目錄

壹、前言

個人資料保護法（以下簡稱個資法）已於104年12月30日修正公布部分條文，並於105年3月15日施行。個資法所保護之客體涵蓋紙本及經電腦處理之個人資料，機關於蒐集個人資料前，應具有特定目的及符合特定情形，始得為之，並應履行告知義務，告知當事人所欲利用之期間、地區、對象、方式等，且有關個人資料之處理與利用應限於所告知之特定目的範圍內；如有超出特定目的範圍外之利用，應符合法定之要件。此外，個資法設有團體訴訟機制，損害賠償總額上限為新臺幣2億元，涉及刑事責任者，最高可處有期徒刑5年，為此，業務涉及個人資料之機關不可不慎。

經濟部（以下簡稱本部）主管全國經濟行政及經濟建設事務，業務內容繁複且影響人民甚深，因執行業務所保有之個人資料為數可觀。為避免本部及所屬機關執行業務時，因不諳法律之執行內容，而承擔相關法律責任，特編印本部個人資料保護作業手冊，以協助本部及所屬機關遵守相關個資法令。

本手冊依據個資法、個資法施行細則、經濟部個人資料保護管理作業要點等規定研擬，並以個資法施行細則第12條第2項所列11款程序事項為架構，同時導入P-D-C-A（Plan-Do-Check-Act）方法論，以規劃、執行、檢核、持續改善等方式，建立本部之個人資料保護作業程序。內容包括組織的任務分工、個人資料蒐集處理利用之流程、當事人權利行使、個人資料檔案盤點及風險分析、事故預防、通報及應變、認知宣導及教育訓練、個人資料安全管理、使用紀錄、軌跡資料及證據保存、委外監督、資料安全稽核、持續改善措施等。本手冊此次修訂，主要係依據行政院110年8月11日院授發協字第1102001106號函訂定之行政院及所屬各機關落實個人資料保護聯繫作業要點(以下簡稱聯繫作業要點)，為加強對非公務機關個人資料檔案安全維護情形之監管，降低個資外洩風險，保障民眾權益，爰增訂對非公務機關個人資料保護之監管作業程序，修正個人資料安全稽核檢查表參考範例表單，並於附錄增列聯繫作業要點、公布非公務機關

及其負責人違反個人資料保護法情形之處分參考原則等規定，俾本部及所屬機關同仁參考利用以落實執行。

本部各單位及所屬機關應就其業務需求與屬性、作業模式及其他因素，參考本手冊之規定，據以針對所保有之個人資料，進行個人資料檔案安全維護之規劃與建置，落實相關之作業流程與要求，並定期檢視各項程序之執行情形，同時加強個人資料安全稽核作業以及追蹤改善措施，以符合個資法之相關規定。

貳、人員及資源配置

一、依據

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 1 款規定辦理，以推動本部及所屬機關之個人資料保護政策。

二、本部人員編制與職掌

（一）經濟部個人資料保護推動執行小組(以下簡稱本部個資小組)屬常態任務編組，置召集人一人，由本部次長兼任，負責推動、協調及督導本部個人資料保護管理業務；執行秘書一人，由本部法規會執行秘書擔任，承召集人之命，負責綜理本小組有關業務；本小組委員由本部所屬機關（構）個資保護召集人及本部幕僚單位個資保護專責人員兼任之。

（二）本部個資小組職掌如下：

1.本部個人資料保護管理制度及配套措施之擬議。
2.個人資料保護相關法規專業訓練及宣導作業之擬議。
3.持續檢視個人資料管理制度是否符合法律、司法實務及科學技術之變更。
4.個資外洩事件通報暨危機處理。
5.個人資料保護管理作業相關稽核作業之督導。
6.其他個人資料保護執行事項。

三、本部各單位及所屬機關人員配置

（一）本部一級單位及所屬機關辦理下列事項，應設置個人資料保護聯絡窗口：

1.公務機關間個人資料保護業務之協調聯繫及緊急應變通報。
2.非資通安全面個人資料安全事件之通報。
3.重大個人資料外洩事件之民眾聯繫單一窗口。
4.本部一級單位及所屬機關個人資料專人名冊之製作及更新。
5.本部一級單位及所屬機關個人資料專人與職員工教育訓練名單及紀錄之彙整。

6.個資法令之諮詢。

（二）本部及所屬機關之一級單位辦理下列事項，應指定專人處理：

1.執行當事人依個資法第 10 條及第 11 條第 1 項至第 4 項所定請求之督導。
2.執行個資法第 11 條第 5 項及第 12 條所定通知之督導。
3.個資法第 17 條所定公開或供公眾查閱。
4.個資法第18條及個資法施行細則第12條所定個人資料檔案安全維護。
5.職員工之個人資料保護意識提升及教育訓練計畫之執行。
6.個人資料保護事項之協調聯繫。
7.單位內個人資料損害預防及危機處理應變之通報。
8.本部及所屬機關個人資料保護方針及政策之執行、單位內個人資料保護之自行查核。
9.其他有關單位內個人資料保護管理之規劃及執行。

（三）本部各單位及所屬機關得視組織人員及業務狀況，配置相當資源或成立工作小組(如事故應變小組、內部稽核小組等)辦理前款各目事項。

四、本部及所屬機關應依其任務指派情形，建立個資保護召集人、聯絡窗口、專責人員及工作小組成員名冊並保持最新狀態。

參、個人資料蒐集、處理或利用作業程序

一、依據

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 5 款規定辦理，以有效規範個人資料之蒐集、處理、利用等行為。

二、個人資料之蒐集、處理或利用基本原則

個人資料之蒐集、處理或利用，應以誠實信用方式為之，不逾越特定目的之必要範圍、並與蒐集之特定目的有正當合理關聯（個資法第 5 條）。

三、個人資料蒐集程序

（一）本部各單位及所屬機關蒐集個人資料時，應有特定目的並符合特定情形（個資法第 15 條）。

（二）本部各單位及所屬機關蒐集個人資料之特定目的，以個資法之特定目的及個人資料之類別規定者為限。

（三）新增之業務如有涉及個人資料之蒐集，本部各單位及所屬機關應簽奉核定後為之（參考範例一、二、三）。

（四）前述業務如必須蒐集一人以上之個人資料或為執行業務而有必要持續蒐集個人資料時，得以一次性簽奉核定為之。

（五）本部各單位及所屬機關向當事人(即個人資料本人)蒐集個人資料時，應明確告知當事人下列事項(個資法第 8 條第 1 項)：

1.機關或單位名稱。
2.蒐集之目的。
3.個人資料之類別。
4.個人資料利用之期間、地區、對象及方式。
5.當事人依個資法第 3 條規定得行使之權利及方式。
6.當事人得自由選擇提供個人資料時，不提供對其權益之影響。

但有下列情形之一者，得免為告知（個資法第 8 條第 2 項）：

1.依法律規定得免告知。

2.個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

3.告知將妨害公務機關執行法定職務。

4.告知將妨害公共利益。

5.當事人明知應告知之內容。

6.個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

（六）本部各單位及所屬機關蒐集非由當事人提供之個人資料時，應於處理或利用前(或於首次對當事人為利用時併同為之)，向當事人告知下列事項(個資法第 9 條第 1 項及第 3 項)：

1.個人資料來源。

2.機關或單位名稱。

3.蒐集之目的。

4.個人資料之類別。

5.個人資料利用之期間、地區、對象及方式。

6.當事人依個資法第 3 條規定得行使之權利及方式。

但有下列情形之一者，得免為告知（個資法第 9 條第 2 項）：

1.有個資法第 8 條第 2 項所列各款情形之一。

2.當事人自行公開或其他已合法公開之個人資料。

3.不能向當事人或其法定代理人為告知。

4.基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

（七）本部各單位及所屬機關以個資法第 15 條第 2 款「經當事人同意」之方式蒐集個人資料時，得備妥個人資料蒐集、處理、利用同意書（參考範例三），以取得當事人同意。

四、個人資料處理程序

（一）本部各單位及所屬機關處理個人資料時，應有特定目的並符合特定情形（個資法第 15 條）。

（二）本部各單位及所屬機關處理個人資料之特定目的，以個資法

之特定目的及個人資料之類別規定者為限。

（三）個人資料之正確性

1.為維護個人資料之正確性，本部各單位及所屬機關於記錄、輸入、編輯、更正個人資料時，應檢查確認。
2.本部各單位及所屬機關保有之個人資料有誤或缺漏時，應由資料蒐集單位簽奉核定後（參考範例四），移由資料保有單位補充或更正之，並留存相關紀錄(個資法第 11 條第 1 項)。
3.因可歸責於本部各單位及所屬機關之事由，未為補充或更正之個人資料，應於補充、更正後，由資料蒐集單位以通知書通知曾提供利用之對象（個資法第 11 條第 5 項)。

（四）個人資料之刪除(銷毀)

1.本部各單位及所屬機關應定期檢視個人資料之有效性及可用性，刪除或銷毀不必要之個人資料。
2.本部各單位及所屬機關保有個人資料蒐集之特定目的消失、期限屆滿或違法蒐集時，本部各單位及所屬機關應主動或依當事人之請求刪除或銷毀該個人資料。但特定目的消失或期限屆滿時，因執行職務所必須或經當事人書面同意者，不在此限（個資法第 11 條第 3 項、第 4 項)。
3.本部各單位及所屬機關依前目規定刪除或銷毀個人資料時，應由資料蒐集單位簽奉核定後（參考範例五)，移由資料保有單位刪除或銷毀。
4.本部各單位及所屬機關於刪除或銷毀個人資料時，應以適當方式記錄並確認其執行結果。

五、個人資料利用程序

（一）本部各單位及所屬機關利用個人資料時，應於法定職務之必要範圍內並與蒐集之特定目的相符（個資法第 16 條)。

（二）本部各單位及所屬機關不得非法利用個人資料，並不得為資料庫之恣意連結，且不得濫用。

（三）本部各單位及所屬機關以個資法第 15 條第 2 款「經當事人同意」方式蒐集個人資料時，對於個人資料之利用應符合該同意書所載之內容，包括個人資料利用之期間、地區、對象、

方式及其他相關事項。

（四）目的外利用

1.本部各單位及所屬機關對於個人資料之利用，如有特定目的外利用之情況，應符合下列情形之一：

(1) 法律明文規定。

(2) 為維護國家安全或增進公共利益所必要。

(3) 為免除當事人之生命、身體、自由或財產上之危險。

(4) 為防止他人權益之重大危害。

(5) 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

(6) 有利於當事人權益。

(7) 經當事人同意。

2.本部各單位及所屬機關就保有之個人資料有特定目的外利用之需求時，個人資料之利用單位應詳為審核並簽奉核定後為之（參考範例六、七、八）。

3.本部及所屬機關依個資法第 16 條但書規定對個人資料為特定目的外之利用，應將個人資料之利用歷程做成紀錄。

六、個人資料之停止蒐集、處理、利用

（一）個人資料之蒐集、處理或利用有違法之情事時，本部各單位及所屬機關應主動或依當事人請求停止蒐集、處理或利用該個人資料（個資法第 11 條第 4 項）。

（二）本部各單位及所屬機關保有個人資料之正確性有爭議、蒐集之特定目的消失、期限屆滿，本部各單位及所屬機關應主動或依當事人之請求停止處理或利用該個人資料。但因執行職務所必須或經當事人書面同意，於個人資料正確性有爭議時並經註明其爭議者，不在此限（個資法第 11 條第 2 項、第 3 項）。

（三）本部各單位及所屬機關依前二款規定，擬停止蒐集、處理、利用個人資料時，應由資料蒐集單位簽奉核定後（參考範例九），移由資料保有單位停止處理或利用該個人資料。

（四）個人資料已停止處理或利用者，本部各單位及所屬機關應確實記錄。

七、施行前所保有個人資料檔案之利用

（一）民國 101 年 9 月 30 日前（含）已蒐集或處理由當事人提供之個人資料，本部各單位及所屬機關得繼續為處理及特定目的內之利用（個資法施行細則第 32 條）。

（二）本部各單位及所屬機關對前款個人資料為補充、更正、刪除、銷毀、或特定目的外之利用者，應依個資法及其相關法令，參酌本手冊相關程序辦理。

肆、受理當事人權利行使之作業程序

一、依據

依據個資法第 3 條、第 10 條、第 11 條、第 13 條及第 14 條之規定辦理，建立本部及所屬機關於受理當事人權利行使時，所應有之作業流程。

二、作業程序

（一）申請方式

1.申請人依個資法第 10 條或第 11 條第 1 項至第 4 項規定向本部各單位及所屬機關請求查詢、閱覽或請求製給複製本、請求更正、補充、刪除、停止蒐集、處理或利用其個人資料時，應填具當事人權利行使申請書（參考範例十），並檢附相關證明文件。文件內容，如有遺漏或欠缺，承辦人應通知申請人限期補正。

2.申請事項如涉及個人資料之補充或更正，應請當事人載明記載錯誤或不完整事項、更正或補充之理由，並提出相關證明文件

3.前目申請，得以親自持送或郵寄方式為之。

（二）確認申請人

1.當事人權利行使應由當事人本人提出申請。

2.承辦人應確認申請人身分，並得於申請人填妥基本資料後，請求出示相關證明文件。

3.如本人無法親自提出申請，得委由代理人為之。委由代理人申請時，應出具委託書(參考範例十一)及雙方之證明文件。

（三）審核程序

1.承辦人確認申請人身分後，應進行請求內容之審核，並於審核期間內，經簽奉核定後以書面通知申請人准駁之決定及後續處理情形。

2.承辦人對於當事人請求答覆查詢、提供閱覽或製給複製本

者,應注意有無下列不予核准之事由(個資法第 10 條但書):

(1) 妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

(2) 妨害公務機關執行法定職務。

(3) 妨害蒐集機關或第三人之重大利益。

3.承辦人對於當事人請求刪除、停止(違法)蒐集、處理或利用其個人資料時,除應注意蒐集之特定目的是否消失或期限是否屆滿,並應注意有無執行職務所必須之否准事由(個資法第 11 條第 2 項至第 4 項)。

(四)審核期間

1.依個資法第 10 條規定提出之請求,應於 15 日內為准駁之決定。必要時,得予延長,延長期間不得逾 15 日,並應將其原因以書面通知申請人(個資法第 13 條第 1 項)。

2.依個資法第 11 條第 1 項至第 4 項規定提出之請求,應於 30 日內為准駁之決定。必要時,得予延長,延長期間不得逾 30 日,並應將其原因以書面通知申請人(個資法第 13 條第 2 項)。

(五)駁回申請之情形

申請案件有下列情形之一者,應以書面駁回其申請:

1.申請書內容或相關文件有遺漏或欠缺,經通知限期補正,逾期仍未補正。

2.有個資法第 10 條但書各款情形之一。

3.有個資法第 11 條第 2 項但書或第 3 項但書所定情形之一。

4.與其他法令規定不符。

(六)費用收取

當事人請求查詢、閱覽或製給個人資料複製本者,準用本部訂定之相關收費標準收取費用(個資法第 14 條)。

(七)其他

當事人請求查詢、閱覽或製給個人資料複製本者,應由承辦單位派員陪同為之,並依檔案法、政府資訊公開法、經濟部

政府資訊及卷宗閱覽須知或本部所屬機關訂定之相關規定辦理。

伍、個人資料盤點及風險評估作業程序

一、依據

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 2 款及第 3 款規定辦理，以界定本部及所屬機關所保有之個人資料檔案，確實掌握期間內所保有之個人資料，並據以進行風險評估及管理，達成個人資料保護與管理之目標。

二、作業程序

（一）個人資料盤點作業

為界定個人資料範圍，本部各單位及所屬機關應規劃個人資料盤點作業。盤點作業應包括下列項目：

1.檢視個人資料檔案

(1) 清查各作業流程中所使用之表單、紀錄，並辨識個人資料有關之表單、紀錄，歸納整理成個人資料檔案。
(2) 使用個人資料盤點表檢視其保有之個人資料檔案，確認個人資料檔案名稱、保有之依據及特定目的、個人資料種類。
(3) 使用個人資料盤點表檢視其保有之個人資料檔案之生命週期，包含蒐集、處理、利用之內容。

2.建立個人資料檔案清冊

將個人資料檔案檢視之成果製作個人資料檔案清冊(參考範例十二個資盤點表)，並妥善保管且定期維護該清冊。

3.公開個人資料檔案資訊

本部各單位及所屬機關應將下列事項公開於網站，或以其他方式供公眾查詢（個資法第 17 條)。

(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。

（二）個人資料風險評估作業

為評估個人資料檔案之風險，本部各單位及所屬機關應規劃個人資料風險評估與管理作業，風險評估作業應包括下列項目：

1.評估個人資料風險

(1) 本部各單位及所屬機關應使用個人資料風險評估表就個人資料檔案內容進行價值識別。個人資料之價值識別得以個人資料之內容、個人資料之數量、個人資料檔案之識別程度，以及其他必要之項目為評估基準。
(2) 於個人資料檔案內容價值識別後，應進行個人資料作業之具體風險類型識別（參考範例十三風險情境表）。
(3) 就識別出之風險，風險發生之衝擊程度及發生之可能性進行風險評估並區分等級。風險發生之衝擊程度得以損害高低以及其他必要之項目為評估基準(參考範例十四個資流程衝擊分析表)。
(4) 就風險發生之衝擊程度及發生之可能性進行識別後，應予以區分風險等級，並就高風險之個人資料檔案作業進行風險處理。

2.處理個人資料風險

依風險評估結果進行風險處理，擬定具體對策。

3.建立風險評估清冊

本部各單位及所屬機關應將風險評估之結果製作個人資料風險評估清冊（參考範例十五個資流程作業風險評估表），並妥善保管且定期維護該清冊。

陸、事故之預防、通報及應變作業程序

一、依據

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 4 款規定辦理，以使本部及所屬機關保有之個人資料，於發生被竊取、竄改、毀損、滅失、洩漏等個資事故時，進行緊急事故應變處理。

二、作業程序

（一）應變計畫

1.本部各單位及所屬機關應將個人資料外洩等事故之處理訂定包括危機任務編組、應變策略、公關溝通及善後處理標準作業程序之危機緊急應變計畫。

2.本部各單位及所屬機關應透過實際演練驗證其有效性，並與風險管理架構相結合，對於處理後之殘餘風險仍高於可容忍程度之事項，應預先規劃危機之預防、應變及復原各階段因應措施。

（二）事故通報

1.本部各單位及所屬機關獲報並經初步確認屬個資外洩之危機事件後，應立即以電話、傳真或任何可資運用之溝通工具，將訊息傳達至經濟部個人資料保護推動執行小組(以下簡稱本部個資小組)並填寫個人資料事故通報單(參考範例十六)，後續再由本部個資小組通報至本部部次長、主任秘書辦公室、研究發展委員會及相關單位。

2.如個資外洩事件涉及資通安全面，本部及所屬機關應另依其資通安全事件通報及應變機制至行政院國家資通安全通報應變網站（以下簡稱通報應變網站）進行通報。

（三）事故應變

1.本部個資小組於接獲通報後，除責成相關單位及機關辦理外，應由該單位及機關視危機態勢，簽奉核定成立危機應變

小組。

2.本部各單位或所屬機關應辦理下列事項：

(1) 應於接獲通報後 24 小時內進行事故分析。事故分析應包含確認事故之種類、事故嚴重程度、影響的範圍以及發生原因。

(2) 於事故分析後，應研擬事故應變處理措施避免事故擴大，並採取證據保全措施，避免異動或改變原始磁碟及證據。

(3) 於事故查明後，應即適當方式通知當事人被侵害之事實以及已採取之措施(參考範例十七)。適當方式得依個資法施行細則第 22 條規定為之。

（四）媒體應對

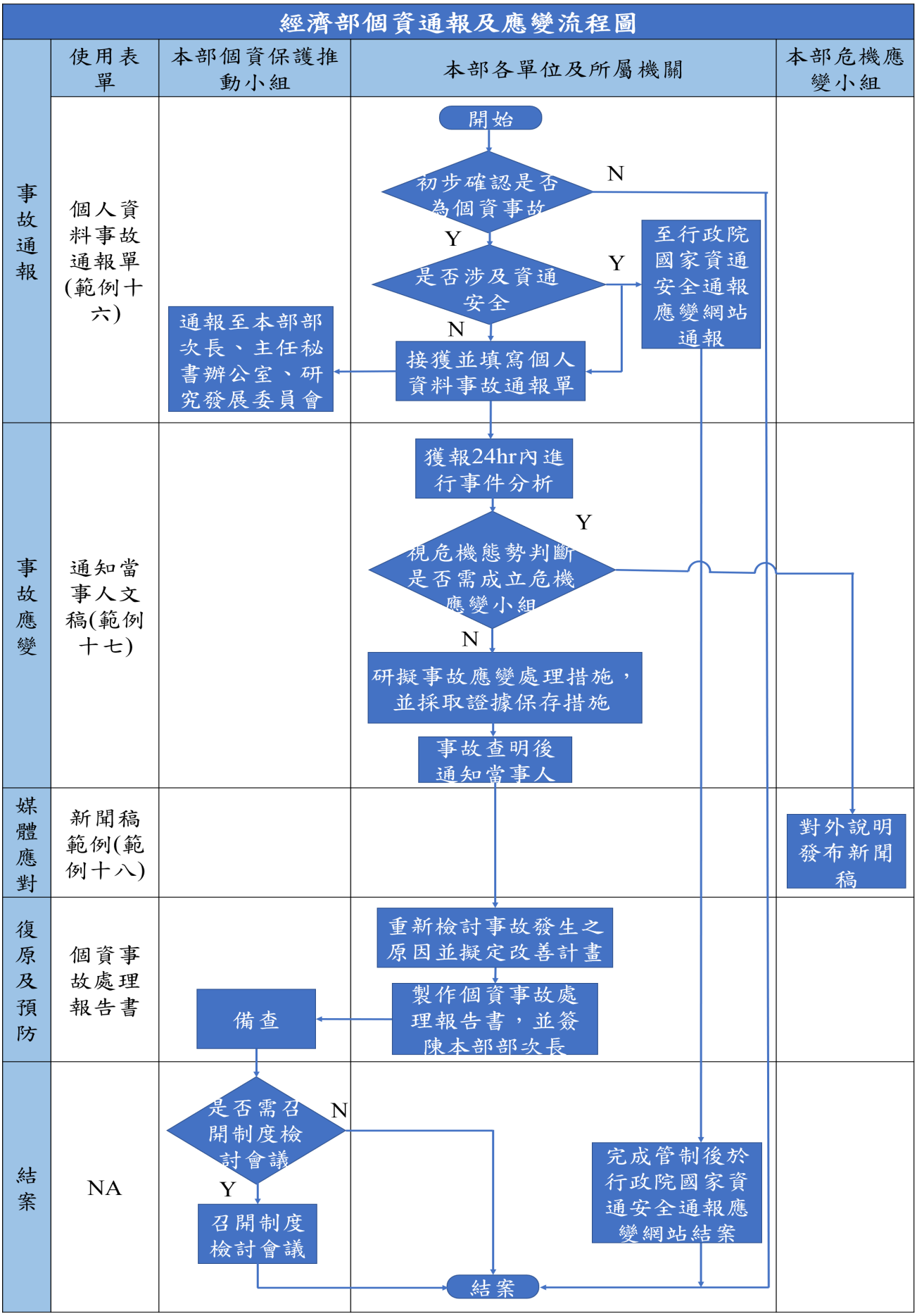
本部各單位及所屬機關於個資事故發生後，應注意媒體報導，如輿論關注須對外說明及澄清，應由危機應變小組發言人適時召開記者會或其他適當方式對外說明，或陳請本部同意後，自行發布新聞稿(參考範例十八)。

