管理顧問業個人資料保護與管理實作

指引手冊

中華民國114年11月

經濟部中小及新創企業署

目錄

壹、前言

立法院於 112 年 5 月 16 日三讀通過個人資料保護法修正案，以促使非公務機關投入人力、技術及成本，落實保護民眾個人資料之責任。

為避免管理顧問業執行業務時，因不諳法律之執行內容，而承擔相關法律責任，特編印管理顧問業個人資料保護與管理實作指引手冊（以下簡稱本手冊），旨在針對管理顧問業實務操作者提供個人資料管理的實務指引。基此，本手冊係從個人資料保護與管理制度整體建置方法著手，納入執行個人資料保護管理時應注意的事項，並透過實際輔導訪查案例說明分析，使讀者更能清楚掌握個人資料保護管理實務之要點。

管理顧問業可參考本手冊之指引，據以針對所蒐集及保有之個人資料，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，以符合個人資料保護法之相關規定。

另外提醒，新修正個人資保護法已於 114 年 11 月 11 日經總統公布，但尚未生效。且因個人資料保護委員會尚未成立，短期內不會施行，故仍以現行有效的個人資保護法為法律依據。建議管理顧問業持續關注新修正個人資保護法的內容及施行日期，滾動式調整個人資料

保護管理制度。

貳、手冊指引

本手冊適用之對象為管理顧問業，係指參考行政院主計總處所訂分類代碼（小類） 為 702，從事提供企業或其他組織有關管理問題諮詢及輔導之行業者。

本手冊依據個人資料保護法（以下簡稱個資法）及個人資料保護法施行細則等規定研擬，內容包括組織的任務分工、個人資料（以下簡稱個資）蒐集處理利用之流程、當事人權利行使、事故預防、通報及應變、認知宣導及教育訓練、個資安全管理、使用紀錄、軌跡資料及證據保存、委外監督、資料安全稽核及持續改善措施等。

本手冊計有實作參考指引、個資事故案例、自我評核作業、常見問題及附錄等五大部分，謹分別說明如下：

一、實作參考指引

本章節以個人資料保護法施行細則第 12 條第 2 項之 11 款安全維護措施為架構，同時導入 PDCA（Plan-Do-Check-Act）方法論，以規劃、執行、檢核及持續改善等方式，建立實作參考指引。而由於個人資料保護法施行細則第 12 條第第 2 項本文規定，相關安全維護措施，係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，故管理顧問業可視本身實際狀況調整之。

二、個資事故案例

本章節介紹三個代表性個資案例，並進行評析，使讀者可從實務案例中學習並進行精進措施。

三、自我評核作業

本章節介紹「管理顧問業個人資料安全自我檢核表」(以下簡稱本表)，以協助並引導管理顧問業因應法規要求與建立個資保護與管理參考，期能透過本表，預先規劃於保護內部個資安全時，所能呈現之具體紀錄、行為，亦可作為對外證明其係具備個資保護能力。

四、常見問題

本章節彙整本署於個資輔導訪查及實務執行上蒐集管理顧問業之常見問題，提供解析說明，使讀者更能清楚掌握個資保護管理之實務運作，並可作為企業內部教育訓練、業務執行之參考及說明，以提升個資管理之正確意識與能力。

五、附錄

本章節提供管理顧問業者有關個資保護之相關文書資料範例與法令依據，以協助業者建立健全之個資保護制度與流程。內容涵蓋以下兩大部分：

（一）實務運用範例

1. 管理顧問業個人資料檔案安全維護計畫（範例）
2. 管理顧問業個人資料安全自我檢核表（範例）
3. 個資事故通知當事人文書（範例）
4. 個人資料蒐集、處理、利用同意書（範例）
5. 個人資料業務委外契約（範例）

（二）法規依據附錄

1. 個人資料保護法
2. 個人資料保護法施行細則
3. 個人資料保護法之特定目的及個人資料之類別
4. 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
5. 個人資料保護法第四十八條第三項「情節重大者」認定之參考原則

上述附錄資料除具完整法令依據，亦兼具實務操作性，以期協助業者落實個資保護與法令遵循。

參、實作參考指引

一、配置管理人員及相當資源

（一）管理顧問業因執行業務而合法蒐集、處理或利用個人資料時，依個人資料保護法施行細則第 12 條第 2 項第 1 款，為有效訂定與執行安全維護計畫，應配置管理之人員及相當資源。

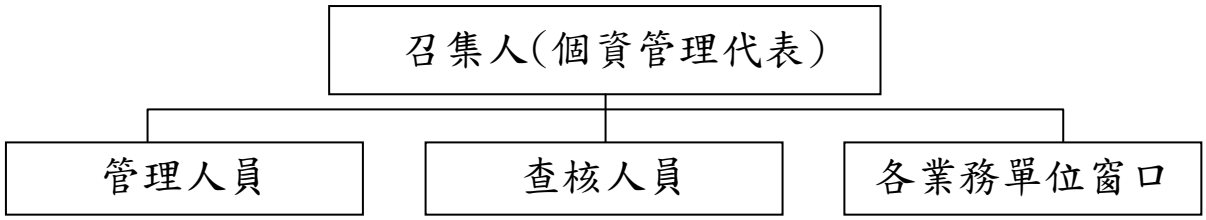
（二）「配置管理人員」是指組織內部應指派管理人員承擔內部個人資料保護的責任，且所負責的個人資料安全維護工作屬於經常性業務。目前我國個資相關規範尚未要求組織必須成立專職個人資料保護與管理之職位（如：資料保護專員、個資長），僅需有管理人員負責組織內部個人資料保護即可。

（三）「配置相當資源」是指組織提供維護及管理個人資料檔案所需要的資源，包括經費及技術支持等。為確實落實個資安全保護，組織應根據自身規模與需求，合理配置人力與資源。若資源配置不足，可能導致保護措施無法充分落實，進而影響整體成效。

（四）實務上，若僅指派少數人進行個資安全維護工作，勢必會有所不足。因此，為落實個人資料保護與管理，規範個人資料蒐集、處理及利用之內部管理程序，並促進個人資料合理利用，可評估制定個人資料保護管理組織架構與權責。另為有效整合各部門個人資料保護運作事宜，可評估設立「個人資料保護管理小組」，負責推動、協調及督導各項個人資料保護相關事宜。

（五）另外，所有作業流程應將個人資料蒐集最小化，僅蒐集適當、相關且限於處理目的必要之個人資料。眾多管理顧問業在疫情時進行數位轉型，並透過資通系統大量蒐集消費者或會員之個人資料。然而卻發生了會員系統或網站因駭客攻擊或資安防護不足，導致個資大量外洩之案件。因此管理顧問業若面臨資源及人力不足時，仍應謹慎評估是否透過資通系統大量蒐集客戶或會員的個人資料。實務上，若蒐集的個人資料越少，發生個資外洩的風險也越小，亦可降低業者投入個資保護措施的資源。

（六）個人資料保護管理小組組成例示(請視本身實際狀況調整)



1. 召集人（個資管理代表）

應由代表人或經其授權之人員擔任，負責核定個人資料保護管理政策、個人資料檔案安全維護計畫之訂定或修正。個資管理代表應為有實權的跨部門管理階層，不宜僅由部門主管擔任，以利全體組織投入資源推展個資管理事務。

2. 管理人員

人數至少一人，負責個人資料檔案安全維護計畫之訂定及執行，並為個人資料保護管理小組之連繫窗口。

3. 各業務單位窗口

由各部門分別指派一人共同組成。負責依個人資料保護管理小組所決議之事項以及制度，推行小組所規劃之個資保護及個資管理制度維運執行作業。

4. 查核人員

由代表人或經其授權之人員指派，且不得與上開 1 至 3 點人員為同一人。負責稽核個人資料檔案安全維護計畫執行情形及成效。

（七）個人資料保護管理小組職掌

1. 管理制度、政策及目標之核定。
2. 審核管理制度之稽核報告與執行成果。
3. 管理責任及資源之分配與協調。
4. 其他整體持續改善機制。

（八）個人資料保護管理小組之召開

1. 每年至少召開一次年度管理審查會議，必要時得召開臨時會議。
2. 由召集人擔任主席，個人資料保護管理小組成員皆應出席。另得依實際作業需求邀請相關人員或外部專家共同與會。

二、界定個人資料範圍並定期確認

（一）依「個人資料保護法施行細則」第 12 條第 2 項第 2 款「界定個人資料之範圍」之規定，業者訂定個人資料蒐集、處理及利用之內部管理程序及個人資料之範圍時，應確認蒐集個

人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍。並應依個人資料保護相關法令，定期查核確認所保有之個人資料現況。

（二）建立個人資料檔案清冊及作業流程說明文件，此一程序主要可協助業者瞭解內部個資蒐集、處理及利用之現況，並藉由程序內之個人資料盤點表，完整清點單位所保有之個人資料檔案，並留存相關紀錄。透過盤點程序，亦能查核所保有個人資料檔案之適法性，以減少違法風險。

（三）個人資料檔案盤點之範圍

1. 所謂「個人資料」，依個資法第 2 條第 1 款規定，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。而所謂「個人資料檔案」，依同法第 2 條第 2 款規定，則係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。

2. 同時，依個人資料保護法施行細則第 5 條規定，個人資料檔案包括備份檔案在內。因此，進行個人資料檔案盤點作業時，亦應將個人資料檔案複製本及備份檔案納入盤點範圍。

3. 進行業務委託時，亦應一併檢視委託事項是否涉及個人資料之蒐集、處理或利用，並將受委託單位因執行分包事項所蒐集、處理或利用之個人資料檔案，納入個人資料檔案盤點範圍。

（四）蒐集、處理及利用個人資料之特定目的

1. 基於業務而蒐集、處理或利用個人資料時，依個人資料保護法第 19 條第 1 項及第 20 條第 1 項規定，應有特定目的，並符合法律規定之要件，於該特定目的必要範圍內為之。執行個人資料檔案盤點時，應參考法務部所頒行「個人資料保護法之特定目的及個人資料之類別」(附錄四)，清查與盤點個人資料蒐集、處理及利用之特定目的，並於盤點清冊上，標明其代號，例如特定目的〇〇一 人身保險、類別C〇〇一 辨識個人者等。

