義之提問

Q1：請問機關內公文檔案資料（如陳情案件）是否屬個資法的蒐集？若是陳情人要求刪除個人資料，是否可行？

A1：請先行確認有無相關法律規定，若無不能刪除之相關規定，那就有依當事人的要求刪除資料之必要，若法律有規定則可以依法拒絕。

Q2：影片中阿郎從公司內部取得客戶資料為何不是蒐集？

A2：這個問題應該從個資使用者的角度來看，公司是以公司的立場蒐集資料，行為主體是公司，而阿郎只是公司員工代為蒐集，所以資料蒐集者還是公司。惟個案中阿郎卻對於公司蒐集的個人資料為特地目的外的利用， 這就要受個資法另外的規範。

Q3：為什麼阿郎從 p2p 軟體上蒐集個人資料，不屬於個資法 19 條中的「取自於一般可得之來源」？

A3：一般在 p2p 軟體上搜尋東西時，會假設該來源是願意分享的，而不是不願分享而不小心流出來。依據法律來看，其實從 p2p 軟體上尋得的個人資料是可以歸類於「取自於一般可得之來源」，雖然蒐集過程合法，但是阿郎在後續的利用上面是違法的。

Q4：很多人會把服務放在網路上面（如 google mail），但在這樣的情況下無法得知實際上的資料儲存位置，若資料儲存在國外時，是否適用個資法的國際傳輸？

A4：這個問題暫時沒有一個確切的解答，詳細部分請待施行細則出來後會進一步地給各位一個正確的答案。

Q5：個資法中有分公務機關及非公務機關，例如第八條，請問衛生署所屬的醫院為何者？

A5：這可能要看署立醫院是否算是行政法人，如果是的話就是，如果不是的話就不算公務機關

Q6：個資法第二條第一款的個資種類有一個社會活動，請問這個分類包括那些個資？

本報告之智慧財產權歸屬於法務部

A6：由於新版個資法的施行細則仍在修訂中，因此可能要等公布後才能得知哪些類型之個資將被歸類於社會活動。但是舊版的細則中也有社會活動這一項目，如果各位有興趣可以去參考一下，不過這些項目在新版的細則中可能會有增修。

Q7：個資法第二條第一款的醫療、病例、健康檢查怎麼區分？

A7：這些屬於模糊法律概念的定義仍在細則修訂中，但是之前我們詢問的結果是會根據「醫療法」界定。

2.個案如何適用個資法之提問

Q1：學校教授為學術上的研究（如國科會）需要，要求資訊中心提供學生資料，資訊中心是否有必要提供？如果去識別化的動作交由工讀生進行是否合理？

A1：個資法上規範的「學術研究機構」有一定的定義，學校教授是否屬學術研究機構還要去確認一下。去識別化有兩種做法，一種是在蒐集時就提供去識別化的選項供當事人填寫，另一種做法是在揭露時去識別化。至於學術機關在去識別化這個動作的一些相關規範，主管機關會在後續做出準則規範，可以密切注意。

Q2：保有個資的依據如果寫「依工作職掌」是否合理？

A2：建議應該寫具體一點，因為一般大眾並不知道機關的工作職掌為何。

Q3：是否可以把全部的目的都納入自己機關的特定目的？如果自身的科室有其他科室的人員來駐點進行業務，那在宣告個資事項時是否要把駐點人員的業務範圍一起宣告？

A4：個資法中規範的目的有些適用公務機關、有些適用非公務機關，公務機關只能選跟本身業務有關的目的，雖然新版個資法已經取消了特定目的的登記制，但特定目的仍須向主管機關報備，主管機關有權否決不合理的特定目的。一般來說個資事項的宣告是整個政府機構整體一起宣告的，因此應該會把所有科室的業務範圍都宣告進去，所以不用擔心這個問題。

本報告之智慧財產權歸屬於法務部

Q5：基於資訊安全而在員工電腦裝側錄軟體，請問是否違反個資法？

A5：裝側錄軟體的話有兩個要點，第一個是一定要告知電腦的使用者，通知這台電腦會側錄畫面。再來必須廣泛的側錄每一個使用者，而不能針對特定個人來側錄。

Q6：若某機關的某同仁因使用個人電腦收 EMAIL 而中了木馬病毒，導致擁有的個資遭駭客盜取販售，若受害人提告而產生的刑責或賠償，請問該機關的個資專責人員是否有責任？

A6：責任有分民事、刑事、行政罰三部分，民事責任主要是針對機關本身，有些企業會在受到求償後再轉而向內部員工要求賠償，但那大多是在員工是屬於惡意的狀況下去要求的。再行政罰的部分只針對非公務機關。刑事部分則是針對違法者本人。

Q7：請問本單位對外網站上列有所有員工的姓名、EMAIL、辦公室電話、照片，如果已有告知員工的話，是否還有資安的疑慮？

A7：要先確定提供這些資料的目的是甚麼，是否是在單位的業務範圍之內，因為政府公開資訊法有規定必須提供必要資訊，但是否有必要提供到那麼多那麼細，可能要確認一下是否在目的範圍內。建議即使告知員工仍然要取得同意較好。

Q8：請問若為公務需要，擬製作員工或其他附屬單位人員聯絡簿或通訊錄，是否可全面散發？如該手冊不慎遺失，被人冒用，有無法律責任？另有員工不願意提供公開，是否無法強制要求公開？

A8：首先確認一下是否有這個必要，全面散發又是多全面？如果有在特定目的之內，又有取得當事人同意，那基本上是沒有問題的。

Q9：請問機關秘書單位檔案管理人員負責將各內部業務單位辦理完成之卷宗歸檔，通常情形下檔案管理人員並不知悉卷宗內容，而且卷宗數量龐大，是否有必要公開所持有個資名稱於網路？

A9：因為一般來說，機關內的個資盤點是以整個機關來看，而不是內部的單一業務來看，因此在他進來歸檔之前，機關內的其他業務單位仍會知道卷宗的內容，因此仍須盡法令上規定的義務。

本報告之智慧財產權歸屬於法務部

Q10：因公務而取得之姓名、身分證、出生年月日等資料，在使用完後是否可以留存，以供下次使用，以減少重複詢問之麻煩，或將檔案轉交同事使用？

A10：依法令來看，特定目的消失後必須主動或「依當事人要求」刪除，因此可以等當事人要求再刪除。若當事人未要求則不須「依當事人要求」刪除。

Q11：請問民間企業之「公司資料」(如進出口、外匯資料）是否屬於個資法保護的範圍？

A11：個資法保護的是自然人的資料，企業屬於「法人」，因此其資料不在保護範圍內，但如果是企業負責人等的自然人資料仍在保護範圍內。

Q12：檢警單位要求調閱電腦 IP/電郵等資料，請問這些資料是否屬於個人資料的範圍？如果這些用途不包含於當初的特定目的，是否需要經過當事人的同意才能提供給檢調機關？

A12：電子郵件算是個人資料，雖然新版個資法的個人資料類別仍在修訂中，但這些資料在舊版的法令中都已經列屬於個人資料的範圍。檢警單位如果是為了行使公務需要，因為是依法有據，一般情況下都有必要提供，如果通知當事人可能會造成一些違反如偵查不公開的原則，我們會建議一般不管是公務機關或非公務機關都盡量配合檢警的要求，但這種提供也不是漫無目的、無限制地提供，因此遇到這種情形時請檢調單位務必正式來函索取，程序上較無問題，也可以留下紀錄，而內部在產生提供給檢調單位的文件時的過程也務必留下紀錄

Q13：請問會議的簽名冊算是個人資料嗎？

A13：姓名是個人資料，姓名的集合當然也是個人資料，這個問題衍生下去的議題就是這些個資是否需要保護？這可能就要視這些資料如果洩漏是否會「足產生損害他人之事情」發生而定。

3.針對個資法相關參考資源之提問

本報告之智慧財產權歸屬於法務部

Q1：個人資料保護法上中央主關機關之函釋或司法判法或解釋是否有公告，或可在法條為索引找到以資參考與分享？

A1：法務部有出版一本「電腦處理個人資料保護法解釋彙編」，是舊版電腦個資法施行期間的解釋函彙總，也有更新到部分新版個資法的內容，可以在法務部的網站下載電子檔以供參考。

（五）教育訓練課程意見調查統計結果

法務部為瞭解第一年度北區（台北市）、中區（台中市）、南區（高雄市）3 場教育訓練課程規劃、講師表現、行政服務以及教學方式是否符合學員的期望及需求，發放意見回饋表調查學員對於本次教育訓練的活動的滿意度，並希望能藉由學員回饋的意見，有效管理及提升後續的教育訓練課程品質。3 場教育訓練課程總共發放 828 份意見回饋表，回收 515 份，回收率為 62.20%。

表 46：初階教育訓練意見調查表回收統計表

日期	場次	實際報到人數	問卷回收數量	回收率
10/12 (三)	高雄場	176 人	114 份	64.77%
10/17 (一)	台北場	512 人	306 份	59.77%
10/19 (三)	台中場	140 人	95 份	67.86%
總計		828 人	515 份	62.20%

資料來源：本計畫活動產出

1.初階高雄場意見回饋表統計結果

高雄場教育訓練課程總共有 176 人參加，總共發放 176 份意見回饋表，回收 114 份，回收率為 64.77%。

有關當日課程的整體看法，很滿意佔 22.15%，滿意佔 63.82%，普通佔 12.55%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達

本報告之智慧財產權歸屬於法務部

98.52%。

有關講師表現的看法，很滿意佔 24.68%，滿意佔 62.97%，普通佔 11.46%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 99.11%。

有關行政服務的看法，很滿意佔 19.82%，滿意佔 59.01%，普通佔 18.47%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 97.3%以上。

表 47：初階高雄場課程、講師、行政意見回饋表統計結果

	很滿意	滿意	普通	不滿意	很不滿意
對今日課程的整體看法	22.15%	63.82%	12.55%	1.18%	0.29%
對講師表現的看法	24.68%	62.97%	11.46%	0.89%	0.00%
對行政服務	19.82%	59.01%	18.47%	1.35%	1.35%

資料來源：本計畫活動產出

表 48：初階高雄場教學方式意見回饋表統計結果

	過多	剛好	過少	不適用
此教育訓練課程使用之教學方式	3.18%	82.30%	9.78%	4.74%

資料來源：本計畫活動產出

2.初階台北場意見回饋表統計結果

台北場教育訓練課程總共有 512 人參加，總共發放 512 份意見回饋表，回收 306 份，回收率為 59.77%。

有關當日課程的整體看法，很滿意佔 18.29%，滿意佔 65.22%，普通佔 14.79%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 98.3%。

本報告之智慧財產權歸屬於法務部

有關講師表現的看法，很滿意佔 29.36%，滿意佔 63.34%，普通佔 6.96%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 99.66%。

有關行政服務的看法，很滿意佔 18.24%，滿意佔 59.20%，普通佔 17.08%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 94.52%。

表 49：初階台北場課程、講師、行政意見回饋表統計結果

	很滿意	滿意	普通	不滿意	很不滿意
對今日課程的整體看法	18.29%	65.22%	14.79%	1.15%	0.55%
對講師表現的看法	29.36%	63.34%	6.96%	0.20%	0.13%
對行政服務	18.24%	59.20%	17.08%	2.99%	2.49%

資料來源：本計畫活動產出

表 50：初階台北場教學方式意見回饋表統計結果

	過多	剛好	過少	不適用
此教育訓練課程使用之教學方式	2.37%	82.91%	6.31%	8.39%

資料來源：本計畫活動產出

3.初階台中場活動意見回饋表統計結果

台中場教育訓練課程總共有 140 人參加，總共發放 140 份意見回饋表，回收 95 份，回收率為 67.86%。

有關當日課程的整體看法，很滿意佔 11.80%，滿意佔 59.87%，普通佔 22.17%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 93.84%。

有關講師表現的看法，很滿意佔 23.37%，滿意佔 56.63%，普通

本報告之智慧財產權歸屬於法務部

佔 17.05%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 97.05%。

有關行政服務的看法，很滿意佔 16.56%，滿意佔 55.08%，普通佔 24.61%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 96.25%。

表 51：初階台中場 課程、講師、行政見回饋表統計結果

	很滿意	滿意	普通	不滿意	很不滿意
對今日課程的整體看法	11.80%	59.87%	21.17%	3.70%	2.46%
對講師表現的看法	23.37%	56.63%	17.05%	1.89%	1.05%
對行政服務	16.56%	55.08%	24.61%	2.68%	1.07%

資料來源：本計畫活動產出

表 52：初階台中場教學方式意見回饋表統計結果

	過多	剛好	過少	不適用
此教育訓練課程使用之教學方式	0.55%	81.03%	12.33%	6.09%

資料來源：本計畫活動產出

4.教育訓練活動意見回饋表建議彙整結果

（1）個資法立法

建議個資法不必訂定當事人得請求閱覽、刪除、更正等權利，如立法目的在於保護個人資料正當依法使用，防止外洩到不肖人士手中，建議只明訂意圖濫用個資以獲取不當利益的人刑責。

（2）課程內容

A. 建議增加公務機關內部單位互相使用對方蒐集資個資，在

本報告之智慧財產權歸屬於法務部

適用個資法時，有哪些應注意的地方（互相使用仍是為公務上之目的，僅是為了免除再去蒐集彙整之麻煩），並增設控管之具體執行方式。

B. 建議蒐集公務機關普遍關心之議題深入介紹，尤其是專責人員應有之責任及工作內容。

C. 建議增加各界見解不同或爭議部分，以及講述主管機關（或法務部）之見解或傾向。

D. 建議本訓練課程對個資有明確了解，希望能很快有進階課程以因應業務需求，後續課程也應該對實際上的安全流程控管做更實際性、細節的說明。

（3）講義編寫

A. 建議放置個資法全部條文於教材中。

B. 講義字體過淡且過小，建議放大字體，或將投影片增加至頁面 2/3 部分。

C. 建議提供講義電子檔。

D. 建議將授課內容攝影成光碟，可提供各機關辦理教育訓練，擴大個資法宣導。

（4）報名報到等行政事宜

A. 台北場次參加人員過多，導致部分議題無法作細部討論，建議加開場次解決此問題。

B. 建議增開上課梯次，讓更多相關人員可以參與訓練。

C. 由於會場人數眾多，導致報到太過於耗時，建議報到及發放便當等行政作業應再善加規劃。

（5）建議講師課程進行

本報告之智慧財產權歸屬於法務部

A. 建議增加法規講解。

B. 建議講師若能將法規以樹狀圖等有脈絡的方式來開場會有更好之學習效果及課程發展。

C. 建議應逐條詳細說明及舉例，並配合罰則說明。

（6）實例說明之建議

A. 建議多了解課程與公務部門關聯性，舉相關公務機關例子。

B. 建議資料盤點可以以實例為操作，不能雖說資料盤點很重要卻不知如何盤點才是適當的。

C. 希望能在課程中增加案例 Q&A 之腦力激盪。

（7）課程時間之建議

A. 建議專業內容可分為上下場次，專業內容過多稍嫌負擔過重，講師應配合議程上下課。

B. 可增加上課時間。

（六）結語

為使公務人員對於個人資料保護法的了解與應用，以及協助公務機關個人資料專責人員對於個人資料管理政策之遵循，舉辦初階人才培訓課程，學員踴躍參與課程，並於課程中與講師進行良好互動。除了本次辦理的初階培訓教育訓練課程外，後續也將持續配合設計中階及進階等不同層次的課程。

（七）初階公務機關個資保護專責人員培訓簡報（詳見本報告第 525-570 頁）。

（八）初階公務機關個資保護專責人員培訓台北場、台中場、高雄場簽到表（因簽到表內含有參與人員之個人資料，故在此予以移除，詳細簽到資料已附於呈繳法務部之「第一年度公務機關個人資料保護專責人

本報告之智慧財產權歸屬於法務部

員培訓教育之紀錄彙整及成果追踪報告」)。

（九）初階公務機關個資保護專責人員培訓台北場、台中場、高雄場照片集

資料來源：本計畫活動拍攝

圖 50：中區教育訓練課程於台中公務人力發展中心七樓簡報室舉行

資料來源：本計畫活動拍攝

圖 51：法務部法律事務司鍾瑞蘭副司長為學員致詞

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 52：勤業眾信聯合會計師事務所游靖芬副理擔任講師

資料來源：本計畫活動拍攝

圖 53：學員參加狀況踴躍

本報告之智慧財產權歸屬於法務部

八、第二年度公務機關個人資料保護專責人員培訓教育之紀錄彙整及成果追踪報告

（一）前言

經濟合作暨發展組織(Organisation for Economic Cooperation and Development, OECD)、亞太經濟合作會議 （Asia-Pacific Economic Cooperation, APEC）等國際組織及歐盟自 1980 年代起，陸續加強隱私保護原則之訂定，法務部也順應國際發展趨勢，自民國 90 年起便針對「電腦處理個人資料保護法」提出修正。立法院已於民國 99 年 4 月 27 日三讀通過「個人資料保護法（以下稱個資法）」，細則草案也於 100 年完成預告，為確保公務機關個人資料保護機制建置之順利推展，法務部特別委託財團法人資訊工業策進會科技法律研究所，針對公務人員舉辦「公務機關個人資料保護專責人員培訓教育訓練」系列課程，希冀透過教育訓練協助各行政單位提升對於個人資料隱私保護的認知及專責人員的能力，使專責人員能協助公務機關符合個人資料保護法法規遵循的義務，並進一步宣導「個人資料保護執行管理暨考核作業手冊」，提供公務機關建置個人資料風險認知與管理的範本，以及個資保護事務實作的程序，以協助各級公務機關建立標準流程與考核作業，進而達成因應未來新修正個資法的施行並減少個資外洩及國家賠償責任之發生。第二年度培訓教育統計報名情況踴躍，總培訓人數達 554 人。

