目錄

零售業個資保護宣導說明會

資策會科技法律研究所

2024.11.12

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

Institute for Information Industry

簡報大綱

01 零售業個資檔案安全維護管理辦法之介紹

02 安全維護計畫（範本）之說明

01 零售業個資檔案安全維護管理辦法之介紹

前言

■ 2023年 5 月經濟部裁罰案例

A百貨業

A業者接獲匿名網路勒索信件，被竊取內容包含業務資料、公司及供應商資料與90萬用戶個資等。經濟部辦理行政調查，經審業者函復改善情形及佐證資料，系爭個資外洩事故仍有未確實通知當事人、未明確揭示蒐集個資主體(包括本公司及其關係企業）、未採行適當個資安全維護措施（無留存自行檢查、內部稽核、銷毀等紀錄)等。因此依據個資法第48條及第50條規定處分，業者與其代表人**各**裁罰新台幣20萬元罰鍰。

■ 2024年9月經濟部裁罰案例

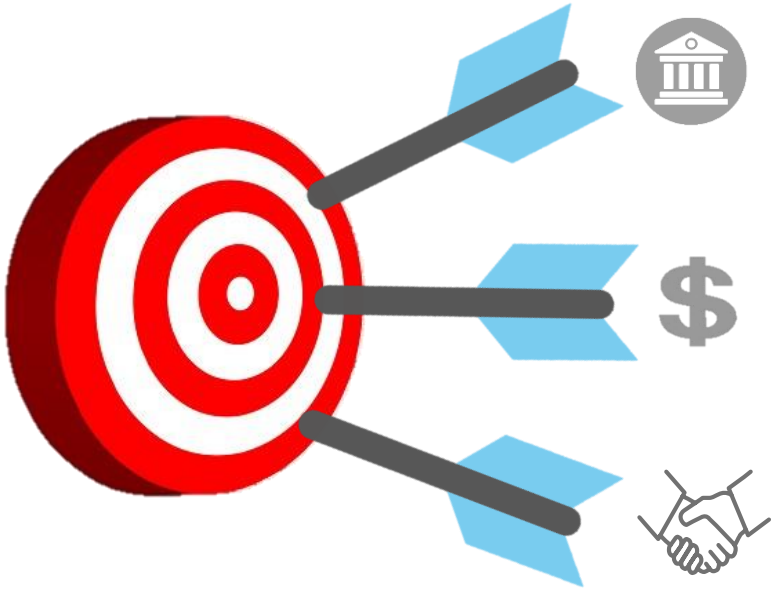
B電子器材零售業

B業者遭駭客入侵資料庫，竊取資料包含公司及供應商資料與50萬用戶個資等。經濟部辦理行政調查，發現平台上程式存在安全漏洞，內部缺乏個資管理與應變措施，待改善事項包括：(1)應補足個資外洩事件事件通報相關程序；(2)應提供本次受害案件之鑑識報告及遭駭後之改善措施；(3)對於所屬人員未實施定期個資保護認知宣導及教育訓練；(4)對委外廠商應要求善盡個人資料保密義務及個人資料安全相關責任，於隱私保護聲明中須提及第三方接觸個資之實情，並每年進行實地稽核。因此依據個資法第48條第2項及第50條規定處分，業者與其代表人**各**裁罰新台幣20萬元罰鍰。

個人資料保護法施行後再次修正

2010.04.27	2010.05.26	2012.09.26	2012.10.01	2015.12.30	2016.03.15	2023.05.31
個人資料保護法三讀通過	總統令公布個人資料保護法	施行細則正式公告	個人資料保護法正式施行	個人資料保護法修正	個人資料保護法修正條文暨細則施行	個人資料保護法增修部分條文

個資母法>>>施行細則>>>各機關辦法>>>行業標準



設立個資保護獨立監督機關

- 新增個資法第1條之1，成立個人資料保護委員會
- 籌備處於112/12/5成立
- 具獨立性、專責性及機關性

加重企業違反個資安全維護義務的罰鍰

- 首次違反立即裁罰並限期改正，裁罰2～200萬元
- 逾期未改正或情節重大案件，裁罰15～1500萬元

強化聯繫會議功能

- 精進案件通報與監督程序
- 落實執法及強化行政檢查

個資保護行政檢查(1/2)

行政檢查

預防性

例行性

行政院及所屬各機關落實個人資料保護聯繫作業要點
第四點

1. 中央目的事業主管機關應於每年一月底前擬定依個資法第二十二條第一項規定辦理之行政檢查計畫送國發會，並於提報聯繫會議後，確實執行。
2. 中央目的事業主管機關應組成個資行政檢查小組，辦理前項之年度行政檢查，及因應、處理個資外洩案件；其成員得包括具有法律、資訊專業之機關資深人員及外部專家。
3. 中央目的事業主管機關應評估所管非公務機關之個資外洩風險，將其中具有高風險者優先列入第一項之年度行政檢查對象。
4. 前項所定高風險者，得參考第六點各款情形及發生個資外洩事件之次數等因素綜合考量。

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

5

個資保護行政檢查(2/2)

行政調查

行政院及所屬各機關落實個人資料保護聯繫作業要點

第九點

1. 中央目的事業主管機關得依個資法第二十二條至第二十六條規定，對該非公務機關為適當之監督管理措施。
2. 中央目的事業主管機關就個資外洩案件辦理行政調查，得於必要時請求警察機關或法務部調查局提供協助。
3. 中央目的事業主管機關就個資外洩案件，經查明違反個資法之規定者，應視具體調查結果，依個資法第四十七條至第五十條規定辦理；並得依情節輕重及個資外洩事件造成之影響，依個資法第二十五條規定處分。
4. 中央目的事業主管機關對於非公務機關有個資法第四十八條第二項或第三項情形者，應處罰鍰，並令其限期改正，屆期未改正者，按次處罰。

