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

商業服務業
個人資料保護手冊

PERSONAL DATA PROTECTION MANUAL FOR
BUSINESS SERVICES INDUSTRY

商業服務業
個人資料保護手冊

PERSONAL DATA PROTECTION MANUAL FOR
BUSINESS SERVICES INDUSTRY

CONTENTS
目錄

壹、前言

近年來國內外屢傳企業個資外洩事件，為提升交易安全，許多業者已開始投入建置個資管理制度的行列，對內部所持有個資之蒐集、處理或利用進行保護與管理，強化個資保護與資安管理已是不可忽視的需求。另立法院已於112年5月16日三讀通過個人資料保護法修正案，促使非公務機關投入人力、技術及成本，落實保護民眾個人資料之責任。

為強化業者落實對個人資料之保護，經濟部於112年8月1日發布施行「綜合商品零售業個人資料檔案安全維護管理辦法」，並於113年11月13日發布修正為「零售業個人資料檔案安全維護管理辦法」，新增納入之一般零售業者應於辦法發布施行之日起六個月內（113年5月12日前）完成安全維護計畫之訂定。

為避免業者執行業務時，因不諳法律之執行內容，而承擔相關法律責任，特編印《商業服務業個人資料保護手冊》（以下簡稱本手冊），針對商業服務業提供個人資料保護與資安防護的實務管理參考指引。基此，本手冊分為兩大部分，**第1部分「個人資料保護與資訊安全」**包含8篇文章，介紹個人資料保護法的合規要求及常見的資安防護重點，以幫助業者避免違法風險或個資外洩事件；**第2部分「個資手冊問與答QA」**，彙整業者曾諮詢過的法規疑義或資安防護問題，提供20題常見問題的解答，幫助業者解惑。本手冊透過案例分析與深入淺出的說明，期望能使讀者更清楚掌握個資保護管理的實務重點，從而有效落實個人資料保護與資安防護的要求。

貳、手冊指引

本手冊適用之對象為商業服務業，即以零售、批發為主要經營模式的業者，但排除其他目的事業主管機關主管的零售、批發等業別（如屬電信管制射頻器材零售由NCC主管）。本手冊依據個資法、個資法施行細則、零售業個人資料檔案安全維護管理辦法等規定研擬，本手冊計有人資料保護與資訊安全、個資手冊問與答QA、附錄等三大部分，謹分別說明如下：

一、個人資料保護與資訊安全

本章節包含8篇文章，介紹個人資料保護法的合規要求及常見的資安防護重點，個資保護議題分別有「什麼是個人資料？」、「個資當事人預設同意與拒絕接受行銷之案例分析」、「個資國際傳輸應如何落實法律遵循」、「自評表填寫案例教學」等4篇文章；資安防護議題分別有「淺談社交工程防範對個人資料保護之重要性」、「資訊安全技術對於個人資料保護的關鍵作用」、「如何確保伺服器設備安全以強化個資保護」、「應如何進行資訊系統防護以避免個資外洩」等4篇文章。每篇文章均有案例說明及分析，使讀者可從實務案例中學習並進行精進措施。

二、個資手冊問與答QA

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。

三、附錄

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、零售業個人資料檔案安全維護計畫（範本），共四個附錄文件。

第 1 部分

個人資料保護與資訊安全

壹、什麼是個人資料？

案例

小華最近在一家連鎖咖啡店辦會員卡，提供姓名、電話號碼、電子郵件地址等基本資料。幾個月後，他發現自己經常收到店家的促銷訊息，甚至連消費紀錄和平時喜歡點的飲品也被精確地記錄下來。小華開始擔心，這些資料是不是被咖啡店使用了？而哪一些資料是屬於個人資料呢？

什麼是個人資料？

個人資料，顧名思義，是與個人相關的資料。根據《個人資料保護法》（下稱個資法）規定，個人資料指的是能夠直接或間接識別出某位自然人的任何資訊。例如，姓名、出生年月日、身分證號碼、聯絡方式。同時，個人資料的種類應不限於條文所列舉，若有其他資料能夠直接或間接識別某位自然人亦屬於個人資料。簡單來說，只要資料能與某個特定個人連結起來，不管這些資料是透過紙本文件或電子檔案保存，都應受到個資法的保護。

