法務部
公務機關個人資料保護方案計畫
研究成果報告書

個人資料保護法制與機關相關規範報告

財團法人資訊工業策進會

日期：民國101年05月

目錄

圖目錄

表目錄

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

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。

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，

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

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。

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。

（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）.

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）.

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

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。

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

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。

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。

（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).

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）.

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）.

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

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。

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）.

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.

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

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.

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)

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）.

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).

（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。

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。

（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

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。

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。

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

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

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

（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

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。

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

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

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

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

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

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

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

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

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。

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

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

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

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

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。

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

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。

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

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

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

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。

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

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

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

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

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

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。

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。

（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。

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。

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。

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。

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

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。

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。

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

（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。

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、

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）。

（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）。

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。

（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。

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。

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

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？

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

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

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

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。

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。

（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。

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，

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

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

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。

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

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。

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。	♦ 范姜真媺教授： 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」）。

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

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

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.陳銘雄教授

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.陳銘雄教授

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

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. 陳銘雄教授

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？

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。

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，

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

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。

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？

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

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？

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。

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

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。

我國去前年五月（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、

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

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

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

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

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

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

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

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

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)

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：

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？					

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？					

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？					

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？					

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？					

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					

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					

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

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

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。

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。

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：

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

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：

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

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。

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：					

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

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

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

開機時間	未關機	關機時間	未關機
電力系統	正常	消防系統	正常
異 常 情 形			
狀況摘要			
處理情形			
備忘事項			
填表人員		機房管理人員	
安全官		科　　長	
執行人：　　主管：			

資料來源：地政司中部辦公室表單

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

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

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

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。

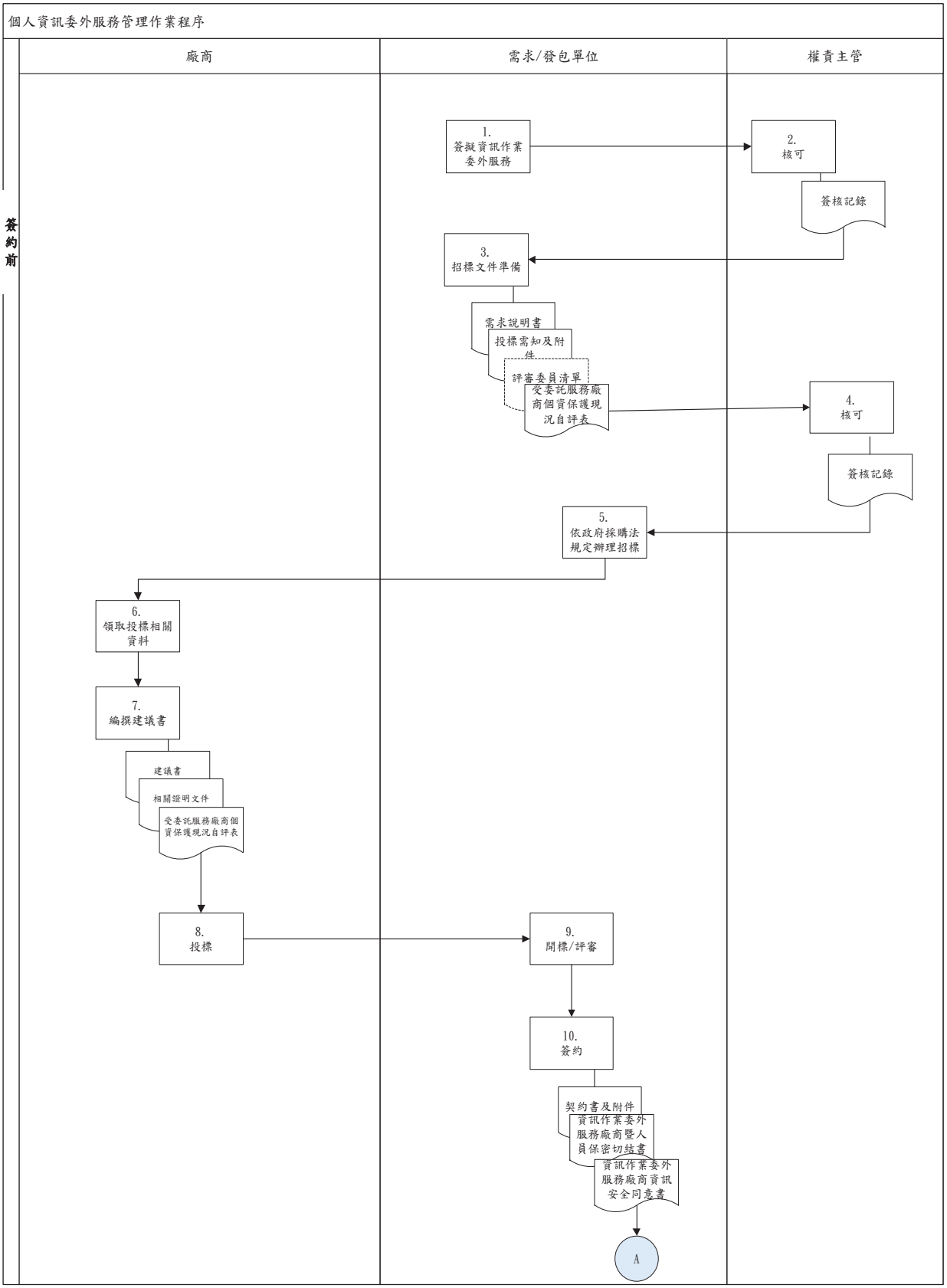
e.採購評選委員會組織準則。

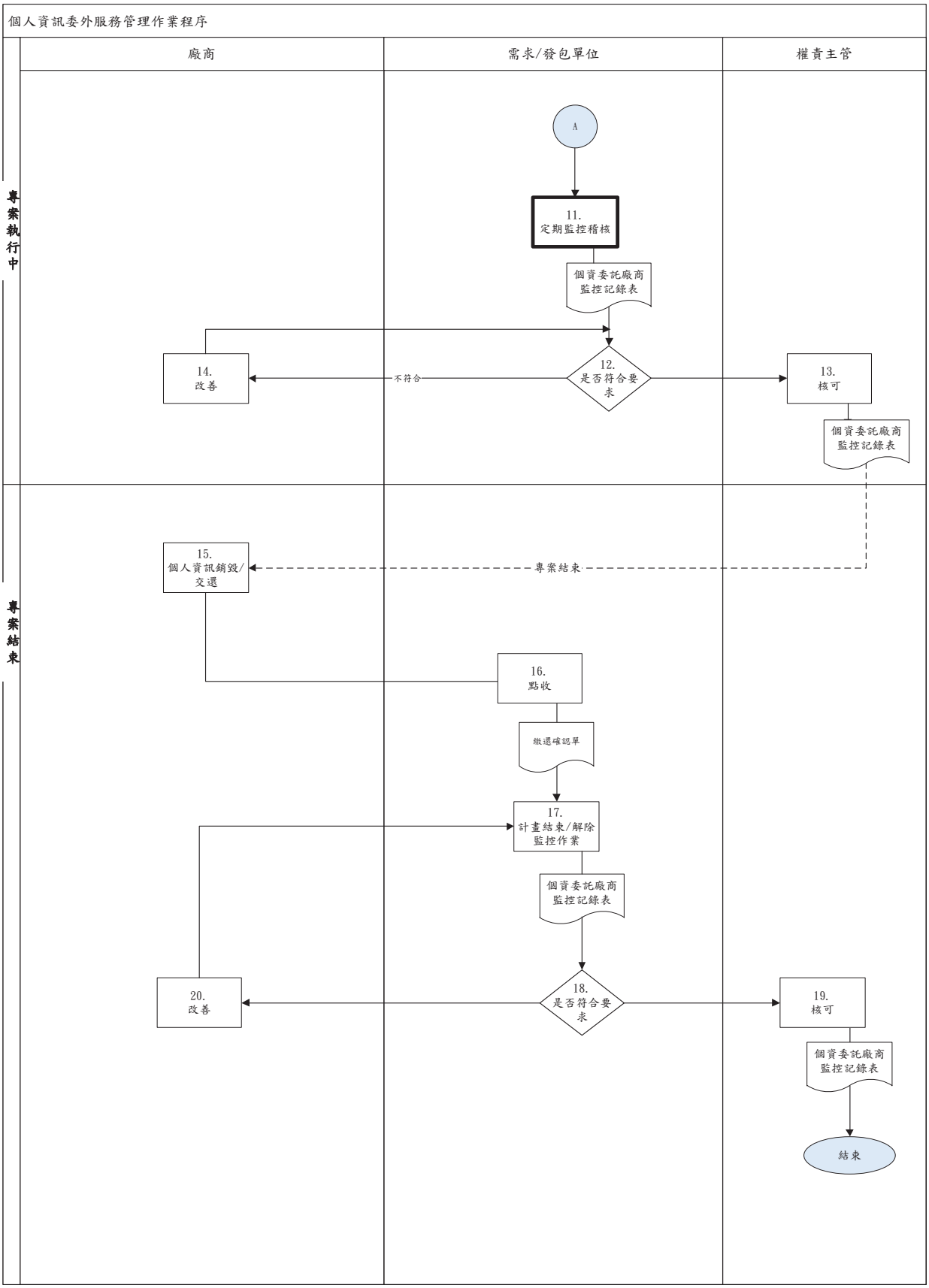
B. 其他有關之規章、辦法或規定，如：各機關資訊作業委外服務實施要點（行政院台 83 速授審字第 0205 號）

