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

經濟部商業發展署

零售業
個資安全宣導暨安全維護計畫規劃說明會

資策會科技法律研究所
114年4月30日

stli 科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

講 師 簡 介

張 維正 wilburchang@iii.org.tw

現職：資策會科法所 法律研究員

學歷：

國立高雄科技大學 科技法律研究所

國立高雄科技大學 電機工程學系

專業證照：

- TPIPAS個資管理師
- ISO/IEC 27001:2022 主導稽核員

大　綱

壹　零售業個人資料檔案安全維護管理辦法

- 個人資料保護法
- 個人資料保護法施行細則
- 重要法規介紹及法遵事項說明

貳　安全維護計畫規劃及範本說明

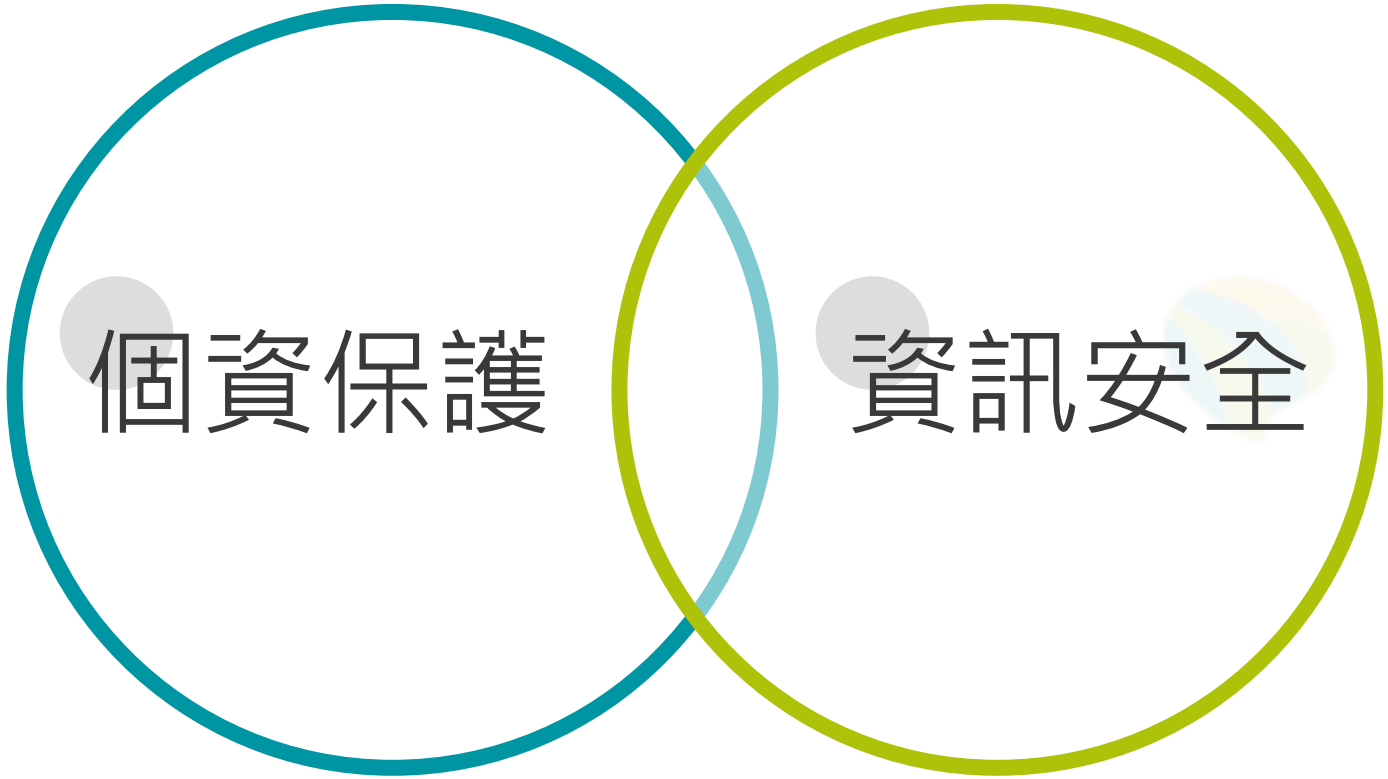
- 安全維護計畫範本
- 安全維護計畫內容說明
- 落實安維計畫措施之方式

壹. 零售業
個人資料檔案安全維護管理辦法

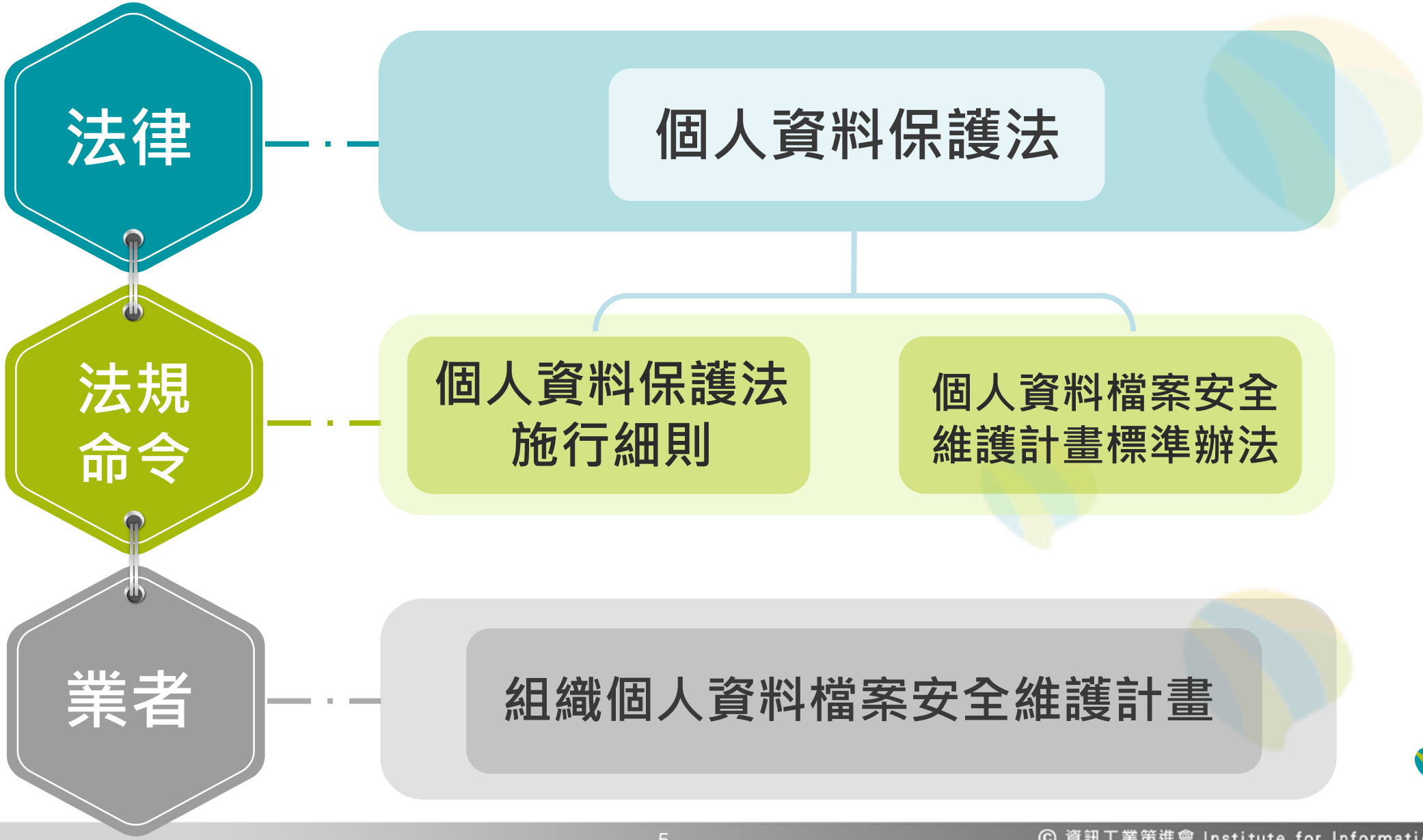
個資保護與資訊安全之關係

個人資料保護與資訊安全間，二者有**部分內容重疊**

現今數位化時代需**仰賴資訊安全，以落實個資保護**



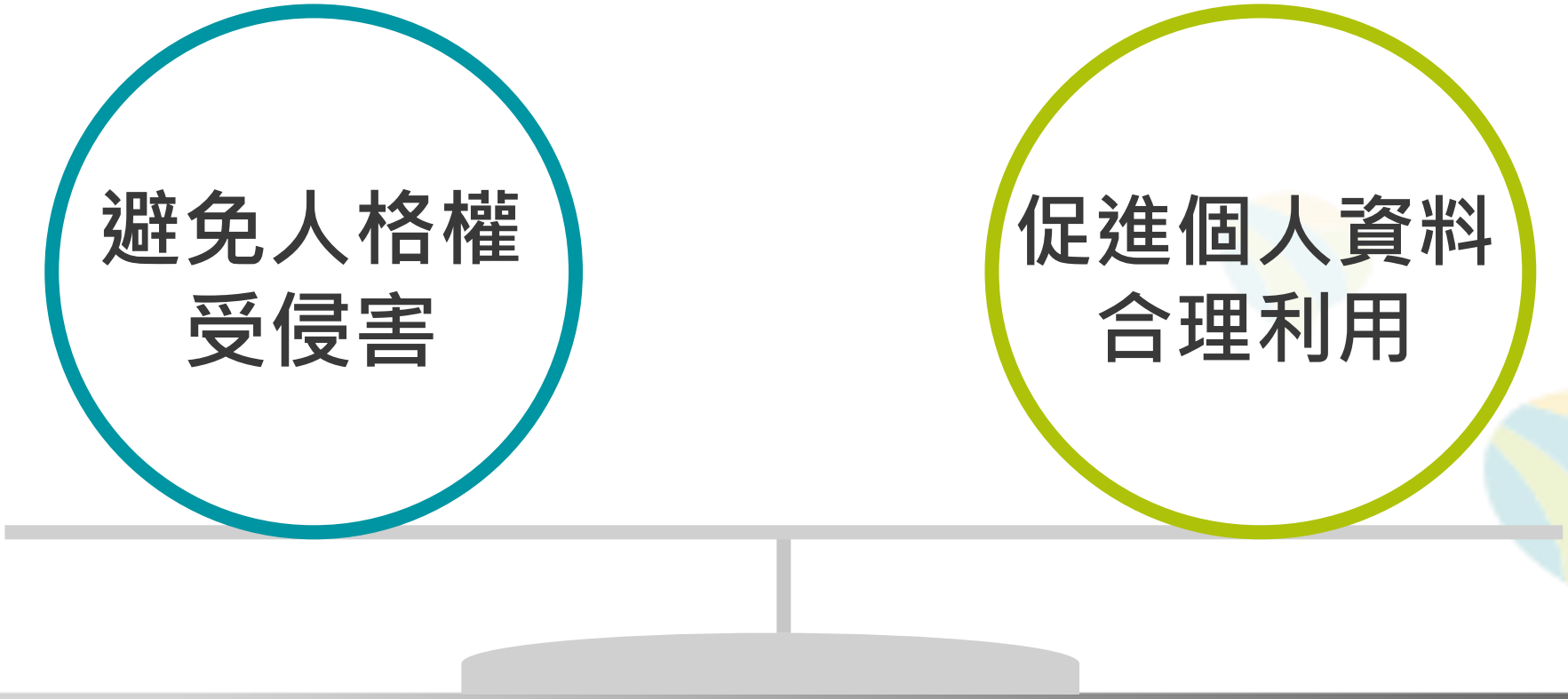
個人資料保護法規架構



個人資料保護法意旨

個人資料保護法第1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。



個人資料定義(1/2)

個人資料保護法第2條第1款

> 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。

個人資料

- **一般個資**：姓名、生日、電話、身分證字號等
- **特種個資**：病歷、醫療、基因、性生活、健康檢查、犯罪前科

間接識別
(施行細則§3)

該資料與其他資料**對照**、**組合**、**連結**等，才能識別出特定人

例如

直接識別

電話號碼

＋

間接識別*

電信業者

*臺灣臺北地方法院103年度小上字第155號民事判決

圖示來源：Flaticon.com

個人資料定義(2/2)

個人資料保護法第51條第1項

> 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。

非個人資料
- **亡者個資***（涉及在世人資料除外）
