經濟部商業發展署
Administration of Commerce, MOEA

# 綜合商品零售業

## 個人資料保護與管理 實作指引手冊

中華民國112年11月

# 目錄

# Chapter1

# 前言

# 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。又綜合商品零售業常有以會員制或其他方式保有個人資料之情形，為強化業者對個人資料之保護，經濟部依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定「綜合商品零售業個人資料檔案安全維護管理辦法」(以下簡稱本辦法)。

本辦法於 112 年 8 月 1 日發布施行，綜合商品零售業者應於辦法發布施行之日起六個月內(113 年 1 月 31 日前)完成安全維護計畫之訂定。為避免綜合商品零售業者執行業務時，因不諳法律之執行內容，而承擔相關法律責任，特編印綜合商品零售業個人資料保護與管理實作指引手冊(以下簡稱本手冊)，旨在針對綜合商品零售業實務操作者提供個資管理的實務指引。基此，本手冊係從個資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，並透過實際個資輔導訪查案例說明分析，使讀者更能清楚掌握個資保護管理實務之要點。

綜合商品零售業者可參考本手冊之指引，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，以符合綜合商品零售業個人資料檔案安全維護管理辦法之相關規定。

# Chapter2

# 手冊指引

## 貳、手冊指引

本辦法適用之對象為綜合商品零售業者，指從事以非特定專賣形式銷售多種系列商品之零售，已辦理公司、有限合夥或商業設立登記，且資本額達新臺幣一千萬元以上，並有招募會員或可取得交易對象個人資料之業者，或受經濟部指定之公司、有限合夥或商業。但不包括應經特許、許可或受專門管理法令規範之行業。

本手冊依據個資法、個資法施行細則、綜合商品零售業個人資料檔案安全維護管理辦法等規定研擬，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、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。

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

一、實作參考指引

本章節以綜合商品零售業個人資料檔案安全維護管理辦法第 6 條程序事項為架構，同時導入 P-D-C-A（Plan-Do-Check-Act）方法論，並部分參考 BS 10012 PIMS 個人資訊管理系統國際標準，以規劃、執行、檢核、持續改善等方式，建立實作參考指引。

二、個資事故案例

本章節介紹七個代表性個資案例，每個案例進行案例評析，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「綜合商品零售業個人資料安全稽核檢查表」(以下簡

稱本表），以協助並引導業者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。

四、常見問題

本章節由經濟部於個資輔導訪查及實務執行上蒐集業者常見之問題，並進行研究提供說明，使讀者更能清楚掌握個資保護管理之實務運作，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

個人資料保護法、個人資料保護法施行細則、綜合商品零售業個人資料檔案安全維護管理辦法、綜合商品零售業個人資料檔案安全維護計畫(範本)、綜合商品零售業個人資料安全稽核檢查表、個人資料保護法之特定目的及個人資料之類別、個資相關流程識別清單、個人資料盤點表、個資事故通知當事人範本、委外廠商個資安全維護聲明書（範例）等，共十個附錄文件。

# Chapter3

# 實作參考指引

# 參、實作參考指引

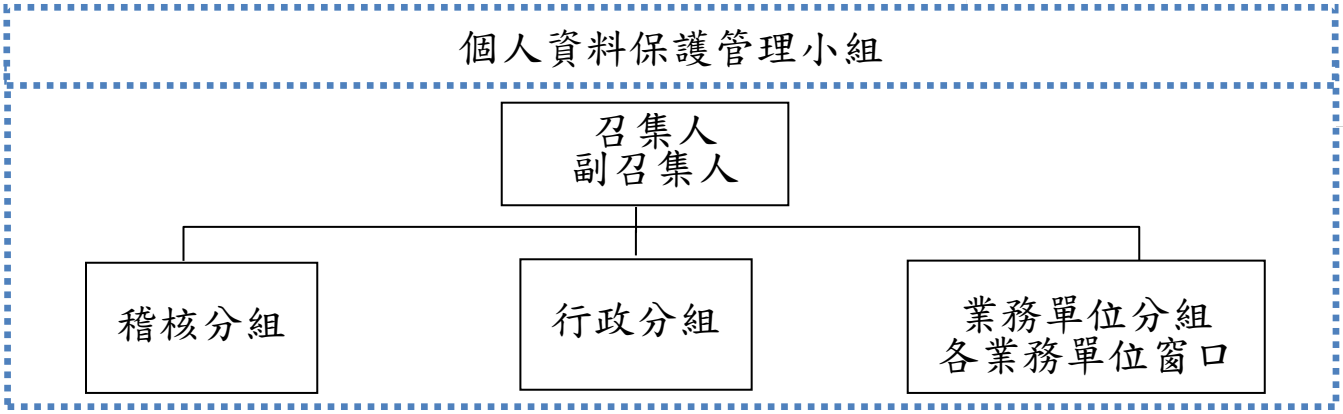
## 一、配置管理人員及相當資源

（一）業者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，以及「綜合商品零售業個人資料檔案安全維護管理辦法」第 5 條之規定，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」意思是，組織內部應透過專任或兼任方式指派專責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。我國的個資相關規範並沒有要求組織必須成立專職個人資料保護與管理的資料保護專員或個資長，只需要有專責人員負責組織內部個人資料保護即可。

（三）配置「相當資源」的意思，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、技術支持等。以落實資料保護角度來說，組織若要確實做好個人資料安全維護，所投入的資源與人力應和組織規模成相當比例，否則可能會成效不彰。

（四）實務上在規模較大的組織，若只有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，並促進個人資料之合理利用，應制定個人資料保護管理組織架構與權責。為有效整合各部門個人資料保護運作事宜，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）業者訂定個人資料管理組織辦法，可參考以下 BS 10012 PIMS 個人資訊管理系統國際標準之部分內容：

1. 個人資料保護管理小組召集人負責下列事項，召集人並得指派副召集人協助辦理。

1.1 召開與主持管理審查會議。

1.2 個人資料保護與管理責任之分配及協調。

1.3 個人資料保護制度與政策之審查與督導。

1.4 個人資料管理政策相關辦法、計劃與程序書之審議。

1.5 個人資料安全事件之檢討及監督。

1.6 啟動個人資料安全事故應變處理措施。

1.7 向上報告個人資料保護管理績效，及違反規定人員的懲處建議。

1.8 其他個人資料保護與管理事項之審議。

2. 個人資料保護管理工作分組架構與負責事項：

2.1 個人資料保護管理工作分組隸屬於個人資料保護管理小組，代表各部門參與個人資料保護管理之實際推動，並負責個人資料保護與管理跨部門議題之初步討論與擬定，向個人資料保護管理小組召集人報告。

2.2 個人資料保護管理工作分組成員由個人資料保護管理小組召集人指派。

2.3 工作分組設行政分組、稽核分組、業務單位分組等，並得依業務需要調整。

3. 行政分組負責下列事項：

3.1 行政分組分組長為個資小組之執行秘書，負責個資小組相關協調事宜。

3.2 個人資料保護與管理相關管理制度等文件之制訂、修訂及保管。

3.3 規劃及執行個人資料保護與管理技術控制與基礎設施之提升計畫。

3.4 規劃及執行個人資料保護與管理內部人員認知與教育訓練計畫，並留存訓練有效性評估紀錄。

3.5 確立個人資料檔案之軌跡資料記錄與保存機制。

3.6 事故通報與處理及應變相關活動之聯繫、協調及處理。

3.7 研擬個人資料保護與管理政策、個人資料保護管理辦法、隱私權聲明等規範。

3.8 檢視個人資料保護法、施行細則等相關法令之異動，適時提供內部改善或調整方向之建議。

3.9 個人資料保護相關法令諮詢與相關法務事宜之處理。

3.10 中央及地方主管機關個資法令事務之協調聯繫。

3.11 受理及回覆當事人依法提出個人資料相關訴訟求償事宜。

3.12 規劃與協調個人資料保護管理活動持續運作，包括個人資料相關流程識別及個資檔案盤點、維護、隱私衝擊與風險評估作業等。

3.13 擔任對外個人資料保護單一聯繫窗口，負責個人資料安全事故處理及重大個人資料外洩事件對外聯繫。

3.14 確立委外作業合約符合個資法施行細則第八條之監督事項。

3.15 受理個資法第三條當事人權利相關事宜。

3.16 其他行政分組應辦理之個人資料管理作業。

4. 稽核分組負責下列事項：

4.1 擬定個人資料保護內部稽核計畫，如遇組織面、業務面、外部環境面、技術面或有其他重大變更，應儘速重新擬定稽核計畫並實施稽核。

4.2 執行個人資料保護內部稽核作業，並依限完成。

4.3 彙整與陳報個人資料保護內部稽核報告。

4.4 追蹤個人資料保護內部稽核發現之改善活動。

4.5 其他稽核分組應辦理之個人資料管理作業。

5. 業務單位分組負責下列事項：

5.1 負責執行個資小組決議事項，配合辦理個人資料安全維護，落實個人資料保護管理機制，確保管理制度正常運行。

5.2 執行個人資料告知及隱私權相關資訊溝通及管理。

5.3 執行單位個人資料保護管理活動，包括個人資料檔案盤點與維護等作業。

5.4 定期陳報單位個人資料保護管理推動狀況。

5.5 通報並協助處理單位內之個人資料事故，並妥善保存處理流程及方式備查。

5.6 處理個資當事人依法提出個人資料權利之請求事宜。

5.7 協助受理客戶、當事人提出之個人資料相關權利、申訴或抱怨，並通報行政分組。

5.8 針對各部門之委外廠商及辦理個資法施行細則第八條之監督事項。

5.9 各部門之資料如需傳輸至其他組織或涉及跨境傳輸、儲存或其他處理方式，應向行政分組通報備查。

5.10 如有歐盟、我國或其他國家個資法令適用之例外狀況，應通報行政分組協助處理。

5.11 其他業務單位分組應辦理之個人資料管理作業。

6. 各部門應配合辦理下列事項：

6.1 指派專人傳達個資保護政策及相關規範之遵循義務。

6.2 識別個人資料保護與管理相關作業流程。

6.3 盤點個人資料檔案。

6.4 執行隱私衝擊分析、風險評估及風險改善。

6.5 通報並協助處理個人資料安全事件。

6.6 配合當事人權利行使、緊急事故應變與處理程序之演練。

6.7 配合個人資料管理制度及政策之相關文件、表單增修。

6.8 參與個資保護相關教育訓練，以充分了解個資保護目標之重要性，及相關個資稽核缺失之影響。

6.9 其他為落實個人資料保護相關管理制度及政策之作業。

7. 下列事項由人力資源部門負責辦理：

配合個人資料保護與管理制度之導入，將相關安全管理需求落實於人員任免遷調、獎懲作業。

8. 個人資料保護管理審查議題

為確保個人資料保護與管理政策落實執行，個人資料保護管理小組每年應至少進行一次個人資料保護管理審查，審查議題包含但不限於下列項目：

8.1 前次管理審查議案之處理進度及方式。

8.2 個人資料管理制度相關績效之趨勢，如稽核結果、缺失項目、改善方式、有效性量測結果等。

8.3 與個人資料相關之潛在風險及因應措施，包含內部人員回饋之意見、外部環境、業務之變動、其他等內、外部關注方(含可影響、或受影響之個人或組織)之議題。

8.4 個資風險評估結果。

8.5 個人資料保護內部稽核情形。

8.6 個人資料保護相關程序之增、修訂情形。

8.7 資訊技術或產品升級、替換或變動之影響評估及結果。

8.8 主管機關之評鑑、稽核或其他要求。

8.9 當事人抱怨、申訴事件處理。

8.10 已發生之個人資料安全事件及處理結果。

8.11 其他可改善個資保護之意見。

9. 個人資料保護管理審查之結果，應包含前條相關議案之決議，並留存相關紀錄。

## 二、界定個人資料範圍並定期確認

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」及「綜合商品零售業個人資料檔案安全維護管理辦法」第 7 條第 1 項之規定，綜合商品零售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，並定期清查所保有之個人資料現況。

建立個人資料檔案清冊及個人資料作業流程說明文件，此一程序主要可協助案者對於內部個資蒐集、處理及利用之現況有所瞭解，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，且透過盤點程序，亦能使業者查核所保有個人資料檔案之適法性，以減少違法之風險。

### (一) 個人資料檔案盤點之範圍

1. 所謂「個人資料」，依個人資料保護法第 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，業者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. 而業者就業務進行委託時，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之範圍。

（二）蒐集、處理及利用個人資料之特定目的

1. 業者蒐集、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 項本文規定，應有特定目的，並符合法律規定之要件，例如蒐集及處理時之法律規定要件如下：

1.1 法律明文規定。

1.2 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。

1.3 當事人自行公開或其他已合法公開之個人資料。

1.4 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過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。

1.5 經當事人同意。

1.6 為增進公共利益所必要。

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

1.8 對當事人權益無侵害。

2. 因此，業者基於業務而蒐集、處理或利用消費者個人資料時，應有特定目的，同時符合個資法之要件，於該特定目的必要範圍內為之。所以，業者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」(附錄六)，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。

3. 但是，當業者於蒐集、處理及利用個人資料後，想要將這些個人資料為目的外的使用時，例如業者基於舉辦說明會的目的，取得參加活動者之資料，原目的如只有為處理報名手續，但事後該業者想利用這些個人資料進行行銷，也就是個人資料保護法第 20 條第 1 項但書上的目的外利用，就必須符合以下擇一之要件：

3.1 法律明文規定。

3.2 為增進公共利益所必要。

3.3 為免除當事人之生命、身體、自由或財產上之危險。

3.4 為防止他人權益之重大危害。

3.5 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。

3.6 經當事人同意。

3.7 有利於當事人權益。

4. 除此之外，個人資料保護法第 20 條第 3 項與第 4 項也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，如果對方當事人表示拒絕接受行銷時，就應該立即停止利用該當事人的個人資料來行銷，但其他並未接受到當事人主張停止蒐集、處理及利用的目的，就不受影響。而在業者進行首次行銷時， 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，例如該業者如果採取書面拒絕行銷的申請時，應支付相關的郵寄費用。

5. 特定目的應以實際業務目的臚列即可。若於法務部所公布的「個人資料保護法之特定目的及個人資料之類別」找不到適合之項目，建議應該要將蒐集、處理及利用個人資料的特定目的清楚地合理闡述。實務上很常見的情形是許多組織將大部分可能用到之特定目的匡列進去，但過於寬鬆的特定目的，難以使當事人了解蒐集的真正目的，因此個資法遵上建議特定目的應該扣合業務執行範圍，也不要用

「 … 」或「包含但不限於」等不明確之用語。總而言之，特定目的的匡列應該以當事人能夠清楚且明白瞭解蒐集個人資料之目的為準。

（三）個資盤點方法與範例(※個資盤點清冊範例請參照附錄八)

1. 實務上個資盤點之作法很多，沒有保證完全無疏漏的方法，但組織進行個資盤點時，大多建議以分析個資蒐集使用流程著手，盤點出公司所蒐集、處理以及利用的個人資料。這種方式可以比較精準的掌握組織蒐集使用個資的狀態，比較不容易有疏漏，也可以降低漏盤風險。盤點其內容包括下列項目：

1.1 整理組織各作業流程中所保有的各類文件、檔案、簿冊，清查確認其是否含有個人資料。

1.2 清查所有涉及個人資料的文件，歸納整理成個人資料檔案，並建立個資盤點清冊。

1.3 使用個資盤點清冊檢視組織保存的個人資料種類、確認個人資料檔案名稱、保存的特定目的及依據，以及保存現況。

1.4 使用個資盤點清冊檢視並確認，在平常業務的蒐集、處理及利用個人資料的過程當中，是否有違法的可能。

1.5 妥善保管個資盤點清冊並且定期維護。

2. 個資盤點建議

2.1 個資漏盤是實務上常見的缺失，尤其常發生於新拓展或委外處理的業務。

2.2 我國個資法規定，在個資法適用範圍內，受委託蒐集、處理或利用個人資料的單位，執行蒐集、處理或利用個人資料的行為，視同委託機關的行為。

2.3 一般公司常認為委外處理就不用將該業務納入個資盤點是錯誤的觀念。委外的個資相關業務仍要納入盤點範圍，尤其近年來常見發生委外廠商個人資料外洩事故，應更加注意。