2. 業者若欲將已蒐集、處理及利用之個人資料，為目的外使用時（如：基於舉辦活動目的，取得參加活動者之資料，

原目的僅為處理報名手續，但事後欲利用此個人資料進行行銷)，則必須符合個人資料保護法第 20 條第 1 項但書之情形。

3. 另外，個人資料保護法第 20 條第 2 項與第 3 項亦針對行銷行為特別規定。業者依法利用個人資料進行行銷時，若該當事人表示拒絕接受行銷時，應即停止利用其個人資料來行銷；若未接受到當事人主張停止蒐集、處理及利用其個資，則不受影響。業者首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付相關所需之費用（如：採取書面拒絕行銷之申請時，應支付相關郵寄費用)。

4. 「特定目的」應以實際業務目的臚列即可。若於法務部所公布「個人資料保護法之特定目的及個人資料之類別」未有適合之項目，建議應將蒐集、處理及利用個人資料之特定目的合理且明確闡述。實務上，許多組織將可能用到之特定目的一併匡列，惟過於寬鬆的特定目的，難以讓當事人明白資料蒐集的真正目的，因此以遵循法律的角度而言，建議特定目的應扣合業務執行範圍，避免使用「 … 」或「包含但不限於」等不明確之用語。總而言之，匡列特定目的應以當事人能夠清楚知曉蒐集個人資料之目的為準。

（五）個資盤點方法與範例

1. 實務上個資盤點作法繁多，皆無法保證完全無疏漏，因此進行個資盤點時，建議以分析個資蒐集使用流程著手，盤點出所蒐集、處理以及利用之個人資料。此種方式可較精準地掌握組織蒐集使用個資之狀態，進而減少疏漏並降低漏盤風險。
2. 作業流程識別及個人資料盤點，應配合風險評鑑作業頻率，每年至少執行一次。如遇組織變更、作業流程變更、個資檔案重要異動或發生重大個資保護事故等，個人資料保護管理小組得規劃針對特定範圍，進行作業流程識別及個人資料盤點。

三、建立個人資料風險評估及管理機制

（一）為正確評估並有效管理個人資料檔案可能面臨之風險，業者因執行業務而蒐集、處理或利用個人資料時，依個人資料保護法施行細則第 12 條第 2 項第 3 款規定，應依界定之個人資料範圍及其蒐集、處理、利用個人資料之流程，評估可能產生之個人資料風險，並根據風險評估之結果，訂定適當管控機制。

（二）本程序可藉由經盤點完成之盤點表內容，界定個人資料檔案風險值，並透過風險回應措施，有效採取安全維護措施及應變機制，以降低個資事故發生可能性。

（三）個人資料之風險評估及管理機制，通常可分作「風險評估」及「風險管理」兩部分，前者在於識別導致風險發生之原因，包括瞭解組織或資產本身之脆弱性（弱點）及辨識可能之威脅來源，後者則在於研擬風險對策，有效因應個人資料所面臨之風險。

四、訂定個人資料侵害事故預防、通報及應變作業程序

（一）因執行業務而合法蒐集、處理或利用個人資料時，依個人資料保護法施行細則第 12 條第 2 項第 4 款之規定，應建立個人資料侵害事故之預防、通報及應變機制，使業務執行人員知悉並瞭解相關程序，才能提升人員危機意識及應變能力，確保個人資料侵害事故發生時，能夠立即採取適當措施。

（二）我國個資法規範個資事故之態樣，非僅侷限於竊取，其明定公務機關或非公務機關違反個資法規定，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。對於事故通知當事人之內容應該要明確，包含個人資料被侵

害之事實及所採取之因應措施等。

（三）通知個資當事人可透過言詞、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。當前述通知方式所需花費過鉅時，得斟酌技術之可行性與當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。

（四）訂定之個人資料侵害事故預防、通報及應變作業程序內容至少應包括下列項目：

1. 採取適當措施，控制事故對當事人造成之損害，並於發現事故時起 72 小時內，通報主管機關（本署）。如向地方主管機關通報者，並應副知中央主管機關（本署）。
2. 查明事故發生原因及損害狀況，並通知當事人或其法定代理人，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。
3. 檢討缺失，並訂定預防及改進措施，避免事故再度發生。

五、個人資料蒐集、處理及利用之內部管理程序

（一）企業所屬人員為執行業務而蒐集、處理一般個人資料時，應檢視是否符合個資法第 19 條之要件；利用時，應檢視是否

符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合個資法第 20 條第 1 項但書情形。

（二）蒐集個人資料，應依個資法第 8 條及第 9 條有關告知義務之規定辦理。個資告知聲明應明確包含以下內容，如：機關名稱、蒐集目的、個資類別、個資使用方式及個資當事人權益等。須特別注意，對於蒐集目的說明不應模糊，或以概括方式表述。若告知內容與實際個資蒐集及利用情形不符，將不符合「明確告知」之法定要求。因此，提供給個資當事人之個資聲明，必須因應不同業務內容，調整使用目的說明。

（三）為確保業務執行遵循個人資料利用之最小必要原則，個人資料檔案之主辦業務單位，應逐項確認其保有利用之必要性。如個人資料蒐集之特定目的消失或期限屆滿，除因執行職務所必須或經當事人書面同意得繼續保有利用外，應依規定刪除或銷毀該個人資料。

（四）依據個人資料保護法第 21 條之規定，原則上可將個人資料進行國際傳輸，倘有但書情形，中央目的事業主管機關得依法限制之。為確保當事人個資受到充分保護，將個人資料作國際傳輸時，應該告知該當事人個人資料所欲國際傳輸之區

域，同時對資料接收方進行監督，包括預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式，以及當事人行使個資料法第 3 條所定權利之相關事項。

（五）個資法係採分散式管理，由各中央目的事業主管機關監管各該業別非公務機關之個資保護事項，目前依個資法第 21 條規定公告限制國際傳輸者，計有國家通訊傳播委員會公告限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區、衛生福利部公告限制社會工作師事務所將當事人個人資料國際傳輸至大陸地區、勞動部公告限制人力仲介業將當事人個人資料國際傳輸至大陸地區。本署則尚未針對國際傳輸有公告限制之情形。惟管理顧問業如有將當事人個人資料為國際傳輸之情形，仍應持續關注本署日後是否有公告限制，並遵守相關規範。

（六）個人資料保護法是以當事人隱私自主權為核心，特別重視向當事人揭露相關資訊的義務，故組織應將內部個資指引適當的於組織對外公告之隱私權政策/服務條款揭露。

六、設備安全管理、資料安全管理及人員管理措施

（一）設備安全管理

業者對所蒐集保管之個人資料檔案，應設置適當之安全設備或採取防護措施。安全設備或防護措施，應包括下列事項：

1. 紙本資料檔案之安全保護設施。
2. 電子資料檔案存放之電腦、自動化機器相關設備、可攜式設備或儲存媒體，配置安全防護系統或加密機制。
3. 存有個人資料之紙本或其他儲存媒介物，報廢汰換或轉作其他用途時，應採取適當之銷毀或防範措施。

（二）資料安全管理

業者因執行業務以資通訊系統蒐集、處理或利用個人資料者，應採取下列資訊安全措施：

1. 使用者身分確認及保護機制

帳號密碼應符合一定複雜度，包含：密碼長度、數字、英文大小寫要求，並要求定期更改密碼確保安全。

2. 個人資料顯示之隱碼機制

蒐集、處理或利用個人資料時，如有加密或遮蔽之必要，應採取適當加密或遮蔽機制，避免用戶真實資料遭第三方瀏覽。

3. 網際網路傳輸之安全加密機制

不使用明碼方式傳輸:使用 HTTP 或 FTP 此類未加密協定傳輸資料時，容易被有心人士竊取。應使用高強度加密法，例如傳輸加密機制應使用 Tls1.2 及 Tls1.3，並將 Tls1.0 及 Tls1.1 關閉。

4. 個人資料檔案與資料庫存取控制及保護監控措施

（1）存取權限控制：限制特殊權限帳號方能登入資料庫操作及設定。

（2）監控與日誌紀錄：當資料庫活動異常時，應即時發出告警，並通知相關人員，保存所有資料庫操作紀錄，包含登入、查詢、更改、刪除等。

5. 防止外部網路入侵對策

安裝與建置防毒軟體、防火牆、入侵偵測系統（Intrusion Detection System,IDS）及入侵預防系統

（Intrusion Prevention System,IPS）。防火牆應設定允許存取來源、目的及服務，將非法流量阻擋。入侵偵測系統可透過檢測網路流量，防止外部利用系統漏洞或攻擊手法入侵。網頁防火牆可阻擋針對網頁攻擊（如 SQL Injection）、跨站攻擊及惡意檔案上傳等。

6. 非法或異常使用行為之監控及因應機制

定期確認蒐集、處理或利用個人資料之電腦、相關設備或系統具備必要之安全性，包括但不限採取適當之安全機制，以因應惡意程式及系統漏洞所造成之威脅。例如：定期更新病毒碼與執行掃毒作業、定期針對系統與程式漏洞安裝修補程式，倘遇有重大更新時，應即時安裝修補程式。

7. 針對防止外部網路入侵對策及非法或異常使用行為之監控與因應機制，應定期演練及檢討改善。

（三）人員管理措施

1. 要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。

2. 所屬人員離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂保密切結書。

3. 企業應依據業務作業需要及性質，設定所屬人員不同之權限，並定期檢視所屬人員不同權限之適當性及必要性。

七、認知宣導及教育訓練

（一）依個人資料保護法施行細則第 12 條第 2 項第 7 款之規定，應定期辦理個人資料保護認知宣導及教育訓練，並依照計畫執行人員在計畫範圍及組織內之角色，提供相應之專業教育訓練，以確保負責或協助辦理計畫範圍內個人資料安全維護事項經常性工作之人員，具備辦理安全維護事項能力。所有人員均應接受教育訓練，訓練內容應包括下列事項：