- **公司公開資料**等

不適用個資法之例外**

家庭活動

將自己或親友照片公開於社群媒體上

公開場所

將行車記錄器畫面公開於網路上

*法務部105年1月29日法律字第10503502210號函
**法務部102年3月27日法律字第10203502790號函釋

適當之安全措施

個人資料保護法第27條第1項

> 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。

個資安全維護措施*：技術面及組織面

- 個人資料安全維護之整體持續改善
- 使用紀錄、軌跡資料及證據保存
- 資料安全稽核機制
- 設備安全管理
- 認知宣導及教育訓練
- 資料安全管理及人員管理
- 個人資料蒐集、處理及利用之內部管理程序
- 事故之預防、通報及應變機制
- 個人資料之風險評估及管理機制
- 界定個人資料之範圍
- 配置管理人員及相當資源

*個人資料保護法施行細則第12條第2項

安全維護計畫實施辦法由來

個人資料保護法第27條第2項

- 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。
- 同條第3項：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。

個資法

經濟部商業發展署

制訂零售業個人資料檔案安全維護管理辦法

業者

訂定個人資料檔案安全維護計畫

適用零售業個資安維辦法之條件

安全維護辦法第3條

本辦法所稱零售業（以下簡稱業者），指非其他中央目的事業主管機關主管之從事實體店面，或實體店面兼營網際網路方式銷售商品之零售，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。

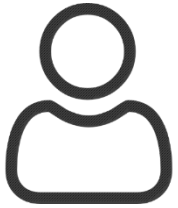
1. 實體店面、實體兼營網路
2. 公司登記、商業登記、有限合夥登記
3. 資本額達NT 1,000萬以上(含)
4. 招募會員、交易對象個資

例：訂單（姓名、電話等）

專責人員之責任與業務(1/2)

安全維護辦法第5條

> 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，並定期向業者之代表人或經其授權之人員提出報告。



專責人員

- 規劃
- 訂定
- 修正
- 執行

1. 安維計畫
2. 個資相關作業

報告

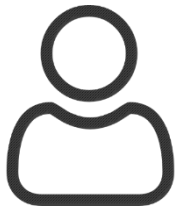
代表人、管理人、其他有代表權人

圖示來源：Flaticon.com