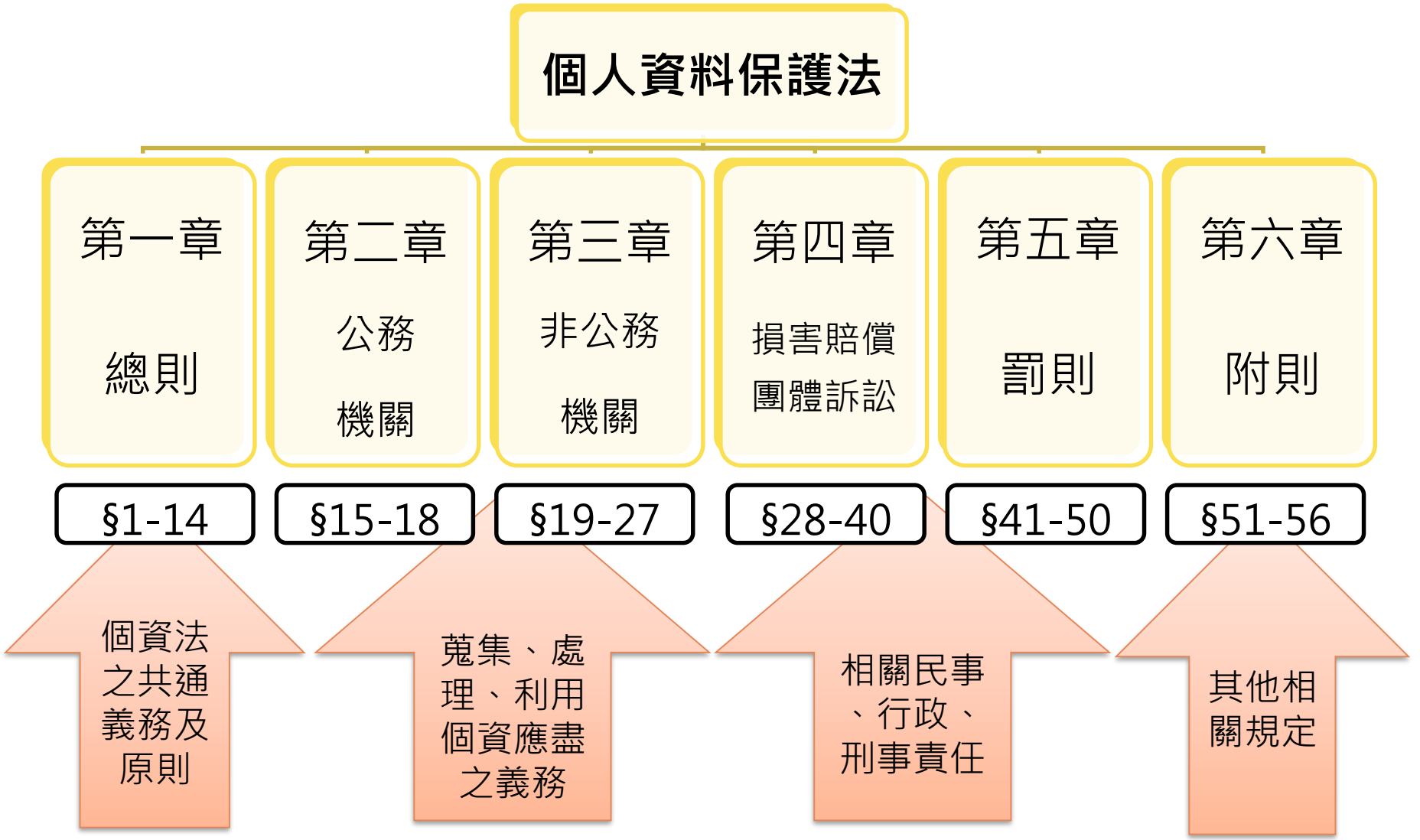
第十點

中央目的事業主管機關對個資外洩案件之行政調查流程，除重大矚目之個資外洩案件依第十一點規定確認管轄機關者外，其餘行政調查程序，依附件二流程圖辦理。

① 行政院、立法院或監察院關注之個資外洩案件。
② 經媒體顯著披露之個資外洩案件，例如經平面媒體全國性版面報導、電子媒體專題討論。

6

個資法之架構



個人資料保護法與相關法制架構

法律

個資法

命令

個資法
施行細則

個人資料檔案
安全維護計畫
標準辦法

民間部門

個人資料檔案安全維護計畫

說

寫

做

個資檔案安全維護規範現況-2024年

主管機關	業別	辦法數
文化部	電影事業	1
數位部	數位經濟相關產業（包含：電子購物及郵購業、軟體出版業、電腦程式設計、諮詢及相關服務業、資料處理、主機及網站代管服務業、其他資訊服務業，以及其他資訊服務業）	1
經濟部	**綜合商品零售業**、製造業及技術服務業、自來水事業、電業及公用天然氣事業、著作權集體管理團體	5
金管會	指定外籍移工匯兌公司、指定非公務機關（金融控股、銀行、證券、期貨、保險、電子支付、其他經金管會公告之金融服務業、財團法人）	2
通傳會	電信事業、用戶數達三千戶以上之提供網際網路接取服務之設置未使用電信資源之公眾電信網路者、有線廣播電視、電視、訂戶數達三千戶以上之直播衛星廣播電視服務事業、經營國內新聞台或購物頻道事業、電信消費爭議處理機構及其他公告通傳事業等八類	1
交通部	民用航空運輸業、船舶運送業、汽車運輸與計程車業、交通部指定非公務機關（觀光旅館業、旅館業、民宿、旅行業、觀光遊樂業）、停車場經營業	5
教育部	短期補習班、私立兒童課後照顧服務中心、私立專科以上學校及私立學術研究機構、私立高級中等以下學校及幼兒園、運動彩券業、海外臺灣學校及大陸地區臺商學校	6
內政部	交友服務業、殯葬服務業、營建類非公務機關、移民業務機構、祭祀團體、政黨及全國性民政財團法人、宗教團體、地政類非公務機關、合作及人民團體類非公務機關、警政類非公務機關	10
勞動部	私立職業訓練機構、人力供應業、人力仲介業	3
衛福部	醫院、精神復健機構、私立長期照顧服務機構、護理機構、社會福利機構、中藥批發零售業、化粧品批發零售業、醫療器材批發零售業、西藥批發零售業、非輻射電子醫療器材設備製造業、食品業、	11
財政部	報關業、保稅倉庫物流中心、記帳士與記帳及報稅代理人、菸酒事業、公益彩券發行機構	5
公平會	多層次傳銷業	1
工程會	工程技術顧問業	1
原能會	游離輻射設備製造業	1
中央銀行	票據交換所	1
農委會	農藥販賣業、農業金融	2
陸委會	大陸委員會指定非公務機關	1
僑委會	僑務委員會指定特定非公務機關	1
合計		**58**

零售業個資安維辦法(1/5)

新法已於11/13正式公告施行，將本辦法名稱修正為「**零售業個人資料檔案安全維護管理辦法**」

中華民國一百十三年十一月十三日經濟部經商字第 11368002820 號令修正發布名稱及全文 22 條；並自發布日施行

（原名稱：綜合商品零售業個人資料檔案安全維護管理辦法；新名稱：零售業個人資料檔案安全維護管理辦法）

- 因應零售業兼營線上通路日益普及，廣泛使用資通系統蒐用消費者個資，為避免發生個資外洩致廣泛衝擊，修正本辦法以加強管理、確保零售業之個資檔案安全維護。
- 新修正辦法已於113/11/13正式公告施行。
- 修正重點：

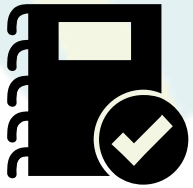
一.修正本辦法適用對象之名稱及定義。（修正條文第三條）

二.業者對於個人資料有加密、備份之必要者或傳輸個人資料時，及以資通系統直接或間接蒐集、處理或利用個人資料時，應實施之資料安全管理措施。（修正條文第九條及第十條）

三.本次修正納入零售業者應完成安全維護計畫訂定之期程。(修正條文第二十一條)

零售業個資安維辦法(2/5)

經濟部依個人資料保護法第27條第3項規定修正訂定「**零售業個人資料檔案安全維護管理辦法**」，
全文共計**22**條，其要點如下：



一. 本辦法之授權依據。（§1）
二. 本辦法之主管機關。（§2）
三. 本辦法之適用對象。（§3）
四. 業者應落實個人資料檔案之安全維護及管理。（§4）
五. 業者應指定專責人員負責個人資料檔案安全維護之相關任務。（§5）
六. 業者應訂定個人資料檔案安全維護計畫。（§6）
七. 業者應界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查及為適當之處置。（§7）
八. 業者蒐集及傳輸個人資料時應符合之規定。（§8）
九. 業者對資料安全管理及人員管理應採取之措施。（§9）
十. 業者應採取之安全措施。（§10）
十一. 業者應對所屬人員施以認知宣導或教育訓練。（§11）
十二. 業者應訂定個人資料侵害事故發生之預防、通報與應變機制、個人資料檔案安全維護稽核機制與訂定使用紀錄、軌跡資料及證據保存之措施。（§12、14、15）
十三. 業者應對保有之個人資料設置必要之安全設備及採取必要之防護措施。（§13）
十四. 業者業務終止後，對其保有之個人資料之處理方法及留存紀錄。（§16）
十五. 業者應檢視所定安全維護計畫之合宜性，並持續改進個人資料保護機制。（§17）
十六. 業者對於當事人行使本法第三條規定之權利所採行之辦理方式。（§18）
十七. 業者委託他人蒐集、處理或利用個人資料時，應對受託者為適當之監督。（§19）
十八. 業者利用個人資料為行銷時應符合之規定，並提供當事人或法定代理人拒絕行銷之機制。（§20）
十九. 業者應完成安全維護計畫訂定之期程及主管機關得派員檢查該計畫。（§21）
二〇. 本辦法之施行日。（§22）

零售業個資安維辦法(3/5)

§3 適用對象

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。

- 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。
- 諸如中藥、西藥、醫療器材、化妝品零售業及多層次傳銷業等排除適用。

修正納入非綜合商品零售業之零售業者，應於新辦法發布施行之日起六個月內**完成安全維護計畫之訂定**

違反後果

業者若未依本辦法採取適當安全維護措施，致個資被竊取、竄改、滅失或洩漏，或未訂定安全維護計畫，經濟部將依個資法第48條第2項處以2～200萬元罰鍰，並令其限期改正，屆期未改正者，按次處15～1500萬元罰鍰。（情節重大者首次即裁罰15～1500萬；§50對代表人得處以與公司同一額度罰鍰之處罰）

零售業適用業別

代碼	行業標準分類	中央目的事業主管機關
471	綜合商品**零售業**	經濟部（商業發展署）
472	食品、飲料及菸草製品**零售業**	經濟部（商業發展署）
473	布疋及服飾品**零售業**	經濟部（商業發展署）
474	家庭器具及用品**零售業**	經濟部（商業發展署）
476	文教、育樂用品**零售業**	經濟部（商業發展署）
481	建材**零售業**	經濟部（商業發展署）
483	資訊及通訊設備**零售業**	~~【電信器材屬管制射頻器材之製造、輸入】：國家通訊傳播委員會~~ **【非屬電信管制射頻器材之通訊設備零售業】**：經濟部（商業發展署） ~~【電信器材屬管制射頻器材之單純零售業】：國家通訊傳播委員會為主管機關~~
484	汽機車及其零配件、用品**零售業**	經濟部（商業發展署）
485	其他專賣**零售業**	經濟部（商業發展署）
486	**零售攤販業**	經濟部（商業發展署）

除綜合零售業，
新增9類零售業

零售業個資安維辦法(4/5)

§9 資料安全及人員管理之措施

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。
五. 傳輸個人資料時，應依不同傳輸方式，採取適當之安全措施。
六. 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。
七. 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。

標準要求：擬定程序以檢驗安全措施及機制的有效性

§10 資通系統安全措施

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：
一. 資通訊系統存有個人資料者，應設定認證機制，其帳號及密碼須符合一定之複雜度。
二. 評估使用情境，採行個人資料之隱碼機制，就個人資料之呈現予以適當且一致性之遮蔽。
三. 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，採取適當之安全機制，定期檢測並因應系統漏洞所造成之威脅。
四. 與網路相聯之資通訊系統存有個人資料者，應隨時更新並執行防毒軟體，及定期執行惡意程式檢測。
五. 建置防火牆、電子郵件過濾機制或其他入侵偵測設備等防止外部網路入侵對策，並定期更新。
六. 資通訊系統存有個人資料者，應設定異常存取資料行為之監控及定期演練因應機制。
七. 處理個人資料之資通訊系統進行測試時，應避免使用真實個人資料；使用真實個人資料者，應訂定使用規範。
八. 處理個人資料之資通訊系統有變更時，應確保其安全性未降低。
九. 定期檢視處理個人資料之資通訊系統，檢查其使用狀況及存取個人資料之情形。

前項各款機制，應定期檢討改善。

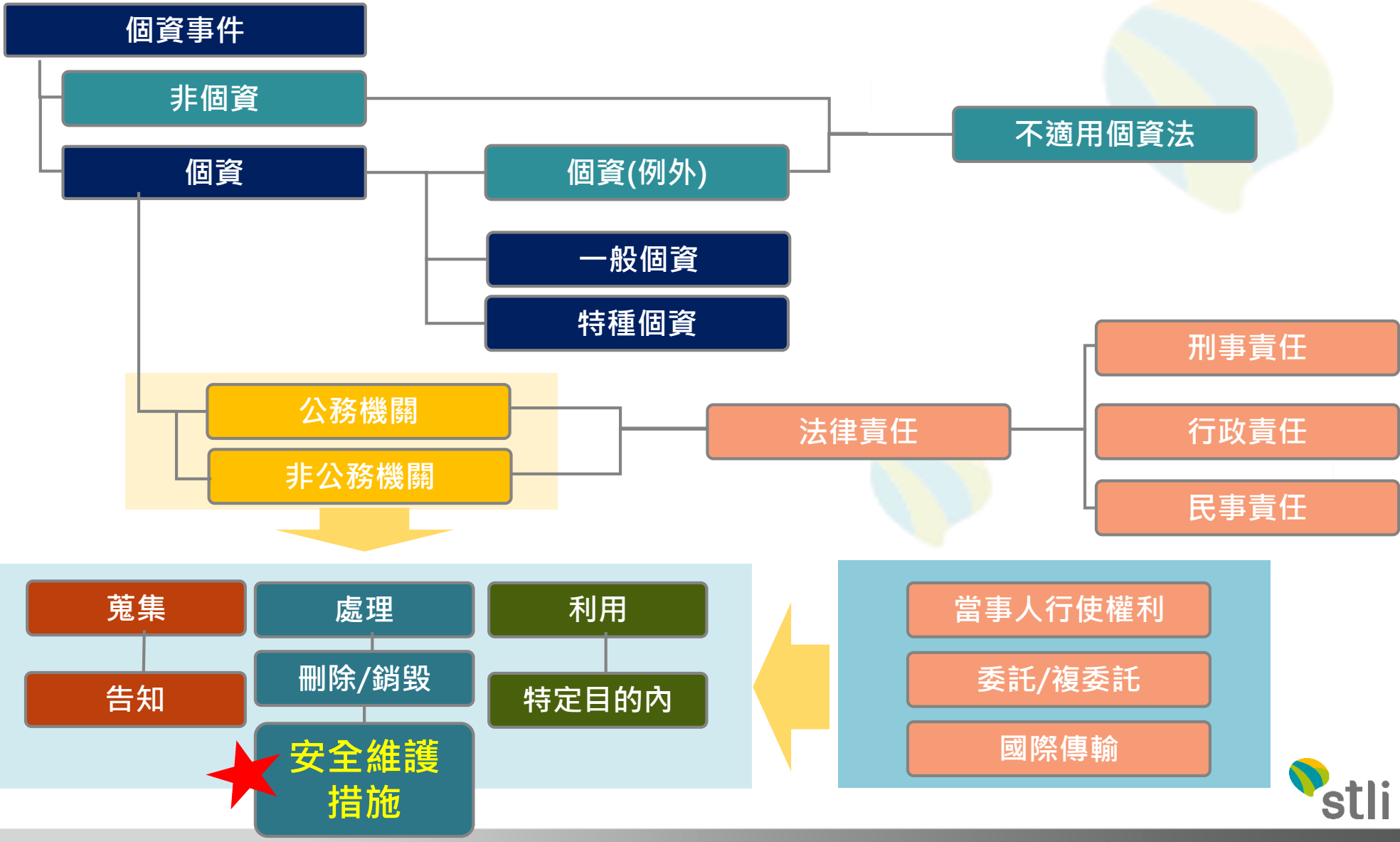
*資安法第3條第1款：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

