法務部
公務機關個人資料保護方案計畫
研究成果報告書

公務機關個人資料保護執行程序
暨考核作業手冊

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

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。

一、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。

二、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。

三、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。

貳、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。

一、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。

二、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

（一）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。

（二）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：

1.100 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。

2.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。

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，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。

4.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：

（1）成立管理組織，配置相當資源

（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。

5.100 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。

6.100 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。

7.100 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。

8.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。

三、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：

（一）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。

（二）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：

1.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。

2.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。

3.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。

4.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。

5.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。

（三）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。

四、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：

（一）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。

（二）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。

（三）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。

（四）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。

五、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：

（一）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。

（二）各中央目的事業主管機關訂定

1.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。

2.訂定機關內部之個人資料管理要點

3.應訂定機關進行行政檢查之處理要點

（三）公開下列事項於電腦網站上，提供公眾查閱

1.個人資料檔案名稱。

2.保有機關名稱及聯絡方式。

3.個人資料檔案保有之依據及特定目的。

4.個人資料之類別。

（四）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。

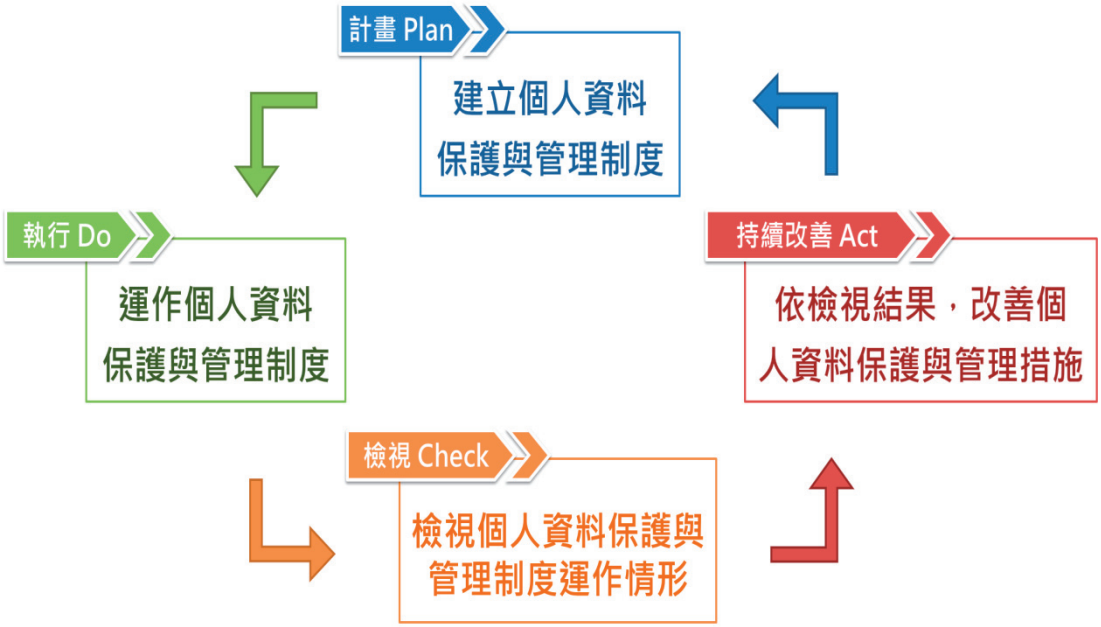
參、個人資料保護政策與架構

一、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。

二、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 1：PDCA流程圖

三、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：

（一）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；

（二）包括遵守個資法相關法令、規章與其它要求之承諾；

（三）管理措施文件化、實施與維持；

（四）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；

（五）因應申訴以及諮詢之相關程序；

（六）定期審查，以確保管理政策的適宜性；

（七）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：

（一）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；

（二）法令與其他規章對個人資料保護管理要求；