（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

（7）作業流程





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

（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

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>

	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

	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

	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:_____				

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

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

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

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

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			☐	☐	☐

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

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。

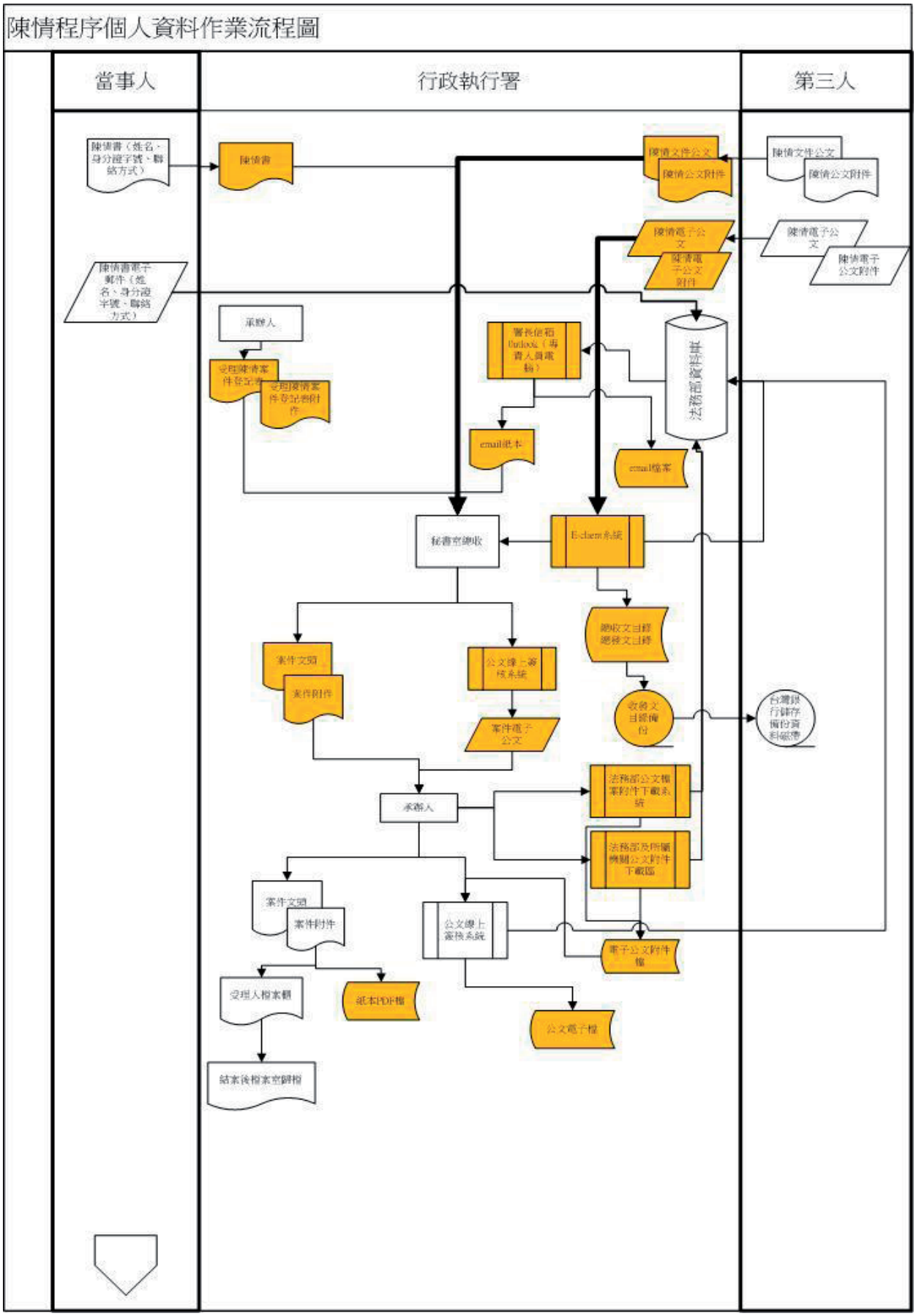
（4）導入成果報告

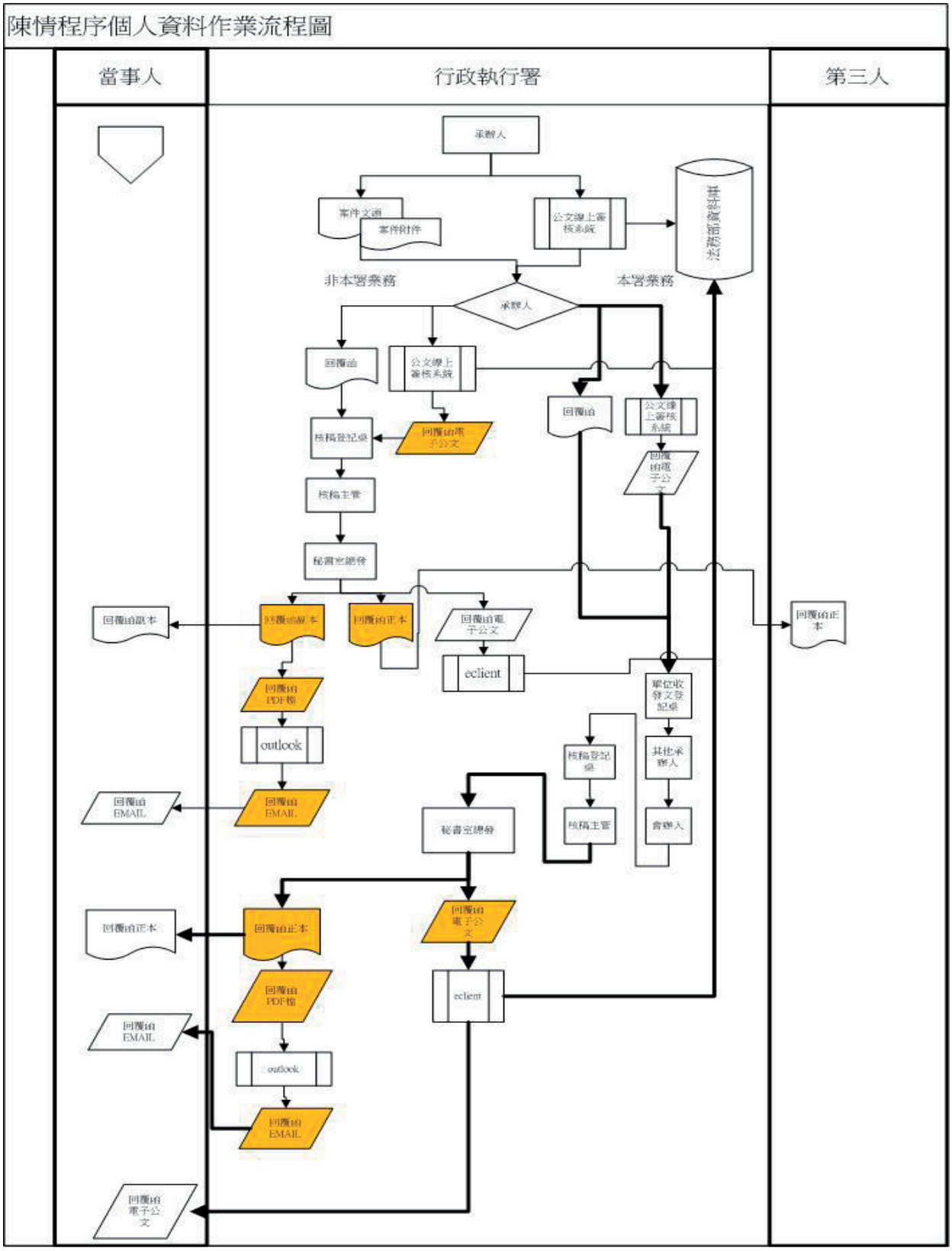
配合個資法之實施，經法務部選定檢察署及行政執行署就兩單位之陳情程序試行導入「個資盤點程序」。

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

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）





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

（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

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

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？

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

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

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

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。

（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:

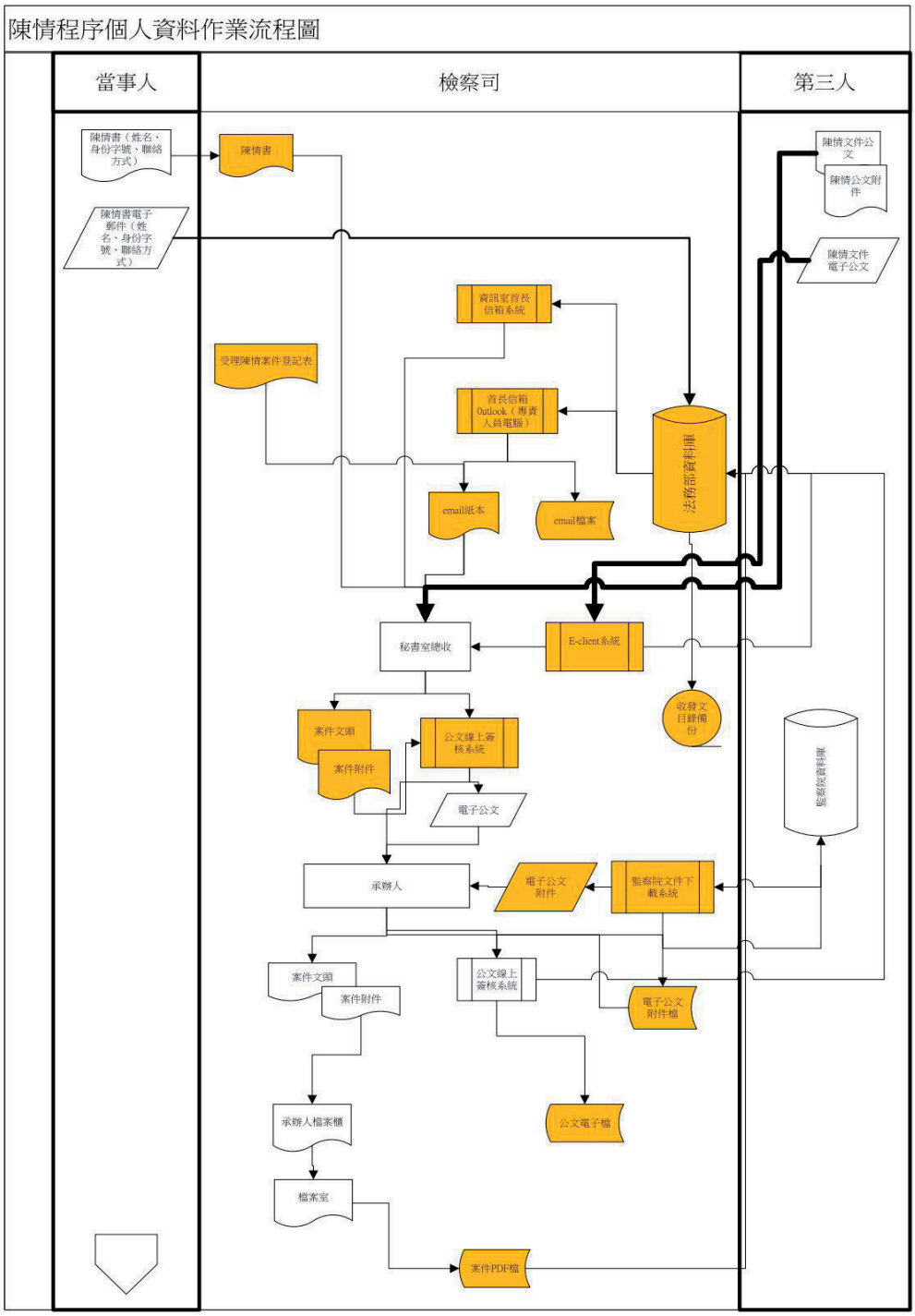
個人資料盤點清冊

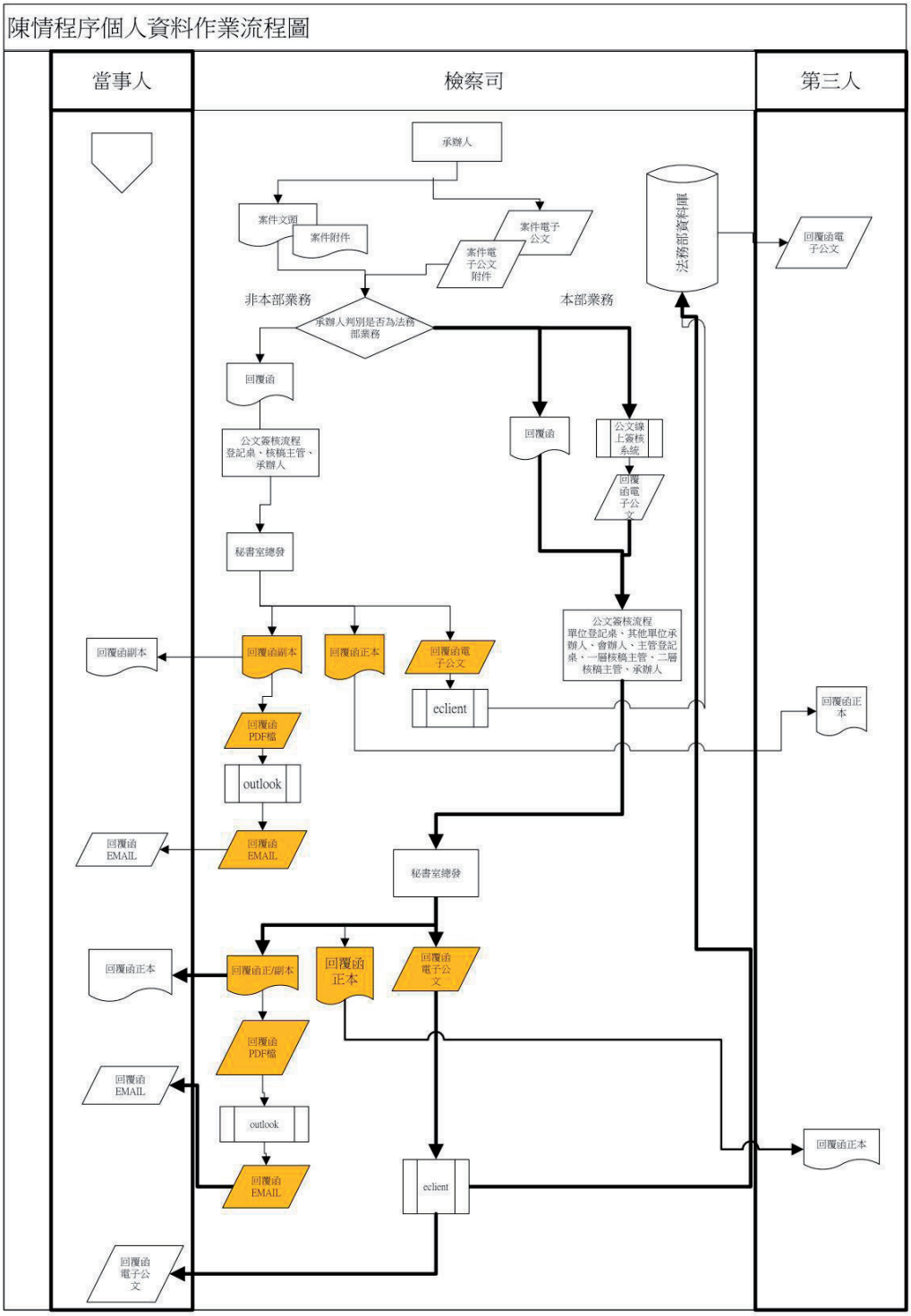
No	作業流程名稱	個人資料文件、檔案名稱	個人資料項目	特定目的	特定情形	蒐集方法	保存場所	保存形態	保存期間	件數	廢棄方法	管理人	存取權限	當事人權利行使對象	委託提供
1	陳情程序	陳情書	姓名、身份證字號、聯絡方式	陳情	執行法定職務（行政程序法§170Ⅰ）	直接	承辦人檔案櫃	紙本	10年			承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/核稿主管	可	有
2	陳情程序	受理陳情案件登記表	姓名、身份證字號、聯絡方式	陳情	執行法定職務（行政程序法§170Ⅰ）	直接	承辦人檔案櫃	紙本	10年			承辦人	承辦人/會辦人/總收文/總發文/收發文登記桌/核稿登記桌/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

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





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

（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

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？

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

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

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？

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。

（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

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:

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

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」）

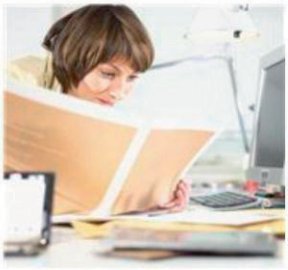
7.試行機關導入演練課程簡報

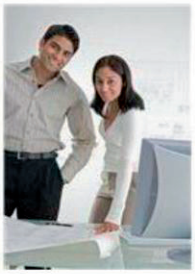
個人資料保護法介紹

資訊工業策進會 科技法律研究所
廖淑君 研究員
james@iii.org.tw
2012年5月09日

大綱

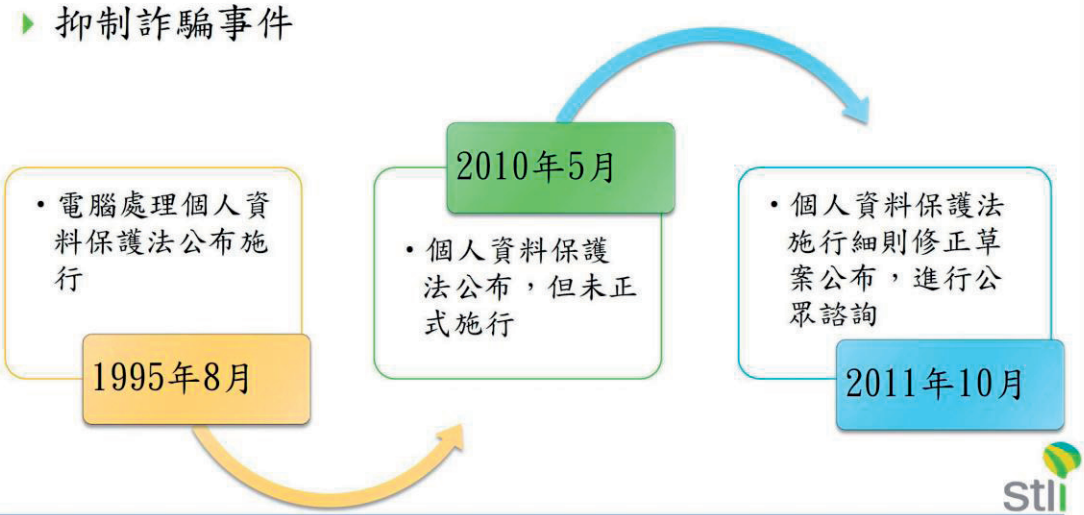
- 前言
- 個人資料保護法介紹-以公務機關為主
- 公務機關對於個人資料保護法通過之因應





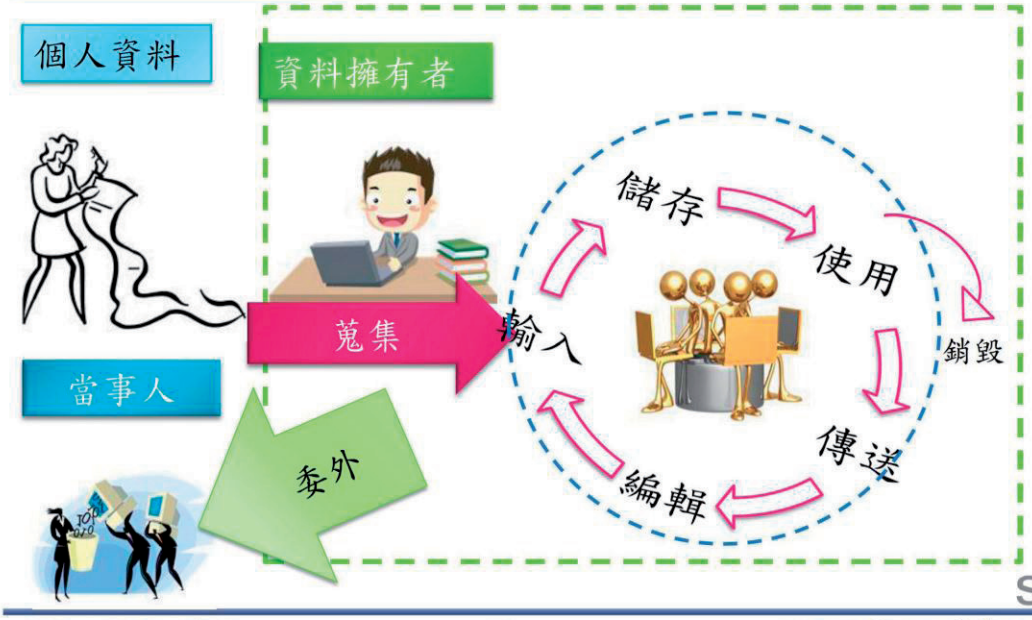
個人資料保護法的修法緣由與歷程

- 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



個人資料保護法架構(1/2)