1. 個人資料保護相關法令規定。

如：個資法、個人資料保護法施行施細則等。

2. 所屬人員之責任範圍。

如：個資管理組織成員（個資管理代表、專責人員、查核人員）、資訊人員及接觸個資人員等角色之責任。

3. 內部個人資料保護事項之機制、程序及管理措施。

企業所訂定之個資安全維護計畫及其他內部個資保護程序，例如個資委外管理、個資事故通報、當事人權利行使及個資稽核作業等程序。

（二）實務上在執行時可採取多種作法，以提高所屬人員的個資保護意識，參考作法如下：

1. 定期舉辦宣導個人資料法遵管理相關教育訓練，使成員均知曉個資管理制度內容，以及個資保護之重要性，使個資管理制度得以有效執行。
2. 定期寄發電子報給所屬人員，在例行會議中宣布個資管理政策，或在資訊系統之公共資料夾設置「個人資料保護專區」等方式，強化個資保護認知宣導效果。
3. 個資保護相關教育訓練，除可自行培訓講師外，亦可委託外部專家講習，或指派企業內相關成員參與外部訓練等方式進行。
4. 辦理個資保護相關教育訓練或講習時，應留存相關紀錄，如課程簽到表及測驗成績等，以利後續稽核時能提出辦理宣導及教育訓練之佐證。

八、個人資料安全維護稽核機制

（一）因執行業務而合法蒐集、處理或利用個人資料時，依個人資料保護法施行細則第 12 條第 2 項第 9 款之規定，應指定資料安全稽核之查核人員，定期稽核安全維護計畫之執行情形及成效，並將稽核結果，向企業之代表人或經其授權之人員提出稽核結果報告。如有發現不符合事項時，應予以紀錄及追蹤，分析缺失發生之原因，採取矯正或預防措施，以改善個人資料安全維護計畫之有效性和效率。

（二）為確保查核制度獨立及確實執行，企業指定之專責人員與本條規定之查核人員，不得為同一人。

九、個人資料安全維護之整體持續改善

（一）因執行業務而合法蒐集、處理或利用個人資料時，依個人資料保護法施行細則第 12 條第 2 項第 11 款之規定，應參酌相關因素，依據實務運作及法令變化等情形，檢視或修正安全維護計畫，進行滾動式調整，以求實踐個人資料保護之相關政策及機制，達個人資料安全維護之整體持續改善之成果。

（二）企業所定個人資料安全維護之整體持續改善方案，每年應參酌安全維護計畫執行狀況、技術發展、法令修正或其他因素，檢視所定安全維護計畫之合宜性，必要時應予修正。

十、使用紀錄、軌跡資料及證據保存

（一）管理顧問業應留存個人資料使用紀錄、軌跡資料或相關證據及紀錄，原則上至少留存 5 年。但法令另有規定或契約另有約定者，不在此限。

（二)應至少留存5年之目的為證明企業已確實執行安全維護計畫，善盡防止個人資料遭侵害之義務。依個人資料保護法第 30 條「損害賠償請求權，自請求權人知有損害及賠償義務人時起，因 2 年間不行使而消滅；自損害發生時起，逾 5 年者，亦同。」因此建議管理顧問業留存使用紀錄、軌跡資料及相關證據資料,且至少應留存 5 年,以供日後發生爭議時佐證。

（三)是以，企業對於個人資料之使用紀錄、軌跡資料及證據保存，應訂定相關機制並予以落實。本處所指機制應包含，為執行個人資料檔案安全措施，所紀錄之個人資料使用情況、軌跡資料及相關證據。規範標的是指個資的使用紀錄、軌跡資料及證據，非指個資本體而言。

十一、業務終止後之個人資料處理方法

（一）合法蒐集、處理及利用消費者個人資料之特定目的消失或期限屆滿時，依據個人資料保護法第 11 條第 3 項之規定，業者應主動或依個人資料當事人之請求，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。

（二）另外，業者於業務終止後，自不得再繼續使用其所保有之個人資料檔案，並應作妥善處置。業者應視其終止業務之原因，將所保有之個人資料予以銷毀、刪除、移轉或其他停止處理或利用等方式處理，並於處理過程中，保存處理方法、地點、時間、執行人員、接受移轉資料之對象及合法移轉依據等資料，以便日後得以提出佐證。

（三）依個資法第 30 條規定「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 2 年間不行使而消滅；自損害發生時起，逾 5 年者，亦同。」爰建議銷毀、移轉、刪除、停止處理或利用個人資料之紀錄至少應留存 5 年。規範標的是指個資的銷毀、移轉及刪除措施等資料，而非個資本體。

（四）以上規範與個人資料本體（如當事人報名活動所留存姓名、連絡方式等個人資料）的保存無關。個人資料保存應有一定期限，企業應依照該個人資料性質訂定。若有法定保存期間之規定，需依照法定保存期間保存以符合法規要求，或由企業自訂之保存期限進行保存，例如舉辦抽獎活動，就活動參與人之個資（個資本體），可訂於活動結束後銷毀。

（五）實務運作上，在銷毀個人資料及其相關載體時，可製作銷毀清冊，於清冊上載明銷毀之標的、數量、時間、作法及執行單位，並經權責主管覆核，以作為存證紀錄，以供日後查核之佐證。

十二、個人資料委外處理管理程序

（一）依據我國個人資料保護法施行細則第 8 條之規定，具體要求業者委託他人蒐集、處理或利用個人資料時，應對受託人為適當之監督，並於委託契約或相關文件中，明確約定其內容，以確保受託人蒐集、處理或利用個人資料符合相關法令要求。

（二）依據個人資料保護法第 4 條規定，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。另依人資料保護法施行細則第 7 條之規定，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。因此，應於委託契約或相關文件要求受委託廠商於蒐集、處理或利用個人資料時，於個人資料保護法適用範圍內，視同委託機關，應遵守委託機關應適用之規定。

（三）委託他人蒐集、處理或利用個人資料時，應訂定委託契約或相關文件，並明確約定雙方權利義務及對受託者為以下適當監督之事項：

1. 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。
2. 受託者就個人資料保護法施行細則第 12 條第 2 項採取之措施。
3. 有複委託者，其約定之受託者。
4. 受託者或其受僱人違反個人資料保護法、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。
5. 委託機關如對受委託者有保留指示者，其保留指示之事項。
6. 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。

7. 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。

8. 受託者認委託機關之指示有違反個人資料保護法、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。

（四）委外流程控管步驟

1. 步驟一：選擇受託人

以適當評估方式選擇具品質廠商（如委外廠商執行業務安全評估表），評估項目可包含廠商員工數、資料處理方式、委託資料之價值（機密性）、服務內容及存取系統重要性等。

2. 步驟二：締結委託契約

契約可包含如下內容：應遵守委託人之指示與個資法之要求，除為確保資料正確處理之備份外，不得擅自進行資料重置，受託人應依據委託人之書面指示進行當事人權利之回覆、受託人應於個資事故發生時立即通知委託人、受託人應採取適當之技術與組織上之措施以確保資料安全、關於複委託之約定及委託人保有監督權等。

3. 步驟三：監督受託人

委託他人蒐集、處理或利用個人資料時，應定期確認受託者執行之狀況，並將確認結果(含追蹤改善)記錄之。委託人可採用實地稽核或請受託人填寫相關評核表之方式進行監督控管。評核要項可包含管理資源是否充足、是否有效進行個資盤點、是否有效落實風險評估、事故應變程序、蒐集處理利用之內部管理程序、資料安全管理、人員管理、認知宣導與教育訓練是否充足、設備安全管理、稽核機制、記錄保存及持續改善之情形等。

4. 步驟四：終止後的處理

委託終止後，應要求委外廠商將受託的個人資料銷毀或返還，並提供相關佐證。

（五）委託作業常見問題

1. 有委託他人蒐集、處理或利用個人資料之情形，但未訂定委託契約。
2. 契約內容未包含個資保護條款。
3. 相關人員未簽具保密切結書。
4. 未依據個人資料保護法施行細則第 7 條、第 8 條訂定相關條款。

5. 未定期確認委外廠商個人資料保護執行情形，如：委外查核。

6. 契約終止後，未要求委外廠商將受託的個人資料銷毀或返還。

肆、個資事故案例

一、○○管理顧問經當事人請求刪除個人資料疑未處理一案

案例說明：

當事人檢舉○○業者，自從接到○○業者的第一通行銷電話開始，就已經要求將個資刪除，但陸續接到至少三通電話，且該公司皆未能提供個資刪除的佐證資料。

案例評析：

依據個資法第 3 條規定，當事人就其個人資料依本法規定得行使之下列權利，且不得預先拋棄或以特約限制之：四、請求停止蒐集、處理或利用。五、請求刪除。另依第 11 條第 3 項規定，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。

而根據臺灣士林地方法院內湖簡易庭 103 年度湖小字第 537 號判決指出，非公務機關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。而本案被告因個資當事人於表示拒絕接受行銷後，未即停止利用其個人資料行銷，違反個資法而遭法院判賠。

另業者是否已就當事人之請求將個資刪除，即是否依據個資法第27條第1項規定，就保有個人資料檔案者採行適當之安全措施？以及是否有個資法第 29 條無故意或過失之情形？參考臺灣臺北地方法院106 年度北小字第 2161 號判決、臺灣臺北地方法院 111 年度訴字第5578號、臺灣高等法院112年度上字第656號等判決意旨，法院皆要求應由保有個人資料檔案之非公務機關負舉證責任，故○○業者，應就當事人請求將個資刪除，即是否依據個資法第27條第1項規定，就保有個人資料檔案者採行適當之安全措施負相關舉證責任。

因此，建議業者，在銷毀當事人個人資料時，可製作銷毀清冊，於銷毀清冊上載明銷毀之標的、數量、時間、作法及執行單位，並經權責主管覆核，以作為存證紀錄，以供日後發生爭議時，提出佐證。

二、○○管理顧問業經當事人檢舉違法蒐集個資一案

案例說明：

當事人認為○○業者違法蒐集其個人資料，因向主管機關檢舉，並要求吊銷○○業者的公司執照。雖然○○業者提出係拼湊公開資訊進行交叉比對而推測出當事人的個人資料，惟經主管機關調查後發現，○○業者不僅未能提出證明如何推測出當事人之個人資料，且拼湊出的推測作法，亦無法確保當事人個人資料的正確性，如果僅憑推測而將其個資利用作為廣告寄送使用，還可能發生寄錯人的情形，並衍生其他紛爭。