專責人員之責任與業務(2/2)

專責人員是否有條件要求：現行法律未規定

建議專責人員接受訓練並取得相關證照



專責人員

基礎	進階
TPIPAS個資管理師	TPIPAS個資內評師
臺灣個人資料保護與管理制度	
	ISO27001主導稽核員（資安）

圖示來源：Flaticon.com

查核人員之責任與業務

安全維護辦法第14條第1項

- 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，向業者之代表人或經其授權之人員提出報告。
- 同條第3項：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。

查核人員

- 為公司內部專門或負責稽核的人員
- 負責執行稽核安全維計畫，並向代表人或有管理權人報告稽核結果

查核人員與專責人員不得為同一人

圖示來源：Flaticon.com

安全維護計畫內容

安全維護辦法第6條

- 業者應依本辦法規定訂定安全維護計畫，載明下列事項：

1. 個人資料蒐集、處理及利用之內部管理程序
2. 個人資料之範圍
3. 資料安全管理及人員管理
4. 認知宣導及教育訓練
5. 事故之預防、通報及應變機制
6. 設備安全管理
7. 資料安全稽核機制
8. 使用紀錄、軌跡資料及證據保存
9. 業務終止後，個人資料處理方法
10. 個人資料安全維護之整體持續改善方案

個人資料蒐集、處理及利用之內部管理程序

蒐集

指以任何取得個人資料的方式：直接蒐集、間接蒐集

處理

為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送

利用

指將蒐集之個人資料為處理以外之使用

個人資料之範圍及項目

安全維護辦法第7條第1項

> 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。

特定目的

消費者類

- 行銷
- 消費者、客戶管理服務
- 網路購物及其他電子商務服務

員工人事類

- 人事管理
- 全民健康保險
- 勞工保險

個資項目

- 姓名
- 住址
- 行動電話
- 出生年月日
- 身分證字號等

刪除、銷毀個人資料

安全維護辦法第7條第2項

> 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。

1. **定期清查保有的個資**
   - 定期進行**個資盤點**
2. **不屬於特定目的範圍**
   特定目的消失保存期限期滿
   - 刪除、銷毀、停止蒐集、處理、利用或其他處置