個人資料生命週期



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）

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

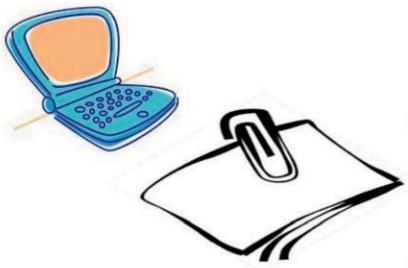
- 行政監督

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

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

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)

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

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)

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)

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)

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）

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

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

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
指紋、婚
病歷、聯
活動及其
別該個人

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

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

對於當事人之告知：間接蒐集

- 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
  - 當事人明知應告知之內容
  - 當事人自行公開或其他已合
  - 不能向當事人或其法定代理
  - 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

- 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
  - 資料利用之期
  - 區、對象及
  - 依第3條規定得行使之權利及方式

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)

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)

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

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

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)

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

蒐集
處理
利用

- 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

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

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）

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

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

EX: 法務部個人資料保護管理要點(2/2)(尚未下達生效)

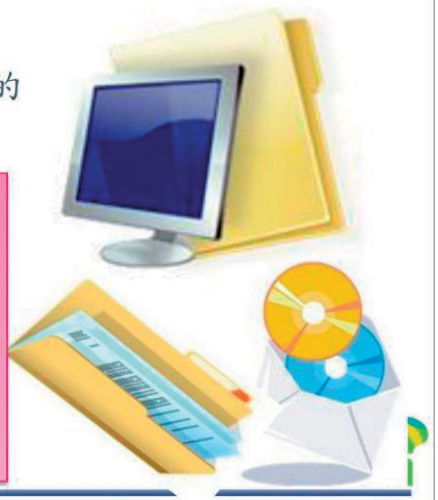
- 當事人行使權利之處理：
  - 明定當事人請求答覆查詢、提供閱覽、製給複製本、更正、補充、停止蒐集、處理、利用或刪除之處理程序、請求查詢、閱覽或製給個人資料複製本適用「法務部及所屬機關提供政府資訊收費標準」之規定並依「法務部受理申請提供政府資訊及閱覽卷宗須知」辦理、明定本部保有之個人資料檔案仍適用政府資訊公開法或相關法律規定，限制公開或不予提供。（草案第十九點至第二十三點）
- 個人資料檔案安全維護：
  - 明定專人應依本要點及相關法令規定辦理個人資料檔案安全維護事項、建立個人資料檔案應建立管理制度及人員安全管理規範、明定個人資料檔案安全稽核之組織及程序規定、個人資料檔案發生非法入侵情事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

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）

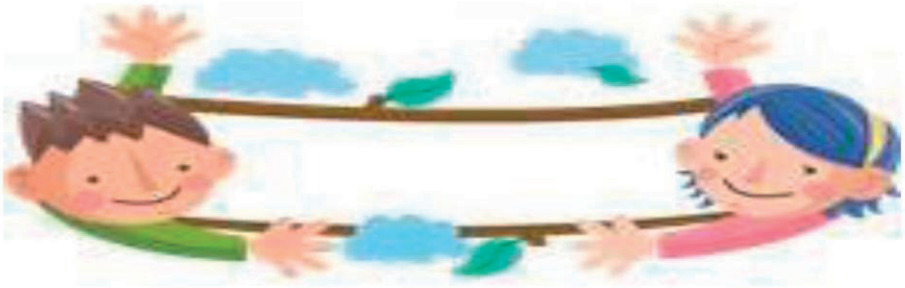


Ex:法務部保有個人資料檔案公開項目彙整表

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

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)

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

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)

損害賠償(2/2)

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

- 財產損害賠償
- 非財產損害
- 回復名譽之適當處分

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

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）

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)

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

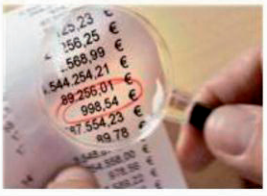
行政檢查
行政處罰
採取必要處分，以保護當事人權益不被繼續侵害

科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

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

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

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

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)

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

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)

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)

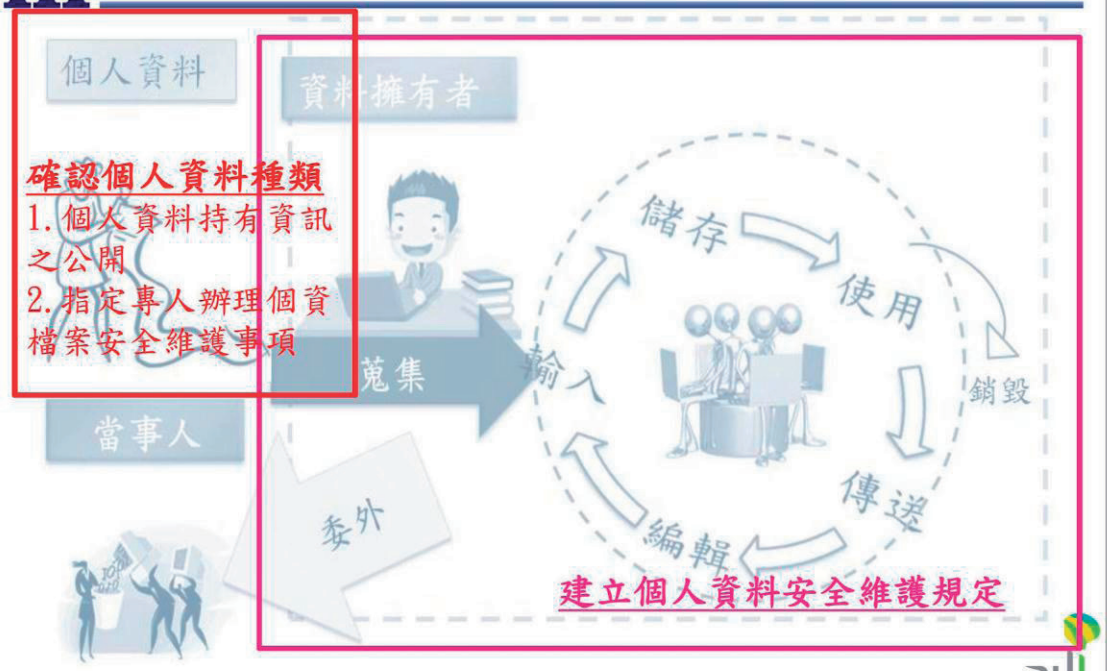
對於個人資料保護法通過之因應

科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

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

對於個人資料保護法通過之因應(1/2)



對於個人資料保護法通過之因應(2/2)

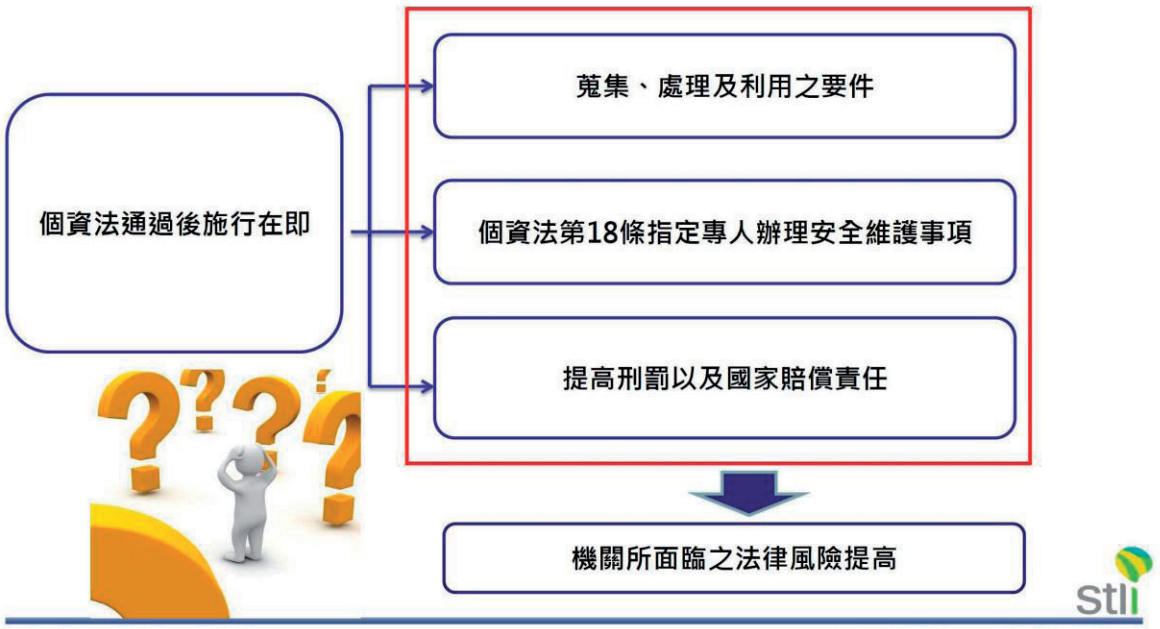
- 個人資料持有資訊之公開
  - 應將特定事項公開於電腦網站供公眾查詢，例如法務部公告“法務部保有個人資料檔案公開項目彙整表”
- 各公務機關應指定「專人」辦理個人資料檔案安全維護事項
  - 例如:法務部設置個人資料保護管理執行小組
- 公務機關保有個人資料檔案者，訂定個人資料安全維護規定
  - 例如:法務部草擬“法務部個人資料保護管理要點”
- 公務人員個資保護認知及法治概念之增進

資料來源：資策會科法所

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

前言

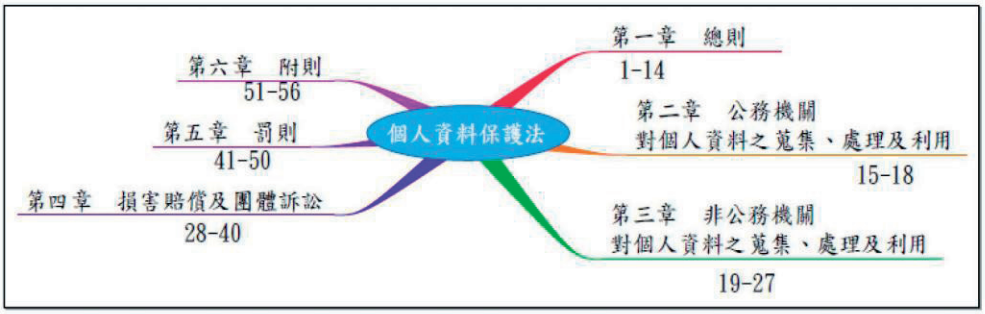


大綱

◆目的

◆作業手冊介紹

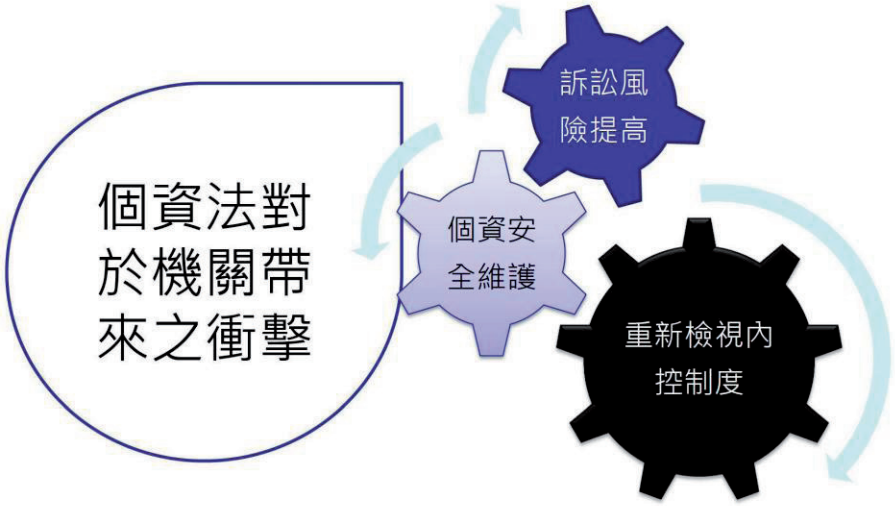
個資法之法規範目的



•目的

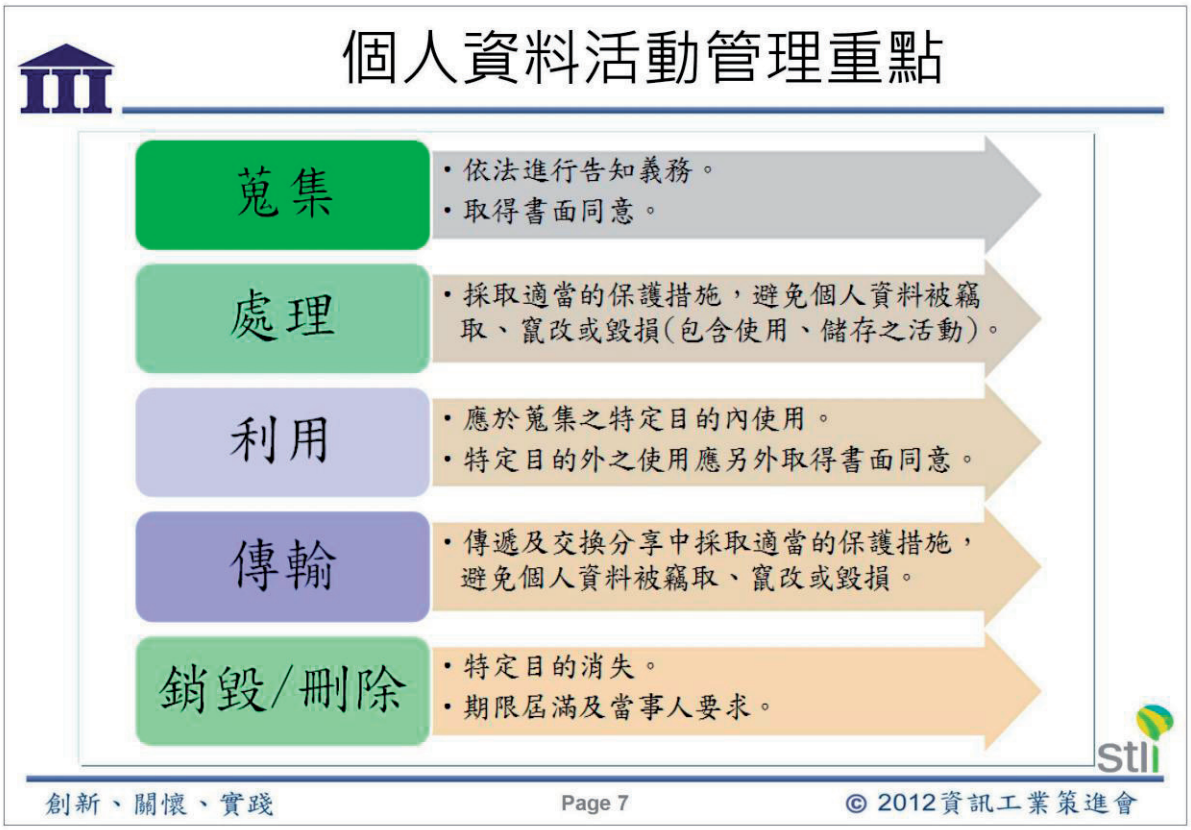
規範個人資料之蒐集、處理及利用，
以避免人格權受侵害，
並促進個人資料之合理利用