案例評析：

個人資料保護法第 5 條規定，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。

本案中○○業者，基於行銷之目的，拼湊公開資訊進行交叉比對而推測出當事人的個人資料，並發送廣告信件的作法，且於信件中提及當事人姓名、房產及貸款資訊等敏感性個人資料，卻又未揭露資訊來源。對於當事人而言，直覺是透過非法管道竊取個資之行為，難謂

尊重當事人之權益，而依誠實及信用方法為之作法。故而引起當事人之反感，進而向主管機關檢舉。

就算退萬步而言，業者認為拼湊公開資訊進行交叉比對而推測出當事人的個人資料，應符合個人資料保護法第 19 條第 1 項第 3 款後段「其他已合法公開之個人資料」，但如需進行處理或利用，仍應尊重當事人之權益，依誠實及信用方法為之，至少應誠實告知當事人資料之來源及當事人對於個人資料之蒐集、處理或利用之申訴管道，以免當事人對業者檢舉或起訴。

三、○○管理顧問業於首次寄送廣告信件時未提供當事人表示拒絕接受行銷之方式

案例說明：

○○業者於首次寄送廣告信件時，雖然提供聯絡電話及 LINE 聯絡方式，但未依個人資料保護法第 20 條第 3 項之規定，提供當事人表示拒絕接受行銷之方式，經當事人向主管機關檢舉。經主管機關調查後對○○業者作出行政處分，要求針對不符合「於首次行銷時，應提供當事人表示拒絕接受行銷之方式」之行為限期改正，倘未於期限內回覆或改正不完全者，將依個資法第 48 條與第 50 條規定，視情節裁罰。

案例評析：

實務上，許多業者於首次寄送廣告信件給當事人時，往往便宜行事，僅提供連絡方式，而未依據個人資料保護法的規定，告知當事人表示拒絕行銷的方式。依據個人資料保護法第 20 條第 2 項及第 3 項規定：「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」。

由於現在民眾對於隱私權的保障相當重視，因此，建議業者應於首次寄送廣告信件給當事人時，明確告知當事人表示拒絕接受行銷之方式，以免遭到當事人檢舉或起訴。

伍、自我評核作業

參照本手冊附錄一、參考範例中範例二之「管理顧問業個人資料安全自我檢核表」，提供業者個人資料保護與管理之基礎要求，以協助引導業者因應法規要求與建立個資保護與管理參考，並鼓勵自主管理，期能透過本表，考量營運風險與需求，進而訂定符合營運現況之個人資料保護與管理制度。業者可透過本表，預先規劃於保護內部個人資料安全時，所能呈現之具體紀錄、行為，亦可作為對外證明其係具備個資保護能力，並積極投入的表現。

一、目的

本表旨在提供管理顧問業個人資料保護與管理之基礎要求，以法令遵循為主，協助並引導管理顧問業因應法規要求與建立內部個資保護與管理制度。因性質係引導並鼓勵管理顧問業自主管理，建議管理顧問業可參考本表，但不以此為限，可通盤考量營運風險與業務發展，訂定符合管理顧問業本身營運需求之個人資料保護與管理制度。

二、使用對象

依行政院主計總處之分類為管理顧問業，行政院主計總處分類代碼(小類) 為 702 者。

三、如何使用本表

（一）填寫本表時，建議管理顧問業內部由負責業務之主管、法務、資訊與相關管理人員共同填寫，以對主管機關法令規範之遵循及個人資料保護與管理制度有更深入了解。

（二）本表填寫步驟如下：

1. 依序由第 1.1 款填寫至第 12.2 款，一共 47 款檢核項目，以本表之稽核內容為基準，並可參考「備註」欄位，了解本查核項之具體內容或程序文件範例，比對管理顧問業本身現行個人資科保護與管理措施作法，將比對後之結果作為判斷之依據，擇一勾選符合程度（「符合」／「不符合」／「不適用」欄位），並將相關說明及證明文件及紀錄填寫於填寫於「說明」欄位。

2. 填寫本表時，可併參酌「個人資料保護法」及「個人資料保護法施行細則」等規範。

陸、常見問題

Q1. 蒐集個資的企業違反個資法的風險為何？

一、政府對業者個資保護已改採「主動監理」的積極管理作為

歷程一、行政精進措施，加強行政檢查的力道

行政院於 112 年 3 月下達的「行政院防止非公務機關個資外洩精進措施」，其中明定中央目的事業主管機關應成立常設之個資行政檢查小組，並擬定年度行政檢查計畫，將高風險業者評估優先列入加強檢查對象。在今年已經有許多業者受到主管機關之行政檢查，未來每年主管機關都將持續進行相關工作，各家業者，尤其是保有個資數量較多、曾發生個資外洩事件或被通報為 165 平台上的高風險業者，都可能接受行政檢查的風險。

歷程二、立法院修法，提高罰鍰

此外，為促使非公務機關投入人力、技術及成本，落實保護民眾個人資料之責任，並有助於政府打擊詐欺相關政策推動。「個人資料保護法」修正案於 112 年立法三讀通過並於 6 月 2 日起生效。本次修法將非公務機關違反安全維護義務由先命其限期改正，屆期未改正始處罰鍰，改為逕行處罰同時命改正，並提高罰鍰金額最重可至 1,500 萬元，屆期未改正者並可按次處罰。

三、企業違反個資法規定的民事、刑事及行政責任

非公務機關違反個資法規定之民事損害賠償責任			
賠償責任	**賠償金額**	**最高賠償總額**	**備註**
非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。(第 29 條第 1 項)	如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。(第 28 條第 3 項)	對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。(第 28 條第 4 項)	如為被害人有實際財產的損害額時(例如企業外洩被害人之個資，遭詐騙集團利用對被害人詐騙，導致個資當事人被詐騙特定金額)，被害人可就實際損害額範圍，請求損害賠償。(第 28 條第 1 項)

非公務機關違反個資法規定之刑事責任	
違反事項	**刑事責任**
特種個資之蒐集、處理或利用(第 6 條第 1 項)	五年以下有期徒刑，得併科新臺幣一百萬元以下罰金（第 41 條）
非公務機關違反蒐集、處理之特定目的、法定情形之規範(第 19 條)	
非公務機關違法利用或特定目的外利用個資(第 20 條第 1 項)	
國際傳輸限制(第 21 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(第 42 條)	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 42 條)

非公務機關違反個資法規定之行政責任		
違反事項	**行政責任**	**備註**
特種個資之蒐集、處理或利用(第 6 條第 1 項)	新臺幣五萬元以上五十萬元以下罰鍰（第 47 條）	第 25 條第 1 項 非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣（市）政府除依本法規定裁處罰鍰外，並得為下列處分： 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、沒入或命銷燬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
非公務機關違反蒐集、處理之特定目的、法定情形之規範(第 19 條)		
非公務機關違法利用或特定目的外利用個資(第 20 條第 1 項)		
國際傳輸限制(第 21 條)		
直接／間接告知義務(第 8、9 條)	新臺幣二萬元以上二十萬元以下罰鍰(第 48 條第 1 項）	
當事人請求答覆查詢、提供閱覽或製給複製本(第 10 條)		
維護個人資料之正確性、應刪除、停止處理或利用個人資料之情形(第 11 條)		
個資侵害事故通知當事人(第 12 條)		
受理當事人權利行使之處理期限(第 13 條)		
個人資料行銷(第 20 條第 2、3 項)		

規避、妨礙或拒絕中央目的 事業主管機關之行政檢查(第 22 條第 4 項)	新臺幣二萬元以上二十萬元以下罰鍰（第 49 條）	名或名稱與負責人。 第 50 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。
未採行適當之安全措施、未採行中央目的事業主管機關指定之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者(第 27 條第 1、2 項)	新臺幣二萬元以上二百萬元以下罰鍰，情節重大者，新臺幣十五萬元以上一千五百萬元以下罰鍰（第 48 條第 2 項、第 3 項）	

Q2. 管理顧問業應如何著手建立個資保護與管理制度？

一、參考本手冊初步進行自評

可先初步依附錄二「管理顧問業個人資料安全自我檢核表」進行自評，評估組織目前的個資防護措施是否足夠以及法遵上的差異，也可同步或再評估是否有委請外部專家顧問進行輔導的需要，如掌有大量消費者個資者，建議評估進一步取得適當之個資及資安管理制度證書。

二、進立完整的個資保護與管理制度步驟如下：

（一）現況診斷與差異分析

透過本手冊「伍、 自我評核作業」先初步進行自評，檢視組織現有個人資料保護制度、組織業務運作特性或文件表單等進行差異分析。

（二）建立個資管理系統文件

透過本手冊「貳、手冊指引」，因應組織之業務運作特性，客製化製作屬於組織內之個人資料管理制度文件，包含個人資料保護政策、管理程序書、工作指導書、文件表單及紀錄。

（三）制度輔導落實與內部稽核

依照組織所制訂管理文件落實整體個資制度，包含個資流程識別、個資外洩事故演練、當事人行使權益、教育訓練、相關活動之執行紀錄，透過內部稽核作業檢視制度落實程度及驗收成果。

（四）外部稽核並取得證書

未來可考量透過第三方驗證機構執行個人資料管理制度（PIMS）驗證、稽核作業，取得 BS 10012 或 ISO 27701 等國際標準的證書或臺灣個人資料保護與管理制度（Taiwan Personal Information Protection and Administration System, TPIPAS）證書。如有透過資通系統大量蒐集、處理及利用交易相對人或會員個人資料之情形，建議可同時取得資訊安全管理制度(ISMS)，例如 ISO 27001 的證書。

Q3. 業者兼營兩種以上經主管機關分別訂有個資安維辦法之行業，應如何適用相關個資安維辦法？

一、按個人資料保護法(下稱個資法)非公務機關之中央目的事業主管機關之判準，應以具體個案中非公務機關蒐集、處理或利用個人資料之實際業務所涉行業為斷，再由該目的事業主管機關本於權責採取適當之監督管理措施，始能落實個資保護之執行，若同一法人主體所經營數項事業係不同「目的事業」，則「一併監督管理與其業務相關之個人資料保護事項」，宜由原各該主管機關為之(法務部 105 年 9 月 7 日法律字第 10503511140 號函意旨參照)。