表 53：第二年度培訓課程出席人數統計表

日期	場次	地點	培訓人數
初階培訓			
100/12/19（一）	花蓮	花蓮市市公所三樓簡報室	89 人
中階培訓			
101/02/29（三）	台中	台中市公務人力發展中心七樓視聽教室	36
101/03/07（三）	台北	台大法學院澤霖館 1 樓國際會議廳	172
101/03/09（五）	高雄	國立科學工藝博物館 S203 研習教室	54
101/03/14（三）	花蓮	花蓮縣文化局文化電影院	28
小計			290 人
進階培訓			

本報告之智慧財產權歸屬於法務部

101/03/21（三）	台北	台中市公務人力發展中心七樓視聽教室	93
101/03/28（三）	台中	台大法學院澤霖館 3 樓多媒體教室	22
101/04/06（五）	高雄	國立科學工藝博物館 S107 研習教室	44
101/04/11（三）	花蓮	花蓮縣文化局文化電影院	16
小計			175 人

資料來源：由資策會科法所製作

（二）培訓課程說明

第二年度「公務機關個人資料保護專責人員培訓教育訓練」課程，主要分為初階東部場；中階北部場、中部場、南部場、東部場；進階北部場、中部場、南部場、東部場，培訓課程主要分為下列各項內容：

1.初階公務機關個人資料保護專責人員培訓教育訓練

課程內容包含個人資料外洩案例分析與個人資料保護法條文簡介，使專責人員瞭解法規之要求並具備個人資料保護基本認知。

首先整理了一些近年來公務機關及非公務機關相關的個資外洩新聞事件，透過新聞事件的分析，讓學員作為工作上的借鏡，並引以為戒，同時，也讓學員瞭解，個人資料安全不僅僅是與其工作上的議題，更與我們的生活息息相關。

接著個人資料保護法簡介說明新版「個人資料保護法」的修法緣由及進程、個資法施行細則研修方向，讓學員清楚瞭解新舊法之間的差異性。先就總則說明個人資料的定義、那些個人資料不得蒐集、處理或利用、個資法賦予當事人行使的權利、機關受理當事人請求的准駁回覆期限以及向當事人蒐集個人資料時，應明確告知當事人哪些事項等。

繼續下探公務機關對個人資料之蒐集、處理及利用在特定目的之內、外的規範以及相關的對應措施，以及在特定目的之內、外的規範、相關的對應措施、國際傳輸的限制以及說明中央目的事業主管機關或直轄市、縣(市)政府的行政監督權。接續為損害賠償及團體訴訟部分，

本報告之智慧財產權歸屬於法務部

說明舉證責任倒置原則、損害賠償及團體訴訟等部分。

最後，內容說明刑罰以及行政罰，以及附則，內容說明那些情形(如：單純個人或家庭活動之目的)不適用於個資法的規定、間接蒐集資料的告知期限及逾期未告知的罰則。再輔以放映行政院國家資通安全會報技術服務中心於 98 年舉辦的資安系列競賽資安動畫金像獎佳作「維護個資鬥陣行」，將個人資料外洩的案例以生動活潑的動畫方式呈現，透過案例的探討，讓學員將課堂上所學習到的個資法新知，應用在影片的情境中。

在判例探討部分，以舊版「電腦處理個人資料保護法」的真實法院判例來進行探討，一方面，幫助學員將個資法的知識學以致用，另一方面，從判例中也可以瞭解新舊法之間在判別上的差異性，無形中，加深學員對於新法的印象，以及面對新版個人資料保護法，該如何因應。介紹個人資料保護法的相關規定及其對組織可能產生的衝擊。

2.中階公務機關個人資料保護專責人員培訓教育訓練

中階課程以個人資料保護管理實務上 PDCA 的相關作法與原則，使專責人員瞭解單位如何善盡良善管理責任。並介紹與宣導「個人資料保護執行程序暨考核作業手冊」重要內容，藉此落實執行個人資料保護業務。提供「BS 10012」與「JISQ-15001」等國際個人資料保護標準之原則與方法，提供學員強化資料之安全維護的概念。

課程先行介紹個人資料保護管理實務上 PDCA「Plan（計畫）→Do（執行）→Check（查核）→Act（改善）」的相關作法與原則，說明個人資訊管理系統 PDCA 循環的整體過程，同時，透過對個人資料保護法的分析，讓學員瞭解新法對於組織會造成那些影響點與風險，並從個人資料保護對組織的影響，導引至管理實務上 PDCA 的相關作法與原則，讓學員清楚瞭解，整個個人資料保護要透過不斷地 PDCA 進行管理流程的循環。

接續國際標準，先介紹「BS 10012」個人資料管理系統　本章特別說明英國「BS 10012」個人資料管理系統。有關「管理系統」建立的標準，也是導入 PDCA 循環的概念，對於推動個人資料保護之組

本報告之智慧財產權歸屬於法務部

織、法制及配套措施等皆可提供實務上的參考，亦能與國際 ISO 標準規範接軌。下午課程介紹「JISQ-15001」個人資料保護管理系統指引，本章特別安排介紹「JISQ-15001」個人資料保護管理系統指引，讓學員可以參考日本等國際間相關的管理制度。

最後，就法務部委託財團法人資訊工業策進會編製的「個人資料保護執行管理暨考核作業手冊」的介紹與宣導，以作為公務機關執行個人資料保護的參考依據。

3.進階公務機關個人資料保護專責人員培訓教育訓練

進階課程主要介紹對個人資料之定義、蒐集與製作個人資料清冊之執行方法，並透過 Workshop 方式使專責人員於課堂練習執行，以協助後續辨識各行政單位所擁有之個人資料。近一步，透過 Workshop 方式使專責人員了解與熟悉衝擊分析執行方式；最後，以實例說明，實務上需啟動個人資料侵害事故之緊急應變計畫之條件與情境介紹以及計畫內容，並透過 Workshop 方式使專責人員了解單位於相關事故發生時應具備之角色與權責。

個人資料檔案蒐集首先向學員說明為何要蒐集個人資料檔案清冊，以及在組織中那些資料屬於個人資料的範圍，最後向學員說明整個個人資料檔案清冊的架構。配合主題，由講師親自帶領學員，透過實作的方式，將「公務人員退休流程」實際繪製成個人資料流程圖，讓學員透過個人資料流程圖，可以清楚且明顯的判別出，到底那些資料是必須記錄於個人資料檔案清冊中的。

接續，在個資管理衝擊分析，介紹風險評鑑的概論，以及風險評鑑的執行方式，最後說明風險評鑑與衝擊分析之間的關係，讓學員可以清楚瞭個人資料在風險評鑑與衝擊分析的概念。並配合個資管理衝擊分析主題進行練習，透過實作的方式，讓學員自行定義個人資料的價值、弱點以及威脅項目，透過現場腦力激盪的方式，讓學員可以依據不同的狀況，建立出符合其業務性質的風險評鑑及衝擊分析的方式。

最後，個資侵害事故應變部分，以公務機關個資外洩的新聞事件為例，透過新聞事件的分析，說明發生個人資料外洩事件時，組織內

本報告之智慧財產權歸屬於法務部

部應有的緊急應變程序，以及應具備的相關機制及文件，讓學員瞭解，當組織不慎遇到個資外洩事件時，該如何將該事件對組織可能造成的傷害降到最低。並以公務機關個資外洩的真實新聞事件為例，讓學員自行分析，在不同的單位以及角度上，面對個資外洩事件，分別應如何應變。

（三）活動內容

第二年度「公務機關個人資料保護專責人員培訓教育」已於 101 年 04 月 11 日於完成每場 6 小時之初階課程東部場；中階課程北部、中部、南部、東部場；進階課程北部、中部、南部、東部場之培訓教育。

1.初階公務機關個人資料保護專責人員培訓教育花蓮場

（1）時間：100 年 12 月 19 日

（2）地點：花蓮市市公所三樓簡報室

（3）議程：

表 54：初階花蓮場議程

時間	議題
9:00 ~ 10:20	長官致詞
	個人資料安全議題
	個人資料保護法簡介
	總則
10:40 ~ 12:00	公務機關對個人資料之蒐集、處理及利用
	非公務機關對個人資料之蒐集、處理及利用
	損害賠償及團體訴訟
13:00 ~ 14:20	罰則
	附則
	資訊安全影片欣賞與案例探討
14:40 ~ 15:40	判例探討
	面對新版個人資料保護法，該如何因應？

本報告之智慧財產權歸屬於法務部

15:40 ~ 16:00	Q & A 時間

資料來源：本計畫活動產出

2.中階公務機關個人資料保護專責人員培訓教育台中場

（1）時間：101 年 02 月 29 日

（2）地點：台中市公務人力發展中心七樓視聽教室

（3）議程：

表 55：中階台中場議程

時間	議程
09：00~09：10	長官致詞
09：10~10：20	個人資料保護管理實務上 PDCA 的相關作法與原則
	介紹「BS 10012」個人資料管理系統
10：20~10：40	休息時間
10：40~12：00	介紹「BS 10012」個人資料管理系統
12：00~13：00	午餐時間
13：00~14：00	介紹「JISQ-15001」個人資料保護管理系統指引
14：00~14：20	休息時間
14：20~15：40	個人資料保護執行管理暨考核作業手冊介紹
15：40~16：00	Q&A 時間

資料來源：本計畫活動產出

3.中階公務機關個人資料保護專責人員培訓教育台北場

（1）時間：101 年 03 月 07 日

（2）地點：台大法學院霖澤館 1 樓國際會議廳

（3）議程：

表 56：中階台北場議程

時間	議程

本報告之智慧財產權歸屬於法務部

09：00~09：10	長官致詞
09：10~10：20	個人資料保護管理實務上 PDCA 的相關作法與原則
	介紹「BS 10012」個人資料管理系統
10：20~10：40	休息時間
10：40~12：00	介紹「BS 10012」個人資料管理系統
12：00~13：00	午餐時間
13：00~14：00	介紹「JISQ-15001」個人資料保護管理系統指引
14：00~14：20	休息時間
14：20~15：40	個人資料保護執行管理暨考核作業手冊介紹
15：40~16：00	Q&A 時間

資料來源：本計畫活動產出

4.中階公務機關個人資料保護專責人員培訓教育高雄場

（1）時間：101 年 03 月 09 日

（2）地點：國立科學工藝博物館 S203 研習教室

（3）議程：

表 57：中階高雄場議程

時間	議程
09：00~09：10	長官致詞
09：10~10：20	個人資料保護管理實務上 PDCA 的相關作法與原則
	介紹「BS 10012」個人資料管理系統
10：20~10：40	休息時間
10：40~12：00	介紹「BS 10012」個人資料管理系統
12：00~13：00	午餐時間
13：00~14：00	介紹「JISQ-15001」個人資料保護管理系統指引
14：00~14：20	休息時間
14：20~15：40	個人資料保護執行管理暨考核作業手冊介紹
15：40~16：00	Q&A 時間

資料來源：本計畫活動產出

5.中階公務機關個人資料保護專責人員培訓教育花蓮場

本報告之智慧財產權歸屬於法務部

（1）時間：101 年 03 月 14 日

（2）地點：花蓮縣文化局文化電影院

（3）議程：

表 58：中階花蓮場議程

時間	議程
09：00~09：10	長官致詞
09：10~10：20	個人資料保護管理實務上 PDCA 的相關作法與原則
	介紹「BS 10012」個人資料管理系統
10：20~10：40	休息時間
10：40~12：00	介紹「BS 10012」個人資料管理系統
12：00~13：00	午餐時間
13：00~14：00	介紹「JISQ-15001」個人資料保護管理系統指引
14：00~14：20	休息時間
14：20~15：40	個人資料保護執行管理暨考核作業手冊介紹
15：40~16：00	Q&A 時間

資料來源：本計畫活動產出

6.進階公務機關個人資料保護專責人員培訓教育台北場

（1）時間：101 年 03 月 21 日

（2）地點：台大法學院霖澤館 3 樓多媒體教室

（3）議程：

表 59：進階台北場議程

時間	議程
09：00~09：10	長官致詞
09：10~10：10	個人資料檔案蒐集
10：10~10：30	休息時間
10：30~11：00	個人資料檔案蒐集 - 練習時間
11：00~12：00	個資管理衝擊分析
12：00~13：00	午餐時間

本報告之智慧財產權歸屬於法務部

13：00~13：30	個資管理衝擊分析 - 練習時間
13：30~14：40	個資侵害事故應變
14：40~15：00	休息時間
15：00~15：40	個資侵害事故應變 - 練習時間
15：40~16：00	Q&A 時間

資料來源：本計畫活動產出

7.進階公務機關個人資料保護專責人員培訓教育台中場

（1）時間：101 年 03 月 28 日

（2）地點：台中市公務人力發展中心七樓視聽教室

（3）進階議程：

表 60：進階台中場議程

時間	議程
09：00~09：10	長官致詞
09：10~10：10	個人資料檔案蒐集
10：10~10：30	休息時間
10：30~11：00	個人資料檔案蒐集 - 練習時間
11：00~12：00	個資管理衝擊分析
12：00~13：00	午餐時間
13：00~13：30	個資管理衝擊分析 - 練習時間
13：30~14：40	個資侵害事故應變
14：40~15：00	休息時間
15：00~15：40	個資侵害事故應變 - 練習時間
15：40~16：00	Q&A 時間

資料來源：本計畫活動產出

8.進階公務機關個人資料保護專責人員培訓教育高雄場

（1）時間：101 年 04 月 06 日

（2）地點：國立科學工藝博物館 S107 研習教室

本報告之智慧財產權歸屬於法務部

（3）議程：

表 61：進階高雄場議程

時間	議程
09：00~09：10	長官致詞
09：10~10：10	個人資料檔案蒐集
10：10~10：30	休息時間
10：30~11：00	個人資料檔案蒐集 - 練習時間
11：00~12：00	個資管理衝擊分析
12：00~13：00	午餐時間
13：00~13：30	個資管理衝擊分析 - 練習時間
13：30~14：40	個資侵害事故應變
14：40~15：00	休息時間
15：00~15：40	個資侵害事故應變 - 練習時間
15：40~16：00	Q&A 時間

資料來源：本計畫活動產出

9.進階公務機關個人資料保護專責人員培訓教育花蓮場

（1）時間：101 年 04 月 11 日

（2）地點：花蓮縣文化局文化電影院

（3）議程：

表 62：進階花蓮場議程

時間	議程
09：00~09：10	長官致詞
09：10~10：10	個人資料檔案蒐集
10：10~10：30	休息時間
10：30~11：00	個人資料檔案蒐集 - 練習時間
11：00~12：00	個資管理衝擊分析
12：00~13：00	午餐時間
13：00~13：30	個資管理衝擊分析 - 練習時間
13：30~14：40	個資侵害事故應變

本報告之智慧財產權歸屬於法務部

14：40~15：00	休息時間
15：00~15：40	個資侵害事故應變 - 練習時間
15：40~16：00	Q&A 時間

資料來源：本計畫活動產出

（四）教育訓練課程意見調查統計結果

為了解第二年度初階（花蓮場）、中階（台北場、台中場、高雄場、以及花蓮場)，以及進階（台北場、台中場、高雄場、以及花蓮場)， 9 場教育訓練課程規劃、講師表現、行政服務以及教學方式是否符合學員的期望及需求，活動現場發意見回饋表調查學員對於本次教育訓練的活動的滿意度，並希望能藉由學員回饋的意見，有效管理及提升後續的教育訓練課程品質。9 場教育訓練課程總共發放 554 份意見回饋表，回收 336 份，回收率為 60.65%。