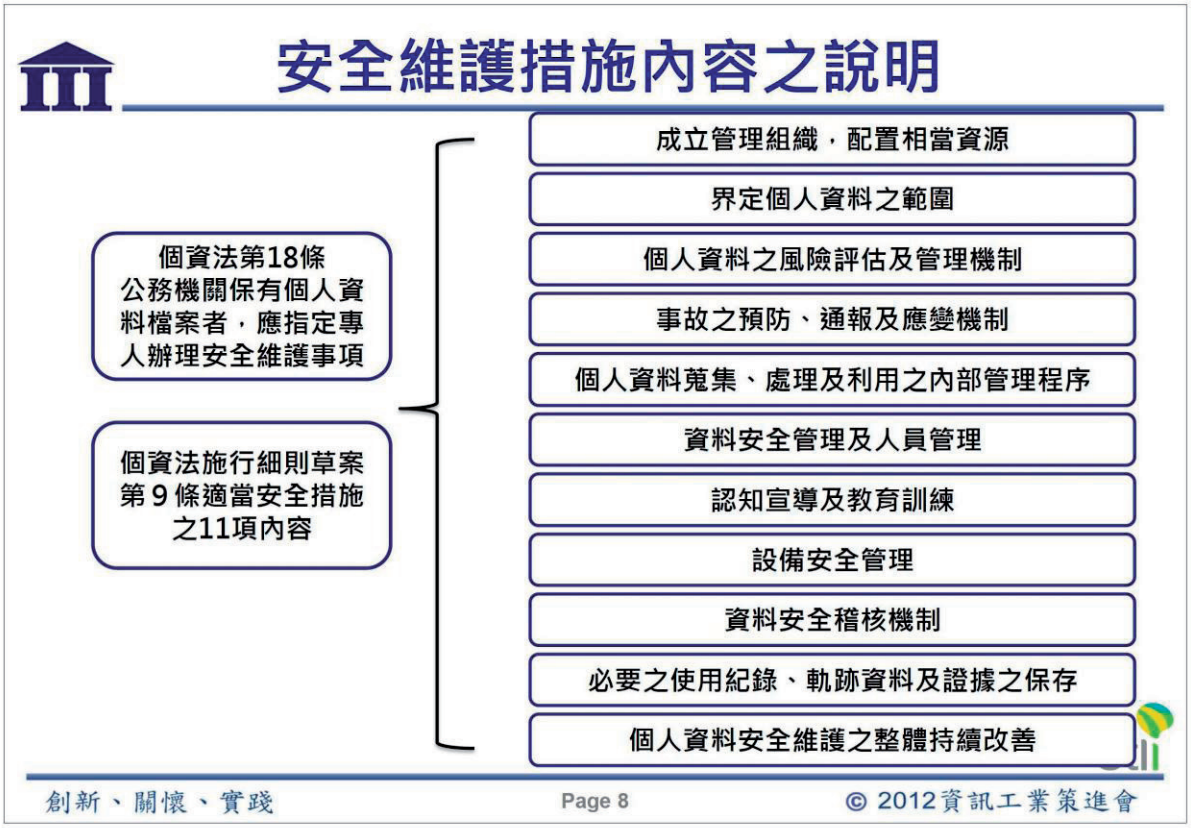
因應個人資料保護法對機關之影響



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。



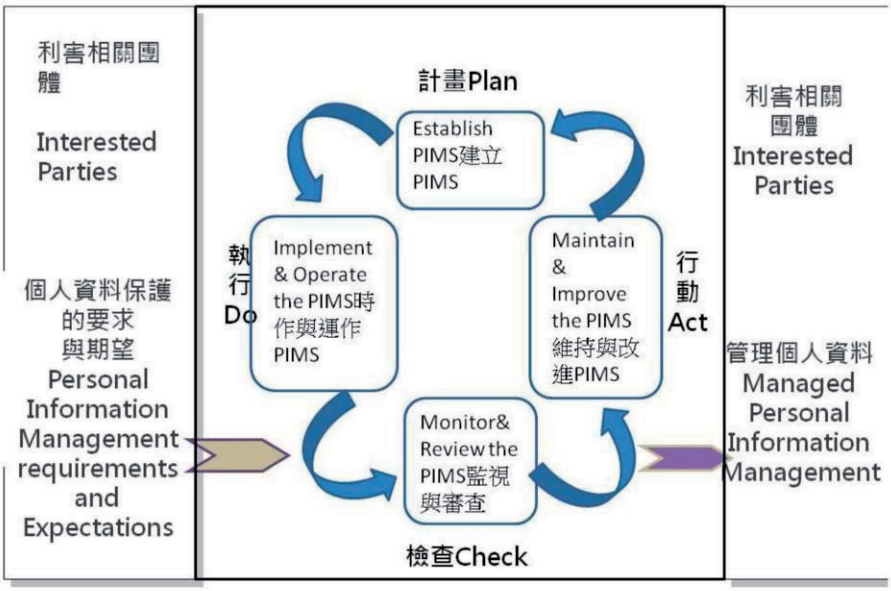


手冊之目的

- 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

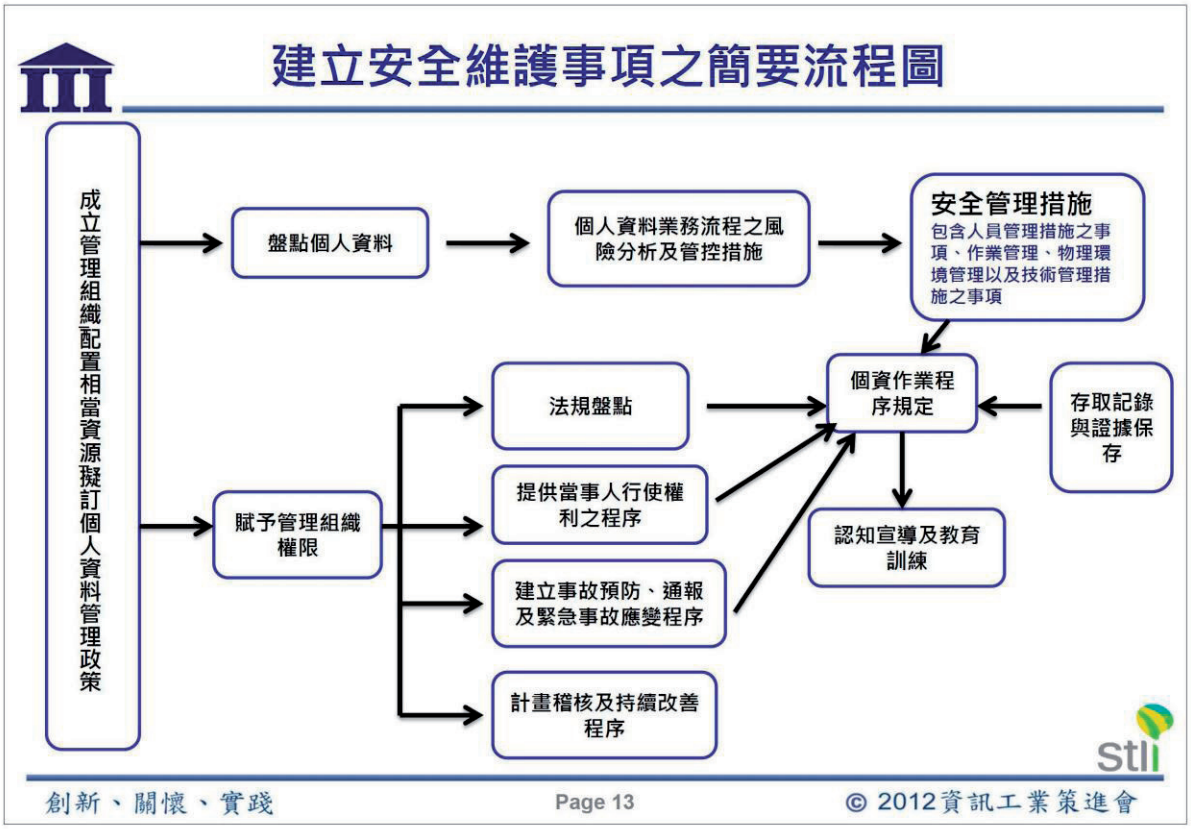
個人資料保護之PDCA架構

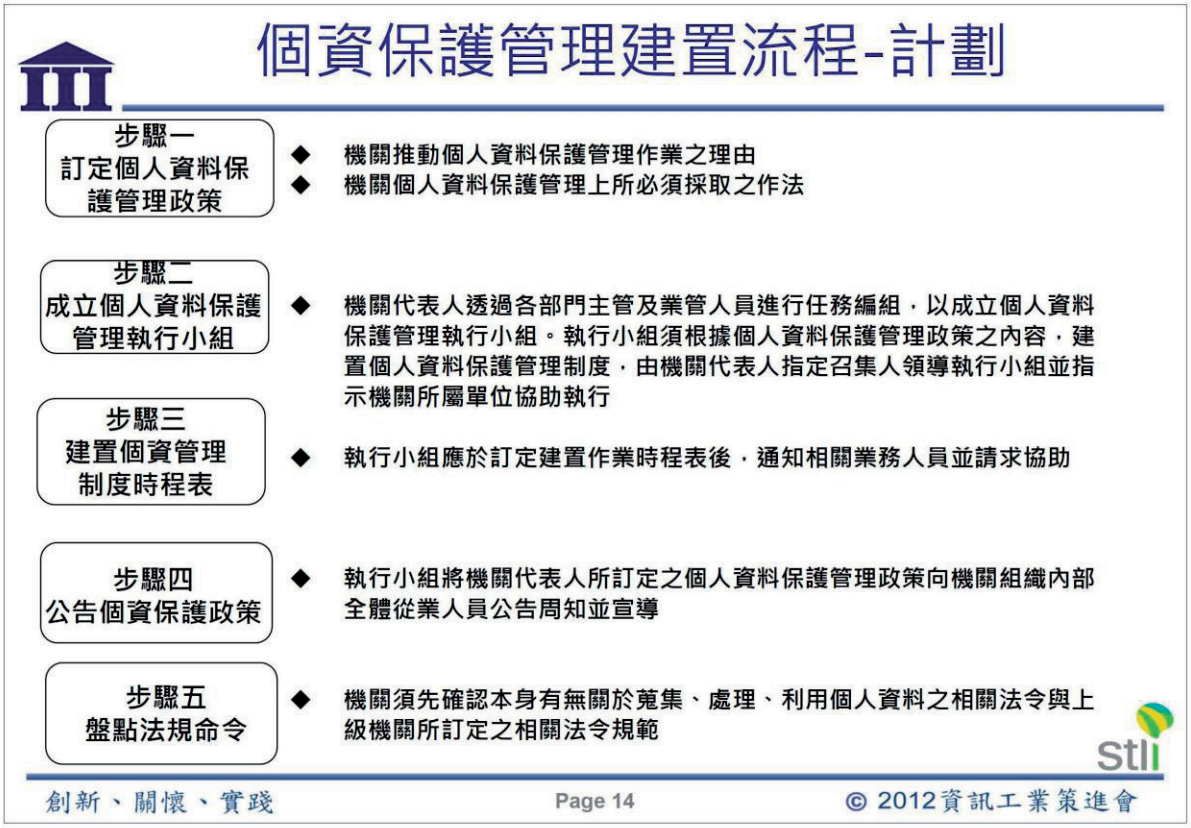


本圖出處：**BS10012**個人資料管理制度

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





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。

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**

個資保護管理建置流程-檢視

步驟十二
個資管理
報告檢視

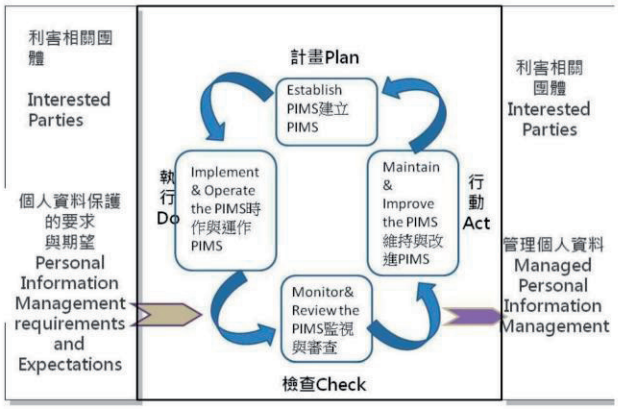
◆檢視個人資料保護管理制度之運作情形，並進行改善

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

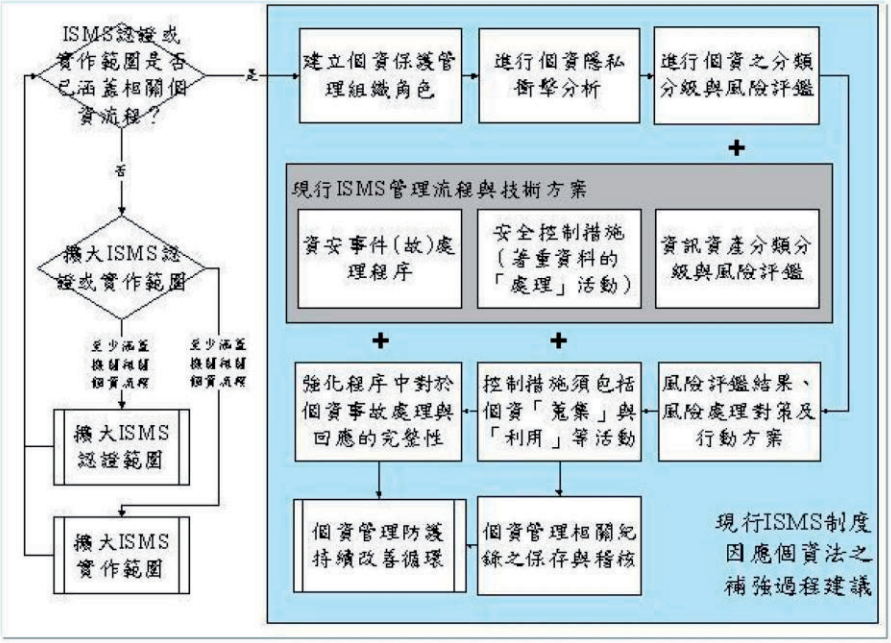
步驟十三
實施修正個人資料保護管理制度

◆ 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

ISMS與個資保護導入之整合



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 ？

個資事件/故應變

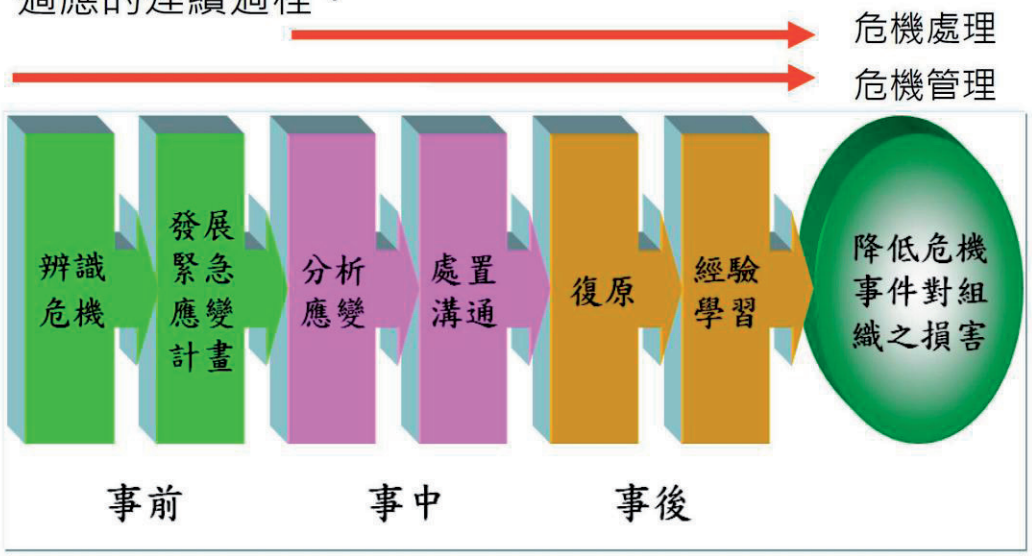
- 結合現有國家資通安全應變機制、公務機關事件分級之通報與處理以及研考會所公告之風險管理及危機處理作業手冊。
- 整合組織單一事件/故通報與處理程序
  - ➢如增列個資外洩類別
- 考量個資法之要求
  - ➢如查明後通知當事人之方式
- 定期演練測試
- 處置態度
  - ➢危機處理

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

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。

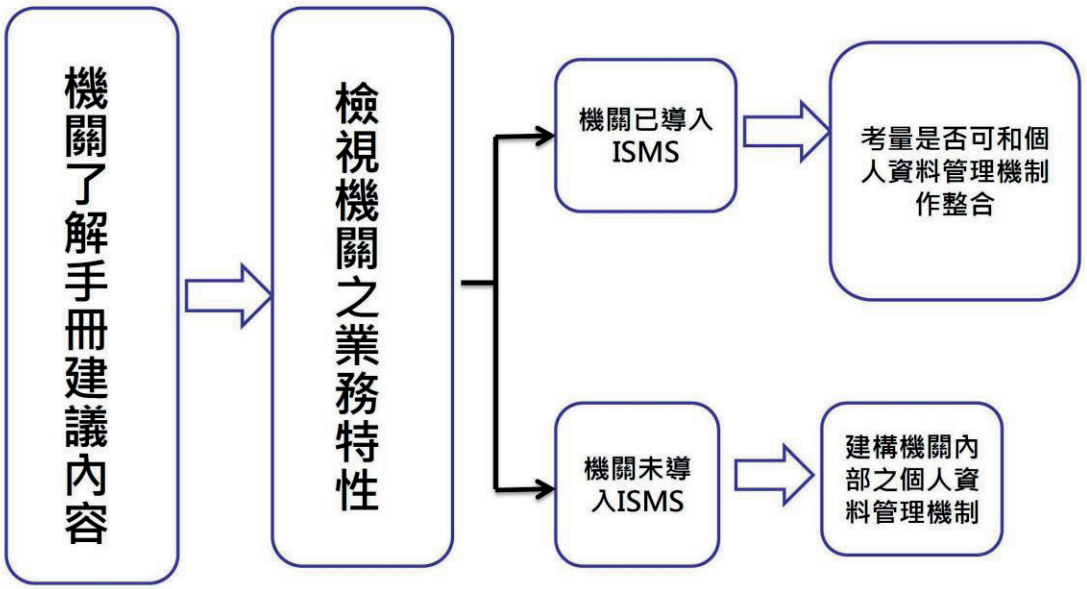
應針對危機事件訂定緊急應變計畫，並透過測試演練，驗證有效性。

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。

手冊應用流程



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