二、是以，同一法人主體所營數項目的事業，若各該目的事業主管機關訂有個資安維辦法亦應適用之。

Q4. 個資法第 50 條規定，於非公務機關授權代表人以外之人辦理個資安維計畫事宜者，應如何適用一節？

一、機關授權代表人以外之人辦理個資安維計畫事宜者，應如何適用一節，按非公務機關之代表人、管理人或其他有代表權人，對於該非公務機關，本有指揮監督之責(個資法第 50 條立法理由參照)。

二、次按個資法第 50 條規定係參照行政罰法第 15 條、第 16 條規定而來，故上開條文所稱「代表人」、「管理人」或「其他有代表權人」係指該人具有指揮監督非公務機關之權責，非指個人資料之管理人或非公務機關授權辦理個資安維計畫事宜之人(法務部 102 年 6 月 5 日法律字第 10203503410 號函附件編號 15 參照)

(國家發展委員會 112 年 8 月 10 日發法字第 1120013043 號函參照)

Q5. 外國公司在臺分公司是否適用相關個資安維辦法？

個資法所稱非公務機關，依屬地原則，不論我國人或外國人在我國領域內有違反個資法之行為，應適用我國個資法之規定，是以，若外國企業至我國領域內蒐集、處理或利用個人資料(包括在臺灣設分公司)，自應有我國個資法之適用(法務部 102 年 6 月 6 日法律字第 10100088140 號函意旨參照)。

(國家發展委員會 112 年 8 月 10 日發法字第 1120013043 號函參照)

柒、附錄

一、參考範例

範例一：管理顧問業個人資料檔案安全維護計畫(範本)

(管理顧問業名稱)個人資料檔案安全維護計畫(範本)

訂定(或修訂)日期：中華民國○○○年○○月○○日

**範本內容僅供參考，請依個人資料保護相關法規、內部管理作業程序及實際業務情形訂定貴公司（商業）之個人資料檔案安全維護計畫。

壹、依據

個人資料保護法第27條第3項。

貳、目的

落實個人資料檔案之安全維護及管理，防止被竊取、竄改、毀損、滅失或洩漏。

參、公司規模及特性

一、負責人：○○○

二、地址：○○

三、員工人數：約○○人

四、保有個人資料數量(含員工/廠商/客戶等)：約○○筆

五、主要業務/營業項目：

肆、個人資料檔案之安全維護管理措施

一、配置管理之人員及資源

（一）管理人員：

1. 管理代表：由本公司代表人授權擔任，負責核定本計畫及相關事項之訂定或修正。
2. 專責人員：○○人(至少1名)。負責規劃、訂定、修正及執行本計畫及相關事項，並每○○日(或週、月、年)向管理代表提出報告。
3. 查核人員：○○人(至少1名)。負責每○○日(或週、月、年)稽核本計畫執行情形及成效。

（二）預算：每年約新臺幣○○元。（註：包含管理人員薪資、設備費用等，請依貴團體實際狀況填寫）

二、蒐集、處理及利用個人資料之範圍及特定目的

（一）個人資料範圍：

本計畫所稱之個人資料，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）特定目的：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿等運用。

(註：本項請依「個人資料保護法之特定目的及個人資料之類別」，說明特定目的項目。)

三、個人資料之風險評估及管理機制

（一）風險評估

1. 經由本公司電腦下載或外部網路入侵而外洩。
2. 經由接觸涉有個人資料之業務書件而外洩。
3. 員工及第三人竊取、毀損或洩漏。
4. 業間互為傳輸時之外洩（包括分公司間傳輸、與相關業者間傳輸等）
5. ○○。(註：倘經評估有其他風險，請自行增列。)

（二）管理機制

1. 適度設定所屬人員權限，並妥適保管文件。
2. 每○○日(或週、月、年)進行網路資訊安全維護及控管。
3. 電子檔案資料視實際需要以加密方式傳輸。
4. 加強對員工之管制及設備之強化管理。
5. ○○。(註：可依貴公司實際情形自行調整或增列。)

四、事故之預防、通報及應變機制

（一）預防：

1. 指定人員辦理安全維護事項，防止本公司保有之個人資料被竊取、竄改、毀損、滅失或洩漏。
2. 本公司保有之個人資料檔案，限承辦人員使用或存取，使用或存取範圍限與其本身業務相關，且存取檔案時須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之。非承辦人員參閱、使用或存取相關個人資料檔案或書件時，應經負責人或經授權之管理人員同意。
3. 存有個人資料之儲存媒體(含可攜式媒體)，視必要性採取適當之加密機制；存有個人資料之紙本文件於不使用或下班時，遵守桌面淨空，置於抽屜或儲櫃並上鎖。
4. 存有個人資料之紙本及存放媒介物於報廢汰換或轉作其他用途前，確實刪除資料或格式化，或採物理方式破壞、銷毀。
5. 電腦系統安裝防毒軟體並定期更新病毒碼，避免惡意程式與系統漏洞對作業系統之威脅。
6. 對內或對外從事個人資料傳輸時，加強管控避免外洩。
7. 加強所屬人員教育宣導，並嚴加管制。
8. ○○。(註：可依貴公司實際情形自行調整或增列。)

（二）通報及應變：

1. 所屬人員發現個人資料遭竊取、竄改、毀損、滅失或洩漏等安全事故時，即時向○○(請填負責人或管理組織名稱)通報；發生安全事故，自發現時起72小時內，以「個人資料事故通報及紀錄表」通報經濟部中小及新創企業署。
2. 發生個人資料安全事故時，儘速以適當方式通知當事人事故發生之事實、已採取之處理措施以及本公司窗口電話等資訊。
3. 發生個人資料安全事故後，針對事故發生原因研議改進措施。
4. 定期(每年至少1次)就個人資料安全事故進行演練及提出檢討改善報告。演練流程應包含通知當事人及通報主管機關。
5. ○○。(註：可依貴公司實際情形自行調整或增列。)

五、個人資料蒐集、處理及利用之內部管理措施

（一）直接向當事人蒐集個人資料時，明確告知當事人以下事項：

1. 公司（商業）名稱。
2. 蒐集目的或其他特定目的。
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. 當事人得請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。
6. 當事人得自由選擇提供個人資料，以及如不提供對其權益之影響。

（二）所蒐集之個人資料非由當事人提供者，應於處理或利用前，向當事人告知其個人資料來源及前項應告知之事項，若當事人表示拒絕提供，應立即停止處理、利用其個人資料。

（三）另本公司保有之個人資料利用期限屆滿時，除因法令規定、執行業務所必須或經當事人書面同意者外，將主動刪除或銷毀其個人資料，並留存相關紀錄。

（四）當事人得向本公司表示拒絕提供，或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料之聯絡窗口為○○○；聯絡電話：○○○○○○。並將聯絡窗口及電話等資料，揭示於本公司（商業）營業處所或網頁。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。

（五）負責保管及處理個人資料檔案之人員，其職務有異動時，應將所保管之儲存媒體及有關資料檔案移交，以利管理。

（六）本公司（商業）員工如因其工作執掌相關而須輸出、輸入個人資料時，須鍵入其個人之使用者代碼及識別密碼，並須在使用範圍及使用權限內為之。識別密碼應保密，不得洩漏或與他人共用。

（七）由指定管理人員每○○日(或週、月、年)清查所保有之個人資料是否符合特定目的，若有非屬特定目的必要範圍之資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置，並留存相關紀錄。

（八）本公司有之個人資料如需作特定目的外利用，應先行檢視是否符合個人資料保護法第20條第1項但書之規定。

（九）本公司（商業）如有委託他人蒐集、處理或利用個人資料時，當對受託者為適當之監督並與其明確約定相關監督事項。

（如未委託他人則可以選擇加以刪除）

（十）本公司（商業）因故終止業務時，原保有之個人資料，即依規定不再使用，並採銷毀、移轉或其他妥適方式處理。

（十一）○○。(註：可依貴公司（商業）實際情形自行調整或增列。)

六、設備安全管理、資料安全管理及人員管理措施

（一）設備安全管理

1. 建置個人資料之有關電腦設備，資料保有單位應定期保養維護，於保養維護或更新設備時，並應注意資料之備份及相關安全措施。
2. 建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。
3. 應指派人員管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經單位主管同意並作成紀錄不得攜帶外出或拷貝複製。
4. 本公司（商業）保有之個人資料檔案應定期(例如：每二週)備份。
5. 電腦、自動化機器或其他存放媒介物需報廢汰換或轉作其他用途時，本公司（商業）負責人或營業處所主管應檢視該設備所儲存之個人資料是否確實刪除。
6. 電腦設備報廢或不使用時，確實刪除電腦硬體設備中所儲存之個人資料檔案。
7. ○○。(註：可依貴公司（商業）實際情形自行調整或增列。)

（二）資料安全管理

1. 電腦存取個人資料之管控：

（1)本公司(商業)所屬員工應妥善保管個人電腦存取資料之硬體，並設定登入及螢幕保護程式密碼。個人資料使用完畢，應即退出電腦使用檔案,不得留置於電腦上。下班前應關閉電腦電源，並將所保有其他個人資料之媒介物置於專用抽屜內上鎖保管。

（2）本公司（商業）員工如因其工作職掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

（3)個人資料檔案使用完畢應即退出，不得任其停留於電腦終端機上。

（4）定期進行電腦系統防毒、掃毒之必要措施。

（5）重要個人資料（如護照號碼、國民身分證統一編號）應另加設管控密碼，非經陳報公司（商業）主管核可，並取得密碼者，不得存取。

（6）建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。

（7）○○。(註：可依貴公司（商業）實際情形自行調整或增列。)

2. 紙本資料之保管：

（1）本公司（商業）保有個人資料存在於紙本者，應存放於公文櫃內並上鎖，員工非經公司（商業）主管或負責人或業務主管同意不得任意複製或影印。

（2）對於記載個人資料之紙本丟棄時，應先以碎紙設備進行處理。

（3）○○。(註：可依貴公司（商業）實際情形自行增列。)