2.4 個人資料管理制度上，建議於各部門個資盤點後，應該

再由主要推動個資管理制度之單位或公司內部的稽核單位進行複查，避免有漏盤之狀況發生。

3. 個人資料作業流程識別及個人資料盤點之作業程序

綜合商品零售業者應建立個人資料作業流程識別及個人資料盤點之作業程序，適用於各部門所轄之個人資料作業流程識別及個人資料盤點相關流程。業者可參考以下 BS 10012 PIMS 個人資訊管理系統國際標準之部分內容，訂定適合之作業程序：

3.1 作業流程識別程序

於個人資料管理作業執行之初，須先進行與個人資料相關服務流程識別，辨識含有個人資料相關之作業流程，並根據識別結果填具「個資相關流程識別清單」(附錄七)。

3.2 個人資料盤點項目與程序

根據作業流程識別結果，對含有個人資料相關之作業流程內的個人資料檔案進行盤點，並填具「個人資料盤點表」(附錄八)。

3.3 個人資料相關作業流程識別清單及個人資料盤點表製作與維護

3.3.1 個人資料相關作業流程識別清單及個人資料盤點表製作

應分別就該部門之個人資料相關作業流程識別及個人資料盤點製作「個人資料相關作業流程識別清單」及「個人資料盤點表」。

3.3.2 維護表單內容之正確性

個人資料保護管理小組應進行彙整與維護「個人資料相關作業流程識別清單」及「個人資料盤點表」，應於作業流程及個資檔案新增、作廢、異動(如作業流程及個人資料檔案內容調整或管理人員異動)時，適時更新調整之「個人資料相關作業流程識別清單」及「個人資料盤點表」。

3.4 個人資料相關作業流程識別作業

3.4.1 個人資料相關作業流程識別清單包括編號、主流程名稱及子流程名稱。

3.4.2 主流程名稱係指與會牽涉到個人資料之主要業務或服務流程的名稱。

3.4.3 子流程名稱係指上述服務或流程之細項流程。

3.4.4 選定與個人資料相關作業流程

就「個人資料相關作業流程識別清單」之流程識別結果，選定包含個人資料檔案之作業流程進行後續個人資料盤點作業。

3.5 個人資料盤點作業

3.5.1 個人資料盤點表欄位

3.5.1.1 個人資料盤點表包含作業流程名稱、個人資料檔案基本資訊、資料流、一般個資、特殊類別個資、自訂高風險個資、其他可識別個資、特殊保護方式、保存等欄位。

3.5.1.2 作業流程名稱係指包含編號、主流程名稱、子流程名稱等欄位。

3.5.1.3 個人資料檔案基本資訊包含個人資料檔案名稱、檔案型態、當事人、保有依據、保有依據說明、特定目的、個人資料類別等欄位。

3.5.1.4 資料流包含組織身分、資料來源、組織內部提供者、組織內部接收者、資料處理者、第三方、國際傳輸、組織身分補充欄位等欄位。

3.5.1.5 一般個資包含姓名、生日、身分證號、護照號碼、特徵、婚姻、家庭、教育、職業、聯絡方式、財務情況、社會活動、網路識別資料、定位資料等欄位。

3.5.1.6 特殊類別個資包含種族、政治、信仰、工會身分、生物資料、性傾向、性生活、基因、病歷、醫療、健康檢查、犯罪前科。

3.5.1.7 自訂高風險個資包含財產資料、所得資料、營業

資料、納稅資料等欄位。

3.5.1.8 其他可識別個資包含其他直接識別、其他間接識別等欄位。

3.5.1.9 特殊保護方式包含控制措施欄位。

3.5.1.10 保存包含儲存位置、法定保存期限、自訂保存期限、銷毀方式等欄位。

3.5.2 檔案型態、當事人及保有依據

3.5.2.1 檔案型態係依據部門內已規範之檔案型態屬性。

3.5.2.2 當事人係所蒐集個人資料之來源，客戶，如客戶、離職同仁。

3.5.2.3 具保有依據係保有該個人資料檔案依據相關法令、合約或書面同意等。

3.5.3 特定目的及個人資料類別

特定目的及個人資料類別係依據法務部公告之個資法之「特定目的及個人資料之類別」。

3.5.4 資料流

3.5.4.1 組織身分：盤點單位對所蒐集個人資料檔案之角色，如資料控制者、資料處理者或共同資料控制者。

3.5.4.2 資料來源：個人資料蒐集之方式，如直接蒐集、間接蒐集或直接及間接蒐集。

3.5.4.3 組織內部提供者：與該個人資料檔案之蒐集、處理及利用流程有關且為資料來源之部門。

3.5.4.4 組織內部接收者：與該個人資料檔案之蒐集、處理及利用流程有關且為資料交付出去之部門。

3.5.4.5 資料處理者：代為蒐集、處理及利用個人資料之機構或人員。

3.5.4.6 第三方：與組織之個資檔案蒐集、處理及利用流程有關，但無法歸屬於前述利害關係人類型之機構或人員，如其他公務機關名稱、國稅局等。

3.5.4.7 國際傳輸：個人資料檔案之蒐集、處理及利用流

程中涉及跨國境傳輸。

3.5.5 一般個資、特殊類別個資及其他可識別個資

姓名、生日、身分證號、護照號碼、特徵、婚姻、家庭、教育、職業、聯絡方式、財務情況、社會活動、網路識別資料、定位資料、種族、政治、信仰、生物資料、性傾向、性生活、基因、病歷、醫療、健康檢查、犯罪前科、其他直接識別、其他間接識別等個人資料項目之識別係依據個資法所定義之個人資料。

3.5.6 自訂高風險個資

依據部門內已規範之高風險個資屬性，識別所盤點之個人資料檔案，是否包含高風險個資。

3.5.7 特殊保護方式

依據個資屬性所實施之適當控制措施，例如檔案加密、欄位隱碼等。

3.5.8 保存

3.5.8.1 儲存位置：係指個人資料檔案之儲存位置。

3.5.8.2 保存年限：區分法定保存期限及自訂保存期限，分別指定業務相關法規與子法等所規範之法定保存期限及部門內所規範之個人資料檔案的保存年限。

3.5.8.3 銷毀方式：係指個人資料檔案之銷毀方式。

3.6 作業流程識別及個人資料盤點時機

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內之流程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，以及「綜合商品零售業個人資料檔案安全維護管理辦法」第 17 條之規定，應建立個人資料之風險評估及管理機制，並執行個人資料風險評估及管理作業。但是在執行個人資料風險評估及管理作業前，應確認個人資料盤點作業之完整性及正確性，以確保個人資料風險評估及管理作業之有效性。

（二）本程序可協助業者藉由盤點程序所完成之盤點表內容，界定個人資料檔案之風險值，並透過風險回應措施，有效的採取安全維護措施及應變機制，以降低個資事故發生的可能性。

（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。

1. 風險評估

「風險評估」的目的在於識別可能導致風險發生的原因(包含本身的弱點與可能的威脅來源 )。風險的發生可能來自四面八方，無論來自內部或外部、天然的或人為，惡意或非惡意，都可能形成風險。風險通常會利用組織或資產的弱點，對組織造成潛在損害或實質上的損失。

目前實務上最常發生的情形，像是來自組織外部、人為的且惡意的駭客入侵。另外，還包含利用組織或資產本身所存在的弱點，間接導致損害的產生，例如紙本文件具有易燃、方便攜帶的特性，而毀損、滅失或竊取含有個人資料的紙本文件。

2. 風險管理

「風險管理」是針對個人資料所面臨的可能風險，提出相對應的管理策略。組織針對其保有之個人資料風險評估出來後，即可找到自身弱點所在，進而研擬風險對策進行管

控。

原則：關於風險評估之具體標準及實務作法，可參考經濟部標準檢驗局公布的 CNS 27005「資訊技術—安全技術—資訊安全風險管理」與 CNS 31000「風險管理—原則與指導綱要」等國家標準。內容包含下列 4 項處理原則：

2.1 風險修改

在符合風險評鑑及風險處理要求下，選擇適切及經過衡量的控制措施，以管理風險。控制措施內容可以是矯正、消弭、預防、偵測及監視等方式。藉由施行、移除或改變控制措施可管理風險等級，進而使殘餘風險被控制在可接受範圍。

2.風險保留

風險經評估過後，若特定的風險明顯符合組織內部個人資料管理政策的風險接受準則，則該風險可以保留，但建議組織可以預先提撥風險準備金，用以確保風險結果實現時，能支應相關費用與損害賠償。

3.風險避免

當特定風險持續增加或持續發生，而且接受或保留風險可能會為組織帶來損失或不利影響時，應該規劃避免風險的措施（包括避免產生風險的情形繼續發生，或變更目前產生風險的運作情形）。例如將實體檔案或儲存媒體存放於上鎖空間中；設置防火牆等機制；加強員工個資保護相關教育訓練等。

4.風險分擔

經過風險評估後，可以將特定風險結果請求第三方進行有效管理。例如透過分包方式將監視資料系統的風險，轉交由資訊安全機構協助相關業務。值得注意的是，組織所管理風險的賠償責任，無法透過分包方式轉由第三方承擔。

四、訂定個人資料安全維護規定

（一）個人資料侵害事故預防、通報及應變作業程序。

業者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，以及「綜合商品零售業個人資料檔案安全維護管理辦法」第 12 條之規定， 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，確保消費者個人資料侵害事故發生時，能夠立即採取適當措施，其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，並於發現事故時起七十二小時內，通報主管機關(經濟部商業發展署)。如向地方主管機關通報者，並應副知中央主管機關(經濟部商業發展署)。
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。
4. 通知個資當事人的方式可以透過言詞、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。當前述通知方式需要的花費過鉅的時候，組織在斟酌技術的可行性與當事人隱私的保護情況下，可以透過網際網路、新聞媒體或其他適當公開方式為之。
5. 除了避免個資事故發生之相關安全措施，組織應於事前訂定個資事故緊急應變措施，以防個資事故發生時可緊急應變處理，於短時間將損害降至最低。實務上常見組織訂有個資事故緊急應變之程序，但實際內容卻無明確通報窗口與運作機制，這樣會導致事故發生時組織內部無法有效應變。
6. 個資事故緊急應變措施應該有明確的流程，如此一來才能於事故發生的第一時間緊急處理。另外，組織所訂定之個

資事故緊急應變措施，關於通報部分，往往僅有規定內部通報，而疏忽個資法通知當事人部分。

7. 我國個資法規範個資事故之態樣，並非侷限於竊取而已，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。

8. 對於事故通知當事人之內容應該要明確，並以書函、簡訊等方式通知當事人個人資料被侵害之事實、事故經過、個人資料處理情形及事後所採取之因應措施等。相關人員事後需檢討事故發生之原因並研擬預防措施，對於因個資事故可能發生之訴訟或損害，也應該加以分析評估。

※個資事故通知當事人範本參照附錄九

（二）符合個人資料保護法相關法令規定之內部管理程序。

業者蒐集、處理或利用個人資料時，應該符合個人資料保護相關法令，以及依「綜合商品零售業個人資料檔案安全維護管理辦法」第 6 條第 1 款之規定，應訂定相關的內部管理程序，包括以下事項：

1. 蒐集、處理或利用有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之消費者個人資料者，檢視是否符合個人資料保護法第 6 條第 1 項但書所定情形。

2. 檢視消費者個人資料蒐集或處理，是否符合個人資料保護法第 19 條第 1 項所定之法定情形及特定目的；經當事人同意而為蒐集或處理者，並應確保符合個人資料保護法第 7 條第 1 項之規定。

3. 檢視消費者個人資料之利用，是否符合蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否符合個人資料保護法第 20 條第 1 項但書所定情形；經當事人同意而為特定目的外之利用者，並應確保符合個人資料保護法第 7 條第 2 項之規定。

4. 檢視消費者個人資料之蒐集是否符合個人資料保護法第 8 條第 2 項或第 9 條第 2 項得免為告知之事由；無得免為

告知之事由者，並應確保符合個人資料保護法第 8 條第 1 項或第 9 條第 1 項之規定。

5. 利用消費者個人資料行銷而當事人表示拒絕接受行銷者，確保符合個人資料保護法第 20 條第 2 項及第 3 項之規定。

6. 委託他人蒐集、處理或利用消費者個人資料者，確保符合個人資料保護法施行細則第 8 條之規定，並於委託契約或相關文件明確約定其內容。

7. 當事人行使個人資料保護法第 3 條所定權利之相關事項：

   7.1 提供當事人行使權利之方式。

   7.2 確認當事人或其代理人之身分。

   7.3 檢視是否符合個人資料保護法第 10 條但書、第 11 條第 2 項但書及第 11 條第 3 項但書所定得拒絕其請求之事由。

   7.4 依據前目規定拒絕當事人行使權利者，應附理由通知當事人。

   7.5 就當事人請求為准駁決定及延長決定期間之程序，並應確保符合個人資料保護法第 13 條之規定。X

   7.6 當事人請求更正或補充其個人資料者，其應為釋明之事項。

   7.7 就當事人查詢、請求閱覽或製給複製本之請求酌收必要成本費用者，應明定其收費標準。

   7.8 設置聯絡窗口供當事人申訴與諮詢。

8. 維護消費者個人資料正確性之機制；個人資料正確性有爭議者，並應確保符合個人資料保護法第 11 條第 1 項、第 2 項及第 5 項之規定。

9. 定期檢視消費者個人資料蒐集之特定目的是否已消失或期限是否已屆滿；其特定目的消失或期限屆滿者，並應確保符合個人資料保護法第 11 條第 3 項之規定。

10. 組織除了訂定個資法相關法令規定之內部管理程序，最重要的是要遵守程序規範。個資管理制度上著重「說、寫、做 」三者需一致，也就是程序書、人員認知與實際執行方

式要同一。實務上常見空有內部管理程序，卻無落實、程序書規範和組織內部執行不一，或是程序書與內部業務根本無法扣合，這在個資管理制度上都不是有效管理，也容易造成管理上風險。

11. 委外管理也是實務上常被忽略的部分，組織於程序書上往往制定相當嚴謹之管理規範，例如每半年對委外廠商進行查核、委外廠商合作終止後會進行個資刪除銷毀，但實際上卻無執行，造成個資管理上之漏洞，需加以注意。

12. 實務運作上，組織之隱私權政策、隱私權聲明或是公告，都必須納入上述有關個資法之管理事項。並且建立文件化之程序。隱私權公告與個資告知聲明，應確保在蒐集個人資料之前，提供給當事人或讓其能顯而易見。例如業者為了受理民眾申辦電信相關業務，可於業者門市現場明顯處，以立牌方式公告說明其隱私權聲明，以達到告知隱私權政策的目的。

13. 個資告知聲明要清楚說明，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。須特別注意的是，對於蒐集目的的說明不應該模糊，或以概括方式表述。如果告知的內容並不符合實際個資蒐集使用情形，可能就不符合「 明確告知 」規定。因此，業者提供給個資當事人的個資聲明，必須因應不同業務內容，調整使用目的說明。

14. 國際傳輸

依據個人資料保護法第 21 條，以及綜合商品零售業個人資料檔案安全維護管理辦法第 8 條第 3 項之規定，業者原則上可以將個人資料進行國際傳輸，但是有下列之情況，中央目的事業所管機關可以限制之：

14.1 涉及國家重大利益。

14.2 國際條約或協定有特別規定。

14.3 接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。

14.4 以迂迴方法向第三國（地區）傳輸個人資料規避個人資料保護法。

14.5 除此之外，為了確保個人資料受到充分保護，業者將個人資料作國際傳輸時，應該告知該消費者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，以及當事人行使個人資料保護法第三條所定權利之相關事項。

14.6 個人資料保護法係採分散式管理，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，目前依個人資料保護法第 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。經濟部則尚未針對國際傳輸有公告限制之情形。惟綜合商品零售業者如有將當事人個人資料為國際傳輸之情形，仍應持續關注經濟部日後是否有公告限制，並遵守相關規範。