對象及範圍

可以直接或間接連結到特定人的資料，個資法所指的「人」是誰？在個資法第2條明定只有「自然人」的資料屬於個資，而個資法施行細則第2條規定，所謂的自然人是現在生存的個人，這也意味著死亡後的人的資料不屬於個資法認定的個資範疇，惟若牽涉尚生存者仍為個資[1]。另外，不屬於自然人的法人或其他團體等相關資料也不屬於保護範疇[2]。

1 法務部法律字第10503502210號函釋。
2 臺灣桃園地方法院108年度訴字第188號刑事判決參照。

個人資料並無特定的呈現或保存方式，包括紙本文件、電子檔案都會是個人資料。因此，企業無論是在線上或實體紙本蒐集到的顧客資料，只要與個人相關，都應依照個資法進行管理。

直接識別與間接識別

- **直接識別資料：**例如姓名、身分證號碼、指紋等，透過該資料本身，就可以直接連結至特定個人，不需要搭配其他資料，屬於直接識別。
- **間接識別資料：**有些資料單獨看可能無法立即辨認個人，但透過與其他資訊結合，就能間接識別出特定個人。例如，電話號碼、電子郵件地址、甚至是消費紀錄。即使單獨的電話號碼無法直接識別出某個人，只要能與其他資料對照、組合、連結，這個號碼也算是個人資料。

個資的範圍有多廣？

《個資法》適用於任何可以辨識個人的資料，而這些資料的形式可以是多樣的，包括線上及線下蒐集的資訊。例如，企業從消費者那裡收集到的資料，不管是線上會員註冊還是實體商店的訂單資料，只要與個人有關聯，企業就必須依法保護。

特種個人資料

有些個人資料屬於比較敏感的類型，例如病歷、醫療、基因、性生活、健康檢查及犯罪前科。這些資料被稱為特種個人資料，在法律上有更嚴格的保護標準。除非有符合個資法的特定情況，企業一般不得隨意蒐集、處理或利用這類資料。

然而，縱使未區分所謂一般個資與特種個資（或者「一般性資料」與「敏感性資料」），所有足以識別個人的資訊均應受到同等程度的保護，甚至於某些特定的個人資料或因其敏感性，可能需要更高的保護標準。

其他實務上已承認的類型

遇到非列舉的個人資料種類時，實務上判斷是否屬於個人資料，可參考法院判決與主管機關的解釋來認定，以下提供實務上所承認的個資種類：

1. GPS定位資訊[3]。
2. 個人的心跳、呼吸及睡眠等資訊[4]。
3. 電話號碼[5]。
4. 通聯記錄（包含時間與對象）及通話內容[6]。
5. 車牌影像資料[7]。
6. 金融卡或信用卡卡號[8]。
7. 薪資收入或所得等[9]。

案例解答

在小華的案例中，他提供的姓名、電話號碼、電子郵件地址屬於個人資料，因為這些資訊能夠直接識別出他本人。此外，消費紀錄和個人的飲品偏好等資訊也屬於個人資料，儘管從這些資料中單獨看不一定能直接識別某個人，但一旦與其他資料結合（如會員卡資訊），就可以間接識別出小華。因此，這些資料都受到個資法的保護。

企業應該如何遵循個資法？

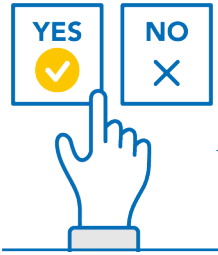
像小華這樣的情況，其實在現代的商業環境中非常常見。企業蒐集和使用顧客資料已成為經營常態，但許多企業對於「個人資料」的定義還不夠瞭解，可能導致資料保護上的疏漏，進而影響消費者的權益。