資料來源：資策會科法所

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

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）

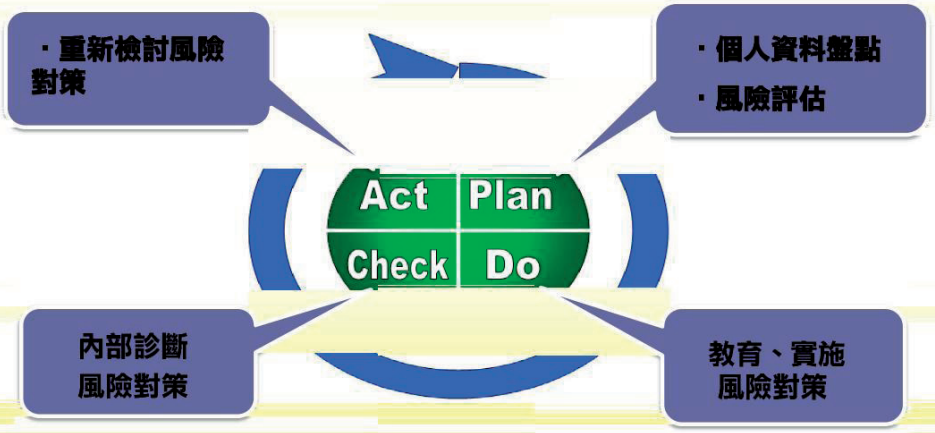
從個人資料作業的識別各個情境、評估風險，並訂定風險對策（風險評估）

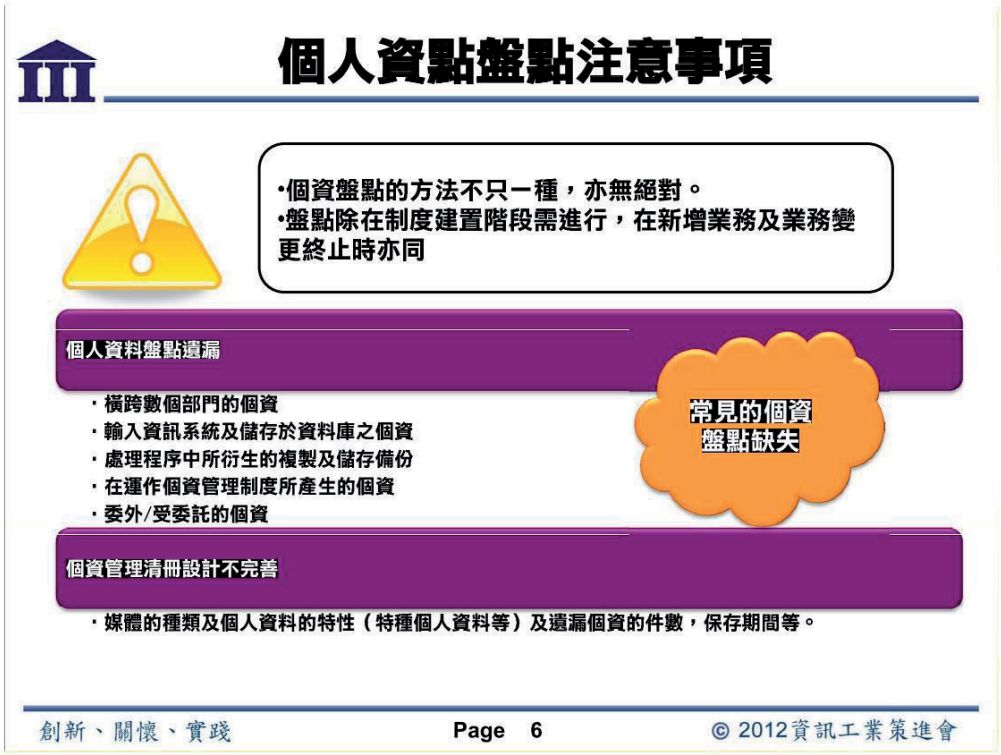
實施所訂定的風險對策，合法適當地處理個人資料，以達到保護當事人的權益

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

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）





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

- 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

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

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

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。

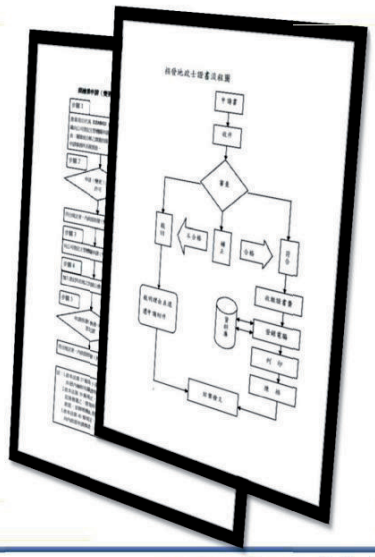
- 名片(非檔案化)
- 簽呈、會議紀錄(非以蒐集個資為目的)
- 主管行程表、會議簽到表(個資種類少)
- 報價單(專為業務聯絡用而委由業管人員處理)
- 便當訂購表、下午茶訂購表(重要性極低)

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



個資作業流程圖繪製

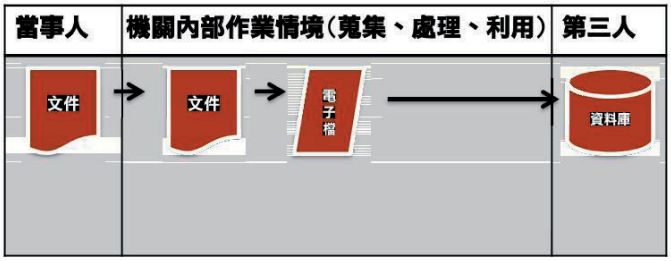
當事人 | 蒐集 | 處理 | 利用 | 委外

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

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

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

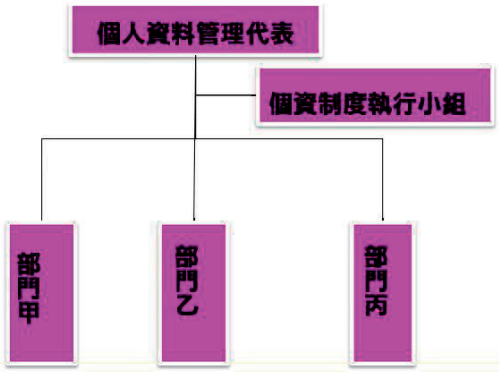
個資陳情作業流程盤點清冊參考

檢察司

行政執行署

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。



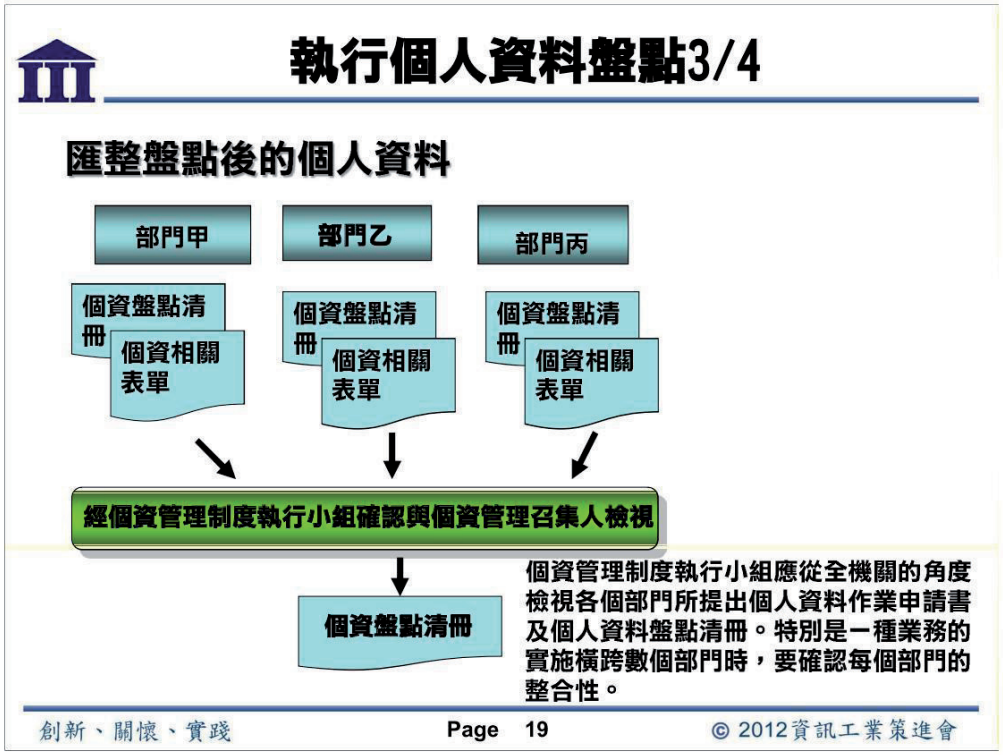
業務劃分	負責盤點個人資料人員
部門的固定業務（於該部門就可結束的業務）	負責該業務的部門主管與業管人員
橫跨複數部門的業務	各個相關部門的主管與業管人員
運作個資管理制度	個資管理制度執行小組