（三）個人資料委外處理管理程序

依我國個人資料保護法施行細則第 8 條及「綜合商品零售業個人資料檔案安全維護管理辦法」第 19 條之規定，具體要求綜合商品零售業者將個人資料之蒐集、處理或利用委託他人為之，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本法相關法令之要求。

1. 個資委外法律關係

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。」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，視同本公司，並遵守「綜合商品零售業個人資料檔案安全維護管理辦法」之規定。

2. 委外監督

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：

2.1 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。

2.2 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。

2.3 有複委託者，其約定之受託者。

2.4 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，應向本公司通知之事項及採行之補救措施。

2.5 委託機關如對本公司有保留指示者，其保留指示之事項。

2.6 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。

2.7 受託者僅得於本公司指示之範圍內，蒐集、處理或利用個人資料。

2.8 受託者認本公司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，應立即通知本公司。

3. 委外流程控管步驟

3.1 步驟一：選擇受託人

以適當評估方式選擇具品質的廠商適當評估方式，例：委外廠商執行業務安全評估表，評估項目可包括：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。

3.2 步驟二：締結委託契約

如：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。

※委外廠商個資安全維護聲明書（範例）參照附錄十

3.3 步驟三：控管受託人

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。評核要項可包括：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。

3.4 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。

4. 委託作業常見問題

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；契約內容未包含個資保護條款；相關人員未簽具保密切結書；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；未定期確認委外廠商個人資料保護執行情形，如：委外查核；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…等。

（四）個人資料安全管理程序

業者因執行業務而蒐集、處理或利用消費者個人資料時，應依個人資料保護法施行細則第 12 條第 2 項第 6 款、第 8 款，以及綜合商品零售業個人資料檔案安全維護管理辦法第 9、10、13 條之規定，訂定個人資料安全管理程序，包括資

料安全管理、人員管理、安全措施、設備安全管理，以及第8條第2項於傳輸個人資料時，應採取避免洩漏之必要保護措施，以確保個人資料檔案之機密性、完整性及可用性，防免個人資料被竊取、竄改、毀損、滅失或洩漏。因此業者應針對所保有之個人資料檔案進行下列資料安全管理事項之維護：

1. 資料安全管理

1.1 依據業務作業需要及性質，建立管理機制以規範個人資料蒐集、處理、利用及其他相關流程，並設定所屬人員不同之權限。

1.2 定期檢視所屬人員不同權限之適當性及必要性。

1.3 要求所屬人員就所保有之個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他存放媒介物時，應妥善保管個人資料之儲存媒介物。

2. 人員管理

2.1 與所屬人員約定個人資料保管及保密義務。

2.2 所屬人員離職時取消原在職之識別碼，並要求將執行業務所持有他人個人資料辦理交接，不得於離職後繼續使用。

3. 安全措施

3.1 採行使用者身分確認及保護機制。

3.1.1 使用多因素認證機制（ Multi-Factor authentication, MFA ），帳號密碼應符合一定複雜度。密碼複雜度：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。

3.1.2 連線紀錄管理：當使用者登出或登入閒置超過一定時間時，自動將連線紀錄刪除，確保不被未經授權者接管使用。

3.2 採行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，應採取適當之加密或遮蔽機制，避免用戶真實資

料可能遭第三方瀏覽。

3.3 採行網際網路傳輸之安全加密機制。

3.3.1 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。

3.3.2 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。

3.4 採行個人資料檔案與資料庫之存取控制及保護監控措施。

3.4.1 監控與日誌紀錄：當資料庫活動異常時發出告警通知相關人員。紀錄與保存所有資料庫操作，包含登入、查詢、更改、刪除等。

3.4.2 存取權限控制：限制特殊權限帳號才能登入資料庫操作及設定。

3.5 採行防止外部網路入侵對策。

3.5.1 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）。

3.5.2 防火牆：設定允許存取來源、目的及服務，將非法流量阻擋。

3.5.3 入侵偵測系統：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。

3.5.4 網頁防火牆：阻擋針對網頁攻擊例如：SQL Injection、跨站攻擊，惡意檔案上傳。

3.6 採行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，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。

3.9 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

4. 設備安全管理

4.1 依據作業內容及環境之不同，實施必要之安全環境管制，妥善維護資料檔案之安全保護設施及訂定管理程序。

4.2 將電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制，並訂定管理程序。

4.3 訂定紙本及電子資料之銷毀程序，並於電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，應以適當方式銷毀或確實刪除該媒體中所儲存之個人資料，確保個人資料完全移除，避免洩漏個人資料。

（五）使用紀錄、軌跡資料及證據保存。

1. 個人資料保護法第 12 條第 2 項第 10 款規定，得採取使用紀錄、軌跡資料及證據保存等適當安全維護措施。而在綜合商品零售業個人資料檔案安全維護管理辦法，則進一步規範：

2. 第 15 條：綜合商品零售業者訂定第六條第八款所定使用紀錄、軌跡資料及證據保存之措施，應包括下列事項：一、留存個人資料使用紀錄。二、留存自動化機器設備之軌跡資料或其他相關之證據資料。綜合商品零售業者，依前項規定留存個人資料使用紀錄、自動化機器設備之軌跡資料或其他相關之證據資料，其保存期限至少五年。

3. 本條立法理由：綜合商品零售業者為證明確實執行安全維護計畫，已盡防止個人資料遭侵害之義務，爰於第一項明定業者應保留之證據，以供日後發生爭議時之佐證。依個資資料保護法第 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，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。」爰於第二項明定留存之使用紀錄、軌跡資料及相關證據資料，至少應留存五年。

4. 是以，業者對於個人資料的使用紀錄、軌跡資料及證據保存，應訂定相關機制並予以落實。這邊所指的機制應包含，為了執行個人資料檔案安全維護計畫及處理方法所定各種

個人資料保護機制、程序及措施，所記錄的個人資料使用情況、軌跡資料及相關證據。

5. 在綜合商品零售業個人資料檔案安全維護管理辦法第 15 條的規範的標的，是指個資的使用紀錄、軌跡資料及證據，非指個資本體而言。

## 五、個資保護認知宣導及教育訓練

(一) 綜合商品零售業者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 7 款，以及綜合商品零售業個人資料檔案安全維護管理辦法第 11 條之規定，應定期辦理個人資料保護認知宣導及教育訓練，依照計畫執行人員在計畫範圍及組織內之角色，提供相應的專業教育訓練，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，具有辦理安全維護事項之能力。所有人員均應該接受教育訓練，訓練內容應包括下列事項：

1. 個人資料保護相關法令之規定。
2. 所屬人員之責任範圍。
3. 各種個人資料保護事項之機制、程序及管理措施。

(二) 實務上業者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，可參考以下作法：

1. 定期舉辦宣導個人資料法遵管理相關之教育訓練，以使成員均得瞭解個人資料管理制度之內容，以及個人資料保護之重要性，使個人資料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人資料管理政策，或在資訊系統中之公共資料夾設置「 個人資料保護專區 」等方式，強化個人資料保護認知宣導效果。
3. 個人資料保護相關之教育訓練，業者除可自行培訓講師外，也可以委託外部專家講習，或者是指派企業內之相關成員參與外部訓練等方式進行。

4. 辦理個人資料保護相關之教育訓練或講習時，應記得留存如課程簽到表或測驗成績等相關紀錄，以利後續之稽核時能順利提出有辦理宣導及教育訓練之佐證。

## 六、 查核與改進

依照 PDCA 之精神，組織內規劃並逐步實踐個人資料保護相關安全維護事項的同時，亦應針對其規劃及實踐之個人資料保護相關措施進行「查核」(個人資料安全稽核)，並力求持續「改進」(個人資料安全維護之整體持續改善)。

### (一)「查核-Check」(個人資料安全稽核)

1. 綜合商品零售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 9 款，以及綜合商品零售業個人資料檔案安全維護管理辦法第 14 條之規定，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，向綜合商品零售業者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，應予以記錄及追蹤，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的有效性和效率。
2. 為確保查核制度獨立及確實執行，綜合商品零售業者依第五條規定指定之專責人員與本條第一項規定之查核人員，不得為同一人。

### (二)「改進-Act」(個人資料安全維護之整體持續改善)

1. 綜合商品零售業者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，以及綜合商品零售業個人資料檔案安全維護管理辦法第 17 條之規定，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，以求動態地實踐個人資料保護之相關政策、機制，達個人資料安全維護之整體持續改善之成果。
2. 業者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。

七、 業務終止

（一）業者合法蒐集、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，依據綜合商品零售業個人資料檔案安全維護管理辦法第 16 條第 1 項之規定，綜合商品零售業者於業務終止後，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。爰終止業務之業者，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，以便日後得以提出舉證。

（三）而依個人資料保護法第 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，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。」爰明定銷毀、移轉、刪除、停止處理或利用個人資料之紀錄至少應留存五年。

（四）以上規範與個人資料本體(例如當事人的活動報名表)的保存無關。個人資料保存應該有一定之期限，組織應依照該個人資料性質訂定。若有法定保存期間的規定，需依照法定保存期間保存以符合法規要求，或企業自訂之保存期限進行保存，不一定需要保存 5 年，例如舉辦抽獎活動，就活動參與人的個資(個資本體)，可訂於活動結束後銷毀。

（五）在綜合商品零售業個人資料檔案安全維護管理辦法第 16 條的規範的標的，是指個資的銷毀、移轉及刪除措施(非個資本體)等資料。

（六）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，並經權核主管覆核，以作為存證紀錄，以供日後查核之佐證。

## 八、個人資料庫之共享使用

業者如與其他其他關係企業或主體共享使用所蒐集之客戶個人資料庫，應明確告知當事人個人資料保護法第 8 條第 1 項之事項。實務上常見業者之「隱私權政策」僅載明「會員個人資料蒐集、處理及利用之主體為本公司(本公司包括 00 公司及其關係企業)」，由於 00 所屬關係企業之具體名稱未逐一揭示或提供資訊供消費者確認，對消費者或會員來說，其蒐集、利用之機關主體不明，違反個人資料保護法第 8 條第 1 項第 1 款之情形。

## 九、個資存放雲端之安全控管

業者應妥善評估使用雲端服務儲存消費者或會員個人資料之妥適性及必要性，並應確認其儲存之資料庫安全性。有鑑於雲端技術的發達，個人資料的跨境傳輸已是常態，尤其業者多尋求租用境外雲端服務，來執行相關業務。依據個人資料保護法目前的規定，仍以原則開放、例外限制的方式來對境外傳輸進行規範，但業者仍然應確保個人資料被移轉到境外進行處理利用時，仍受到充分的保護。因此，業者在使用境外雲端服務時，須特別注意雲端服務提供者之合約條款，是否有盡到相關安全義務，例如透過一些國際標準之認證來做為判斷基礎，以確保消費者或會員個人資料放在雲端上的安全。

# Chapter4

# 個資事故案例

## 肆、個資事故案例

案例一：○○航空個資外洩案(臺灣臺北地方法院 106 年度北小字第 2161 號判決)

「被告(即○○航空)因原告訂購機票而取得原告之姓名、電話號碼及搭乘客機活動等個人資料，依法應採行適當之安全措施以防止該個人資料被竊取或洩漏，被告倘未能舉證證明已盡此注意義務，即可認有過失，原告因而個資被竊取或外洩，自得依個人資料保護法第 29 條之規定請求被告為財產上或非財產上之損害賠償。

而關於本件被告過失行為與原告個資外洩之間具備相當因果關係等歸責要件之舉證，即被告未依法訂立個人資料檔案安全維護計畫及安全稽核機制致駭客入侵竊取原告個資，抑或因而遭被告公司人員外洩等情，惟此等事實因宥於網際網絡科技浩瀚並參雜人為因素之變異而有高度舉證困難，責令被害人擔負完全之舉證責任實有不公；而被告既為以此交易營利之企業經營者，原告交付個資後即由其支配掌握，其對於個資被竊取或外洩風險之控制及分擔能力俱優於原告；抑有進者，航空業者對旅客個資之維護義務，除建立在個人資料隱私權之保護外，亦有防免旅客個資外洩致影響飛航安全等重大風險實現，是本院斟酌本件訴訟性質、兩造之舉證能力及被告違反義務之情節及風險分配之合理性，而比照我國實務就公害訴訟降低被害人因果關係舉證責任之見解，認被告行為所生之危險已有相當合理確定性，即推定有一般因果關係之存在（最高法院 102 年度台上字第 31 號判決參照），被告倘認無一般或個別因果關係存在，自應提出確切之反證證明。」

案例評析：

倘業者保有之消費者個資外洩，法官會要求企業經營者舉證有採行適當之安全措施，證明已履行法律上要求的注意義務，若企業無法舉證證明，消費者得依個人資料保護法第 29 條之規定請求企業為財產上或非財產上之損害賠償。故企業平時就應依個人資料保護法及主管機關頒布之個人資料檔案安全維護管理辦法，訂定個人資料檔案安全維護計畫，並落實個人資料檔案之安全維護及管理，防止個人資料被竊取、

竄改、毀損、滅失或洩漏。

案例二：○○購票平臺個資外洩

2017 年被害人使用手機登入○○購票平臺，購買 2 張電影票，卻在兩個禮拜後，接到假冒○○購票平臺的會計部門人員的電話，對方核對了被害人的姓名、電話，以及購票日起、場次與金額，接著謊稱作業人員疏失，誤植 20 筆原告之訂票紀錄（約 8,000 元），將會每月扣款，因而誆稱需要被害人協助授權才能向被害人的銀行退費。

由於對方清楚說明了訂票資訊，這也導致被害人不疑有他而上當，一共被騙走 25 萬 7,892 元。因此，張女透過臺灣士林地方法院，向經營○○購票平臺的公司提告，請求侵權行為損害賠償共 32 萬元，包含被騙損失的 25 萬多元，以及個資法第 29 條規定的 2 萬元賠償，還有個資外洩帶來的精神慰撫金 5 萬元。二審判決結果指出經營○○購票平臺的公司也應對用戶遭詐欺侵權行為的損害賠償，負起 7 成過失責任，最後判定廠商應賠償 18 萬餘元，且不得上訴。

判決內容指出，根據刑事警察局統計，在用戶購票與接到詐騙電話期間，警方在兩週內，已經分別接獲 30 件與 26 件的民眾通報○○購票平臺為高風險平臺。而從當年的資安事件分析報告中，也可得知這些交易所涉的內容僅有該公司完整掌有，因此足以認定資料是從○○購票平臺外洩。而個資外洩與後續遭詐騙而造成的損害，有相當因果關係，如果沒有這些明確資料，民眾應不致於陷於錯誤而遭詐騙。另外，法院認定其網路平臺之內部及外部風險控制存有諸多缺陷，並且未能完全落實其個人資料保護的管理。例如，法院也參考了當時資安業者調查的資安事件報告，蒐證暨分析目標主機，發現有多項 Log 記錄不完整的情況，甚至目標伺服器的 Audit Log 並無當年度完整的記錄，以及像是 SSH 登入權限未限縮並稽核，還有內部機敏資料被上傳到外部雲端硬碟的狀況。

案例評析：

業者需重視內部及外部風險控制，與個資保護，以盡適當安全防護之責。一旦被通報為高風險網站，應盡快採取因應採取並諮詢外部資安及個資顧問，協助企業找出漏洞，提升資安防護措施並落實個資保護作為，避免個資外洩的情形持續發生並衍生許多詐騙案件。

案例三：某魯肉飯連鎖餐飲業者遭遇勒索軟體攻擊

2021 年某魯肉飯連鎖餐飲業者遭遇勒索軟體攻擊，業者共遭遇了兩波攻擊，由於首波攻擊後，業者拒絕對方勒索，因此第二次攻擊後，對方利用公司電子郵件帳號寄送勒索信，而信中指出已竊取該公司部分資料，如不付贖金，將公開他們手上的資料。

該公司已主動發布資安事件公告，並陸續通知會員，說明會員資料(包括姓名、電子郵件信箱、電話號碼、地址、身分證字號等)被竊取的風險。

該公司由於各項系統及資料均有備份管理，因此他們皆能夠完成復原工作，但他們也調整了備份機制的頻率、調整防火牆政策，同時尋求系統商協助，增加端點防護軟體進行分析與防護，以利於後續可能事件的反應。