企業在日常經營中，應該建立健全的個資管理機制，確保資料的蒐集、處理和利用符合法規。對於一般個資和特種個資，企業都應當謹慎處理，確保不會外洩或濫用顧客資料。這樣不僅是法律義務，也是維護顧客信任的重要方式。

總而言之，企業在商業活動中蒐集到的個人資料範圍非常廣泛，從基本的聯絡資訊到消費習慣、偏好等，都應受到相應的保護。隨著科技發展和數位資訊應用越來越普遍，企業若能深入理解個資法的規範，不僅能避免法律風險，也能提升顧客信任，促進長遠發展。

---

3 國家發展委員會107年11月21日發法字第1072002136號函釋。
4 法務部法律字第10703505830號函釋。
5 國家發展委員會109年7月24日發法字第1090015912號函釋。
6 臺灣高等法院106年度上易字第819號刑事判決。
7 國家發展委員會110年6月9日發法字第1102000884號函釋。
8 法務部法律字第10100100770號函釋。
9 法務部法律字第10603509150號函釋。



貳、個資當事人預設同意與拒絕接受行銷之案例分析

隨著數位化的發展，《個資法》的重要性在業界愈加顯著。對於企業而言，如何在行銷推廣活動中合法使用客戶的個人資料，並處理當事人拒絕接受行銷訊息的請求，成為重要課題。以下將從個資法的角度，結合實務見解與行政機關函釋，深入探討兩個常見的案例，並提供具體的建議。

案例

1. **會員資料蒐集：**A公司推出會員計畫，消費者透過註冊成為會員來獲得優惠。在註冊過程中，消費者需提供姓名、電話、電子郵件和購物偏好等資料，A公司則會用這些資料進行行銷推廣和顧客行為分析。
2. **行銷預設同意：**B公司提供電子收據服務，結帳時消費者可選擇用電子郵件接收收據，但系統已經預設勾選「同意接收行銷訊息」，聲明會根據消費者的購物習慣發送個性化的行銷資訊。

案例分析

1. 會員資料蒐集的合法性

消費者在註冊會員時自願提供個人資料，這類蒐集資料的行為是合法的，但必須遵守《個資法》第7條和第8條的規定。企業需讓消費者了解資料的用途，比如優惠服務或行銷推廣，並取得「明確同意」。這要求企業提供清楚的隱私政策，告知資料用途及是否會分享給第三方，並且要有簡便的機制讓消費者隨時撤回同意。

例如，A公司應該在電子郵件行銷中提供「取消訂閱」的選項，讓消費者可以隨時停止接收行銷訊息。這樣可以確保A公司符合法律規範，並保護消費者的權益。

2. 預設同意的問題與法規風險

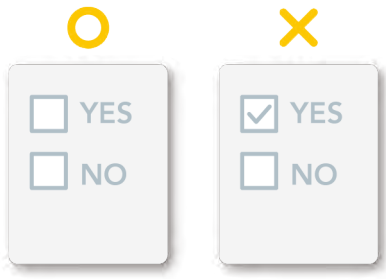
在此案例中，B公司在預設勾選同意接收行銷訊息的作法上，可能違反《個資法》中「明確同意」的原則。根據個資法規定，企業在蒐集資料時必須清楚告知消費者，並且不能預設同意。預設勾選的方式容易讓消費者在不知情的情況下默默同意接收行銷訊息，這樣的行為是不合法的。企業雖然提供了取消勾選的選項，但依然存在法律風險。依據國家發展委員會的函釋[10]，預設勾選行為難以滿足「明確同意」的標準。即使消費者未主動反對，也不能視為其已充分知情並同意，這可能導致企業面臨罰則或品牌形象受損。

企業應取消預設勾選的行為，改為提供一個明確的選擇框，讓消費者自主決定是否願意接收行銷訊息。這樣不僅能符合個資法的要求，也能提升消費者對資料使用的透明度與信任感。

3. 推定同意的適用範圍

《個資法》第7條第3項提到的「推定同意」，指的是當消費者主動提供資料且沒有明確表示反對時，企業可以假設消費者同意。然而，這與預設同意不同。如果資料是透過預設勾選來收集，則不符合「推定同意」的要求。