零售業個資安維辦法(5/5)

作業程序	零售業個資安維辦法	所需文件
人員及資源配置	4、5	**組織架構圖**
清查個人資料檔案	7	**個資盤點表** **作業流程圖**
風險評估作業程序	4	**風險評鑑表**
個人資料蒐集、處理或利用作業程序	7、8	**安全維護計畫** **程序文件書** **表單**(如告知聲明、個資同意書、當事人權利申請書、教育訓練簽到表、刪除銷毀申請單…) **執行紀錄**
受理當事人權利行使之作業程序	18	
事故之預防、通報及應變作業程序	12	
認知宣導及教育訓練作業程序	11	
個資安全管理作業程序	9(資料/人員)、10(系統)、13(設備)	
資料安全稽核作業程序	14	
行銷作業程序	20	
委託監督作業程序	19	
使用紀錄、軌跡資料及證據保存作業程序	15	
業務終止個人資料處理作業程序	16	
持續改善作業程序	17	

02 安全維護計畫（範本）之說明

我國個資法規範架構暨個資流程圖



適當之安全措施

Plan

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

Do

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

Action

11.個人資料安全維護之整體持續改善

Check

9.資料安全稽核機制
10.使用紀錄、軌跡資料及證據保存

個資法施行細則第12條第2項
安全維護事項

零售業個資檔案安全維護計畫(1/15)

(公司名稱)個人資料檔案安全維護計畫

訂定日期：中華民國〇〇〇年〇〇月〇〇日
修訂日期：中華民國〇〇〇年〇〇月〇〇日

版更紀錄，確保版本正確

壹、零售業之組織及規模

一、名稱：_____(零售業)
二、地址：〇〇〇
三、負責人：〇〇〇
四、資本額：新臺幣〇〇〇元(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。

§4

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(2/15)

- 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)

§5

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

§14

(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）

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(3/15)

四、個人資料蒐集、處理及利用之內部管理程序 §8

(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)指定管理人員每〇〇日(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。

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(4/15)

§7

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。

- **確認資料範圍、特定目的**
- **注意頻率規定**

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(5/15)

§10

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.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○○(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.每○○日(週、月、季、年)進行防毒、掃毒等必要之安全措施。

8.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。

9.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。

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，應定期(每年至少1次)進行演練及提出檢討改善報告。

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(6/15)

§9

六、資料安全管理

(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。

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(7/15)

§12

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。

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(8/15)

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

個人資料侵害事故通報與紀錄表		
事業名稱 ＿＿＿＿＿＿＿＿	通報時間：　年　月　日　時　分	
	通報人：　　簽名(蓋章)	
通報機關 ＿＿＿＿＿＿＿＿	職稱：	
	電話：	
	Email：	
	地址：	
事件發生時間		
事件發生種類	□竊取	個資侵害之總筆數(大約) ＿＿＿＿＿＿＿＿
	□洩漏	
	□竄改	
	□毀損	□一般個資＿＿＿＿筆 □特種個資＿＿＿＿筆
	□滅失	
	□其他侵害事故：＿＿	
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時起算七十二小時內通報	□是　□否，理由：	

零售業個資檔案安全維護計畫(9/15)

§10&13

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)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)本公司將每月（或每週、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。

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(10/15)

§14

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。

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(11/15)

§15

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，需每〇〇日(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，非經〇〇(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。

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(12/15)

§16

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。

§17

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。

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(13/15)

§18

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。

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(14/15)

§19

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。

僅供參考，請依實際情形調整

零售業個資檔案安全維護計畫(15/15)

§20

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。

僅供參考，請依實際情形調整

個資保護諮詢專線：02-6631-1577 《個資守護 你我齊行》

Thank you

資安防護實務案例分享

財團法人資訊工業策進會
資安科技研究所

大綱

- 個資外洩事件資安案例分享
- 個資外洩事件主要樣態分析
- 個資法遵要求暨行政檢查常見問題與建議

個資外洩事件資安案例分享

個資外洩事件資安案例分享(1/4)

利用FortiOS SSL-VPN認證堆積緩衝區溢位漏洞，以GUEST身分登入

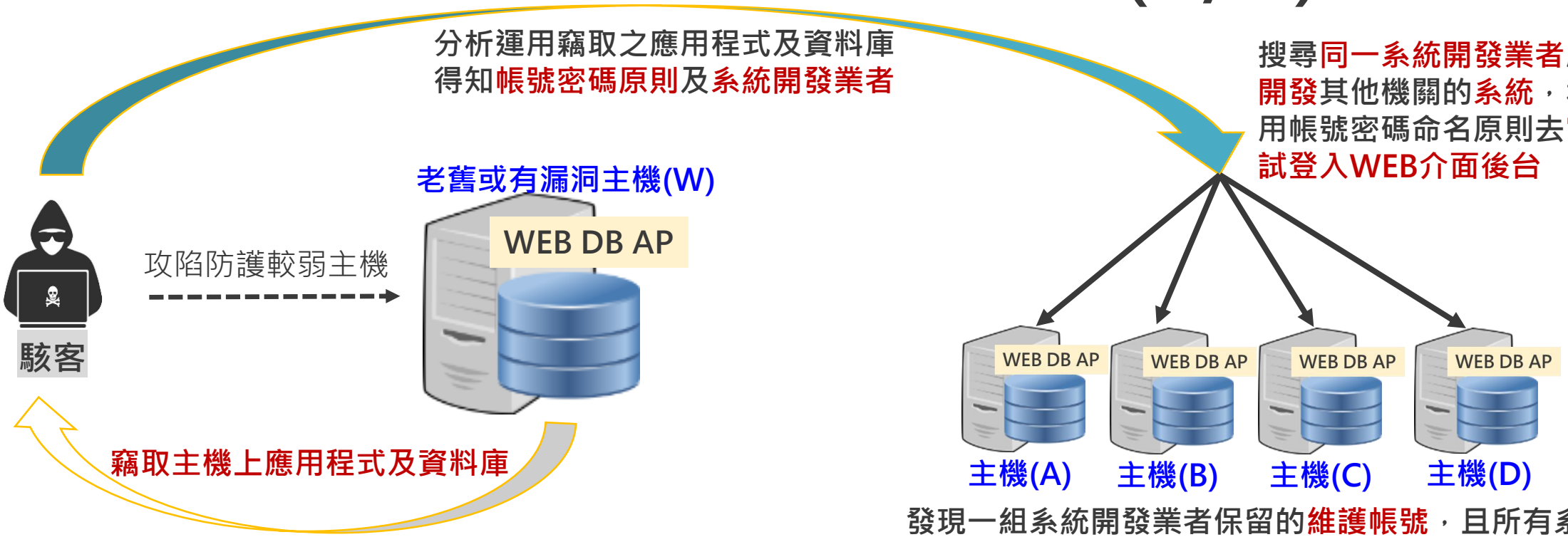
以GUEST身分進行提權，取得最高權限後，執行Anydesk在內部網路進行橫向攻擊，植入Eking Ransomware。

事件發生後只能確定CRM、BPM資料被加密無法使用，但不能確定是否有個資外洩。

提醒事項：

- 重大**弱點修補**
- **限縮VPN** 存取內網**範圍**
- **停用 Anydesk**等類似遠端工具
- 含個資**資料庫加密**
- 重要主機導入**端點監控(EDR)**
- 定期**備份**及災害復原**演練**
- **啟用**個資相關資料庫**軌跡紀錄**

個資外洩事件資安案例分享(2/4)



提醒事項：

- 系統主機弱點務必修補，並增加防護縱深
- 系統開發方式儘量不要將WEB、DB、AP配置在同一個實體主機
- 密碼資料庫、或個資資料庫務必加密或去識別化
- 妥善管理特權帳號，並強制首次登入需更換密碼
- 定期檢視防火牆等防護設備及主機紀錄
- 啟用個資相關資料庫軌跡紀錄，及異常警示
- 系統商應告知業主須有相對應的系統環境防護措施
- 如業主仍不願意更換使用系統商已不更新的系統，應將風險明確告知

個資外洩事件資安案例分享(3/4)

使用者透過搜尋引擎取的內容及檔案

準備匯入的內容及檔案被Google取走後建成索引。

提醒事項：

- 加強人員訓練，含個資之檔案務必加密
- 關閉網站目錄瀏覽
- 勿將準備匯入的機敏資料置於網頁伺服器中
- 利用robots.txt隱藏不希望被收錄的目錄
- 利用noindex設定不希望被建成索引的資料
- 如發現機敏資料被google search建成索引，應立即向google申請刪除

個資外洩事件資安案例分享(4/4)