為了維護會員權益，業者也提供會員該如何因應的做法，包括盡速更改會員密碼，以及其他網站密碼(如果用戶設定了相同的密碼)，同時，他們先行提醒，若接獲自稱業者客服人員等不明人士來電，應提高警覺，小心對方要求提供財務資料或詐騙等行為，建議打 165 防詐騙專線求證。

案例評析：

過去常發生個資外洩的企業型態，如網路業、金融業者或醫療保健業等，但隨著傳統業者進行數位化轉型的腳步，透過虛實整合強化市場行銷的力道，尤其利用 APP 等資通系統大量蒐集、處理及利用消費者或會員之個人資料的趨勢，已使得任何行業都有發生資安及個資事件的風險，更必須在數位化轉型的同時強化資安防護措施並落實個資保護作為。

案例四：某百貨業者遭網路攻擊，該公司發布即時重大訊息

某百貨業者遭網路攻擊，該公司在 00 年 00 月於臺灣證券交易所發布即時重大訊息，說明部分資訊系統受資安事件影響。相隔兩日，在臉書粉絲專頁指出其顧客會員系統從 14 日即無法正常運作，正持續修復中。根據這次公告內容，他們偵測到部份資訊系統受到駭客網路攻擊，資訊部門已啟動相關防禦機制與復原作業，並與外部資安公司技術專家協同處理，同時也已通報政府執法部門。

案例評析：

在臺灣，隨著這幾年上市櫃公司不斷傳出發生資安事件，金管會在 2021 年開始修正相關法令，強化上市上櫃公司資訊安全管理機制，由以下三大面向推動強化公司資通安全管理：

一、資訊揭露：

要求上市櫃公司於發生重大資安事件時，應即時發布重大訊息，另亦應於年報及公開說明書中敘明資通安全管理政策及方案、投入資源、資安風險影響程度與因應及所遭受重大資通安全事件之影響。其中，在發布重訊方面，金管會表示，一旦造成公司重大損害或影響，必須在台股開盤前 2 個小時（上午 7 點以前），要對外發布重大訊息，若未揭露依法可處以「3 萬~500 萬元罰鍰」。

二、公司治理：

金管會業依資本額規模、市值、業務性質及營運狀況等劃分上市櫃公司為 3 等級，分階段要求配置資訊安全人力資源，其中第一級公司 115 家已於 111 年底完成設置資安長、資安專責主管及人員；第二級公司 1387 家預計於 112 年底前完成設置資安專責主管及人員。另為積極協助上市櫃公司完善資通安全防護及管理機制，證交所及櫃買中心並已訂定資通安全管控指引供公司參考。

三、監理協助：

金管會透過鼓勵方式推動上市（櫃）公司依風險等級分期加入台灣電腦網路危機處理暨協調中心共享資安情資；此外公司導入「ISO 27001」、「CNS 2700」 等資訊安全管理系統標準或「取得其他第三方驗證」之標準，並已納入 111 年度公司治理評鑑指標加分項目。

案例五：《個資法》上路後首例，某量販店濫發廣告信判賠 2.6 萬
某男子在 101 年 6 月寫電子郵件向某量販店表明退出會員，並要求刪除會員資料，量販店也回函告知男子「不會再收到型錄、優惠訊息」，但男子在拒絕量販店廣告電郵之後的半年間仍收到 52 封，某男子因而提告，並向某大賣場求償 10 萬元。

雖然量販店辯稱這些郵件是制式的產品促銷，「僅是大量垃圾郵件中的小部分」，不會造成消費者困擾。但法官審酌，男子已要求刪除個人資料，量販店仍利用某男子的個資寄送廣告電郵，明顯觸法。

依《個人資料保護法》規定每一事件（郵件）可判賠 500 元以上、2 萬元以下，最高總額不超過 2 億元。法官認定新法實施前，寄 36 封廣告電郵給男子，應賠 1 萬元，實施後寄 16 封，一封賠 1000 元，共判量販店須賠 2 萬 6000 元。

案例評析：
對於一間具規模的公司，資訊系統架構是非常多且複雜的，會員資料可能分散在不同系統、主機及雲端服務上，且因為時間久遠及員工異動的狀況下，系統人員對於異常情形常無法有效執行的問題。
此外，還有行銷單位的問題，通常行銷單位都會有很多份的名單，來源也許來自於公司會員資料庫、線上活動、實體活動及配合的活動平台，這些名單也會部分重疊。
因此，當事人要求公司(不管是透過官網、電話或電子郵件)將其會員資料刪除後，由於公司第一手處理的員工未即時透過相關流程以及系統的確認，很容易發生未能全面的將當事人留存在公司各個系統或作業面上的當事人個資刪除。
提醒業者應建立及落實個人資料作業流程識別及個人資料盤點之作業程序，並配合當事人權利行使的內部控管作業流程，從管理及技術上的措施，以因應當事人權利行使之時進行工作的落實完成。

案例六：某汽車運輸業用戶 10 萬個資遭流出，機敏資料門戶大開

2023 年國外一名安全研究員 Anurag Sen 發現，某汽車運輸業共享汽機車服務其中一組雲端資料庫沒有加密保護，任何知道該資料庫 IP 位址的人都可存取用戶姓名、手機、電子郵件、地址、經過 base64 編碼之圖檔，以及部分信用卡資訊等機敏資料。

根據資料庫搜尋引擎 Shodan 紀錄顯示，該資料庫資料量高達 4.2TB，存放於該汽車運輸業者的雲端伺服器中，且並未受到密碼保護，任何使用者只要知道 IP 地址，即可進入資料庫查詢 3 個月內知會員異動資料，而網路瀏覽器 Shodan 數據顯示，該資料庫約從 2022 年 5 月就開始洩漏資料，直到 2023 年 1 月才被發現，國外研究員於 1/28 日發送電子郵件通知該汽車運輸業者，然而卻未收到回應，且該資料庫還在持續更新。

外媒聯絡數位發展部，數位發展部第一時間將此事轉由「台灣電腦網路危機處理際協調中心(TWCERT/CC)」處理，讓資料庫無法進入。

該汽車運輸業者證實知悉資料外洩，並立即切斷該資料庫 IP 的外部連接，將再次對主機系統做弱點及滲透掃描，並確保用戶交易過程全程採加密，以及導入 ISO27701 隱私資訊管理系統，加強資安防護。

案例評析：

有鑑於雲端技術的發達，尤其業者多尋求租用雲端服務，業者更應重視個資存放雲端之安全控管，妥善評估使用雲端服務儲存消費者或會員個人資料之妥適性及必要性。本案業者的資料庫未加密已長達 9 個月，若曾遭惡意駭客存取，可能引發釣魚郵件、信用卡盜刷等風險。

個資存放雲端之安全控管：

1. 資料庫位置使用非公開 IP，阻絕不明外部存取要求
2. 依主管機關規定擬定相關個資安全維護計畫資料
3. 監控資料庫活動，以便及時發現異常流量
4. 確實執行與管理 ISO27001,27701 等資安制度要求，增強防護
5. 事故發生後立即填寫侵害通報與紀錄表，通報主管機關並立即發布聲明稿，向用戶說明事件緣由及防護措施
6. 確認有無其他系統存在風險，並確認事故影響範圍，避免災情擴大
7. 檢討資料安全管理措施，擴大與第三方資安廠商合作

8. 擬定完善諮詢管道及用戶補償措施，提醒用戶可能風險
9. 導入 EDR(端點偵測與回應)、MDR(威脅偵測應變)，加強端點防護

案例七：某百貨業者 爆 90 萬筆個資外洩

○年○月 17 日，不知名人士在駭客論壇上表示掌握某百貨 90 萬筆客戶的個資，亦包括公司內部所有的業務資料、供應商數據、發票、訂單、付款資料等，甚至還有 30 個專案原始碼，總計超過 150GB，駭客並稱個資中包括會員帳號密碼還附上不少電腦畫面截圖，有媒體形容該百貨業者是「整個資料庫被打包帶走」。

對此，該百貨業者證實，近日有收到匿名網路勒索信件，第一時間已立即啟動損害機制，目前內部資安團隊已完成軟體以及作業系統安全性更新，同時提高資安防護層，呼籲共同打擊此類不法行為，並全力配合警方偵辦調查。

該百貨業者也說，經內部清查確認，外流個資與公司資料庫有所落差，因此駭客未必是從該百貨駭入，但仍提醒會員定期修改密碼，以保障個資安全，也勿將密碼等資料交付他人，避免遭不當利用。

案例評析：

業者因執行業務而合法蒐集、處理或利用個人資料時，應建立個人資料侵害事故之預防、通報及應變機制，以確保消費者個人資料侵害事故發生時，能夠立即採取適當措施，其內容至少應包括下列項目：

- 採取適當措施，控制事故對當事人造成之損害，並於發現事故時起七十二小時內，通報主管機關。如向地方主管機關通報者，並應副知中央主管機關。
- 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。
- 檢討缺失，並訂定預防及改進措施，避免事故再度發生。

本案百貨業者證實，有收到匿名網路勒索信件，並稱第一時間已立即啟動損害機制，惟若單純提醒會員定期修改密碼之內容，僅係防詐騙提醒，並無會員個人資料被侵害之事實及已採取之因應措施之通知內容，難認非公務機關已踐行法定通知義務。依個人資料保護法施行細則第 22 條第 2 項之規定，難認該業者已踐行個人資料保護法第 12 條

規定通知當事人之法定通知義務。

# Chapter5

# 自我評核作業

# 伍、自我評核作業

透過「綜合商品零售業個人資料安全稽核檢查表」(附錄五，以下簡稱本表)，提供業者個人資料保護與管理之基礎要求，以協助並引導業者因應法規要求與建立個資保護與管理參考，並鼓勵業者自主管理，期能透過本表，考量營運風險與需求，並訂定符合業者營運現況之個人資料保護與管理制度。而業者更可透過本表，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

本表旨在提供我國相關業者個人資料保護與管理之基礎要求，以法令遵循為主，協助並引導業者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業者自主管理，建議業者可參考本表，但不以此為限，可通盤考量營運風險與業務發展，訂定符合業者本身營運需求之個人資料保護與管理制度。

## 二、使用對象

從事以非特定專賣形式銷售多種系列商品之綜合商品零售業者。

## 三、如何使用本表

1. 本表係依據經濟部於 112 年 8 月 1 日發布之「綜合商品零售業個人資料檔案安全維護管理辦法」之規定，並參照經濟部於行政檢查及行政調查時常見之問題統整，可協助業者依序展開個人資料保護與管理之控制措施。
2. 填寫本表時，建議業者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。

3. 本表填寫步驟如下

3.1 依序由第 1.1 款填寫至第 23.1 款，一共 59 款檢核項目，以本表之稽核內容為基準，並可參考「對應條文」及「備註」欄位，了解本查核項之具體內容或程序文件範例，比對業者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。

3.2.填寫本表時，可併參酌「個人資料保護法」、「個人資料保護法施行細則」，及「綜合商品零售業個人資料檔案安全維護管理辦法」等規範。

# Chapter6

# 常見問題

# 陸、常見問題

Q1. 蒐集個資的企業違反個資法的風險？

說明：

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(賣場)等業者，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。

**歷程三、經濟部明定綜合商品零售業的個資安全維護義務的辦法**

112 年 8 月 1 日訂定的「綜合商品零售業個人資料檔案安全維護管理辦法」，要求綜合商品零售業者需全面採行落實適當之安全措施。故未來經濟部不論是因應所管業者發生個資外洩進行個資行政調查，或對業者進行例行性個資行政檢查，都有更明確的法源依據進行監管。

二、違反個資保護的企業可能面臨高額罰鍰、信用危機、業務被迫中止、破產的系統風險

國內企業一旦違反個資安全維護義務，將面臨到高額罰鍰最重可至1,500 萬元，屆期未改正者並可按次處罰。如不幸發生個資外洩，也將造成企業的信用危機，以國外為例，2018 年 3 月《紐約時報》披露，Facebook 將用戶的個人資料被賣給了劍橋分析公司(Cambridge Analytica)，而劍橋分析公司利用這些資料來預測和影響選民的投票，上開報導對 Facebook 造成極大的重創，Facebook 曾在一天內市值暴跌超過 1000 億美元，這也創下美股史上最大單日跌幅。而在個資外洩事件曝光後，號召刪除臉書的活動，也開始在網路上蔓延。近年來，國內各大公益團體被駭客盯上，捐款資料屢屢外洩，導致有部分捐款人因此選擇停捐，對長期仰賴捐款的非營利組織而言，「停捐」是極大衝擊。此外，也可能發生業務被迫中止，例如 2023 年 5 月歐盟監管機構表示，因為臉書母公司 Meta 將歐盟用戶的數據傳輸到美國，侵犯了隱私權，Meta 被勒令在 2023 年 10 月前停止將用戶數據傳輸到美國。2022 年 Meta 在英國也面臨新官司，被要求停止替「定向廣告」（targeted advertisements）收集個資，這項舉動已觸及臉書的商業模式核心。而在國內，由於企業發生個資外洩的案件頻傳，國發會亦提醒各部會，除了可對違反個資法的企業處以罰鍰外，我國個資法第 25 條第 1 項也有類似的強制措施，主管機關可禁止企業蒐集、處理或利用個人資料、刪除經處理之個人資料檔案等行政處分，一旦主管機關採取，將對企業的營運造成重大衝擊。而在國外「劍橋事件」案例中，劍橋分析公司失去大量的客戶和供應商，因此無法再繼續營運，並聲請破產。以上案例，值得業者警惕。

## 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<br>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： |
| 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) | | 一、禁止蒐集、處理或利用個人資料。<br>二、命令刪除經處理之個人資料檔案。<br>三、沒入或命銷燬違法蒐集之個人資料。<br>四、公布非公務機關之違法情形，及其姓名或名稱與負責人。<br><br>第 50 條<br>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。 |
| 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） | |
| 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.綜合商品零售業應如何著手建立個資保護與管理制度？

說明：

一、參考本手冊初步進行自評

可先初步依附錄五「綜合商品零售業個人資料安全稽核檢查表」進行自評，認知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、文件表單及記錄。

(三)制度輔導落實與內部稽核：

依照所制訂四階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。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. 涉及以網際網路方式零售商品之個資保護事項主管機關認定？

說明：

一、 經濟部已將網際網路零售業安維辦法及相關業務移交予數位部，則自應由數位部續行查處原經濟部所認定適用所移撥之安維辦法當中，轄下以網際網路方式零售商品之零售業。本案「00」所涉以網際網路方式零售商品之個資保護事項，自宜由承受該業務之數位部主責辦理。

二、 至民眾購買 00 股份有限公司產品後，為取得贈品及售後保固等服務，於該公司網站登錄，係基於電器製造業務而生，產品之售後保固等節應屬製造業之相關後續服務，其與本案情形不同，且其應係依主管機關列表285家用電器製造業為該案主管機關屬經濟部之認定，併予釐清。

（國家發展委員會 112 年 8 月 7 日發法字第 1120012957 號函參照）

Q4. 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？

說明：

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。

（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？

說明：

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)

Q6. 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？

說明：

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)

Q7. 前端向消費者「蒐集」、「處理」、「利用」其個資部分，是否三個階段相關紀錄軌跡均須依法保存五年？

說明：

是，應留存相關軌跡紀錄，以明確個人資料使用歷程情形，以供日後倘發生爭議時之佐證。另個資法第 30 條規定之損害賠償請求權，當事人自損害發生時起五年內可行使。故為避免發生損害請求賠償時，相關紀錄已遭提前銷毀，明定應至少留存五年。

Q8. 若本公司向消費者告知該抽獎個資將於活動結束後兩個月銷毀，是否仍應依法保存五年？

說明：

消費者個資可依照活動辦法規範於活動結束後兩個月內銷毀，惟銷毀軌跡紀錄仍應保留 5 年。

Q9. 以 Facebook 抽獎、直播抽獎等方式相關紀錄軌跡銷毀，依法應包括方法、時間、地點及證明銷毀之方式，是否要載明「在辦公司(填上公司地址、部門)，將檔案丟到資源回收桶→清空銷毀」並錄影存證來製作紀錄，或是有其他方式？