表 63：第二年度教育訓練意見調查表回收統計表

等級	日期	場次	實際報到人數	問卷回收數量	回收率
初階	04/11 (三)	東區（花蓮場）	89 人	36 人	40.04%
中階	02/29 (三)	中區（台中市）	36 人	28 人	77.78%
	03/07 (三)	北區（台北市）	172 人	100 人	58.14%
	03/09 (五)	南區（高雄市）	54 人	39 人	72.22%
	03/14 (三)	東區（花蓮場）	28 人	17 人	60.71%
進階	03/21 (三)	北區（台北市）	93 人	53 人	56.99%
	03/28 (三)	中區（台中市）	22 人	19 人	86.36%
	04/06 (五)	南區（高雄市）	44 人	31 人	70.45%
	04/11 (三)	東區（花蓮場）	16 人	13 人	81.25%
		總計	554 人	336 份	60.65%

資料來源：本計畫活動產出

1.各場次意見回饋表統計結果

（1）初階花蓮場意見回饋表統計結果

本報告之智慧財產權歸屬於法務部

初階花蓮場培訓訓練課程總共有 89 人報名，總共發放 89 份意見回饋表，回收 36 份，回收率為 40.04%。

有關對於當日課程的整體看法，很滿意佔 26.54%，滿意佔 50.24%，普通佔 21.80%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 98.58%。

講師表現的看法，很滿意佔 34.64%，滿意佔 59.78%，普通佔 5.59%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 100%。

有關對於行政服務的看法，很滿意佔 27.94%，滿意佔 58.82%，普通佔 13.24%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 100%。

表 64：初階花蓮場滿意度回饋表統計結果

	很滿意	滿意	普通	不滿意	很不滿意
整體看法	26.54%	50.24%	21.80%	1.42%	0.00%
講師表現	34.64%	59.78%	5.59%	0.00%	0.00%
行政服務	27.94%	58.82%	13.24%	0.00%	0.00%

資料來源：本計畫活動產出

表 65：初階花蓮場教學方式回饋表統計結果

	過多	剛好	過少	不適用
教學方式	7.7.8%	79.64%	10.78%	1.80%

資料來源：本計畫活動產出

（2）中階台中場意見回饋表統計結果

本報告之智慧財產權歸屬於法務部

中階台中場教育訓練課程總共有 36 人報名，總共發放 36 份意見回饋表，回收 28 份，回收率為 77.78%。

有關對於當日課程的整體看法，很滿意佔 7.78%，滿意佔 56.89%，普通佔 31.14%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 95.81%。

有關對於第一位講師表現的看法，很滿意佔 7.14%，滿意佔 62.86%，普通佔 27.86%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 97.86%。對於第二位講師表現的看法，很滿意佔 21.54%，滿意佔 65.38%，普通佔 10.77%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 97.69%。

有關對於行政服務的看法，很滿意佔 17.86%，滿意佔 57.14%，普通佔 23.21%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 98.21%以上。

表 66：中階台中場滿意度回饋表統計結果

	很滿意	滿意	普通	不滿意	很不滿意
整體看法	7.78%	56.89%	31.14%	2.99%	1.20%
第一位講師表現	7.14%	62.86%	27.86%	1.43%	0.71%
第二位講師表現	21.54%	65.38%	10.77%	1.54%	0.77%
行政服務	17.86%	57.14%	23.21%	0.00%	1.79%

資料來源：本計畫活動產出

表 67：中階台中場教學方式回饋表統計結果

本報告之智慧財產權歸屬於法務部

	過多	剛好	過少	不適用
教學方式	11.00%	52.00%	23.00%	14.00%

資料來源：本計畫活動產出

（3）中階台北場意見回饋表統計結果

中階台北場教育訓練課程總共有 172 人報名，總共發放 172 份意見回饋表，回收 100 份，回收率為 58.14%。

有關對於當日課程的整體看法，很滿意佔 21.11%，滿意佔 62.31%，普通佔 14.57%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 97.99%。

有關對於講師表現的看法，很滿意佔 27.05%，滿意佔 61.12%，普通佔 9.82%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 98%。

有關對於財團法人資訊工業策進會講師表現的看法，很滿意佔 35.53%，滿意佔 58.51%，普通佔 5.53%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 99.57%。

有關對於行政服務的看法，很滿意佔 23.23%，滿意佔 65.66%，普通佔 10.61%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 99.49%以上。

表 68：中階台北場滿意度回饋表統計結果

	很滿意	滿意	普通	不滿意	很不滿意

本報告之智慧財產權歸屬於法務部

整體看法	21.11%	62.31%	14.57%	1.84%	0.17%
第一位講師表現	27.05%	61.12%	9.82%	1.40%	0.60%
第二位講師表現	35.53%	58.51%	5.53%	0.21%	0.21%
行政服務	23.23%	65.66%	10.61%	0.51%	0%

資料來源：本計畫活動產出

表 69：中階台北場教學方式回饋表統計結果

	過多	剛好	過少	不適用
教學方式	3.00%	62.00%	19.00%	16.00%

資料來源：本計畫活動產出

（4）中階高雄場意見回饋表統計結果

中階高雄場教育訓練課程總共有 54 人報名，總共發放 54 份意見回饋表，回收 39 份，回收率為 72.22%。

有關對於當日課程的整體看法，很滿意佔 32.91%，滿意佔 48.29%，普通佔 17.09%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 98.29%。

有關對於第一位講師表現的看法，很滿意佔 36.92%，滿意佔 51.79%，普通佔 7.69%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 96.41%。有關對於第二位講師表現的看法，很滿意佔 55.15%，滿意佔 42.78%，普通佔 2.06%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 100%。

有關對於行政服務的看法，很滿意佔 35.90%，滿意佔

本報告之智慧財產權歸屬於法務部

46.15%，普通佔 17.95%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 100%。

表 70：中階高雄場滿意度回饋表統計結果

	很滿意	滿意	普通	不滿意	很不滿意
整體看法	32.91%	48.29%	17.09%	1.71%	0%
第一位講師表現	36.92%	51.79%	7.69%	3.59%	0%
第二位講師表現	55.15%	42.78%	2.06%	0%	0%
行政服務	35.90%	46.15%	17.95%	0%	00%

資料來源：本計畫活動產出

表 71：中階高雄場教學方式回饋表統計結果

	過多	剛好	過少	不適用
教學方式	4.00%	66.00%	16.00%	14.00%

資料來源：本計畫活動產出

（5）中階花蓮場意見回饋表統計結果

東區(花蓮場)中階教育訓練課程總共有 28 人報名，總共發放 28 份意見回饋表，回收 17 份，回收率為 60.71%。

有關對於當日課程的整體看法，很滿意佔 32.35%，滿意佔 54.90%，普通佔 11.76%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 99.02%。

有關對於第一位講師表現的看法，很滿意佔 50%，滿意佔 48.75%，普通佔 1.25%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 100%。有關對於第二位講師表現的看法，很滿意佔 46%，滿意佔 52%，普通佔 2%，由

本報告之智慧財產權歸屬於法務部

整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 100%。

有關對於行政服務的看法，很滿意佔 34.38%，滿意佔 46.88%，普通佔 18.75%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 100%。

表 72：中階花蓮場滿意度回饋表統計結果

	很滿意	滿意	普通	不滿意	很不滿意
整體看法	32.35%	54.90%	11.76%	0.98%	0.00%
第一位講師表現	50.00%	48.75%	1.25%	0.00%	0.00%
第二位講師表現	46.00%	52.00%	2.00%	0.00%	0.00%
行政服務	34.38%	46.88%	18.75%	0.00%	0.00%

資料來源：本計畫活動產出

表 73：中階花蓮場教學方式回饋表統計結果

	過多	剛好	過少	不適用
教學方式	3.00%	85.00%	6.00%	6.00%

資料來源：本計畫活動產出

（6）進階台北場意見回饋表統計結果

北區(台北場)進階教育訓練課程總共有 93 人參加，總共發放 53 份意見回饋表，回收 53 份，回收率為 56.99%。

有關對於當日課程的整體看法，很滿意佔 12.18%，滿意佔 66.99%，普通佔 18.59%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 97.76%。

本報告之智慧財產權歸屬於法務部

有關對於講師表現的看法，很滿意佔 24.15%，滿意佔 65.28%，普通佔 9.06%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 98.49%。

有關對於行政服務的看法，很滿意佔 13.46%，滿意佔 75.96%，普通佔 10.58%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 100%。

表 74：進階台北場滿意度回饋表統計結果

	很滿意	滿意	普通	不滿意	很不滿意
整體看法	12.18%	66.99%	18.59%	2.24%	0.00%
講師表現	24.15%	65.28%	9.06%	1.51%	0.00%
行政服務	13.46%	75.96%	10.58%	0.00%	0.00%

資料來源：本計畫活動產出

表 75：進階台北場教學方式回饋表統計結果

	過多	剛好	過少	不適用
教學方式	1.72%	89.66%	8.62%	0.00%

資料來源：本計畫活動產出

（7）進階台中場意見回饋表統計結果

進階台中場教育訓練課程總共有 22 人參加，總共發放 22 份意見回饋表，回收 20 份，回收率為 90.91%。

有關對於當日課程的整體看法，很滿意佔 10.53%，滿意佔 66.67%，普通佔 22.81%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 100%。

本報告之智慧財產權歸屬於法務部

有關對於講師表現的看法，很滿意佔 29.47%，滿意佔 65.26%，普通佔 5.26%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 100%。

有關對於行政服務的看法，很滿意佔 15.79%，滿意佔 63.16%，普通佔 21.05%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 100%。

表 76：進階台中場滿意度回饋表統計結果

	很滿意	滿意	普通	不滿意	很不滿意
整體看法	10.53%	66.67%	22.81%	0.00%	0.00%
講師表現	29.47%	65.26%	5.26%	0.00%	0.00%
行政服務	15.79%	63.16%	21.05%	0.00%	0.00%

資料來源：本計畫活動產出

表 77：進階台中場教學方式回饋表統計結果

	過多	剛好	過少	不適用
教學方式	2.56%	88.46%	7.69%	1.28%

資料來源：本計畫活動產出

（8）進階高雄場意見回饋表統計結果

南區(高雄市)教育訓練課程總共有 44 人參加，總共發放 44 份意見回饋表，回收 31 份，回收率為 70.45%。

有關對於當日課程的整體看法，很滿意佔 22.04%，滿意佔 65.05%，普通佔 12.37%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 99.46%。

本報告之智慧財產權歸屬於法務部

有關對於講師表現的看法，很滿意佔 32.26%，滿意佔 63.87%，普通佔 3.87%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 100%。

有關對於行政服務的看法，很滿意佔 29.03%，滿意佔 62.90%，普通佔 8.06%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 100%。

表 78：進階高雄場滿意度回饋表統計結果

	很滿意	滿意	普通	不滿意	很不滿意
整體看法	22.04%	65.05%	12.37%	0.54%	0.00%
講師表現	32.36%	63.87%	3.87%	0.00%	0.00%
行政服務	29.03%	62.90%	8.06%	0.00%	0.00%

資料來源：本計畫活動產出

表 79：進階高雄場教學方式回饋表統計結果

	過多	剛好	過少	不適用
教學方式	1.57%	93.70%	4.72%	0.00%

資料來源：本計畫活動產出

（9）進階花蓮場意見回饋表統計結果

東區(花蓮場)教育訓練課程總共 16 人參加，總共發放 16 份意見回饋表，回收 13 份，回收率為 81.25%。

有關對於當日課程的整體看法，很滿意佔 46.15%，滿意佔 51.28%，普通佔 2.56%，由整體結果顯示，學員對於本次教育訓練課程品質及效果滿意度課程內容之合適度、與學員目前、未來工作職務之關連性、課程時間長度與內容之設計以及教育訓練場地環境的滿意度達 100%。

有關對於講師表現的看法，很滿意佔 52.31%，滿意佔

本報告之智慧財產權歸屬於法務部

47.69%，由整體結果顯示，講師能有效地呈現其對於課程內容的專業能力，除了可清楚地傳達此課程的概念及內容，亦能舉出與學員工作挑戰方面有相關之例證，講師的授課態度、敬業精神以及整體表現的滿意度為 100%。

有關對於行政服務的看法，很滿意佔 38.46%，滿意佔 61.54%，由整體結果顯示，學員對於本次教育訓練活動事前之各項服務、活動現場之各項服務的滿意度達 100%。

表 80：進階花蓮場滿意度回饋表統計結果

	很滿意	滿意	普通	不滿意	很不滿意
講師表現	52.31%	47.69%	0.00%	0.00%	0.00%
行政服務	38.46%	61.54%	0.00%	0.00%	0.00%

資料來源：本計畫活動產出

表 81：進階花蓮場教學方式回饋表統計結果

	過多	剛好	過少	不適用
教學方式	2.37%	82.91%	6.31%	8.39%

資料來源：本計畫活動產出

2.教育訓練活動意見回饋表建議彙整結果

（1）個資法立法

建議提供法務部預計相關法規配套措施的清單與預估施行日期。

（2）課程內容

A. 建議將課程著重於如何利用「個人資料保護執行管理暨考核作業手冊」執行相關事務。

B. 課程設計著重理論，對實際個人資料保護業務執行無著墨，對專責人員解決推動困難的幫助不大。

本報告之智慧財產權歸屬於法務部

C. 希望於未來舉辦的教育訓練中增加實務個案研究分析課程，以成功個案說明分析，相信能更讓同仁了解個資法的實務操作。

D. 建議講義最後應附上個人資料保護法法條條文，以方便學員對照。

E. 中階課程介紹太多外國標準，建議應多針對國內個人資料保護法法條進行討論，他國法條只要整理比較稍作說明即可。

F. 教材資料太過綱要、簡略，無法立即派上用場。

G. 建議講師應適度停頓詢問學員意見及問題。

H. 公務員有較多委外案件，是否可舉例在委外契約中個人資料保護訂定的範本以供日後訂定契約時參考對於各界見解不同或爭議部分，應講述主管機關(或法務部)之見解或傾向。

I. 建議培訓教材內容應檢附講師學經歷及議程表。

J. 公務機關皆為依法行政，故應朝個資法規面多做相關說明。

K. 建議增加公務機關內部單位互相使用對方蒐集資個資，在適用個資法時，有哪些應注意的地方（互相使用仍是為公務上之目的，僅是為了免除再去蒐集彙整之麻煩），並增設控管之具體執行方式。

L. 建議蒐集公務機關普遍關心之議題深入介紹，尤其是專責人員應有之責任及工作內容，並增加各界見解不同或爭議部分，以及講述主管機關（或法務部）之見解。

（3）行政事項

A. 建議建置線上查詢系統供各部會承辦人詢問相關實例問題。

B. 建議將課程做成數位學習教材，規定每人要上網學習。

本報告之智慧財產權歸屬於法務部

C. 建議提供講義電子檔供學員下載。

D. 培訓課程時間太短，如果能安排一天半的時間會更好。

E. 建議增開培訓課程上課梯次，讓更多相關人員可以參與訓練。

F. 建議提早行文以利辦理作業。

（五）議題整理

1.個資法法令解釋與法規遵循措施

Q1：請問下述機關內部的運作資料是否屬於個資法保護範圍？考勤、單位、職等、職稱、薪資相關資料（俸級、薪點、加班費、所得稅、福利金、互助金...）、公務電話、電子郵件、學歷、經歷、考試資格、教育訓練紀錄、考績、獎懲、陞遷、獎金、公保、勞保、健保資料、差勤相關資料（上/下班打卡、請假紀錄、加班紀錄...）、停車資料（車牌號碼、行照號碼...）、存款資料、儲金利息？

A1：有關個人資料的定義，建議參考「電腦處理個人資料保護法之個人資料類別」，以確認個資法保護的標的。

Q2：資訊系統因為身分識別需要而利用身分證字號為系統帳號（公務人員無識別碼），或是系統內部管理與 log 紀錄的保存是否皆為保存個資？

A2：根據個人資料保護法施行細則第五條：軌跡資料係指個人資料在蒐集、處理、利用過程中所產生非屬於原蒐集個資本體之衍生資訊（LOG FILES），包括（但不限於）資料存取人之代號、存取時間、使用設備代號、網路位址（IP）、經過之網路路徑...等，可用於比對、查證資料存取之適當性。因此，為符合本法個人資料保護與個人資料合理利用之立法意旨，個人資料檔案除備份檔案之外，亦應包括軌跡資料在內。

Q3：公務資料（如：同時具有機關、職稱與姓名）等因業務需要公告，是否違反個資法？

本報告之智慧財產權歸屬於法務部

A3：可參考政府資訊公開法第七條規定應公開之項目；其中第三款所規定，應主動公開項目包含：政府機關之組織、職掌、地址、電話、傳真、網址及電子郵件信箱帳號；並未要求提供承辦人員之姓名、職稱等資訊，相關執行作法可參考行政院、內政部等機關之政府資訊公開作法，僅將單位及聯絡方式提供，未留承辦人員姓名、職稱之方式。另如為執行法定職務上之必要條件下，符合個人資料保護法第 15 條所述之情形，故並無違反個人資料保護法之虞。

Q4：個資法賠償上限兩億是指一個人兩億還是一個案件兩億？

A4：一個案件兩億。

Q5：民眾提出將自己的資料刪除，那機關完成刪除後要如何回覆，只回覆「已刪除」這樣可以嗎？

A5：最好可以提供民眾相關的紀錄，可能是電腦上刪除資料的螢幕畫面、刪除資料的 log 或是紙本檔案銷毀的紀錄（照片）等。

2.教育訓練

Q1：法務部提供之個資訓練課程為很好之作法，建議在個資課程上，能廣泛提供實務訓練課程名額給機關內部業務單位人員參與，以增進將來機關推動個資保護之效果？

A1：感謝這位長官對此教育訓練課程之活動的支持。由於目前預算及經費上之考量下，僅能提供部分名額供各機關之專責人員進行培訓，未來如果各方面的條件皆允許之狀況下，將再提供更多之名額供各機關業務單位人員參與。

Q2：法務部辦理本場次培訓僅談及「BS10012」與「JISQ-15001」標準，建議也可提及個資保護的相關標準─「ISO29100」？

A2：由於國際目前大多參照 BS10012 及 JISQ-15001，且在時間有限及資源有限之條件下，僅能針對 BS10012 及 JISQ-15001 做初步的介紹，未來如果在各方條件之許可下，亦可考慮針對 ISO29100 做一介紹。

Q3：請教法務部針對高階主管是否會安排 PIMS 宣導課程，以取

本報告之智慧財產權歸屬於法務部

得機關高層支持，以利個資相關事項推動?