（三）人員管理

1. 本公司（商業）依業務需求，應適度設定所屬員工(例如主管、非主管員工)不同之權限，以控管其個人資料之情形。
2. 本公司（商業）所屬人員使用電腦設備蒐集、處理、利用個人資料，應以專屬帳號密碼登入電腦系統，存取個人資料檔案權限應與所職掌業務相符。專屬帳號密碼均應保密，不得洩漏或與他人共用。
3. 本公司（商業）員工每天（週、月）應變更識別密碼乙次，並於變更識別密碼後始可繼續使用電腦。
4. 本公司（商業）員工應妥善保管個人資料之儲存媒介物，執行業務時依個人資料保護法規定蒐集、處理及利用個人資料。
5. 本公司（商業）與員工所簽訂之相關勞務契約列入保密條款及相關之違約罰則，以確保其遵守對於個人資料內容之保密義務（含契約終止後）。
6. 對於新進員工應特別給予指導，務使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

7. 負責個人資料檔案管理人員於職務異動時，應將保管之檔案資料移交，接辦人員應另行設定密碼。
8. ○○。(註：可依貴公司（商業）實際情形自行調整或增列。)

七、認知宣導及教育訓練

（一）每年派遣所屬人員○人參與相關單位辦理之個人資料保護法宣導或數位學習教育訓練至少○小時(或每年自行辦理個人資料保護法基礎認知宣導及教育訓練○次，請依貴團體實際情況填寫)。參加或自辦教育訓練應留存相關紀錄或佐證資料（例如：簽到表、課後評量結果或照片等佐證資料）。

（二）對於新進人員給予特別指導，確保其明瞭個人資料保護相關法令規定及責任範圍及應遵守之相關管理措施。

（三）○○。(註：可依貴公司（商業）實際情形自行增列。)

八、個人資料安全維護稽核機制

（一）本公司（商業）定期(每年至少乙次)辦理個人資料檔案安全維護稽核，查察本公司（商業）是否落實本計畫規範事項，檢查結果向負責人(或管理組織)提出報告，相關文件至少保存5年。

（二）若檢查結果不符合法令或有不符合法令之虞，依下項事項規劃改善措施：

1. 確認不符合法令之內容及發生原因。
2. 提出改善及預防措施方案。
3. 紀錄檢查情形及結果。

（三）○○。(註：可依貴公司（商業）實際情形自行調整或增列。)

九、使用紀錄、軌跡資料及證據保存

本公司（商業）建置個人資料之電腦，其個人資料使用查詢紀錄，每年需將該紀錄檔備份並設定密碼，另亦將儲存該紀錄之儲存媒介物保存於適當處所以供備查。

(註：本項請依實際情形說明業者如何保存，例如：個人資料使用查詢紀錄、自動化機器設備之軌跡資料(電腦設備或其他相關之證據資料須加以保存並製作備份保存於適當處所，以供必要時說明其所訂計畫之執行情況。)

十、個人資料安全維護之整體持續改善

（一）本公司（商業）將隨時依據計畫執行狀況，注意相關技術發展及法令修正等事項，檢討本計畫是否合宜，並予必要之修正。

（二）針對個資安全稽核結果不符合法令之虞者，規劃改善與預防措施。

十一、業務終止後之個人資料處理方法

本公司（商業）結束營業後，所保有之個人資料不得繼續使用，並依實際情形採下列方式處理，並留存相關紀錄至少五年（請勾選或填寫下列事項）：

（一）銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

□書面個人資料已送碎紙機絞碎。

□儲存於電腦磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物之個人資料已格式化刪除資料或以物理方式破壞其功能，如折斷光碟片、擊毀硬碟等。

□其他：（請自行填寫）

以上行為請拍照存證（照片需印日期並揭露地點）或錄影存證（影片需有日期並揭露地點）。

（二）移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

移轉之原因：

□業務需求

□其他（請自行填寫）：

移轉之對象：

移轉之方法：

□紙本傳遞。

□以電腦磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物傳遞。

□其他（請自行填寫）：

移轉之時間（請自行填寫）：中華民國___年___月___日

移轉之地點（請自行填寫）：

受移轉對象得保有該項個人資料之合法依據：

（三）其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

其他刪除、停止處理或利用之方法（請自行填寫）：

其他刪除、停止處理或利用之時間（請自行填寫）：

其他刪除、停止處理或利用之地點（請自行填寫）：

十二、附表：個人資料侵害事故通報及紀錄表

<table>
<tr><td colspan="3">個人資料侵害事故通報與紀錄表</td></tr>
<tr><td rowspan="5">事業名稱
_____
通報機關
_____</td><td colspan="2">通報時間：　年　月　日　時　分</td></tr>
<tr><td colspan="2">通報人：　　簽名(蓋章)</td></tr>
<tr><td colspan="2">職稱：</td></tr>
<tr><td colspan="2">電話：</td></tr>
<tr><td colspan="2">Email：
地址：</td></tr>
<tr><td>事件發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="6">事件發生種類</td><td>□竊取</td><td rowspan="3">個資侵害之總筆數(大約)
_____</td></tr>
<tr><td>□洩漏</td></tr>
<tr><td>□竄改</td></tr>
<tr><td>□毀損</td><td rowspan="3">□一般個資_____筆
□特種個資_____筆</td></tr>
<tr><td>□滅失</td></tr>
<tr><td>□其他侵害事故：___</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>個資侵害可能結果</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時起算七十二小時內通報</td><td colspan="2">□是　□否，理由：</td></tr>
</table>

註1：各欄位資訊若尚未明確，得先填寫「不明」，並俟明確後再通報更新。

註2：上開七十二小時通報主管機關，例假日均納入時效計。

範例二：管理顧問業個人資料安全自我檢核表(範本)

管理顧問業個人資料安全自我檢核表

_____(填表單位)

**範本內容僅供參考，請依個人資料保護相關法規、內部管理作業程序及實際業務情形訂定貴公司（商業）之個人資料檔案安全維護計畫。

填表說明：

一、自我檢核結果欄：依自我檢核實際狀況，併相關佐證資料填具自我檢核結果。

（一）符合：實際作業已依自我檢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：未依自我檢核內容要求制定相關程序，或未依相關程序執行並產生實作紀錄。

（三）不適用：實際作業排除自我檢核內容之適用。

二、說明欄位：應記錄自我檢核之參考佐證資料，或簡述實際作業狀況。

自我檢核項目	自我檢核內容	自我檢核結果(業者勾選)	檢核結果說明(業者填寫)	參考
1.管理人員及資源配置	1.1 是否已配置人員或適當組織管理及維護保有之個人資料？	□符合□不符合□不適用		請檢附個資管理單位組織圖、分工及相關辦法，並提出個資窗口所協助之各項個資保護工作事項，如：參與會議、文件化管理控制措施等。

自我檢核項目	自我檢核內容	自我檢核結果(業者勾選)	檢核結果說明(業者填寫)	參考
	1.2 是否配置適當資源？	□符合□不符合□不適用		請檢附預算、設備費用等。
2.界定個人資料之範圍	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		請檢附公司依業務類別建立個人資料清冊及盤點紀錄。
	2.2 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		
	2.3 是否進行個資盤點?個資盤點是否確實？	□符合□不符合□不適用		
	2.4 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		說明蒐集個資前所進行宣告並取得當事人同意之紀錄。
	2.5 是否有目的外之利用？目的外利用是否符合法定要件？	□符合□不符合□不適用		說明公司宣告進行目的外利用並取得同意；其後的利用亦應與蒐集目的相符合。
3.風險評估	3.1 是否進行風險評估？	□符合□不符合□不適用		請檢附風險評鑑底稿。
	3.2 針對風險進行因應？	□符合□不符合□不適用		
4.個人資料事故預防、應變及通報機制 ※當年度無事故者，4.2-4.6應填不適用。 ※當年度有事故者，請檢附事	4.1 是否有通報及應變程序？	□符合□不符合□不適用		請檢附個人資料事故之預防、通報及應變機制之管理文件。
	4.2 事故發生時是否確實通報？	□符合□不符合□不適用		
	4.3 事故發生後是否採取應變措施？	□符合□不符合□不適用		
	4.4 是否於適當期間內通知當事人？	□符合□不符合□不適用		

自我檢核項目	自我檢核內容	自我檢核結果 (業者勾選)	檢核結果說明 (業者填寫)	參考
故發生後個人資料通報紀錄表。	4.5 事後是否採取預防措施？	□符合□不符合 □不適用		
	4.6 是否將事故處理情形通知主管機關？	□符合□不符合 □不適用		
5.個人資料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		請檢附最新個資盤點資料，確認皆已識別保有依據。
	5.2 個人資料之利用，符合特定目的之範圍？	□符合□不符合 □不適用		
	5.3 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		請說明蒐集個資並取得當事人同意之情形。
	5.4 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		請檢附告知事項。
	5.5 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		
	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		請檢附個資蒐集、處理、利用、刪除程序文件，以及個資銷毀、刪除紀錄。
	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		請檢附檢核紀錄、告知事項。
	5.8 是否有目的外之利用？目的外利	□符合□不符合 □不適用		

自我檢核項目	自我檢核內容	自我檢核結果 (業者勾選)	檢核結果說明 (業者填寫)	參考
	用是否符合法定要件？			
	5.9 是否利用蒐集之個人資料進行行銷？	□符合□不符合 □不適用		
6.資料安全、人員管理及設備安全	6.1 紙本資料檔案，是否採取安全保護設施？	□符合□不符合 □不適用		請說明紙本資料檔案安全保護設施。
	6.2 電子資料檔案存放之電腦、自動化機器相關設備、可攜式設備或儲存媒體，是否配置安全防護系統或加密機制？	□符合□不符合 □不適用		請說明針對個資電子檔案之控管規範。
	6.3 是否以適當方式銷毀紙本或電子個人資料，並視需要留存適當之銷毀紀錄？	□符合□不符合 □不適用		請說明採行紙本或電子資料銷毀之方式，以及所留存之佐證紀錄。
	6.4 資通訊系統是否採行使用者身分確認及保護機制？	□符合□不符合 □不適用		請說明資通訊系統使用者身分之認證機制及保護機制，如其帳號及密碼須符合一定之複雜度。
	6.5 是否採行個人資料顯示之隱碼機制？	□符合□不符合 □不適用		請說明資料庫之結構和設計、個人資料之去識別化措施。
	6.6 傳輸消費者個人資料時，是否依不	□符合□不符合 □不適用		請說明對外傳送個資檔案之