舉例來說，如果消費者主動提供電子郵件來接收電子收據，但未反對接收行銷訊息，這可以視為推定同意。但若是預設勾選「同意接收行銷訊息」，這樣的行為就不合法。



10 國家發展委員會107年11月21日發法字第1072002136號函釋。

4. 拒絕行銷的權利

消費者有權拒絕接收行銷訊息，企業應提供簡單明確的途徑讓消費者行使這項權利。例如，企業可在電子郵件行銷訊息中提供明顯的「取消訂閱」按鈕，或在會員系統中設置方便的選項，讓消費者可以隨時停止接收行銷資訊。這不僅符合法律規範，也能減少消費者的反感，提升品牌形象。

結論與建議

企業經常大量利用消費者個人資料投放廣告以提升銷售業績。然而，依據我國個資法的規定，無論是蒐集會員資料還是提供廣告行銷等服務，都必須在取得當事人「明確同意」的前提下進行。具體而言，業者應注意以下幾點：

- **明確同意**

  在蒐集個人資料時，必須讓消費者充分知悉資料將被用於何種用途，並且取得其自主同意。隱私政策應清楚、具體，並提供撤回同意的便捷機制。

- **取消預設同意**

  企業應避免預設勾選同意接收行銷訊息的作法，因為可能會違反個資法。應提供清晰的選擇框，讓消費者自主決定是否願意接收行銷訊息。

- **推定同意的正確使用**

  推定同意僅能在當事人主動提供資料且未表示拒絕的情況下適用。若資料是在當事人未積極參與的情況下自動蒐集，則不符合推定同意的要件。

- **拒絕行銷的權利**

  應提供簡單明確的途徑讓消費者行使拒絕行銷權利。

最後，企業應不斷檢視關於資料蒐集與使用流程，確保在行銷推廣中符合個資法的規範，避免潛在的法律風險並提升消費者信任度。

參、個資國際傳輸應如何落實法律遵循

案例分析

P公司為一零售業者且為某跨國企業在我國之子公司，近期因總公司之營運政策變更，預計會採用中國大陸業者提供之雲端服務儲存資料，則P公司應該如何達成我國個人資料保護法規的要求？

國際傳輸定義為「指將個人資料作跨國（境）之處理或利用」[11]，可知只要是將個人資料以任何形式傳送至我國以外之國家或地區，無論接收個人資料之對象為何，均會構成國際傳輸個資之行為。

現今個人資料大多會以電子化或數位化之形式作業，並透過網際網路進行傳輸或儲存於雲端系統，因此許多日常之資料傳送行為可能會涉及國際傳輸，若業務範圍擴及國外或為跨國企業，則更需要留意是否有國際傳輸之情形。當公司會將個人資料進行國際傳輸時，必須要落實告知資料當事人之義務，將國際傳輸之詳細內容告知當事人才符合法規。

一、國際傳輸之形態

公司應如何判斷自身業務是否有涉及國際傳輸，以下將說明常見之國際傳輸型態：

1. 關係企業

我國公司若在國外設有分公司或成立子公司者，或我國公司為外國企業設立之分公司或子公司者，而因業務需求會將客戶之資料傳送給分公司、母

11 個人資料保護法第2條第6款。

公司或子公司，例如：A公司經營連鎖零售賣場並有招收會員，且A公司在日本設有子公司B及賣場，於臺灣申辦的會員至日本賣場也可以使用會員服務（累積點數、消費紀錄等），如此A公司會將會員的個人資料提供給B公司。

雖然A公司與B公司間為關係企業，但國際傳輸並未排除公司內部或關係企業間傳輸之情形，因此仍然屬於將個人資料進行國際傳輸，則A公司將所蒐集到的會員個人資料提供給B公司處理、利用，即為個人資料國際傳輸。