說明：

可製作銷毀清冊，將銷毀的方法、時間、地點等紀錄記載。例如舉辦抽獎活動蒐集的個人資料，在活動結束後兩個月，即(某年某月某日)由活動承辦人在權責主管的監視下進行銷毀，方式為承辦人於個人辦公座位上將電腦中保存的電子檔刪除，並將資源回收桶清空。而在每年個資內部稽核時，可由稽核人員檢視銷毀清冊，並抽查承辦人的電腦，是否已確實銷毀而無保存資料。又倘涉及經營提供社群網路服務之入口網站(如 Facebook)者，核屬數位發展部權管之「入口網站經營、資料處理、網站代管及相關服務業之業務」，倘該部另有規定者，仍應符合其規定。

Q10. 承上題，關於本公司內部人事資料(包括但不限於人事資料、應徵者資料、健康檢查資料等)是否「蒐集」、「處理」、「利用」其個資部分，是否三個階段相關紀錄軌跡均須依法保存五年？

說明：

是，應留存相關軌跡紀錄，以明確個人資料使用歷程情形，避免爭議，以供日後發生爭議時之佐證。另個資法第 30 條規定之損害賠償請求權，當事人自損害發生時起五年內可行使。故為避免發生損害請求賠償時，相關紀錄已遭提前銷毀，爰明定應至少留存五年。又倘涉及就業服務法或勞動基準法等勞動契約關係部分，倘勞動部另有規定者，仍應符合其規定。

Q11. 消費者若是以直播留言、Facebook 對話窗或其他通訊方式提供個資參與抽獎，此類個資可能因不同服務平台規範不同，而有持續存在或是短期內消失，是否仍需保留五年？

說明：

可依不同服務平台規範訂定不同保存期間，惟應告知當事人，並於保存期限屆至後進行銷毀，並保留銷毀紀錄至少 5 年。又倘涉及經營提供社群網路服務之入口網站(如 Facebook)者，核屬數位發展部權管之「入口網站經營、資料處理、網站代管及相關服務業之業務」，倘該部另有規定者，仍應符合其規定。

Q12. 承 11 題，此類電子方式提供之個資如何依照《綜合商品零售業個人資料檔案安全維護管理辦法》第 16 條證明銷毀方式、刪除方法、地點等？

說明：

可製作銷毀清冊，將銷毀的方法、時間、地點等紀錄進行記載。例如舉辦抽獎活動蒐集的個人資料，在活動結束後兩個月，即(某年某月某日)由活動承辦人在權責主管的監視下進行銷毀，方式為承辦人於個人辦公座位上將電腦中保存的電子檔刪除，並將資源回收桶清空。而在每年個資內部稽核時，可由稽核人員檢視銷毀清冊，並抽查承辦人的電腦，是否已確實銷毀而無保存資料。

Q13. 企業因業務所需，於實體店面攝錄消費者影像一事，於個資法上應如何檢視合法性？

說明：

一、 對於企業因業務所需，於實體店面攝錄消費者影像一事，於個資法上可循下列步驟檢視合法性：

1. 攝錄影像是否為個人資料

此應檢視攝錄鏡頭依其位置，所拍攝消費者影像是否具有識別性，即可否辨別特定消費者，而與其他消費者有所區別(實務上通常實體店面內的監視錄影設備所攝錄之消費者影像多具有識別性)。

2. 是否適用個資法

依國發會函釋之見，企業基於業務而攝錄消費者影像，即便於公開場所為之，但仍不屬於個資法第 51 條第 1 項第 2 款得排除個資法之例外，因此需適用個資法。

3. 蒐集、處理個人資料是否具備「(正當)特定目的」及「個資法第 19 條第 1 項所列法律依據之一」，且不超過達成目的所須的「必要範圍」：

(1)特定目的

企業於實體店面蒐集消費者影像之特定目的通常為「場所進出安全管理（含竊盜、毀損之預防、舉證等）」、「消費糾紛舉證」等正當目的。

(2)法律依據

依照前述目的，企業應可對應主張個資法第 19 條第 1 項第 2 款「與當事人有契約或類似契約之關係」(為「消費糾紛舉證」之目的）及同條項第 6 款「為增進公共利益所必要」(為「場所進出安全管理」之目的)，作為蒐集、處理個人資料的法律依據。

(3)必要範圍

此處應檢視企業所蒐集之資料是否限於達成目的所須之必要範圍，此於實務上較無一致性標準，需個案判斷（例如為場所進出安全管理之目的攝錄影像，但如該設備尚能收音而蒐集消費者於店內之私人對話，恐即逾越必要範圍）。

4. 企業是否向消費者依個資法第 8 條告知法定事項

除以張貼告示等方式明確讓進入店內之消費者知悉企業攝錄影像外，我國實務上幾乎未見企業針對攝錄影像一事，向消費者告知個資法第 8 條第 1 項所列各款事項（企業名稱、蒐集個資目的、類別、利用之期間/地區/對象/方式、當事人權利及行使方式等）。目前個資法主管機關尚未明確對此表示意見，企業或可主張攝錄消費者於店內之影像屬個資法第 8 條第 2 項第 6 款「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」，作為例外免除告知義務之依據。

5. 利用個人資料是否符合蒐集之特定目的

此處應依具體個案檢視企業利用監視錄影畫面之行為，是否與蒐集之目的相符（例如提交司法機關調查、於法律程序提出舉證等）；若其行為逾越原蒐集之目的，再行檢視是否符合個資法第 20 條第 1 項但書所列各款例外事由之一，否則即屬違法。

6. 其他合規義務

除上述行為的個資法合規檢視外，企業對於店內錄影所保有的個人資料(檔案)，即應與其他消費者個人資料為相同對待，遵循個資法之其他義務，例如個人資料保存期限、當事人權利行使、委外監督等。

二、 至於店員個人對消費者的私人攝錄行為，在實務上多為事後個案判斷是否侵害被攝人權利、有無正當事由等，較難於事前有一致性的判斷標準。司法實務上對於私人「為蒐證目的」攝錄影像蒐集個人資料，即有不構成違法侵害權利的空間，而後續如何利用攝錄畫面（例如僅提出於法律程序舉證，或發佈於社群平台公審等），則會有不同的法律風險。

# Appendix

# 附錄

# 附錄

## 一、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

### 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。

## 二、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。

三、綜合商品零售業個人資料檔案安全維護管理辦法

1. 中華民國 112 年 8 月 1 日發布全文 22 條

第　一　條　　本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。

第　二　條　　本辦法所稱主管機關：在中央為經濟部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。

第　三　條　　本辦法適用之對象為綜合商品零售業者，指從事以非特定專責形式銷售多種系列商品之零售，已辦理公司、有限合夥或商業設立登記，且資本額達新臺幣一千萬元以上，並有招募會員或可取得交易對象個人資料之業者，或受經濟部指定之公司、有限合夥或商業。但不包括應經特許、許可或受專門管理法令規範之行業。

第　四　條　　綜合商品零售業者應依其業務規模及特性，衡酌經營資源之合理分配，規劃、訂定、檢討與修正安全維護措施，並納入個人資料檔案安全維護計畫（以下簡稱安全維護計畫），落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第　五　條　　綜合商品零售業者應指定安全維護計畫之專責人員，負責規劃、訂定、修正、執行安全維護計畫及其他相關事項，並定期向綜合商品零售業者之代表人或經其授權之人員提出報告。

第　六　條　　綜合商品零售業者，應依本辦法規定訂定安全維護計畫，載明下列事項：

一、個人資料蒐集、處理及利用之內部管理程序。

二、個人資料之範圍。

三、資料安全管理及人員管理。

四、認知宣導及教育訓練。

五、事故之預防、通報及應變機制。

六、設備安全管理。

七、資料安全稽核機制。

八、使用紀錄、軌跡資料及證據保存。

九、業務終止後，個人資料處理方法。

十、個人資料安全維護之整體持續改善方案。

第　七　條　　綜合商品零售業者訂定前條第一款及第二款所定事項時，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，並定期清查所保有之個人資料現況。

綜合商品零售業者經定期檢視發現有非屬特定目的必要範圍內或特定目的消失、期限屆至而無保存必要之個人資料，應予刪除、銷毀、停止蒐集、處理、利用或其他適當之處置。

第　八　條　　綜合商品零售業者蒐集個人資料時，應遵守本法第八條及第九條有關告知義務之規定，及符合前條第一項所定之類別及範圍。

綜合商品零售業者於傳輸個人資料時，應採取避免洩漏之必要保護措施。

綜合商品零售業者將當事人個人資料為國際傳輸

前，應檢視是否受中央主管機關限制，並告知當事人擬傳輸之國家或區域。

第　九　條　　綜合商品零售業者訂定第六條第三款所定資料安全管理及人員管理之措施，應包括下列事項：

一、依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，並定期確認權限內容之必要性及適當性。

二、檢視各相關業務之性質，規範個人資料蒐集、處理、利用及其他相關流程之負責人員。

三、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。

四、取消所屬人員離職時原在職之識別碼，並要求將執行業務所持有他人個人資料辦理交接，不得攜離使用。

第　十　條　　綜合商品零售業者應採取下列安全措施：

一、使用者身分確認及保護機制。

二、個人資料顯示之隱碼機制。

三、網際網路傳輸之安全加密機制。

四、個人資料檔案與資料庫之存取控制及保護監控措施。

五、防止外部網路入侵對策。

六、非法或異常使用行為之監控及因應機制。

前項第五款對策及第六款機制，應定期演練及檢討改善。

第 十一 條　　綜合商品零售業訂定第六條第四款所定認知宣導及教育訓練計畫，應包括定期對所屬人員進行個人資料保護認知宣導與教育訓練，使其明瞭相關法令之規定、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及管理措施。

第 十二 條　　綜合商品零售業者訂定第六條第五款所定事故之預防、通報及應變機制，應包括下列事項：

一、採取適當措施，控制事故對當事人造成之損害，並於發現事故時起七十二小時內，通報主管機關。如向地方主管機關通報者，並應副知中央主管機關。

二、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。

三、檢討缺失，並訂定預防及改進措施，避免事故再度發生。

綜合商品零售業者於發生個人資料被竊取、洩漏、竄改或其他侵害事故時，應依前項事故之預防、通報及應變機制迅速處理，保護當事人之權益。

綜合商品零售業者發生前項事故者，主管機關得依本法第二十二條第一項規定進入為行政調查、命相關人員為必要之說明、配合措施或提供相關證明資料，並視調查結果為後續處置。

第一項第一款通報紀錄格式如附表。

第 十三 條　綜合商品零售業者訂定第六條第六款所定設備安全管理措施，應包括下列事項：

一、紙本資料檔案之安全保護設施及管理程序。

二、電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制。

三、紙本及電子資料之銷毀程序；電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料。

第 十四 條　綜合商品零售業者訂定第六條第七款所定資料安全稽核機制，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，向綜合商品零售業者之代表人或經其授權之人員提出報告。

綜合商品零售業者依前項稽核結果發現計畫不符法令或不符法令之虞者，應即改善。

綜合商品零售業者依第五條規定指定之專責人員與第一項規定之查核人員，不得為同一人。

第 十五 條　綜合商品零售業者訂定第六條第八款所定使用紀錄、軌跡資料及證據保存之措施，應包括下列事項：

一、留存個人資料使用紀錄。

二、留存自動化機器設備之軌跡資料或其他相關之證據資料。

綜合商品零售業者，依前項規定留存個人資料使用紀錄、自動化機器設備之軌跡資料或其他相關之證據資料，其保存期限至少五年。

第 十六 條　　綜合商品零售業者訂定第六條第九款所定業務終止後，個人資料處理方法之措施，應包括下列事項：

一、銷毀：方法、時間、地點及證明銷毀之方式。

二、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。

三、刪除、停止處理或利用：方法、時間或地點。

前項措施應製作紀錄，其保存期限至少五年。

第 十七 條　　綜合商品零售業者訂定第六條第十款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。

第 十八 條　　綜合商品零售業者於當事人或其法定代理人行使本法第三條規定之權利時，應採取下列方式辦理：

一、有本法第十條但書、第十一條第二項但書或第三項但書得拒絕當事人或其法定代理人行使權利之事由者，併附理由通知當事人或其法定代理人。

二、遵守本法第十三條處理期限之規定。

三、告知依本法第十四條規定得酌收必要成本費用。

綜合商品零售業者得提供聯絡窗口及聯絡方式，以供當事人或其法定代理人行使前項權利。

第 十九 條　　綜合商品零售業者委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第八條規定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。

第 二十 條　綜合商品零售業者依本法第二十條第一項規定利用個人資料為行銷時，應明確告知當事人綜合商品零售業者登記名稱及個人資料來源。

綜合商品零售業者首次利用個人資料為行銷時，應提供當事人或其法定代理人表示拒絕接受行銷之方式，並支付所需費用；當事人或其法定代理人表示拒絕接受行銷者，應立即停止利用，並周知所屬人員。

第二十一條　綜合商品零售業者應於本辦法發布施行之日起六個月內完成安全維護計畫之訂定。

綜合商品零售業者應保存前項安全維護計畫；主管機關得派員檢查。

第二十二條　本辦法自發布日施行。

## 四、綜合商品零售業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(或法人)之個人資料檔案安全維護計畫。

### 壹、綜合商品零售業之組織及規模

一、名稱：_____(**綜合商品零售業**)

二、地址：○○○

三、負責人：○○○

四、資本額：新臺幣○○○元(註：所稱資本額，在有限公司、無限公司或兩合公司係指資本總額；在股份有限公司係指實收資本額；在有限合夥係指實收出資額；在商業係指資本額。)

### 貳、個人資料檔案安全維護管理措施

**一、依據：**

個人資料保護法第 27 條第 3 項及綜合商品零售業個人資料檔案安全維護管理辦法第 4 條規定。

**二、個人資料檔案安全維護計畫之訂定及修正**

(一)訂定目的：為防止個人資料被竊取、竄改、毀損、滅失或洩漏，爰訂定「個人資料檔案安全維護計畫」(下稱本計畫)，本綜合商品零售業員工應依本計畫辦理個人資料檔案安全管理及維護事宜。

(二)本計畫將參酌業務規模及特性，衡酌經營資源之合理分配等因素，檢視其合宜性，並經負責人或其授權人員於核定後予以修正。

**三、專責人員及資源配置**

(一)專責人員：

1.姓名：○○○。(至少 1 名)

2.職責：

(1)規劃、訂定、修正、執行安全維護計畫及其他相關事項。

(2)定期(每年至少 1 次)就執行前開任務情形向負責人或經其授權人員提出書面報告。

(二)稽核人員/單位：

1.姓名/單位：○○○。(至少1名)

2.職責：資料安全稽核機制

(1)不得與專責人員為同一人。

(2)定期稽核安全維護計畫之執行情形及成效，並將稽核結果，向代表人或經其授權之人員提出報告。

(三)預算：每年新臺幣○○○元。(包含管理薪資、設備費用等，可記載一定範圍之金額，依實際狀況填寫)

**四、個人資料蒐集、處理及利用之內部管理程序**

(一)向當事人蒐集個人資料時，明確告知當事人以下事項：

1.本公司(或法人)名稱。

2.蒐集目的。

3.個人資料之類別。(註：可參考法務部「個人資料保護法之特定目的及個人資料之類別」https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=fl010631。)

4.個人資料利用之期間、地區、對象及方式。

5.當事人得向本公司(或法人)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(或法人)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)指定管理人員每○○日(或週、月、季、年)清查本公司(或法人)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。

(五)本公司(或法人)保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。

(六)傳輸個人資料時，應採取避免洩漏之必要保護措施。如將當事人個人資料為國際傳輸前，應檢視是否受中央主管機關限制，並告知當事人擬傳輸之國家或區域。

**五、個人資料之範圍及項目**

(一)個人資料範圍：指本公司(或法人)蒐集、處理及利用之自然人姓名、出生年月日、國民身分證統一編號、護照號碼、聯絡方式及其他得以直接或間接方式識別該個人之資料(註：可參考個人資料保護法第 2 條第 1 款填寫)。

(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，例如：人事管理(〇〇二)、全民健康保險、勞工保險、國民年金保險或其他社會保險(〇三一)、消費者、客戶管理與服務(〇九〇)等。)