個資盤點與風險評估

個資法施行細則第12條第2項

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

個人資料盤點

- 個人資料檔案名稱
- 個人資料類型
- 個人資料項目
- 個人資料筆數
- 特定目的
- 法定情形
- 蒐集來源
- 保存方式與期限等

風險評估（評鑑）

- 個資作業流程
- 可能產生的風險
- 風險對公司的影響
- 風險對當事人的影響
- 發生風險的機率
- 風險等級的認定
- 因應風險的方式等

蒐集時告知當事人事項

安全維護辦法第8條第1項

> 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。

直接蒐集
個資法第8條

間接蒐集
個資法第9條

告知事項

- 非公務機關名稱
- 蒐集之目的
- 個人資料之類別
- 個人資料利用之期間、地區、對象及方式
- 當事人依第三條規定得行使之權利及方式
- 當事人得自由選擇提供個人資料時，不提供將對其權益之影響

當事人行使權利(1/2)

安全維護辦法第18條

第1項　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：

1. 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
2. 遵守個資法第十三條處理期限之規定
3. 告知查詢、請求閱覽或製給複製本得酌收必要成本費用

第2項　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

個資法第3條當事人具有之權利

- 查詢或請求閱覽
- 請求製給複製本
- 請求補充或更正
- 請求停止蒐集、處理或利用
- 請求刪除

當事人行使權利(2/2)

個人資料保護法 —— 拒絕理由與處理期限

第10條但書

拒絕查詢、閱覽、製給複製本之情形

1. 妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益
2. 妨害公務機關執行法定職務
3. 妨害該蒐集機關或第三人之重大利益

第11條第2項、第3項但書

拒絕停止處理、利用正確性有爭議個資；刪除、停止處理或利用個資之情形

1. 因執行職務或業務所必須
2. 經當事人書面同意

第13條

受理當事人請求之期限

1. 查詢、提供閱覽或製給複製本：15日內准駁，必要時可延長，延長期間不能超過15日
2. 更正或補充資料：30日內准駁，必要時可延長，延長期間不能超過30日

個人資料國際傳輸(1/2)

安全維護辦法第8條第3項

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。

個資法第21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。

1. 涉及國家重大利益
2. 國際條約或協定有特別規定
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
4. 以迂迴方法向第三國（地區）傳輸個人資料規避本法

個人資料國際傳輸(2/2)

常見之個人資料國際傳輸型態

主動傳輸（提供）

- 本公司位於國外的部門
- 位於國外的其他公司（包含母子公司、關係企業等）
- 位於國外的自然人

使用雲端系統傳輸（提供）

多數雲端服務業者，會將實體伺服器（機房）設置於國外，因此資料會儲存（落地）於國外，屬於國際傳輸之一種

建議檢視公司目前所使用之雲端服務，其伺服器所在的國家或地區為何

圖示來源：Flaticon.com

利用個人資料行銷

安全維護辦法第20條

- 業者利用個人資料為行銷時，應明確告知當事人零售業者立案名稱及個人資料來源。
- 業者首次利用個人資料為宣傳、推廣或行銷時，應提供當事人或其法定代理人表示拒絕接受宣傳、推廣或行銷之方式，並支付所需費用；當事人或其法定代理人表示拒絕接受宣傳、推廣或行銷者，應立即停止利用，並周知所屬人員。

零售業者

行銷

會員消費者

告知

- 公司名稱
- 個資來源

如果當事人拒絕行銷

零售業者

通知

所屬人員

圖示來源：Flaticon.com

委託監督

安全維護辦法第19條

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8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。

契約中明確約定之內容

- 監督時應盡的事項
- 委託契約中應約定的項目
- 監督的過程（內容）要留存紀錄

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. 受託者採取的安全措施
3. 如有複委託，複委託之對象
4. 受託者違反個資相關法規時，應向委託機關通知之事項及採行之補救措施
5. 必須要委託機關同意方能執行之事項
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

範例僅供參考，應依公司實際業務及個資政策調整。

委託個資作業契約範例(1/4)

本公司（零售業者）委託○○公司（資訊服務、活動行銷業者等）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：

1. 告知義務

如有受委託代為蒐集個人資料之行為，應依個人資料保護法第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。

2. 使用規範

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

3. 採取措施

應依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
6) 認知宣導及教育訓練
7) 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

委託個資作業契約範例(2/4)

範例僅供參考，應依公司實際業務及個資政策調整。

4. 複委託

依個資內容與公司規範決定是否允許複委託

- 若需將本公司委託之業務複委託其他廠商時，須經本公司事前書面同意。本公司若同意○○公司得以複委託方式提供服務，○○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本公司之損害時，○○公司與複委託廠商應對本公司之損害負連帶賠償之責。
- 若○○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。

5. 緊急事故通知義務

○○公司或○○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，應立即向本公司指定窗口通知相關原因事實及採行之補救措施。○○公司應盡最大努力協助調查，提供所有必要之資料，並為各項必要之配合行為。

委託個資作業契約範例(3/4)

範例僅供參考，應依公司實際業務及個資政策調整。

6. 保留指示之遵守

1) 受本公司委託蒐集、處理或利用之個人資料，應進行相關保護措施，並應符合本公司要求及符合現今科技水準之資訊安全保護措施。
2) 應依○○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。
3) 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之控管。
4) 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。
5) 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。
6) 同意本公司得定期檢測○○公司個人資料保管機制及系統安全性。
7) 受本公司委託蒐集、處理或利用之個人資料，並定期清查並製作個資盤點清冊。