（三）機關已往與目前的個人資料保護管理作為；

（四）其他利害相關者要求；

（五）持續改善的機會與需求；

（六）個人資料保護管理所需資源；

（七）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。

四、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：

（一）成立管理機關，配置相當資源資源。

（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。

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：

（一）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：

1.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。

2.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。

（二）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。

1.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。

2.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。

3.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。

4.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。

（三）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：

1.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）。

2.依個資數量，以個資數量若外洩時，對機關影響之大小。

3.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。

（四）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：

1.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。

2.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。

3.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。

4.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。

（五）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：

1.規定盤點相關法令、上級機關所訂之法令規範

2.規定有關盤點個人資料的程序

3.規定有關個人資料風險評估、分析及風險對策的程序

4.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

5.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

6.規定有關蒐集、處理、利用個人資料的程序

7.規定有關安全、適當管理個人資料的措施及程序

8.規定有關對應當事人權利行使的程序

9.有關機關內部人員教育訓練的規定

10.規定有關個人資料保護制度文件紀錄管理程序

11.規定有關訂對應處理個人資料申訴及諮詢時的程序

12.有關機關內部檢查、稽核的規定

13.規定有關管理制度矯正預防措施之程序

14.規定有關機關代表人持續改善制度之程序

15.規定有關違反內部規定的罰則

16.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。

（六）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。

（七）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。

（八）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。

（九）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。

（十）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。

（十一）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。

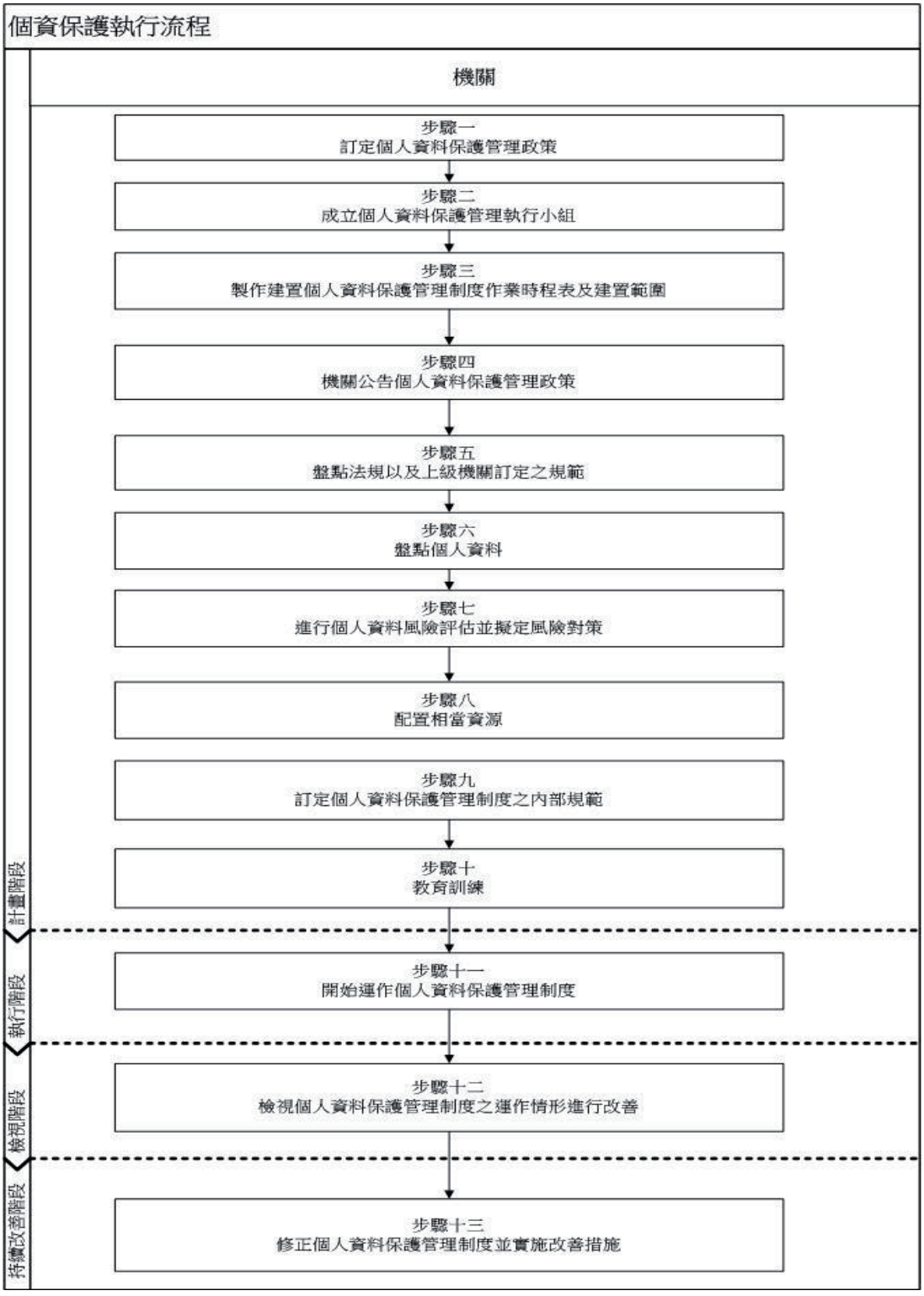
肆、個資保護管理建置流程

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圖：



資料來源：本報告自行繪製

圖 2：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 1：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規範	3.1.2 外部環境分析 －瞭解個資管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 3.1.4 作業流程分析 －定義和個資	界定個人資料範圍
計畫階段（Plan）	步驟六 盤點個人資料		界定個人資料之範圍

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
		相關之流程與應用系統範圍 3.1.6 個資項目盤點	
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 訂定個人資料保護管理制度之內部規範	3.1.9 安全控制措施規劃 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	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
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	3.3.2 個資管理稽核活動	檢視前述程序運作情形

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
	制度之運作情形進行改善		
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