(三)指定管理人員每〇〇日(或週、月、季、年)定期清查本公司(或法人)所保有之個人資料檔案及其蒐集、處理或利用個人資料之作業流程，據以建立個人資料檔案清冊及個人資料作業流程說明文件。

**六、資料安全管理**

(一) 資通訊系統存取個人資料之管控：

1. 依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，並定期確認權限內容之必要性及適當性。
2. 檢視各相關業務之性質，規範個人資料蒐集、處理、利用及其他相關流程之負責人員。
3. 於儲存個人資料之電腦設置識別密碼、保護程式密碼及相關安全措施。
4. 個人資料檔案使用完畢應即關閉檔案，不得任其停留於螢幕上。

5. 每○○日(週、月、季、年)進行防毒、掃毒等必要之安全措施。
6. 重要個人資料檔案應另加設密碼，非經陳報○○(請填負責人、管理組織或其他經授權之人員，依貴團體實際情形填寫)核可不得存取。
7. 所屬人員非經本公司(或法人)○○(請填負責人、管理組織或其他經授權之人員，依貴團體實際情形填寫)核可，不得任意複製本公司(或法人)保有之個人資料檔案。
8. 本公司(或法人)蒐集、處理或利用個人資料時，應設置使用者身分確認及保護機制、個人資料顯示之隱碼機制(註：如將身分證字號末4碼以****標示，或將姓名其中1個字以○標示)、網際網路傳輸之安全加密機制、個人資料檔案與資料庫之存取控制及保護監控措施，防止外部網路入侵對策及非法或異常使用行為之監控及因應機制。
9. 就防止外部網路入侵對策及非法或異常使用行為之監控及因應機制，應定期(每年至少1次)進行演練及提出檢討改善報告。

(二)紙本資料之保管：

1. 記載有個人資料之紙本文件，在未使用時存放於公文櫃內並上鎖。所屬人員非經○○(請填負責人、管理組織或其他經授權之人員，依貴團體實際情形填寫)核可，不得任意複製、拍攝或影印。
2. 丟棄記載有個人資料之紙本文件時，應先以碎紙設備進行處理。

## 七、人員管理

(一)所屬人員登錄電腦之識別密碼，每○○日(或週、月)變更1次。

(二)所屬人員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。

(三)本○○(公司或法人)與所屬人員間之勞務、承攬及委任契約均列入保密及個資條款及違約罰則，以促使其遵守個人資料保密等相關義務(含契約終止後)。

(四)所屬人員離職時，應即取消其登錄電腦之使用者代碼(帳號)及識別密碼。其在職期間所持有之個人資料應確實移交，不得私自複製、留存並

在外繼續利用。

**八、認知宣導及教育訓練**

(一)每年對所屬人員施以個人資料保護法基礎認知宣導及教育訓練，使其明瞭個人資料保護相關法令之規定、責任範圍與各種個人資料保護事項之機制、程序及管理措施。前述教育宣導及訓練應留存相關紀錄或佐證資料（例如：簽到表或登錄紀錄等佐證資料）。

(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。

**九、事故之預防、通報及應變機制**

(一)預防措施

1. 指定專人辦理安全維護事項，防止本公司(或法人)保有之個人資料被竊取、竄改、毀損、滅失或洩漏。
2. 加強管控本公司(或法人)所屬人員對內或對外之個人資料傳輸，避免外洩。
3. 加強所屬人員教育宣導，並嚴加管制。

(二)應變措施

1. 發現本公司(或法人)有個人資料遭竊取、洩漏、竄改或其他侵害事故者之情形，應立即通報代表人或經其授權之人員並查明發生原因及損害狀況，及依實際狀況採取相關應變措施，以控制事故對當事人之損害。
2. 儘速以適當方式通知當事人或其法定代理人個人資料被侵害之事實、本公司(或法人)已採取之因應措施及聯絡電話窗口等資訊。
3. 針對事故發生原因檢討缺失，並研議預防及改進措施，避免類似事故再次發生。

(三)通報措施

本公司(或法人)應自發現事故時起算 72 小時內，填具「個人資料侵害事故通報及紀錄表」，以電子郵件方式向經濟部通報，並將視案情發展適時通報處理情形，以及將整體查處過程、結果及檢討等函報經濟部。

## 十、設備安全管理

(一)指派專人管理儲存個人資料之電腦及其他儲存媒介物，定期清點、保養維護。

(二)電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制。

(三)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。

(四)指派專人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。

(五)本公司（或法人）保有之個人資料檔案應定期(例如：每二週)備份。

(六)重要個人資料備份應異地存放，並應建置防止個人資料遭竊取、竄改、損毀、滅失或洩漏等事故之機制。

(七)電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料。

(八)更新或維修電腦設備時，應指定專人在場，確保個人資料之安全及防止個人資料外洩。

(九)依據作業內容及環境之不同，實施必要之安全環境管制，以妥善維護並控管個人資料蒐集、處理或利用過程中所使用之實體設備。

## 十一、資料安全稽核機制

(一)定期(每年至少 1 次)辦理個人資料檔案安全維護稽核，檢查本公司（或法人）是否落實本計畫規範事項，針對檢查結果不符合及潛在風險事項規劃改善措施，確保相關措施之執行。執行改善與預防措施時，應依下項事項辦理：

1. 確認不符合事項之內容及發生原因。
2. 提出改善及預防措施方案。
3. 紀錄檢查情形及改善與預防措施方案執行結果。

(二)前項檢查情形及執行結果應載入稽核報告中，由代表人或經其授權之人員簽名確認，稽核報告至少保存五年。

## 十二、使用紀錄、軌跡資料及證據保存

(一)本公司(或法人)建置個人資料之電腦，其個人資料使用紀錄，需每○○日(或週、月)備份並設定密碼，儲存該紀錄之儲存媒介物保存於適當處所以供備查。(註：本項請依實際情形填寫)

(二)個人資料使用紀錄以紙本登記者，應存放於公文櫃內並上鎖，非經○○(請填負責人、管理組織或其他經授權之人員，依貴團體實際情形填寫)核可，不得任意取出。

(三)本公司(或法人)應保存以下紀錄：

1. 個人資料提供或移轉第三人。
2. 當事人行使個資法第三條之權利及處理過程。
3. 個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀。
4. 人員權限新增、變動及刪除。
5. 消費者個人資料之蒐集、處理及利用紀錄，以及自動化機器設備之軌跡資料。

(四)以上使用紀錄、軌跡資料及相關證據至少留存 5 年。

**十三、業務終止後之個人資料處理方法**

本公司（或法人）於業務終止後，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：

(一)銷毀：方法、時間、地點及證明銷毀之方式。

(二)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。

(三)刪除、停止處理或利用：方法、時間或地點。

(四)以上處理措施應製作紀錄，其保存期限至少五年。

**十四、個人資料安全維護之整體持續改善方案**

(一)本公司（或法人）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，並予必要之修正。

(二)針對個資安全稽核結果有不符合法令之虞者，規劃改善與預防措施並納入安全維護計畫。

**十五、當事人權利行使**

當事人或其法定代理人行使個人資料保護法第三條規定之權利時，採取下列方式辦理：

(一)提供聯絡窗口及聯絡方式。

(二)確認為個人資料當事人本人、法定代理人或經其委託之人。

(三)有個人資料保護法第十條但書、第十一條第二項但書或第三項但書得拒絕當事人或其法定代理人行使權利之事由者，併附理由通知當事人或其法定代理人。

(四)遵守個人資料保護法第十三條處理期限之規定。

(五)告知依個人資料保護法第十四條規定得酌收必要成本費用。

**十六、委託作業**

本公司（或法人）委託他人蒐集、處理或利用個人資料之全部或一部時，應依個人資料保護法施行細則第八條規定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，以及採取下列方式辦理：

(一)選擇受託人前，應確認需要委外的範圍，並以適當評估方式選擇具適當個資安全維護能力的受託人。

(二)應與受託人締結委託契約，要求受託人依本公司（或法人）應適用之個資管理規定執行契約。

(三)於委託契約或相關文件明確約定適當之監督事項及方式。

(四)要求受託者僅得於本公司（或法人）指示之範圍內，蒐集、處理或利用個人資料。

(五)要求受託者認本公司（或法人）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，應立即通知本公司（或法人），並於契約中訂定委外廠商於知悉資通或個資安全事件情況時，應即向本公司（或法人）權責人員或通報窗口，以指定之方式進行通報。

(六)對受託者應定期查核受託者執行之狀況，並將確認結果記錄之。(如委外查核報告以及查核缺失追蹤情形)

(七)委託關係終止或解除時，受託者應將個人資料載體之返還或將個人資料刪除。

## 十七、行銷

(一)本公司(或法人)依個人資料保護法第二十條第一項規定利用個人資料為行銷時，應明確告知當事人本公司(或法人)名稱及個人資料來源。

(二)本公司(或法人)首次利用個人資料為行銷時，應提供當事人或其法定代理人表示拒絕接受行銷之方式，並支付所需費用；當事人或其法定代理人表示拒絕接受行銷者，應立即停止利用，並周知所屬人員。

## 十八、附表：個人資料侵害事故通報及紀錄表

### 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="6">事業名稱<br>_____<br>通報機關<br>_____</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：</td></tr>
<tr><td colspan="2">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)<br>_____</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<br>□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>
</table>

| | |
|---|---|
| 擬採通知當事人之時間及方式 | |
| 是否於發現個資外洩時起算七十二小時內通報 | □是　□否，理由： |

經濟部(商業司)通報聯繫窗口

電子郵件：OOOO

聯絡電話：OOOO

## 五、綜合商品零售業個人資料安全稽核檢查表

_____(填表單位)

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：未完全依稽核內容要求訂定相關程序，或未完全依相關程序執行並產生實作紀錄；並請於說明欄儘可能詳述未符合之情形與樣態。

（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 | 查核結果 | 說明 | 對應條文 | 備註 |
|---|---|---|---|---|---|
| 1.個人資料檔案安全維護計畫之訂定及修正 | 1.1 是否規劃、訂定、檢討與修正安全維護措施，並訂定個人資料檔案安全維護計畫(下稱安維計畫)，載明下列事項？<br>一、個人資料蒐集、處理及利用之內部管理程序。<br>二、個人資料之範圍。<br>三、資料安全管理及人員管理。<br>四、認知宣導及教育訓練。<br>五、事故之預防、通報及應變機制。<br>六、設備安全管理。<br>七、資料安全稽核機制。<br>八、使用紀錄、軌跡 | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第4條、第6條<br>「個人資料保護法」第27條第1項、第2項。 | 請檢附個人資料檔案安全維護計畫及相關管理文件。 |

| | | | | | |
|---|---|---|---|---|---|
| | 資料及證據保存。<br>九、業務終止後，個人資料處理方法。<br>十、個人資料安全維護之整體持續改善方案。 | | | | |
| | 1.2 是否定期檢視及配合相關法令修正安維計畫？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第4條 | 請檢附最近一前檢視紀錄及修正佐證，以及代表人或經其授權之人員核定之佐證。 |
| 2.配置專責人員並執行任務 | 2.1 是否指定安全維護計畫之專責人員，負責規劃、訂定、修正、執行安全維護計畫及其他相關事項？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第5條 | 請檢附個資管理單位組織圖、分工及相關辦法，並提出個資專責人員所協助之各項個資保護工作事項，如：參與會議、盤點及風險評鑑工作、事件處理等。 |
| | 2.2 專責人員是否就前項事項定期向綜合商品零售業者之代表人或經其授權之人員提出報告？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第5條 | 請檢附最近一次報告書，以及代表人或經其授權之人員核定之佐證。 |

| | | | | | |
|---|---|---|---|---|---|
| 3.界定個人資料範圍並定期確認 | 3.1 是否訂定作業規範以清查所保有之個人資料，依特定目的之必要性界定其類別或範圍，並建立檔案？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第7條第1項 | 請檢附個資盤點作業流程文件。 |
| | 3.2 是否定期確認所保有之個人資料有無變動並更新檔案？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第7條第1項 | 請檢附最近一次個人資料檔案清冊，並經權責主管核定之紀錄。 |
| 4.個人資料蒐集、處理及利用之內部管理程序 | 4.1 是否訂有個人資料蒐集、處理及利用之內部管理程序，以確保資料蒐集、處理及利用具備特定目的並具有法定要件，並確保有非屬特定目的必要範圍內或特定目的消失、期限屆至而無保存必要之個人資料，應予刪除、銷毀、停止蒐集、處理、利用或其他適當之處置？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第7條第2項 | 請檢附個人資料蒐集、處理及利用之內部管理程序文件。 |
| | 4.2 是否定期檢視無保存必要之個人資料，予以刪除、銷毀、停止蒐集、處理、利用或其他適當之處置？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第7條第2項 | 請檢附最近一次檢視紀錄以及相關處置紀錄。 |

| | | | | | |
|---|---|---|---|---|---|
| 5.告知義務 | 5.1 向當事人蒐集個人資料時,是否明確告知當事人下列事項？<br>一、本公司名稱。<br>二、蒐集之目的。<br>三、個人資料之類別。<br>四、個人資料利用之期間、地區、對象及方式。<br>五、當事人依個人資料保護法第3條規定得行使之權利及方式。<br>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。 | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第8條第1項 | 告知當事人之佐證紀錄。 |
| | 5.2 蒐集非由當事人提供之個人資料,是否於處理或利用前,向當事人告知個人資料來源及下所列事項？<br>一、本公司名稱。<br>二、蒐集之目的。<br>三、個人資料之類別。<br>四、個人資料利用之期間、地區、對象及方式。<br>五、當事人依個人資料保護法第3條規定得行使之權利及方式。 | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第8條第1項 | 告知當事人之佐證紀錄。 |

| | | | | | |
|---|---|---|---|---|---|
| 6. 資料傳輸 | 6.1 傳輸個人資料時，是否依不同傳輸方式，採取適當之安全措施？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第8條第2項 | 請說明傳輸個人資料之相關管控措施。例如以電子郵件傳送敏感之個資檔案時，是否採加密機制？ |
| | 6.2 進行個人資料國際傳輸前，是否檢視及遵循經濟部限制國際傳輸之命令或處分？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第8條第3項 | 請進行說明。 |
| | 6.3 進行個人資料國際傳輸前，是否告知當事人個人資料擬傳輸之國家或區域？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第8條第3項 | 請提出告知當事人之佐證紀錄。 |
| 7. 資料安全管理 | 7.1 是否依據業務作業需要及性質，建立管理機制以規範個人資料蒐集、處理、利用及其他相關流程，並設定所屬人員不同之權限？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第9條第1款、第2款 | 請說明並檢附個資權限管理措施。 |
| | 7.2 是否定期檢視所屬人員不同權限之適當性及必要性？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第9條第1款、第2款 | 請檢附最近一次個資系統權限申請表單以及帳號權限審查紀錄。 |
| | 7.3 是否要求所屬人員就所保有之個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其 | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第9條第3款 | 請說明並檢附資料安全管理措施。 |

| | | | | | |
|---|---|---|---|---|---|
| | 他存放媒介物時，應妥善保管個人資料之儲存媒介物？ | | | | |
| 8. 人員管理 | 8.1 是否與所屬人員約定個人資料保管及保密義務？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第9條第3款 | 請檢附所屬人員清單(正職、短期約僱)及所簽署之保密切結書。 |
| | 8.2 所屬人員離職時是否取消原在職之識別碼，並要求將執行業務所持有他人個人資料辦理交接，不得於離職後繼續使用？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第9條第4款 | 請檢附所屬近一年來離職人員清單(正職、短期約僱)及所簽署之保密切結書或離職單。 |
| 9. 安全措施 | 9.1 是否採行使用者身分確認及保護機制？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第10條第1項第1款 | 請說明使用者身分確認及保護機制，並檢附相關佐證。 |
| | 9.2 是否採行個人資料顯示之隱碼機制？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第10條第1項第2款 | 請說明個人資料顯示之隱碼機制，並檢附相關佐證。 |
| | 9.3 是否採行網際網路傳輸之安全加密機制？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第10條第1項第3款 | 請說明網際網路傳輸之安全加密機制，並檢附相關佐證。 |
| | 9.4 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<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第10條第1項第4款 | 請說明個人資料檔案與資料庫之存取控制及保護監控措施，並檢附相關佐證。 |