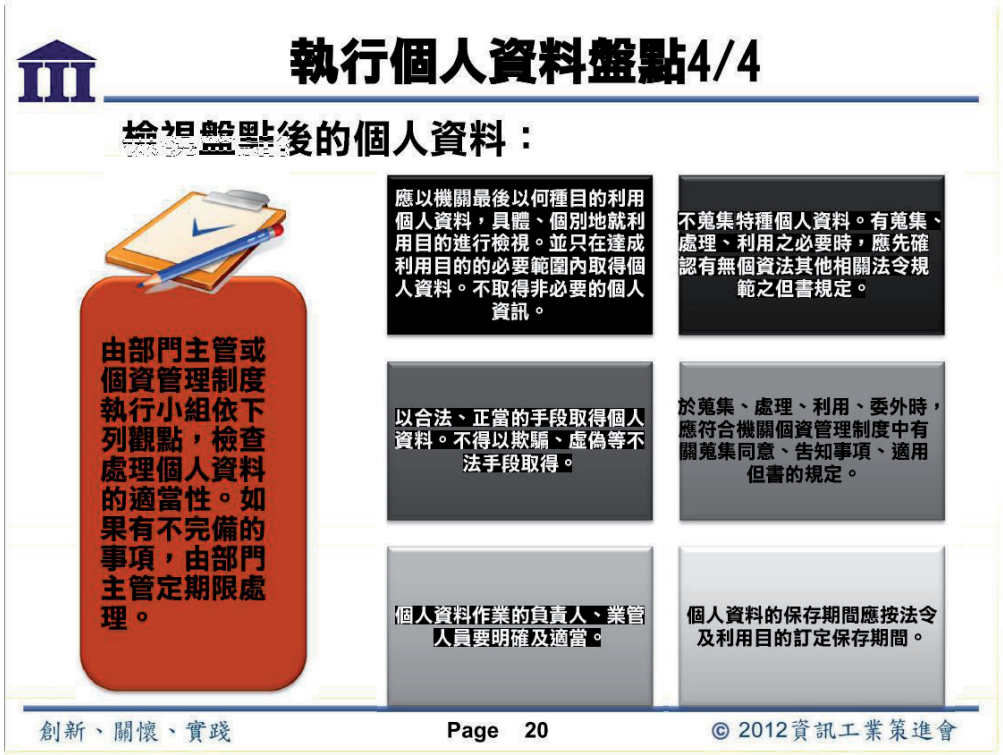
執行個人資料盤點2/4

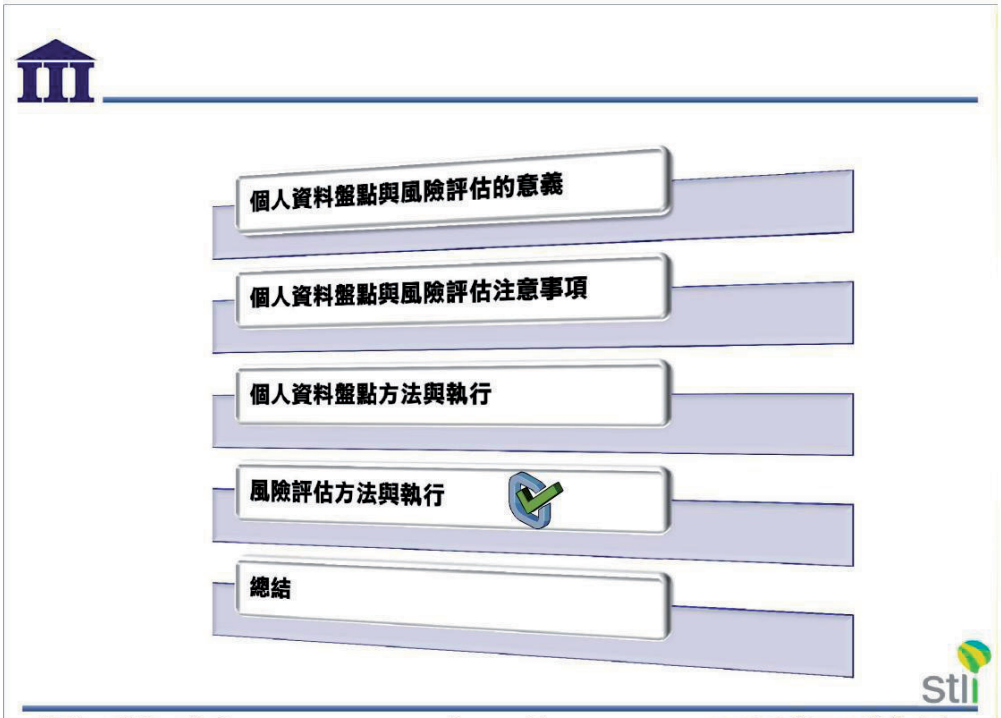
盤點個人資料時點：

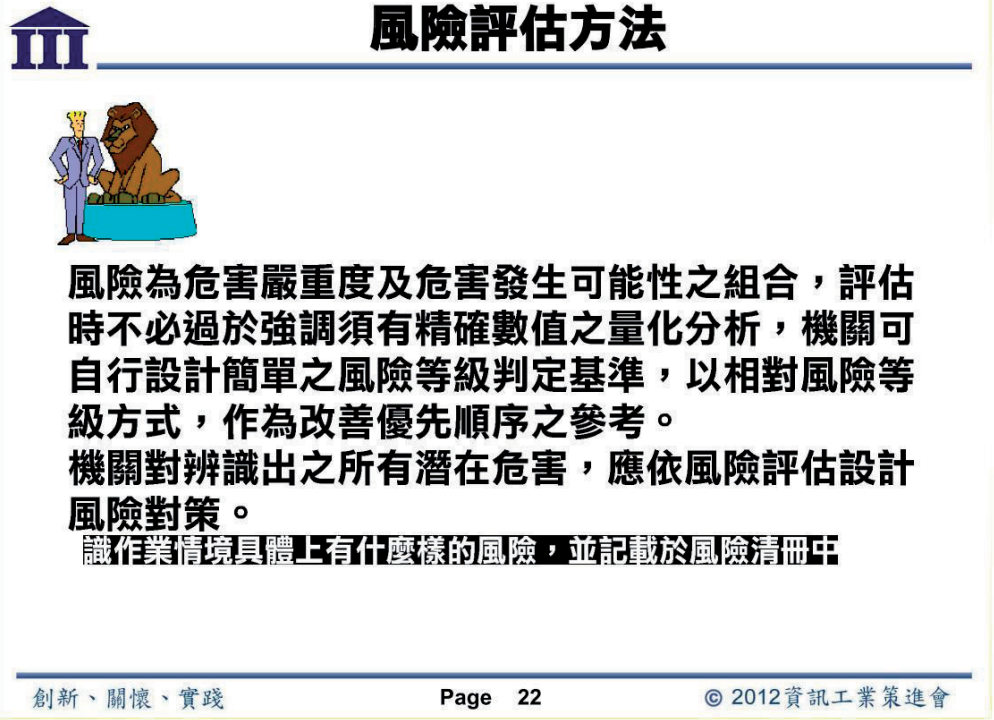
定期（至少一年一次以上）重新檢視盤點的個人資料有無變化。有發生變化時，根據上述程序處理。定期檢視是為防止處理個人資料有遺漏及變化。

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









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

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

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

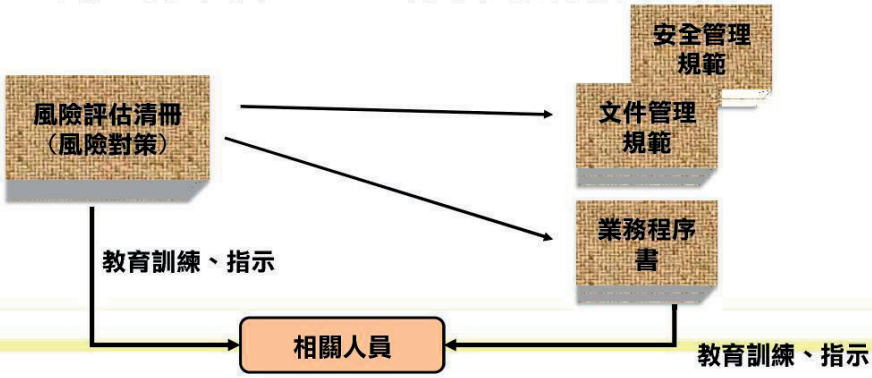
執行風險評估4/6

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 ）。

執行風險評估5/6

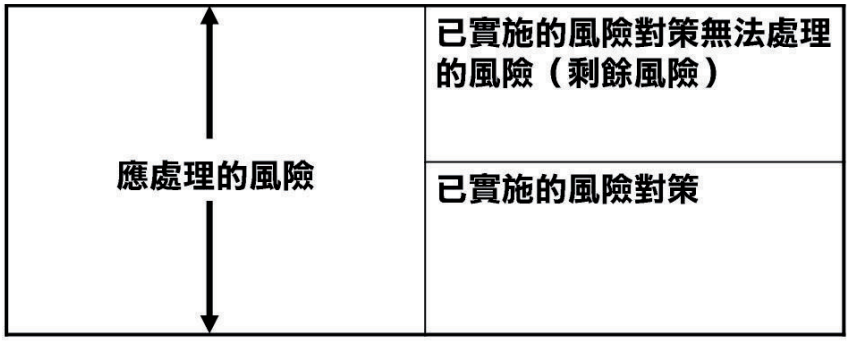
■ 反映到相關內部規範：所訂定的風險對策，必須徹底讓相關部門負責人瞭解。除將風險對策反應在相關內部規範或作業程序書，使相關業管人員可以隨時參照外，也必須加以教育訓練與指示。