一、計劃

（一）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：

1.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。

2.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：

（1）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。

（2）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。

（3）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

（4）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。

（二）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。

（三）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。

（四）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。

（五）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。

（六）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。

（七）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。

（八）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。

（九）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：

1.規定盤點相關法令、上級機關所訂之法令規範

2.規定有關盤點個人資料的程序

3.規定有關個人資料風險評估、分析及風險對策的程序

4.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

5.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

6.規定有關蒐集、處理、利用個人資料的程序

7.規定有關安全、適當管理個人資料的措施及程序

8.規定有關對應當事人權利行使的程序

9.有關機關內部人員教育訓練的規定

10.規定有關個人資料保護制度文件紀錄管理程序

11.規定有關訂對應處理個人資料申訴及諮詢時的程序

12.有關機關內部檢查、稽核的規定

13.規定有關管理制度矯正預防措施之程序

14.規定有關機關代表人持續改善制度之程序

15.規定有關違反內部規定的罰則

16.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：

1.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。

2.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。

3.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。

4.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。

5.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。

6.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。

7.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：

（1）規定進出辦公室的管理、防止個人資料失竊等的措施

（2）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

（3）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

（4）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。

8.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。

9.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：

（1）目的

（2）時期、期間、對象（包含全體人員）

（3）內容、方法、場所

（4）機關（負責主管）

（5）通知程序

（6）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）

（7）確認教育訓練效果的方法

（8）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。

10.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。

11.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；

12.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。

13.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：

（1）確認不符合事項的內容

（2）清查不符合事項的原因，建立矯正處置及預防措施

（3）定出期限實施所建置的處置與措施

（4）紀錄所實施的矯正處置及預防措施的結果

（5）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。

14.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：

（1）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

（2）包含申訴等外部意見

（3）對前次矯正預防及修正結果的後續追蹤

（4）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

（5）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

（6）機關行政事項領域的變化

（7）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。

15.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。

16.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

（十）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。

二、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。

三、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。

四、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。

伍、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。

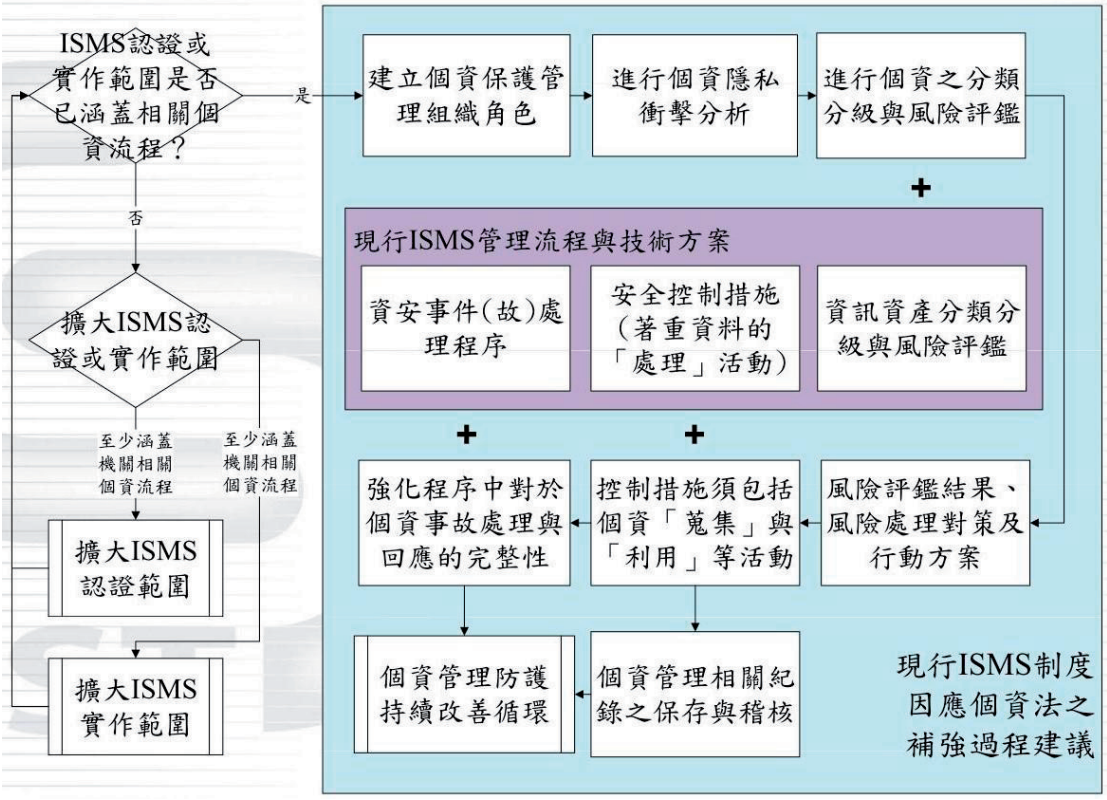
個資法會針對個資蒐集前，進行告知、特定目的及書面同意進行規範，而 ISMS 就不會涵蓋這些重點。但是 ISMS 所強調的安全防護控制措施，

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 3：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。