A3：依照法務部目前之規劃，將會對中央部會進行 PIMS 之宣導課程，其他單位則可依實際需求向法務部提出申請或自行辦理相關課程。

Q4：活動以 E-mail 通知僅訂不會將個資傳給第三方與使用範圍，但無規範保留期限及後續使用情形？加上公務機關委外廠商舉辦活動，須提供個資以進行保險、扣稅、登記...等事宜，如何確保廠商活動結束後，個資有進行銷毀或是交予主辦機關？

A4：建議可事先於契約上註明，並以相關文件為續處理，並在事後監督委外廠商確實執行該銷毀或交辦之作業。

Q5：個資法不只在公務機關推廣，在民間中小企業亦要落實，有鑑於此建議應比照勞委會發行專責人員相關專業證照，也可培育相關評鑑人員。

A5：國內之個資認證機制目前已有經濟部商業司發行之 TPIPAS，而國外最佳實務上亦有 BS10012 證照可供取得。

Q6：教育訓練除專責人員外，建議公務機關主管與高層也接受訓練，以提昇對於個資保護的認知與需求，進而支持落實與後續推廣。

A6：本次教育訓練採專案方式進行，受經費限制，因此場次及參訓人數都有限制，法務部會再研擬後續的教育訓練及推廣的方案。

Q7：建議應實行證照化、專業列管、定期巡教育訓練，以收長遠經營之效。且法條修訂時，再召回上列冊之專業人員回訓。

A7：本次教育訓練採專案方式進行，受經費限制，因此場次及參訓人數都有限制，法務部會再研擬後續的教育訓練及推廣的方案。

3.PIMS 等相關個人資料保護制度及其導入

Q1：為因應個資法之施行，公務機關導入 PIMS，是否需如同導入 ISMS，委請顧問公司協助導入?

A1：可依各公務機關實際需求與其他因素之考量，自行決定是否

本報告之智慧財產權歸屬於法務部

委請顧問公司協助導入。

Q2:PIMS 有無可能導入 ISMS,並透過 ISMS 的監督與審查機制,來進行 PIMS 的內稽與管審，並進行矯正及預防措施的追蹤?

A2：因 ISMS 與 PMIS 為兩套不同之制度，故並非導入 ISMS 便可進行 PIMS 之內部稽核與管理審查，但可將兩者整併進行。

Q3：ISMS 之查檢表計 133 個控制項目，PIMS 有無相應的查檢表或控制項目?

A3：PIMS 之條文即為相關之控制項目。

Q4:PIMS 的風險評估可否合併 ISMS 一同辦理?資訊資產清冊與個人資料盤點清冊之差異性為何? 資訊資產清冊有無可能涵蓋個人資料盤點清冊?

A4：可整合併入 ISMS 之風險評估，惟其風險評鑑之方式需稍作修正。個資清冊並不同於資訊資產清冊，除了項目不同外，個資清冊另含有流程及生命週期之概念在內。故資訊資產清冊無法涵蓋個人資料盤點清冊。

Q5：請問 PIMS 可和 BS10012 畫上等號嗎 ??

A5：建議將 BS10012 當作一參考之標準，於實務上仍須以個人資料保護法及其細則作為依據。

Q6：在國家標準（例如 ISMS 遵循之 CNS27001 與 CNS27002 等標準）尚未發布前，公務機關應遵循何種標準？

A6：目前可先參考 BS10012 及 JISQ-15001 或法務部委請資策會研擬之「非公務機關個人資料檔案安全維護計畫」或「業務終止後個人資料處理方法」草案，待相關標準建立初步之程序後，再行遵循。

Q7：ISMS 各項程序及標單與 PIMS 如何整併？

A7：因 ISMS 與 PMIS 為兩套不同之制度，如須整併，則須重新評估相關程序之可行性及合併後所新增之風險。惟可將兩者之稽核時間或應變組織整併進行。

本報告之智慧財產權歸屬於法務部

4.公務機關進行個人資料保護之制度、措施設計

Q1：在公務機關受理各項案件處理過程中，如傳遞含有個人資料的文件或公文時，其所採取適當的保護措施與目前公務機關處裡秘密等文件之程序是否雷同，或者兩者之保護層次應另行區分，並制定兩套保護措施?

A1：如果其保護措施完善且雷同(如：檔案加密、專人親送、密封、送達人不知其密碼等)，便可依照現行之資料傳遞相關程序進行。如部分保護措施無較完善之程序可依照，建議可針對個人資料保護制度之程序進行制定。

Q2：監督與稽核人員係以外部或內部稽核為宜，與機關內部公務機密保護措施是否有重複之虞?

A2：若現行之相關制度下已有負責內部稽核之人員，則以現有負責稽核之人員為宜。

Q3：損害預估與保險，如何預估? 有無標準或相關規定可供參考?

A3：目前並無準確預估之方法可提供參考，但可從相關之賠償金額(500~20,000/每人每件)作為一參考依據。

5.公務機關進行個人資料保護經費、人力、系統資源配置

Q1：依據個資法，個資法施行前，組織對於所蒐集之個人資料，應對當事人進行補告知，然進行補告知可能需要耗費相當人力、物力、費用，是否有建議之作法可減省成本?

A1：建議可參考下列方式對當事人進行補告知：言詞、書面、電話、簡訊、電子郵件、電子文件等方式。且組織可針對個人資料保護法第八條所述，判斷是否符合免告知之事項。

Q2：有關收文部分，收文人員不必知道公文內的個資，該如何處理?又如何因應本所將於 4 月份導入之公文線上簽核系統?

A2：公務機關所收發公文，其內含之個資料應可就個人資料保護法第 15 條及第 16 條進行蒐集及處理；若單位仍對實務上與法律有所

本報告之智慧財產權歸屬於法務部

擔心，可從建立個資保護之程序著手進行規範(如收文人員收文後，應立即以專人親送的方式將該公文轉交其所屬之單位等)。就目前政府所開發之公文線上簽核系統，其內含之資料，應已建立相關之防範措施，若單位仍擔心有所疏漏，可利用稽核的方式進行相關之檢核，並針對該謙和系統提出改善之需求。

Q3：資訊設備所需之設備及經費，是否有專案經費補助或上級單位會統一撥交相關必要設備?

A3：設備與經費目前仍須等待法務部相關人員進行會議討論後，再行編列相關之預算；至於以經費補助或統一撥交則須視預算而定。

Q4：建議中央將鄉鎮公所的編制，規定應增加「資訊類」人員，以提升各公所之處理及執行能力？

A4：此部分須符合國家政策，目前僅能向相關單位建議，惟此超出法務部之執掌，故無法給予明確之答覆。

Q5：建議檔案管理局檢討公文永久檔案之標準，例如許多之人事資料皆列為永久檔案，是否有其必要?

A5：將於檔案管理局進行相關會議後，再行針對公文永久檔案之保存一事進行評估。

Q6：機關對內/外部人員是否有個資(針對不同類型之個人資料)保護施行步驟之標準作業程序？

A6：建議學員可以參考「個人資料保護執行管理技考核作業手冊」，手冊中皆有個資保護的標準作業程序。

6.公務機關內部作業程序

Q1：個人資料保護執行管理暨考核作業手冊(草案)，是否有將那些屬於法制人員、資訊人員、政風人員、或應屬於業務單位的職掌或分工有明確的訂定?若目前未納入，是否可考慮增加?或於講義第 133 頁分工上增加?

A1：學員可參考個人資料保護執行管理暨考核作業手冊(草案)

本報告之智慧財產權歸屬於法務部

中，個資管理組織與角色職責分工的範例，來對應各階段活動的個資存取權責與角色確立組織人員。

Q2： 據了解法務部委託資策會研擬「非公務機關個人資料檔案安全維護計畫」或「業務終止後個人資料處理方法」範本，請問何時可以提供各機關參考。

A3:「非公務機關個人資料檔案安全維護計畫」，內容包含，組織成立與資源配置、計畫規範程序、安全管理措施、宣導與教育訓練、稽核與改善程序、記錄機制等。該辦法草案之內容與日前法務部預告的施行細則草案第九條之規定相符。而「業務終止後個人資料處理方法辦法」草案則訂定有關業務終止時應踐行之義務以及後續處理個人資料上應注意的事項。前述之辦法草案，將待彙整專家學者意見之後予以修正公告。

Q3：請問「個資法施行細則」目前修訂之狀況為何？

A4：目前仍在依行政院要求進行相關評估作業。

Q4：承上，較受爭議及阻礙為那些法條？

A5：目前業界對於個資法第六條(有關醫療、基因、性生活、健康檢查及犯罪前科等特種個人資料，現行規定除法律明文、公務機關執行公務、當事人自行公開、學術研究等四項要件外，不得蒐集、處理或利用。業界質疑有窒礙難行之處)及第五十四條(蒐集資料應於一年前完成告知，法務部建議刪除此規定，改為原則上應於處理或利用前，告知當事人。產業界憂慮刑責過重，法務部傾向視違規樣態分列)之爭議及反彈較大。第五十四條要求，蒐集資料應於一年前完成告知，法務部建議刪除此規定，改為原則上應於處理或利用前，告知當事人。產業界憂慮刑責過重，法務部傾向視違規樣態分列刑責輕重，並儘速提出修正案。

Q6：請問「個資法施行細則」何時會發布施行？

A6：目前仍在審慎評估中。

Q7：請問「個人資料保護法」有可能需要修改嗎？

A7：目前施行之各項法律條文，必依當下之社會環境進行修正，

本報告之智慧財產權歸屬於法務部

以期善盡保護人民之責。

7.個人資料保護制度實例

Q1：是否可舉國外相關實例說明落實個人資料保護之「具體」組織、架構以及盤點之作法，並敘明該機關名稱？

A1：目前國內部分機構進行之相關個人資料保護架構、盤點作法等皆依照其德勤(Deloitte)全球之標準進行，於國內外已輔導許多公司通過 BS10012 及 JISQ 2005 等相關個人資料保護之認證。

Q2：請問是否可舉實例說明 ISMS 與 PIMS 之整合方式，並敘明該機關（亦或國外之案例）名稱，並說明進行整合或不整合之優缺點。

A3：PIMS 之電子檔案相關處理、利用、保存及銷毀之方式，皆須依賴資訊人員及設備之配合，此部分即可與 ISMS 整合進行稽核或是改善(例如機房整體安全環境等)。整合後將可減少稽核次數及人力，但每次稽核的時間便可能須延長，且如單位內之專責人員僅有一人，須同時了解 ISMS 及 PIMS 之相關需求，便會提高該專責人員處理相關問題時發生錯誤之風險，且由於 ISMS 及 PIMS 並無法完全互相取代，與許多地方上之整合須重新考量，並重新修訂其相關文件。如不整合，則專責人員可有較充裕之時間及精力了解 ISMS 及 PIMS 之需求，於面對相關問題時，可以迅速且較正確的處理；惟此可能增加稽核之次數及所屬專責人員之人力。

Q4：請舉實例說明個資法爭議或案例，其原因、處理之過程與帶來之啟示？

A4：目前由於個資法尚未正式實行上路，尚無相關之爭議或案例可供參考，惟可參考過去電腦處理個人資料保護法或國外個資外洩之相關案例進行研討。

8.個資管理盤點及風險評估

Q1：請問是否可提供風險評鑑參考用弱點及威脅清單？

A1：由於各機關會產生的弱點及威脅狀況皆不盡相同，建議各機

本報告之智慧財產權歸屬於法務部

關依照單位業務性質定意符合業務內容之弱點及威脅，其風險評鑑出來的結果才會符合機關的性質。

Q2：風險評鑑主要在於排序風險。同給分過程相當主觀，也許給完分後，整體檢視時會再調整個別項目（如：X 項目比 Y 項目嚴重），是否乾脆直接排序（如：直接從第一名排至最後一名），將會較為精準，後續也可再進行標準化。

A2：只要可以清楚呈現各機關所面臨的風險，確實可以依照單位業務性質等因素考量風險評鑑的形式，會較為符合機關的需求。

Q3：若下放到各單位進行，對整個機關而言標準不一，如何客觀化？

A3：在下放到各單位之前，對於資產價值、弱點以及威脅的定義一定要建立統一的標準並予以文件化，如此下放到各單位進行風險評鑑時，標準才能一致。

Q4：請提供盤點產出參考格式、個資檢查之參考發現事項以及個資弱點參考項目。

A4：各機關會產生的弱點及威脅狀況皆不盡相同，建議各機關依照單位業務性質定義符合業務內容之弱點及威脅來建立清冊，較符合機關的需求。

（六）結語

法務部「公務機關個人資料保護專責人員培訓教育訓練」系列課程，初階課程首先建立學員對於個人資料保護法以及公務機關責任之基礎認識；中階課程則是進入實務階段，以國際個資保護管理的標準為框架，提供「個人資料保護執行管理暨考核作業手冊」之草案說明，使受訓學員參考以建制機關內部個人資料處理的標準流程與考核作業。最後，進階課程結合初階與中階課程的精髓，併同公務機關將來所要依循的「個人資料保護執行管理暨考核作業手冊」之預擬程序進行實作演練，首先建立個人資料檔案清冊，作為個資盤點的工具，並加以風險評鑑與分析，使受訓學員真正能融合理論與實務，以及事故應變的相關措施與方法。

本報告之智慧財產權歸屬於法務部

透過系列課程之研習，各公務機關亦提出日常業務與個人資料保護與管理相關的寶貴的意見與建言，本執行團隊亦已就意見與建言進行分類整理，希冀提供法務部於日後個資保護與管理業務的推行。觀察國際之潮流，各國政府以及國際組織皆致力於發展其個人資料保護相關法規範、國際合作模式以及個人資料管理系統，以達保護個人資料之效果。我國之新版個人資料保護法即是配合相關保護之概念修正而來，透過「公務機關個人資料保護專責人員培訓教育訓練」之初階、中階以及進階之課程，培養公務機關個人資料保護專責人員對於個資法相關規範之認識，同時也透過介紹及實作管理制度課程，使專責人員得以了解於機關內建置個人資料保護系統之流程與辦法。希冀於個資法施行之後，各公務機關皆能遵循個資法之要件及規範，確實達成保護個人資料之目標。

（七）中階公務機關個資保護專責人員培訓簡報（詳見本報告第 571-656 頁）。

（八）進階公務機關個資保護專責人員培訓簡報（詳見本報告第 657-712 頁）。

（九）初階公務機關個資保護專責人員培訓花蓮（東部）場，中、進階公務機關個資保護專責人員培訓台北場、台中場、高雄場、花蓮（東部）場簽到表（因簽到表內含有參與人員之個人資料，故在此予以移除，詳細簽到資料已附於呈繳法務部之「第二年度公務機關個人資料保護專責人員培訓教育之紀錄彙整及成果追踪報告」）。

本報告之智慧財產權歸屬於法務部

（十）初階公務機關個資保護專責人員培訓花蓮（東部）場照片集

資料來源：本計畫活動拍攝

圖 54：法務部邱銘堂專門委員致詞

資料來源：本計畫活動拍攝

圖 55：學員出席情況踴躍

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 56：勤業眾信會計師事務所曾韵經理講授課程

本報告之智慧財產權歸屬於法務部

（十一）中、進階公務機關個資保護專責人員培訓台北場、台中場、高雄場、花蓮（東部）場照片集

資料來源：本計畫活動拍攝

圖 57：中階台中場-法務部鍾瑞蘭副司長蒞臨致詞

資料來源：本計畫活動拍攝

圖 58：中階台中場-學員參與狀況熱烈

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 59：中階台中場-資策會李彥震諮詢師精彩解說「個人資料保護執行管理暨考核作業手冊」