| | | | | | |
|---|---|---|---|---|---|
| | 9.5 是否採行防止外部網路入侵對策？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第10條第1項第5款 | 請說明防止外部網路入侵對策，並檢附相關佐證。 |
| | 9.6 是否採行非法或異常使用行為之監控及因應機制？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第10條第1項第6款 | 請說明非法或異常使用行為之監控及因應機制，並檢附相關佐證。 |
| | 9.7 前二項之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，是否定期演練及檢討改善？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第10條第2項 | 請提出最近一次個資事故演練及檢討改善之佐證資料。 |
| 10.認知宣導及教育訓練 | 10.1 是否定期對所屬人員進行個人資料保護認知宣導與教育訓練，使其明瞭相關法令之規定、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及管理措施？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第6條第4款<br>「個人資料保護法施行細則」第12條第2項第7款 | 請檢附最近一次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。 |
| 11.事故之預防、通報、應變及改善機制 | 11.1 有無訂定因應個人資料被竊取、洩漏、竄改或其他侵害事故之預防、通報及應變機制？並包括下列事項？<br>一、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，填寫「個人資料侵害事故通報及紀 | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第12條第1項、第4項 | 請檢附個資事故之預防、通報及應變機制之管理文件 |

| | | | | | |
|---|---|---|---|---|---|
| | 錄表」通報經濟部。<br>二、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。<br>三、檢討缺失，並訂定預防及改進措施，避免事故再度發生。 | | | | |
| | 11.2 是否於發生個人資料被竊取、洩漏、竄改或其他侵害事故時，依前項事故之預防、通報及應變機制迅速處理？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第12條第2項<br>「個人資料保護法」第12條<br>「個人資料保護法施行細則」第22條第1項、第2項 | 請檢附事故通報文件。 |
| | 11.3 發生前項事故者，是否配合經濟部進行行政調查、為必要之說明、配合措施或提供相關證明資料(例如委託第三方進行調查之報告及強化措施)，並將事故處理情形、查處過程、結果及檢討等函報經濟部？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第12條第3項 | 請檢附事故處理報告及改善措施之佐證資料。 |
| 12.設備安全管理措施 | 12.1 是否妥善維護紙本資料檔案之安全保護設施及訂定管理程序？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第13條第1款 | 請說明個資檔案安全保護措施及管理文件。 |

| | | | | | |
|---|---|---|---|---|---|
| | 12.2 是否將電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制，並訂定管理程序？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第13條第2款 | 請說明個資檔案安全保護措施及管理文件。 |
| | 12.3 是否訂定紙本及電子資料之銷毀程序，並於電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，採取適當防範措施，避免洩漏個人資料？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第13條第3款 | 請說明個資檔案銷毀或轉作其他用途之作業流程及管理文件，並檢附最近一次個資儲存媒介物銷毀或轉作其他用途之紀錄。 |
| 13. 資料安全稽核機制 | 13.1 是否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，向代表人或經其授權之人員提出報告。 | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第14條第1款 | 請檢附最近兩次之稽核報告，以及代表人或經其授權之人員核定之佐證。 |
| | 13.2 依前項稽核結果發現計畫不符法令或不符法令之虞者，是否立即改善？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第14條第2款 | 請檢附改善報告及改善之佐證資料，以及代表人或經其授權之人員核定之佐證。 |
| | 13.3 資料安全稽核之查核人員是否與安全維護計畫之專責人員非為同一人？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第14條第3款 | 請檢附最近一次稽核之小組成員名單。 |
| 14. 使用紀錄、軌跡資料及證據保 | 14.1 是否留存個人資料使用紀錄至少5年？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦 | 請說明留存個人資料使用紀錄之作業方 |

| | | | | | |
|---|---|---|---|---|---|
| 存 | | | | 法」第15條第1項、第2項 | 式，並提供留存個人資料使用紀錄至少5年的佐證。 |
| | 14.2 是否留存自動化機器設備之軌跡資料或其他相關之證據資料至少5年？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第15條第1項、第2項 | 請說明留存自動化機器設備之軌跡資料或其他相關之證據資料個人資料使用紀錄之作業方式，並提供留存並至少5年的佐證。 |
| 15.業務終止後，個人資料處理方法。 | 15.1 業務終止後，保有之個人資料是否銷毀，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？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第16條第1項第1款、第2項 | 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，相關銷毀紀錄。 |
| | 15.2 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<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第16條第1項第2款、第2項 | 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，保有之個人資料相關移轉紀錄。 |
| | 15.3 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<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第16條第1項第3款、第2項 | 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，保有之個人資料刪除、停止處 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 理或利用之相關紀錄。 |
| 16.個人資料安全維護之整體持續改善方案 | 16.1 是否每年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，必要時並予以修正？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第17條 | 請檢附最近一次安全維護計畫檢視及評估是否修正之紀錄，以及代表人或經其授權之人員核定之佐證。 |
| | 16.2 是否針對含有個人資料相關流程進行分析可能發生之風險？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第17條<br>「個人資料保護法施行細則」第12條第2項第3款 | 請檢附風險評估底稿及風險評鑑報告，以及代表人或經其授權之人員核定之佐證。。 |
| | 16.3 是否依據風險分析之結果訂定適當之管控措施？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第17條<br>「個人資料保護法施行細則」第12條第2項第3款 | 請檢附風險處理計畫及追蹤改善措施之佐證，以及代表人或經其授權之人員核定之佐證。。 |
| 17.當事人權利行使 | 17.1 是否訂定當事人依個人資料保護法第3條行使權利之程序？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第18條第1項<br>「個人資料保護法」第3條 | 請檢附當事人依個人資料保護法第3條行使權利之程序文件。 |

| | | | | | |
|---|---|---|---|---|---|
| | 17.2 如有個人資料保護法第10條但書、第11條第2項但書或第3項但書得拒絕當事人或其法定代理人行使權利之事由者，有無併附理由通知當事人或其法定代理人？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第18條第1項第1款<br>「個人資料保護法」第10條但書、第11條第2項但書、第3項但書 | 請檢附最近一年依個人資料保護法第3條行使權利之清單(含事由、處理時間及結果)。如有拒絕當事人或其法定代理人行使權利之事由者，請檢附通知當事人或其法定代理人之相關理由紀錄。 |
| | 17.3 受理當事人或其法定代理人依個人資料保護法第10條規定之請求，有無遵守個人資料保護法第13條處理期限之規定？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第18條第2款<br>「個人資料保護法」第10條、第13條 | 請檢附最近一年依個人資料保護法第3條行使權利之清單(含事由、處理時間及結果)。 |
| | 17.4 當事人或其法定代理人查詢或請求閱覽個人資料或製給複製本者，如酌收必要成本費用，是否進行告知？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第18條第3款<br>「個人資料保護法」第14條 | 請檢附必要成本費用之資料並事前告知當事人之佐證。 |
| | 17.5 是否提供聯絡窗口及聯絡方式，以供當事人或其法定代理人行使前4項之權利？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第18條2項 | 請檢附對外揭露聯絡窗口及聯絡方式，以供當事人或其法定代理人行使前4項權利之佐證。 |

| | | | | | |
|---|---|---|---|---|---|
| 18. 委託作業 | 18.1 委託他人蒐集、處理或利用個人資料時，是否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？<br>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。<br>二、受託者就個人資料保護法第12條第2項採取之措施。<br>三、有複委託者，其約定之受託者。<br>四、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，應向本公司通知之事項及採行之補救措施。<br>五、委託機關如對本公司有保留指示者，其保留指示之事項。<br>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。<br>七、受託者僅得於本公司指示之範圍內，蒐集、處理或利用個人資料。 | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人資料檔案安全維護管理辦法」第19條<br>「個人資料保護法施行細則」第8條第1項、第2項、第4項 | 請檢附個資委外之廠商清單及合約文件。 |

| | | | | | |
|---|---|---|---|---|---|
| | 八、受託者認本公司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，應立即通知本公司。 | | | | |
| | 18.2 是否於第1項之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，視同本公司，並遵守「綜合商品零售業個人資料檔案安全維護管理辦法」之規定。 | □符合<br>□不符合<br>□不適用 | | 「個人資料保護法」第4條<br>「個人資料保護法施行細則」第7條 | 請檢附個資委外之廠商清單及合約文件。 |
| | 18.3 委託他人蒐集、處理或利用個人資料時，是否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？ | □符合<br>□不符合<br>□不適用 | | 「個人資料保護法施行細則」第8條第3項 | 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。 |
| 19.行銷規範 | 19.1 利用個人資料為行銷時，是否明確告知當事人本公司登記名稱及個人資料來源？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人[資料檔案安全維護管理辦法」第20條第1項 | 請檢附明確告知當事人綜合商品零售業者登記名稱及個人資料來源之 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 佐證。 |
| | 19.2 首次利用個人資料行銷時，是否提供當事人或其法定代理人免費表示拒絕行銷之方式？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人[資料檔案安全維護管理辦法」第20條第2項 | 請說明當事人免費表示拒絕行銷之方式，並檢附佐證。 |
| | 19.3 當事人或其法定代理人表示拒絕行銷後，是否立即停止利用其個人資料行銷，並周知所屬人員？ | □符合<br>□不符合<br>□不適用 | | 「綜合商品零售業個人[資料檔案安全維護管理辦法」第20條第2項 | 請檢附當事人表示拒絕行銷之清單(含處理時間及結果)，以及立即停止利用其個人資料行銷之佐證。 |
| 20.個人資料庫之共享使用 | 20.1 是否有其他關係企業或主體共享使用本公司所蒐集之客戶個人資料庫，並明確告知當事人個人資料保護法第8條第1項之事項？ | □符合<br>□不符合<br>□不適用 | | 「個人資料保護法」第8條 | 請說明具體共享使用之主體名稱，以及共享使用之原因及安全控管措施。另檢附告知當事人之佐證。 |
| | 20.2 是否使用其他關係企業或主體所蒐集之客戶個人資料庫加以處理及利用，並明確告知當事人個人資料保護法第9條第1項之事項？ | □符合<br>□不符合<br>□不適用 | | 「個人資料保護法」第9條 | 請檢附於處理及利用前告知當事人之佐證。 |
| 21.使用資通訊系統蒐集、處理或利用個人資料 | 21.1 是否就使用資通訊系統蒐集、處理或利用消費者或會員個人資料之服務範圍取得資安或個資驗證？ | □符合<br>□不符合<br>□不適用 | | 中央目的事業主管機關依「個人資料保護法」第22條第1項為職權調查之事項。 | 請檢附外部稽核證書(或驗證通過證明書)，例如 ISO 27001、27701，以確認 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 驗證範圍包含本系統開發生命週期及對客戶提供之服務流程，以及持續有效。 |
| 22.個資存放雲端之安全控管 | 22.1 是否確保消費者或會員個人資料放在雲端上的安全？ | □符合<br>□不符合<br>□不適用 | | 中央目的事業主管機關依「個人資料保護法」第22條第1項為職權調查之事項。 | 請說明如何確認Datebase的安全以及放在那個國家？並提出合約及相關佐證(如雲端業者出具的證明書)。 |
| 23.網路零售行為的遵法性 | 23.1 如有進行網路零售之行為,是否遵循網路零售業主管機關之相關規定(如「網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法」)? | □符合<br>□不符合<br>□不適用 | | 中央目的事業主管機關依「個人資料保護法」第22條第1項為職權調查之事項。 | 請說明進行網路零售之網站(網址)或方式。 |

## 六、個人資料保護法之特定目的及個人資料之類別

（民國 101 年 10 月 1 日修正)

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
○　九三　財產保險
○　九四　財產管理
○　九五　財稅行政
○　九六 退除役官兵輔導管理及其眷屬服務照顧
○　九七 退撫基金或退休金管理
○　九八　商業與技術資訊
○　九九　國內外交流業務
一○○ 國家安全行政、安全查核、反情報調查
一○一 國家經濟發展業務
一○二 國家賠償行政
一○三 專門職業及技術人員之管理、懲戒與救濟
一○四 帳務管理及債權交易業務
一○五 彩券業務
一○六 授信業務
一○七 採購與供應管理
一○八 救護車服務
一○九 教育或訓練行政
一一○ 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○ 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、個資相關流程識別清單

# 個人資料相關流程識別清單

填表日期：　　年　　月　　日

| 編號 | 主流程名稱 | 子流程名稱 | 個資流程 |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 八、個人資料盤點表

### (一) 個人資料盤點表格式範例

| 作業流程名稱 | | 個人資料檔案基本資訊 | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 主流程名稱 | 子流程名稱 | 個人資料檔案名稱 | 檔案型態 | 當事人 | 保有依據 | 保有依據說明 | 特定目的 | 個人資料類別 |
| | | | | | | | | |

| 資料流 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 組織身分 | 資料來源 | 組織內部提供者 | 組織內部接收者 | 資料處理者 | 第三方 | 國際傳輸 | 組織身分補充欄位 |
| | | | | | | | |

| 一般個資 | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 姓名 | 生日 | 身分證號 | 護照號碼 | 特徵 | 婚姻 | 家庭 | 教育 | 職業 | 聯絡方式 | 財務情況 | 社會活動 | 網路識別資料 | 定位資料 |
| | | | | | | | | | | | | | |

| 特殊類別個資 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 種族 | 政治 | 信仰 | 工會身分 | 生物資料 | 性傾向 | 性生活 | 基因 | 病歷 | 醫療 | 健康檢查 | 犯罪前科 |
| | | | | | | | | | | | |

| 自訂高風險個資 | | | | 其他可識別個資 | | 特殊保護方式 |
|---|---|---|---|---|---|---|
| | | | | 其他直接識別 | 其他間接識別 | 控制措施 |
| | | | | | | |

| 保存 | 備註 | 單位名稱 |
|---|---|---|

| 儲存位置 | 法定保存期限 | 自訂保存期限 | 銷毀方式 | | 第一層單位名稱 | 第二層單位名稱 |
|---|---|---|---|---|---|---|
| | | | | | | |