7. 委託關係終止或解除

應依本公司指示，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。

委託個資作業契約範例(4/4)

範例僅供參考，應依公司實際業務及個資政策調整。

8. 委託個資之稽核

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

9. 問題通報

僅得於本公司指示之範圍內，蒐集、處理或利用個人資料。如認本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，應立即通知本公司。

10. 規定適用

受本公司委託蒐集、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，視同本公司，應遵守「零售業個人資料檔案安全維護管理辦法」之規定。

11. 聲明書效力

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

資料安全管理及人員管理(1/2)

安全維護辦法第9條

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：

1. 權限設定

- 建立管理機制
- 依業務需求，設定人員接觸個資的權限
- 定期確認權限的必要性及適當性

2. 業務負責人

- 檢視個資相關業務之性質
- 規範個資相關作業負責人員

3. 保管與保密

- 保管儲存個資之媒介物
- 約定保管及保密義務

例如：紙本、電腦、隨身碟等

資料安全管理及人員管理(2/2)

安全維護辦法第9條

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：

4. 離職交接

- 取消離職人員的通行碼、帳號等
- 交接持有的個資。

5. 傳輸安全

- 傳輸個人資料時，應依不同傳輸方式，採取適當之安全措施。

6. 加密與備份

- 個人資料有加密之必要者，應於蒐集、處理或利用時，採取適當之加密措施。
- 個人資料有備份之必要者，應對備份資料採取適當之保護措施。

資通系統之安全措施

資通系統 | 蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

安全維護辦法第10條

業者以資通安全管理法所稱資通系統直接或間接蒐集、處理或利用個人資料，應採取下列安全措施：

安全措施：每年至少一次演練、檢討改善

1. 設定身分認證機制，且帳號密碼有一定複雜度。
2. 個人資料之隱碼機制，適當且一致性之遮蔽。
3. 定期檢測電腦設備或系統之漏洞，並採取因應措施。
4. 連接網路之系統，採用防毒軟體並定期掃描。
5. 防止外部網路入侵對策，並定期更新。
6. 測試系統時避免使用真實資料，若要使用應訂定規範。
7. 系統變更時，確保不會降低安全性。
8. 定期檢視系統，檢查使用狀況及存取個資之情形。

設備安全管理

安全維護辦法第13條

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：

1. 紙本資料檔案

- 安全保護措施
- 管理程序

2. 電子資料檔案

- 存放資料的電腦或自動化機器相關設備
- 安全防護系統或加密機制

3. 資料銷毀程序

- 紙本資料與電子資料的銷毀程序
- 電腦或其他儲存資料的設備，要報廢或轉化其他用途，應採取適當防範措施

紀錄保存

安全維護辦法第15條第1項

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：

- 留存個人資料使用紀錄
- 留存自動化機器設備之軌跡資料或其他相關之證據資料

建議保存項目 至少保存5年

個資使用紀錄

1. 客服
2. 消費習慣統計
3. 行銷

Email、簡訊、實體DM

軌跡資料（Log）

1. 存取會員資料
2. 權限異動
3. 系統異常事件

業務終止後個資處理方式(1/2)