Hackers

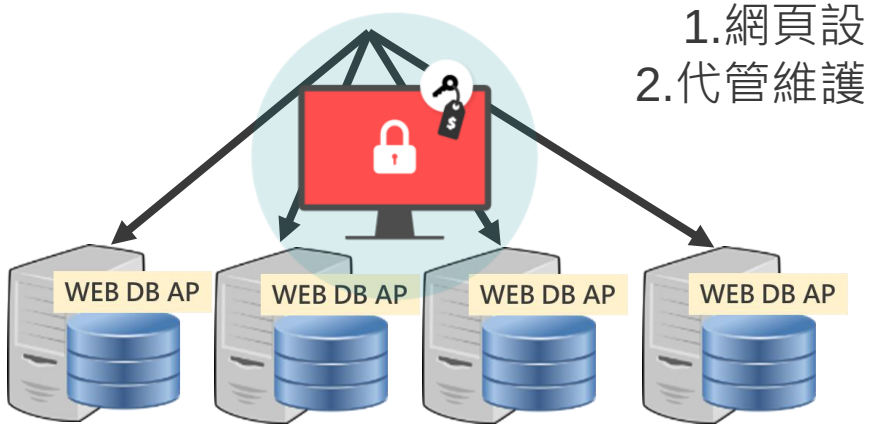
SQL Injection

主機代管商A
提供**網頁設計商B**防毒軟體
做基本資安防護代管

網頁設計商B

業務範疇:
1.網頁設計
2.代管維護主機

利用網頁與資料庫之間的安全漏洞，並透過使用者搜尋引擎取得帳號資訊，以進一步竊取主機上客戶訂房的相關重要個資。



四家旅宿業者遭駭客攻擊導致個資外洩

提醒事項：

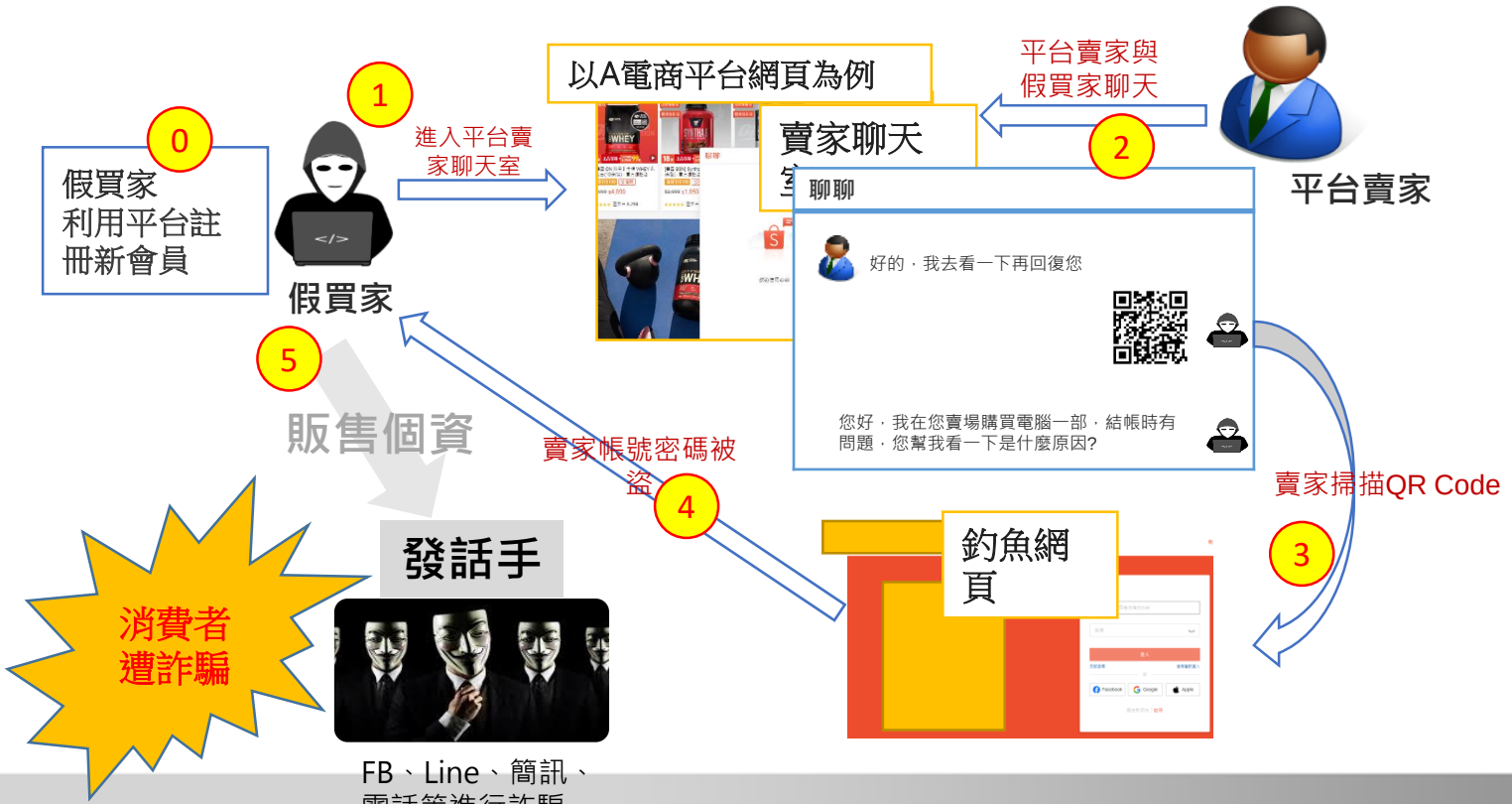
- 定期執行**系統**及**主機弱掃**作業
- 執行**源碼檢測**掃描
- 落實資訊資產盤點，針對**閒置系統進行下線**
- 規範制定**安全程式碼撰寫原則**
- 針對**弱點進行修補及複測**

個資外洩事件主要樣態分析

個資外洩主要樣態分析

個資外洩主要樣態有以下兩種：
型態一：(偏大型電商)C2C電商平台之**假買家利用平台賣家聊天功能騙取賣家**資訊進行詐騙。
型態二：(偏中小型電商)多數**委外系統商**針對電商**帳號管理與防護措施不足**。

型態一



型態二

- **電商以選擇性方式購買服務，忽略資安重要性。**
  - ✓ 建議將**基本資安防護列為合約必備項目**，例如：WAF、監控及定期資安檢測。
- **每家電商發送一組高權限帳號，後續帳號建立，無任何管控。**
  - ✓ 每家電商**帳號發放，需有數量限制**，並定期**清查**及**移除閒置帳號**(例如：每家業者限制3個帳號)。
- **電商帳號登入，有效識別性不足。**
  - ✓ 方式一：電商每個**帳號需綁定裝置設備**，一旦更換設備登入，需有確定本人登入機制(如：以驗證碼方式再次確認)。
  - ✓ 方式二：電商**後台登入**，強制以**2FA方式登入**。

個資法遵要求暨行政檢查常見問題與建議

個資法施行細則第12條第2項涵蓋範圍

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。

行政檢常見未合規結果分析

個人資料安全維護之整體持續改善

- 急於漏洞防堵，缺乏根因分析

事故之預防、通報及應變機制

- 缺少通報及應變處理流程、未向當事人通知個資事件發生

資料安全及人員管理

- 對於個資資料庫的保護及人員(含委外)權限管理不足

資料安全稽核機制

- 稽核制度未落實、缺少專業稽核人員

認知宣導及教育訓練

- 缺乏以個資為主題的教育訓練

界定個人資料之範圍

- 對個資盤點不熟悉或不確實

行政檢查未合規項目建議改善方式(1/2)

個人資料安全維護之整體持續改善

- 經過相關事件調查後(主機、網頁弱點掃描、各項LOG分析、滲透測試)找出漏洞後，應進行**根因分析**完成調查**報告**
- 將調查結果**制定改善預防計畫**，並定期追蹤量測有效性。

事故之預防、通報及應變機制

- 建立**通報應變處理組織及流程**、知悉個資外洩事件後須於72小時內通報主管機關
- 當事人**通知**個資事件發生之**內容**(被侵害事實、已採取之因應措施、後續處置方式)
- 如無法明確知道外洩個資之範圍，應通知**訂單區間內全部會員**

資料安全管理及人員管理

- 未有個資資料庫**資料庫隱碼**、存取**軌跡紀錄**
- 未針對**委外**進行**監督管理**
- 管理者 (特權帳號)身分認證不夠嚴謹，**金鑰保管**方式不正確

行政檢查未合規項目建議改善方式(2/2)

界定個人資料之範圍

- 未能完整盤點**跨分公司**、**跨部門**個資資料(未指定高權限人員執行)
- 未將明確釐清個資是否涉及**境外傳輸**(雲端資料所在地)
- **未確實**進行**風險評估**及風險處理並制定因應對策

資料安全稽核機制

- **未落實內部稽核**，內部無相關稽核專業人才
- 委由外部資安顧問公司稽核，但**未**對稽核結果進行**改善追蹤**
- 將委由資安公司進行弱點掃描、滲透測試、資安事件調查之報告當作稽核報告

認知宣導及教育訓練

- 將新人教育、勞工安全教育、資安認知等課程視為個資安全教育訓練
- 參與教育訓練之人員不夠全面、針對訓練**未有評量機制**
- 個資**主要執行人員**應接受**專業**課程**訓練**

Thank you

行政檢查常見狀況暨個資最佳實務

零售業個資保護的挑戰與解決方案

鼎昊法律事務所

2024/11

蕭崴仁 律師

DingHao

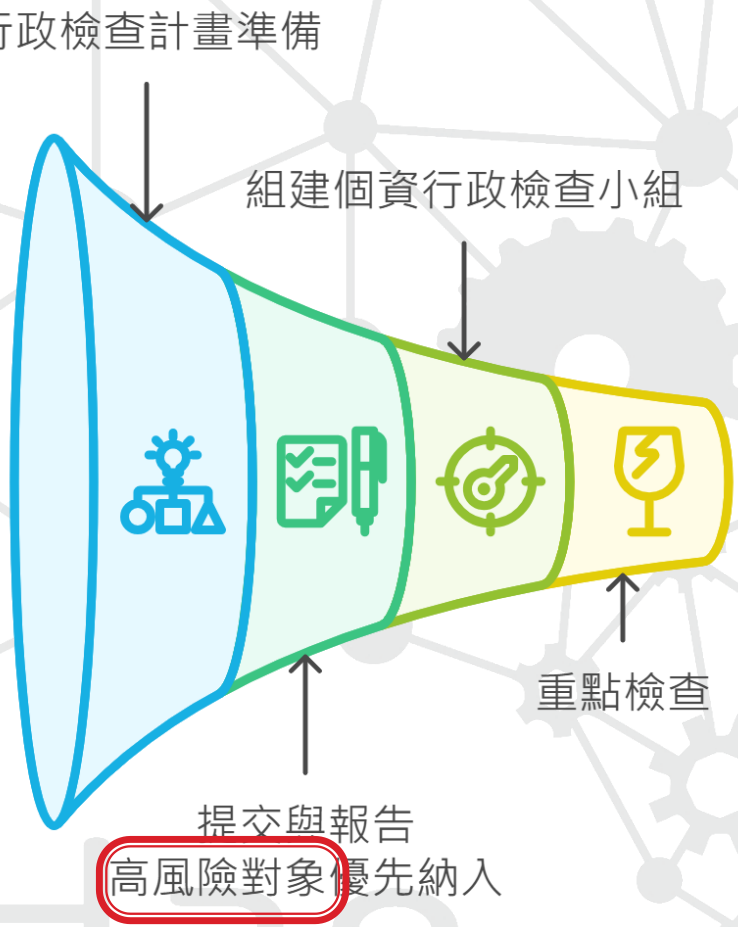
蕭崴仁律師

現職	鼎昊法律事務所 律師
學歷	臺北大學法律系碩士 臺灣大學法律系財經法學組學士
經歷	資訊工業策進會科技法律研究所 法律研究員 長江大方國際法律事務所 律師
專業證照	中華民國律師高考及格 ISO 27001主導稽核員考試及格 RICHO Privacy Mark Auditor Course 台灣智慧財產管理規範（TIPS）執行體系自評員 臺灣個人資料保護與管理制度（TPIPAS）個人資料驗證師/內評師/管理師
專案經歷	資資通安全法律案例彙編(計畫主持人/財團法人資訊工業策進會委託) 健康數據合規性查訪(計畫主持人/財團法人資訊工業策進會委託) 電子商務個人資料管理制度推動計畫（研究員/經濟部商業司委託） 資通訊安全產業推動計畫（研究員/經濟部工業局委託） 電子商務個人資料管理制度建置計畫（研究員/經濟部商業司委託） 三貝德數位文創、嘉佳星多媒體、天下雜誌集團、紅樓創新技術、橘熊科技、統一速達等多間公司個資管理制度建置專案 計畫主持人 臺灣個人資料保護與管理制度（TPIPAS）各級專業人員課程 資深講師 臺灣個人資料保護與管理制度（TPIPAS）驗證暨特定範圍檢視 主導驗證員 經濟部商業司網路購物產業價值升級與環境建構計畫資安訪視小組 法遵檢視員 消費者文教基金會義務律師團委員 世新大學兼任講師
著作	《科技法律透析月刊》編輯（103年至105年） 《個資保護1.0》編輯 《個資解碼：一本個資保護工作者必備的工具書》編輯 《資通安全法規彙編》執行編輯