（五）復原及預防

1.本部各單位及所屬機關應於（二）至（四）之程序完成後，重新檢討事故發生之原因並擬定改善計畫；必要時，得重新進行風險評估及個人資料管理機制之設計。

2.本部各單位及所屬機關應將事故檢討及改善計畫，製作個資事故處理報告書，並簽陳本部部次長核定後，送交本部個資小組備查；必要時，得由本部個資小組召集人召開制度檢視會議。

3.若個資事故涉及資通安全，於完成復原或損害管制後應於通報應變網站進行結案。



圖表 1 經濟部個資通報及應變流程圖

柒、認知宣導及教育訓練作業程序

一、依據

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 7 款規定辦理，以有效推行個人資料保護與管理制度之各項認知宣導，並對於所有同仁，依據不同之需求以及權責分工，進行不同程度之教育訓練。

二、作業程序

（一）本部各單位及所屬機關應定期規劃個人資料保護與管理制度或個資法令之相關教育訓練，促使所屬人員了解個資保護之重要性，以提高蒐集、處理、利用個人資料之適法性及安全性意識，妥善保護個人資料。

（二）本部各單位及所屬機關得針對不同層級之人員，規劃不同程度之個資保護教育訓練。

（三）教育訓練之內容得包括：個資法及施行細則、個人資料保護管理作業程序、個人資料盤點暨風險評估實作、個資外洩事件危機處理應變、個資保護作業內部稽核實作等。

（四）為確保教育訓練之有效性，得以一定之方式（如測驗、有獎徵答、問卷調查等）進行評量。

捌、個人資料安全管理作業程序

一、依據

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 6 款及第 8 款規定辦理，以有效規範個人資料之安全管理作業，防止個人資料被竊取、竄改、毀損、滅失。

二、作業程序

（一）資料安全管理

1.本部各單位及所屬機關應建立個人資料檔案分級分類管理制度，並針對接觸人員建立安全管理規範。
2.本部各單位及所屬機關應針對資料存取、系統存取、網路存取等設定控制機制。
3.本部各單位及所屬機關設定資料存取控制時，應考量業務性質及作業之必要，根據資料處理之方式設計之。其處理方式包含但不限於記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或傳送。
4.如有職務異動、變更、離職、負責人員調動、電腦報廢等因素，應立即進行權限變更。
5.其他資料安全管理事項請參照經濟部資通安全管理規範辦理。

（二）人員管理

1.本部各單位及所屬機關應確實掌握蒐集、處理及利用個人資料檔案之相關業務流程負責人。
2.於進用人員時，本部各單位及所屬機關應進行適當的安全性評估。
3.本部各單位及所屬機關得要求相關人員簽訂保密協定，善盡保護個人資料之義務。
4.其他人員安全管理事項請參照經濟部資通安全管理相關規範辦理。

（三）設備管理

1.個人資料檔案處理之相關設備及周邊環境應有相關控管保護機制，以確保檔案之安全性，不易遭外洩及竊取之可能。
2.個人資料檔案處理，應有適當之監控措施，確保使用之軟/硬體設備為安全之控管版本，並應用防護及監控軟體進行個人資料保護及記錄。
3.關於檔案資訊環境與設備之安全控管之其他規定，請參照經濟部資通安全管理相關規範辦理。

（四）本部各單位及所屬機關就前述事項，得視其組織業務、人員、預算等，以及個人資料之數量、敏感度等，考量所欲達成之個人資料保護目的，以適當比例為之。

玖、使用紀錄、軌跡資料及證據保存作業程序

一、依據

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 10 款規定辦理，以管理與維護本部各單位及所屬機關處理個人資料、執行個人資料保護與管理制度所產生之相關使用紀錄、軌跡資料、證據等。

二、範圍

使用紀錄、軌跡資料、證據指下列資料：

（一）實施個人資料保護與管理制度之使用紀錄。

（二）個人資料檔案之使用紀錄或軌跡資料;前述軌跡資料指個人資料在蒐集、處理、利用過程中所產生非屬於原蒐集個資本體之衍生資訊（LOGFILES），包括（但不限於）資料存取人之代號、存取時間、使用設備代號、網路位址（IP）、經過之網路路徑…等，可用於比對、查證資料存取之適當性。

（三）其他必要之證據保存資料。

三、作業程序

（一）使用紀錄、軌跡資料、證據之管理

1.本部各單位及所屬機關得指定專人管理各種使用紀錄、軌跡資料、證據。

2.各項使用紀錄、軌跡資料、證據之保存，依檔案法與相關法令，及經濟部資通安全管理相關規範之規定為之。

（二）使用紀錄、軌跡資料、證據之銷毀或刪除

1.本部各單位及所屬機關應於每年十二月將超過保管期限之使用紀錄、軌跡資料、證據等銷毀或刪除。

2.各項使用紀錄、軌跡資料、證據之銷毀或刪除，依檔案法與相關法令及經濟部資通安全管理相關規範之規定為之。

壹拾、對非公務機關個人資料保護之監管作業程序

一、依據

本部各單位及所屬機關應依據聯繫作業要點規定辦理,以落實非公務機關個人資料檔案之安全維護。

二、訂定辦法

中央目的事業主管機關應依據個資法第 27 條第 3 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之標準等相關事項之辦法（以下簡稱安全維護辦法）:

（一） 尚未訂定安全維護辦法之非公務機關：

中央目的事業主管機關對於所監管之非公務機關尚未訂定安全維護辦法者，應綜合考量下列情形，定期檢討訂定該辦法之必要性：

1. 非公務機關之規模、特性。
2. 保有個人資料之數量或性質。
3. 與民眾日常生活關係密切程度。
4. 個資外洩衝擊層面廣泛程度。
5. 個資外洩將造成當事人身心危害、社會地位受損或衍生財務危機等重大影響。
6. 個人資料存取環境。
7. 個人資料傳輸之工具及方法。
8. 國際傳輸之頻率。

（二） 安全維護辦法應至少就下列事項予以規定：

1. 中央目的事業主管機關就所主管之非公務機關使用資通訊系統蒐集、處理或利用個人資料，而有下列情形之一者，應加強管理：

(1)保有消費者交易、使用商品或接受服務等過程之一般或特種個人資料，且符合中央目的事業主管機關所定應加強管理之條件。

(2)其他經中央目的事業主管機關認定應加強管理者。

2.就應加強管理者之規定，應至少包括下列資料安全管理措施：

(1)使用者身分確認及保護機制。

(2)個人資料顯示之隱碼機制。

(3)網際網路傳輸之安全加密機制。

(4)個人資料檔案及資料庫之存取控制與保護監控措施。

(5)防止外部網路入侵對策。

(6)非法或異常使用行為之監控與因應機制。

3.非公務機關個資外洩時，依安全維護辦法應通報之對象、時點、應通報事項、後續行政檢查等事項；其通報地方目的事業主管機關者，並應副知中央目的事業主管機關。中央目的事業主管機關訂定或修正發布安全維護辦法，應函知國家發展委員會（以下簡稱國發會）。

三、個資外洩案件通報

（一） 中央目的事業主管機關接獲非公務機關通報或副知，或非因通報或副知而自行知悉個資外洩案件，經確認屬該機關管轄後，應於接獲通報、副知或知悉時起 72 小時內，填列聯繫作業要點附件一「監督通報紀錄表」，通報國發會；並得依個資法第 22 條至第 25 條規定，對該非公務機關為適當之監督管理措施。

（二） 中央目的事業主管機關應就個資外洩案件之後續行政措施及處置情形，按季通報國發會；重大矚目之個資外洩案件之後續行政措施及處置情形，應即時通報國發會。

四、個資外洩案件處理

（一） 中央目的事業主管機關就個資外洩案件，經查明違反個資法之規定者，應視具體調查結果，依個資法第 47 條至第 50 條規定處理。

（二） 中央目的事業主管機關對個資外洩案件之行政檢查流程，除重大矚目之個資外洩案件依聯繫作業要點第 9 點規定確認管轄機關者外，其餘行政檢查程序，依聯繫作業要點附件二「中央目的事業主管機關對個資外洩案件之行政檢查流程圖」辦理。

壹拾壹、委外監督作業程序

一、依據

依據個資法第 4 條、個資法施行細則第 8 條規定辦理，以釐清本部及所屬機關與其受託人之責任歸屬，明定委託機關應對受託者採取適當之監督，以確保委託處理個人資料之安全管理。

二、作業程序

（一）本部各單位及所屬機關委託廠商蒐集、處理或利用個人資料者，應為適當之監督。

（二）本部及所屬機關應將委託業務區分委託對象選擇、業務履行、業務關係終止或解除等階段，分別進行個人資料保護監督管理。

（三）委託對象選擇階段

1.研擬委託業務時應考量有無個人資料蒐集之需求並確認蒐集、處理或利用之特定目的以及是否具有個資法第 6 條、第 15 條之特定情形及符合個資法第 16 條之規定。

2.選擇委託對象時，應將受託者之個人資料安全維護措施辦理情形列為廠商之評選項目（安全維護措施詳參個資法施行細則第 12 條第 2 項各款）。

3.選定受託者後，應於委託契約載明個資法施行細則第 8 條所列監督事項及監督方式（參考範例十九、範例二十）。

（四）業務履行階段

1.應定期確認受託者執行之狀況，並將確認結果記錄之（參考範例二十一）；必要時，得親自或委託專業人員進行實地訪查後，以書面敘明理由，請廠商限期改善；或請委外廠商依照執行現況自我檢核並提供作業說明及佐證資料(參考範例二十二)，以利本部各單位及所屬機關存查及監督委託業務執行現況。

2.受託者未依期限改善時，本部各單位及所屬機關得依情節輕重，以書面通知終止或解除契約之部分或全部、要求減少部分或全部價金或按契約總價之一定比例計收違約金，並得請求損害賠償。

（五）業務關係終止或解除階段

委託關係終止或解除時，應要求受託者依約定方式確實刪除、銷毀或返還因執行受託業務所保有之個人資料，並提供刪除、銷毀或返還個人資料之時間、方式、地點等紀錄；必要時，得進行實地查訪。

壹拾貳、資料安全稽核程序

一、依據

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 9 款及第 11 款規定辦理，以瞭解個資保護管理制度之實際執行狀況，並藉以瞭解相關缺失，並持續進行改善，使個資保護管理制度能夠更加完善。

二、稽核工作

本部各單位及所屬機關得由專責人員或成立稽核小組，進行個資保護作業稽核工作，稽核工作內容如下：

（一）審查內部各單位之個資保護運作情形。

（二）記錄並報告稽核結果。

（三）妥善保存稽核文件，並遵守保密規定。

（四）追蹤改善措施。

三、作業程序

（一）稽核範圍

本部各單位及所屬機關於個人資料保護作業之執行情形。

（二）稽核時間

1.於每年 12 月底之前完成稽核作業，並製作個資管理稽核報告。

2.必要時，得隨時進行內部稽核。

（三）稽核報告

報告內容應包含個資管理制度之執行狀況以及稽核後之改善計畫，稽核項目如下：

1.任務編組

是否配置管理人員及相當之資源進行個人資料保護工作。

2.蒐集、處理、利用之作業

檢視蒐集、處理或利用個人資料之流程中，是否依照法律規定以及內部管理程序進行。

3.當事人權利行使之作業

當事人行使權利時，本部各單位及所屬機關是否按照當事人權利行使流程進行回覆。

4.個資盤點與風險分析

確認個資盤點作業是否確實完成，並針對各個風險為分析並處置。

5.事故通報與應變程序

於事故發生時，是否依規定通報，並作出應變處置及預防等措施。

6.認知宣導與教育訓練

是否針對所屬人員進行認知宣導與教育訓練，並確實記錄。

7.安全管理

是否針對資料安全管理、人員管理、設備管理等層面進行管控。

8.使用紀錄、軌跡資料及證據保存

執行個資保護與管理制度等相關紀錄，是否確實保存。

9.委外監督管理

委外蒐集、處理或利用個人資料之情形，是否做好適當之監督。本部各單位及所屬機關得視各單位之組織編制或業務內容，根據稽核項目表（參考範例二十二）之內容，進行稽核項目之增刪。

10.資料安全稽核

是否定期稽核，製作稽核結果報告及進行改正。

11.缺失改善及矯正預防

是否採取適當措施，訂定執行期限及持續追蹤。

（四）稽核方式

1.稽核小組或稽核專責人員按稽核內容及當年度執行內部稽核人員名冊，擬定年度稽核規劃。

2.根據年度稽核規劃，於執行稽核預定日前 2 週內，選出執行內部稽核人員。

3.為確保稽核之客觀及公正性，內部稽核執行人員不得稽核所

屬部門。

4.內部稽核執行人員於執行內部稽核預定日前1週內，製作稽核項目表，並根據稽核項目表記錄稽核結果與說明。

5.稽核所發現之缺失，應做成改善計畫，並完成個資管理稽核報告後備查。

6.應定期確認個人資料安全執行之狀況，並將確認結果記錄之（參考範例二十三）。

7.本部各單位及所屬機關辦理有關防疫個資稽核作業時，應依嚴重特殊傳染性肺炎中央流行疫情指揮中心所定「防疫個人資料稽核指引」辦理。

壹拾參、持續改善作業程序

一、依據

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 11 款規定辦理，以持續改善本部個人資料保護與管理制度之相關程序規範，達成個資保護與管理之目標。

二、作業程序

（一）個人資料保護管理制度應由經濟部個人資料保護推動執行小組(以下簡稱本部個資小組)檢視並持續改善。

（二）本部個資小組召集人，於下列情形之一並認為有必要時，得召開制度檢視會議：

1.法令修正時。
2.重大個資外洩事故。
3.其他重大事由。

三、本部各單位及所屬機關

（一）本部各單位及所屬機關於下列情形之一並認為有必要時，得召開制度檢視會議：

1.法令修正時。
2.重大個資外洩事故。
3.稽核人員根據稽核結果提出改善計畫時。
4.其他重大事由。

（二）個人資料保護管理制度檢視會議，應做成紀錄報告書以利修正改善。

壹拾肆、附錄

一、參考範例

範例一：公文申請蒐集個人資料-法定職務

簽於○○○　　檔 號：

保存年限：

主旨：為辦理○○作業蒐集、處理個人資料，謹簽請核示。

說明：

一、依個人資料保護法(以下簡稱個資法)第 15 條及經濟部及所屬機關個人資料保護管理要點第 8 點規定辦理。

二、因辦理○○作業，基於○○○業務之需要[註](例：代號一○一國家經濟發展業務)，及本單位法定職務（請說明之)，擬蒐集、處理個人資料。

三、蒐集之個人資料種類包括：姓名、身分證編號、出生年月日、住址...等。

四、依個資法第 8 條第 2 項第 2 款規定，公務機關因執行法定職務所必要而蒐集個人資料，得免除告知義務，本案因辦理旨揭作業之必要而需蒐集相關個人資料，爰擬免告知當事人有關個資法第 8 條第 1 項規定事項。

擬辦：奉 核定後，進行○○作業，並依法蒐集、處理個人資料。

註：特定目的應列明法務部公告之「個人資料保護法之特定目的及個人資料之類別」項目

範例二：公文申請蒐集個人資料-當事人同意

簽於○○○　　檔 號：

保存年限：

主旨：為辦理○○作業蒐集、處理個人資料，謹簽請核示。

說明：

一、依據個人資料保護法(以下簡稱個資法)第 15 條及經濟部及所屬機關個人資料保護管理要點第 8 點規定辦理。

二、因辦理○○作業，基於○○業務需要[註](例：代號一○一 國家經濟發展業務)，擬於取得當事人同意後，蒐集、處理個人資料。

三、蒐集之個人資料種類：姓名、身分證編號、出生年月日、住址等。

四、依個資法第 8 條第 1 項規定，應履行告知義務，告知內容詳如附件（參考範例三個人資料蒐集、處理、利用同意書)。

擬辦：奉核定後，進行○○作業，並依法蒐集、處理個人資料。

註：特定目的應列明法務部公告之「個人資料保護法之特定目的及個人資料之類別」項目

範例三：個人資料蒐集、處理、利用同意書

個人資料蒐集、處理、利用同意書

為遵守個人資料保護法規定，並保障當事人之權利，謹依法告知下列事項：

1. 機關名稱：(例：經濟部◯◯局)
2. 蒐集之特定目的[1]：(例：代號一◯一 國家經濟發展業務)
3. 個人資料之類別[2]：(例：姓名、身分證編號、出生年月日、住址…等)
4. 個人資料利用之期間、地區、對象及方式[3]：
   (1) 期間:(例：蒐集後一年)
   (2) 地區：(例：中華民國主權範圍內)
   (3) 對象：(例：自行使用)
   (4) 方式：(例：公告)
5. 依個人資料保護法第 3 條規定，當事人可行使以下權利[4]：
   (1) 查詢或請求閱覽。
   (2) 請求製給複製本。
   (3) 請求補充或更正。
   (4) 請求停止蒐集、處理及利用。
   (5) 請求刪除。

   若有上述需求，請與本單位聯繫，於填妥本單位當事人權利行使申請書後，本單位將依法進行回覆。另依個人資料保護法第 14 條規定，查詢或請求閱覽個人資料或製給複製本者，本單位得酌收必要成本費用。
6. 若未提供正確個人資料,本單位將無法提供您特定目的範圍內之相關服務[5]。

本人已充分知悉貴單位上述告知事項，並同意貴單位蒐集、處理、利用本人之個人資料。

立同意書人:

中華民國　　年　　月　　日

---

1. 公務機關應於法定職務必要範圍內蒐集處理或利用當事人之個人資料。請斟酌法定職務之內容，並參考法務部公告之個人資料保護法之特定目的項目表，填寫蒐集之特定目的。
2. 個人資料之類別請參照法務部公告之個人資料保護法之個人資料之類別填寫。
3. 個人資料之利用應於特定目的必要範圍內為之，特定目的範圍外之利用必須符合個人資料保護法第 16 條但書之要件，始為合法。另，特定目的之範圍將影響是否應該主動或依當事人請求為停止處理、利用及刪除之依據，本項請務必填寫完整。
4. 當事人權利行使為個資法明定之當事人權利，請務必提供權利行使管道及方式。
5. 若有其他對於當事人重要權益之影響，請務必於本項中一併告知。

範例四：公文申請補充、更正個人資料

簽於◯◯◯　　檔　　號：

保存年限：

主旨：為辦理個人資料補充、更正，謹簽請核示。

說明：

一、依據個人資料保護法(以下簡稱個資法)第 11 條及經濟部及所屬機關個人資料保護管理要點第 9 點規定辦理。

二、因個人資料錯誤、缺漏（當事人◯◯◯），依據個資法第 11 條第 1 項規定，補充、更正個人資料（個人資料檔案名稱、檔案類型）。

三、個人資料之類別：姓名、身分證編號、出生年月日、住址…等。

四、該個人資料曾提供◯◯◯利用，依據個資法第 11 條第 5 項規定，應通知◯◯◯。

擬辦：奉核定後，進行補充、更正該個人資料，並函知◯◯◯。

範例五：公文申請刪除、銷毀個人資料

簽於○○○　　檔　　號：

保存年限：

主旨：為辦理個人資料之刪除、銷毀，謹簽請核示。

說明：

一、依據個人資料保護法(以下簡稱個資法)第 11 條及經濟部及所屬機關個人資料保護管理要點第 11 點規定辦理。

二、原辦理○○作業，基於業務需要[註](例：代號○七二 政令宣導或經當事人同意)而處理、利用之個人資料檔案(檔案名稱、檔案類型)，茲因個人資料蒐集之特定目的消失，依據個資法第 11 條第 3 項規定，應主動刪除、銷毀個人資料檔案。

三、個人資料之類別：姓名、身分證編號、出生年月日、住址…等。

擬辦：奉核定後，進行將個人資料檔案紙本銷毀（或其他方式銷毀），及將電子檔案刪除，並為確實記錄。

註：特定目的應列明法務部公告之「個人資料保護法之特定目的及個人資料之類別」項目

範例六：公文申請個人資料特定目的外利用

簽於○○○　　檔　　號：

保存年限：

主旨：為辦理個人資料之特定目的外利用，謹簽請核示。

說明：

一、依據個人資料保護法(以下簡稱個資法)第 16 條及經濟部及所屬機關個人資料保護管理要點第 8 點規定辦理。

二、原辦理○○作業，基於○○業務之特定目的以及執行法定職務（請說明，例：代號一○一 國家經濟發展業務）而蒐集、處理、利用之個人資料（檔案名稱、檔案類型），茲因辦理○○業務，另符合○○之特定目的（例：代號○七二 政令宣導），因○○業務係為執行○○政策，為增進公共利益所必要，符合個資法第 16 條但書第 2 款[註]，得為個人資料之原特定目的外之利用。