(二) 盤點說明

| 欄位 | | 填寫說明 |
|---|---|---|
| 作業流程名稱 | 主流程名稱 | 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。 |
| | | ＊如會計業務、人事業務等，請勿空白。 |
| | 子流程名稱 | 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，並列出子流程名稱。 |
| | | ＊如：付款作業、差勤管理作業、教育訓練作業等，請勿空白。 |
| 個人資料檔案基本資訊 | 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。 |
| | | ＊如個人資料檔案包含一種或多種附件，請於檔案名稱以括號註明，參考填寫範例如下，請勿空白： |
| | | 薪津表(含年終獎金、加班費、考績獎金)，並根據附件內容一併對應後續欄位填寫。 |
| | 檔案型態 | 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：上述數位形式文件如保存於可攜式媒體。 |
| | | 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。 |
| | | ＊如個人資料檔案包含多種檔案型態，請另外分筆列示，勿合併填寫。 |
| | 當事人 | 組織所蒐集個資的對象，例如： |
| | | 1.客戶/消費者(自然人) |
| | | 2.法人之負責人、法人之聯絡人、廠商之相關人員 |
| | | 3.正職員工/聘僱員工/派遣員工 |
| | | 4.其他人員 (不在上述定義中之人員，如利害關係人等) |
| | | ＊本欄位請勿空白；如填寫「其他人員」，請簡要註明，填寫範例為：其他人員(申請人)。 |
| | 保有依據 | 是否有蒐集個資的合法基礎，例如： |
| | | 1.當事人同意。 |

| | | |
|---|---|---|
| | | 2.當事人書面同意。 |
| | | 3.與當事人有契約或類似契約關係。 |
| | | 4.履行法定義務。 |
| | | 5.保護當事人或其他自然人的重要利益。 |
| | | 6.基於公共利益處理個資。 |
| | | 7.其他。 |
| | | 若為 3.請於保有依據說明欄位填寫該契約名稱，例如：○○總約定書等。<br>若為 4.請於保有依據說明欄位填寫法規名稱。<br>若為 7.請於保有依據說明欄位詳細說明。 |
| | **保有依據說明** | 詳細說明資料保有之依據或合法基礎。 |
| | **特定目的** | 可參考法務部公告之「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，或依蒐集目的詳細描述。 |
| | | 除依上述規定填寫之外，另可參考個資法第 8 條告知當事人事項，填寫個人資料蒐集之目的。 |
| | **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。 |
| **資料流** | **組織身份** | 依照盤點單位對該個人資料檔案之角色，選取"資料控制者"、"資料處理者"或"共同資料控制者"。相關定義如下： |
| | | 資料控制者：可決定個人資料處理之目的與方法之自然人或法人、公務機關、局處或其他機構。 |
| | | 資料處理者：代控制者處理個人資料之自然人或法人、公務機關、局處或其他機構。 |
| | | 共同資料控制者：兩個或兩個以上資料控制者共同決定處理之目的及方式。 |
| | **資料來源** | 依照個人資料蒐集之方式，選取"直接蒐集"、"間接蒐集"或"直接及間接蒐集"。相關定義如下： |
| | | 由當事人直接提供個人資料者為直接蒐集；非由當事人主動提供個人資料者為間接蒐集。 |
| | **組織內部提供者** | 資料來源的內部單位；如無請以 N/A 表示。 |
| | **組織內部接收者** | 資料交付出去的內部單位；如無請以 N/A 表示。 |

| | | |
|---|---|---|
| | **資料處理者** | 代為處理個人資料之自然人或法人、公務機關、局處或其他機構。例如：<br>1.委外廠商<br>2.依法代為執行法定職務之機關 |
| | **第三方** | 與組織之個資檔案之蒐集、處理及利用流程有關，但無法歸屬於前述利害關係人類型之組織或人員等。例如：<br>1.法院，因執行司法案件需要，行文本公司調閱相關資料。<br>2.國稅局，因執行稅務調查需要，派員至本公司調閱相關資料。<br>＊若無此情況請以 N/A 表示。 |
| | **國際傳輸** | 我國境內之資料控制者或資料處理者在活動過程中將個人資料檔案傳輸至我國境外。<br>＊如傳輸至多個國家，請分別列示，如：日本、新加坡。 |
| | **組織身分補充欄位** | 若組織身分為資料處理者，請於組織身分補充欄位填寫該資料控制者之組織名稱。<br>若組織身分為共同資料控制者，請於組織身分補充欄位填寫另一共同資料控制者之組織名稱。 |
| **一般個資** | **姓名** | 個資當事人之姓名，包含英文姓名。<br>＊本欄位以 Y 或 N 表示，請勿空白。 |
| | **生日** | 出生年月日，如僅有出生年，則無需識別。<br>＊本欄位以 Y 或 N 表示，請勿空白。 |
| | **身分證號** | 國民身分證統一編號<br>＊本欄位以 Y 或 N 表示，請勿空白。 |
| | **護照號碼** | 護照號碼<br>＊本欄位以 Y 或 N 表示，請勿空白。 |
| | **特徵** | 如年齡、性別、出生地、國籍、聲音、身高、體重、血型、抽煙、喝酒、個性等之評述意見<br>＊本欄位以 Y 或 N 表示，請勿空白。 |
| | **婚姻** | 如 C〇二二 婚姻之歷史：前次婚姻或同居、離婚或分居等細節及相關人之姓名等。<br>＊本欄位以 Y 或 N 表示，請勿空白。 |
| | **家庭** | 如 C〇二一 家庭情形：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。<br>如 C〇二二 婚姻之歷史：前次婚姻或同居、離婚或分居等細節及相關人之姓名等。 |

| | | |
|---|---|---|
| | | 如C〇二三 家庭其他成員之細節：子女、受扶養人、家庭其他成員或親屬、父母、同居人及旅居國外及大陸人民親屬等。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **教育** | 如C〇五一 學校紀錄：大學、專科或其他學校等。 |
| | | 如C〇五二 資格或技術：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。 |
| | | 如C〇五三 職業團體會員資格：會員資格類別、會員資格紀錄、參加之紀錄等。 |
| | | 如C〇五四 職業專長：專家、學者、顧問等。 |
| | | 如C〇五五 委員會之會員資格：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。 |
| | | 如C〇五六 著作：書籍、文章、報告、視聽出版品及其他著作等。 |
| | | 如C〇五七 學生(員)、應考人紀錄：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。 |
| | | 如C〇五八 委員工作紀錄：委員參加命題、閱卷、審查、口試及其他試務工作情形記錄。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **職業** | 如C〇三八 職業：學校校長、民意代表或其他各種職業等。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **聯絡方式** | 能夠聯絡到個資當事人的方式，例如地址、室內電話、公司電話、手機號碼、電子郵件、地址等，都可稱之為聯絡方式。同一項個人資料檔案內若有多種當事人聯絡方式，統一於此欄位註明即可。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **財務情況** | 如個資檔案包含月收入、負債、固定薪資與預扣款、紅利獎金、資產與投資(股票)、借貸、辦識財物者或其他填寫個人財務狀況之欄位。 |
| | | 如C〇八一：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。 |
| | | 如C〇八二 負債與支出：支出總額、租金支出、貸款支出、本票等信用工具支出等。 |
| | | 如C〇八三 信用評等：信用等級、財務狀況與等級、收入狀況與等級 |
| | | 如C〇八四 貸款：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。 |

| | | |
|---|---|---|
| | | 如C〇八五 外匯交易紀錄。 |
| | | 如C〇八六 票據信用：支票存款、基本資料、退票資料、拒絕往來資料等。 |
| | | 如C〇八七 津貼、福利、贈款。 |
| | | 如C〇八八 保險細節：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。 |
| | | 如C〇八九 社會保險給付、就養給付及其他退休給付：生效日期、付出與收入之金額、受益人等。 |
| | | 如C〇九一 資料主體所取得之財貨或服務：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。 |
| | | 如C〇九二 資料主體提供之財貨或服務：貨物或服務之有關細節等。 |
| | | 如C〇九三 財務交易：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。 |
| | | 如C〇九四 賠償：受請求賠償之細節、數額等。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **社會活動** | 參加有關社會上各行各業或者某一社會性質問題調查或走訪的活動，具有以社會為媒介的性質，是基於“社會”這一事物而產生的。例如演講活動、旅行紀錄、社團活動、休閒活動等，這些都可稱之為社會活動。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **網路識別資料** | 指透過設備、應用程式、工具及通訊協定，諸如網際網路協定位址、瀏覽歷程記錄識別碼、無線射頻識別系統標籤或其他識別工具，使當事人可被連結到網路上之識別碼，例如：Cookie、IP、MAC。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **定位資料** | 指可識別當事人所在位置之資訊。例如：GPS定位、基地台位置資訊、WiFi無線接收裝置的MAC位址。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| **特殊類別個資** | **種族** | 例如：美洲印第安人或阿拉斯加原住民、亞裔、黑人或非裔美國人、夏威夷原住民或其他太平洋島民、白人。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **政治傾向** | 指意識形態，例如：社會主義、威權主義、無政府主義、保守主義、自由主義或當事人支持政黨之相關資料。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **信仰** | 例如宗教信仰：基督教、天主教、伊斯蘭教、佛教、印度教、道教或地 |

| | | |
|---|---|---|
| | | 方民俗信仰等資料。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **工會身分** | 當事人加入工會之資料。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **生物資料** | 指透過特定技術處理所得關於當事人身體、生理或行為特徵而確認其特定識別性之個人資料，例如：臉部圖像資料、指紋、虹膜資料、視網膜資料。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **性傾向** | 例如：異性戀、同性戀或雙性戀之資料。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **性生活** | 指性取向或性慣行之個人資料 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **基因** | 指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 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **病歷** | 指醫療法第六十七條第二項所列之各款資料，包括下列資料： |
| | | 一、醫師依醫師法執行業務所製作之病歷。 |
| | | 二、各項檢查、檢驗報告資料。 |
| | | 三、其他各類醫事人員執行業務所製作之紀錄。 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **醫療** | 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 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **健康檢查** | 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 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| | **犯罪前科** | 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 |
| | | ＊本欄位以Y或N表示，請勿空白。 |
| **自訂高風險個** | | 組織可自行決定組織的高風險個人資訊，數量不限，例如： |
| | | 金融機構帳戶之號碼、性騷擾申訴案件調查紀錄。 |
| | | |

| | | |
|---|---|---|
| **人資訊** | | |
| **其它可識別個資** | **其它直接識別** | 雖然不在現有的個資欄位清單上，但屬於可以直接辨識該自然人之個資，不需與其它相關資料做連結、比對或參照，例如當事人的簽名、相片等均屬於此類。 |
| | | ＊本欄位請簡要說明，如無請填 N/A，請勿空白。 |
| | **其它間接識別** | 在個人資料檔案中可能只含有無法直接識別出特定當事人的個人資料，但可以經由組織內其他資料來源進行資料比對、連結或參照的方式，找出當事人的身分，則此資料就屬於可以間接方式識別該個人的資料。 |
| | | ＊本欄位請簡要說明，如無請填 N/A，請勿空白。 |
| **特殊保護方式** | **控制措施** | 依據法令法規或其他要求或考量，針對個人資料須做特別處理者，如隱碼等擬匿名化(pseudonymization)措施，請簡要說明，填寫範例如下： |
| | | – 姓名隱碼(一碼) |
| | | – 身分證統一編號隱碼(四碼) |
| | | – 檔案設定密碼保護 |
| | | – 存放之資料夾有權限控管 |
| | | – 檔案櫃上鎖 |
| | | – 庫房有進出管制，專人保管鑰匙。 |
| | | ＊如無進階控制措施，本欄位以 N/A 表示，請勿空白。 |
| **保存** | **儲存位置** | 該個人資料檔案之律定保存地點(如：辦公室檔案櫃、個人抽屜、電腦機房主機、資料庫主機…等)，請簡要說明。 |
| | | ＊儲存位置請註明單位名稱加保存地點，請勿空白。 |
| | **法定保存期限** | 該個人資料檔案依據○○法，之保存期限(如：3 年、7 年…等)，請說明法定依據，填寫範例如下： |
| | | 會計法：___年 |
| | | ＊如無法定保存期限之依據，請以 N/A 表示，本欄位請勿空白。 |
| | **自訂保存期限** | 該個人資料檔案依據本組織自訂之保存期限(如：3 年、7 年…等)，請列出內部規章名稱，填寫範例如下： |
| | | ○○手冊/規定/規範：___年 |
| | | ＊列舉內部相關規範名稱及保存年限，若無內部規範請填寫「依法定保存期限辦理」，若無內部規範且無法定保存期限，請以 N/A 表示，請勿空白。 |

| | | |
|---|---|---|
| | **銷毀方式** | 該個人資料檔案之銷毀方式，填寫範例如下： |
| | | －紙本資料由○○單位統一辦理銷毀作業。 |
| | | －電子檔由承辦人自行刪除。 |
| | | －依 OO 法/規定本項資料不得銷毀。 |
| | | ＊若資料從未銷毀，請以 N/A 表示，本欄位請勿空白。 |
| **備註** | | 任何可補充說明的資訊。 |
| **單位名稱** | | 填表人之單位名稱。 |

九、個資事故通知當事人範本

## 非公務機關發生個資事故時對個資當事人通知之範例

**一、通知範圍**

應通知受事故影響之當事人，如無法確定個資事故當事人範圍，則應通知所有可能受事故影響之個資當事人。

**二、通知管道**

原則上以便利，且可對該個資當事人發生通知效力之方式即可，如電子郵件、簡訊或電話，如以電話通知所耗費之成本或時間較高，可以電子郵件或簡訊之方式為之。

**三、通知內容（至少應包含）**

(一)個資當事人個人資料被侵害之事實

(二)非公務機關已採取之因應措施（處理情形）

(三)後續供當事人查詢之專線與其他查詢管道

**四、簡易之簡訊或電子郵件通知範例**

親愛的消費者/會員您好：

非常抱歉，(公司或網站名稱)因(原因)發生個人資料外洩事故，且已有消費者接獲詐騙集團電話。提醒您，詐騙集團通常於週末或下班時間以(手法)誆騙消費者。如接獲疑似詐騙電話，請不要聽從指示操作 ATM 或網路銀行等或提供任何個人資料，並立即通報 165 警政署反詐騙專線。

針對這次事件，本公司已(改善措施)，未來也會持續加強資訊安全與個人資料保護管理，以降低消費者個資被侵害之風險。

如有關於訂單或本次個資事故之疑問，請於(上班時間)與本公司客服人員聯絡(電話)；上班時間以外請以(提供其他可行方式)聯絡本公司。

(公司名稱)　敬上

十、委外廠商個資安全維護聲明書（範例）

本公司受○○公司(綜合商品零售業者)委託蒐集、處理或利用個人資料，為確保個人資料檔案於蒐集、處理及利用時，皆尊重當事人之權益且合法，並依據個人資料保護法、個人資料保護法施行細則以及綜合商品零售業個人資料檔案安全維護管理辦法等相關規定建立適當之管理及安全措施，同意遵循下列規範：

一、告知義務

如有受委託代為蒐集個人資料之行為，應依個資法第 8 條、第 9 條規定，履行告知義務，或於首次處理或利用前為告知當事人。

二、蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間

保證僅於○○公司指示之範圍、類別、特定目的及其期間內，蒐集、處理或利用個人資料。

三、採取適當之安全措施

應依綜合商品零售業個人資料檔案安全維護管理辦法採取下列措施並訂定訂定安全維護計畫：

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。

四、複委託

(一)若需將○○公司委託之業務複委託其他廠商時，須經甲方事前書面同意。○○公司若同意乙方得以複委託方式提供服務，本公司及複委託廠商仍負有依照本聲明履行之責任，複委託廠商因執行業務而造成○○公司之損害時，本公司與複委託廠商應對○○公司之損害負連帶賠償之責。

(二)本公司受委託業務，就涉及蒐集、處理或利用個人資料或檔案之業務，不得複委託其他廠商執行。

五、緊急事故通知義務

本公司或本公司之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或有個人資料被竊取、洩漏、竄改或其他侵害事故時，應立即向○○公司指定窗口通知相關原因事實及採行之補救措施。本公司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。

六、保留指示之遵守

(一)受○○公司委託蒐集、處理或利用之個人資料，應進行相關保護措施，並應符合○○公司要求及符合現今科技水準之資訊安全保

護措施。

(二)應依本公司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)針對所儲存的個人資料，應該秉持保留最少的原則，並且制定資料處理與儲存程序來做好個人資料的控管。

(四)個人資料蒐集之特定目的消失或期限屆滿時，應主動刪除、停止處理或利用該個人資料。

(五)針對各項資安控制措施，每年應定期實施測試，以確保控制的有效性。

(六)同意○○公司得定期檢測本公司個人資料保管機制及系統安全性。

(七)受○○公司(綜合商品零售業者)委託蒐集、處理或利用之個人資料，並定期清查並製作個資盤點清冊。

七、委託關係終止或解除

應依○○公司指示，於委託關係終止或解除時，返還儲存個人資料之載體，並銷毀為履行委託契約而蒐集之個人資料。

八、委託個人資料之稽核

應依個人資料保護相關法規就受○○公司委託之業務定期（每年）稽核及記錄，並配合○○公司之稽核業務，依○○公司之指示提供相關文件。

九、問題通報

僅得於○○公司指示之範圍內，蒐集、處理或利用個人資料。如認○○公司之指示有違反本法、其他個人資料保護法律或其法規命令

者，應立即通知◯◯公司。

十、規定適用

受◯◯公司委託蒐集、處理或利用個人資料之行為，於個人資料保護法適用範圍內，視同◯◯公司，應遵守「綜合商品零售業個人資料檔案安全維護管理辦法」之規定。

十一、聲明書效力：

本聲明書視同雙方合約之一部分，倘有違反者，◯◯公司得不經催告逕行終止雙方合約；若◯◯公司受有損害，並得請求損害賠償。

立聲明書人(委外廠商)：

負　責　人：

地　　址：

電　　話：

中華民國　年　月　日

主辦單位 —— 經濟部商業發展署

執行單位 —— KPMG 安侯企業管理股份有限公司