什麼時候進行行政檢查？

- 個人資料保護法第22條第1項：「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。」

行政檢查的規劃與評估



行政檢查的規劃與評估

國際頻率

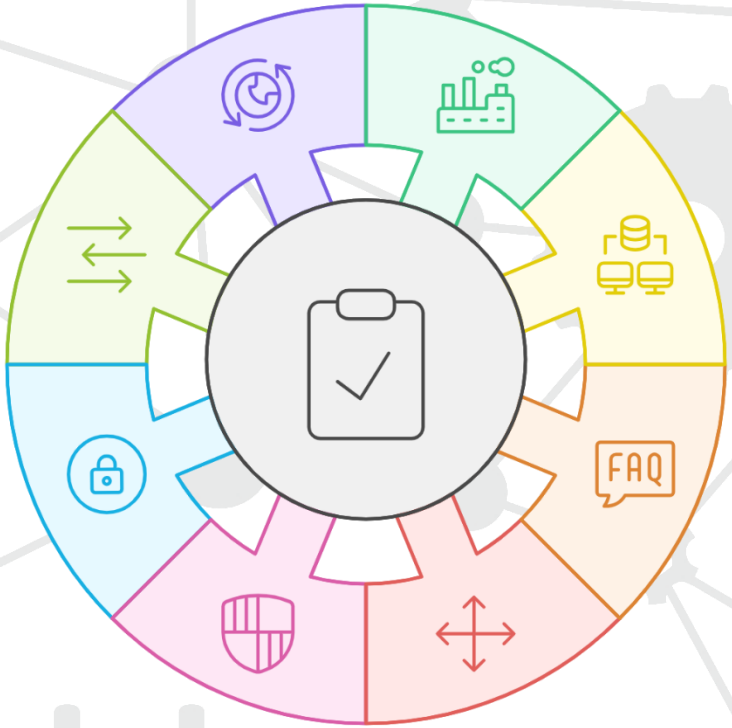
考慮國際資料傳輸的頻率。

組織規模

評估組織的規模和能力。

傳輸方法

檢查用於資料傳輸的工具和方法。



資料量

考慮所持有的個人資料的數量和性質。

存取環境

檢視資料存取環境的安全性。

密切程度

評估組織與公眾的日常生活關係。

個人傷害

考量資料外洩對個人的潛在傷害。

影響範圍

分析資料外洩的潛在廣泛影響。

檢查什麼？

- 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。」
- 個人資料保護法施行細則第12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。」

常見狀況－計畫未完成

為防止消費者個資外洩，經濟部繼要求4,000家大型綜合零售業（如超商、超市、百貨、量販店等）訂定個人資料安全維護計畫後，現再**擴大適用範圍至專責特定商品的零售業**，包括連鎖服飾、文具書店、鞋類、電器、資訊、家庭用品以及菸酒等資本額千萬元以上之零售業，估計將有3萬多家業者受到影響，須於期限內訂定個資安全維護計畫。

經濟部預告「零售業個人資料檔案安全維護管理辦法」修正草案，擴大適用範圍至專責特定商品的零售業，以確保消費者個資安全。該辦法將更名為「零售業個人資料檔案安全維護管理辦法」，將在修正草案公告實施後，同樣給予六個月緩衝期，須訂定個人資料檔案安全維護計畫。

商發署官員解釋，修正案將擴大到布疋服飾、家庭器具及用品、文教育樂用品、資訊及通訊設備、家電用品、汽機車零組件用品、菸酒專賣店等資本額千萬元以上的零售業，包括誠品書店、連鎖服飾店如NET、全家福等鞋店、燦坤、全國電子等，約有3萬多家業者受到影響。經濟部主管實體店的零售業，而純電商由數位部主管。

經濟部表示，將會**主動查核**，若業者未能提出個資安全維護計畫或違反相關規定，依「個資法」第48條，將處以2萬元至200萬元罰鍰，限期未改善或情節重大者，處以15萬元至1,500萬元罰鍰，並按次處罰。

防個資外洩！經部預告第二波零售業須訂個資安全計畫 共3萬多家「這些業者」受影響｜產業熱點｜產業｜經濟日報

常見狀況-未充分告知


訂閱/取消電子報
請輸入您的Email
訂閱
驗證碼：
請輸入驗證碼(不分英文大小寫)
看不清楚
按此重新產生»
送出
登入使用進階功能
隱私權政策
Copyright © 2024

常見狀況-未界定個人資料與風險評估

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

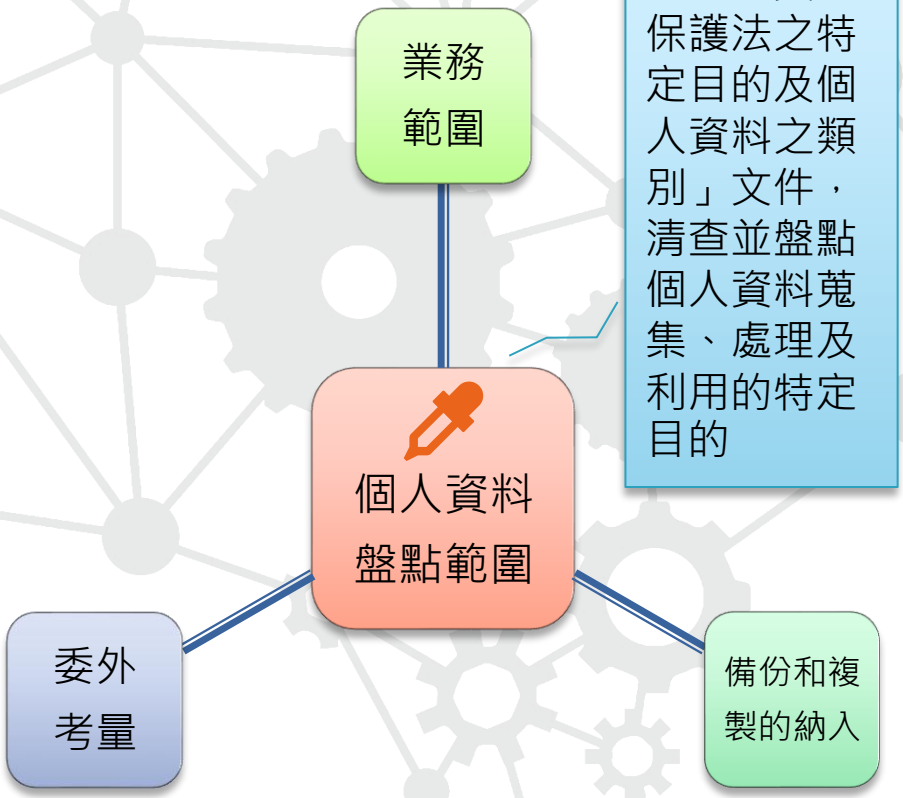
資料流							
組織身分	資料來源	組織內部提供者	組織內部接收者	資料處理者	第三方	國際傳輸	組織身分補充欄位

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



參考法務部所公布的「個人資料保護法之特定目的及個人資料之類別」文件，清查並盤點個人資料蒐集、處理及利用的特定目的

常見狀況 - 資料安全措施不足

01
特種個資

02
法定情形

03
特定目的

07
行銷

04
告知義務

05
行銷

06
個資委外

08
資料正確性

09
特定目的消失

常見狀況 – 欠缺稽核機制

瑞典大型保險公司 Folksam 於2020年發生一起資料外洩事件，影響約一百萬名瑞典客戶。Folksam 在一次**內部稽核**中發現，客戶的個人資料被不當分享給多家科技巨頭，包括 Facebook、Google、Microsoft、LinkedIn 和 Adobe。根據 Folksam 市場與銷售主管 Jens Wikström 表示，此次資料分享是為了分析登入 Folksam 網站的客戶行為，以便向客戶提供量身定制的優惠，但不幸的是分享方式不符合規範。Folksam 已立即停止資料分享，並要求各科技公司刪除已收到的資料。目前 Folksam 表示，尚無證據顯示這些資料被第三方不當使用。Folksam 同時展開相關流程改進，確保未來不再發生類似情況。

Folksam data breach leaks info of 1M Swedes to Google, Facebook, more

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？ 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	□符合 □不符合 □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 「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。

最佳實務－依法進行

個資法規 – 個資保護專區 – 資訊園地 – 經濟部商業發展署全球資訊網

結語與QA

Goodness is the only investment that never fails. – Henry David Thoreau

個資資安保護與管理制度-蕭崴仁律師

鼎昊法律事務所
DingHao Attorneys-at-Law

台北市中山區南京東路二段137號5樓

02 2518 2363

wjhsiao@dinghaomcc.com

個資施行
資通項目重點查驗
項目說明與建議

許哲銓老師 (東吳大學資管系)

為何零售業的個人資料安全如此重要性

- 消費者信任： 個人資料安全是建立消費者信任。
  - 消費者的消費足跡與軌跡的保護，消費者對於個資隱私的權利聲明。
- 法律規範： 各國政府紛紛制定了嚴格的個人資料保護法規，要求企業必須採取適當措施保護消費者個人資料。
  - 經濟部　綜合商品零售業個人資料檔案安全維護管理辦法
- 商業風險： 個人資料洩露事件可能導致企業聲譽受損、客戶流失、以及巨額的賠償費用，對企業的長期發展造成重大影響。