2. 雲端系統

現今許多公司會將個人資料儲存於雲端，而雲端系統仍須要將資料儲存於實體伺服器，因此儲存於雲端上之資料會落地於某處之實體機房，如果實體機房是位於境外則會涉及國際傳輸，例如：C公司使用M公司提供之雲端服務，而M公司是將機房設置於新加坡，因此C公司保有的資料會落地於新加坡。

當公司有使用雲端系統時，應留意所使用之雲端平台是將資料存放於何地的機房，即使只有部分的個資儲存於雲端，但機房設於境外，仍然屬於將個資進行國際傳輸。

二、國際傳輸之法遵建議

當公司對於個資之處理或利用有涉及到國際傳輸時，有二項個人資料保護法之規定必須注意及遵守，分別為「主管機關限制」[12] 與「告知義務」[13]。另外公司將當事人個人資料進行國際傳輸前，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[14]：

1. 主管機關限制

公司原則上可以自由進行國際傳輸，但主管機關認為有必要管制的時候，會另外作出限制。主管機關通常會以發布行政函釋之方式，公告所管轄之

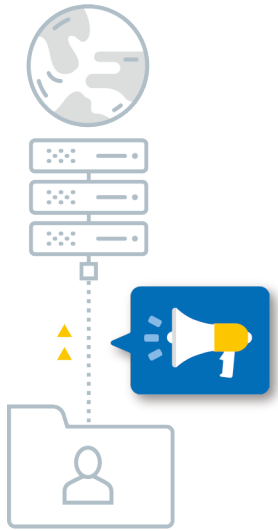
12 個人資料保護法第21條。
13 個人資料保護法第8條。
14 零售業個人資料檔案安全維護管理辦法第8條第3項。

產業別關於國際傳輸之限制項目，例如：勞動部曾以大陸地區之個人資料保護相關法律及法令規範尚未完備為由，限制人力仲介業將當事人個人資料國際傳輸至大陸地區[15]。

建議公司隨時留意所隸屬之中央目的事業主管機關是否有發布相關函釋，限制個資國際傳輸的國家或地區，避免將個資傳輸至禁止之國家或地區，以符合主管機關之要求。如果主管機關未作出任何限制，公司則可以將個資進行國際傳輸。

2. 告知義務

公司於蒐集個人資料時，應明確告知當事人關於個人資料利用之地區。[16] 若有國際傳輸則要落實告知當事人個人資料利用之地區，而所謂個人資料利用之地區為擬傳輸之對象所在之區域或雲端機房所在之區域，此項資訊必須於蒐集個資時告知當事人。



建議公司重新檢視會員條款、個人資料保護條款或隱私權政策等關於告知當事人之聲明，確認當中資料利用之地區是否有說明國際傳輸之區域，方能符合個人資料保護之法遵要求。

案例解答

綜上所述，P公司應該先檢視中央目的事業主管機關是否有對國際傳輸進行限制，若主管機關未作出限制或限制之內容與P公司之狀況無關，則P公司於蒐集個資時，明確告知會將個資傳輸至中國大陸，便能夠符合法律要求。

15 勞動部112年2月20日勞動發管字第1120500319A號公告。
16 個人資料保護法第8條第1項第4款。

肆、商業服務業及零售業個資保護自評表填寫範例教學

一、商業服務業個資防護自評表

「經濟部主管商業服務業者個資防護自評表」（以下簡稱本表），係為經濟部商業發展署制定，以推動商業服務業者（以下簡稱業者）營運之個人資料保護與管理基本防護查核，以引導業者建立自主個人資料保護與管理。

目的

本表旨在提供我國商業服務業者以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，可綜合考量營運風險及業務發展，訂定符合業者本身營運需求之個人資料保護與管理制度。

使用對象

以批發及零售為主要營業行為並有招募會員或可取得交易對象個人資料之業者。

如何使用本表

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」等規範建議業者內部由負責業務之主管、法務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。