擬辦：奉核定後，依法進行特定目的外利用。

註：應依個資法第 16 條但書第 1 款至第 6 款事由之一，援引敘明做為特定目的外利用之依據，並本於職權敘明符合該規定之情形。

範例七：公文申請個人資料之特定目的外利用-當事人同意

簽於○○○　　檔　　號：

保存年限：

主旨：為辦理個人資料之特定目的外利用，謹簽請核示。

說明：

一、依據個人資料保護法(以下簡稱個資法)第 16 條及經濟部及所屬機關個人資料保護管理要點第 8 點規定辦理。

二、原辦理○○作業，基於○○業務之特定目的以及執行法定職務（請說明，例：代號一○一 國家經濟發展業務）而蒐集、處理、利用之個人資料（檔案名稱、檔案類型），茲因辦理○○業務，另符合○○之特定目的（例：代號○七二 政令宣導），以及徵求當事人同意，符合個資法第 16 條但書第 7 款，得為個人資料之原特定目的外之利用。

三、本案依法應告知當事人之事項，詳如附件特定目的外利用同意書格式（參考範例八特定目的外利用同意書）。

擬辦：奉核定後，依法取得當事人同意並進行特定目的外利用。

範例八：特定目的外利用同意書

特定目的外利用同意書

為遵守個人資料保護法(以下簡稱個資法)規定，並保障當事人之權利，謹依法告知下列事項：

1. 機關名稱：(例：經濟部○○局)
2. 原蒐集之特定目的：(例：國家經濟發展業務)(法務部公告之個資法之特定目的第一○一項)[1]
3. 其他利用之特定目的：(例：政令宣導)(法務部公告之個資法之特定目的第○七二項)
4. 個人資料之類別[2]：(例：姓名、身分證編號、出生年月日、住址等)
5. 個人資料利用之期間、地區、對象及方式[3]：
   (1) 期間：(例：蒐集後一年)
   (2) 地區：(例：中華民國主權範圍內)
   (3) 對象：(例：自行使用)
   (4) 方式：(例：網站公告)
6. 依個資法第 3 條規定，當事人可行使以下權利[4]：
   (1) 查詢或請求閱覽。
   (2) 請求製給複製本。
   (3) 請求補充或更正。
   (4) 請求停止蒐集、處理及利用。
   (5) 請求刪除。

   若有上述需求，請與本單位連繫，於填妥本單位當事人權利行使申請書後，本單位將依法進行回覆。另依個資法第 14 條規定，查詢或請求閱覽個人資料或製給複製本者，本單位得酌收必要成本費用。
7. 若您拒絕同意，本單位將無法提供您特定目的範圍外之相關服務[5]。

本人已充分知悉貴單位上述告知事項，並同意貴單位蒐集、處理、利用本人之個人資料。

立同意書人:

中華民國　　年　　月　　日

---

1. 公務機關應於法定職務必要範圍內利用當事人之個人資料。請斟酌法定職務之內容，並參考法務部公告之特定目的項目表，填寫蒐集之特定目的。
2. 個人資料之類別請參照法務部公告之個人資料類別表填寫。
3. 個人資料之利用應於特定目的必要範圍內為之，特定目的範圍外之利用必須符合個人資料保護法 16 條但書之要件，始為合法。另，特定目的之範圍將影響是否應該主動或依當事人請求為停止處理、利用及刪除之依據，本項請務必填寫完整。
4. 當事人權利行使為個資法明定之當事人權利，請務必提供權利行使管道及方式。
5. 若有其他對於當事人重要權益之影響，請務必於本項中一併告知。

範例九：公文申請停止（蒐集）處理、利用

簽於○○○　　檔 號：

保存年限：

主旨：為辦理個人資料之停止(蒐集、）處理、利用，謹簽請核示。

說明：

一、依據個人資料保護法第 11 條及經濟部及所屬機關個人資料保護管理要點第 11 點規定辦理。

二、原辦理○○作業，基於○○業務需要[1](例：代號○七二 政令宣導之特定目的或當事人書面同意[2])而(蒐集、）處理、利用之個人資料檔案（檔案名稱、檔案類型)，茲因個人資料蒐集之特定目的消失(或正確性有爭議、或期限屆滿、或違法蒐集處理利用)，應依法停止(蒐集、）處理、利用。

三、個人資料之類別：姓名、身分證編號、出生年月日、住址…等。

擬辦：奉核定後，依法將該個人資料為註記及停止(蒐集、）處理、利用，並為確實記錄。

---

1 特定目的應列明法務部公告之個資法之特定目的項目。

2.105 年 3 月 15 日施行之個資法第 15 條修正放寬當事人同意之方式。不以書面為限，請視本案蒐集個資時經當事人同意之方式敘明之。

範例十：當事人權利行使申請書

文件編號：

當事人權利行使申請書

申請日期：中華民國○年○月○日

申請事項	□查詢、閱覽□製給複製本 □補充、更正□刪除□停止處理、利用□停止違法蒐集、處理或利用
原因說明	
欲申請之資料	
當事人基本資料	
姓名： 電話： 住址： 證明文件：□身分證□健保卡□駕照□護照□其他	
代理人基本資料（非本人申請時）	
代理人姓名： 代理人之住址： 代理人之電話： 與當事人之關係： 證明文件：□委託書 其他身分份證明文件：□身分證□健保卡□駕照□護照□其他	
申請人簽名	（非本人申請時，應由代理人簽名並加蓋當事人印章）
備註	1. 查詢、閱覽、製給複製本之申請於受理日起 15 日內回覆，延長期間不得超過 15 日，並且將書面通知延長原因。 2. 補充、更正、刪除、停止處理、利用、停止違法蒐集處理或利用之申請，於受理日起 30 日內回覆，延長期間不得超過 30 日，並且將延長原因以書面通知當事人。 3. 具有個資法第 10 條但書及第 11 條但書之特定要件時，將駁回申請，並告知原因。 4. 對於查詢、閱覽、製給複製本之申請，得酌收成本費用。
處理情形（受理單位填寫）	
擬辦事項	是否延長回覆期間 □無延長回覆期間 □延長回覆期間，延長____天。 （延長原因：_____） 准駁情形 □核准申請 □駁回申請，(駁回原因：_____)
批示	
以上事項擬奉核示後函復當事人	

範例十一：委託書

委託書

立委託書人_____，茲因ＯＯＯ，特委託_____持用本人之印章及有關文書證件，辦理個人資料權利行使之事宜，恐口無憑，特立本委託書乙份為據。

委託人：　　（簽名或蓋章）
住　址：
身分證統一編號：
出生年月日：

受託人：　　（簽名或蓋章）
住　址：
身分證統一編號：
出生年月日：

中華民國　　年　　月　　日

範例十二：個資盤點表

單位名稱	
單位主管	
盤點人員	

主要業務、職掌	細部作業名稱	個人資料檔案名稱	主管單位	保有單位	檔案形態	保有依據	是否需告知	特定目的	個人資料類別	§17對外公告
					□紙本類 □電子類 □電子檔-可攜式媒體 □系統資料庫		□Y □N			□Y □N

（續下表）

資料來源	內部傳送	外部傳送	委外	個人資料項目	特種個人資料	保管方式	保存期限	銷毀方式	備註	單位名稱
				□姓名 □生日 □身分證號 □護照號碼 □特徵 □指紋 □婚姻 □家庭 □教育 □職業 □聯絡方式 □財務情況 □社會活動 □其他：_____	□無 □病歷 □醫療 □基因 □性生活 □健康檢查 □犯罪前科		□法定保存期限：____ □自訂保存期限：____			

個資盤點表填寫說明

欄位	填寫說明
主要業務、職掌	依單位業務、職掌內容、業務項目等，列出主要的作業流程名稱。
細部作業名稱	前項作業流程名稱，依其日常的辦理流程，再個別區分成細部作業。
個人資料檔案名稱	包含可識別當事人之個人資料檔案名稱。
主管單位	負責制定該個人資料檔案項目與欄位之部門。(業務主管部門或個資檔案之規劃部門)
保有單位	保存及管理個人資料檔案之部門。
檔案形態	檔案型態分為下列四種： 1.紙本類：指實體紙本文件。 2.電子類：包含報表、文件掃描檔、照片、圖片、傳真、影像檔等相關電子文件檔案，如 WORD、EXCEL、PDF、WMV 等數位型式之檔案。 3.電子檔-可攜式媒體：指上述數位形式文件保存於可攜式媒體。 4.系統資料庫：指個人資料僅保存於資訊系統內，未另外列印成紙本或另存成電子檔案。 需分筆列示於個人資料盤點清冊。
保有依據	是否有法定保有依據或契約或機關自定之保有依據。
是否需告知	請判斷是否需依個資法第 8 條及第 9 條規定，蒐集、處理或利用個人資料時應明確履行告知義務。 如需告知，請填 Y；得免為告知，請填 N。
特定目的	依法務部公告之「個人資料保護法之特定目的及個人資料之類別」填寫個人資料蒐集或處理之特定目的。
個人資料類別	依法務部公告之「個人資料保護法之特定目的及個人資料之類別」填寫個人資料類別。
§17 對外公告	請判斷該個人資料檔案是否依個資法第 17 條規定，對外公告個人資料檔案名稱、類別、特定目的、保有依據等必要項目。 如需對外公告，請填 Y；若無需公告，請填 N。

資料來源	該個人資料檔案取得管道或建立之方法。
內部傳送	與該個人資料檔案之蒐集、處理或利用有關之內部部門。
外部傳送	與組織之個資檔案提供外部利用有關，本項指無法歸屬於本機關之單位或人員等。
委外	提供之服務與個資檔案之蒐集、處理及利用流程有關，且會接觸到個資內容之委外機(構)或人員。
個人資料項目	姓名、生日、身分證號碼、護照號碼、特徵、指紋、婚姻、家庭、教育、職業等。
特種個人資料	病歷、醫療、基因、性生活、健康檢查、犯罪前科。
保管方式	該個人資料檔案之保管方式(如：放置於辦公室檔案櫃並上鎖、儲存於承辦人電腦並將檔案加密、資料庫主機…等)。
保存期限	法定保存期限：該個人資料檔案依據檔案法等相關法律規定之保存期限(如：3 年、5 年…等)，並請說明法定依據。 自訂保存期限：該個人資料檔案依據本機關自訂之保存期限(如：3 年、5 年…等)。
銷毀方式	該個人資料檔案之銷毀方式(如：由總務單位統一辦理銷毀作業…等)。
備註	任何可補充說明的資訊。
單位名稱	個資檔案所屬之單位名稱。

個資盤點表-填寫範例

主要業務、職掌	細部作業名稱	個人資料檔案名稱	主管單位	保有單位	檔案形態	保有依據	是否需告知	特定目的	個人資料類別	§17 對外公告
○○○業務之規劃、推動與輔導	○○○活動報名作業	○○○活動報名表	經濟部○○司	○○科	■紙本類 □電子類 □電子檔-可攜式媒體 □系統資料庫	○○法、○○要點	■Y □N	一○一國家經濟發展業務	C○○一辨識個人者、C○○三政府資料中之辨識者。	■Y □N

（續下表）

資料來源	內部傳送	外部傳送	委外	個人資料項目	特種個人資料	保管方式	保存期限	銷毀方式	備註	單位名稱
當事人自行提供	經濟部○○處	內政部○○司	○○行銷公司	■姓名 □生日 ■身分證號 □護照號碼 □特徵 □指紋 □婚姻 □家庭 □教育 □職業 ■聯絡方式 □財務情況 □社會活動 □其他：_____	■無 □病歷 □醫療 □基因 □性生活 □健康檢查 □犯罪前科	放置於辦公室檔櫃並上鎖	■法定保存期限：○○法：○年 ■自訂保存期限：檔案保存年限基準表：○年	保存期限屆滿後○○司統一辦理銷毀作業	N/A	○○科

範例十三：風險情境表

風險大分類	風險子分類	個資潛在風險事件
1.紙本類	1.1 處理	1.1.1 紙本文件於內部處理過程中，是否在長時間不使用或於下班時收存於辦公室上鎖之資料櫃。
	1.2 保存	1.2.1 紙本文件之保存(含暫存區)地點是否具備進出管控措施。
		1.2.2 紙本文件歸檔、入倉(庫)或集中保管前，是否確實清點數量及內容。
		1.2.3 紙本文件存放地點是否已有消防、滅火、溫度控制等設施。
	1.3 傳遞	1.3.1 紙本文件於內部傳遞過程中，是否具有簽收/點收等控管措施。
		1.3.2 紙本文件提供外部利用是否均有公文往返等使用紀錄。
	1.4 銷毀	1.4.1 包含個資之紙本文件是否禁止回收使用。
		1.4.2 紙本文件於內部進行銷毀時，是否均銷毀致無法辨識。
		1.4.3 紙本文件交由受委託廠商銷毀前，是否已簽訂包含雙方權利義務及賠償條款之契約或保密協議。
		1.4.4 紙本文件交由受委託廠商進行銷毀時，是否已妥善進行監銷並留存紀錄。
2.電子類	2.1 傳輸	2.1.1 同仁透過對外寄發、傳輸個資檔案是否均進行加密。
		2.1.2 同仁對外傳輸個資檔案是否均有傳輸記錄，如 Email 寄件備份、FTP 傳輸記錄、網路硬碟等。
	2.2 保存	2.2.1 存於本機電腦之個資檔案，是否均有加密或存放於專用且安全之資料夾。
	2.3 銷毀	2.3.1 電子檔案保存期限屆滿後是否均進行刪除。

3. 電子檔-可攜式媒體	3.1 傳遞	3.1.1 將個人資料檔案使用可攜式媒體傳遞時，是否均進行加密。
	3.2 銷毀	3.2.1 儲存個人資料之可攜式媒體不再使用或損毀時，是否均進行刪除資料或實體破壞。
4. 系統資料庫	4.1 存取權限	4.1.1 資訊系統之使用者帳號是否均定期審查。
		4.1.2 系統是否具備職務區隔機制，並給予適當之存取權限。
	4.2 使用紀錄	4.2.1 資訊系統是否已具有記錄使用者活動日誌功能。
		4.2.2 單位主管或其授權人員是否定期審查資訊系統使用者之活動日誌。
5. 委外作業類	5.1 選商	5.1.1 委外案件是否均會評估及選擇可提供符合組織對個人資料保護需求之受委託廠商(如一年內未曾發生個資外洩事件、重大資安事件或有無通過 ISO 27001、BS10012、TPIPAS、ISO29100 等驗證)。
	5.2 簽約	5.2.1 在委託外部單位處理個人資料是否有簽訂契約，並包含適當安控措施是否足夠。
		5.2.2 組織與受委託廠商所簽訂之契約中是否已包含是否得將個人資料處理作業進行轉包/分包之規定。
		5.2.3 若允許轉包/分包，受委託廠商與其複委託廠商(下包商)所簽訂之契約是否已要求複委託廠商實行與受委託廠商相同等級之安控措施。
		5.2.4 組織與受委託廠商所簽訂之契約中是否已明確規範，當資料逾保存期限或契約終止時，有關個人資料之銷毀、交還原組織或其他處理方式。
	5.3 履約	5.3.1 於委託外部單位處理個人資料契約期間內，是否定期監督或實地審查受委託廠商之安控措施是否落實執行。
		5.3.2 組織是否定期依據與受委託廠商所簽訂之契約進行監督，當資料逾保存期限或契約終

		止時確認有關個人資料之銷毀、交還原組織或其他處理之方式。
	5.4 小額採購	5.4.1 如以小額採購方式委託外部單位蒐集、處理、利用或銷毀個人資料時，是否均簽訂書面協議並落實監督作業。

範例十四：個資流程衝擊分析表

單位名稱	
單位主管	
評估人員	

作業流程名稱		衝擊分析項目				衝擊值	備註	單位名稱
主要業務、職掌	細部作業名稱	個資數量	個資敏感度	損害組織信譽	個資當事人隱私衝擊			
		5:每年產生大於1000筆	5:包含姓名、身分證號、私人連絡方式(電話+地址)、財務情況、指紋、特種個資	5:若作業發生個資外洩事故，將導致機關形象、信譽受到非常嚴重損害，如：導致國際性媒體報導負面新聞、造成民眾集結遊行抗爭或上級機關關切等情形。	5:洩漏資訊，對個資當事人造成重大影響，如：勒索、綁架。	衝擊值係以衝擊構面之評分加總		
		3:每年產生100~1000筆	3:包含姓名、身分證號、護照、私人聯絡方式(電話及地址)、其他非特種特資欄位	3:若作業發生個資外洩事故，將導致機關形象、信譽受到嚴重損害，如：導致3家以上媒體報導負面新聞或造成民眾至機關抗議或陳情等情形。	3:洩漏資訊，對個資當事人有部分影響，如：遭受不明騷擾、詐騙。			
		1:每年產生小於100筆	1:僅含姓名、聯絡方式(電話)	1:若該作業發生個資外洩事故，將導致機關形象、信譽受到輕微損害，如：導致部分媒體報導負面新聞、造成多位民眾電話抱怨等情形。	1:洩漏資訊，對個資當事人產生些微影響			

個資流程衝擊分析表填寫說明

欄位	填寫說明
主要業務、職掌	依個資盤點表之「主要業務、職掌」欄位填寫。
細部作業名稱	依個資盤點表之「細部作業名稱」欄位填寫。
個資數量	依每年保有個資之筆數，以「衝擊分析項目」個資數量欄位所述級距進行評估。
個資敏感度	保有之個資資料，以「衝擊分析項目」個資敏感度欄位所述級距進行評估。
損害組織信譽	保有之個資資料，以「衝擊分析項目」損害組織信譽欄位所述級距進行評估。
個資當事人隱私衝擊	保有之個資資料，以「衝擊分析項目」個資當事人隱私衝擊欄位所述級距進行評估。
衝擊值	個資數量、個資敏感度、損害組織信譽、個資當事人隱私衝擊之評分加總。
備註	任何可補充說明的資訊。
單位名稱	個資檔案所屬之單位名稱。

個資流程衝擊分析表-填寫範例

作業流程名稱		衝擊分析項目				衝擊值	備註	單位名稱
主要業務、職掌	細部作業名稱	個資數量	個資敏感度	損害組織信譽	個資當事人隱私衝擊			
		5:每年產生大於1000筆	5:包含姓名、身分證號、私人連絡方式(電話+地址)、財務情況、指紋、特種個資	5:若作業發生個資外洩事故，將導致機關形象、信譽受到非常嚴重損害，如：導致國際性媒體報導負面新聞、造成民眾集結遊行抗爭或上級機關關切等情形。	5:洩漏資訊，對個資當事人造成重大影響，如:勒索、綁架。	衝擊值係以衝擊構面之評分加總		
		3:每年產生100~1000筆	3:包含姓名、身分證號、護照、私人聯絡方式(電話及地址)、其他非特種特資欄位	3:若作業發生個資外洩事故，將導致機關形象、信譽受到嚴重損害，如：導致3家以上媒體報導負面新聞或造成民眾至機關抗議或陳情等情形。	3:洩漏資訊，對個資當事人有部分影響，如：遭受不明騷擾、詐騙。			
		1:每年產生小於100筆	1:僅含姓名、聯絡方式(電話)	1:若該作業發生個資外洩事故，將導致機關形象、信譽受到輕微損害，如：導致部分媒體報導負面新聞、造成多位民眾電話抱怨等情形。	1:洩漏資訊，對個資當事人產生些微影響			
○○○業務之規劃、推動與輔導	○○○活動報名作業	5	3	1	3	12	N/A	○○科

範例十五：個資流程作業風險評估表

單位名稱	
單位主管	
評估人員	

作業流程名稱		風險控管分類			衝擊值(A)	個資侵害風險發生可能性(B)	風險值	備註	單位名稱
主要業務、職掌	細部作業名稱	風險分類大	風險分類子	個資檔案控管措施(風險情境)	從個人資料衝擊分析表將衝擊值帶入	5：控管嚴謹度低、經常被忽略、現行個資檔案控管方式沒有詳細規範。	風險值=個資作業流程衝擊值(A)×風險發生可能性(B)		
						3：控管嚴謹度中等、偶發性被忽略、現行個資檔案控管方式僅有部分規範。			
						1：控管嚴謹度高、充分落實，現行個資檔案控管方式已有詳細規範。			
						0：不適用			

個資流程作業風險評估表填寫說明

欄位	填寫說明
主要業務、職掌	依個資流程衝擊分析表之「主要業務、職掌」欄位填寫。
細部作業名稱	依個資流程衝擊分析表之「細部作業名稱」欄位填寫。
風險大分類	依「細部作業名稱」囊括之個人資料檔案形態填入，詳細內容請參考風險情境表。 若「細部作業名稱」囊括之個人資料檔案含委外作業，則需加入委外作業類。
風險子分類	依前欄之風險大分類展開風險子分類逐一填入，詳細內容請參考風險情境表。
個資檔案控管措施(風險情境)	依前欄之風險子分類展開該類別風險情境，詳細內容請參考風險情境表。
衝擊值	從個人資料衝擊分析表將衝擊值填入。
個資侵害風險發生可能性評估	以「個資侵害風險發生可能性」欄位所述級距進行評估。 於受評估之個資作業流程中，該風險情境不存在者，填「0」(不適用)。
風險值	個資作業流程衝擊值x風險發生可能性。
備註	任何可補充說明的資訊。
單位名稱	個資檔案所屬之單位名稱。