安全維護辦法第16條

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：

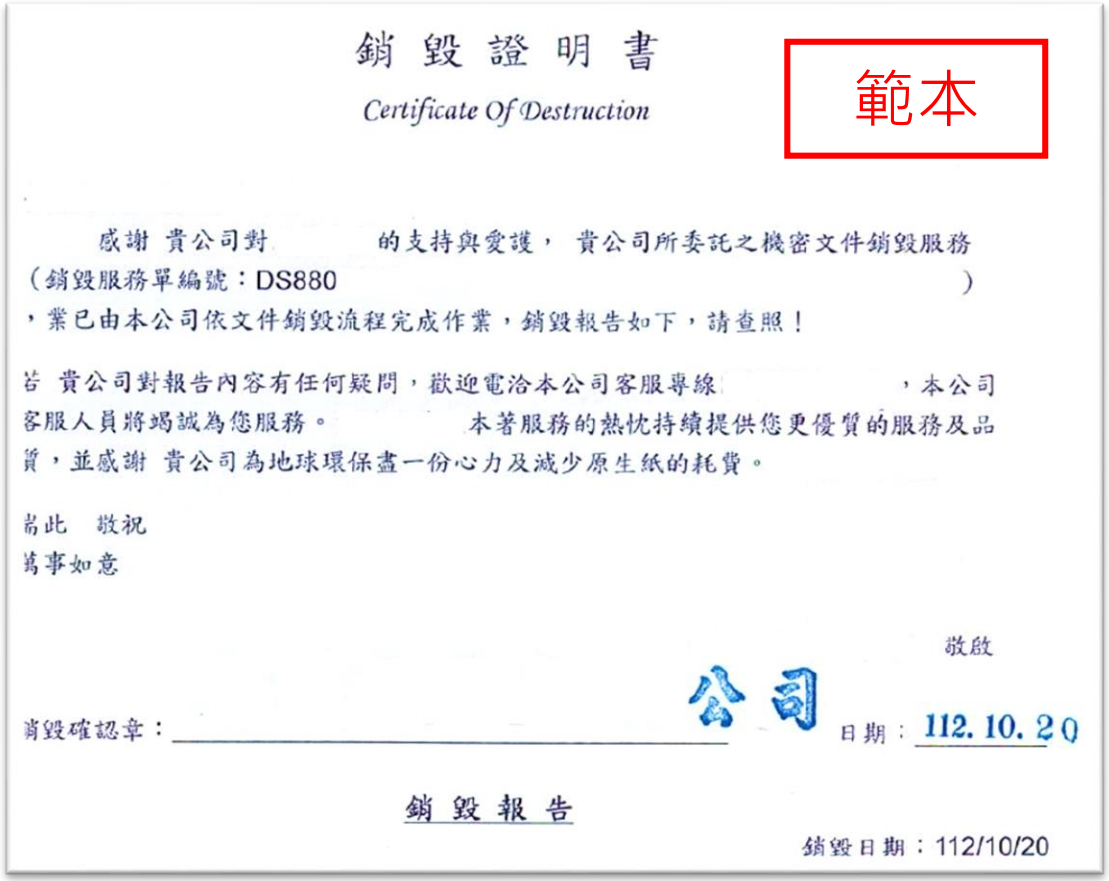
應製作紀錄，並至少留存五年

- **銷毀**：方法、時間、地點及證明銷毀之方式
- **轉移**：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
- **刪除、停止處理或利用**：方法、時間或地點

業務終止後個資處理方式(2/2)

定期清查保有的個人資料檔案

非特定目的範圍、特定目的消失或保存期限屆滿等個人資料，亦應保留銷毀或刪除之紀錄至少5年，紀錄之內容與業務終止後處理方式相同。



銷 毀 證 明 書

Certificate Of Destruction

範本

感謝 貴公司對　　的支持與愛護， 貴公司所委託之機密文件銷毀服務（銷毀服務單編號：DS880　　），業已由本公司依文件銷毀流程完成作業，銷毀報告如下，請查照！

若 貴公司對報告內容有任何疑問，歡迎電洽本公司客服專線　　，本公司客服人員將竭誠為您服務。　　本著服務的熱忱持續提供您更優質的服務及品質，並感謝 貴公司為地球環保盡一份心力及減少原生紙的耗費。

耑此　敬祝

萬事如意

敬啟

銷毀確認章：　　公司　　日期：112. 10. 20

銷 毀 報 告

銷毀日期：112/10/20

以紙本資料銷毀為例

公司如有委託廠商協助水銷紙本資料：

1. 銷毀方法：水銷
2. 銷毀時間：日期
3. 銷毀地點：廠商處
4. 銷毀證明：廠商出具銷毀證明書

建議拍攝銷毀過程

事故之預防、通報及應變機制(1/2)

安全維護辦法第12條第1項

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：

發生事故

- **應變措施**：採取控制措施，防止事故或損害擴大
- **通知**：
  1. 於得知事故起，72小時內通報主管機關
  2. 查明事故及損害，通知當事人或其法定代理人
- **改善**：查明事故根因，並訂定預防及改進措施

圖示來源：Flaticon.com

事故之預防、通報及應變機制(2/2)

安全維護辦法第12條第4項

■ 通報紀錄表

個人資料侵害事故通報紀錄表		
化粧品批發零售業者名稱： 通報機關：	通報時間：　年　月　日　時　分 通報人：　簽名（蓋章）　職稱： 電話： Email: 地址：	
事件發生時間		
事件發生種類	□竊取 □洩漏 □竄改 □毀損 □滅失 □其他侵害事故	個資侵害之總筆數（大約） ＿＿＿＿＿＿筆 □一般個資＿＿＿＿＿＿筆 □特種個資＿＿＿＿＿＿筆
發生原因及事件摘要		
損害狀況		
個資侵害可能結果		
擬採取之因應措施		
擬採通知當事人之時間及方式		
是否於發現個資外洩後七十二小時通報	□是　□否，理由	