本表填寫步驟如下

1. 依序由第1題組填寫至第16題組，以本表之稽核內容為基準，並可參考「備註」欄位之說明，瞭解本稽核項目之具體內容或程序文件範例，比對業者本身現行個人資料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」）於「自評結果」欄位，並將相關證明文件、紀錄填寫於「說明」欄位。
2. 「自評結果」欄位：依稽核實際狀況，參考相關佐證資料填具自評結果。

☐ 符合	☐ 不符合	☐ 不適用
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。	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。	實際作業排除稽核內容之適用。

稽核項目 **1** **配置管理之人員及相當資源**

（個人資料保護法施行細則第12條第2項第1款）

稽核內容	自評結果	說明（實作建議）	備註
1.1 **是否設個人資料管理單位或適當組織？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已有設置個人資料管理組織，負責統籌本公司個資保護工作事項，並由各部門自行執行個資盤點、風險評鑑工作。 參照附件 ・個資管理單位組織圖 ・成員表 ・權責分工表	請檢附個資管理單位組織圖、分工及相關辦法，並提出個資窗口所協助之各項個資保護工作事項，如：參與會議、盤點及風險評鑑工作、事件處理等。

稽核項目 **2** **界定個人資料之範圍**

（個人資料保護法施行細則第12條第2項第2款）

稽核內容	自評結果	說明（實作建議）	備註
2.1 是否每年定期清查其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?	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂定個資盤點作業規範，每年定期執行個資盤點作業，建立並更新個資檔案清冊及作業流程圖。 參照附件 ・個資盤點作業書 ・個資業務流程圖 ・個資檔案清冊	請檢附個人資料檔案清冊及個人資料作業流程說明文件，並經權責主管核定之紀錄。

稽核項目 **3** **個人資料之風險評估及管理機制**

（個人資料保護法施行細則第12條第2項第3款）

稽核內容	自評結果	說明（實作建議）	備註
3.1 是否每年定期評估其因蒐集、處理或利用個人資料可能面臨的法律或其他風險，並訂定適當之管控及因應措施？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司每年定期執行風險評估及風險評鑑作業，並根據前次風險評鑑結果，針對高風險作業採取適當管控及因應措施。 參照附件 ・風險管理作業書 ・風險評鑑表報告 ・高風險處理計畫	請檢附風險評估過程底稿、風險評鑑報告及風險處理計畫。

稽核項目 **4** **事故之預防、通報及應變機制**

（個人資料保護法施行細則第12條第2項第4款）

稽核內容	自評結果	說明（實作建議）	備註
4.1 個資事故應變機制是否包含降低、控制事故對當事人造成損害之作法及因應措施？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂定個資事故應變機制，包含降低、控制事故對當事人造成損害之作法及因應措施。 參照附件 ・個資事故通報應變作業書	請說明應變機制對降低、控制事故對當事人造成損害之作法。
4.2 個資事故應變機制是否包含適時以電子郵件、簡訊、電話或其他便利當事人知悉之適當方式通知當事人個人資料被侵害之事實與已採取之因應措施，及後續供當事人查詢之專線與其他查詢管道？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂定個資事故應變機制，包含適時以電子郵件、簡訊、電話或其他便利當事人知悉之適當方式通知當事人個人資料被侵害之事實與已採取之因應措施，及後續供當事人查詢之專線與其他查詢管道。 參照附件 ・個資事故通報應變作業書	請說明應變機制對通知當事人之作法。
4.3 個資事故應變機制，是否包含避免類似事故再次發生之矯正及預防機制？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂定個資事故應變機制，包含避免類似事故再次發生之矯正及預防機制。 參照附件 ・個資事故通報應變作業書	請說明應變機制對避免類似事故再次發生之矯正及預防機制。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
4.4 **是否就個資事件通報，其通報流程為何？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂定個資事故應變機制，通報流程自發現事故時起算72小時內，填具個人資料侵害事故通報及紀錄表，以電子郵件方式向主管機關通報，並將視案情發展適時通報處理情形。 參照附件 ・個資事故通報應變作業書	請檢附事故通報文件。