個資流程作業風險評估表-填寫範例

作業流程名稱		風險控管分類			衝擊值(A)	個資侵害風險發生可能性(B)	風險值	備註	單位名稱
主要業務、職掌	細部作業名稱	風險大分類	風險子分類	個資檔案控管措施(風險情境)	從個人資料衝擊分析表將衝擊值帶入	5：控管嚴謹度低、經常被忽略、現行個資檔案控管方式沒有詳細規範。 3：控管嚴謹度中等、偶發性被忽略、現行個資檔案控管方式僅有部分規範。 1：控管嚴謹度高、充分落實，現行個資檔案控管方式已有詳細規範。 0：不適用	風險值=個資作業流程衝擊值(A)×風險發生可能性(B)		
○○○業務之規劃、推動與輔導	○○○活動報名作業	1.紙本類	1.1 處理	1.1.1 紙本文件於內部處理過程中，長時間不使用或下班時收存於辦公室上鎖之資料櫃。	12	1	12	N/A	○○科

○○○業務之規劃、推動與輔導	○○○活動報名作業	1.紙本類	1.2 保存	1.2.1 紙本文件之保存(含暫存區)地點具備進出管控措施。	12	3	36	N/A	○○科
○○○業務之規劃、推動與輔導	○○○活動報名作業	1.紙本類	1.2 保存	1.2.2 紙本文件歸檔、入倉(庫)或集中保管前，確實清點數量及內容。	12	1	12	N/A	○○科
○○○業務之規劃、推動與輔導	○○○活動報名作業	1.紙本類	1.2 保存	1.2.3 紙本文件存放地點有消防、滅火、溫度控制等設施。	12	3	36	N/A	○○科
○○○業務之規劃、推動與輔導	○○○活動報名作業	1.紙本類	1.3 傳遞	1.3.1 紙本文件於內部傳遞過程中，具有簽收/點收等控管措施。	12	5	60	N/A	○○科

○○○業務之規劃、推動與輔導	○○○活動報名作業	1.紙本類	1.3傳遞	1.3.2 紙本文件提供外部利用均有公文往返等使用紀錄。	12	1	12	N/A	○○科
○○○業務之規劃、推動與輔導	○○○活動報名作業	1.紙本類	1.4銷毀	1.4.1 包含個資之紙本文件均不進行回收使用。	12	3	36	N/A	○○科
○○○業務之規劃、推動與輔導	○○○活動報名作業	1.紙本類	1.4銷毀	1.4.2 紙本文件於內部進行銷毀時，均銷毀致無法辨識。	12	3	36	N/A	○○科
○○○業務之規劃、推動與輔導	○○○活動報名作業	1.紙本類	1.4銷毀	1.4.3 紙本文件交由受委託廠商銷毀前，已簽訂包含雙方權利義務及賠償條款之契約或保密協議。	12	5	60	N/A	○○科

○○○業務之規劃、推動與輔導	○○○活動報名作業	1.紙本類	1.4 銷毀	1.4.4 紙本文件交由受委託廠商進行銷毀時，妥善進行監銷並留存紀錄。	12	3	36	N/A	○○科
○○○業務之規劃、推動與輔導	○○○活動報名作業	5.委外作業類	5.1 選商	5.1.1 委外案件均會評估及選擇可提供符合組織對個人資料保護需求之受委託廠商(如一年內未曾發生個資外洩事件、重大資安事件或有無通過ISO 27001、BS10012、TPIPAS、ISO29100 等驗證)。	12	5	60	N/A	○○科

○○○業務之規劃、推動與輔導	○○○活動報名作業	5.委外作業類	5.2 簽約	5.2.1 在委託外部單位處理個人資料有簽訂契約，並包含適當安控措施是否足夠。	12	3	36	N/A	○○科
○○○業務之規劃、推動與輔導	○○○活動報名作業	5.委外作業類	5.2 簽約	5.2.2 組織與受委託廠商所簽訂之契約中包含是否得將個人資料處理作業進行轉包/分包之規定。	12	1	12	N/A	○○科

○○○業務之規劃、推動與輔導	○○○活動報名作業	5.委外作業類	5.2 簽約	5.2.3 若允許轉包/分包，受委託廠商與其複委託廠商(下包商)所簽訂之契約已要求複委託廠商實行與受委託廠商相同等級之安控措施。	12	3	36	N/A	○○科
○○○業務之規劃、推動與輔導	○○○活動報名作業	5.委外作業類	5.2 簽約	5.2.4 組織與受委託廠商所簽訂之契約中明確規範，當資料逾保存期限或契約終止時，有關個人資料之銷毀、交還原組織或其他處理方式。	12	3	36	N/A	○○科

○○○業務之規劃、推動與輔導	○○○活動報名作業	5.委外作業類	5.3 履約	5.3.1 於委託外部單位處理個人資料契約期間內，定期監督或實地審查受委託廠商之安控措施是否落實執行。	12	3	36	N/A	○○科
○○○業務之規劃、推動與輔導	○○○活動報名作業	5.委外作業類	5.3 履約	5.3.2 組織定期依據與受委託廠商所簽訂之契約進行監督，當資料逾保存期限或契約終止時確認有關個人資料之銷毀、交還原組織或其他處理之方式。	12	3	36	N/A	○○科

○○○業務之規劃、推動與輔導	○○○活動報名作業	5.委外作業類	5.4 小額採購	5.4.1 如以小額採購方式委託外部單位蒐集、處理、利用或銷毀個人資料時，均簽訂書面協議並落實監督作業。	12	0	0	N/A	○○科

範例十六：個人資料事故通報單

<table>
<tr><th colspan="4">通報單位填寫</th></tr>
<tr><td>通報單位</td><td></td><td>通報時間</td><td>年　　月　　日
時　　分</td></tr>
<tr><td>個資事故說明</td><td colspan="3">一、個資事故發生與發現之日期與時間：

二、洩漏單位
□ 本部單位洩漏
□ 委外廠商洩漏

三、遭受揭露之個資範圍與敘述：(如：個人資料檔案名稱、個人資料類別及個人資料數量等)

四、遭受揭露個資之儲存媒體：(如：紙本、電子檔案、系統資料庫、光碟片、USB碟、可攜式硬碟或記憶卡等)</td></tr>
<tr><td>承辦單位</td><td colspan="2">會辦單位</td><td>批示</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><th colspan="4">個人資料保護推動執行小組　受理窗口(法規會)填寫</th></tr>
<tr><td>受理人</td><td></td><td>受理時間</td><td>年　月　日
時　分</td></tr>
<tr><td>事故分析及判定</td><td colspan="3">經初步分析後判定為：
□ 個資事故/事故權責單位名稱：
□ 疑似個資事件（持續觀察，暫不處理）
□ 非個資事件　（不處理，逕行結案）
說明：</td></tr>
<tr><td>承辦人</td><td colspan="2">科長</td><td>單位主管</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
</table>

範例十七：通知當事人文稿

○○○ 您好：

茲因經濟部(以下簡稱本部)「○○系統」遭植入惡意後門程式，致使台端之個人資料遭駭客竊取並公布於○○上，經調查確認本案確為個人資料外洩事故。

本部對此一事故極為重視，特說明本次事故之處理，以化解台端之疑慮。

1、台端之個人資料因本部網站遭駭客植入惡意程式導致外洩，影響您的隱私權益，依個人資料保護法規定，本部需通知您有關本案之實際情況及本部已採取之因應措施。

2、(此案例為系統遭駭客入侵導致個人資料外洩，因應措施可參考下述說明)本部業已進行 APT 惡意程式掃描，移除被植入之後門程式，並將網站程式重新上架，另已通知 Google 公司移除其搜尋引擎所儲存之快取資料，……，以避免您登錄於本部系統的個人資料再次被搜尋到。

3、若台端仍有疑慮，可與本部○○○聯絡，聯絡電話：○○○-○○○○，將由專人為您說明及釋疑。

本部對此次事件造成台端之困擾，再次致上歉意。本部必記取此次事件之經驗，將再加強網站程式之安全性檢測，並強化資訊系統程式開發過程之安全性管理，確保類似事件不再發生，以保護個資當事人之隱私與權益。

通知單位：○○○

中華民國　○年 ○ 月 ○ 日

範例十八：新聞稿

經濟部「○○系統」遭駭客植入惡意後門程式
已完成清除惡意程式，網站重新開放使用

針對○月○日經濟部(以下簡稱本部)「○○系統」保有的個人資料遭外洩乙案，本部於○日接獲○○投訴後，立即依據內部之個人資料保護與資通安全規定，成立調查小組，迅速追查事件原因。

經查，本事件為本部○○系統遭駭客植入惡意後門程式導致資料外洩，針對本事件之處理如下：

1、(此案例為系統遭駭客入侵導致個人資料外洩，因應措施可參考下述說明)本部業已進行 APT 惡意程式掃描，移除被植入之後門程式，並將系統重新上架，另已通知 Google 公司移除其搜尋引擎所儲存之快取資料，……，以避免當事人之個人資料被搜尋到。

2、對於個人資料遭外洩之當事人，本部深感抱歉，若當事人因此權益受損，本部將依法負起必要之責任。

3、本部將再加強網站程式之安全性檢測，並強化資訊系統程式開發過程之安全性管理，確保類似事件不再發生，以保護個資當事人之隱私與權益。

本事件將依本部個人資料保護與資通安全相關程序，進行檢討及改善相關作業。

範例十九：契約個人資料保護條款(一般版)

個人資料保護條款範本

廠商依本契約受機關委託蒐集、處理或利用個人資料及檔案（指自然人之姓名、身分證統一編號、職業、聯絡方式、社會活動、其他得以直接或間接方式識別該個人之資料等個人資料保護法(以下簡稱個資法)所指個人資料）時，廠商應遵守下列約定：

第 1 條　蒐集、處理或利用時之義務

廠商基於本契約蒐集、處理或利用個人資料時，應符合個資法第 15 條或第 16 條要件、經濟部及所屬機關個人資料保護管理要點等相關規定。

廠商基於本契約蒐集、處理或利用特種個人資料時，應遵守個資法及經濟部及所屬機關個人資料保護管理要點等相關規定，並檢附符合個資法第 6 條第 1 項但書各款任一要件之說明。

廠商不得利用機關所提供或因執行本契約所蒐集之個人資料及檔案，為自己或他人利益從事本契約委託範圍以外之處理或利用行為，包括但不限於行銷或商業推銷等相關活動、連結比對廠商本身保有資料進行處理利用，或以任何方式或方法交付予履約無關之第三人。

廠商僅得於機關以下指示之範圍內，蒐集、處理或利用個人資料

□預定蒐集、處理、利用

特定目的_____

期間_____

地區_____

對象_____

利用方式_____

其他事項_____

□詳計畫、需求書或建議書徵求文件。

□機關保留指示之事項

□其他指示:

廠商認為機關之指示有違反個資法、其他法律或其法規命令者，應立即通知機關。

第 2 條　安全管理措施

廠商在執行業務所必須之範圍內，應依個資法第 27 條規定採行個資法施行細則第 12 條所規定之安全管理措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

前項安全管理措施應包含下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：

(1)配置管理之人員及相當資源。

(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(含備援機制)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)使用紀錄、軌跡資料及證據保存。

(11)個人資料安全維護之整體持續改善。

(12)其他機關書面指示業務執行應注意事項。

第 3 條　□雙方約定複委託予第三人執行時(含資料上傳雲端平台)，廠商義務

廠商執行本契約，就涉及蒐集、處理或利用個人資料或檔案之業務擬複委託予第三人執行者，應事先取得機關書面同意。廠商於取得機關書面同意前，應先提供該第三人之名稱、聯絡資料、保密同意書及說明複委託執行業務之範圍或事項，與該第三人具備執行、配合本契約約定之能力之相關書面資料或該第三人出具之聲明書。

廠商應依第 1 條規定限定受複委託第三人蒐集、處理、利用個人資料之範圍，並對該受複委託第三人依個資法及經濟部及所屬機關個人資料保護管理要點等相關規定進行適當之監督。受複委託第三人於委託範圍內蒐集、處理、利用個人資料之行為，視同廠商行為，廠商應負所有責任。

廠商與該第三人之間應以契約約定，該第三人應在受複委託之範圍內負擔與廠商相同之本契約下之廠商義務與責任，機關並得直接對該第三人進行查核或要求改正。

廠商並應確保該第三人，於受託執行業務期間屆滿或經機關要求時，將因履行複委託業務而取得之個人資料及檔案全數返還予廠商或機關，其備份應全數銷毀刪除，不得以任何形式自行留存、保留存取權限或提供予其他第三人利用；並提供該第三人刪除、銷毀或返還個人資料之時間、方式、地點等紀錄或證明。

廠商如需將個人資料儲存或備份於第三人之雲端平台，亦為本契約所約定之複委託，除依前 4 項之約定辦理外，廠商於取得機關書面同意前，除第 1 項文件外，應另提供評估個人資料之敏感性、儲存或備份於雲端平台之必要性、雲端平台服務之安全性、雲端平台服務業者是否可以配合刪除個人資料等事項之書面報告。

廠商委由雲端平台服務業者提供雲端平台以履行契約時，機關得指示廠商另行與該雲端平台服務業者約定安全維護措施，例如資料備援機制等。

□廠商執行本契約，就涉及蒐集、處理或利用個人資料或檔案之業務，不得複委託第三人執行。

第 4 條　當事人權利行使時之義務

機關若受理當事人依個資法第 3 條規定行使當事人權利時，廠商應於機關指定期限內，配合提供必要資料或說明；當事人若逕向廠商及其受託人行使個資法第 3 條所定權利者，廠商及其受託人應依相關規定予以答覆，於有疑義時應通知機關協助處理，並留存所有紀錄以供機關查核。

第 5 條　配合義務

廠商依個資法第 15 條第 2 款或第 16 條但書第 7 款規定，經當事人同意而為蒐集或特定目的外利用時，就該同意內容與取得方式應事先送交機關審查。廠商依個資法第 6 條第 1 項第 6 款規定，經當事人書面同意而為蒐集、處理及利用者，亦同。

機關於本契約期間內，得要求廠商提供或說明涉及個人資料業務之處理流程相關資料(包括但不限於所蒐集之個人資料檔案、個人資料檔案保有之依據及特定目的、個人資料之類別等相關資訊及其蒐集、處理、利用等相關資料)，廠商不

得拒絕。

□廠商應於簽約後 1 個月內參考機關個人資料保護相關規範，訂定「個人資料保護專案計畫書」送機關備查，計畫書中應包含個資法令及機關要求之安全維護事項，如資料安全、設備安全及人員安全管理、訓練宣導、事故預防及通報應變機制、內部稽核等內容。若有變更計畫內容，應函送機關備查。

第 6 條　緊急事故通知義務

廠商有因執行本契約，致個人資料被竊取、洩漏、竄改或其他侵害之情形時，於發現後，應立即通知機關並採取因應措施，以避免或降低損害範圍；廠商於查明後應將其違反情形、涉及個資範圍、採行及預定採行之補救措施，經機關同意後，依法以適當方式通知當事人。

第 7 條　定期確認

機關得針對廠商的個人資料安全管理措施實施情形進行確認，並將確認結果記錄之；必要時，得派員進行實地訪查或委託專業人員進行查核，廠商應予配合。

機關於訪查或查核後，認有缺失，得以書面敘明理由請廠商限期改善。

第 8 條　損害賠償責任

廠商違反本契約第 1 條至第 6 條、第 7 條第 1 項或第 9 條，或機關依第 7 條第 2 項提出限期改善建議，廠商未依期限改善時，機關得依情節輕重為以下的處理;若機關受有損害，並得請求損害賠償：

一、以書面通知廠商終止或解除契約之部分或全部。

二、要求減少部分或全部價金。

三、按契約總價的千分之_____，計收懲罰性違約金。

廠商因執行本契約業務而違反個資法、個資法施行細則等規定，致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。機關如因廠商執行本契約而違反個資法、個資法施行細則，而遭受損害時，得向廠商請求損害賠償。若因此遭第三人請求損害賠償時，應由廠商負責處理並

承擔一切法律責任(如於訴訟中，廠商應協助機關為必要之答辯及提供相關資料，並應負擔因此所生之訴訟費用、律師費用及其他相關費用，並負責清償機關因此對第三人所負之損害賠償責任)。

第 9 條　履約中或契約終止時資料的刪除或返還

除機關、廠商雙方另有約定或法律另有規定外，廠商應於受託執行業務期間屆滿或經機關要求時，將因履行受託業務而取得之個人資料及檔案全數返還予機關，其備份應全數銷毀刪除，不得以任何形式自行留存、保留存取權限或提供予第三人利用；並提供刪除、銷毀或返還個人資料之時間、方式、地點等紀錄。

前項返還，廠商得以交付機關指定之第三人為之。

第 1 項刪除、銷毀作業，機關於必要時，得實地查訪，廠商應予配合。

範例二十：契約個人資料保護條款(套用契約版)

廠商依本契約受機關委託蒐集、處理或利用個人資料及檔案（指自然人之姓名、身分證統一編號、職業、聯絡方式、社會活動、其他得以直接或間接方式識別該個人之資料等個人資料保護法(以下簡稱個資法)所指個人資料）時，廠商應遵守下列約定：

(一) 蒐集、處理或利用時之義務

1. 廠商基於本契約蒐集、處理或利用個人資料時，應符合個資法第 15 條或第 16 條要件、經濟部及所屬機關個人資料保護管理要點等相關規定。
2. 廠商基於本契約蒐集、處理或利用特種個人資料時，應遵守個資法及經濟部及所屬機關個人資料保護管理要點等相關規定，並檢附符合個資法第6條第1項但書各款任一要件之說明。
3. 廠商不得利用機關所提供或因執行本契約所蒐集之個人資料及檔案，為自己或他人利益從事本契約委託範圍以外之處理或利用行為，包括但不限於行銷或商業推銷等相關活動、連結比對廠商本身保有資料進行處理利用，或以任何方式或方法交付予履約無關之第三人。
4. 廠商僅得於機關以下指示之範圍內，蒐集、處理或利用個人資料

   □預定蒐集、處理、利用

   特定目的_____

   期間_____

   地區_____

   對象_____

   利用方式_____

   其他事項_____

   □詳計畫、需求書或建議書徵求文件。

   □機關保留指示之事項

   □其他指示：
5. 廠商認為機關之指示有違反個資法、其他法律或其法規命令者，應立即通知機關。

(二) 安全管理措施

1. 廠商在執行業務所必須之範圍內，應依個資法第 27 條規定採行個資法施行細則第 12 條所規定之安全管理措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。
2. 前目安全管理措施應包含下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：
   (1)配置管理之人員及相當資源。
   (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(含備援機制)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)使用紀錄、軌跡資料及證據保存。
   (11)個人資料安全維護之整體持續改善。
   (12)其他機關書面指示業務執行應注意事項。

(三)□雙方約定複委託予第三人執行時(含資料上傳雲端平台)，廠商義務

1. 廠商執行本契約，就涉及蒐集、處理或利用個人資料或檔案之業務擬複委託予第三人執行者，應事先取得機關書面同意。廠商於取得機關書面同意前，應先提供該第三人之名稱、聯絡資料、保密同意書及說明複委託執行業務之範圍或事項與該第三人具備執行、配合本條約定之能力之相關書面資料或該第三人出具之聲明書。
2. 廠商應依第 1 款規定限定受複委託第三人蒐集、處理、利用個人資料之範圍，並對該受複委託第三人依個資法及經濟部及所屬機關個人資料保護管理要點等相關規定進行適當之監督。受複委託第三人於委託範圍內蒐集、處理、利用個人資料之行為，視同廠商行為，廠商應負所有責任。
3. 廠商與該第三人之間應以契約約定，該第三人應在受複委託之範圍內負擔與廠商相同之本契約下之廠商義務與責任，機關並得直接對該第三人進行查核或要求改正。
4. 廠商並應確保該第三人，於受託執行業務期間屆滿或經機關要

求時,將因履行複委託業務而取得之個人資料及檔案全數返還予廠商或機關，其備份應全數銷毀刪除，不得以任何形式自行留存、保留存取權限或提供予其他第三人利用；並提供該第三人刪除、銷毀或返還個人資料之時間、方式、地點等紀錄或證明。

5. 廠商如需將個人資料儲存或備份於第三人之雲端平台,亦為本契約所約定之複委託,除依前 4 目之約定辦理外,廠商於取得機關書面同意前,除第 1 目文件外,應另提供評估個人資料之敏感性、儲存或備份於雲端平台之必要性、雲端平台服務之安全性、雲端平台服務業者是否可以配合刪除個人資料等事項之書面報告。
6. 廠商委由雲端平台服務業者提供雲端平台以履行契約時,機關得指示廠商另行與該雲端平台服務業者約定安全維護措施,例如資料備援機制等。

□廠商執行本契約，就涉及蒐集、處理或利用個人資料或檔案之業務，不得複委託第三人執行。

（四） 當事人權利行使時之義務

機關若受理當事人依個資法第 3 條規定行使當事人權利時，廠商應於機關指定期限內，配合提供必要資料或說明；當事人若逕向廠商及其受託人行使個資法第 3 條所定權利者，廠商及其受託人應依相關規定予以答覆，於有疑義時應通知機關協助處理，並留存所有紀錄以供機關查核。

（五） 配合義務

1. 廠商依個資法第 15 條第 2 款或第 16 條但書第 7 款規定,經當事人同意而為蒐集或特定目的外利用時,就該同意內容與取得方式應事先送交機關審查。廠商依個資法第 6 條第 1 項第 6 款規定，經當事人書面同意而為蒐集、處理及利用者，亦同。
2. 機關於本契約期間內,得要求廠商提供或說明涉及個人資料業務之處理流程相關資料(包括但不限於所蒐集之個人資料檔案、個人資料檔案保有之依據及特定目的、個人資料之類別等相關資訊及其蒐集、處理、利用等相關資料),廠商不得拒絕。