零售業常見的個人資料安全風險

- 防護上的困境與限制：
  - 客戶使用會員系統app，揭露當事人的姓名與聯絡資訊
    - 發生情境：當使用者的帳密遭受竊取，透過會管名單的外洩，產生其他業者的資料庫憑證攻擊，衍生帶狀性的財損。
  - 公眾人物的消費足跡，遭受有員工內部揭露
    - 發生情境：知名人士前往某特定店家消費，購物商品清冊遭店員洩漏。
  - 連鎖零售商的POS系統遭到黑客攻擊，數以萬計的顧客信用卡資訊被竊取。
    - 發生情境：對所有會員資料進行加密，即使資料被非法訪問也無法被解讀。

綜合商品零售業個人資料處理

盤點所有可能碰觸到個人資料的部門、權限以及調查其所需個資的特定目的

- 綜合商品在零售業中，個人資料所需注意的範圍中，包含有
  - 個人資料外洩： 消費者個人資訊 (如姓名、電話、地址、消費紀錄等) 未經授權地被洩露出去，可能導致詐騙、身份盜用等問題。
  - 非法使用個人資料： 企業將消費者個人資料用於未經授權的目的，例如將消費紀錄用於行銷而不經消費者同意。
  - 資料洩漏： 企業的內部系統或設備發生故障，導致個人資料被意外洩露。
  - 未妥善保護個人資料： 企業未採取足夠的安全措施，導致個人資料容易受到駭客攻擊或其他安全威脅。
- 因此個人資料因不當處理或未盡有效保護作業，將影響消費者因應個人資料外洩產生不當的利用衍生出相關法律問題。

綜合商品零售業個人資料檔案安全維護管理辦法
第六條第二款、個人資料之範圍。

產業管理制度中可進行積極管理作為

資訊安全防護

確保相關電腦機房的安全管理策略

1. ISO 27001
2. 透過框架來建立、實施、維護和持續改進資訊安全管理。
3. 住要重點用於資訊安全風險管理，包括保密性、完整性和可用性。

雲平台範圍　ISO 27017

針對雲計算環境中的資訊安全管理，適用於提供雲服務的數據中心。 客戶虛擬環境的保護和分離，虛擬機器 (Virtual Machines) 配置，監控雲端活動

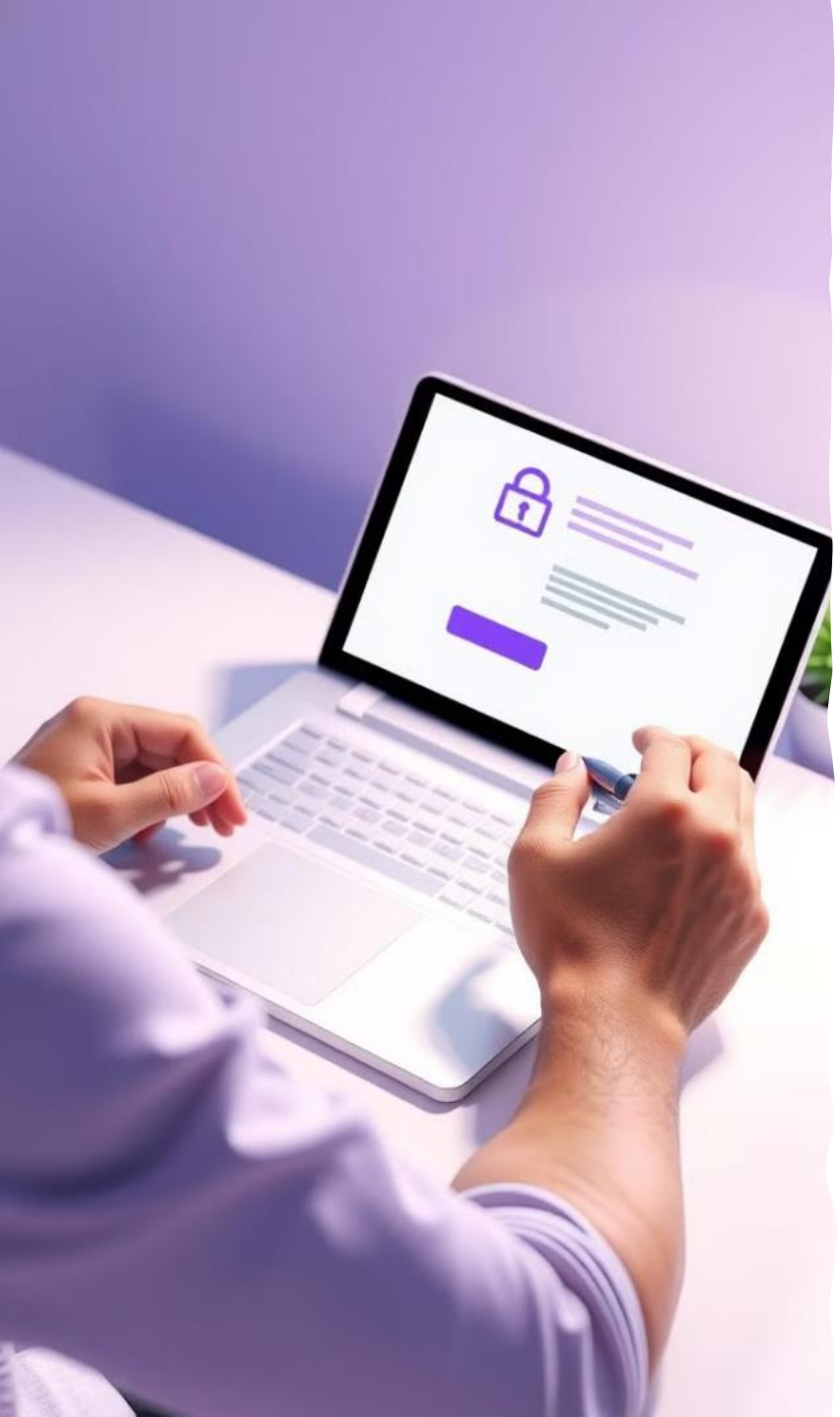
個資安全防護

考量個人資料存放項目，落地的數據資訊 (對於雲端服務上個人資料的蒐集、處裡、利用或傳輸等，已經受到適當有效的安全保護)

ISO 27018

交易資料範圍

PCI DSS（Payment Card Industry Data Security Standard）是針對處理、存儲或傳輸支付卡數據的組織的安全標準。



蒐集處理利用之內部管理程序

綜合商品零售業個人資料檔案安全維護管理辦法
第六條第一款、個人資料蒐集、處理及利用之內部管理程序。

- 系統涉及當事人蒐集個人資料時，是否有相關當事人同意紀錄。
- 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，建議提供相關當事人當事人通報勾選事件紀錄。
- 當事人表示拒絕行銷後，立即停止利用其個人資料行銷，並於系統中自動化紀錄當事人宣告紀錄與提出如何排除行銷規劃作業程序。
- 相關因應法規當事人權益所提出個人資料刪除或銷毀其個人資料，並留存相關紀錄。

個人資料之風險評估及管理機制

- 資通安全技術作業實施辦法
  - 風險評估
    - 個人資料於不同營業單位電腦下載或外部網路入侵而外洩風控辦法
    - 個人資料於公司與分公司之間，營業處所之間傳輸、與相關業者間傳輸
  - 管理機制
    - 公司涉及個資操作人員帳號密碼管理機制
    - 個人資料揭露公司所屬人員權限與閱覽紀錄
    - 檔案資料交換加密傳輸機制

綜合商品零售業個人資料檔案安全維護管理辦法
第六條第三款、資料安全管理及人員管理。

事故管理與規範設計)

綜合商品零售業個人資料檔案安全維護管理辦法
第六條第五款、事故之預防、通報及應變機制

事故通報應變

基於安全管理，當發生個人資料因故疑似外洩時，公司可依據演練作業程序，滿足法規72小時內通報作業。

1

規劃通報應變程序

提出公司實施作業流程，未曾發生業者可建立參考指引

2

事故調查作業

提出公司將採行的事故發生後，事件調查流程，包含如何封存相關事件紀錄，並規劃事件調查處理程序，提出可能稽核的範圍說明

3

如何匡列可能遭受侵害範圍，並適度通報當事人，並確保當事人權益。

事故發生後的執行策略，包含調查過程中的安全管理提升機制為何？

4

設備安全管理

綜合商品零售業個人資料檔案安全維護管理辦法
第六條第六款、設備安全管理 第七款資料安全稽核機制
第八款 使用紀錄、軌跡資料及證據保存。

1

電腦安全管理

公司所需利用存放、查詢或列印輸出個資電腦是否完成相關安全管理作業。電腦設備的密碼保護機制與管理方式。人員離開電腦前是否自動退出相關個人資料查詢系統 (**系統可計時登出**)。

2

網路安全

員工電腦是否納入防火牆管理範圍。員工使用電腦防毒軟體管理作業程序。非公司員工是否可操作相關個人資料查詢範圍系統。

3

資料儲存與銷毀

相關伺服器儲存作業是否完整留存紀錄。存放媒體資料個資銷毀作業。配置專責人員檢核相關紙本與硬體電腦存放裝置銷毀作業紀錄。

紀錄保存

1

個資管理紀錄

是否保存個資（含紙本及數位檔案）管理紀錄（如存取及利用紀錄、調閱紀錄、軌跡資料、銷毀紀錄？）

2

調閱查找紀錄

建立所有個資調閱查找的事件紀錄表單

3

稽核檢查

稽核同仁因定期紀錄檢核事件紀錄表確認是否異常(進行稽核檢查紀錄)

4

電子軌跡保存

電子軌跡證據保存。是否建立自動化電子軌跡保存作業

資料安全與人員管理

綜合商品零售業個人資料檔案安全維護管理辦法
第六條第七款、資料安全稽核機制。 第十條安全措施

個人資料是否進行去識別化作業？

- 應提出資料庫環境如何進行去識別化作業 (加密方式、遮蔽方式等)
- 可參考數發部所推行個資隱碼保護指引規範

資料存取控制措

- 相關管理人員是否留存所有個資範圍查詢紀錄
- 相關管理人員是否可批次查詢多筆個人資料
- 管理人員進行資料批次匯出時是否留存相關紀錄
- 因業務需求所進行資料檔案交換時是否完成加密作業
- 備份資料庫檔案的加密方式為何？
- 防火牆規劃與公司員工電腦安全存取策略以及稽核機制
- 機房安全管理稽核機制 (雲端需提出金鑰取用的申請與使用紀錄流程)