資料來源：本計畫活動拍攝

圖 60：中階台中場-法務部胡美蓁編審、資策會顧振豪組長、李彥震諮詢師，以及勤業眾信會計師事務所宋子莉副理，回覆學員提問

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 61：中階台北場-法務部陳維練司長蒞臨致詞

資料來源：本計畫活動拍攝

圖 62：中階台北場-學員參與踴躍

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 63：中階台北場-資策會顧振豪組長、施叔良資深業務經理、李彥震諮詢師，以及勤業眾信會計師事務所游靖芬副理，回覆學員提問

資料來源：本計畫活動拍攝

圖 64：中階台北場-學員提問踴躍

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 65：中階高雄場-法務部邱銘堂專門委員致詞

資料來源：本計畫活動拍攝

圖 66：中階高雄場-學員參與踴躍

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 67：中階高雄場-法務部胡美蓁編審、資策會顧振豪組長、施叔良資深業務經理、李彥震諮詢師，以及勤業眾信會計師事務所宋子莉副理，回覆學員提問

資料來源：本計畫活動拍攝

圖 68：中階高雄場-學員積極提問

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 69：中階花蓮（東部）場-法務部郭全慶專門委員致詞

資料來源：本計畫活動拍攝

圖 70：中階花蓮（東部）場-學員參與踴躍

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 71：中階花蓮（東部）場-資策會顧振豪組長、施叔良資深業務經理、李彥震諮詢師，以及勤業眾信會計師事務所游靖芬副理協助學員解答

資料來源：本計畫活動拍攝

圖 72：中階花蓮（東部）場-資策會施叔良資深業務經理、勤業眾信會計師事務所游靖芬副理授課授課

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 73：進階台北場-法務部鍾瑞蘭副司長致詞

資料來源：本計畫活動拍攝

圖 74：進階台北場-資策會顧振豪組長與勤業眾信會計師事務所曾韵經理為學員解答

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 75：進階台北場-學員提問熱烈

資料來源：本計畫活動拍攝

圖 76：進階台北場-學員參與踴躍

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 77：進階台中場-法務部鍾瑞蘭副司長致詞

資料來源：本計畫活動拍攝

圖 78：進階台中場-學員進行分組練習

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 79：進階台中場-學員分享實作結果

資料來源：本計畫活動拍攝

圖 80：進階台中場-資策會顧振豪組長與勤業眾信會計師事務所陳鴻棋副理，解答學員提問

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 81：進階高雄場-法務部郭全慶專門委員致詞

資料來源：本計畫活動拍攝

圖 82：進階高雄場-學員參與踴躍

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 83：進階高雄場-學員進行分組實例演練

資料來源：本計畫活動拍攝

圖 84：進階高雄場-法務部胡美蓁編審、資策會顧振豪組長，以及勤業眾信會計師事務所陳鴻棋副理為學員解答

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 85：進階花蓮（東部）場-法務部邱銘堂專門委員致詞

資料來源：本計畫活動拍攝

圖 86：進階花蓮（東部）場-學員分享實例演練心得

本報告之智慧財產權歸屬於法務部

資料來源：本計畫活動拍攝

圖 87：進階花蓮（東部）場-學員積極提問

資料來源：本計畫活動拍攝

圖 88：進階花蓮（東部）場-資策會顧振豪組長與勤業眾信會計師事務所陳威棋副理，為學員解答

本報告之智慧財產權歸屬於法務部

捌、結語

目前整體國家政府機關內，已有一定之資訊安全管理機制存在，然而，因應行政院組織再造，公部門彼此間面對組織整合與政府資訊環境的變動，相關制度規範亦必須重新檢視，現存資訊管理之範疇與權責勢必產生異動。

不可否認，個人資料管理與保護措施將與政府推動之資訊安全管理措施產生某種程度之接軌，雖然此兩者在保護重點或範疇上不盡相同，但其推動之方法由管理機制面、流程面、風險管理面、稽核查核面與改進層面，並無差異。個人資料保護法實施後，公務機關除推動實施機關內對於個人資料保護作業落實，除了與當事人權益行使之相關作業外，對於個人資料保護與資訊安全之相關作業，勢必與國家資通安全會報已建立之資通安全機制，行政院各項資通安全準則產生高度之關聯。

參考資訊安全推動之經驗，對於個人資料保護與管理，可能形成五個不同面向的實施細節：

一、展現落實個人資料管理的權責：良善的政策與程序或紀錄、教育訓練、人員執掌、必要的支援系統或科技應用。

二、政府對於業務委外，包含資料處理委外、作業委外、推廣活動委外或跨部會間之資料交換等情形，勢必應有嚴謹之作法，並針對具備風險性的資料交換或委外，進行定期評估或查核，以確實遵循相關法規。

三、當事人權益之保護，勢必對於目前公務機關的作業與便民服務措施的實踐方式有所衝擊，如何同時兼顧政務推動之方便，以及遵循個人資料保護法規，將因各公務機關不同業務之差異可能有不同的衝擊與影響。

四、資訊安全控管由數位化資訊系統擴大到所有類型資料，且目前雲端運算的風行與政府資訊改造朝向綠化、無紙化、自動化的主要潮流，又將資訊安全控管的幅度與複雜性，帶到新的層面，因而落實資訊安全控管，將是一個持續演進的過程，也為公務人員在法令遵循時，帶來科技更新時與業務衝擊之挑戰。

五、公務人員執行公務時，必以不違法為前提與主要思考，因而在個人資料保護法實施後，公務人員如何將落實執行之過程與紀錄，作為個人努力遵行成果

本報告之智慧財產權歸屬於法務部

之展現，甚至成為保護公務人員與公務機關的主要證據，將是一個新興趨勢。

而個人資料保護法的實施，亦將衝擊公部門與為數眾多的民間企業，由於個人資料保護重在執行層面之落實，且刻不容緩，因而需要在新法實施之前，依現行法進行必要性的宣導與教育、制定執行措施指導手冊，並應建置機關輔導系統。復因個人資料保護法修正草案將有日出條款之施行日期緩衝期，行政院科技顧問組協同相關部會規劃完成「行政院『塑造資安文化、推升資安產值』產業科技策略會議關鍵推動方案」，由各主責部會在施政措施上予以落實。

本計畫於執行期間透過強化公務機關個人資料之保護與管理，落實執行個人資料保護法之作法，以及研提各公務機關個人資料保護及管理之執行措施範本，以便提供全國各公務機關參考，並有效保護機關之個人資料及落實非公務機關個資保護之監督管理，強化對於個人資料與隱私保護的標準作業流程（包括對非公務機關之監督管理）及考核需求，達成落實憲法保障人民資訊隱私權、資訊科技政策及達到安全、安心與信賴的資訊環境之目標。

本報告之智慧財產權歸屬於法務部

附錄、公務機關個人資料保護執行程序暨考核作業手冊附錄

附錄一、管理制度之參考表單

附件一：個人資料保護管理政策

個人資料保護管理政策

○○○○○○（機關名稱）係以從事○○○○○（行政業務項目、範圍），為了符合我國個人資料保護法之要求，本機關將依以下原則蒐集、處理及利用當事人所提供的個人資料。

一、本機關將遵守個人資料保護法相關法令、機關所訂定之指引及其他有關法令規範。

二、本機關將訂定個人資料保護管理相關之規範、作業準則以落實執行個人資料保護管理，並透過定期檢查、內評或檢視之方式，持續改善之。

三、本機關於建置個人資料保護管理制度後，將公告全體人員周知以落實執行運作。

四、本機關於告知事項中將明示以下內容：機關將於利用目的範圍內，蒐集、處理及利用當事人所提供之個人資料，並於不逾越當事人提供個人資料之利用目的必要範圍內為處理、利用行為，亦將採取適切之個人資料保護措施。

五、為維護當事人所提供之個人資料為正確且最新之狀態，將採取適切措施預防個人資料的被竊取、洩漏、竄改等侵害。並提升本機關資訊安全相關措施以保護所蒐集、處理以及利用之個人資料，同時持續改善機關內部所建置之個人資料管理制度。於確認發生個資外洩事故時，將迅速採取緊急應變措施作為，並將事實通知當事人。

六、本機關於當事人提出有關其提供個人資料之查閱、複製、更正、刪除等之申請時，將依個資保護法之相關規定確實、迅速回應之。

中華民國○○○年○○月○○日

本報告之智慧財產權歸屬於法務部

附件二：個人資料保護組織規定

個人資料保護組織規定

一、目的

為規範有關個人資料保護管理相關權限及責任訂定本規則。

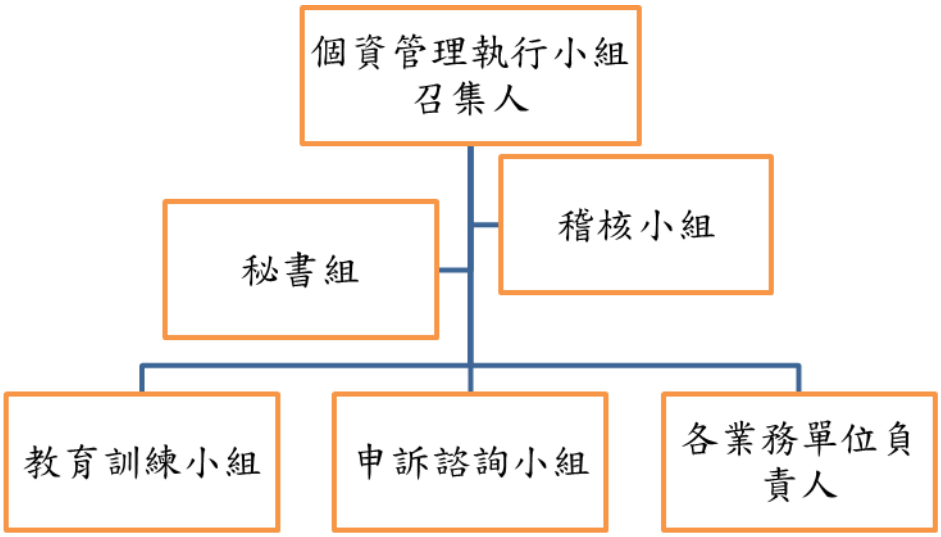
二、機關代表人之職責

機關代表人應準備個人資料保護管理制度建置、執行、維護及改善所需之不可或缺之資源。

三、職責及權限之範圍

機關依內部之職責分工，製作以下個人資料保護機關架構圖以明確個人資料保護管理機關；將個人資料保護要點與各部門之職責、權限以一覽表訂定之，並將機關架構圖與一覽表公告全體人員周知。

個人資料保護機關架構圖



四、職責與權限

（一）機關代表人

1.制訂及維護個人資料保護管理政策

本報告之智慧財產權歸屬於法務部

2.準備個人資料保護管理制度執行所需之資源

3.任命個人資料保護管理執行小組、稽核小組

4.改善修正個人資料保護管理制度

（二）個人資料管理執行小組

1.負責個人資料保護管理制度執行及運作

2.任命個人資料保護教育訓練小組、申訴諮詢負責窗口負責人及其他必要建置之機關負責人

3.管理個人資料保護管理制度之執行與運作

4.向機關代表人報告個人資料保護管理制度之運作情形

5.規劃個人資料保護管理制度之全年計畫

6.製作及核可內部規則、表單

（三）稽核小組

1.負責個人資料保護管理制度之內部稽核

2.規劃稽核計畫

3.任命執行稽核人員

4.管理稽核執行

5.向機關代表人報告稽核結果

6.教育訓練執行稽核人員

（四）教育訓練小組

1.負責個人資料保護管理制度教育訓練

2.規劃教育訓練計畫

3.任命執行教育訓練人員

4.管理教育訓練

（五）申訴諮詢小組

本報告之智慧財產權歸屬於法務部

1.負責個人資料保護管理制度之申訴諮詢

2.建置當事人權利行使、申訴諮詢窗口應對機關

3.追蹤當事人權利行使、申訴諮詢之處理情形

（六）各部門負責人

1.負責於各部門執行及運作個人資料保護管理制度

2.管理所屬部門之個人資料

3.監督、確認所屬部門內部個人資料保護管理制度之運作情形及紀錄

4.監督全部安全管理措施之執行

（七）關於機關代表人、個人資料保護管理執行小組、各負責人、幕僚部門以及各部門人員之職責分配，請見下表：

五、本規則於每年○月檢視，於必要時修訂之。

本報告之智慧財產權歸屬於法務部

附件三：個人資料保護管理制度作業計畫表

編號	步驟名稱	開始	完成	期間	負責組織	備註
1	訂定個人資料保護管理政策					
2	成立個人資料保護管理執行小組					
3	製作建置個人資料保護管理制度作業時程表及建置範圍					
4	機關公告個人資料保護管理政策					
5	盤點法規以及上級機關訂定之規範					
6	盤點個人資料					
7	進行個人資料風險評估並擬定風險對策					
8	配置相當資源					
9	訂定個人資料保護管理制度之內部規範					

本報告之智慧財產權歸屬於法務部

編號	步驟名稱	開始	完成	期間	負責組織	備註
10	教育訓練					
11	開始運作個人資料保護管理制度					
12	檢視個資保護管理制度之運作情形並進行改善					
13	修正個人資料保護管理制度並實施改善措施					

本報告之智慧財產權歸屬於法務部

附件四：法規盤點程序

法規盤點程序

一、法規盤點

本機關應調查個人資料保護法及其他相關法律規定，並確實遵守之。若有受委託行使公權利之情形，進行法規盤點時，亦必須注意委託機關所應遵循之相關法規。

二、蒐集取得法令及其他規範

個人資料保護法及其他相關蒐集、取得法令由○○部門之業管人員整理之。

三、調查法令及其他規範

○○部門之業管人員對於個人資料保護相關法令及其他規範進行調查。

四、登載法令及其他規範

○○部門之業管人員於部門負責人裁示後，將調查結果登載於「法規盤點清冊」中。

五、公告周知登載內容

○○部門之業管人員將所登載之個人資料保護法及其他規範內容，向本機關全體人員公告周知。

六、檢視修訂法令及其他規範

○○部門之業管人員為維持個人資料保護法及其他相關法令規範為最新之狀態，應定期於每年○月檢視法規之更新狀況；另外，於機關行政業務項目、範圍有新增變動時，亦必須重新檢視法規盤點清冊之內容。

本報告之智慧財產權歸屬於法務部

附件五：個人資料盤點程序

個人資料盤點程序

一、個資盤點程序

（一）各部門業管人員針對因行政業務項目或服務所蒐集、處理以及利用之個人資料進行盤點，該程序及盤點清冊內容須得個人資料保護管理執行小組之核決。

（二）由各個業務部門清查所持有的個人資料。

（三）清查個人資料應考量下列事項進行：個資的生命週期；蒐集、處理利用程序；業管人員；保存形式；保存處所；委託提供流向；刪除銷燬方法等事項。

二、登載個人資料

盤點機關應於盤點所管理之個人資料後，由業務部門負責人向個人資料保護管理執行小組報請核定後，登載於「個人資料盤點清冊」。

三、個人資料盤點清冊檢視修訂

個人資料保護管理執行小組為維持個資盤點清冊為最新之狀態，應於以下情形發生時，不定期檢視並修訂「個資盤點清冊」:

（一）於機關行政業務項目、範圍新增變動時

（二）個人資料保護法及其他相關法令規範修訂

（三）利害關係人有所請求

本報告之智慧財產權歸屬於法務部

附件六：風險評估程序

風險評估程序

一、機關將記載於個人資料盤點清冊中之個人資料，進行風險評估，並採取必要的對策。

二、個人資料的風險評估

個人資料保護管理執行小組對各部門及機關全體所盤點出的個人資料，與各部門的業管人員商議後，斟酌違反法令導致個人資料被竊取、洩漏、竄改或者其他侵害、目的外利用等情形進行綜合的考量，以評鑑風險之高低。

三、檢討風險管理機制。

對個人資料風險評估之結果，由個人資料保護管理執行小組進行檢討對策，並決定風險管理機制之內容。

四、個人資料保護管理執行小組將決定之風險因應方案記載於「安全管理規則」中，由各部門業管人員於部門內部確實宣傳周知之。

五、個人資料保護管理執行小組應定期於每年○月，或於機關行政業務項目、範圍有新增變動時；或個人資料保護法及其他相關法令規範有修訂；或資訊安全技術、機關內部管理方法；或利害關係人有所請求時，檢視「風險分析清冊」並修訂之。