□3. 廠商應於簽約後 1 個月內參考機關個人資料保護相關規範,訂定「個人資料保護專案計畫書」送機關備查，計畫書中應包含

個資法令及機關要求之安全維護事項，如資料安全、設備安全及人員安全管理、訓練宣導、事故預防及通報應變機制、內部稽核等內容。若有變更計畫內容，應函送機關備查。

（六） 緊急事故通知義務

廠商有因執行本契約，致個人資料被竊取、洩漏、竄改或其他侵害之情形時，於發現後，應立即通知機關並採取因應措施，以避免或降低損害範圍；廠商於查明後應將其違反情形、涉及個資範圍、採行及預定採行之補救措施，經機關同意後，依法以適當方式通知當事人。

（七） 定期確認

1. 機關得針對廠商的個人資料安全管理措施實施情形進行確認，並將確認結果記錄之；必要時，得派員進行實地訪查或委託專業人員進行查核，廠商應予配合。
2. 機關於訪查或查核後，認有缺失，得以書面敘明理由請廠商限期改善。

（八） 損害賠償責任

1. 廠商違反本條第 1 款至第 6 款、第 7 款第 1 目或第 9 款，或機關依第 7 款第 2 目提出限期改善建議，廠商未依期限改善時，機關得依情節輕重為以下的處理；若機關受有損害，並得請求損害賠償：
   (1)以書面通知廠商終止或解除契約之部分或全部。
   (2)要求減少部分或全部價金。
   (3)按契約總價的千分之□，計收懲罰性違約金。
2. 廠商因執行本契約業務而違反個資法、個資法施行細則等規定，致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。
3. 機關如因廠商執行本契約而違反個資法、個資法施行細則，而遭受損害時，得向廠商請求損害賠償。若因此遭第三人請求損害賠償時，應由廠商負責處理並承擔一切法律責任（如於訴訟中，廠商應協助機關為必要之答辯及提供相關資料，並應負擔因此所生之訴訟費用、律師費用及其他相關費用，並負責清償機關因此對第三人所負之損害賠償責任）。

（九） 履約中或契約終止時資料之刪除或返還

1. 除機關、廠商雙方另有約定或法律另有規定外，廠商應於受託執行業務期間屆滿或經機關要求時，將因履行受託業務而取得之個人資料及檔案全數返還予機關，其備份應全數銷毀刪除，不得以任何形式自行留存、保留存取權限或提供予第三人利用；並提供刪除、銷毀或返還個人資料之時間、方式、地點等紀錄。
2. 前目返還，廠商得以交付機關指定之第三人為之。
3. 第 1 目刪除、銷毀作業，機關於必要時，得實地查訪，廠商應予配合。

範例二十一：委外廠商查核項目

個人資料委外作業查核檢查表

填表說明：

一、查核結果欄：依查核實際狀況，參考相關佐證資料填具查核結果。

（一） 符合：實際作業已依查核內容制定相關規範，並已有相關實作紀錄，或已建立標準規範而尚未有實際作業。

（二） 不符合：完全未依查核內容要求制定相關程序，或完全未依相關程序執行並產生實作紀錄。

（三） 不適用：實際作業排除查核內容之適用。

二、說明欄位：應記錄查核之參考佐證資料，或簡述實際作業狀況。

查核項目	查核內容	查核結果	說明
1.人員及資源配置	1.1 是否已配置專責人員或組織管理及維護保有之個人資料？	□符合□不符合□不適用	
	1.2 配置適當資源？	□符合□不符合□不適用	
2.界定個人資料	2.1 是否定義個人資料並建立盤點清冊？	□符合□不符合□不適用	
	2.2 個人資料是否包含特種個資？若有，是否詳述其法令依據及蒐集內容？	□符合□不符合□不適用	若未蒐集特種個資則填不適用
	2.3 個資盤點是否確實？	□符合□不符合□不適用	
3.風險評估	3.1 進行風險評估？	□符合□不符合□不適用	
	3.2 製成風險評鑑表？	□符合□不符合□不適用	
	3.3 針對風險進行因應？	□符合□不符合□不適用	
4.事故通報應變	4.1 有通報及應變程序？	□符合□不符合□不適用	

	4.2 事故發生時確實通報？	□符合□不符合□不適用	當年度無事故者，4.2-4.6 應填不適用
	4.3 事故發生後採取應變措施？	□符合□不符合□不適用	
	4.4 於期限內通知當事人？	□符合□不符合□不適用	
	4.5 事後採取預防措施？	□符合□不符合□不適用	
	4.6 將事故處理情形通知機關？	□符合□不符合□不適用	
5.蒐集處理利用之內部管理程序	5.1 資料蒐集、處理具備特定目的並具有法定要件？	□符合□不符合□不適用	
	5.2 依規定取得當事人同意（當事人同意之情形）？	□符合□不符合□不適用	
	5.3 是否清楚直接或間接蒐集個人資料之適法性，如履行告知義務及時點（未履行告知義務時，是否符合免告知之情形）？	□符合□不符合□不適用	
	5.4 告知內容是否包含個資法第八條規定項目？	□符合□不符合□不適用	若符合個資法第八條第二項或第九條免告知則填不適用
	5.5 個人資料之利用，符合特定目的之範圍？	□符合□不符合□不適用	
	5.6 是否已訂定個人資料蒐集、處理及利用目的消失或屆滿之資料銷毀、刪除程序？	□符合□不符合□不適用	

	5.7 是否有定期檢核及記錄以確認特定目的外之利用？	□符合□不符合 □不適用	
	5.8 目的外利用是否符合法定要件？	□符合□不符合 □不適用	
	5.9 是否利用因執行本契約所蒐集之個人資料進行行銷？	□符合□不符合 □不適用	
	5.10 是否提供個人資料予第三人？	□符合□不符合 □不適用	
	5.11 是否有進行複委託，進行前是否得機關同意並經複委託廠商簽訂保密協議？	□符合□不符合 □不適用	無複委託應填不適用
	5.12 是否定期對複委託方進行監督並記錄？	□符合□不符合 □不適用	無複委託應填不適用
	5.13 當事人權利行使流程？	□符合□不符合 □不適用	
	5.14 將當事人權利行使回覆情形做成紀錄供機關備查？	□符合□不符合 □不適用	
	5.15 是否清楚瞭解個人資料之使用及其保存期限？	□符合□不符合 □不適用	
	5.16 契約終止或解除，是否刪除、銷毀所持有之個人資料？	□符合□不符合 □不適用	
	5.17 契約終止或解除，是否返還個人資料之載體？	□符合□不符合 □不適用	
	5.18 員工離職時，是否依規定繳回其使用或保管之資訊資產(如個人電腦、隨身	□符合□不符合 □不適用	

	碟)?		
	5.19 新承接人員是否有變更各系統密碼?	□符合□不符合 □不適用	
6.資料安全與人員管理	6.1 是否進行去識別化作業?	□符合□不符合 □不適用	
	6.2 是否有資料存取控制措施?	□符合□不符合 □不適用	
	6.3 是否進行加密?	□符合□不符合 □不適用	
	6.4 資料之傳送是否進行管控?	□符合□不符合 □不適用	
	6.5 使用資訊系統或其他系統進行個人資料交換時,是否有採取適當保護措施(如傳輸過程中進行加密)?	□符合□不符合 □不適用	
	6.6 是否有遠端存取控管措施(如限制遠端存取個人資料、傳輸過程加密)?	□符合□不符合 □不適用	如無開放遠端存取應填不適用
	6.7 保有資料者是否遵守保密協定?	□符合□不符合 □不適用	
	6.8 人員進出情形是否具體掌控?	□符合□不符合 □不適用	
7.認知宣導與教育訓練	7.1 是否確實進行認知宣導與教育訓練?	□符合□不符合 □不適用	
	7.2 是否進行課後評量?	□符合□不符合 □不適用	
	7.3 是否對新進人員進行教育訓練?	□符合□不符合 □不適用	
8.設備安全管理	8.1 是否對設備及環境進行控管與保護?	□符合□不符合 □不適用	
	8.2 是否定期檢查或	□符合□不符合	

	維護更新設備？	□不適用	
	8.3 是否針對存放個人資料之媒體於報廢或再利用前進行處理(如硬碟消磁)？	□符合□不符合□不適用	
9.稽核機制	9.1 是否設有稽核制度？	□符合□不符合□不適用	
	9.2 是否定期實施稽核？	□符合□不符合□不適用	
10.紀錄保存	10.1 是否保存個資(含紙本及數位檔案)管理紀錄(如存取及利用紀錄、調閱紀錄、軌跡資料、銷毀紀錄)？	□符合□不符合□不適用	
	10.2 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？	□符合□不符合□不適用	
11.持續改善	11.1 是否定期檢視個資保護措施？	□符合□不符合□不適用	
	11.2 是否針對缺失進行改善？	□符合□不符合□不適用	
	11.3 是否依機關所提出之建議進行改善？	□符合□不符合□不適用	

資訊系統委外開發廠商增列查核項目

查核項目	查核內容	查核結果	說明
1.安全系統設計原則	1.1 是否已制訂系統發展生命週期的安全設計原則，並實作於資訊系統？	□符合□不符合 □不適用	
	1.2 應用程式編碼時，是否已參考 OWASP 組織每年公告之撰寫程式的安全原則(Secure Coding Principles)或行政院國家資通安全會報技術服務中心之技術公告，以提升編碼之安全性？	□符合□不符合 □不適用	
	1.3 網頁應用程式編碼時，是否已參考 OWASP 組織每年公告之安全風險議題，避免撰寫不當產生風險？ 如：跨網站的指令碼(Cross Site Scripting)、注入缺失(Injection Flaw)、惡意檔案執行(Malicious File Execution)、不安全的物件參考(Insecure Direct Object Reference)及跨網站的偽造要求(Cross-Site Request Forgery)等不安全源碼之問題。	□符合□不符合 □不適用	
2.安全開發環境	2.1 系統開發環境是否有適當的保護？	□符合□不符合 □不適用	
	2.2 系統開發所使用的輔助工具軟體安全性是否進行評估？	□符合□不符合 □不適用	

	2.3 系統開發所使用之電腦是否定期執行各項漏洞修補程式或安全性更新？	□符合□不符合 □不適用	
	2.4 系統開發所使用之電腦是否全面使用防毒軟體並即時更新病毒碼？	□符合□不符合 □不適用	
3.測試資料的保護	3.1 測試作業是否避免以真實資料進行？	□符合□不符合 □不適用	
	3.2 如須使用真實資料進行測試是否有進行實體隔離或存取權限管制？	□符合□不符合 □不適用	

範例二十二：委外廠商自我查核項目

個人資料委外廠商自我查核檢查表

填表說明：

一、 查核結果欄：由委外廠商依查核實際狀況，參考相關佐證資料填具查核結果。

（一） 符合：實際作業已依查核內容制定相關規範，並已有相關實作紀錄，或已建立標準規範而尚未有實際作業。

（二） 不符合：完全未依查核內容要求制定相關程序，或完全未依相關程序執行並產生實作紀錄。

（三） 不適用：實際作業排除查核內容之適用。

二、 說明欄位：應記錄查核之參考佐證資料，或簡述實際作業狀況。

查核項目	查核結果	說明(請填寫檢核結果或抽核發現)	備註
1. 已識別出受委託個人資料蒐集、處理或利用個人資料之範圍、類別、特定目的及期間	□符合 □不符合 □不適用		如：於契約敘明委託範圍內涵蓋之個人資料範圍、類別、特定目的及期間
2. 已針對受委託之個人資料檔案配置管理人員及相當資源	□符合 □不符合 □不適用		如：檢視受委託範圍內是否有指派專人管理個資安全並投入足以維護安全措施之相當資源(如：人、設備等)
3. 已將受委託之個人資料檔案進行適當盤點並完成風險評鑑與處理作業	□符合 □不符合 □不適用		如：是否進行個資盤點及風險評鑑作業，並根據風險評鑑結果調整安全維護措施強度

4.已針對受委託之個人資料檔案規劃個人資料事故通報機制 (包含違反個資法、其他個人資料保護法律或法規命令時，已規劃向委託機關通知及採行之補救措施)	□符合 □不符合 □不適用		如：是否建立整體個資事故通報機制(需包含溝通管道、應變處理原則)、是否將相關通報機制納入契約條款
5.已將受委託之個人資料檔案規劃蒐集、處理及利用程序	□符合 □不符合 □不適用		如：是否建立涵蓋全組織個人資料檔案蒐集、處理及利用程序
6.已針對涉及受委託之個人資料人員施以宣導及教育訓練	□符合 □不符合 □不適用		如：針對涉及個人資料之人員進行宣導及教育訓練
7.已針對受委託之個人資料檔案落實安全管控措施	□符合 □不符合 □不適用		如：針對處理、儲存個人資料之設備進行網路或實體限制措施；依資料敏感程度規劃資料儲存加密、上鎖等措施
8.已將受委託之個人資料檔案納入日常或定期稽核的範圍中	□符合 □不符合 □不適用		如：定期或不定期進行稽核並將稽核發現進行矯正預防措施
9.已瞭解委託機關保留指示事項，並配合指示事項辦理相關活動	□符合 □不符合 □不適用		如：1.事先約定受託範圍內之資訊設備使用及管控， 如：禁止USB使用等 2.事先約定資料傳輸、儲存需進行加密

10.已規劃當委託關係終止或解除時，將保存之個人資料或載體返還委託機關或刪除、銷毀之管理機制	□符合 □不符合 □不適用		如：以紙本或其他載體交遞資料，應具備簽收確認機制(具名)，並確認是否轉做其他使用及儲存於載體保存之資料是否如實刪除如：內部電腦、資訊設備之共用資料夾及其他資訊出口(如網際網路、Email寄件備份等)，應一併檢查
11.進行複委託時已將委託機關有關個資保護要求納入複委託契約之內容	□符合 □不符合 □不適用		如：是否允許複委託應納入契約規範；受託廠商及複委託廠商均應有適當個資安全維護措施及保密協議，並對複委託方進行監督

範例二十三：稽核項目

個人資料安全稽核檢查表

填表說明：

一、 稽核結果欄：依稽核實際狀況，參考相關佐證資料填具查核結果。

（一） 符合：實際作業已依稽核內容訂定相關規範，並已有相關實作紀錄，或已建立標準規範而尚未有實際作業。

（二） 不符合：完全未依稽核內容要求訂定相關程序，或完全未依相關程序執行並產生實作紀錄。

（三） 不適用：實際作業排除稽核內容之適用。

二、 說明欄位：應記錄稽核之參考佐證資料或簡述實際作業狀況。

稽核項目	稽核內容(得視情形增刪)	稽核結果	說明
1.人員及資源配置	1.1 是否已配置專責人員或組織管理及維護保有之個人資料？	□符合□不符合□不適用	
	1.2 配置適當資源?	□符合□不符合□不適用	
2.蒐集、處理、利用作業	2.1 資料蒐集、處理是否具備特定目的並具有法定要件？	□符合□不符合□不適用	
	2.2 蒐集程序是否依規定奉簽核後為之？	□符合□不符合□不適用	
	2.3 是否依規定取得當事人同意（當事人同意之情形）？	□符合□不符合□不適用	
	2.4 是否履行告知義務（未履行告知義務時，是否符合免告知之情形）？	□符合□不符合□不適用	
	2.5 是否依規定簽奉核定後補充、更正個人資料？	□符合□不符合□不適用	
	2.6 是否依規定簽奉核定後刪除、銷毀個人資料？	□符合□不符合□不適用	
	2.7 個人資料之利用，是否符合特定目的之範圍？	□符合□不符合□不適用	

	2.8 是否有目的外之利用？	□符合□不符合 □不適用	
	2.9 目的外利用是否符合法定要件？	□符合□不符合 □不適用	
	2.10 是否依規定簽奉核定後停止處理、利用個人資料？	□符合□不符合 □不適用	
3.當事人權利行使程序	3.1 是否依設置當事人權利行使處理流程？	□符合□不符合 □不適用	
	3.2 受理當事人權利行使時，是否有為確認身分之動作？	□符合□不符合 □不適用	
	3.3 非當事人本人申請時，代理人是否出具相關證明文件？	□符合□不符合 □不適用	
	3.4 受理申請後，是否依規定進行簽核？	□符合□不符合 □不適用	
	3.5 延長回覆期間時，是否將原因以書面通知當事人？	□符合□不符合 □不適用	
	3.6 駁回當事人申請時，是否具備法定要件？	□符合□不符合 □不適用	
	3.7 駁回當事人申請時，是否以書面將拒絕事由告知當事人？	□符合□不符合 □不適用	
4.盤點與風險分析	4.1 是否進行個資盤點？	□符合□不符合 □不適用	
	4.2 個資盤點是否確實？	□符合□不符合 □不適用	
	4.3 是否建立盤點清冊？	□符合□不符合 □不適用	
	4.4 是否依個資法第 17 條規定將資訊公開？	□符合□不符合 □不適用	
	4.5 是否進行風險評估？	□符合□不符合 □不適用	

	4.6 是否製成風險評鑑表？	□符合□不符合 □不適用	
	4.7 是否針對風險進行因應？	□符合□不符合 □不適用	
5.事故通報與應變程序	5.1 是否有通報及應變程序？	□符合□不符合 □不適用	
	5.2 事故發生時是否確實通報？	□符合□不符合 □不適用	當年度無事故者， 5.2-5.6 應填不適用
	5.3 是否採取應變措施？	□符合□不符合 □不適用	
	5.4 是否於適當期間內通知當事人？	□符合□不符合 □不適用	
	5.5 事後是否採取預防措施？	□符合□不符合 □不適用	
	5.6 是否作成事故報告書，並送本部執行小組備查？	□符合□不符合 □不適用	
	5.7 接獲非公務機關通報或副知，或非因通報或副知而自行知悉個資外洩案件，是否於接獲通報、副知或知悉時起 72 小時內，填列監督通報紀錄表，通報國發會？	□符合□不符合 □不適用	請檢附通報紀錄表。 非為負責該項業務者應填不適用。
6.認知宣導與教育訓練	6.1 是否確實進行認知宣導與教育訓練？	□符合□不符合 □不適用	
	6.2 是否進行課後評量？	□符合□不符合 □不適用	
	6.3 是否對新進人員進行教育訓練？	□符合□不符合 □不適用	
7.資料安全、人員管理及設備安全	7.1 是否進行去識別化作業？	□符合□不符合 □不適用	
	7.2 是否有資料存取控制	□符合□不符合	

	措施？	□不適用	
	7.3 是否進行加密？	□符合□不符合 □不適用	
	7.4 資料之傳送是否進行管控？	□符合□不符合 □不適用	
	7.5 保有資料者是否遵守保密協定？	□符合□不符合 □不適用	
	7.6 人員進出情形是否具體掌控？	□符合□不符合 □不適用	
	7.7 是否對設備及環境進行控管與保護？	□符合□不符合 □不適用	
	7.8 是否定期檢查或維護更新設備？	□符合□不符合 □不適用	
	7.9 是否以適當方式（如：碎紙機銷毀、焚毀、水銷等）銷毀紙本個人資料，並視需要留存適當之銷毀紀錄？是否使用可達成適當碎紙效果(無法再拼湊或用肉眼辨識內容)之碎紙機進行個人資料之銷毀？	□符合□不符合 □不適用	
	7.10 是否以適當方式（如：低階格式化、軟體複寫、消磁或物理破壞等）銷毀存有個人資料之儲存媒體，並視需要留存適當之銷毀紀錄？	□符合□不符合 □不適用	
	7.11 使用、處理個人資料檔案之系統帳號，是否經申請並由權責主管核可？權限賦予是否符合業務須知（Need-to-Know）與執行工作所需合理權限原則？	□符合□不符合 □不適用	

	7.12 是否針對機關(單位)同仁及外部人員(如：合作機關(構)、廠商、工讀生等）配賦唯一的使用者識別碼並具備合適的身分鑑別措施？是否建立適當之複核機制？	□符合□不符合□不適用	
	7.13 人員離職或職務異動時，是否由原屬權責主管審查存取授權之異動？	□符合□不符合□不適用	
	7.14 如將個人資料檔案置於公用電腦或網路共用資料夾，是否進行加密或遮蔽？	□符合□不符合□不適用	
	7.15 以電子郵件傳送敏感級以上個資檔案時，是否採加密機制，並確認加密機制之有效性？	□符合□不符合□不適用	
	7.16 存放個人資料檔案之電腦是否定期執行各項漏洞修補程式或安全性更新？	□符合□不符合□不適用	
	7.17 存放個人資料檔案之電腦是否全面使用防毒軟體並即時更新病毒碼？	□符合□不符合□不適用	
	7.18 存放個人資料檔案之電腦設備委外維修或報廢時，是否事先移除個人資料？	□符合□不符合□不適用	
	7.19 存放個人資料檔案之電腦設備攜出或借出時，是否經權責主管授權核准？	□符合□不符合□不適用	
8.個人資料使用紀錄、軌跡	8.1 是否對保存之個資進行紀錄(如存取及利用紀	□符合□不符合□不適用	

資料及相關證據應妥善保管、定期覆核	錄、調閱紀錄、軌跡資料)、證據之管理措施？		
	8.2 是否定有保管期限？	□符合□不符合□不適用	
	8.3 延長保管期限時，是否依照規定？	□符合□不符合□不適用	
	8.4 是否依保管期限確實刪除或銷毀？	□符合□不符合□不適用	
	8.5 因業務需求經權責主管授權執行個人資料之處理行為，是否留存包括使用者身分與其行為內容等之使用紀錄或軌跡資料以供事後查核或舉證？	□符合□不符合□不適用	
	8.6 權責主管或管理人員，是否定期審查相關使用紀錄或軌跡資料？	□符合□不符合□不適用	
9.委外作業	9.1 是否有委外蒐集、處理或利用個人資料之情形並簽訂書面契約？	□符合□不符合□不適用	當年度無委外作業者，9.1-9.5 應填不適用
	9.2 是否將受託者之個人資料安全維護措施列入評選項目？	□符合□不符合□不適用	
	9.3 是否定期確認受託者執行狀況，並作成紀錄？	□符合□不符合□不適用	
	9.4 提出限期改善時，是否持續追蹤改善情形？	□符合□不符合□不適用	
	9.5 契約終止或解除時，是否要求受託者確實刪除、銷毀或返還？	□符合□不符合□不適用	
10.資料安全稽核機制	10.1 是否訂定定期檢視各項個資保護措施之資料安全稽核作業機制？	□符合□不符合□不適用	
	10.2 稽核作業結束後，是	□符合□不符合	