一、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。

二、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。

三、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。

四、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。

五、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。

六、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。

（一）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：

1.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？

2.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。

3.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。

（二）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：

1.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。

2.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。

3.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。

4.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。

5.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。

6.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。

（三）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：

1.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。

2.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。

3.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。

4.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。

5.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。

（四）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：

1.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。

2.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。

3.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。

陸、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。

一、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。

（一）查核之範圍、目的與適用對象

1.範圍：

（1）個人資料保護作業遵循相關法規的符合性之審查。

（2）個人資料保護作業達成目標的程度之審查。

（3）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。

2.目的：

（1）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。

（2）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。

（3）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。

（4）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。

3.適用對象：

本單位暨所屬機關個人資料處理及使用單位。

（二）查核之責任

1.查核應對受稽單位業務之使用者負責。

2.查核應以內部稽核為基礎，進行風險評鑑。

3.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。

（三）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：

1.主任查核員的責任

（1）查核之文書審查、工作分配。

（2）規劃與管理所有查核階段。

（3）彙整文書審查結果。

（4）控制和處理困難問題。

（5）主持查核單位與受查核單位間的會議。

（6）稽核議題之裁決。

（7）即時反映重大問題。

（8）提報查核結果。

2.查核員的責任

（1）完成分派的查核工作。

（2）配合主任查核支援其他查核工作。

（3）紀錄和報告所有的查核發現。

（4）即時向受查核單位提出相關查核情況。

（5）妥善保存所有查核相關文件及遵守保密規定。

（6）查核過程須維持獨立客觀及專業水準。

（7）追蹤矯正預防及改善措施的有效執行。

（四）查核之規劃

1.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。

2.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：