本報告之智慧財產權歸屬於法務部

附件七：緊急應變程序

緊急應變程序

一、發生外洩個人資料等緊急事故時，本機關依下列程序，由個人資料保護管理執行小組依事故狀況應對措施處理之。如個人資料保護管理執行小組無法處理時，由部門負責人代理之。若部門負責人亦不在時，由機關代表人任命緊急應對負責人。

二、確認個人資料發生緊急事故之通報途徑

經機關外部通報或是由機關內部確認事故發生時，本機關人員按下列途徑迅速通報：

（一）各負責人、業管人員不在時，向機關代表人報告。

（二）通報途徑要讓機關全體人員得隨時參照。

（三）因各負責人、業管人員不在而跳級向上級負責人通報時，事後要儘速補向各負責人、業管人員報告。

三、查明事實及啟動緊急應變程序

（一）個人資料保護管理執行小組於查明事故發生之事實關同時，須確認發生的原因與影響的範圍。

（二）個人資料保護管理執行小組須採取防止事故擴大之措施。

四、決定緊急應變處理負責人

個人資料保護管理執行小組應按發生事故的內容安排相對應的緊急應變處理負責人。

五、執行應對

（一）各應對負責人應隨時將應對內容向個人資料保護管理執行小組報告，使個人資料保護管理執行小組能掌握緊急事故應變之全體狀況。

本報告之智慧財產權歸屬於法務部

（二）個人資料保護管理執行小組或其代理人應隨時紀錄應對內容。於必要時隨時向機關代表人報告。

（三）通知或公告發生個人資料事故之當事人

個別通知當事人時，應誠心道歉並將事故發生之事實關係及個人資料外洩、毀損或滅失之相關內容儘速通知當事人。

無法通知個別當事人時，應於網頁或報紙上公告事故發生之概要，於必要時設置免費電話，採取使當事人迅速得知事故發生之措施。

六、查明個人資料事故之因應方式

（一）各緊急事故應變處理負責人於查明事故發生原因後，按個人資料保護管理執行小組指示，採取適當之應對措施。

（二）緊急事故發生時，個人資料保護執行小組須對外公告事故發生之事實，並且向上級或相關機關通報事故發生原因及後續處理事項。

七、網頁公告

公告內容包含向上級及相關機關通報有關事故的概要、發現事故發生後之處理經過與處理之詳細內容、事故與當事人個人資料之關係、再次發生事故之預防方法、執行狀況、以及相關人員的處分情形

八、檢視事故處理之內容

根據應對紀錄，確認是否適當執行緊急事故。

九、追究查明事故發生之原因，擬訂防止再度發生事故方法。

十、防止事故再度發生方法

個人資料保護管理執行小組根據矯正預防措施確認運作或於日常業務中發現不符合事項時之規定，啟動執行矯正預防措施。

十一、本規則於每年○月定期實施檢視並於必要時修訂之。

本報告之智慧財產權歸屬於法務部

附件八：個人資料作業管理規定

一、蒐集

（一）特定目的、特定情形

本機關各部門於執行部門業務而有蒐集個人資料時,按下列事項為之：

1.明確利用個人資料之目的，於達成特定目的必要範圍內蒐集個人資料。

2.檢視蒐集個人資料之情形是否符合有無法律明文規定、與當事人有契約或類似契約之關係、當事人自行公開或其他已合法公開之個人資料、經當事人書面同意、與公共利益有關或個人資料取自於一般可得之來源，且無但書之排外情形，例如對該當事人資料之禁止處理或利用，顯有更值得保護之重大利益者。

3.各部門負責人判別其部門業管人員所蒐集的個人資料是否合乎使用目的、特定情形及必要之限度。

4.各部門業管人員將所蒐集之個人資料按個人資料盤點程序經個人資料保護管理執行小組核決後，登載於個人資料盤點清冊。

（二）合法正當蒐集

本機關蒐集之個人資料時，依合法、正當之誠實信用方式為之。

二、處理

本機關各部門於執行部門行政業務而有處理個人資料時，按下列事項為之：

（一）各部門負責人決定其部門內部處理個人資料業管人員，並設定處理權限範圍。

（二）各部門業管人員按個人資料盤點清冊所登載之特定目的，確定處理是否合於蒐集時告知當事人之特定目的，並於達成特定目的必要範圍內處理個人資料。

本報告之智慧財產權歸屬於法務部

（三）處理個人資料之情形是否符合有無法律明文規定、與當事人有契約或類似契約之關係、當事人自行公開或其他已合法公開之個人資料、經當事人書面同意、與公共利益有關或個人資料取自於一般可得之來源，且無排除條款，例如當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者。

（四）各部門負責人判別其部門業管人員所處理的個人資料是否合乎使用目的、特定情形及必要之限度。

（五）各部門業管人員將所蒐集之個人資料按個人資料盤點程序整理歸納之，經個人資料保護管理執行小組核決後，登載於個人資料盤點清冊。

三、利用

（一）本機關藉由公告周知「個人資料保護管理政策」及明確記載利用目的的「個人資料盤點清冊」，使全體人員於達成特定目的之必要範圍內利用所蒐集、處理之個人資料。利用個人資料若逾越特定目的之必要範圍產生疑義時，由該部門負責人向個人資料保護管理執行小組確認利用目的，並核決告知事項內容及告知義務履行方法。

（二）本機關各部門於執行部門行政業務而有利用個人資料時，按下列程序為之：

1.各部門負責人決定其部門內部利用個人資料業管人員，並設定處理權限範圍。

2.各部門業管人員按個資盤點清冊所登載之特定目的，確定利用是否合於蒐集時告知當事人之特定目的，於達成特定目的必要範圍內利用個人資料。

3.於特定目的外利用個人資料時，是否符合有法律明文規定，增進公共利益，為免除當事人生命、身體、自由或財產上之危險，防止他人權益之重大危害，經當事人書面同意等情形。

4.各部門負責人判別其部門業管人員所利用的個人資料是否合乎使用目的、特定情形及必要之限度。

5.各部門業管人員將所利用之個人資料按個人資料盤點程序經個人資

本報告之智慧財產權歸屬於法務部

料保護管理執行小組核決後，登載於個人資料盤點清冊。

四、特種個人資料之蒐集、處理、利用限制

本機關有關醫療、基因、性生活、健康檢查、犯罪前科等特種個人資料，非有法令規定，不得蒐集。但於符合法令規定的情形下，並經個人資料保護管理執行小組核決後，按蒐集、處理、利用程序為之。

五、特種個人資料之管理

本機關有關於特種個人資料之蒐集、處理、利用及國際傳輸，由各部門業管人員經部門負責人審核後向個人資料保護管理執行小組提出，由個人資料保護管理執行小組核決後，按蒐集、處理、利用程序為之。

六、告知義務之履行

（一）免為告知義務之確認

本機關各部門業務業管人員於蒐集個人資料履行告知義務前，確認有無下列免為告知情形，經部門負責人判別，向個人資料保護管理執行小組報告審議後，登載於個人資料盤點清冊：

1.直接向當事人蒐集時：法律規定、履行法定義務必要、妨害公務機關執行法定職務、妨害第三人重大利益、當事人明知應告知內容。

2.間接向當事人蒐集時：1.之各項、當事人自行公開或其他已合法公開、不能向當事人或法定代理人為告知等免為告知之情形。

（二）告知事項內容

本機關各部門業務業管人員於確認無免為告知情形，向當事人為告知下列事項：

1.機關名稱

2.蒐集目的

3.個人資料類別

4.個人資料利用之期間、地區、對象及方式

5.如有委託給第三人，受委託單位名稱、委託的個資種類、方式。

本報告之智慧財產權歸屬於法務部

6.當事人權利行使方式

7.不提供時對當事人權益的影響

8.聯絡人姓名、連絡方式

9.資料於符合特定目的下所為之共同利用時，共同利用單位名稱、共同利用個資種類、方式。

七、告知義務履行方式

於直接蒐集之情形，各部門業務業管人員告知義務履行方式如下：

（一）紙本蒐集

本機關以紙本蒐集當事人個資時，應預備告知事項文件，以口頭陳述或出示紙本文件方式，以錄音或紙本方式取得告知紀錄。

（二）網站蒐集

本機關自網路蒐集個人資料時，在當事人輸入個人資料頁面前，以視窗顯示告知事項，以勾選閱讀告知事項選項並留存相關瀏覽歷史紀錄。

（三）傳真／電子郵件蒐集

本機關以傳真或電子郵件方式蒐集個人資料時，以傳真或電子郵件中包含告知事項進行告知，並留存傳真、及電子郵件寄送紀錄。

（四）電話蒐集

本機關以電話方式蒐集個人資料時，以口頭方式進行告知，並錄音留存告知紀錄。

八、國際傳輸之作業規定

機關對個人資料之國際傳遞及利用，依相關法令為之。

九、刪除與銷燬之規定

（一）機關於個人資料蒐集之特定目的或期限屆滿時，應主動或依當事人

本報告之智慧財產權歸屬於法務部

之請求，刪除或停止處理或利用個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

（二）違反本法規定蒐集、處理或利用個人資料時，機關應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。

十、本規則於每年○月定期實施檢視，於必要時修訂之。

本報告之智慧財產權歸屬於法務部

附件九：個人資料維護及委外管理程序

一、確保個人資料正確性

本機關按個人資料盤點清冊所訂定之利用目的及保存期間、達成利用目的所必要之範圍內，管理並維護個人資料於正確、最新之狀態。

二、安全管理措施

本機關按個人資料作業流程圖，識別個人資料於個人資料生命週期中蒐集、處理、利用等各情境之風險，於風險盤點清冊進行風險評估及分析，決定防止外洩、毀損、滅失及其他個人資料安全管理所必要之預防方法及風險發生時之措施。其所決定之內容訂定於安全管理措施規則中，機關須採取必要且妥適之安全管理措施。

三、對於委外管理程序

基於個資法之要求，機關建立委外管理程序，以妥善管理所蒐集、處理以及利用之個人資料。為妥善保護個人資料，機關對於委外廠商之評鑑、選擇、契約、監督及再評鑑將依下述程序為之：

（一）委外廠商之選擇標準

1.由個人資料保護管理執行小組訂定委外廠商選擇標準，經機關代表人核決後執行。

2.選擇標準於每年○月實施檢視並於必要時修訂之。

（二）委外廠商之評鑑

將個人資料相關業務委託時，各部門負責人於委託前應先詢問委外廠商有關個人資料保護個人資料情形，將其內容記載於選擇委外廠商評鑑表。並根據個人資料保護管理執行小組訂定委外廠商選擇標準對委外廠商進行評鑑。

（三）委外廠商之選擇

根據委外廠商評鑑表之評鑑結果選擇委外廠商，並經個人資料保

本報告之智慧財產權歸屬於法務部

護管理執行小組核決，決定委外廠商。

（四）締結契約

1.對於委外廠商委託個人資料相關業務前，按業種、規模、委託業務之內容，於個人資料保護管理執行小組管理下，締結個人資料委外契約書。個人資料保護管理執行小組須於契約締結前，就委外契約確認係在特定利用目的內。

2.該契約書保存期間，由簽約部門負責人至少保存至個人資料保存期間之期間屆至為止。

3.個人資料委外契約書應記載下列事項，並保存至個人資料保存期間屆至為止：

（1）明確委託人與受託人之責任

（2）有關個人資料安全管理事項

（3）有關再委託之事項

（4）向委託人報告個人資料處理情形之內容及報告次數

（5）委託人得以確認遵守契約內容之事項

（6）不遵守契約內容時之處罰

（7）發生個人資料事故及事件時之通報、聯絡事宜

（8）管理個人資料委外廠商一覽表

（9）應將經評鑑選擇之委外廠商，依委託業務內容、契約締結日期、緊急聯絡人、業管人員等記載於個人資料委外廠商一覽表，由個人資料保護管理執行小組管理之。個人資料委外廠商一覽表之更新管理由個人資料保護管理執行小組隨時更新。

（五）確認委外廠商事項

委外廠商之管理於斟酌評鑑結果、委託業務，由部門負責人或個人資料保護管理執行小組於每年郵寄調查表單或親自訪談，最少每一

本報告之智慧財產權歸屬於法務部

年度執行一次委外廠商個人資料處理情形評鑑。

（六）對委外廠商再評鑑

部門負責人於每年度調查期間屆至前對委外廠商實施再評鑑。

四、本規則於每年○月定期實施檢視，於必要時修訂之。

本報告之智慧財產權歸屬於法務部

附件十：當事人權利行使程序

當事人行使之權利

一、本機關於收受個人資料當事人行使權利申請後，將依個人資料保護法之要求，迅速回應當事人之申請。

二、依個資法第 3 條之規定，當事人就以下之事項，可向本機關行使其權利。

（一）查詢或請求閱覽

（二）請求製給複製本

（三）請求補充或更正

（四）請求停止蒐集、處理或利用

（五）請求刪除

三、僅限於個人資料保護法第 10 條規定但書之情形，始可拒絕當事人行使權利申請。

四、當事人權利行使之程序

（一）以「承辦窗口負責人」為當事人行使權利之負責窗口。由承辦窗口負責人以外之人員收受當事人權利行使之請求時，於確認當事人請求內容後轉送承辦窗口負責人。有緊急情況時，由個人資料保護管理執行小組應對之，可行使當事人權利之當事人資格

本機關所保存之個人資料僅供當事人本人及當事人之法定代理人申請查詢，不受理非當事人或委託他人提出之查詢申請。

（二）當事人權利行使時時應檢具之文件

1.對本機關行使當事人權利時應檢具下列文件：

（1）當事人本人提出申請者：

A. 當事人權利行使申請書。

B. 當事人須出示其身份證、健保卡、護照、駕照、學生證、

本報告之智慧財產權歸屬於法務部

居留證或其他足資證明身分之證件以供查驗。

（2）法定代理人提出申請：

A. 代理人須出示其身份證、健保卡、護照、駕照、學生證、居留證或其他足資證明身分之證件以供查驗。

B. 當事人權利行使申請書以及授權書，授權書必須經當事人親筆簽名。

2.當事人查詢資料應檢具真實文件並據實填寫相關資料，如有虛偽不實者，本機關得拒絕其查詢。

五、當事人權利行使之回覆

本機關經審核確認當事人或其法定代理人符合上述資格規定之要件後，應就本機關所保存之現有個人資料進行查詢，並以書面將當事人權利行使之結果回覆當事人。

六、處理期間

（一）本機關受理當事人行使查詢、閱覽、製給複製本申請後，應於受理日起十五日內回覆結果；如駁回時並附駁回之原因。

（二）本機關受理當事人行使更正補充、刪除、停止處理利用申請後，應於受理日起三十日內回覆結果；如駁回時並附駁回之原因。

七、成本費用

對於查詢、閱覽、製給複製本個人資料之申請，本機關得酌收成本費用。

八、本規則於每年○月進行檢視，於必要時修訂之。

本報告之智慧財產權歸屬於法務部

附件十一：教育訓練計畫

一、教育訓練小組於每年○月以本機關全體人員為對象，擬訂本機關全年教育訓練計畫，並經個人資料保護管理執行小組核可之。

二、教育訓練小組所任命之教育訓練執行人員根據本機關全年教育訓練計畫，提出個別部門教育訓練計畫及教育訓練執行紀錄，並經教育訓練小組核可之。

三、教育訓練內容應包括：

（一）符合個人資料保護管理制度的重要性及優點

（二）為符合個人資料保護管理制度之職責

（三）違反個人資料保護管理制度可能之結果

（四）反映上一年度教育訓練結果之事項

（五）若單位有新進人員或因職務變動第一次從事個人資料相關行政業務人員時，應使其迅速參加個人資料保護管理制度相關教育訓練。

四、執行

（一）教育訓練執行人員按個別部門教育訓練計畫及教育訓練執行紀錄執行本機關教育訓練。

（二）教育訓練結束時，為瞭解參加教育訓練人員對於本機關個人資料保護管理制度之理解程度，將實施隨堂考試或問卷調查。

（三）確認人員出席教育訓練情形，對缺席人員於該部門課程結束後一週內進行補課。執行教育訓練二週內後完成個別部門教育訓練計畫及教育訓練執行紀錄之執行教育訓練紀錄。

五、報告教育訓練結果與審查

（一）教育訓練執行人員根據個別部門教育訓練計畫及教育訓練紀錄之教育訓練執行紀錄與隨堂考試或問卷調查結果，向教育訓練小組報告教育訓練之有效性並評價、確認教育訓練結果之有效性。