	否將稽核結果製作報告備查？	□不適用	
	10.3 是否針對稽核結果進行後續改正作業，並保留矯正作業執行紀錄？	□符合□不符合□不適用	
11.缺失改善與矯正預防作業	11.1 是否訂定矯正及預防程序，於各類查核發現不符合、觀察或建議事項時，進行根因分析，並採取適當之矯正及預防措施？	□符合□不符合□不適用	
	11.2 是否對各類查核發現之不符合事項之矯正與預防措施訂定合理之執行期限且追蹤執行結果，並有相關紀錄備查？	□符合□不符合□不適用	
	11.3 針對各類查核發現之不符合事項矯正措施，是否於執行期限內完成？是否持續追蹤至改善完成？	□符合□不符合□不適用	
12.對非公務機關個人資料保護之監管	12.1 是否定期檢討依個資法第27條第3項訂定相關辦法之必要性？	□符合□不符合□不適用	請說明依聯繫作業要點第5點所列情形綜合考量之檢討結果。 已訂定相關辦法或無監管非公務機關者，應填不適用。
	12.2 已訂定相關辦法者，就該辦法所規定之事項，是否完整？	□符合□不符合□不適用	請說明是否依聯繫作業要點訂定。

			未訂定相關辦法者，應填不適用。
	12.3 是否檢視個資法第22條第1項規定之情形，採取行政檢查？	□符合□不符合□不適用	請說明檢視之結果。 無監管非公務機關者，應填不適用。
	12.4 採取行政檢查時，是否符合個資法第 22 條至第 24 條之規定？	□符合□不符合□不適用	請檢附實施檢查之紀錄。 未採取行政檢查者，應填不適用。
	12.5 非公務機關有違反個資法規定之情事者，進行處分時是否符合個資法第 25 條之規定？	□符合□不符合□不適用	請檢附處分書。 未採取處分者，應填不適用。
	12.6 公布非公務機關之違法情形及其姓名或名稱與負責人時，是否妥善考量相關因素？	□符合□不符合□不適用	請說明公布之方式並檢附公布內容。 未公布者，應填不適用。

二、個人資料保護法

1. 中華民國八十四年八月十一日總統（84）華總（一）義字第 5960 號令制定公布全文 45 條
2. 中華民國九十九年五月二十六日總統華總一義字第 09900125121 號令修正公布名稱及全文 56 條；施行日期，由行政院定之，但現行條文第 19～22、43 條之刪除，自公布日施行（原名稱：電腦處理個人資料保護法）
   中華民國一百零一年九月二十一日行政院院臺法字第 1010056845 號令發布除第 6、54 條條文外，其餘條文定自一百零一年十月一日施行
3. 中華民國一百零四年十二月三十日總統華總一義字第 10400152861 號令修正公布第 6～8、11、15、16、19、20、41、45、53、54 條條文；施行日期，由行政院定之
   中華民國一百零五年二月二十五日行政院院臺法字第 1050154280 號令發布定自一百零五年三月十五日施行
   中華民國一百零八年一月十日法務部法律字第 10803500010 號、國家發展委員會發法字第 1080080004A 號會銜公告第 53 條、第 55 條所列屬「法務部」之權責事項，改由「國家發展委員會」管轄

第一章總則

第一條　為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。

第二條　本法用詞，定義如下：

一、個人資料：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。

二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

三、蒐集：指以任何方式取得個人資料。

四、處理：指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。

五、利用：指將蒐集之個人資料為處理以外之使用。

六、國際傳輸：指將個人資料作跨國（境）之處理或利用。

七、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。

八、非公務機關：指前款以外之自然人、法人或其他團體。

九、當事人：指個人資料之本人。

第三條　當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：
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。

第四條　受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。

第五條　個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

第六條　有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：
一、法律明文規定。
二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
三、當事人自行公開或其他已合法公開之個人資料。
四、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，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。
依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一

項、第二項及第四項規定，並以書面為之。

第七條　第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。

第十六條第七款、第二十條第一項第六款所稱同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。

公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意。

蒐集者就本法所稱經當事人同意之事實，應負舉證責任。

第八條　公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

一、公務機關或非公務機關名稱。

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。

有下列情形之一者，得免為前項之告知：

一、依法律規定得免告知。

二、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。

三、告知將妨害公務機關執行法定職務。

四、告知將妨害公共利益。

五、當事人明知應告知之內容。

六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

第九條　公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人

告知個人資料來源及前條第一項第一款至第五款所列事項。

有下列情形之一者，得免為前項之告知：

一、有前條第二項所列各款情形之一。

二、當事人自行公開或其他已合法公開之個人資料。

三、不能向當事人或其法定代理人為告知。

四、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。

五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

第一項之告知，得於首次對當事人為利用時併同為之。

第十條　公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：

一、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。

二、妨害公務機關執行法定職務。

三、妨害該蒐集機關或第三人之重大利益。

第十一條　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，或經當事人書面同意，並經註明其爭議者，不在此限。

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。

因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

第十二條　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。

第十三條　公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。
公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

第十四條　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。

第二章公務機關對個人資料之蒐集、處理及利用

第十五條　公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：
一、執行法定職務必要範圍內。
二、經當事人同意。
三、對當事人權益無侵害。

第十六條　公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：
一、法律明文規定。
二、為維護國家安全或增進公共利益所必要。
三、為免除當事人之生命、身體、自由或財產上之危險。
四、為防止他人權益之重大危害。
五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
六、有利於當事人權益。
七、經當事人同意。

第十七條　公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同：

一、個人資料檔案名稱。

二、保有機關名稱及聯絡方式。

三、個人資料檔案保有之依據及特定目的。

四、個人資料之類別。

第十八條　公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第三章非公務機關對個人資料之蒐集、處理及利用

第十九條　非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

一、法律明文規定。

二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

五、經當事人同意。

六、為增進公共利益所必要。

七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

八、對當事人權益無侵害。

蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

第二十條　非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：

一、法律明文規定。

二、為增進公共利益所必要。

三、為免除當事人之生命、身體、自由或財產上之危險。
四、為防止他人權益之重大危害。
五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
六、經當事人同意。
七、有利於當事人權益。
非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。
非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

第二十一條　非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：
一、涉及國家重大利益。
二、國際條約或協定有特別規定。
三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。
四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。

第二十二條　中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。
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。
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。
對於第一項及第二項之進入、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。

第二十三條　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。

第二十四條　非公務機關、物之所有人、持有人、保管人或利害關係人對前二條之要求、強制、扣留或複製行為不服者，得向中央目的事業主管機關或直轄市、縣（市）政府聲明異議。

前項聲明異議，中央目的事業主管機關或直轄市、縣（市）政府認為有理由者，應立即停止或變更其行為；認為無理由者，得繼續執行。經該聲明異議之人請求時，應將聲明異議之理由製作紀錄交付之。

對於中央目的事業主管機關或直轄市、縣（市）政府前項決定不服者，僅得於對該案件之實體決定聲明不服時一併聲明之。但第一項之人依法不得對該案件之實體決定聲明不服時，得單獨對第一項之行為逕行提起行政訴訟。

第二十五條　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：

一、禁止蒐集、處理或利用個人資料。

二、命令刪除經處理之個人資料檔案。

三、沒入或命銷毀違法蒐集之個人資料。

四、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。

第二十六條　中央目的事業主管機關或直轄市、縣（市）政府依第二十二條規定檢查後，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。

第二十七條　非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。
前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。

第四章損害賠償及團體訴訟

第二十八條　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。
被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。
依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。
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，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。
第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

第二十九條　非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。
依前項規定請求賠償者，適用前條第二項至第六項規定。

第三十條　損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，

亦同。

第三十一條　損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，非公務機關適用民法之規定。

第三十二條　依本章規定提起訴訟之財團法人或公益社團法人，應符合下列要件：

一、財團法人之登記財產總額達新臺幣一千萬元或社團法人之社員人數達一百人。

二、保護個人資料事項於其章程所定目的範圍內。

三、許可設立三年以上。

第三十三條　依本法規定對於公務機關提起損害賠償訴訟者，專屬該機關所在地之地方法院管轄。對於非公務機關提起者，專屬其主事務所、主營業所或住所地之地方法院管轄。

前項非公務機關為自然人，而其在中華民國現無住所或住所不明者，以其在中華民國之居所，視為其住所；無居所或居所不明者，以其在中華民國最後之住所，視為其住所；無最後住所者，專屬中央政府所在地之地方法院管轄。

第一項非公務機關為自然人以外之法人或其他團體，而其在中華民國現無主事務所、主營業所或主事務所、主營業所不明者，專屬中央政府所在地之地方法院管轄。

第三十四條　對於同一原因事實造成多數當事人權利受侵害之事件，財團法人或公益社團法人經受有損害之當事人二十人以上以書面授與訴訟實施權者，得以自己之名義，提起損害賠償訴訟。當事人得於言詞辯論終結前以書面撤回訴訟實施權之授與，並通知法院。

前項訴訟，法院得依聲請或依職權公告曉示其他因同一原因事實受有損害之當事人，得於一定期間內向前項起訴之財團法人或公益社團法人授與訴訟實施權，由該財團法人或公益社團法人於第一審言詞辯論終結前，擴張應受判決事項之聲明。

其他因同一原因事實受有損害之當事人未依前項規定授與訴訟實施權者，亦得於法院公告曉示之一定期間內起訴，

由法院併案審理。
其他因同一原因事實受有損害之當事人，亦得聲請法院為前項之公告。
前二項公告，應揭示於法院公告處、資訊網路及其他適當處所；法院認為必要時，並得命登載於公報或新聞紙，或用其他方法公告之，其費用由國庫墊付。
依第一項規定提起訴訟之財團法人或公益社團法人，其標的價額超過新臺幣六十萬元者，超過部分暫免徵裁判費。

第三十五條　當事人依前條第一項規定撤回訴訟實施權之授與者，該部分訴訟程序當然停止，該當事人應即聲明承受訴訟，法院亦得依職權命該當事人承受訴訟。
財團法人或公益社團法人依前條規定起訴後，因部分當事人撤回訴訟實施權之授與，致其餘部分不足二十人者，仍得就其餘部分繼續進行訴訟。

第三十六條　各當事人於第三十四條第一項及第二項之損害賠償請求權，其時效應分別計算。

第三十七條　財團法人或公益社團法人就當事人授與訴訟實施權之事件，有為一切訴訟行為之權。但當事人得限制其為捨棄、撤回或和解。
前項當事人中一人所為之限制，其效力不及於其他當事人。
第一項之限制，應於第三十四條第一項之文書內表明，或以書狀提出於法院。

第三十八條　當事人對於第三十四條訴訟之判決不服者，得於財團法人或公益社團法人上訴期間屆滿前，撤回訴訟實施權之授與，依法提起上訴。
財團法人或公益社團法人於收受判決書正本後，應即將其結果通知當事人，並應於七日內將是否提起上訴之意旨以書面通知當事人。

第三十九條　財團法人或公益社團法人應將第三十四條訴訟結果所得之賠償，扣除訴訟必要費用後，分別交付授與訴訟實施權之

當事人。
提起第三十四條第一項訴訟之財團法人或公益社團法人，均不得請求報酬。

第四十條　依本章規定提起訴訟之財團法人或公益社團法人，應委任律師代理訴訟。

第五章罰則

第四十一條　意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。

第四十二條　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。

第四十三條　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。

第四十四條　公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。

第四十五條　本章之罪，須告訴乃論。但犯第四十一條之罪者，或對公務機關犯第四十二條之罪者，不在此限。

第四十六條　犯本章之罪，其他法律有較重處罰規定者，從其規定。

第四十七條　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：
一、違反第六條第一項規定。
二、違反第十九條規定。
三、違反第二十條第一項規定。

四、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。

第四十八條　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：

一、違反第八條或第九條規定。

二、違反第十條、第十一條、第十二條或第十三條規定。

三、違反第二十條第二項或第三項規定。

四、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。

第四十九條　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。

第五十條　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。

第六章附則

第五十一條　有下列情形之一者，不適用本法規定：

一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。

二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。

公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。

第五十二條　第二十二條至第二十六條規定由中央目的事業主管機關或直轄市、縣（市）政府執行之權限，得委任所屬機關、委託其他機關或公益團體辦理；其成員因執行委任或委託事務所知悉之資訊，負保密義務。

前項之公益團體，不得依第三十四條第一項規定接受當事人授與訴訟實施權，以自己之名義提起損害賠償訴訟。

第五十三條　法務部應會同中央目的事業主管機關訂定特定目的及個人資料類別，提供公務機關及非公務機關參考使用。

第五十四條　本法中華民國九十九年五月二十六日修正公布之條文施行前，非由當事人提供之個人資料，於本法一百零四年十二月十五日修正之條文施行後為處理或利用者，應於處理或利用前，依第九條規定向當事人告知。

前項之告知，得於本法中華民國一百零四年十二月十五日修正之條文施行後首次利用時併同為之。

未依前二項規定告知而利用者，以違反第九條規定論處。

第五十五條　本法施行細則，由法務部定之。

第五十六條　本法施行日期，由行政院定之。

現行條文第十九條至第二十二條及第四十三條之刪除，自公布日施行。

前項公布日於現行條文第四十三條第二項指定之事業、團體或個人應於指定之日起六個月內辦理登記或許可之期間內者，該指定之事業、團體或個人得申請終止辦理，目的事業主管機關於終止辦理時，應退還已繳規費。已辦理完成者，亦得申請退費。

前項退費，應自繳費義務人繳納之日起，至目的事業主管機關終止辦理之日止，按退費額，依繳費之日郵政儲金之一年期定期存款利率，按日加計利息，一併退還。已辦理完成者，其退費，應自繳費義務人繳納之日起，至目的事業主管機關核准申請之日止，亦同。

三、個人資料保護法施行細則

1. 中華民國八十五年五月一日法務部(85)法令字第10259號令訂定發布全文46條
2. 中華民國一百零一年九月二十六日法務部法令字第 10103107360 號令修正發布名稱及全文33條；並自一百零一年十月一日施行（原名稱：電腦處理個人資料保護法施行細則）
3. 中華民國一百零五年三月二日法務部法令字第 10503502120 號令修正發布第 9～15、17、18 條條文；並自一百零五年三月十五日施行
   中華民國一百零八年一月十日法務部法律字第10803500010號、國家發展委員會發法字第1080080004A號會銜公告第33條所列屬「法務部」之權責事項，改由「國家發展委員會」管轄

第一條　本細則依個人資料保護法（以下簡稱本法）第五十五條規定訂定之。

第二條　本法所稱個人，指現生存之自然人。

第三條　本法第二條第一款所稱得以間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。

第四條　本法第二條第一款所稱病歷之個人資料，指醫療法第六十七條第二項所列之各款資料。

本法第二條第一款所稱醫療之個人資料，指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。

本法第二條第一款所稱基因之個人資料，指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。

本法第二條第一款所稱性生活之個人資料，指性取向或性慣行之個人資料。

本法第二條第一款所稱健康檢查之個人資料，指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。

本法第二條第一款所稱犯罪前科之個人資料，指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

第五條　本法第二條第二款所定個人資料檔案，包括備份檔案。

第六條　本法第二條第四款所稱刪除，指使已儲存之個人資料自個人資料檔案中消失。

本法第二條第四款所稱內部傳送，指公務機關或非公務機關本身內部之資料傳送。

第七條　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。

第八條　委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。

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、受託者就第十二條第二項採取之措施。

三、有複委託者，其約定之受託者。

四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。

五、委託機關如對受託者有保留指示者，其保留指示之事項。

六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。

受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。

第九條　本法第六條第一項但書第一款、第八條第二項第一款、第十六條但書第一款、第十九條第一項第一款、第二十條第一項但書第一款所稱法律，指法律或法律具體明確授權之

法規命令。

第十條　本法第六條第一項但書第二款及第五款、第八條第二項第二款及第三款、第十條但書第二款、第十五條第一款、第十六條所稱法定職務，指於下列法規中所定公務機關之職務：

一、法律、法律授權之命令。

二、自治條例。

三、法律或自治條例授權之自治規則。

四、法律或中央法規授權之委辦規則。

第十一條　本法第六條第一項但書第二款及第五款、第八條第二項第二款所稱法定義務，指非公務機關依法律或法律具體明確授權之法規命令所定之義務。

第十二條　本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及第二十七條第一項所稱適當之安全措施，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措施。

前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：

一、配置管理之人員及相當資源。

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、使用紀錄、軌跡資料及證據保存。

十一、個人資料安全維護之整體持續改善。

第十三條　本法第六條第一項但書第三款、第九條第二項第二款、第

十九條第一項第三款所稱當事人自行公開之個人資料，指當事人自行對不特定人或特定多數人揭露其個人資料。
本法第六條第一項但書第三款、第九條第二項第二款、第十九條第一項第三款所稱已合法公開之個人資料，指依法律或法律具體明確授權之法規命令所公示、公告或以其他合法方式公開之個人資料。

第十四條　本法第六條第一項但書第六款、第十一條第二項及第三項但書所定當事人書面同意之方式，依電子簽章法之規定，得以電子文件為之。

第十五條　本法第七條第二項所定單獨所為之意思表示，如係與其他意思表示於同一書面為之者，蒐集者應於適當位置使當事人得以知悉其內容並確認同意。

第十六條　依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、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。

第十七條　本法第六條第一項但書第四款、第九條第二項第四款、第十六條但書第五款、第十九條第一項第四款及第二十條第一項但書第五款所稱無從識別特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。

第十八條　本法第十條但書第三款所稱妨害第三人之重大利益，指有害於第三人個人之生命、身體、自由、財產或其他重大利益。

第十九條　當事人依本法第十一條第一項規定向公務機關或非公務機關請求更正或補充其個人資料時，應為適當之釋明。

第二十條　本法第十一條第三項所稱特定目的消失，指下列各款情形之一：
一、公務機關經裁撤或改組而無承受業務機關。

二、非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與原蒐集目的不符。
三、特定目的已達成而無繼續處理或利用之必要。
四、其他事由足認該特定目的已無法達成或不存在。

第二十一條　有下列各款情形之一者，屬於本法第十一條第三項但書所定因執行職務或業務所必須：
一、有法令規定或契約約定之保存期限。
二、有理由足認刪除將侵害當事人值得保護之利益。
三、其他不能刪除之正當事由。

第二十二條　本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、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。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。
依本法第十二條規定通知當事人，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。

第二十三條　公務機關依本法第十七條規定為公開，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，指利用政府公報、新聞紙、雜誌、電子報或其他可供公眾查閱之方式為公開。

第二十四條　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。

第二十五條　本法第十八條所稱專人，指具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作之人員。
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。

第二十六條　本法第十九條第一項第二款所定契約或類似契約之關係，

不以本法修正施行後成立者為限。

第二十七條　本法第十九條第一項第二款所定契約關係，包括本約，及非公務機關與當事人間為履行該契約，所涉及必要第三人之接觸、磋商或聯繫行為及給付或向其為給付之行為。

本法第十九條第一項第二款所稱類似契約之關係，指下列情形之一者：

一、非公務機關與當事人間於契約成立前，為準備或商議訂立契約或為交易之目的，所進行之接觸或磋商行為。

二、契約因無效、撤銷、解除、終止而消滅或履行完成時，非公務機關與當事人為行使權利、履行義務，或確保個人資料完整性之目的所為之連繫行為。

第二十八條　本法第十九條第一項第七款所稱一般可得之來源，指透過大眾傳播、網際網路、新聞、雜誌、政府公報及其他一般人可得知悉或接觸而取得個人資料之管道。

第二十九條　依本法第二十二條規定實施檢查時，應注意保守秘密及被檢查者之名譽。

第三十條　依本法第二十二條第二項規定，扣留或複製得沒入或可為證據之個人資料或其檔案時，應掣給收據，載明其名稱、數量、所有人、地點及時間。

依本法第二十二條第一項及第二項規定實施檢查後，應作成紀錄。

前項紀錄當場作成者，應使被檢查者閱覽及簽名，並即將副本交付被檢查者；其拒絕簽名者，應記明其事由。

紀錄於事後作成者，應送達被檢查者，並告知得於一定期限內陳述意見。

第三十一條　本法第五十二條第一項所稱之公益團體，指依民法或其他法律設立並具備個人資料保護專業能力之公益社團法人、財團法人及行政法人。

第三十二條　本法修正施行前已蒐集或處理由當事人提供之個人資料，

於修正施行後，得繼續為處理及特定目的內之利用；其為特定目的外之利用者，應依本法修正施行後之規定為之。

第三十三條　本細則施行日期，由法務部定之。

四、經濟部及所屬機關個人資料保護管理要點

1. 中華民國一百零一年十月二十六日經法字第 10104681660 號函下達
2. 中華民國一百零七年二月十四日經法字第 10704680380 號函下達修正第 5 點、第 6 點、第 7 點、第 11 點及第 22 點
3. 中華民國一百零八年十二月九日經法字第 10804681790 號函下達修正第 22 點

壹、總則

一、經濟部（以下簡稱本部）及所屬機關為執行個人資料保護法（以下簡稱本法），以落實個人資料之保護及管理，特訂定本要點。

二、本部一級單位及所屬機關辦理下列事項，應設置個人資料保護聯絡窗口：

（一）公務機關間個人資料保護業務之協調聯繫及緊急應變通報。
（二）非資通安全面個人資料安全事件之通報。
（三）重大個人資料外洩事件之民眾聯繫單一窗口。
（四）本部一級單位及所屬機關個人資料專人名冊之製作及更新。
（五）本部一級單位及所屬機關個人資料專人與職員工教育訓練名單及紀錄之彙整。
（六）個人資料保護法令之諮詢。