稽核項目 5 蒐集、處理、利用作業

（個人資料保護法施行細則第12條第2項第5款）

稽核內容	自評結果	說明（實作建議）	備註
5.1 **資料蒐集、處理是否具備特定目的並具有法定要件？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司所保有之個人資料，於蒐集、處理時均具備特定目的並具有法定要件。 參照附件 ・個資檔案清冊	請檢附最新個資盤點資料，確認皆已識別保有依據。
5.2 **個人資料之利用，是否符合特定目的之範圍？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司所保有個人資料，於利用時已符合特定目的之範圍。 參照附件 ・個資檔案清冊	請檢附最新個資盤點資料，確認皆已識別保有依據。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
5.3 **是否有目的外之利用？目的外利用是否符合法定要件？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司所保有個人資料進行目的外利用前，已確認具有目的外利用之法定要件。 參照附件 ・個資檔案清冊	請說明機關所蒐集之個資是否具有目的外之利用情形。如有目的外利用，請說明其符合之法定要件。
5.4 **是否依規定取得當事人同意（當事人同意之情形）？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司所保有個人資料之蒐集、處理及利用，事前已取得當事人同意。 參照附件 ・個資同意書	請說明蒐集個資並取得當事人同意之情形。
5.5 **是否履行告知義務（未履行告知義務時，是否符合免告知之情形）？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂有個資告知聲明書，並載明法定事項，透過紙本／線上方式向當事人履行告知義務。 參照附件 ・隱私權政策 ・個資告知聲明書	請檢附告知事項。
5.6 **是否已於首次行銷時提供當事人表示拒絕行銷之管道？如需費用是由機關支付所需費用？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司所保有個人資料用於行銷，首次行銷時已提供當事人可透過客服信箱表示拒絕行銷，並由本公司支付所需費用。 參照附件 ・電子報提醒 ・個資行銷作業書	請說明提供當事人拒絕行銷之方式。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
5.7 是否依當事人拒絕接受行銷之要求，立即停止利用其個人資料為行銷，並週知所屬人員或採行防範所屬人員再次行銷之措施？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司於受理當事人拒絕接收行銷之要求，當日將立即停止利用其個人資料為行銷，並內部週知所屬人員確認已排除行銷名單之外。 參照附件 ・個資行銷作業書	請說明是否有當事人拒絕接受行銷以及作業流程。

稽核項目 6 資料安全管理及人員管理

（個人資料保護法施行細則第12條第2項第6款）

稽核內容	自評結果	說明（實作建議）	備註
6.1 是否識別業務內容涉及個人資料蒐集、處理或利用之人員？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司有定期識別業務內容涉及個人資料蒐集、處理或利用之人員。 參照附件 ・個資管理組織圖 ・成員分工表	請檢附個資管理單位組織圖、分工及相關辦法，以及個人資料檔案清冊。
6.2 是否依其業務特性、內容及需求，設定所屬人員接觸消費者個人資料之權限，並定期檢視其適當性及必要性？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司每年定期檢視所屬人員帳號權限。 參照附件 ・個資系統權限申請表單 ・帳號權限審查紀錄	請檢附個資系統權限申請表單以及帳號權限審查紀錄。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
6.3 **是否與所屬人員約定保密義務？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司於聘用所屬人員時，均已簽定個資保密切結書。 參照附件 ・保密切結書	請檢附所屬人員清單（正職、短期約僱）及所簽屬之保密切結書。
6.4 **是否要求人員離職時，返還保有消費者個人資料之載體，並刪除因執行業務而持有之消費者個人資料？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司要求所屬人員離職前，均須完成辦理交接，包含返還保有消費者個人資料之載體，並刪除因執行業務而持有之消費者個人資料。 參照附件 ・離職交接檢核表	請檢附所屬人員清單（正職、短期約僱）及所簽屬之保密切結書或離職單。
6.5 **消費者個人資料有加密之必要者，於蒐集、處理或利用時，是否採取適當之加密措施？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司評估消費者個人資料有加密之必要者，已採行資料檔案加密或個資遮蔽之措施。 參照附件 ・資料安全管理作業書 ・開啟檔案顯示加密措施之截圖畫面	請說明針對個資電子檔案之控管規範，例如將個人資料檔案置於公用電腦或網路共用資料夾，是否進行加密或遮蔽？並檢附查核結果。
6.6 **傳輸消費者個人資料時，是否依不同傳輸方式，採取適當之安全措施？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司針對紙本、電子檔案之傳送已分別採取適當安全措施。 參照附件 ・資料傳輸管理程序書 ・個資傳輸紀錄	請說明機關對外傳送個資檔案之相關規範，檢附規範制度文件。例如以電子郵件傳送敏感之個資檔案時，是否採加密機制？並請相關佐證。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
6.7 消費者個人資料有備份之必要者，是否對備份資料採取適當之保護措施？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司評估消費者個人資料有備份之必要者，根據備份資料之介質，已採行相應的保護措施，紙本置放於上鎖櫃，電子檔存放於資料庫進行加密。 參照附件 ・資料安全管理作業書	請說明資料備份機制，並檢附規範制度文件。