（二）教育訓練小組向個人資料保護管理執行小組提出個別部門教育訓

本報告之智慧財產權歸屬於法務部

練計畫及教育訓練執行紀錄接受審查。

六、檢討修正計畫

個人資料保護管理執行小組根據審查結果，指示教育訓練小組應於下次教育訓練的內容反映之事項。個人資料保護管理執行小組依審查之內容向機關代表人報告。

七、維護紀錄

有關教育訓練之全部紀錄由教育訓練小組管理之。

八、修訂

本規則於每年○月進行檢視，於有必要時修訂之。

本報告之智慧財產權歸屬於法務部

附件十二：文件紀錄管理規定

一、文件控管

文件的範圍--本機關製作及保存下列構成個資保護管理制度的重要文件：

（一）個人資料保護管理政策

（二）個人資料保護管理相關內部管理規則及其流程

（三）其他實施個人資料保護管理制度應製作之紀錄文件

二、文件管理程序

文件制定公佈及修訂：

（一）「個人資料保護管理政策」由機關代表人制訂公佈。

（二）「個人資料保護管理內部規則」及相關「表格」由個人資料保護管理執行小組製作後，由機關代表人核決後公佈。

（三）文件修訂時，由與制定第 1 版時同樣職位之人修訂核決。

三、文件修訂內容及版本管理

為執行文建版本管理，文件修訂人應於各文件修訂歷程欄為中記載修訂內容及版本別。

四、文件保管管理

（一）文件原本按種類保存於○○部門檔案櫃中。於執行個人資料保護時，使機關人員有閱覽文件之必要時，即可容易取得相關文件參照執行。

（二）文件由個人資料保護管理執行小組或受個人資料保護管理執行小組指定者管理。

（三）文件有重新制定或修訂時，應儘速抽換最新內容。

五、文件檢視

（一）本機關於文件範圍中的文件於每年○月進行檢視，文件有改善之必

本報告之智慧財產權歸屬於法務部

要時，並修訂之。

（二）除定期修訂之時期以外，因本機關會議決議或稽核報告結果，機關代表人或個人資料保護管理執行小組認有必要時得隨時檢視、修訂文件。

六、文件廢止

（一）為使廢止的文件不因過失而被誤用，廢止的文件應刪除或銷燬之。廢止文件因其他目的而有保存之必要時，應於文件封面上以粗體紅字表示廢止文件而保存。

（二）廢止文件的電子檔因其他目的而有保存之必要時，應於開啟文件檔時明顯處記載「廢止」字眼後，保存於「廢止文件」的資料夾中。

七、紀錄管理程序

製作紀錄--紀錄依各種表格單據製作。表格單據亦也可用於會議議事錄之紀錄。

八、紀錄管理

（一）紀錄製作人、核決人、製作時期、保存處所及保存期間按「表格　文件、紀錄一覽表」之「紀錄管理一覽表」所記載。

（二）按「紀錄管理一覽」所定保存處所於保存期間而保管之。

（三）有關永久保存之紀錄，其保存期限以 10 年為期保存之，若保存期限屆至，而仍有繼續保存之必要時，其保存期限再延長 10 年。

九、紀錄識別

各紀錄應明確記載紀錄製作人及製作日期，使能容易識別為何時、由何人製作的紀錄。

十、紀錄廢棄

（一）保存單位負責人應於每年○月將超過保存期間的紀錄廢棄之。

（二）依法規命令訂有保存期間者或個人資料保護管理執行小組認為該紀錄有作為參考資料應加以保存者，紀錄封面應明確記載「廢止文

本報告之智慧財產權歸屬於法務部

件」，以能明顯區別與最新版不同的狀態保存之。

十一、規則修訂

本規則於每年○月檢視，並於必要時修訂之。

本報告之智慧財產權歸屬於法務部

附件十三：申訴諮詢程序

一、接受申訴諮詢

（一）申訴諮詢承辦窗口負責人負責本機關之申訴諮詢。

（二）申訴諮詢承辦窗口負責人以外之人員接受申訴諮詢時，於確認申訴諮詢人之申訴諮詢內容後，迅速轉交給申訴諮詢承辦窗口負責人。申訴諮詢窗口負責人不在而無法應對時，迅速向個人資料保護管理執行小組報告，並由個人資料保護管理執行小組指示部門負責人應對之。

二、接受申訴諮詢之內容

應對人員應迅速將收受的申訴、諮詢內容通報個人資料保護管理執行小組，並得個人資料保護管理人之指示應對方法及核可。

三、應對申訴諮詢

（一）本機關應按申訴諮詢之內容，秉持誠信及採取適當方法應對之。

（二）應對人員應將申訴諮詢內容記載於「接受申訴諮詢表」，並通報個人資料保護管理執行小組。

1.「接受申訴諮詢表」所記載之應對方法內容於得個人資料保護管理執行小組核可後迅速執行應對。

2.申訴諮詢承辦窗口負責人確認應對方法內容

3.申訴諮詢承辦窗口負責人於確認「接受申訴諮詢表」內容後，通報個人資料保護管理執行小組，並依個人資料保護管理人之指示應對方法及核可。

四、個人資料保護管理人針對申訴內容判斷為需要擬定再度發生防止辦法時，得指示部門負責人分析申訴發生原因及執行再度發生防止方法之矯正預防措施。

五、規則修訂

本報告之智慧財產權歸屬於法務部

本規則於每年○月檢視，於必要時修訂之。

本報告之智慧財產權歸屬於法務部

附件十四：稽核程序

一、本機關為符合個人資料保護法之要求，並為確認本機關個人資料保護管理制度適當運作，於每年○月以機關內全體部門實施內部稽核。於稽核小組認為有必要時，得隨時進行內部稽核。

二、為確保稽核之客觀性及公正性，內部稽核執行人員不得稽核所屬部門。

三、內部稽核計畫及其執行、稽核結果報告及維護紀錄之職責與權限按下列程序所訂定執行及維護。

四、稽核小組負責指揮內部稽核。

五、計畫

（一）稽核小組將稽核內容及執行內部稽核人員名冊，於預定執行內部稽核日前一個月，擬訂全年內部稽核計畫書，並得機關代表人核可。

（二）於稽核小組監督下，在確保稽核之客觀性及公平性，從內部稽核名冊選出執行內部稽核人員，並記載於全年內部稽核計畫書之執行內部稽核人員欄內。

（三）執行內部稽核人員根據全年內部稽核計畫書，於執行內部稽核預定日前 2 週內，作成個別部門內部稽核計畫書，並得稽核小組之核可。內部稽核執行人員於執行內部稽核預定日前一週內，製作受內部稽核部門之內部稽核查檢表。

六、執行

（一）內部稽核執行人員根據個別部門內部稽核計畫書，作成每個部門之內部稽核查檢表作為記載執行內部稽核之評鑑及評語。

（二）於內部稽核執行完畢後，受稽核部門負責人於確認內部稽核查檢表記載內容無誤後簽名之。如記載有誤時，當場向內部稽核執行人員提出異議。

七、稽核之判斷標準

本報告之智慧財產權歸屬於法務部

（一）內部稽核之結果按以下分類由稽核小組與內部稽核執行人員判斷之。

（二）判斷結果由稽核小組於執行內部稽核當天或執行內部稽核完畢後，迅速以內部稽核糾正事項確認書通知受內部稽核部門負責人，並得其確認同意。判斷類別及標準如下:

判斷類別	稽核標準
重大不符合	違反個人資料保護法或其他相關規範或發生個人資料外洩等事故，得判斷為重大不符合者。
輕微不符合	雖得判斷為不符合但對於個人資料當事人及機關沒有重大影響者。
要求改善	雖得判斷為不符合但有期待得為改善者。
優良	根據個人資料保護法訂定機關內部規則並充分落實執行規則作法者。

（三）受內部稽核部門負責人對內部稽核糾正事項確認書所記載之內容不服時，得當場向稽核小組提出異議。稽核小組於發生異議時，就異議之內容與內部稽核職人員充分討論後進行判斷。

（四）若有判斷為「重大不符合」者，稽核小組應即刻向個人資料保護管理執行小組及該部門負責人提出包含立刻停止重大違反行政業務之執行等適當之指示，並直接向機關代表人報告所有情形。

八、報告內部稽核結果

（一）稽核小組將記載評鑑與評語之內部稽核查檢表與所製作之內部稽核報告書於執行內部稽核後 1 週內向機關代表人報告之。機關代表人於聽取稽核小組內部稽核報告後，應指示進行矯正預防措施。

（二）根據內部稽核發現糾正、改善事項時之詳細程序依矯正預防措施程序，為改善之指示、執行及改善完畢之報告。

九、紀錄維護

本報告之智慧財產權歸屬於法務部

（一）稽核小組管理、保存內部稽核相關紀錄。

（二）稽核小組向機關代表人所為之報告紀錄均以檢視修正會議紀錄管理、保存之。

十、矯正預防措施

受內部稽核部門負責人對於內部稽核之結果有重大不符合、輕微不符合或要求改善者，應根據矯正預防措施程序採取適當矯正預防措施。

十一、稽核小組將滿足下列資格者製作內部稽核執行人員名冊。稽核小組將所作成之內部稽核執行人員名冊向機關代表人提報後，由稽核小組任命內部稽核執行人員。稽核人員建議具備以下能力:

（一）受過個人資料保護管理課程中階課程以上者

（二）充分瞭解本機關個人資料保護管理制度者

（三）瞭解受內部稽核部門行政業務者

（四）執行內部稽核時能保持客觀、中立者

十二、規則修訂

本規則於每年○月檢視，於必要時修訂之。

本報告之智慧財產權歸屬於法務部

附件十五：矯正、預防措施程序

一、於個資保護管理制度執行及運作時發現有不符合個資法之要求事項時，雖然目前尚不足以成為不符合事項，但置之不理將成為不符合要求事項的現象時，應儘速執行矯正預防措施。

（一）說明矯正預防措施之必要蒐集資訊之例子

（二）日常檢查中發現之不符合事項

（三）機關內外所提出之指正（包含驗證改善要求）

（四）內評所發現之不符合要求事項的現象

（五）客戶的申訴或要求

（六）機關代表人所做的矯正指示

（七）其他、發生緊急事故後及可能成為不符合要求事項的意外等

（八）權責劃分

二、由內評人員所報告的不符合事項由機關代表人核決之，並指示個人資料保護管理執行小組執行矯正預防措施。

三、確認不符合事項的內容

（一）由個人資料保護管理執行小組及該當部門負責人確認不符合事項的內容。

（二）清查不符合事項之原因及提出矯正預防措施方法

在個人資料保護管理執行小組的指示之下，由該當部門負責人清查不符合事項的原因及提出矯正預防措施方法。

（三）核決所提出的矯正預防措施方法

所提出的矯正預防措施之方法須由機關代表人核決。依據不符合事項現象之不同，核決可委由個人資料保護管理執行小組為之。

四、執行矯正預防措施

本報告之智慧財產權歸屬於法務部

（一）於個人資料保護管理執行小組之指示之下，由該當部門負責人執行矯正預防措施。

（二）矯正預防措施結果之紀錄

個人資料保護管理執行小組於該當部門負責人報告後，紀錄其矯正預防措施之結果。

（三）矯正預防措施之有效性量測

由機關代表人對所執行的矯正預防措施之有效性量測。

（四）矯正預防措施執行程序

1.確認不符合事項、報告及指示

（1）於內評時發現時，由內評人員確認「內評查檢表」「內評糾正事項確認書」中所紀錄的不符合事項的內容，於內評執行後 1 週內製作「內評報告書」向機關代表人報告之。

（2）在內評以外發現或取得不符合事項時，由個人資料保護管理執行小組迅速確認不符合事項的內容，以「收受詢問報告書」向機關代表人報告。

（3）機關代表人於核決報告內容後，指示矯正預防措施的指示。

2.清查原因與提出矯正預防措施方法

（1）於個人資料保護管理執行小組指示之下，由該當部門負責人清查不符合事項的原因與提出改善方法。提出矯正預防措施方法中，要設定措施執行完成日期及有效性量測的日程。清查原因、提出矯正預防措施方法及日程表應記載於「矯正預防措施報告書」中，經個人資料保護管理執行小組審核後由機關代表人核決之。

（2）機關代表人得依不符合事項之現象，將其核決權限委任於個人資料保護管理執行小組行使之。

（3）清查原因並非僅修正不符合事項之內容，而是要清查出根本的原因。有效性量測應考量不符合事項的現象後安排適當的日程。

本報告之智慧財產權歸屬於法務部

3.執行矯正預防措施方法

（1）個人資料保護管理執行小組應指示該當部門負責人於矯正預防措施完成日前完成改善。

（2）確認執行的矯正預防措施與紀錄結果個人資料保護管理執行小組應指示該當部門負責人將矯正預防措施之紀錄記載於「矯正預防措施報告書」中。

（3）個人資料保護管理執行小組應確認所執行的矯正預防措施有被適當地執行。矯正預防措施適當性的確認應以紀錄及所執行的內容對照為之。矯正預防措施不適當時，應指示清查其原因並再次執行相關程序。

（4）個人資料保護管理執行小組應向機關代表人報告所適當執行的矯正預防措施的結果，並記載於「矯正預防報告書」後得機關代表人核決。

（5）機關代表人得將核決矯正預防措施結果之權限委任於個人資料保護管理執行小組。委任時之核決人為稽核小組。

（6）審查執行措施之有效性個人資料保護管理執行小組應向機關代表人提出「矯正預防措施報告書」，並得機關代表人核可。

（7）機關代表人得將核決審查矯正預防措施結果之權限委任於稽核小組。委任時之核決人為稽核小組。

五、規則修訂

本規則於每年○月檢視，於必要時修訂之。

本報告之智慧財產權歸屬於法務部

附件十六：持續改善程序

一、檢視修訂時期

機關代表人於每年○月，對本機關個人資料保護管理制度進行檢視修訂。並於機關代表人認為必要時得進行臨時檢視修訂。

二、檢視修訂所需資訊

個人資料保護管理執行小組與稽核小組需於「修訂必要報告」中，記載針對檢視修訂所必要的資訊，並向機關代表人報告之。

三、有關稽核及個資保護管理制度的運作情形的報告

（一）包括諮詢、申訴等機關外部所提供之意見

（二）對於歷次檢視修訂結果之改善矯正情形

（三）個人資料保護法等相關法令、上級機關所訂定指引或其他規範的修正情形

（四）社會經濟情勢變化、一般社會大眾對個人資料保護認知的變化、相關技術進步等各種環境變遷

（五）行政業務項目增加、變更等機關業務領域的變化

（六）機關內外所匯集個人資料保護改善的提議

（七）除上述各項資訊外，「稽核報告書」中於有必要時尚須附加確認個人資料保護管理制度運作情形、檢查結果、新聞報導等參考資料。

四、進行檢視修訂

（一）機關代表人應針對修訂個人資料保護管理制度，召開個人資料保護管理制度檢視修訂會議。檢視修訂會議應參考「稽核報告書」、「修訂議事錄」及相關參

（二）考資料、機關外部環境等相關資訊。

（三）檢視修訂會議應有機關代表人、個人資料保護管理執行小組、稽核小組及建置、實施個人資料保護管理制度成員出席。

本報告之智慧財產權歸屬於法務部

（四）機關代表人應就本機關個人資料保護管理制度有改善處及對策等必要事項進行指示。

五、檢視修訂指示紀錄

機關代表人所指示之檢視修訂內容，應由個人資料保護管理執行小組或其代理人紀錄於「檢視修訂議事錄」。

六、根據指示實施措置

機關代表人所指示的內容，應於所指示的期間內實施檢視修訂後的措置，並由個人資料保護管理執行小組及稽核小組於「檢視修訂議事錄」中之「根據指示實施措置情形」欄位中記載報告內容，向機關代表人報告實施情形。

七、規則修訂

本規則於每年○月檢視，於必要時修訂之。

本報告之智慧財產權歸屬於法務部

附錄二、參考之程序表單

表單一：文件紀錄一覽表之一

附件　法規盤點清冊一覽表

制訂日	核決	
修訂日	製表	
修訂版		

No.	領域	文件名稱	頒布機關名稱	最新版年度	保存閱覽場所	最新版本確認人	最新版本確認日期	備註

本報告之智慧財產權歸屬於法務部

表單二：文件紀錄一覽表之二

附件 紀錄管理一覽表

制訂日	
修訂日	
修訂版	

核決	
製表	

No.	使用文件名稱	規則編號	核決人	製表人	製表時期	運作檢查	保存場所	保存期間	保存負責人	備註

本報告之智慧財產權歸屬於法務部

表單三：文件紀錄一覽表之三

附件 文件一覽表

制訂日	
修訂日	
修訂版	

核決	
製表	

No.	文件分類	文件名稱	制訂日	修訂日	核決人	主管部門	負責人	保存場所	備註

本報告之智慧財產權歸屬於法務部

表單四：個人資料盤點清冊

核決	個人資料保護管理負責人
製表	部門：

個人資料盤點清冊

No	個人資料名稱	資料項目	特定目的	特定情形	蒐集取得方法	保存場所	保存形態	保存期間	件數	廢棄方法	管理人	存取權限	當事人權利行使對	委託提供
1														
2														
3														
4														
5														
6														
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														
20														
21														