三、本部及所屬機關之一級單位辦理下列事項，應指定專人處理：

（一）執行當事人依本法第十條及第十一條第一項至第四項所定請求之督導。
（二）執行本法第十一條第五項及第十二條所定通知之督導。
（三）本法第十七條所定公開或供公眾查閱。
（四）本法第十八條及個人資料保護法施行細則(以下簡稱本法施行細則)第十二條所定個人資料檔案安全維護。
（五）職員工之個人資料保護意識提升及教育訓練計畫之執行。
（六）個人資料保護事項之協調聯繫。
（七）單位內個人資料損害預防及危機處理應變之通報。
（八）本部及所屬機關個人資料保護方針及政策之執行、單位內個人資料保護之自行查核。
（九）其他有關單位內個人資料保護管理之規劃及執行。

貳、個人資料之蒐集、處理及利用

四、本部及所屬機關蒐集、處理或利用個人資料之特定目的，依個人資料保護法之特定目的及個人資料之類別規定者為限。

五、本部及所屬機關蒐集當事人個人資料時，應明確告知當事人下列事項。但符合本法第八條第二項規定情形之一者，不在此限：

（一）機關或單位名稱。
（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，不提供對其權益之影響。

本部及所屬機關明確告知當事人前項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依本法第十五條第二款規定表示同意。

本部及所屬機關蒐集當事人個人資料時，就本法所稱經當事人同意之事實，應負舉證責任。

六、本部及所屬機關蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前點第一項第一款至第五款所列事項。但符合本法第九條第二項規定情形之一者，不在此限。

前項之告知，得於首次對當事人為利用時併同為之。

七、本部及所屬機關依本法第六條第一項但書第六款、第十一條第二項但書及第三項但書規定經當事人書面同意者，應取得當事人同意書；該同意書作成之方式，依電子簽章法之規定，得以電子文件為之。

八、本部及所屬機關依本法第十五條或第十六條規定對個人資料之蒐集、處理、利用時，應詳為審核並簽奉核定後為之。

本部及所屬機關依本法第十六條但書規定對個人資料為特定目的外之利用，應將個人資料之利用歷程做成紀錄。

本部及所屬機關對於個人資料不得為非法之利用，並不得為資料庫之恣意連結，且不得濫用。

九、本部及所屬機關保有之個人資料有誤或缺漏時，應由資料蒐集單位簽奉核定後，移由資料保有單位更正或補充之，並留存相關紀錄。

因可歸責於本部及所屬機關之事由，未為更正或補充之個人資料，應於更正或補充後，由資料蒐集單位以通知書通知曾提供利用之對象。

十、本部及所屬機關保有之個人資料正確性有爭議者，應由資料蒐集單位簽奉核定後，移由資料保有單位停止處理或利用該個人資料。但符合本法第十一條第二項但書情形者，不在此限。

個人資料已停止處理或利用者，資料保有單位應確實記錄。

十一、本部及所屬機關保有個人資料蒐集之特定目的消失或期限屆滿時，應由資料蒐集單位簽奉核定後，移由資料保有單位刪除、停止處理或利用。但符合本法第十一條第三項但書情形者，不在此限。

個人資料已刪除、停止處理或利用者，資料保有單位應確實記錄。

十二、本部及所屬機關依本法第十一條第四項規定應主動或依當事人之請求刪除、停止蒐集、處理或利用個人資料者，應簽奉核定後移由資料保有單位為之。

個人資料已刪除、停止蒐集、處理或利用者，資料保有單位應確實記錄。

十三、本部及所屬機關遇有本法第十二條所定個人資料被竊取、洩漏、竄改或其他侵害情事者，經查明後，應由資料外洩單位依本法施行細則第二十二條所定之適當方式儘速通知當事人。

參、當事人行使權利之處理

十四、當事人依本法第十條或第十一條第一項至第四項規定向本部及所屬機關為請求時，應填具申請書，並檢附相關證明文件。

前項書件內容，如有遺漏或欠缺，應通知限期補正。

申請案件有下列情形之一者，應以書面駁回其申請：

（一）申請書件內容有遺漏或欠缺，經通知限期補正，逾期仍未

補正。

（二）有本法第十條但書各款情形之一。

（三）有本法第十一條第二項但書或第三項但書所定情形之一。

（四）與法令規定不符。

十五、當事人依本法第十條規定提出之請求，應於十五日內為准駁之決定。

前項之准駁決定，必要時得予延長，延長期間不得逾十五日，並應將其原因以書面通知請求人。

十六、當事人請求查詢、閱覽或製給個人資料複製本者，準用經濟部及所屬機關提供政府資訊收費標準或本部所屬機關另行訂定之相關收費標準收取費用。

當事人閱覽其個人資料，應由承辦單位派員陪同為之，並依經濟部政府資訊及卷宗閱覽須知或本部所屬機關訂定之相關規定辦理。

十七、當事人依本法第十一條第一項至第四項規定提出之請求，應於三十日內為准駁之決定。

前項之准駁決定，必要時得予延長，延長期間不得逾三十日，並應將其原因以書面通知請求人。

十八、個人資料檔案，其性質特殊或法律另有規定不應公開其檔案名稱者，得依政府資訊公開法或其他法律規定，限制公開或不予提供。

肆、個人資料檔案安全維護

十九、為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本部及所屬機關指定之個人資料檔案安全維護專人，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。

二十、個人資料檔案應建立管理制度，分級分類管理，並針對接觸人員建立安全管理規範。

二十一、為強化個人資料檔案之存取安全，防止非法授權存取，維護個人資料之隱私性，本部及所屬機關應將個人資料檔案安全稽核作業，納入公務機密檢查及資通安全管理稽核機制中辦

理之。

二十二、本部及所屬機關遇有個人資料檔案發生遭人惡意破壞毀損、作業不慎等危安事件，或有駭客攻擊等非法入侵情事，導致個資外洩事件時，應進行緊急因應措施，並迅速通報至本部個人資料保護推動執行小組；如屬資通安全面之個資外洩事件，應另依其資通安全事件通報及應變機制進行通報。

二十三、個人資料檔案安全維護工作，除本要點外，並應符合行政院與本部及所屬機關訂定之相關資訊作業安全與機密維護規範。

伍、附則

二十四、本部及所屬機關依本法第四條規定委託蒐集、處理或利用個人資料者，適用本要點。

前項委託應為適當之監督，其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）受託者就本法施行細則第十二條第二項採取之措施。
（三）有複委託者，其約定之受託者。
（四）受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。
（五）委託機關如對受託者有保留指示者,其保留指示之事項。
（六）委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

前項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。

受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。

二十五、本部所屬機關因業務性質特殊者，得另訂個人資料保護管理要點規範之。

五、經濟部個人資料保護推動執行小組設置要點

1. 中華民國九十九年七月二十八日經資字第 09904881160 號函下達
2. 中華民國一百零一年一月十一日經資字第 10054880980 號函修正下達
3. 中華民國一百零三年八月二十八日經法字第 10304681251 號函修正下達
4. 中華民國一百零八年一月三十一日經法字第 10804680200 號函修正下達

一、經濟部（以下簡稱本部）為推動及落實本部暨所屬機關與所監督之非公務機關個人資料之保護及管理，特設經濟部個人資料保護推動執行小組（以下簡稱本小組）。

二、本小組屬常態任務編組，置召集人一人，由本部次長兼任，負責推動、協調及督導本部個人資料保護管理業務；執行秘書一人，由本部法規會執行秘書擔任，承召集人之命，負責綜理本小組有關業務；本小組委員由本部所屬機關個資保護召集人及本部幕僚單位個資保護專責人員兼任之。

三、本小組職掌如下：

（一）本部個人資料保護管理制度及配套措施之擬議。

（二）個人資料保護相關法規專業訓練及宣導作業之擬議。

（三）持續檢視個人資料管理制度是否符合法律、司法實務及科學技術之變更。

（四）個資外洩事件通報暨危機處理。

（五）個人資料保護管理作業相關稽核作業之督導。

（六）其他個人資料保護執行事項。

四、本小組下設行政機關分組、產業輔導分組、法規專責分組、資訊技術分組四個工作分組，各分組主、協辦單位及工作內容如下：

（一）行政機關分組：主辦單位為本部法規會，協辦單位為本部各幕僚單位及行政機關，負責推動本部幕僚單位及行政機關之個人資料保護相關管理制度、個資外洩事件通報暨危機處理及個人資料保護宣導等工作。

（二）產業輔導分組：

1. 主辦單位為本部商業司、中部辦公室、技術處、研發會、資訊中心、礦務局、水利署、國際貿易局、工業局、智慧財產局、標準檢驗局、能源局、國營事業委員會、中小企業處及加工出口區管理處等，負責推動所主管非公務機關之個人資料保護相關管理制度、個資外洩事件通報暨危機處理及個人資料保護宣導等工作。
2. 本分組共通性事項之幕僚作業，由商業司負責；如有爭議

時，由商業司簽陳召集人指定之。

（三）法規專責分組：主辦單位為本部法規會，協辦單位為本部暨所屬機關法制單位，負責研訂本部個人資料保護管理要點、協助各機關(單位)擬訂個人資料保護相關管理辦法並協助人事處辦理個人資料保護相關法規專業訓練。

（四）資訊技術分組：主辦單位為本部資訊中心，協辦單位為本部暨所屬機關資訊相關單位，負責推動電腦個人資料安全控制措施、協助各業務單位執行個人資料保護作業。

五、本小組幕僚作業由本部法規會負責辦理，各分組之幕僚作業，除另有規定外，由各分組主辦單位負責辦理。

六、本部暨所屬機關均應建立個資保護召集人、通報窗口及專責人員名冊並保持最新狀況。

七、本小組執行業務所需經費，由本部一般行政經費項下支應。

八、本小組每年召開會議一次；必要時，得召集臨時會。

前項會議由召集人召集之，並擔任主席；如召集人因事不能出席時，由執行秘書代理之。

六、個人資料保護法之特定目的及個人資料之類別

法務部會銜相關部會於101年10月1日以令修正「電腦處理個人資料保護法之特定目的及個人資料之類別」，並修正名稱為「個人資料保護法之特定目的及個人資料之類別」，定自101年10月1日生效。

個資法（簡稱新法）第五十三條規定：「本法所定特定目的及個人資料類別，由法務部會同中央目的事業主管機關指定之」，其修正理由係將電腦處理個資法（簡稱舊法）第三條第九款及第十條第二項規定合併之。查上開舊法條文立法理由略以：關於特定目的及個人資料之類別，宜有細目規定，以便作為公告或其他相關作業之依據。尤其舊法適用之非公務機關採登記執照公告制度，故參考英國個資法申報登記制度有關例示兼概括「特定目的及個人資料類別」等文件，頒訂「電腦處理個資法之特定目的及個人資料之類別」，以供各界參考。

雖新法已廢除非公務機關取得執照後始得蒐集、處理及利用個人資料之制度(新法第五十六條第二項規定)，自無需再申請登記及公告相關事項，惟公務機關及非公務機關為確保個人資料檔案之合法且正當蒐集、處理或利用，宜保存相關之證據文件（新法施行細則第十二條第二項第十一款規定意旨），包含蒐集、處理或利用之「特定目的」內涵，屬安全維護之適當措施之一部分；且公務機關辦理個人資料檔案公開事項作業，尚須說明特定目的及個人資料之類別。故參考歐盟個人資料保護指令第二十九條工作小組於二〇〇六年有關成員國「申報登記要求事項手冊（VademecumonNotificationRequirements)」調查報告，有提供特定目的及個人資料類別清單文件之國家（例如：英國、比例時、西班牙等)，係採例示兼概括並得自由敘述補充之立法例；同時參酌各機關函復本部有關特定目的及個人資料類別之修正意見，適度修正項目與類別，並避免過度繁瑣，以免掛一漏萬。另例示或概括之特定目的及個人資料類別，並非可包含所有可能之活動，公務機關或非公務機關於參考本規定，選擇特定目的及個人資料類別時，仍宜提出詳盡之業務活動說明，列入證據文件或個人資料檔案公開事項作業內，以補充澄清特定目的及個人資料類別實質內涵。爰擬具「電腦處理個資法之特定目的及個人資料之類別」修正草案，並將法規名稱修正為「個人資料保護法之特定目的及個人資料之類別」。

個人資料保護法之特定目的及個人資料之類別

代號	修正特定目的項目
○○一	人身保險
○○二	人事管理（包含甄選、離職及所屬員工基本資訊、現職、學經歷、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、差勤、福利措施、褫奪公權、特殊查核或其他人事措施）
○○三	入出國及移民
○○四	土地行政
○○五	工程技術服務業之管理
○○六	工業行政
○○七	不動產服務
○○八	中小企業及其他產業之輔導
○○九	中央銀行監理業務
○一○	公立與私立慈善機構管理
○一一	公共造產業務
○一二	公共衛生或傳染病防治
○一三	公共關係
○一四	公職人員財產申報、利益衝突迴避及政治獻金業務
○一五	戶政
○一六	文化行政
○一七	文化資產管理
○一八	水利、農田水利行政
○一九	火災預防與控制、消防行政
○二○	代理與仲介業務
○二一	外交及領事事務
○二二	外匯業務
○二三	民政
○二四	民意調查
○二五	犯罪預防、刑事偵查、執行、矯正、保護處分、犯罪被害人保護或更生保護事務
○二六	生態保育
○二七	立法或立法諮詢
○二八	交通及公共建設行政

〇二九　公民營（辦）交通運輸、公共運輸及公共建設
〇三〇　仲裁
〇三一　全民健康保險、勞工保險、農民保險、國民年金保險或其他社會保險
〇三二　刑案資料管理
〇三三　多層次傳銷經營
〇三四　多層次傳銷監管
〇三五　存款保險
〇三六　存款與匯款
〇三七　有價證券與有價證券持有人登記
〇三八　行政執行
〇三九　行政裁罰、行政調查
〇四〇　行銷（包含金控共同行銷業務）
〇四一　住宅行政
〇四二　兵役、替代役行政
〇四三　志工管理
〇四四　投資管理
〇四五　災害防救行政
〇四六　供水與排水服務
〇四七　兩岸暨港澳事務
〇四八　券幣行政
〇四九　宗教、非營利組織業務
〇五〇　放射性物料管理
〇五一　林業、農業、動植物防疫檢疫、農村再生及土石流防災管理
〇五二　法人或團體對股東、會員（含股東、會員指派之代表）、董事、監察人、理事、監事或其他成員名冊之內部管理
〇五三　法制行政
〇五四　法律服務
〇五五　法院執行業務
〇五六　法院審判業務
〇五七　社會行政
〇五八　社會服務或社會工作
〇五九　金融服務業依法令規定及金融監理需要，所為之蒐集處理及利用
〇六〇　金融爭議處理

〇六一　金融監督、管理與檢查
〇六二　青年發展行政
〇六三　非公務機關依法定義務所進行個人資料之蒐集處理及利用
〇六四　保健醫療服務
〇六五　保險經紀、代理、公證業務
〇六六　保險監理
〇六七　信用卡、現金卡、轉帳卡或電子票證業務
〇六八　信託業務
〇六九　契約、類似契約或其他法律關係事務
〇七〇　客家行政
〇七一　建築管理、都市更新、國民住宅事務
〇七二　政令宣導
〇七三　政府資訊公開、檔案管理及應用
〇七四　政府福利金或救濟金給付行政
〇七五　科技行政
〇七六　科學工業園區、農業科技園區、文化創業園區、生物科技園區或其他園區管理行政
〇七七　訂位、住宿登記與購票業務
〇七八　計畫、管制考核與其他研考管理
〇七九　飛航事故調查
〇八〇　食品、藥政管理
〇八一　個人資料之合法交易業務
〇八二　借款戶與存款戶存借作業綜合管理
〇八三　原住民行政
〇八四　捐供血服務
〇八五　旅外國人急難救助
〇八六　核子事故應變
〇八七　核能安全管理
〇八八　核貸與授信業務
〇八九　海洋行政
〇九〇　消費者、客戶管理與服務
〇九一　消費者保護
〇九二　畜牧行政
〇九三　財產保險
〇九四　財產管理

〇九五　財稅行政
〇九六　退除役官兵輔導管理及其眷屬服務照顧
〇九七　退撫基金或退休金管理
〇九八　商業與技術資訊
〇九九　國內外交流業務
一〇〇　國家安全行政、安全查核、反情報調查
一〇一　國家經濟發展業務
一〇二　國家賠償行政
一〇三　專門職業及技術人員之管理、懲戒與救濟
一〇四　帳務管理及債權交易業務
一〇五　彩券業務
一〇六　授信業務
一〇七　採購與供應管理
一〇八　救護車服務
一〇九　教育或訓練行政
一一〇　產學合作
一一一　票券業務
一一二　票據交換業務
一一三　陳情、請願、檢舉案件處理
一一四　勞工行政
一一五　博物館、美術館、紀念館或其他公、私營造物業務
一一六　場所進出安全管理
一一七　就業安置、規劃與管理
一一八　智慧財產權、光碟管理及其他相關行政
一一九　發照與登記
一二〇　稅務行政
一二一　華僑資料管理
一二二　訴願及行政救濟
一二三　貿易推廣及管理
一二四　鄉鎮市調解
一二五　傳播行政與管理
一二六　債權整貼現及收買業務
一二七　募款（包含公益勸募）
一二八　廉政行政
一二九　會計與相關服務

一三〇　會議管理
一三一　經營郵政業務郵政儲匯保險業務
一三二　經營傳播業務
一三三　經營電信業務與電信加值網路業務
一三四　試務、銓敘、保訓行政
一三五　資（通）訊服務
一三六　資（通）訊與資料庫管理
一三七　資通安全與管理
一三八　農產品交易
一三九　農產品推廣資訊
一四〇　農糧行政
一四一　遊說業務行政
一四二　運動、競技活動
一四三　運動休閒業務
一四四　電信及傳播監理
一四五　僱用與服務管理
一四六　圖書館、出版品管理
一四七　漁業行政
一四八　網路購物及其他電子商務服務
一四九　蒙藏行政
一五〇　輔助性與後勤支援管理
一五一　審計、監察調查及其他監察業務
一五二　廣告或商業行為管理
一五三　影視、音樂與媒體管理
一五四　徵信
一五五　標準、檢驗、度量衡行政
一五六　衛生行政
一五七　調查、統計與研究分析
一五八　學生（員）（含畢、結業生）資料管理
一五九　學術研究
一六〇　憑證業務管理
一六一　輻射防護
一六二　選民服務管理
一六三　選舉、罷免及公民投票行政
一六四　營建業之行政管理

一六五　環境保護
一六六　證券、期貨、證券投資信託及顧問相關業務
一六七　警政
一六八　護照、簽證及文件證明處理
一六九　體育行政
一七〇　觀光行政、觀光旅館業、旅館業、旅行業、觀光遊樂業及民宿經營管理業務
一七一　其他中央政府機關暨所屬機關構內部單位管理、公共事務監督、行政協助及相關業務
一七二　其他公共部門（包括行政法人、政府捐助財團法人及其他公法人）執行相關業務
一七三　其他公務機關對目的事業之監督管理
一七四　其他司法行政
一七五　其他地方政府機關暨所屬機關構內部單位管理、公共事務監督、行政協助及相關業務
一七六　其他自然人基於正當性目的所進行個人資料之蒐集處理及利用
一七七　其他金融管理業務
一七八　其他財政收入
一七九　其他財政服務
一八〇　其他經營公共事業（例如：自來水、瓦斯等）業務
一八一　其他經營合於營業登記項目或組織章程所定之業務
一八二　其他諮詢與顧問服務

代　　號　識別類：

C〇〇一　辨識個人者。

例如：姓名、職稱、住址、工作地址、以前地址、住家電話號碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊及戶籍地址、相片、指紋、電子郵遞地址、電子簽章、憑證卡序號、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及其他任何可辨識資料本人者等。

C〇〇二　辨識財務者。

例如：金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號碼、保險單號碼、個人之其他號碼或帳戶等。

C〇〇三　政府資料中之辨識者。

例如：身分證統一編號、統一證號、稅籍編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等。

代　　號　特徵類：

C〇一一　個人描述。

例如：年齡、性別、出生年月日、出生地、國籍、聲音等。

C〇一二　身體描述。

例如：身高、體重、血型等。

C〇一三　習慣。

例如：抽煙、喝酒等。

C〇一四　個性。

例如：個性等之評述意見。

代　　號　家庭情形：

C〇二一　家庭情形。

例如：結婚有無、配偶或同居人之姓名、前配偶或同居人之姓名、結婚之日期、子女之人數等。

C〇二二　婚姻之歷史。

例如：前次婚姻或同居、離婚或分居等細節及相關人之姓名等。

C〇二三　家庭其他成員之細節。

例如：子女、受扶養人、家庭其他成員或親屬、父母、同居人及旅居國外及大陸人民親屬等。

C〇二四　其他社會關係。
例如：朋友、同事及其他除家庭以外之關係等。

代　　號　社會情況：
C〇三一　住家及設施。
例如：住所地址、設備之種類、所有或承租、住用之期間、租金或稅率及其他花費在房屋上之支出、房屋之種類、價值及所有人之姓名等。
C〇三二　財產。
例如：所有或具有其他權利之動產或不動產等。
C〇三三　移民情形。
例如：護照、工作許可文件、居留證明文件、住居或旅行限制、入境之條件及其他相關細節等。
C〇三四　旅行及其他遷徙細節。
例如：過去之遷徙、旅行細節、外國護照、居留證明文件及工作證照及工作證等相關細節等。
C〇三五　休閒活動及興趣。
例如：嗜好、運動及其他興趣等。
C〇三六　生活格調。
例如：使用消費品之種類及服務之細節、個人或家庭之消費模式等。
C〇三七　慈善機構或其他團體之會員資格。
例如:俱樂部或其他志願團體或持有參與者紀錄之單位等。
C〇三八　職業。
例如：學校校長、民意代表或其他各種職業等。
C〇三九　執照或其他許可。
例如：駕駛執照、行車執照、自衛槍枝使用執照、釣魚執照等。
C〇四〇　意外或其他事故及有關情形。
例如：意外事件之主體、損害或傷害之性質、當事人及證人等。
C〇四一　法院、檢察署或其他審判機關或其他程序。
例如：關於資料主體之訴訟及民事或刑事等相關資料等。