https://law.moj.gov.tw/LawClass/LawGetFile.ashx?FileId=0000308010&lan=C

事故之通知當事人

個人資料保護法第12條

> 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

個人資料保護法施行細則第22條

通知方式

言詞

書面

電話

簡訊

電子郵件

通知內容

- 個人資料被侵害的事實
- 已經採取的因應措施

圖示來源：Flaticon.com

行政檢查與行政調查

安全維護辦法第12條第3項

> 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，並視檢查結果為後續處置。

1. 行政檢查 | 例行性查核

2. 行政調查 | 發生事故後調查

政府機關

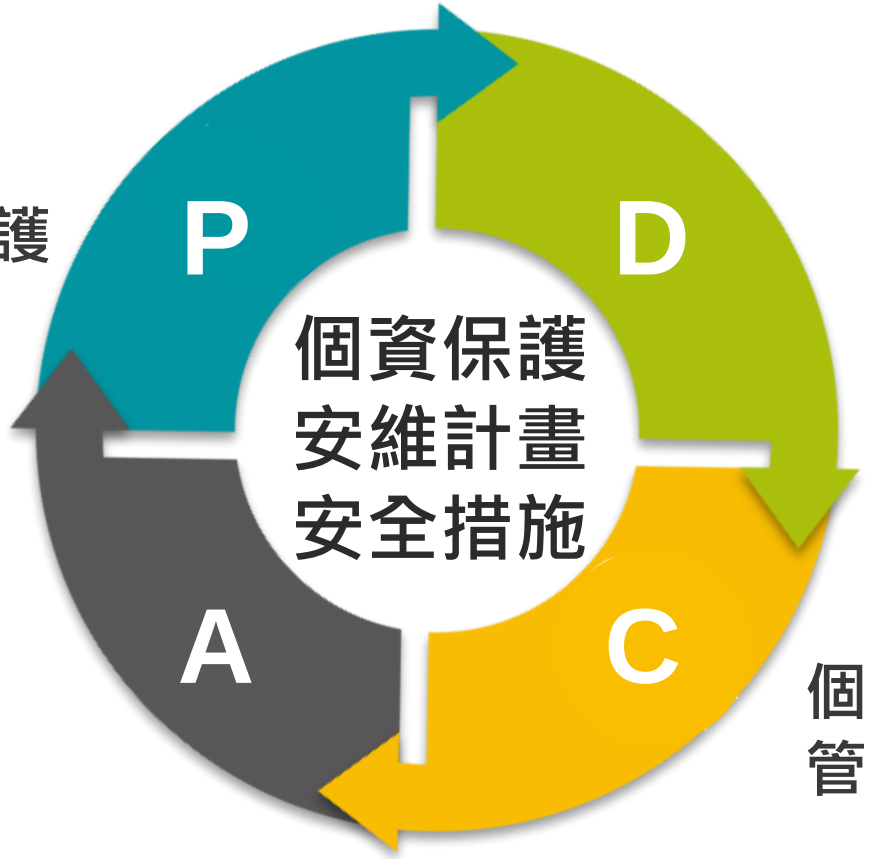
1. 派員進入公司檢查，要求公司人員配合說明、提供資料等
2. 扣留或複製證據資料
3. 率同資訊、電信或法律等專業人員
4. 公司相關人員不得規避、妨礙或拒絕

圖示來源：Flaticon.com

持續改善

安全維護辦法第17條

> 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。



Plan 計畫
規劃
個人資料保護與管理制度

Do 執行
實施
個人資料保護與管理制度

Act 改善
持續
監督與改善

Check 評估
評估
個人資料保護與管理制度有效性

罰則(1/4)

個人資料保護法第47條

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。

裁罰並限期改正 | 處罰5萬-50萬，並限期改正，屆期未改正者，按次處罰

非公務機關

- 無法定事由而蒐集、處理或利用特種個資
- 無法定事由而蒐集或處理一般個資
- 個資利用逾越特定目的
- 違反中央目的事業主管機關對國際傳輸之限制

罰則(2/4)

個人資料保護法第48條第1項

> 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。

限期改正 | 先限期改正，屆期未改正者，按次處罰2萬-20萬

非公務機關

- 未於蒐集資料時，落實告知當事人事項，包含直接蒐集與間接蒐集
- 拒絕或未讓當事人依個資法第3條行使權利
- 發生個資安維案件時，未通知當事人
- 當事人表示拒絕行銷時，未立即停止行銷
- 首次行銷時，未提供當事人拒絕方式，或未支付所需費用

罰則(3/4)

個人資料保護法第48條第2項、第3項

非公務機關違反第27條第1項或未依第2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.....

裁罰並限期改正 | 處罰2萬-200萬，並限期改正，屆期未改正者，按次處罰

非公務機關

- 未採取適當之安全維護措施
- 未訂定個資安全維護計畫

屆期未改正者或情節重大者處罰金額為15萬-1500萬

罰則(4/4)

個人資料保護法

- 第49條：非公務機關無正當理由違反第22條第4項規定者.....
- 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。

其他裁罰事由

處罰2萬-20萬	規避、妨礙或拒絕主管機關進行行政檢查或行政調查
受與公司同一額度金額之處罰	公司之管理人、代表人或其他有代表權人，除非能證明已盡到防止義務

貳. 個人資料檔案安全維護計畫規劃及範本說明

範例僅供參考，應依公司實際業務及個資政策調整。

安全維護計畫範本(1/21)

公司名稱個人資料檔案安全維護計畫

壹、組織及規模

一、公司名稱：○○○

二、地址：○○○

三、負責人：○○○

四、資本額：新臺幣○○○元*

五、經營事業：○○○**

本辦法適用門檻：1000萬

- 訂定日期：中華民國○○○年○○月○○日
- 修訂日期：中華民國○○○年○○月○○日

1. 記錄版更，確保版本正確
2. 作為定期檢視之佐證

*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。
**實體店面方式零售、網際網路方式零售或其他事業等。

安全維護計畫範本(2/21)

範例僅供參考，應依公司實際業務及個資政策調整。

貳、個人資料檔案安全維護管理措施

一、依據：

（一）個人資料保護法第二十七條第三項及零售業個人資料檔案安全維護管理辦法第四條規定。

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），本公司所屬人員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。

安全維護計畫範本(3/21)

範例僅供參考，應依公司實際業務及個資政策調整。

- 依公司實況調整
- 可另外說明配置的資源種類
- 注意人員、資源的合理性

三、專責人員及資源配置

（一）專責人員：

1. 姓名：○○○（至少1名）
2. 所屬單位（部門）：○○○
3. 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) 於每年○月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：○○○（至少1名）
2. 所屬單位（部門）：○○○
3. 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*

*預算可包含管理人員薪資、資訊設備維護費用、顧問費用等，亦可記載一定範圍金額。

範例僅供參考，應依公司實際業務及個資政策調整。

安全維護計畫範本(4/21)

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. 本公司名稱。
2. 蒐集目的。
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. 當事人得向本公司請求查詢、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。

*個資類別可參考法務部「個人資料保護法之特定目的及個人資料之類別」，網址：https://www.moj.gov.tw/2204/2528/2529/2545/12798/post。

安全維護計畫範本(5/21)

範例僅供參考，應依公司實際業務及個資政策調整。

應至少每年清查一次可視需求調整

（四）指定管理人員每年清查本公司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二十條第一項但書之規定。