本報告之智慧財產權歸屬於法務部

表單五：委外廠商選擇評鑑表

業務名稱		
合格判斷標準	該當於下列之一者得選擇爲委外廠商。	
	1	已取得個人資料保護管理制度相關認證
	2	查檢項目1～3項爲「可」且締結「個人資料委託處理契約書」時。
	3	查檢項目**項目の**1～3項爲「不可」時，4～10項爲「可」, ②中填入選擇理由並得個人資料保護管理負責人核可者。
企業名稱/委託業務		
所處理之**個人**資料		

①	評鑑（　年 月 日　評鑑人：　　）		
	取得個人資料保護管理制度相關認證	☐	
	委託處理個人資料契約書	☐	

＜查檢**項目**＞		判斷	
1	制訂個人 料保護管理政策	☐	
2	**設置個人資料保護管理負責人**	☐	
3	**設置有關個人資料保護詢問窗口**	☐	
4	**進出**辦公室管理	☐	
5	**實施個人資料保護教育訓練**	☐	
6	**個人資料作業用電腦有引進防毒軟體等安全管理措施**	☐	
7	**個人資料作業用電腦禁止安裝**檔案交換軟體	☐	
8	**可事先指定或限定所委託個人資料作業之可作業人員**	☐	
9	**執行刪除廢棄安全管理措施**	☐	
10	**實施對再委託之安全管理措施**	☐	

②	**今後的改善方法及其他於評鑑選擇委外廠商**值得參考之資訊

③	**選擇（　　年　　月　　日　選擇人　　OO　　）**
	評鑑結果合格與否　（　是　・　否　）
	＜合格不合格之理由＞

④	**核決（　　年　　月　　日　個人資料保護管理負責人　）**

第 版

本報告之智慧財產權歸屬於法務部

表單六：委外廠商管理一覽表

		個人資料委外廠商管理一覽表				製表日期	
						製表人	
委外廠商名稱	委外廠商負責人姓名	委外業務內容	委外個人資料名稱	委外廠商評鑑結果	契約簽約日	聯絡窗口	機關業務負責窗口
						製表 / / 修訂 / / 第 版	

本報告之智慧財產權歸屬於法務部

表單七：當事人權利行使申請書

年　　月　　日

---機關名稱---

個人資料申訴諮詢窗口

個人資料當事人權利行使申請書

1．　權利行使之內容

1) 行使內容（查詢閱覽、製給複本、補充更正、停止蒐集處理利用、刪除、申訴諮詢）

_____

_____

2) 行使對象之個人資料

_____

_____

2．　權利行使對象之當事人個人資料

姓　名　：_____

住　址　：_____

_____

電話號碼　：_____

證明文件：

1)身份證　2)健康保險卡　3)駕照　4)護照　5）居留證

3．　法定代理人資料

姓　名　：_____印

住　址　：_____

電話號碼　：_____

證明文件：

1)身份證　2)健康保險卡　3)駕照　4)護照　5）居留證

本報告之智慧財產權歸屬於法務部

表單八：當事人權利行使紀錄表

當事人權利行使記錄表

（ 諮詢 ・ 當事人權利行使 ・ 申訴 ・ 其他： ）

年 月 日	
機關首長：	□可 □否

收受	收受日期： 年 月 日 ： 窗口：
當事人 基本資料	姓名： 性別：男 ・ 女
	電話號碼：
	住址：
確認當事人	＜ 當事人本人聯絡 ＞
	打電話：於確認姓名、住址、電話號碼，對照機關保存資料後以電話回覆
	親自來訪：1．□ 身份證 2．□ 健康保險卡 3．□ 駕照 4. □ 護照 5. □ 居留證
	＜ 非當事人本人聯絡 ＞
	與當事人本人之關係： 法定代理人姓名：
	法定代理人住址：
	法定代理人電話號碼：
	法定代理人證明文件： □ 身份證 □ 健康保險卡 □ 駕照
	□ 經當事人本人同意 ※確認當事人本人同意方法如下：
	打電話：□回答姓名・住址・電話號碼・身份證號碼 或 □已以登錄電話號碼回電
	親自來訪：□身份關係文件 或 □回答姓名・住址・電話號碼・身份證號
應對內容	

個人資料保護管理執行小組確認 印 年 月 日	□ 防止再度發生方法 必要(填寫矯正預防措施報告書) □ 防止再度發生方法 不要

製表 / / 修訂 / / 第 版

當事人權利行使或提出申訴諮詢對個人資料保護管理制度或其執行有重大影響者，應由業管人員填寫矯正預防措施報告書，防止同樣事件再次發生。

本報告之智慧財產權歸屬於法務部

表單九：全年內部稽核計畫書

年度 內部稽核全年計畫書(年 月~ 年 月)

機關代表人核可
年 月 日

製表: 年 月 日 製表人:(稽核負責人姓名)

稽核內容			
【目的】			
受稽核部門/應對負責人	內容	內部稽核執行人員	預定日期

製表 / / 修訂 / / 第 版

本報告之智慧財產權歸屬於法務部

表單十：個別部門內部稽核計畫

製表：　　年　　月　　日　／製表人：　〇〇

受內部稽核部門		應對負責人	
內部稽核類別	☐ 定期內部稽核　☐ 後續追蹤內部稽核　☐ 臨時內部稽核		
內部稽核目的			

內部稽核小組 ※主稽人員請以◎標記	
實施處所	
準備資料	
日期	**年　　月　　日**　　：　　～　　：

內部稽核內容	日程
	內容
	後續追蹤事項

製表　/　/　　修訂　/　/　第　版

本報告之智慧財產權歸屬於法務部

表單十一：個別部門內部稽核糾正事項確認表

製表：　　年　　月　　日　／製表人：　〇〇

受內部稽核部門		應對負責人	
內部稽核類別	☐ 定期內部稽核　☐ 後續追蹤內部稽核　☐ 臨時內部稽核		
內部稽核小組			
日期	年　月　日　：　～　：		

指摘事項	內部稽核結果
	糾正事項內容(記載原因明確時其負責人及其內容)
	1. 2. 3.
	判斷(１：重大・２：軽微・３：要求改善)
	1. 2. 3.

製表　/　/　　修訂　/　/　　第　版

本報告之智慧財產權歸屬於法務部

表單十二：風險分析表

負責部門及業務	

生命週期	蒐集、輸入(A)		傳遞、傳送(B)		處理・利用(C)		保存・備份(D)		刪除・廢棄(E)	
業務流程圖 盤點之個人資料	陳情書紙本		陳情書數位檔案							
	個人資料名稱	風險事項	個人資料名稱	風險事項	個人資料名稱	風險事項	個人資料名稱	風險事項	個人資料名稱	風險事項
個人資料作業及風險事項	陳情書	當事人資料填寫錯誤				透過業務流程之分析以了解個人資料之生命週期後（蒐集、輸入、傳遞、傳送、處理、利用、保存、備份、刪除、廢棄），針對不同				

本報告之智慧財產權歸屬於法務部

表單十三：內部稽核報告書

○○年度　內部稽核報告書

報告日期：_____

報告人（個人資料保護稽核負責人）：_____

受內部稽核部門	
實施內部稽核日期	
內部稽核主題	
執行內部稽核人員所屬部門	
＜內部稽核內容＞	
＜內部稽核結果大綱＞	
＜糾正事項・改善指示事項＞	

製表　/　/　　修訂　/　/　第　版

本報告之智慧財產權歸屬於法務部

表單十四：全年教育訓練計畫書

機關代表人核決

年度　全年教育訓練計畫書（　年　月～　年　月）

製表:　　年　月　日　／製表人(教育訓練負責人):

機關全體教育訓練			
【目的】			
【主要內容】			
教育訓練內容/教育訓練對象	執行負責人	予定日期	小時

個別部門教育			
【目的】			
【主要內容】			
教育訓練對象	執行負責人	予定日期	小時
訓練			
【目的】			
【主要內容】			
訓練對象	執行負責人	予定日期	小時

製表　／／　修訂:　／／第　版

本報告之智慧財產權歸屬於法務部

表單十五：個別部門教育訓練計畫、執行紀錄

教育訓練計畫 製表日期 年 月 日 執行教育訓練負責人（ ）		
教育訓練名稱		
教育訓練目的		
教育對象	總計 名	
執行教育訓練人（講師）		
使用資料		
預定執行日期		場所
例） 第 1 次 年 月 日		
第 2 次 年 月 日		
教育訓練內容		
＜反應上次教育訓練內容＞		
＜教育訓練內容＞		
確認教育訓練效果方法	例）問卷調查、隨堂測驗 等	
教育訓練負責人 核決	年 月 日	印
執行教育訓練記錄 製表日期 年 月 日 製表人（ ）		
＜執行教育訓練內容＞		
＜應出席學員人數/出席學員人數＞ 簡任 （ 名／ 名）		
薦任 （ 名／ 名）		
委任 （ 名／ 名）		
派遣、計時人員 （ 名／ 名）		
總 計 （ 名／ 名）		
＜本次教育訓練結果應反映於下次教育訓練事項＞		
教育訓練結果處理	□不需處理 □ 需要追蹤教育訓練 □其他	
處理內容		
教育訓練負責人 審核	年 月 日	印
個人資料保護管理負責人 核決	年 月 日	印

製表 / / 修訂 / / 第 版

本報告之智慧財產權歸屬於法務部

表單十六：矯正預防措施報告書

編號				年月日	
矯正預防措施執行部門		措施負責人 （部門負責人）		提出糾正不符合人	

矯正措施計畫	「不符合內容」（記載為內部稽核報告書<糾正事項・要求改善指示事項>、機關外部糾正等）			
	[原　因]（記載糾正事項發生的根本原因）			
	[防止再度發生方法]（提出消除發生原因之計畫）			
	提出計畫日期:		核決計畫日期:	
	提出計畫人: （部門負責人）		計畫核決人: （個人資料保護管理負責人）	
	預定執行矯正預防措施完畢日期:		是否需要確認矯正預防措施: ■是　□否	
矯正措施執行結果	[執行矯正預防措施 內容]			
	執行完畢日期:		核決日期:	
	提出計畫人: （部門負責人）		計畫核決人: （個人資料保護管理負責人）	
審核	[確認矯正預防措施效果及有效性]			
	執行日期:		核決日期:	
	報告人:		核決人（機關代表人）	

製表 ／ ／ 修訂 ／ ／ 第　版

本報告之智慧財產權歸屬於法務部

表單十七：機關代表人檢視修正會議紀錄

開會日期：
出席人員：
報告人：
記錄人：

【會議記錄】

【檢視修正之必要記錄】

【機關代表人有管檢視修正所指示之內容】

本報告之智慧財產權歸屬於法務部

表單十八：個資管理整體自評分析細項表

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
1	機關	機關是否已指派單位內負責個人資料管理的人員？					
2	機關	機關是否已組成個人資料保護機關，同時可清楚說明維護機關內部個人資料之管理作業權責？					
3	機關	承上題，上述要求是否已有文件化，載明成立個人資料保護管理機關及角色，並配置相當資源？					
4	機關	單位是否指派專人進行個人資料檔之管理及維護？					
5	機關	機關是否已清楚了解機關內有關個人資料之蒐集、處理、利用之範圍？					
6	機關	機關是否已辨識單位個資保護措施與個人資料保護法之適法性是否一致？					
7	機關	單位是否訂定經管理階層核准之宣告客戶、員工個人資料如何與何時被蒐集、利用、以及保護之個人資料管理政策？					
8	告知	機關直接蒐集個人資料是否已取得當事人書面、電話、傳真或電子方式同意？（法令授權免通知者除外）					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
9	告知	機關是否設置網站供公眾查閱個人資料檔案名稱、機關名稱、聯絡方式、資料檔案保有依據及特定目的、個人資料類別等？(公務機關)					
10	告知	機關依法向當事人直接蒐集個資時，是否明確說明蒐集個人資料的機關名稱,目的,個資類別,期間,地區,對象,處理方式/當事人行使權利及方式/不提供之影響？					
11	告知	機關是否提供清楚與明顯的說明予客戶或機關人員，有關個人資料的安全維護方式？					
12	告知	機關是否提供清楚與明顯的說明予客戶或機關人員，有關當事人如何查詢或存取其個人資料？					
13	告知	機關是否提供清楚與明顯的說明予客戶或機關人員，有關當事人如何更正或刪除其個人資料？					
14	告知	機關內間接蒐集之個人資料是否已規劃告知當事人？					
15	告知	機關是否設計提供當事人申訴、抱怨程序與管道？					
16	蒐集處理利用	機關是否有盤點機關內所有的個人資料，並建立清冊以利管理？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
17	蒐集處理利用	機關內是否針對各項個人資料之蒐集、處理、利用及銷燬建立資料流程圖以掌握資料流向及管理方式？					
18	蒐集處理利用	機關進行個人資料蒐集時是否遵循所屬主管機關的法規或公約（例如金融、保險、社會安全、健康照護等）？					
19	蒐集處理利用	機關內是否識別間接蒐集之個人資料之適法性及特定目的之合理性？					
20	蒐集處理利用	機關是否針對特種個資（醫療、基因、性生活、健康檢查、犯罪前科）進行蒐集、利用及處理？					
21	蒐集處理	機關若有蒐集特種資料是否取得法令依據？					
22	蒐集處理	機關若有蒐集特種資料是否清楚了解機關內有關特種資料之用途？					
23	蒐集處理	機關若有蒐集特種資料，是否有適當之安全維護計畫？					
24	蒐集處理利用	機關之個人資料管理是否有建立必要之使用紀錄、軌跡資料（Log Files）及證據之保存措施？					
25	蒐集處理利用	機關內是否有針為個人資料分級進行衝擊分析及風險評鑑？（含備份檔案及軌跡檔案）					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
26	蒐集處理利用	機關內是否有針為個人資料不同等級處理進行安控措施？（含備份檔案及軌跡檔案）					
27	蒐集處理利用	機關之是否執行資料安全管理？					
28	蒐集處理利用	機關是否執行人員安全管理？					
29	蒐集處理利用	機關之否執行設備安全管理？					
30	蒐集處理利用	機關內是否有針對個人資料顯示進行適當的去識別化？					
31	蒐集處理利用	機關與其它單位個人資料交換是否已識別個人資料之適法性及特定目的利用之合理性？					
32	蒐集處理利用	機關與其它單位個人資料交換是否已採取適當保護措施？					
33	蒐集處理利用	對於個資(紙本及數位資料)之存取及利用是否保有完整的紀錄、軌蹟資料					
34	蒐集處理利用	機關是否已針對受委託處理個資案件之單位，於契約上訂有個資保護法令及機關內部個資相關規定要求？					
35	蒐集處理利用	機關是否已針對受委託單位，於契約上訂有明確的監督要求?並執行監督?					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
36	蒐集處理利用	機關是否有將資料傳送於境外，該境外地區是否有個資保護法令(規範)，且已取得中央目的主管機關同意?					
37	訓練	機關是否已進行有效的個人資料保護全面性（含新人）人員宣導及教育訓練？					
38	訓練	機關是否針對負責管理及維護個人資料檔案之專人進行有效的專業教育訓練？					
39	程序	機關是否已建立個人資料內部管理程序或規則，以確保單位內個人資料蒐集、處理、利用、刪除及傳輸符合特定目的要求？					
40	程序	機關是否有設計當事人查詢、變更、刪除資料之程序？					
41	程序	機關是否有設計當發生個人資料被竊取、洩漏、竄改或其它侵害者事件之主動通知程序?					
42	程序	機關是否有設計風險評估及管理程序？					
43	程序	機關內是否有設計個資事故通報程序？					
44	程序	機關內是否有設計個資事故應變處理程序？					
45	程序	機關內是否有設計內部稽核程序？					
46	程序	機關是否有設計文件管理程序？					

本報告之智慧財產權歸屬於法務部

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
47	程序	機關是否有設計當個人資料蒐集目的消失或屆滿之資料刪除程序？					
48	程序	是否訂有個人資料檔案維護計畫及業務終止後個人資料處理方法等相關事項之辦法(中央目的事業主管機關)					
49	程序	是否訂有個人資料檔案維護計畫					
50	程序	是否訂有業務終止後個人資料處理方法					
51	程序	是否訂有抱怨程序					
52	程序	是否訂有証據保存程序					
53	程序	是否訂有維護資料正確性程序					
54	程序	是否有盤點單維護機制					
55	PDCA	機關對於個資之蒐集、處理與利用之流程，是否進行內部稽核？					
56	PDCA	機關是否定期檢視個資政策及個資保護執行結果？					
57	PDCA	機關是否有實施個人資料安全維護之整體持續改善規劃？					
58	其它	機關是否取得 ISO9000 認證（請說明認證範圍）？					
59	其它	機關是否取得 ISO27001 認證（請說明認證範圍）？					

本報告之智慧財產權歸屬於法務部