代　　號　教育、考選、技術或其他專業：

C〇五一　學校紀錄。
例如：大學、專科或其他學校等。
C〇五二　資格或技術。
例如：學歷資格、專業技術、特別執照（如飛機駕駛執照等）、政府職訓機構學習過程、國家考試、考試成績或其他訓練紀錄等。
C〇五三　職業團體會員資格。
例如：會員資格類別、會員資格紀錄、參加之紀錄等。
C〇五四　職業專長。
例如：專家、學者、顧問等。
C〇五五　委員會之會員資格。
例如：委員會之詳細情形、工作小組及會員資格因專業技術而產生之情形等。
C〇五六　著作。
例如：書籍、文章、報告、視聽出版品及其他著作等。
C〇五七　學生（員）、應考人紀錄。
例如：學習過程、相關資格、考試訓練考核及成績、評分評語或其他學習或考試紀錄等。
C〇五八　委員工作紀錄。
例如：委員參加命題、閱卷、審查、口試及其他試務工作情形記錄。

代　　號　受僱情形：
C〇六一　現行之受僱情形。
例如：僱主、工作職稱、工作描述、等級、受僱日期、工時、工作地點、產業特性、受僱之條件及期間、與現行僱主有關之以前責任與經驗等。
C〇六二　僱用經過。
例如：日期、受僱方式、介紹、僱用期間等。
C〇六三　離職經過。
例如：離職之日期、離職之原因、離職之通知及條件等。
C〇六四　工作經驗。
例如：以前之僱主、以前之工作、失業之期間及軍中服役情形等。
C〇六五　工作、差勤紀錄。

例如：上、下班時間及事假、病假、休假、娩假各項請假紀錄在職紀錄或未上班之理由、考績紀錄、獎懲紀錄、褫奪公權資料等。

C〇六六　健康與安全紀錄。

例如：職業疾病、安全、意外紀錄、急救資格、旅外急難救助資訊等。

C〇六七　工會及員工之會員資格。

例如：會員資格之詳情、在工會之職務等。

C〇六八　薪資與預扣款。

例如：薪水、工資、佣金、紅利、費用、零用金、福利、借款、繳稅情形、年金之扣繳、工會之會費、工作之基本工資或工資付款之方式、加薪之日期等。

C〇六九　受僱人所持有之財產。

例如：交付予受僱人之汽車、工具、書籍或其他設備等。

C〇七〇　工作管理之細節。

例如：現行義務與責任、工作計畫、成本、用人費率、工作分配與期間、工作或特定工作所花費之時間等。

C〇七一　工作之評估細節。

例如：工作表現與潛力之評估等。

C〇七二　受訓紀錄。

例如：工作必須之訓練與已接受之訓練，已具有之資格或技術等。

C〇七三　安全細節。

例如：密碼、安全號碼與授權等級等。

代　　號　財務細節：

C〇八一　收入、所得、資產與投資。

例如：總收入、總所得、賺得之收入、賺得之所得、資產、儲蓄、開始日期與到期日、投資收入、投資所得、資產費用等。

C〇八二　負債與支出。

例如：支出總額、租金支出、貸款支出、本票等信用工具支出等。

C〇八三　信用評等。

例如：信用等級、財務狀況與等級、收入狀況與等級等。

C〇八四　貸款。
例如：貸款類別、貸款契約金額、貸款餘額、初貸日、到期日、應付利息、付款紀錄、擔保之細節等。
C〇八五　外匯交易紀錄。
C〇八六　票據信用。
例如：支票存款、基本資料、退票資料、拒絕往來資料等。
C〇八七　津貼、福利、贈款。
C〇八八　保險細節。
例如：保險種類、保險範圍、保險金額、保險期間、到期日、保險費、保險給付等。
C〇八九　社會保險給付、就養給付及其他退休給付。
例如：生效日期、付出與收入之金額、受益人等。
C〇九一　資料主體所取得之財貨或服務。
例如：貨物或服務之有關細節、資料主體之貸款或僱用等有關細節等。
C〇九二　資料主體提供之財貨或服務。
例如：貨物或服務之有關細節等。
C〇九三　財務交易。
例如：收付金額、信用額度、保證人、支付方式、往來紀錄、保證金或其他擔保等。
C〇九四　賠償。
例如：受請求賠償之細節、數額等。

代　　號　商業資訊：
C一〇一　資料主體之商業活動。
例如：商業種類、提供或使用之財貨或服務、商業契約等。
C一〇二　約定或契約。
例如：關於交易、商業、法律或其他契約、代理等。
C一〇三　與營業有關之執照。
例如：執照之有無、市場交易者之執照、貨車駕駛之執照等。

代　　號　健康與其他：
C一一一　健康紀錄。
例如：醫療報告、治療與診斷紀錄、檢驗結果、身心障礙

種類、等級、有效期間、身心障礙手冊證號及聯絡人等。

C一一二　性生活。

C一一三　種族或血統來源。
例如：去氧核糖核酸資料等。

C一一四　交通違規之確定裁判及行政處分。
例如：裁判及行政處分之內容、其他與肇事有關之事項等。

C一一五　其他裁判及行政處分。
例如：裁判及行政處分之內容、其他相關事項等。

C一一六　犯罪嫌疑資料。
例如：作案之情節、通緝資料、與已知之犯罪者交往、化名、足資證明之證據等。

C一一七　政治意見。
例如：政治上見解、選舉政見等。

C一一八　政治團體之成員。
例如：政黨黨員或擔任之工作等。

C一一九　對利益團體之支持。
例如：係利益團體或其他組織之會員、支持者等。

C一二〇　宗教信仰。

C一二一　其他信仰。

代　　號　其他各類資訊：

C一三一　書面文件之檢索。
例如：未經自動化機器處理之書面文件之索引或代號等。

C一三二　未分類之資料。
例如：無法歸類之信件、檔案、報告或電子郵件等。

C一三三　輻射劑量資料。
例如：人員或建築之輻射劑量資料等。

C一三四　國家情報工作資料。
例如：國家情報工作法、國家情報人員安全查核辦法等有關資料。

七、行政院及所屬各機關落實個人資料保護聯繫作業要點

中華民國一百十年八月十一日院授發協字第1102001106號函訂定

一、行政院(以下簡稱本院)為防止非公務機關個人資料檔案外洩(以下簡稱個資外洩)，加強所屬中央目的事業主管機關(以下簡稱中央目的事業主管機關)對非公務機關個人資料保護之監管，以落實非公務機關個人資料檔案之安全維護，特訂定本要點。

二、本院得召開行政機關落實個人資料保護執行聯繫會議(以下簡稱聯繫會議)，執行下列任務：

（一）研議中央目的事業主管機關依個人資料保護法(以下簡稱個資法)第二十七條第三項所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之標準等相關事項之辦法（以下簡稱安全維護辦法）應予規定之相關事項。

（二）統籌個資外洩案件之監督通報。

（三）就重大矚目之個資外洩案件管轄權爭議，確認管轄機關，及該案件行政檢查之協調。

（四）其他個人資料侵害案件之跨部會協調聯繫事務。

本要點所定重大矚目之個資外洩案件，其範圍如下：

（一）行政院、立法院或監察院關注之個資外洩案件。

（二）經媒體顯著披露之個資外洩案件，例如經平面媒體全國性版面報導、電子媒體專題討論。

三、聯繫會議由本院院長指派政務委員一人擔任召集人，三人擔任協同召集人。

聯繫會議由召集人主持；協同召集人視議題參與，並為協同主持人。召集人因故未能出席時，由召集人指定協同召集人一人代理之。

聯繫會議得視個資外洩案件或其他個人資料侵害案件議題之情形，不定期召開，並得視議題需要，邀請中央行政機關、直轄市、縣(市)政府等相關機關代表或專家、學者出席。

聯繫會議之幕僚作業，由國家發展委員會(以下簡稱國發會)辦理。

四、安全維護辦法應至少就下列事項予以規定：

（一）中央目的事業主管機關就所主管之非公務機關使用資通訊系

統蒐集、處理或利用個人資料，而有下列情形之一者，應加強管理：

1. 保有消費者交易、使用商品或接受服務等過程之一般或特種個人資料，且符合中央目的事業主管機關所定應加強管理之條件。
2. 前目以外經中央目的事業主管機關認定應加強管理。

（二）就前款應加強管理者之規定，應至少包括下列資料安全管理措施：

1. 使用者身分確認及保護機制。
2. 個人資料顯示之隱碼機制。
3. 網際網路傳輸之安全加密機制。
4. 個人資料檔案及資料庫之存取控制與保護監控措施。
5. 防止外部網路入侵對策。
6. 非法或異常使用行為之監控與因應機制。

（三）非公務機關個資外洩時，依安全維護辦法應通報之對象、時點、應通報事項、後續行政檢查等事項；其通報地方目的事業主管機關者，並應副知中央目的事業主管機關。

中央目的事業主管機關訂定或修正發布安全維護辦法，應函知國發會。

五、中央目的事業主管機關應就尚未訂定安全維護辦法之非公務機關，綜合考量下列情形，定期檢討訂定該辦法之必要性；其應訂定安全維護辦法者，並應於該辦法就前點第一項所定事項予以規定：

（一）非公務機關之規模、特性
（二）保有個人資料之數量或性質。
（三）與民眾日常生活關係密切程度。
（四）個資外洩衝擊層面廣泛程度。
（五）個資外洩將造成當事人身心危害、社會地位受損或衍生財務危機等重大影響。
（六）個人資料存取環境。
（七）個人資料傳輸之工具及方法。
（八）國際傳輸之頻率。

六、中央目的事業主管機關接獲非公務機關通報或副知，或非因通報

或副知而自行知悉個資外洩案件，經確認屬該機關管轄後，應於接獲通報、副知或知悉時起七十二小時內，填列監督通報紀錄表(如附件一)，通報國發會；並得依個資法第二十二條至第二十五條規定，對該非公務機關為適當之監督管理措施。

中央目的事業主管機關應就個資外洩案件之後續行政措施及處置情形，按季通報國發會；重大矚目之個資外洩案件之後續行政措施及處置情形，應即時通報國發會。

七、中央目的事業主管機關就前點個資外洩案件，經查明違反個資法之規定者，應視具體調查結果，依個資法第四十七條至第五十條規定處理。

八、中央目的事業主管機關對個資外洩案件之行政檢查流程，除重大矚目之個資外洩案件依第九點規定確認管轄機關者外，其餘行政檢查程序，依附件二流程圖辦理。

九、國發會對於重大矚目之個資外洩案件管轄權爭議，應儘速認定管轄機關，並得視需要召開跨部會協調會議。

前項被認定管轄機關如有異議，應於認定管轄文到三日內，敘明具體理由送國發會，提請聯繫會議確認管轄機關。

聯繫會議應邀集相關機關確認前項管轄機關，必要時並得邀請專家、學者出席。

經聯繫會議確認為管轄機關之中央目的事業主管機關，應於國發會指定時間內，依第六點第一項規定填列監督通報紀錄表。

十、中央目的事業主管機關對重大矚目之個資外洩案件辦理行政檢查前，已依行政程序法第十九條向其他機關請求行政協助遭拒絕者，得函送國發會，提請聯繫會議進行協調。

就前項行政檢查之協調，聯繫會議應邀集相關機關討論，經請求協助機關與被請求機關說明後，評估有提供行政協助之必要者，被請求機關即應配合執行。

重大矚目之個資外洩案件經聯繫會議認有行政檢查必要者，其中央目的事業主管機關應即規劃跨部會任務分工，並由聯繫會議邀集相關部會協調。

十一、本院資通安全處、內政部警政署及法務部調查局，應適時向國發會分享個資外洩案件情報。

國發會接獲前項情報後，應通知中央目的事業主管機關為必要之處理。

附件一、監督通報紀錄表

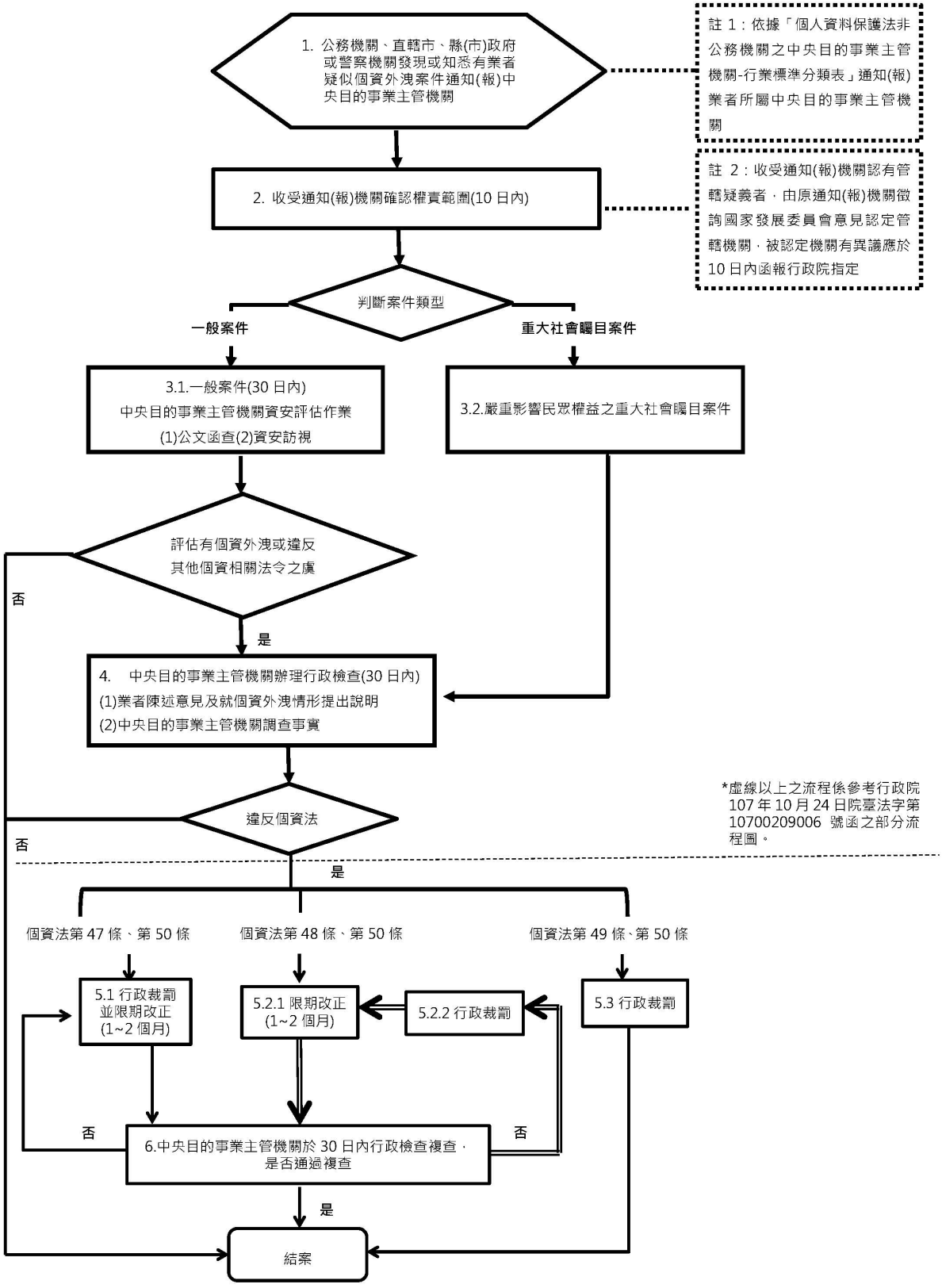
<table>
<tr><td></td><td colspan="3">監督通報紀錄表</td></tr>
<tr><td rowspan="8">首次通報作業
(註1)</td><td>非公務機關名稱
_____

通報機關
_____</td><td colspan="2">通報時間：　年　月　日　時　分
通報人：　　簽名(蓋章)
職稱：
電話：
Email：
地址：</td></tr>
<tr><td>事件發生時間(註2)</td><td colspan="2"></td></tr>
<tr><td rowspan="2">事件發生種類</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td><td>個資侵害之總筆數(大約)
_____</td></tr>
<tr><td>□一般個資 _____筆
□特種個資 _____筆</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個資外洩可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個資外洩後72小時通報</td><td colspan="2">□是　□否，理由</td></tr>
<tr><td rowspan="4">後續行政措施及處置作業</td><td>是否為嚴重影響民眾權益之重大社會矚目案件；倘是，影響層面為何</td><td colspan="2">□是　□通訊傳播 □交通 □勞動
□銀行與金融 □教育 □衛生福利
□其他：_____；□否</td></tr>
<tr><td>主管機關是否有進行行政檢查(含複查)</td><td colspan="2">□是　□否，理由</td></tr>
<tr><td>主管機關就個資外洩事件判斷是否違反個資法</td><td colspan="2">□是　□否，理由</td></tr>
<tr><td>主管機關就個資外洩事件之後續處置</td><td colspan="2"></td></tr>
<tr><td></td><td>結案時間</td><td colspan="2"></td></tr>
</table>

註1：該欄各項資訊係源自非公務機關之外洩通報內容，各欄位資訊若尚未明確，得先填寫「不明」，並得於後續處置作業之通報更新補充。

註2：事件發生時間如填寫「不明」者，請接續註明查知該非公務機關知悉個資外洩之時間。

附件二、中央目的事業主管機關對個資外洩案件之行政檢查流程圖



八、公布非公務機關及其負責人違反個人資料保護法情形之處分參考原則

中華民國一百十一年二月十日國家發展委員會發法字第1112000110號函訂定

一、為期中央目的事業主管機關或直轄市、縣（市）政府（以下簡稱中央或地方主管機關）就其查明非公務機關確有違反個人資料保護法（以下簡稱個資法）規定致個人資料外洩之情事，得依個資法第二十五條第一項第四款規定，公布該非公務機關之違法情形及其姓名或名稱與負責人時，妥善考量相關因素，特訂定本參考原則。

二、中央或地方主管機關依個資法第二十五條第一項第四款規定為處分時，得綜合考量非公務機關之下列情形：

（一）個人資料外洩情形及原因

1. 所涉個人資料類別、數量、發生原因、外洩持續期間。
2. 對當事人權益之影響風險。
3. 外洩係出於故意或過失。

（二）安全維護措施之落實情形

1. 依個資法第二十七條及同法施行細則第十二條規定，採取之安全維護措施及遵循之程度。
2. 先前有無個人資料外洩情事。

（三）於知悉個人資料外洩後，採取之措施

1. 為降低當事人損害所採取之行為。
2. 有無主動通報中央或地方主管機關。
3. 是否積極配合中央或地方主管機關之調查。
4. 是否以適當方式通知當事人。

（四）其他

1. 是否遵循中央或地方主管機關依個資法規定就同一個人資料外洩案件所為之其他處分或改正情形。
2. 因該個人資料外洩獲有直接或間接之利益。

三、中央或地方主管機關依個資法第二十五條第一項第四款規定為處分時，得公布於該機關網站之個人資料保護專區或其他適當之處，並得輔以發布新聞稿等方式。

四、中央或地方主管機關依個資法第二十五條第一項第四款規定為處分時，應注意依該條第二項規定，於防制違反個資法規定情事之

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，並得考量第二點各款情形後，決定適當之公布期間、移除公布內容之機制或於非公務機關改善後另為補充註記。

五、中央或地方主管機關就其調查確定有違反個資法規定，致個人資料外洩之非公務機關，得單獨為個資法第二十五條第一項第四款之處分。

九、防疫個人資料稽核指引

嚴重特殊傳染性肺炎中央流行疫情指揮中心 111 年 8 月 3 日肺中指字第 1114300137 號函

第一條　嚴重特殊傳染性肺炎中央流行疫情指揮中心(以下簡稱本中心)為協助各上級機關、中央目的事業主管機關、直轄市、縣(市)政府(以下簡稱主管機關)妥適執行監督所轄公務機關或非公務機關(以下皆簡稱機關)蒐集、處理及利用防疫個資作業，特訂定本指引。

第二條　防疫個人資料：指嚴重特殊傳染性肺炎(COVID-19)期間為防疫需要所蒐集、處理或利用之個人資料，如實聯制措施等所系統所蒐集、處理或利用之個人資料。

第三條　各持有防疫個人資料之機關應遵循個人資料保護法之規定落實辦理相關義務，並建立自行查核制度。

第四條　主管機關應規劃稽核作業，得指定所屬單位或機關(以下簡稱稽核單位)負責執行稽核作業，或併現行各項稽核作業辦理，審查個資保護運作情形，其稽核重點應包括下列各項目：

一、蒐集告知義務：稽核單位應查察機關蒐集民眾個人資料時， 是否明確告知民眾蒐集機關之名稱、蒐集之目的、蒐集之個人資料項目、個人資料利用之期間、對象及方式、當事人就其個人資料得依個人資料保護法規定，向蒐集之機關行使權利以及當事人不同意提供個人資料對其權益之影響等事項。

二、個資保存期限：除實聯制資料應參考「COVID-19 防疫新生活運動：實聯制措施指引」(下稱實聯制措施指引)辦理外，其餘防疫個人資料應依個人資料保護法或相關法令規定辦理。

三、安全防護作業：稽核單位應查察機關確實依個人資料保護法， 訂定個人資料安全維護規定，採行適當之技術上或組織上安全措施，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，落實資料安全維護義務。機關若 以資通系統蒐集、處理或利用個資，並應依資通安全管理法規定，辦理安全性檢測及資安防護作業，依系統防護需求採 行對應之控制措施，確保系統安全防護水準。

四、銷毀佐證：稽核單位應查察機關刪除作業之相關佐證資料， 如簽核文件或刪除紀錄等。

第五條　各持有防疫個人資料之機關應每年自行辦理防疫個人資料稽核作業，並製作包含個資管理制度之執行狀況以及稽核後改善計畫之稽核報告，主管機關應督導所屬及所管機關辦理及改善情形，本中心每年得抽查相關稽核作業。