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。 ）



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。

資料來源: 資策會科法所

事件通報管理程序

施叔良
財團法人資訊工業策進會

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

應涵蓋範圍

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。

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。

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。

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

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

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。

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

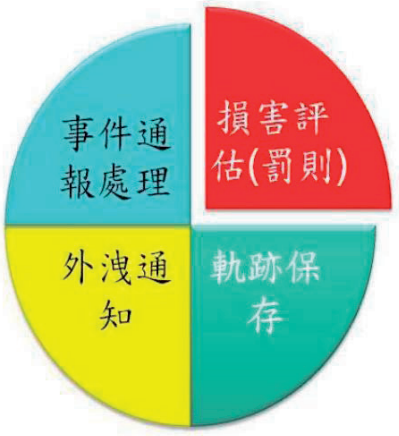
BS10012

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

Workshop

- 請思考設計個資事件通報單應有欄位



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。

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。

- 個資事件法律處理

資料來源: 資策會科法所

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

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。

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

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

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

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

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

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

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

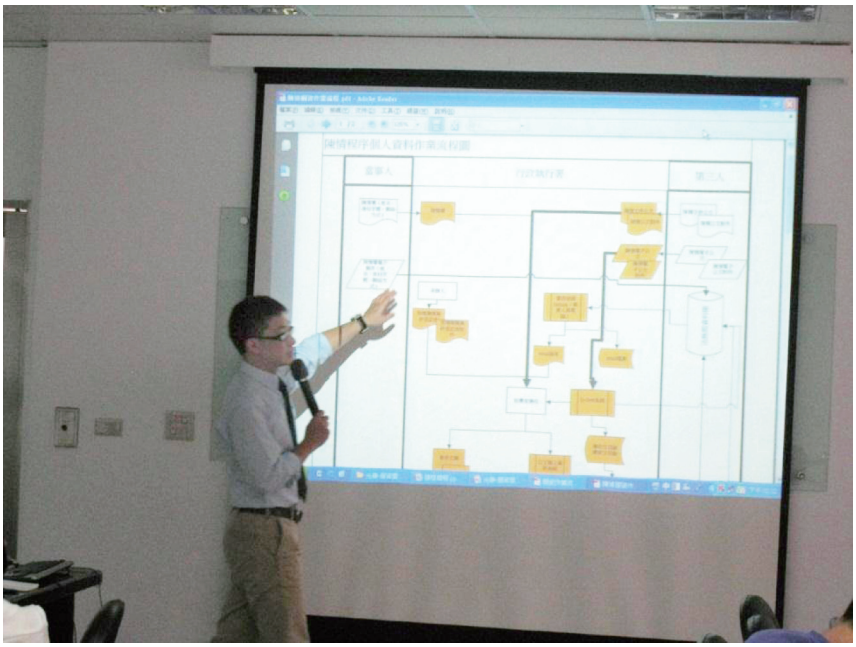
圖 7：資策會顧振豪組長為學員說明本次教育訓練活動的舉行目的

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」

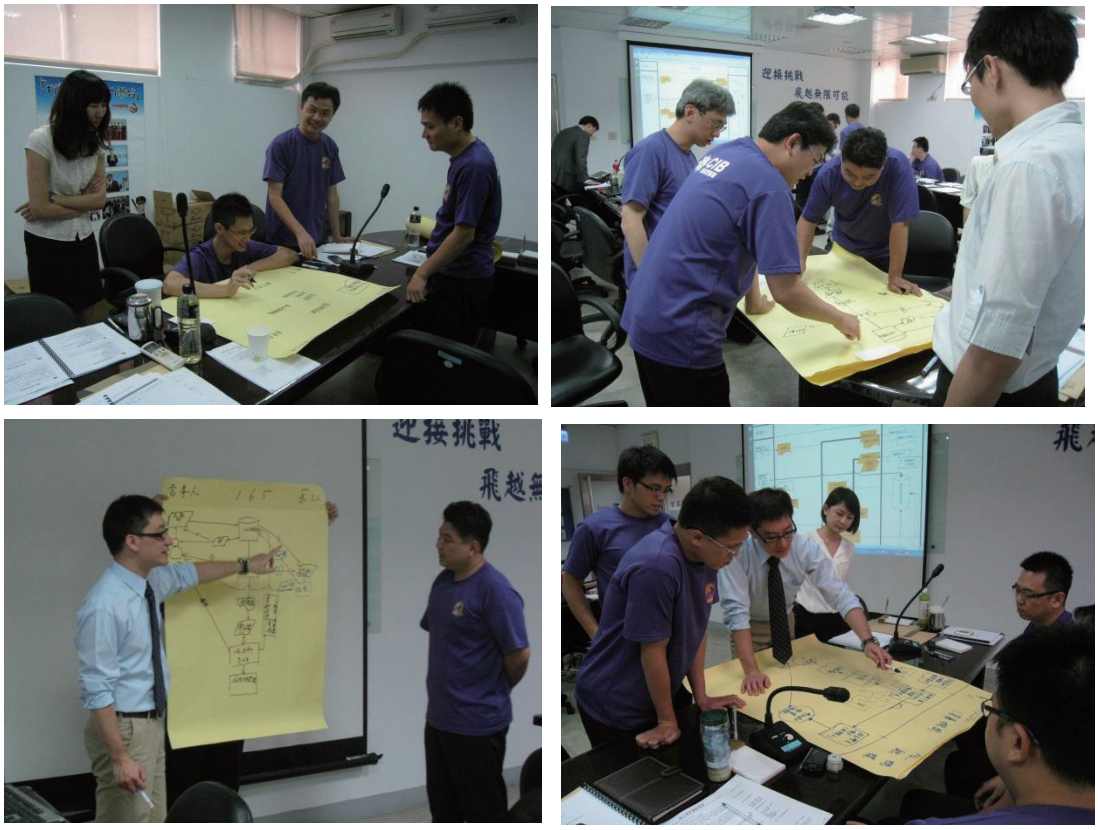
資料來源：資策會科法所拍攝

圖 9：資策會陳秭璇律師負責講授「考核作業手冊」



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

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」

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

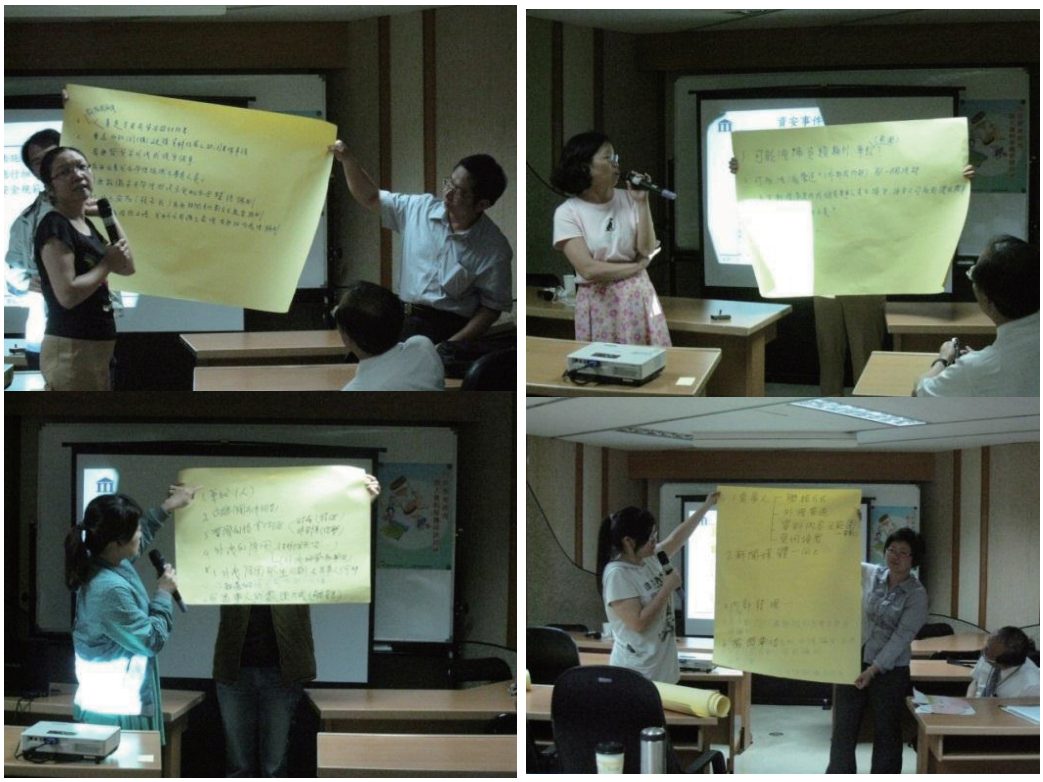
圖 15：資策會張曉芸研究員負責講授「個資盤點與風險評估」

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」



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」

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」

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」

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

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	40.00%	56.92%	3.08%	0.00%	0.00%

(陳秭璇律師)					
對講師表現的看法 (楊光華研究員)	61.54%	38.46%	0.00%	0.00%	0.00%
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：供本計畫活動產出

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%。

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

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

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。

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

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

C. 機關管理者

負責維護機關個資保護現況

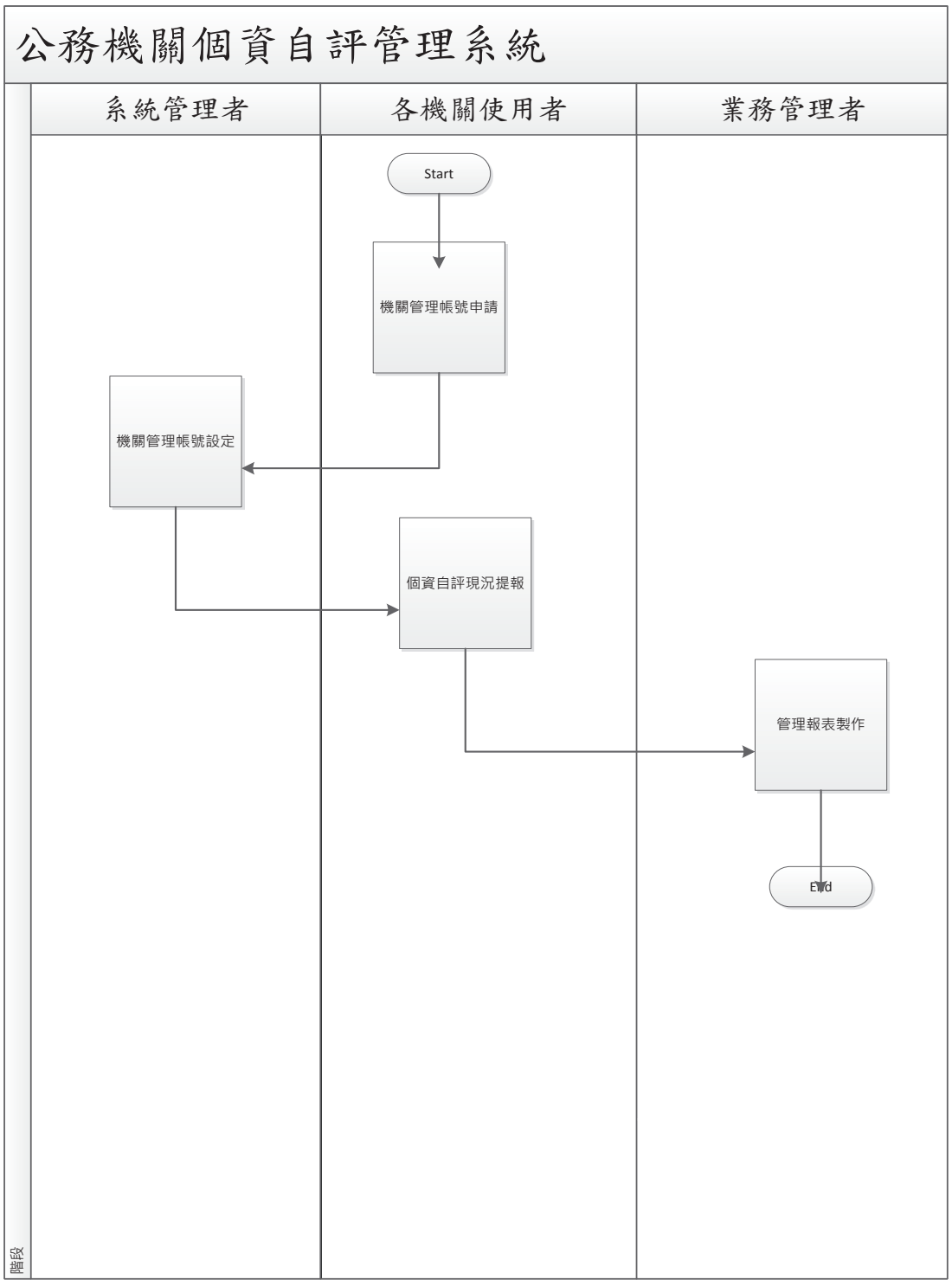
（4）名詞定義

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

（6）流程圖



資料來源:本計畫整理

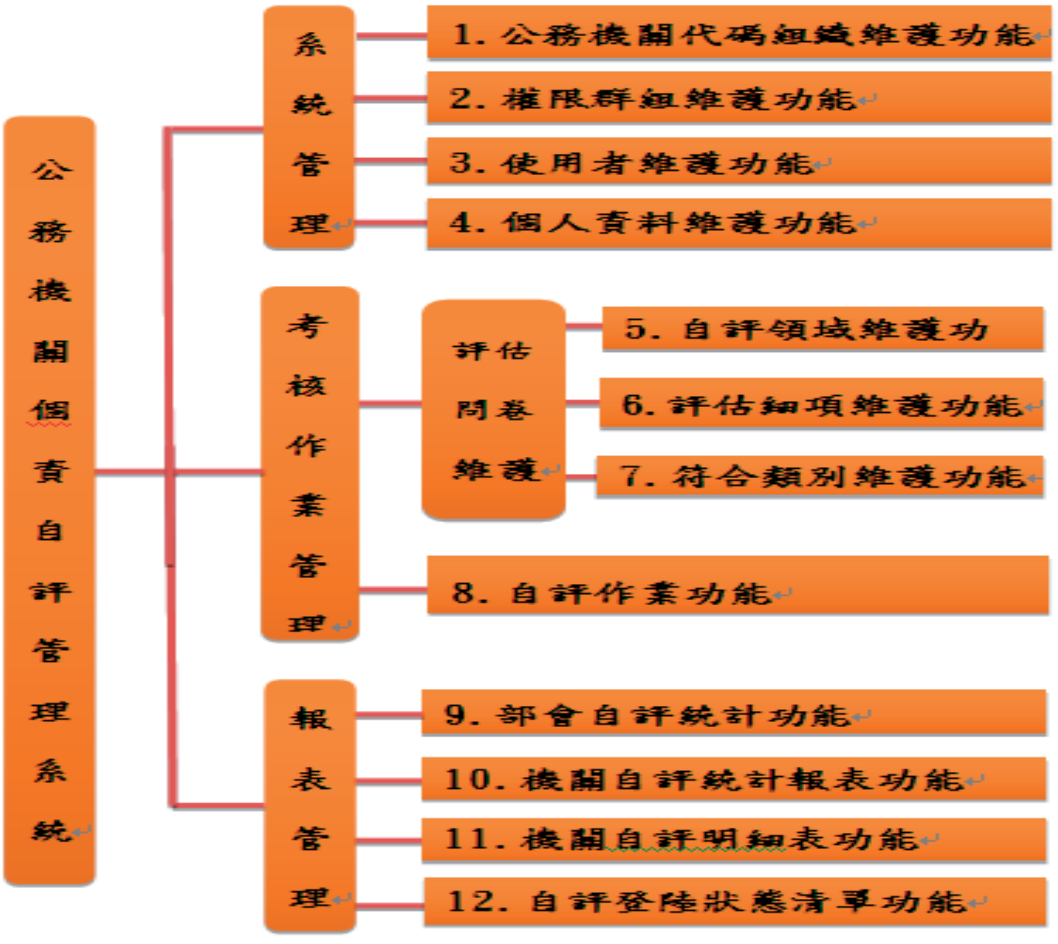
圖 25：公務機關個資自評管理系統流程圖

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

（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

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%。

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

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:

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。

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

（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？					

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）					

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？					

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？					

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？					

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？					

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?					