（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。

安全維護計畫範本(6/21)

範例僅供參考，應依公司實際業務及個資政策調整。

五、個人資料之範圍及項目

（一）個人資料範圍：指本公司蒐集、處理及利用之○○○、○○○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：個人資料特定目的為○○○、○○○等運用等運用。**

（三）指定管理人員每年定期清查本公司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。

應至少每年清查一次
可視需求縮短清查周期

*範圍可參考個人資料保護法第2條第1款，例如：姓名、出生年月日等。
**特定目的可參考法務部「個人資料保護法之特定目的及個人資料之類別」，例如：人事管理、勞工保險、消費者、客戶管理與服務。

範例僅供參考，應依公司實際業務及個資政策調整。

安全維護計畫範本(7/21)

六、資料安全管理及人員管理

（一）資料安全管理：

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. 對內或對外從事個人資料傳輸時，加強管控避免外洩。
6. 重要個人資料檔案應另加設密碼，非經陳報○○核可不得存取。*

*陳報對象可為負責人、部門主管或其他經授權之人等

安全維護計畫範本(8/21)

範例僅供參考，應依公司實際業務及個資政策調整。

7. 每〇日進行防毒、掃毒等必要之安全措施。
8. 所屬人員非經本公司〇〇核可，不得任意複製本公司保有之個人資料檔案。
9. 本公司蒐集、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、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。
10. 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，應每年一次進行演練及提出檢討改善報告。

至少每年一次

（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。所屬人員非經〇〇核可，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。

範例僅供參考，應依公司實際業務及個資政策調整。

安全維護計畫範本(9/21)

七、人員管理

變更密碼時機可視需求調整

（一）所屬人員登錄電腦之識別密碼，每〇日變更一次。

（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）本公司與所屬人員間之勞務、承攬及委任契約均列入保密、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。

（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。

（五）所屬人員離職時，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。

安全維護計畫範本(10/21)

範例僅供參考，應依公司實際業務及個資政策調整。

八、認知宣導及教育訓練

（一）每年對所屬人員實施個人資料保護法之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。

（二）個人資料保護之宣導及教育訓練應留存相關紀錄或佐證資料。

（三）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。

紀錄或佐證資料

1. 簽到表
2. 學習系統紀錄
3. 教材
4. 課後測驗（評量）

安全維護計畫範本(11/21)

範例僅供參考，應依公司實際業務及個資政策調整。

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。
4. 依個人資料保護法、個人資料保護法施行細則及零售業個人資料檔案安全維護管理辦法等規定，採取組織面及技術面之適當安全維護措施。

安全維護計畫範本(12/21)

範例僅供參考，應依公司實際業務及個資政策調整。

（二）應變措施

1. 發現本公司有個人資料遭竊取、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

1. 本公司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記錄表」通報主管機關。如已向地方主管機關通報，應副知中央主管機關。
2. 配合主管機關對事故進行檢查，所屬人員應說明、配合措施或提供相關證明資料
3. 保留事故預防措施、應變措施、通報措施及調查相關資料至少五年。

安全維護計畫範本(13/21)

範例僅供參考，應依公司實際業務及個資政策調整。

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）本公司保有之個人資料檔案應每〇日備份。

（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。

安全維護計畫範本(14/21)

範例僅供參考，應依公司實際業務及個資政策調整。

（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。

門禁措施、消防設備等

（十）資通系統避免使用真實個人資料進行測試，若有使用真實個人資料進時，應訂定使用規範並確實遵守。

（十一）本公司處理個人資料之資通系統有變更時，將確保其安全性未降低。

（十二）本公司將每年檢視處理個人資料的資通系統，評估其使用狀況及存取個人資料的情形；前述檢視作業時併確認蒐集、處理或利用個人資料的電腦、相關設備或系統是否具備必要的安全性，並採取適當的安全機制。

安全維護計畫範本(15/21)

範例僅供參考，應依公司實際業務及個資政策調整。

十一、資料安全稽核機制

（一） 每年○月（或每年）辦理個人資料檔案安全維護稽核，檢查本公司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。

安全維護計畫範本(16/21)

範例僅供參考，應依公司實際業務及個資政策調整。

十二、使用紀錄、軌跡資料及證據保存

（一） 本公司建置個人資料之電腦，其個人資料使用紀錄，每〇日備份並設定密碼，儲存該紀錄之儲存媒介物保存於適當處所以供備查。

（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，非經〇〇核可，不得任意取出。

（三） 本公司應保存以下紀錄：

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五年。

範例僅供參考，應依公司實際業務及個資政策調整。

安全維護計畫範本(17/21)

十三、業務終止後之個人資料處理方法

- **本公司於業務終止後，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） 本公司應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，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。

安全維護計畫範本(18/21)

範例僅供參考，應依公司實際業務及個資政策調整。

十五、當事人行使權利

- **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。

安全維護計畫範本(19/21)

範例僅供參考，應依公司實際業務及個資政策調整。

十六、委託作業

- 本公司委託他人蒐集、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。

安全維護計畫範本(20/21)

範例僅供參考，應依公司實際業務及個資政策調整。

（四） 要求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。

（五） 要求受託者認本公司之指示有違反個人資料保護法、個人資料保護法施行細則、零售業個人資料檔案安全維護管理辦法或其法規命令者，應立即通知本公司，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。

（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。

安全維護計畫範本(21/21)

範例僅供參考，應依公司實際業務及個資政策調整。

十七、行銷

（一）本公司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名稱及個人資料來源。

（二）本公司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。

交流討論

THANK YOU

數位轉型．軟體技術．資安產業．數位經濟