（1）取得授權：機關最高管理階層應授權規劃外部查核。

（2）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。

（3）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。

（4）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。

3.查核工作計畫應依下列原則擬訂：

（1）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。

（2）決定查核目標、查核時間和所需資源。

（3）選擇查核成員及協調查核時程。

（4）研擬查核工作計畫及準備檢核表等相關資料。

（5）外部查核工作計畫應涵蓋業務之主要控制項目。

4.查核檢核表之功能：

（1）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。

（2）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。

（3）查核檢核表可以界定查核的範圍。

（4）查核檢核表可以協助瞭解查核的運作和流程。

（5）查核檢核表可以作為查核及受稽單位間之備忘錄。

（五）查核程序

查核階段區分如下：

1.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：

（1）業務管理及風險控管架構

（2）業務活動範圍

（3）達成業務目標之策略與執行計畫

（4）執行業務時發生事件的處理文件

（5）業務執行成果相關文件

2.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：

（1）訪談受稽業務相關的管理者與使用者。

（2）瞭解受稽業務內部控制與內部查核之管理規章。

（3）審閱受稽業務辦理內部控制與內部查核之書面報告。

（4）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。

（六）查核執行程序

1.機關查核小組

（1）指派主任查核員。

（2）界定查核目標、範圍及準則。

（3）評估查核之可行性。

（4）準備查核工作計畫及工作文件。

（5）挑選查核小組成員，並指派工作。

（6）與受查核單位人員建立初步聯繫。

2.文件審查及執行現場查核活動

（1）舉行啟始會議。

（2）查核中與受查人員之溝通。

（3）引導查核人員與受稽人員。

（4）蒐集與查核相關資訊。

（5）記錄查核發現。

（6）研提查核建議與結論。

（7）舉行結束會議。

3.研擬查核報告

（1）研擬查核報告。

（2）簽報核准後分發查核報告予受查核單位。

4.執行查核後列管追蹤

（七）查核之執行

1.首次會議

（1）介紹查核背景及預期達成的目標。

（2）確認查核目的與範圍。

（3）查核工作計畫之確認。

（4）查核小組的任務分配及受稽單位引導人員之分配。

（5）查核方法的溝通。

（6）查核報告大綱說明。

（7）確認查核的抽、複核方法。

（8）查核的保密承諾。

（9）查核的執行限制與問題澄清。

2.參加人員

（1）查核小組

A. 查核小組組長及成員。

B. 見習查核員及主任查核員。

C. 見證人。

（2）受查核單位

A. 部門主管及員工。

B. 見習人員。

（八）實地查核之進行

1.進入查核區域。

2.受查核單位介紹受查核業務。

3.查核小組說明查核需求。

4.進行必要查核調查。

5.依據查核查核表循序執行查核。

（九）查核之溝通技巧

1.營造融洽氣氛，問題詢問力求簡要。

2.當問題不瞭解時，應讓受稽單位明確知道。

3.表現正面態度，並給受稽單位適當正面的肯定。

4.顯示耐心與理解力，避免打斷受稽單位之發言。

5.詢問應使受稽單位感到自在。

6.問題應針對與受稽單位之業務相關。

（十）查核之提問要領

1.盡量採開放式諮詢；非僅”是”或”不是”。

2.引導受稽單位瞭解提問，以迅速獲得所需答案。

3.查核時可考量以調查結果、長官意見、假設狀況等方式提問。

4.完成提問時，應總結問題的發現及表達感謝配合。

（十一）查核紀錄要項

1.記錄客觀的證據；可接受的陳述。

2.針對查核時所有適當的資訊做紀錄，包括：

（1）對受查核稽單位人員訪談之發現摘要。

（2）引用看見的文件、紀錄或法規。

3.記錄不符合規定事項：

（1）清楚記錄不符合事項及其發現依據。

（2）清楚記錄發現的事實；不要誇大發現。

（3）清楚說明不符合的理由。

（4）清楚記錄發現不符合事項時的在場人員。

（5）記錄不符合事項發生的可能性說明。

（6）記錄不符合事項持續錯誤可能產生的後果。

（十二）查核的事實確認程序

1.取得受稽單位的協助。

2.針對查核所關心的問題進行討論。

3.共同驗證所發現的結果。

4.記錄所有的證據。

5.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。

（十三）查核應注意事項

1.查核報告應具建設性、專業性，並對受稽業務有所助益。

2.查核過程須定期檢討進度與發現。

3.排除負面資訊，並與受查核單位建立良好互動。

4.對於證據不足的資訊，必須做出對受查核單位有利的判斷。

5.重視與疏通被查核方的反應。

（十四）查核小組會議

1.依據查核工作計畫表中的排程舉行。

2.僅限查核小組成員出席。

3.由主任查核員主持。

4.檢討查核工作的有效性。

5.提報查核事項書面報告。

6.評審各項查核書面報告。

7.規劃外部查核之結束會議。

8.主任查核員準備總結報告。

（十五）查核總結內容

1.業務管理的內部控制系統是否有效。

2.內部控制系統有無任何缺失。

3.有無對特定事項須特別注意的說明。

4.管理階層是否承諾對有缺失的內部控制持續改善。

（十六）查核結束會議

1.主任查核員須準備和控制會議議程。

2.決定會議出席者。

3.報告查核目標與範圍。

4.報告受稽業務。

5.報告查核過程的工作限制。

6.報告查核所獲機密性資料的保密處理。