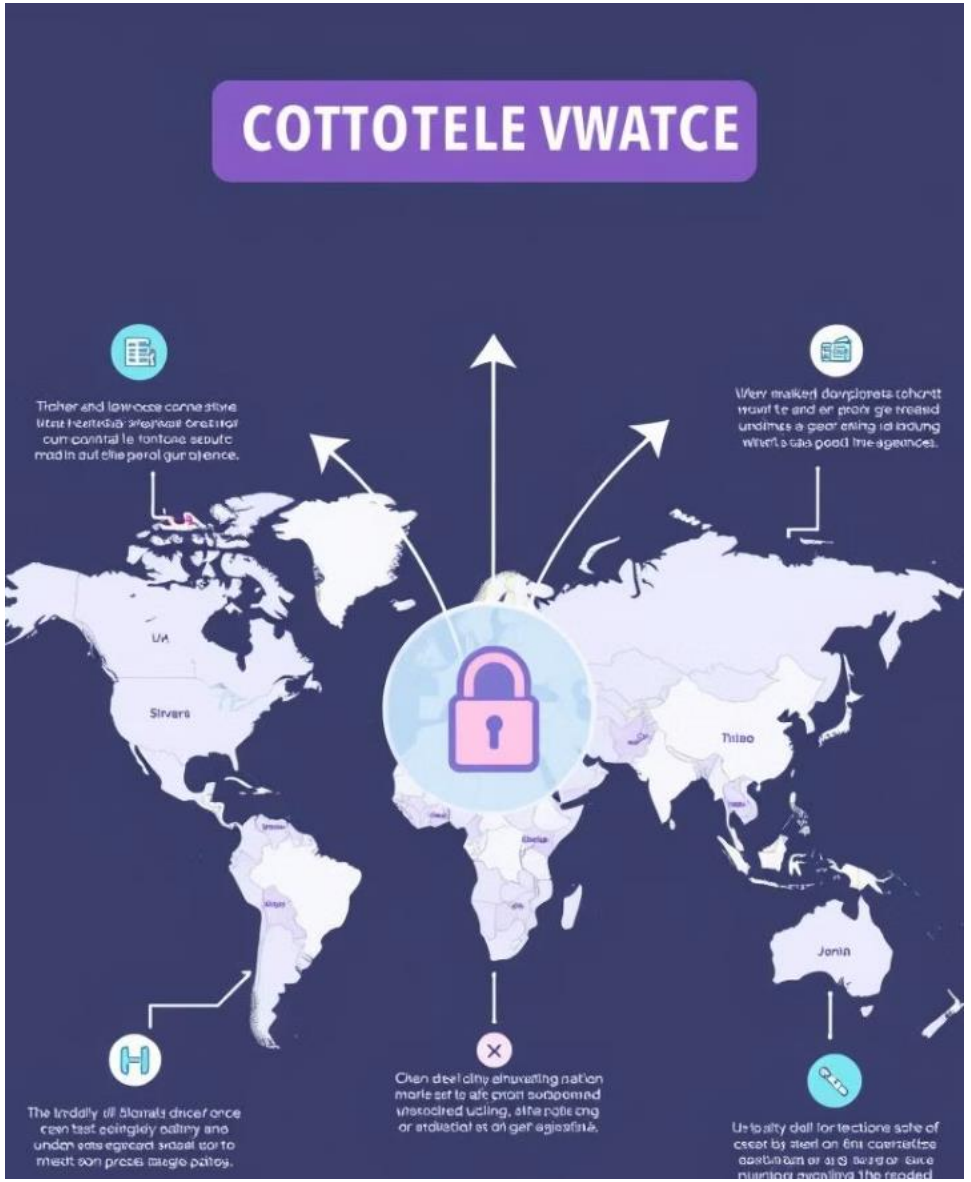
資料安全與人員管理

- 遠端存取控管措施
  - 是否允許外部連線作業
  - 合作協力廠商連線作業程序
  - 是否保存遠端存取事件紀錄
  - 機敏資料是否允許遠端存取
- 電腦、相關設備或系統有定期檢測並因應系統漏洞所造成之威脅
  - **定期**針對內部系統進行積極掃描檢測
  - 建立掃描檢測內稽紀錄表

個資國際傳輸範圍

綜合商品零售業個人資料檔案安全維護管理辦法
第八條第三款

- 相關伺服器所在地未存放於國內機房，應提出公司系統服務架構進行審核確認。
- 由於網路伺服器現今因應資安管理，包含伺服器未置隱藏等所涉及的架構多元性，審查重點說明如下：
  - 系統所存放個人資料所在地範圍界定
  - 備份檔案系統內含個人資料資料庫存放所在地
  - 備援系統所在地
- 若公司系統設計需求，有存放於國外需求，包含國外雲端系統平台，需告知當事人其個人資料所欲國際傳輸之區域，並對傳輸資料**進行監督，提出監督管理機制**。



保存個人資料的重要提醒

- 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。
  - 特別需要注意的項目：個人資料不宜永久保存，應設定個人資料之保存期限，並於期限屆滿或利用目的消失後予以刪除、銷毀或其他處置。
- 請留意於蒐集個人資料前，應取得當事人同意，並明確告知。
  - 個人資料保護法 第 8 條第1 項規定之所有事項。
- 境外傳輸告知事項
  - 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，以及公司是否配置適當的安全控制管理機制。

委託作業

- 個資法保護細則第八條說明，請注意與委託服務機構合作時
  - 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。(業者如何實施監督)
  - 監督執行政策為何
  - 是否將相關規範納入合約書明定權利與義務

目前常見以雲端系統AWS 的保護建議

網路層

- AWS Shield：提供詳細的 DDoS 攻擊報告和事件紀錄
- AWS WAF (Web Application Firewall)：過濾 HTTP/HTTPS 請求日誌儲存
- Amazon GuardDuty：監控是否有惡意活動和異常行為建立事件分析紀錄
- Amazon cloudfront 透過流量加密和存取控制來改善安全性。(CDN)

虛擬主機層

- Amazon CloudWatch：CloudWatch 自動收集和記錄 EC2 實例、RDS 資料庫、ECS 任務等的性能指標和日誌

應用層

- AWS CloudTrail：記錄所有對 AWS 資源的 API 調用，包括用戶、IP 地址、請求和回應等詳細資訊，可運用 cloudwatch logs進行後續分析。
- AWS Config：結合 cloudwatch進行資源配置監控

以雲端系統AWS為例

1

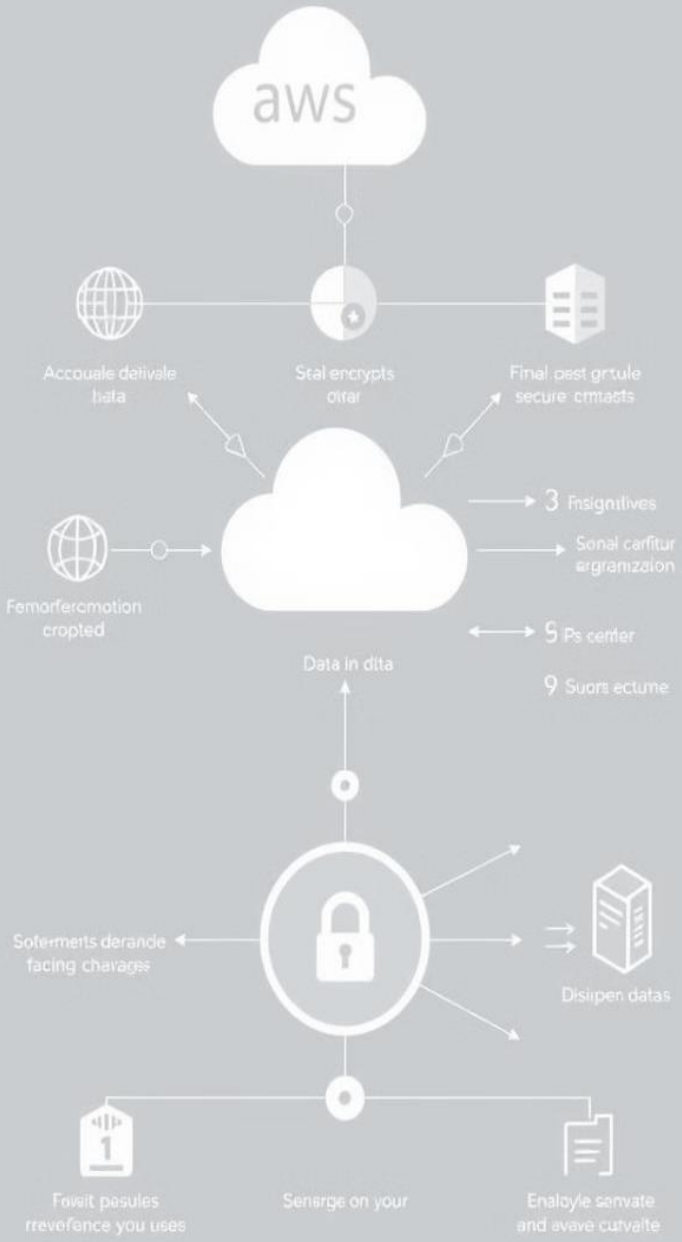
數據層

Amazon RDS / Amazon Aurora：可建立資料庫日誌，發送至cloudwatch 或是s3進行未來分析與監控。Amazon S3: 使用 S3 的伺服器端加密（SSE）功能來加密存儲在 S3 中的個人資料SSE-S3、SSE-KMS 和 SSE-C。AWS KMS (Key Management Service)：建立加密金鑰調用紀錄，並結合 CloudTrail 進行後續監測。