自我檢核項目	自我檢核內容	自我檢核結果 (業者勾選)	檢核結果說明 (業者填寫)	參考
	同傳輸方式，採取適當之安全措施？			相關規範，檢附規範制度文件。例如以電子郵件傳送敏感之個資檔案時，是否採加密機制？
	6.7 是否採行個人資料檔案與資料庫之存取控制及保護監控措施？	□符合□不符合 □不適用		請檢附個資系統權限申請表單以及帳號權限審查紀錄。
	6.8 是否採行防止外部網路入侵對策？	□符合□不符合 □不適用		請說明公司進行系統、個人電腦之安全性更新、漏洞修補、防毒軟體更新之程序，以及所留存之佐證紀錄。
	6.9 是否採行非法或異常使用行為之監控及因應機制？	□符合□不符合 □不適用		請說明是否建置防火牆、電子郵件過濾機制或其他入侵偵測設備，並定期更新及執行惡意程式檢測。
	6.10 是否要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務？	□符合□不符合 □不適用		請檢附公司之個資管理者所簽署之保密切結書。

自我檢核項目	自我檢核內容	自我檢核結果(業者勾選)	檢核結果說明(業者填寫)	參考
	6.11 是否要求所屬人員離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用？	□符合□不符合□不適用		請檢附離職人員所簽署之保密切結書或離職單。
7.認知宣導與教育訓練	7.1 是否定期進行教育訓練？	□符合□不符合□不適用		請檢附對所屬人員之教育訓練簡報、各項相關課程簽到表(需含授課日期) 及課後評量結果。上課內容應包含個人資料保護相關法令之要求、人員之責任範圍及各項個人資料保護相關作業程序。
	7.2 是否對新進人員進行認知宣導？	□符合□不符合□不適用		請說明新進人員所進行認知宣導之程序。
8.使用紀錄、軌跡資料及證據保存	8.1 是否留存個人資料使用紀錄、軌跡資料或相關證據及紀錄，且至少留存五年？	□符合□不符合□不適用		請說明保存個資進行之記錄流程，如定期檢視紀錄，對異常警訊進行確認，並有檢視結果之呈核及記錄留存。
	9.1 業務終止後，保有之個人資料是否	□符合□不符合□不適用		請檢附業務終止後，個人資

自我檢核項目	自我檢核內容	自我檢核結果 (業者勾選)	檢核結果說明 (業者填寫)	參考
9.業務終止後之個人資料處理	銷毀，並留存銷毀方法、時間、地點及證明銷毀方式等相關紀錄至少5年？			料處理方法之管理文件，如有業務終止之情形發生，併同檢附相關銷毀紀錄。
	9.2 業務終止後，保有之個人資料是否移轉，並留存移轉原因、對象、方法、時間、地點，及受移轉對象得保有該項個人資料之合法依據等相關紀錄至少5年？	□符合□不符合 □不適用		請檢附業務終止後，個人資料處理方法之管理文件，如有業務終止之情形發生，併同檢附所保有之個人資料相關移轉紀錄。
	9.3 業務終止後，保有之個人資料是否刪除、停止處理或利用，並留存相關方法、時間或地點等相關紀錄至少5年？	□符合□不符合 □不適用		請檢附業務終止後，個人資料處理方法之管理文件，如有業務終止之情形發生，併同檢附所保有之個人資料刪除、停止處理或利用之相關紀錄。
10.委外作業 (註：網站/系統委外建置，若涉及蒐集、處理或利用個人資料之全部或一部	10.1 委託他人蒐集、處理或利用個人資料之全部或一部時，是否要求受託人依委託人應適用之規定為之？	□符合□不符合 □不適用		請檢附個資委外之廠商清單及合約文件。

自我檢核項目	自我檢核內容	自我檢核結果 (業者勾選)	檢核結果說明 (業者填寫)	參考
時,亦屬個資法第4條之的委託行為)	10.2 委託他人蒐集、處理或利用個人資料之全部或一部時,是否於委託契約或相關文件明確約定適當之監督事項及方式?	□符合□不符合 □不適用		請檢附個資委外之廠商清單及合約文件。
	10.3 委託他人蒐集、處理或利用個人資料之全部或一部時,是否確實執行監督?	□符合□不符合 □不適用		請說明對委外廠商之監督方式或檢附委外稽核報告以及稽核缺失追蹤情形。
	10.4 是否要求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?	□符合□不符合 □不適用		請檢附個資委外之廠商清單及合約文件。
	10.5 是否要求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?	□符合□不符合 □不適用		
11.資料安全稽核機制	11.1 是否設有稽核制度?	□符合□不符合 □不適用		請說明稽核之執行管理措施、辦法。
	11.2 是否定期實施稽核?	□符合□不符合 □不適用		請說明稽核之頻率及執行方式,並檢附最近一次之評估報告。

自我檢核項目	自我檢核內容	自我檢核結果 (業者勾選)	檢核結果說明 (業者填寫)	參考
12.持續改善	12.1 是否定期檢視個資保護措施？	□符合□不符合 □不適用		請檢附相關個人資料安全維護議題會議之記錄。
	12.2 是否針對缺失進行改善？	□符合□不符合 □不適用		請檢附對個資保護之改善措施及佐證文件。

檢核人員	管理顧問業代表
(簽章)	(簽章)

範例三：個資事故通知當事人文書(範本)

**範本內容僅供參考，請依個人資料保護相關法規、內部管理作業程序及實際業務情形訂定貴公司（商業）之個人資料檔案安全維護計畫。

○○ 您好：

茲因○○管理顧問業(以下簡稱本公司「○○系統」遭惡意攻擊，台端之個人資料可能外流，經調查疑似個人資料外洩事故。

本公司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公司網站遭駭客惡意攻擊導致外洩，影響您的隱私權益，經過調查，相關個人資料(列舉)可能有外洩的風險。依個人資料保護法規定，本公司需通知您有關本案之實際情況及本公司已採取之因應措施。
2. 列舉本公司已採取之因應措施。
3. 若台端仍有疑慮，可與本公司○○○聯絡，聯絡電話：○○○-○○○○，將由專人為您說明及釋疑。

本公對此次事件造成台端之困擾，再次致上歉意。本公司將再加強網站程式之安全性檢測及資訊系統之安全性管理，避免類似事件再度發生，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

範例四：個人資料蒐集、處理、利用同意書(範本)

個人資料蒐集、處理、利用同意書

****範本內容僅供參考，請依個人資料保護相關法規、內部管理作業程序及實際業務情形訂定貴公司（商業）之個人資料檔案安全維護計畫。**

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. 公司名稱：（○○管理顧問業）
2. 蒐集之特定目的：（例：營業使用）
3. 個人資料之類別：（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：
   (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：
   (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。
   (6) 依個人資料保護法第20條第2項、第3項規定拒絕行銷之方式及費用。

   若有上述需求，請與本公司聯繫，於填妥本公司當事人權利行使申請書後，本公司將依法進行回覆。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，本公司得酌收必要成本費用。

6. 若未提供正確個人資料，本公司將無法提供您特定目的範圍內之相關服務。

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

立同意書人:

(如為線上蒐集當事人個資之情形，應留存當事人點選同意之軌跡紀錄。)

中華民國　　年　　月　　日

範例五：個人資料業務委外契約（範本）

個人資料業務委外契約

**範本內容僅供參考，請依個人資料保護相關法規、內部管理作業程序及實際業務情形訂定貴公司（商業）之個人資料檔案安全維護計畫。

立約人

甲方__〇〇〇公司__（委託方）

乙方_____（受委託方）

甲方委託乙方執行_____業務，就個人資料之蒐集、處理或利用行為，雙方同意遵守下列條款，並以本約視為原委託契約之一部分，本約未規範之部分悉依原契約之內容執行：

第一條、個人資料告知條款：

為遵守個人資料保護法（以下簡稱個資法）之規定，乙方如有受甲方委託代為蒐集個人資料之行為，應依個資法第 8、第 9 條規定，履行告知義務，或於首次利用個人資料時為告知，告知之書面內容應由甲方提供。

第二條、個人資料之定義、委託範圍：

（一）本約之個人資料其蒐集、處理及利用行為，悉遵照個資法等相關法規之定義。

（二）甲方委託乙方執行____業務涉及有關個人資料蒐集、處理及利用範圍如下：

1.個人資料之特定目的：

2.個人資料之類別：

3.個人資料之範圍：

4.個人資料之利用期間：

第三條、執行____業務關於個人資料防護之約定：

（一）乙方應視公司規模、營運狀況採取下列措施：

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。

（二）乙方對於其所維護或管理之個人資料，應進行相關保護措施，並應符合甲方要求及符合現今科技水準之資訊安全保護措施。乙方應依其所屬人員之工作範圍及職級，訂定不同之存取權限，並記錄所有存取紀錄。

（三）委外作業如涉及個人資料使用應用系統時，乙方於進行應用系統程式變更前，應先進行測試，並提出說明文件及申請（檢附相關文件，如：測試報告），並取得甲方同意。

（四）乙方於執行甲方所委託之業務時，應遵照個人資料保護法、甲方所制（訂）定之個人資料安全標準規範及個人資料安全相關標準作業程序為之，若有違反而造成甲方之損害，乙方應對甲方負本契約第 8 條之賠償責任。

（五）若因可歸責於乙方事由（包含但不限於：惡意程式、病毒、人員操作、複委託單位）造成個人資料外洩進而導致甲方損害，乙方應對甲方負損害賠償責任（包括但不限於訴訟費用及律師費用等）。

（六）乙方應依甲方指示，或於委託關係終止或解除時，應返還儲存個人資料之載體，並銷毀為履行本約而蒐集之個人資料，且不得以任何形式留存。

第四條、保留指揮監督事項：

甲方保留指揮監督事項如下：

（一）乙方若有銷毀受託之個人資料時，應在甲方指派人員之監督下為之，並作成銷毀紀錄交甲方留存。

（二）分開委託之個人資料不得進行相互連結，若欲進行相互連結時，應事前取得甲方之書面同意後始得為之。

（三）乙方於委託契約解除或終止前 1 個月，應提出針對受委託期間曾接受甲方交付之個人資料清冊。並於契約解除或終止時，提出銷毀申請，經甲方同意後，於甲方之監督下執行；或將個人資料清冊所涉個人資料內容交還甲方或交給甲方指定之其他機關之證明，該證明內容應包括交還之項目、數量、時間、方式、簽收人等。乙方另應交付未持有甲方交付之個人資料檔案切結證明。