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？					

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？					

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					

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

（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？	

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？	

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

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

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

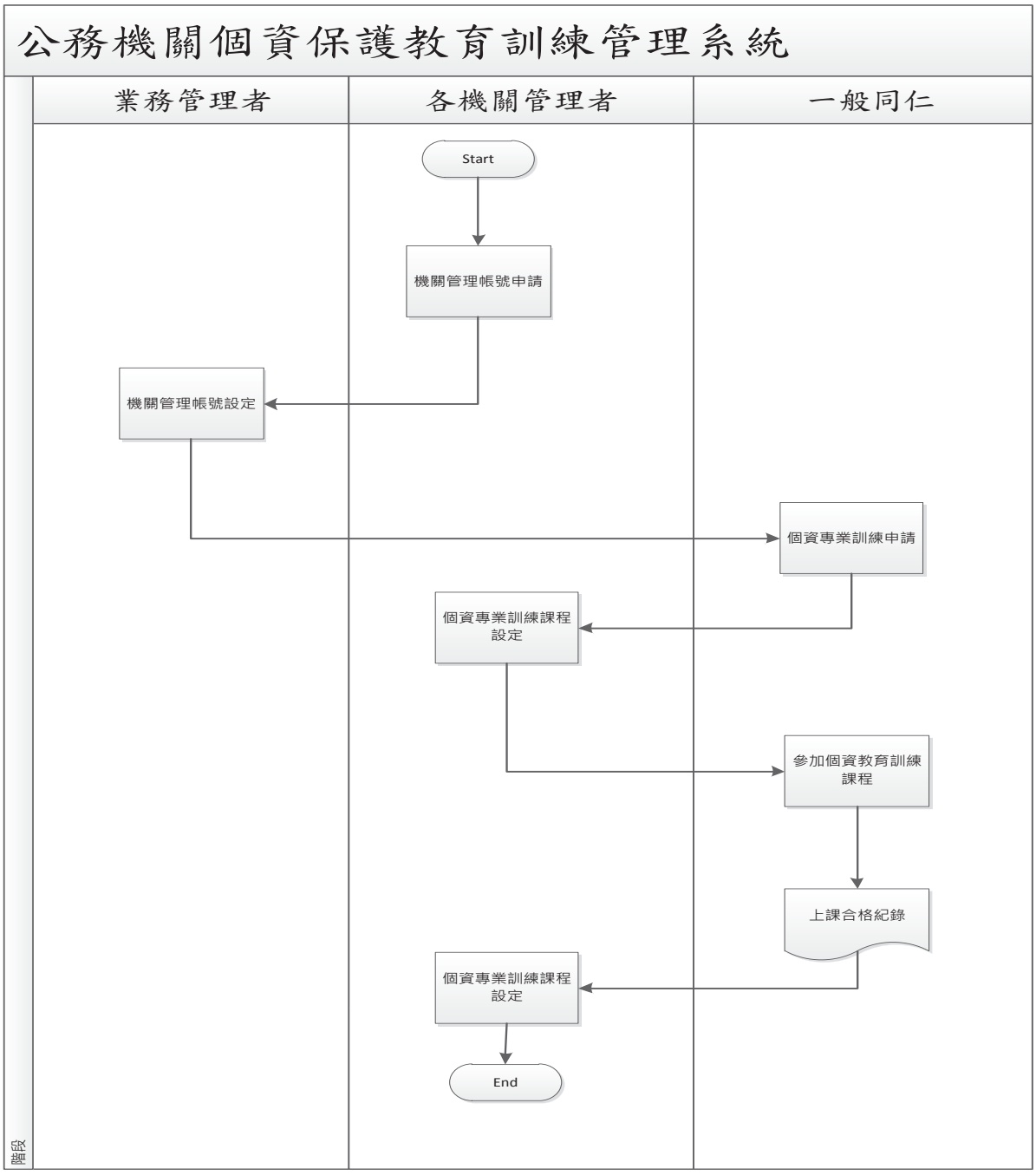
（4）名詞定義

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

（6）流程圖



資料來源:本計畫整理

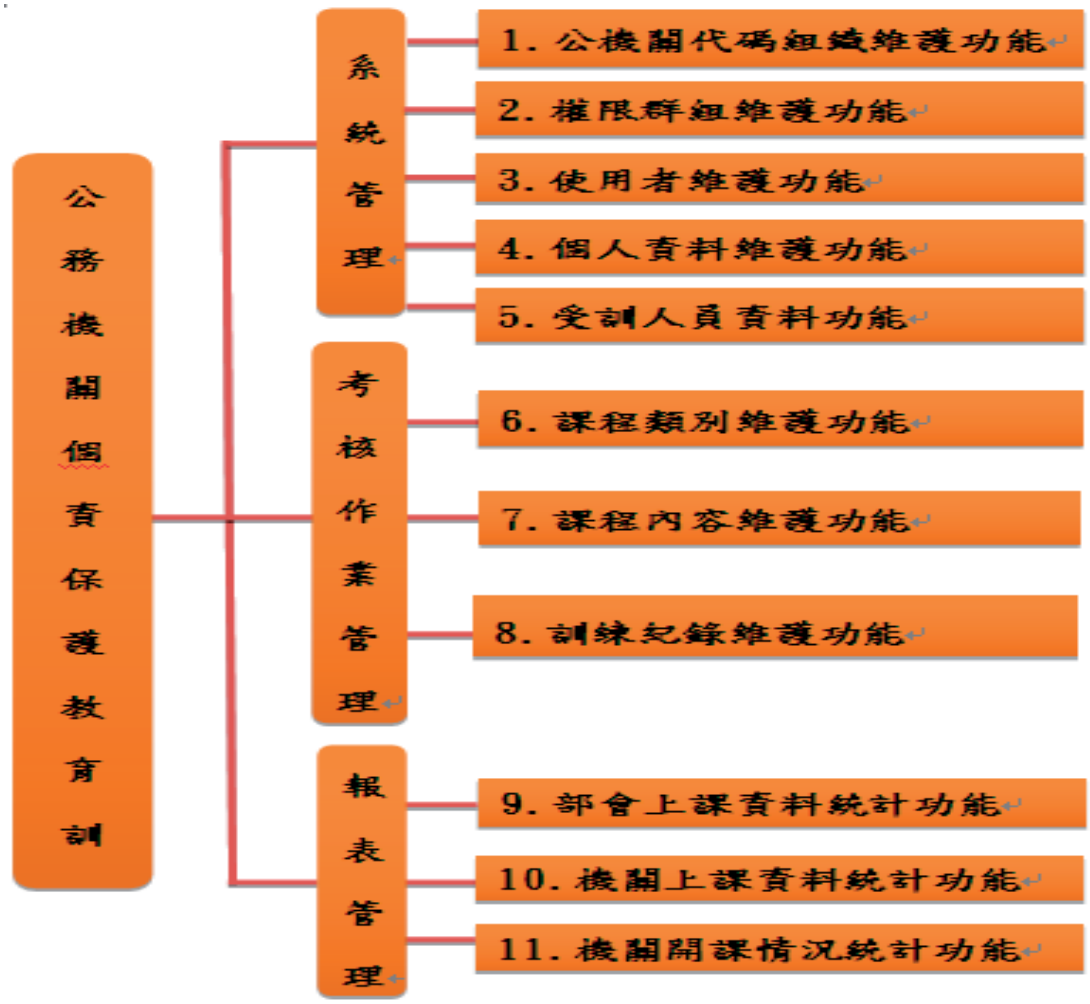
圖 27：公務機關個資保護教育訓練管理系統流程圖

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

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

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：

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) 、

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

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。

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

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

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

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

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

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

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。

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

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。

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。

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。

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。

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。

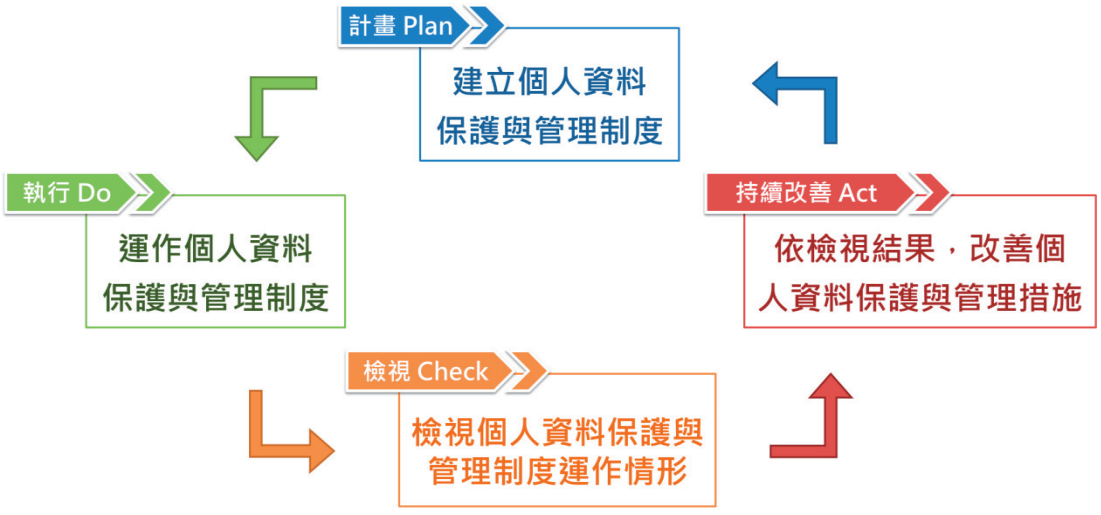
（三）個人資料保護政策與架構

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

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；

（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。

（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。

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

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

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

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

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

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

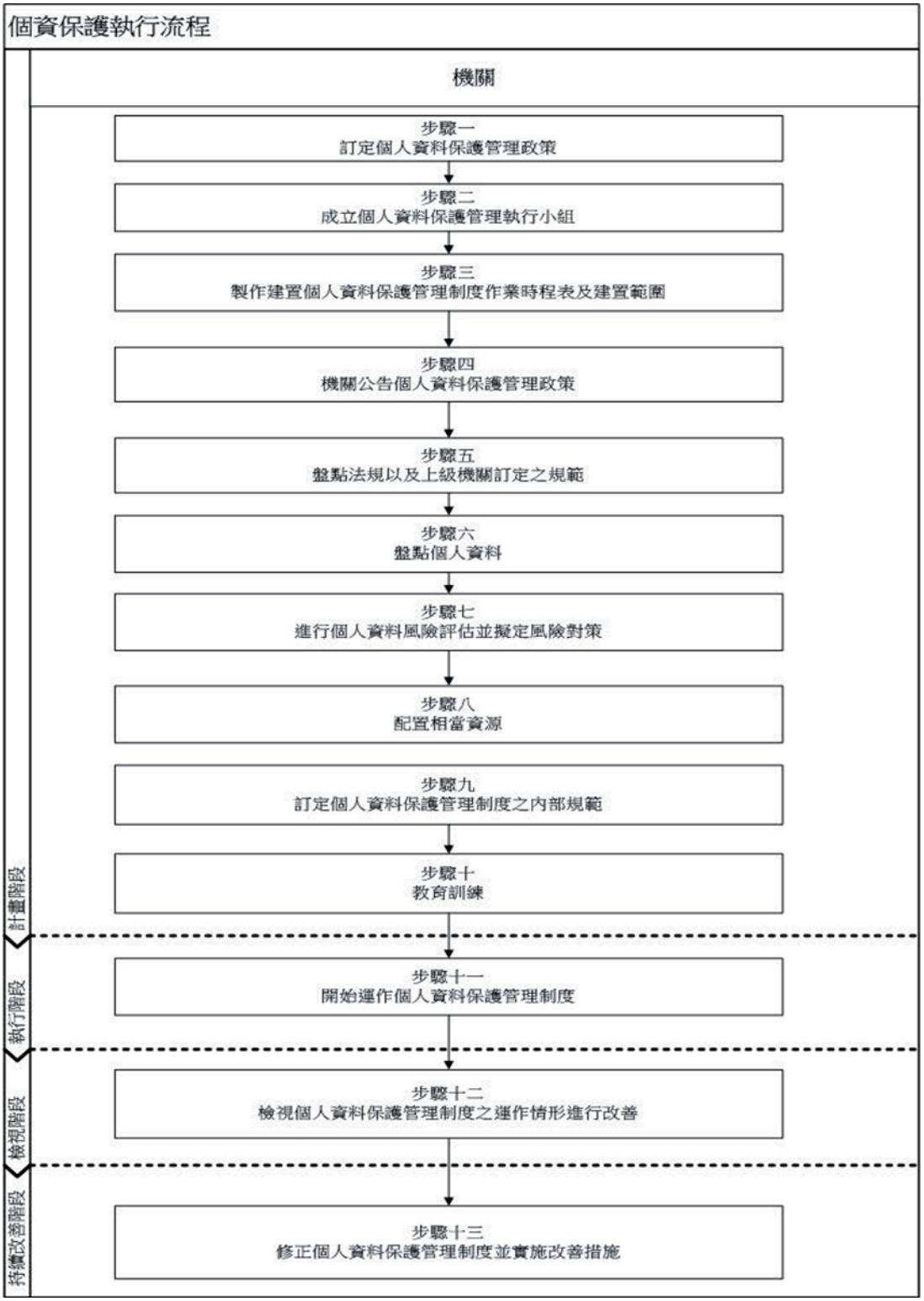
建置個資保護管理流程之目的，在於發展一套個資管理制度使公務機關可因應個資法之要求。首先，個資管理制度須符合我國個

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：



資料來源：本報告自行繪製

圖 30：個資保護管理建置流程圖

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

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/

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

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。

（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

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

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。

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

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

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

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。

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

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）

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

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

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

- 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

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

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

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。

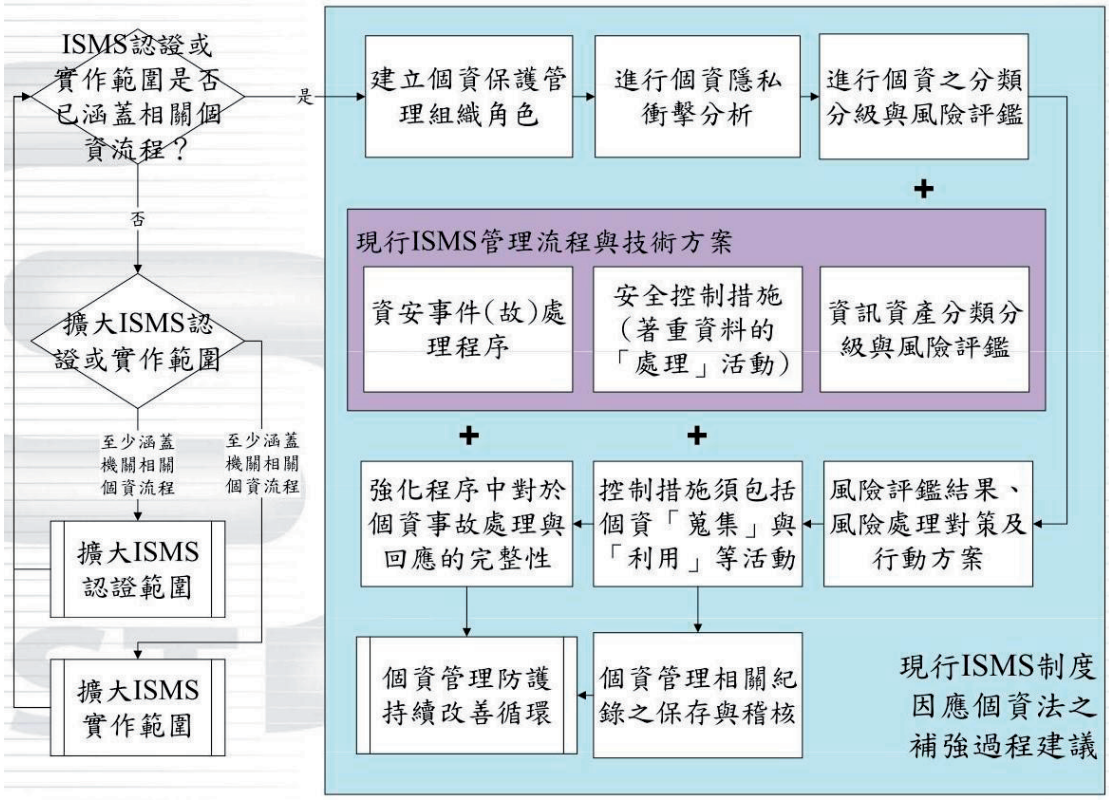
個資法會針對個資蒐集前，進行告知、特定目的及書面同意進行規範，而 ISMS 就不會涵蓋這些重點。但是 ISMS 所強調的安全防護控制措施，剛好可以提供有關個資在處理及利用階段所需之資訊安全防護。

因此，已實施或已通過 ISO/IEC 27001 驗證的機關而言，依照

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。

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

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。

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：

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。

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

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。

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。

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。

（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。

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。

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。

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。

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、

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。

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

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。

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。

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。

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

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

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。

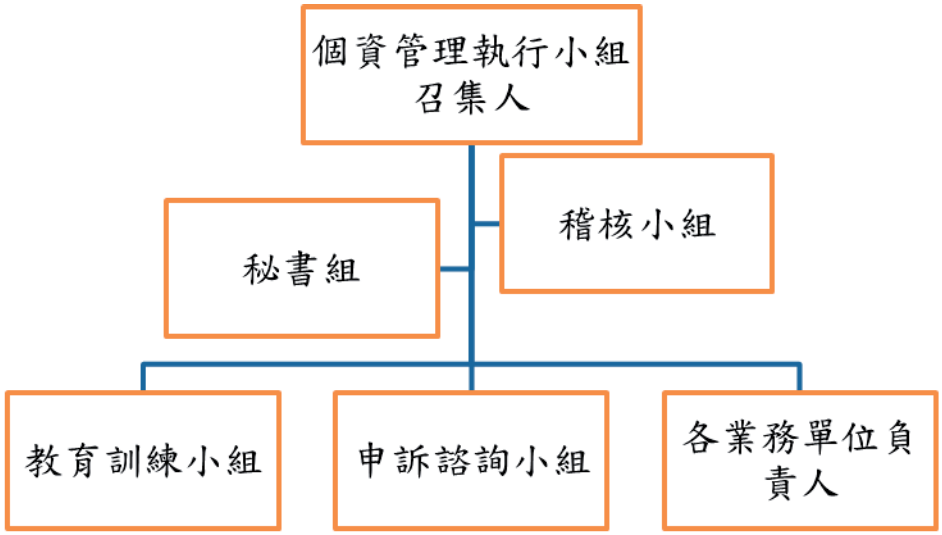
二、機關代表人之職責

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

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

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。

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					

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					

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。

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

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。

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。

（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。

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。

（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

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。

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

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。

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

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

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。

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、

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。

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

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。

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

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

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。

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

本規則於每年○月檢視，於必要時修訂之。

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

（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

（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。

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

（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。

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。

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。

（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。

附錄二、參考之程序表單

表單一：文件紀錄一覽表之一

制訂日	核決	
修訂日	製表	
修訂版		

附件　法規盤點清冊一覽表

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

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

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

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														

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為委外廠商。	
	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項為「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項為「不可」時，4～10項為「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　〇〇　）**
	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

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	

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

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。

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

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

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

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				

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

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

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

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

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】

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）					

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？					

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）					

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?					

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？					

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）？					