2

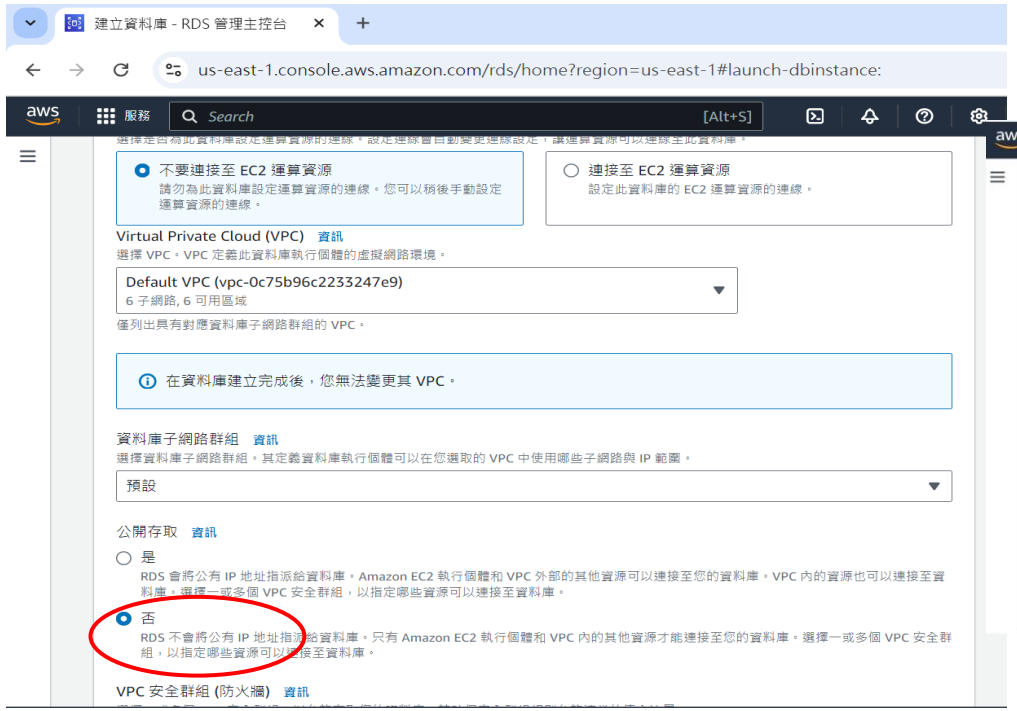
傳輸加密

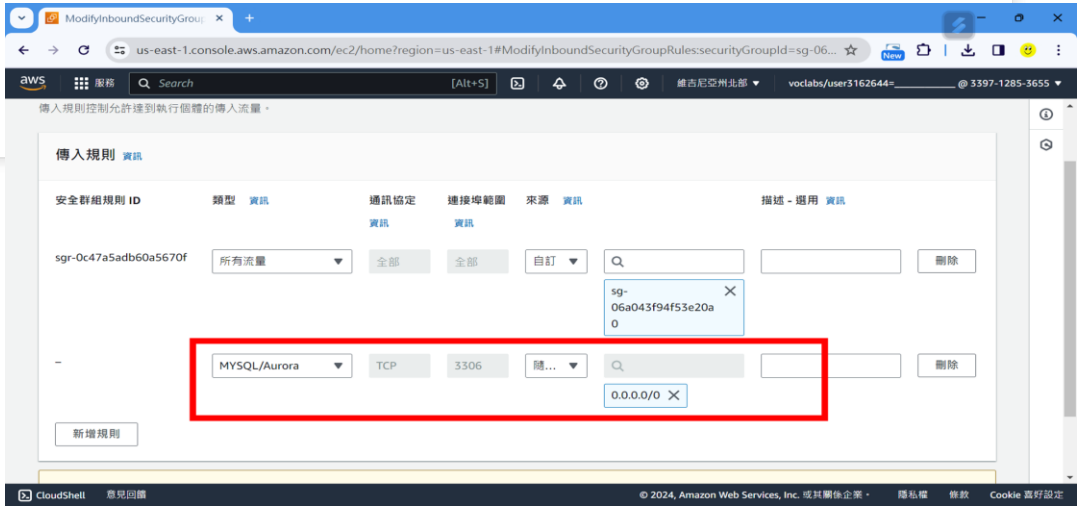
啟動SSL/TLS，確保所有傳輸中的資料使用 SSL/TLS 進行加密。AWS Certificate Manager (ACM): 用於管理和自動續訂 SSL/TLS 證書，以保護網站和應用程序的流量。



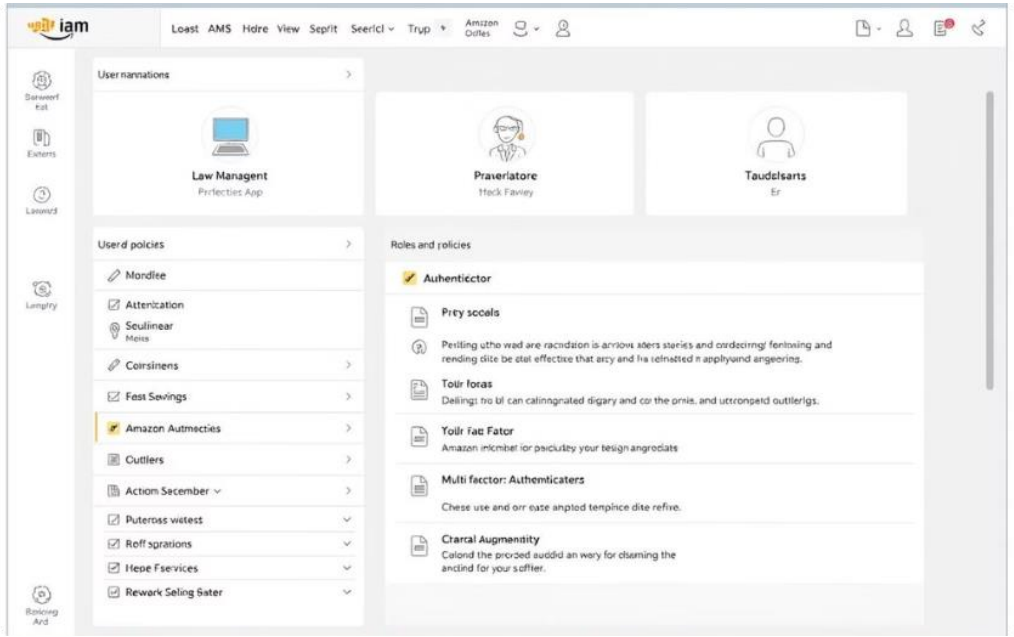
近年會常見的雲端問題

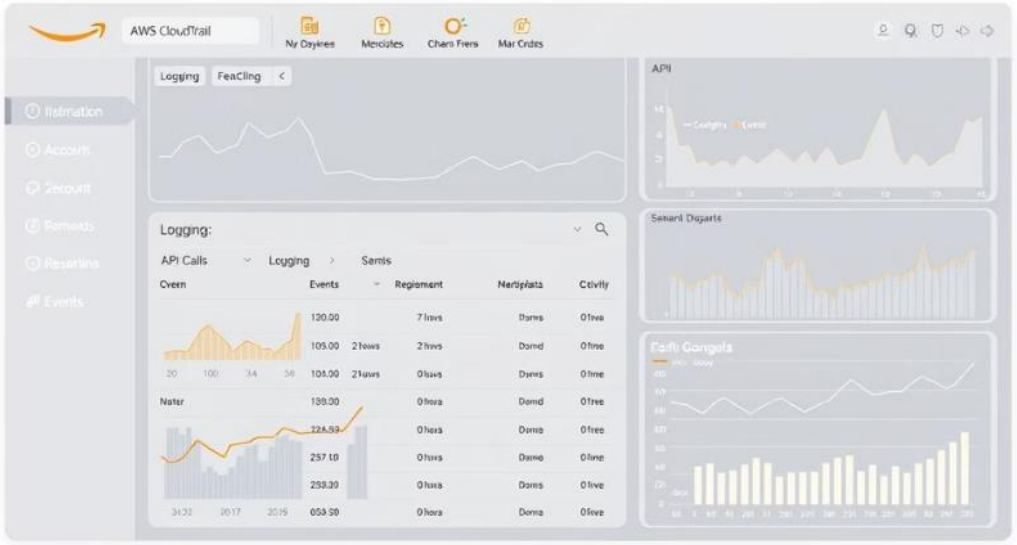
- 安全設定認知不足





善用工具





存取控制

AWS IAM (Identity and Access Management)：建立完整的角色和政策，使用 IAM 角色和政策來控制對 AWS 資源（如 EC2 實例、RDS 資料庫）的存取權限，同時建立MFA (Multi-Factor Authentication)強制執行多重身份驗證來增強帳戶安全性。

數據監控和記錄

AWS CloudTrail：自動記錄對 AWS 資源的 API 調用，使用紀錄。Amazon CloudWatch：日誌和指標，取得收集和分析系統指標和日誌，檢測異常行為和潛在的安全威脅。

謝謝大家的聆聽

有任何問題或建議，歡迎與我聯繫

東吳大學 資訊管理學系 許哲銓 副教授　tchsu@scu.edu.tw

零售業個人資料檔案安全維護管理辦法

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　本辦法所稱零售業（以下簡稱業者），指從事實體店面，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。

第四條　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　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　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　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。

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　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。

業者於傳輸個人資料時，應採取避免洩漏之必要保護措施。

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　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。

五、傳輸個人資料時，應依不同傳輸方式，採取適當之安全措施。

六、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。

七、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。

第十條　業者以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：

一、資通訊系統存有個人資料者，應設定認證機制，其帳號及密碼須符合一定之複雜度。

二、評估使用情境，採行個人資料之隱碼機制，就個人資料之呈現予以適當且一致性之遮蔽。

三、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，採取適當之安全機

制，定期檢測並因應系統漏洞所造成之威脅。

四、與網路相聯之資通訊系統存有個人資料者，應隨時更新並執行防毒軟體，及定期執行惡意程式檢測。

五、建置防火牆、電子郵件過濾機制或其他入侵偵測設備等防止外部網路入侵對策，並定期更新。

六、資通訊系統存有個人資料者，應設定異常存取資料行為之監控及定期演練因應機制。

七、處理個人資料之資通訊系統進行測試時，應避免使用真實個人資料；使用真實個人資料者，應訂定使用規範。

八、處理個人資料之資通訊系統有變更時，應確保其安全性未降低。

九、定期檢視處理個人資料之資通訊系統，檢查其使用狀況及存取個人資料之情形。

前項各款機制，應定期檢討改善。

第十一條　業者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　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。

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。

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　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　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。

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。

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　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。

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　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　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　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。

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　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　業者依本法第二十條第一項規定利用個人資料為行銷時，應明確告知當事人公司登記名稱及個人資料來源。

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　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。

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。

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、零售業之組織及規模

一、名稱：_____（**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。）

五、經營事業：○○○（註：實體店面方式零售/網際網路方式零售/其他事業。）

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)

(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(○○二)、全民健康保險、勞工保險、國民年金保險或其他社會保險(○三一）、消費者、客戶管理與服務(○九○)等。)

(三)指定管理人員每○○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.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○○(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. 每○○日(週、月、季、年)進行防毒、掃毒等必要之安全措施。

8.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。

9.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。

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)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)本公司將每月（或每週、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。

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記錄表

個人資料侵害事故通報及記錄表

<table>
<tr><td colspan="3">個人資料侵害事故通報及記錄表</td></tr>
<tr><td rowspan="6">事業名稱
_____
通報機關
_____</td><td colspan="2">通報時間：　年　月　日　時　分</td></tr>
<tr><td colspan="2">通報人：　　簽名（蓋章）</td></tr>
<tr><td colspan="2">職稱：</td></tr>
<tr><td colspan="2">電話：</td></tr>
<tr><td colspan="2">Email：</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）
_____</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
□特種個資</td></tr>
<tr><td>□滅失</td></tr>
<tr><td>□其他侵害事故：__</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個資侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個資外洩時起算七十二小時內通報</td><td colspan="2">□是 □否，理由：</td></tr>
</table>

經濟部（商業發展署）通報窗口

電子郵件：

聯絡電話：