（四）乙方如因故未能銷毀、交還或交給甲方指定之其他機關之證明，應列冊載明原因及保存的期間、方式，於取得甲方之同意後進行保存。

（五）個人資料之清冊其內容應包括交付各種紙本及電子形式之個人資料。

第五條、複委託：

乙方若需將甲方委託之業務複委託其他廠商時，須經甲方事前書面同意。甲方若同意乙方得以複委託方式提供服務，乙方仍負有依照本約規定履行之責任，複託廠商因執行業務而造成甲方之損害時，乙方與複委託單位應對甲方之損害負連帶賠償之責（包括但不限於訴訟費用及律師費用等）。

第六條、保密協議：

（一）乙方因履行甲方委託契約所取得或知悉甲方之個人資料，應負保密義務。

（二）本約所稱之個人資料，係指甲方所擁有之個人資料，或依法律及契約應由乙方負保密義務之個人資料，不論其係以口頭、書面或電子紀錄等任何形式呈現，除經甲方事先書面同意、甲方自行公開或其他法律另有規定之情況外，乙方及所屬人員均應負保密義務，絕不洩漏、販售、交付或以其他方式予甲方以外之第三人知悉（但經甲方指定之第三人不在此限）、持有或利用，亦不得自行複製、留存而為契約目的以外之利用。

（三）乙方應簽屬保密切結書予甲方，若乙方所屬人員有違反本約有關保密義務之行為，視為乙方之違約行為。

第七條、委託個人資料之稽核：

（一）乙方應依個人資料保護相關法規就受甲方委託之業務定期(每____個月）記錄及稽核，並配合甲方之稽核業務，依甲方之指示提供相關文件，不得拒絕。

（二）乙方為處理委託事務而須處理或利用甲方所蒐集之個人資料時，乙方應遵守個人資料法之相關規定，同時對於甲方所制（訂）定相關標準作業程序，乙方亦應遵守之。甲方認有必要時，並得隨時於本約委託事務之範圍內進行檢查，乙方不得拒絕。

（三）乙方及其所屬人員之行為若違反個人資料法相關規定或甲方制（訂）定之相關標準作業程序蒐集、處理及利用個人資料，進而造成個人資料被竊取、洩漏、竄改或其他侵害者，乙方應立即通知甲方（通知事項包含查明原因及採行之補救措施），且依甲方之指示方式及指示內容通知個人資料之當事人。

（四）甲方若有相當之事實發現乙方及其所屬人員可能涉及違反本約或個人資料保護相關法令規定之行為時，乙方應盡最大努力協助甲方調查，提供所有必要之資料，並為各項必要之配合行為。

（五)若違反個人資料法係由乙方、乙方所屬人員或複委託廠商之行為所致者，乙方應協助甲方對外說明，並於所有訴訟程序，協助甲方舉證已盡相關之個人資料防護義務。

第八條、違約賠償：

乙方如有下列事由之一，視為違約，除應自行負擔相關之民、刑事、行政責任及損害賠償責任外（包含但不限於訴訟費用及律師費用），另應加罰懲罰性違約金新臺幣____元（本約未載明金額者，適用原委託契約對懲罰性違約金之計算規定）：

1.違反本契約第 3 條關於個人資料防護之約定。

2.違反本契約第 4 條甲方保留指揮監督事項之約定。

3.違反本契約第 5 條複委託之約定。

4.違反本契約第 6 條保密義務之約定。

5.違反本契約第 7 條稽核之約定，經通知限期改善而未改善完成者。

第九條、契約解除：

乙方如有違反本約第 3 條第 4 項至第 6 項、第 4 條至第 7 條之任一約定者，甲方得解除本委託契約，契約之解除，不妨礙甲、乙雙方損害賠償請求。

簽約人

甲方：

代表人：

地址：

乙方：

代表人：

地址：

中　華　民　國　　年　　月　　日

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
4. 中華民國一百十二年五月三十一日總統華總一經字第 11200045441 號令修正公布第 48、56 條條文；並增訂第 1-1 條條文；第 48 條條文自公布日施行，第 1-1 條條文施行日期，由行政院定之。中華民國一百十二年十二月二十八日國家發展委員會發法字第 1122002856 號、個人資料保護委員會籌備處個資籌法字第 1120400005 號會銜公告第 53 條、第 55 條所列屬「國家發展委員會」管轄之權責事項，自一百十三年一月一日起改由「個人資料保護委員會籌備處」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。

第一之一條　本法之主管機關為個人資料保護委員會。
自個人資料保護委員會成立之日起，本法所列屬中央目的事業主管機關、直轄市、縣（市）政府及第五十三條、第五十五條所列機關之權責事項，由該會管轄。

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。

非公務機關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二百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處新臺幣十五萬元以上一千五百萬元以下罰鍰。

非公務機關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，其情節重大者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣十五萬元以上一千五百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處罰。

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。
本法中華民國九十九年五月二十六日修正公布之現行條文第十九條至第二十二條、第四十三條之刪除及一百十二年五月十六日修正之第四十八條，自公布日施行。

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
   中華民國一百十二年十二月二十八日國家發展委員會發法字第 1122002856 號、個人資料保護委員會籌備處個資籌法字第 1120400005 號會銜公告第 33 條所列屬「國家發展委員會」之權責事項，自一百十三年一月一日起改由「個人資料保護委員會籌備處」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、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中華民國一百零一年十月一日以令修正「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」，定自中華民國一百零一年十月一日生效。

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

◯二九　公民營（辦）交通運輸、公共運輸及公共建設
◯三◯　仲裁
◯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
◯三二　刑案資料管理
◯三三　多層次傳銷經營
◯三四　多層次傳銷監管
◯三五　存款保險
◯三六　存款與匯款
◯三七　有價證券與有價證券持有人登記
◯三八　行政執行
◯三九　行政裁罰、行政調查
◯四◯　行銷（包含金控共同行銷業務）
◯四一　住宅行政
◯四二　兵役、替代役行政
◯四三　志工管理
◯四四　投資管理
◯四五　災害防救行政
◯四六　供水與排水服務
◯四七　兩岸暨港澳事務
◯四八　券幣行政
◯四九　宗教、非營利組織業務
◯五◯　放射性物料管理
◯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
◯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
◯五三　法制行政
◯五四　法律服務
◯五五　法院執行業務
◯五六　法院審判業務
◯五七　社會行政
◯五八　社會服務或社會工作
◯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

◯六◯　金融爭議處理
◯六一　金融監督、管理與檢查
◯六二　青年發展行政
◯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
◯六四　保健醫療服務
◯六五　保險經紀、代理、公證業務
◯六六　保險監理
◯六七　信用卡、現金卡、轉帳卡或電子票證業務
◯六八　信託業務
◯六九　契約、類似契約或其他法律關係事務
◯七◯　客家行政
◯七一　建築管理、都市更新、國民住宅事務
◯七二　政令宣導
◯七三　政府資訊公開、檔案管理及應用
◯七四　政府福利金或救濟金給付行政
◯七五　科技行政
◯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
◯七七　訂位、住宿登記與購票業務
◯七八　計畫、管制考核與其他研考管理
◯七九　飛航事故調查
◯八◯　食品、藥政管理
◯八一　個人資料之合法交易業務
◯八二　借款戶與存款戶存借作業綜合管理
◯八三　原住民行政
◯八四　捐供血服務
◯八五　旅外國人急難救助
◯八六　核子事故應變
◯八七　核能安全管理
◯八八　核貸與授信業務
◯八九　海洋行政
◯九◯　消費者、客戶管理與服務
◯九一　消費者保護
◯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○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○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○三二　財產。

例如：所有或具有其他權利之動產或不動產等。

C○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○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○三五　休閒活動及興趣。

例如：嗜好、運動及其他興趣等。

C○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○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○三八　職業。

例如：學校校長、民意代表或其他各種職業等。

C○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○四○　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○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。

五、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

中華民國一百十二年二月一十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。

六、個人資料保護法第四十八條第三項「情節重大者」認定之參考原則

中華民國一百十二年十月一十二日國家發展委員會發法字第1122001947號函訂定

一、為使中央目的事業主管機關及直轄市、縣（市）政府（以下簡稱主管機關)就個人資料保護法(以下簡稱本法)第四十八條第三項「情節重大者」之認定，有一致性之處理，特訂定本參考原則。

二、主管機關裁處罰鍰， 應遵守明確性、平等、比例等一般法律原則，並踐行行政程序法及行政罰法所定之法定程序。

三、主管機關就本法第四十八條第三項「情節重大者」之認定，得綜合考量非公務機關之下列情形：

（一）個人資料外洩情形：

1. 所涉個人資料類別是否包含本法第六條所稱「病歷、醫療、基因、性生活、健康檢查、犯罪前科」等特種個人資料。
2. 所涉及當事人之人數多寡。
3. 外洩行為對於當事人所生之影響程度。
4. 外洩是否出於故意或重大過失。

（二）安全維護措施之落實情形：

1. 有無依本法第二十七條第三項所定辦法規定，採取安全維護措施。
2. 是否曾因未盡個人資料安全維護義務，而有發生個人資料外洩情事。

（三）知悉個人資料外洩後採行措施：

1. 有無採取降低當事人損害之行為。
2. 有無依規定主動通報主管機關。
3. 有無規避、妨礙或拒絕主管機關調查之情事。
4. 有無以適當方式通知當事人。

（四）其他：

1. 是否遵循主管機關依本法規定就同一個人資料外洩案件所為之相關處分。
2. 是否因該個人資料外洩獲有直接或間接之利益。

四、依行政罰法第十八條第一項規定,於裁處本法第四十八條第三項認定「情節重大者」罰鍰處分時，並得考量受處罰者之資力(例如：上市或上櫃之事業單位；依法辦理公司登記或商業登記,且實收資本額或在中華民國境內營運資金超過新臺幣一億元之事業單位)。

五、非公務機關經主管機關依本法第四十八條第三項規定,裁處罰鍰並令限期改正，屆期未改正者，應按次處罰。

六、非公務機關之代表人、管理人或其他有代表權人,因該非公務機關依本法第四十八條第三項規定受罰鍰處罰時,除能證明已盡防止義務者外,依本法第五十條規定，應並受同一額度罰鍰之處罰。