7.查核總結報告。

8.查核相關之協議、建議及問題之澄清說明。

（十七）查核報告

查核報告重點：

1.查核發現的摘要。

2.查核的範圍。

3.內部控制符合相關法規及管理要求之說明。

4.內部控制不符合事項之說明。

5.相關的觀察及受查核單位、業務等之記載。

6.清楚記錄不符內部控制事項，讓受查核單位明確瞭解。

7.清楚說明查核報告事項的事實根據。

（十八）查核報告之確認與管考

1.查核報告須經外部查核結束會議相關出席人員確認。

2.查核報告應函送受稽單位。

3.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。

4.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。

5.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。

6.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。

（十九）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。

二、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：

（一）是否於合約中載明應遵循機關之個人資料保護管理原則？

（二）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。

（三）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。

（四）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？

（五）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?

（六）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。

（七）是否確認受託人採取必要之個人資料檔案安全維護措施。

（八）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。

（九）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。

（十）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。

（十一）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。

（十二）受託人之事故通報程序是否建立且留存相關紀錄。

柒、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。

捌、參考文獻目錄

一、行政院研究發展考核委員會，個人資料保護參考指引，101 年。

二、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。

三、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。

四、個人資料保護法，99 年。

五、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。

六、行政院國家資通安全會報，資訊系統風險評鑑，99 年。

七、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。

八、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。

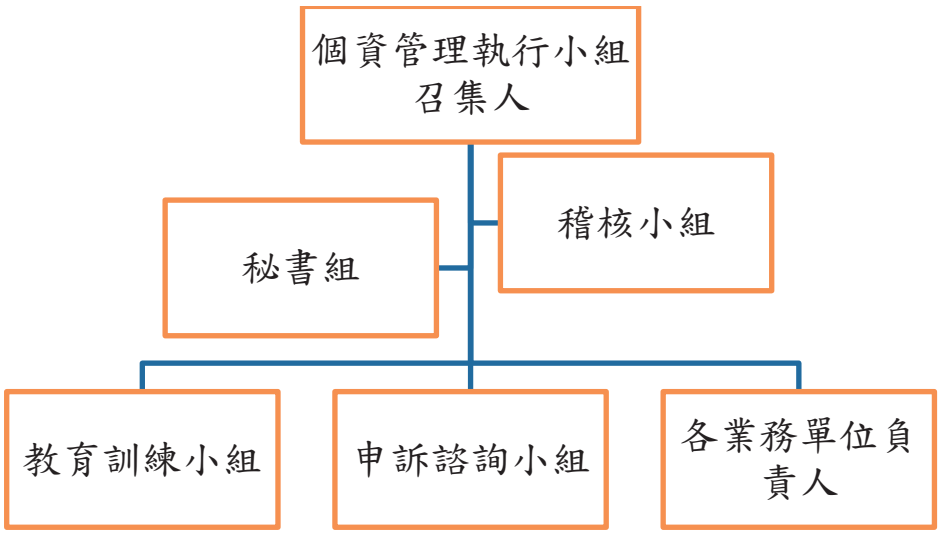
二、機關代表人之職責

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」及相關參考資料、機關外部環境等相關資訊。

（二）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。

（三）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

附件　法規盤點清冊一覽表

制訂日	核決	
修訂日	製表	
修訂版		

No.	領域	文件名稱	頒布機關名稱	最新版年度	保存閱覽場所	最新版本確認人	最新版本確認日期	備註

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？					

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？					

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
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？					
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？					

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					

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
		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?					
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？					
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					

序號	領域	評估細項	符合	部份符合	未符合	不適用	說明
		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）？					