稽核項目 **7** **認知宣導及教育訓練**

（個人資料保護法施行細則第12條第2項第7款）

稽核內容	自評結果	說明（實作建議）	備註
7.1 是否定期對實施所屬人員之個人資料保護與管理認知宣傳及教育訓練？所屬人員是否明瞭上課內容？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司每年定期辦理員工個資保護教育訓練，並有課後測驗確認所屬人員明瞭上課內容。另於公司內網及布告欄進行認知宣導。 參照附件 ・教育訓練課程講義 ・簽到表 ・測驗成績紀錄	請檢附對所屬人員之教育訓練簡報、各項相關課程簽到表（需含授課日期）及課後評量結果。上課內容應包含個人資料保護相關法令之要求、人員之責任範圍及各項個人資料保護相關作業程序。

稽核項目 **8** **設備安全管理措施**
（個人資料保護法施行細則第12條第2項第7款）

稽核內容	自評結果	說明（實作建議）	備註
8.1 是否依據作業內容及環境之不同，實施必要之安全環境管制？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司分別針對紙本、電子檔存放之設備，已訂定管理程序並配置安全防護系統。 參照附件 ・資料安全管理作業書 ・檔案室／櫃之調閱紀錄 ・安全防護系統授權書	請說明對存放儲存媒介物之環境相關消防、監控、進出入等控管措施，並檢附相關照片。
8.2 是否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？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司每年定期檢查，並維護更新相關實體設備。 參照附件 ・設備檢查及維護表	請確認是否定期檢查或維護更新設備？並請檢附定期檢查及維護紀錄。
8.3 是否針對不同作業環境，建置必要之保護設備或技術？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已針對不同作業環境建置必要之保護設備，如檔案室及機房均設有消防設備、監控設備。 參照附件 ・消防、監控設備維護表	請檢附消防、監控設備等維護紀錄。
8.4 資通訊系統是否採行使用者身分認證機制？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司保有個資之資通訊系統已採行使用者身分確認及保護機制。 參照附件 ・資料安全管理作業書	請說明使用者身分認證機制，並檢附相關佐證。 （非必須具備項目）

稽核內容	自評結果	說明（實作建議）	備註
8.5 是否採行個人資料顯示之隱碼機制？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司保有個資之資通訊系統已採行個資隱碼機制。 參照附件 ・資料安全管理作業書 ・隱碼設定規則 ・系統化面截圖	請說明個人資料顯示之隱碼機制，並檢附相關佐證。 （非必須具備項目）
8.6 是否定期檢視蒐集、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，並因應系統漏洞所造成之威脅？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司針對涉及個資之電腦、相關設備或系統，每年定期執行弱點掃描、滲透測試等檢測，並針對發現之風險立即修復。 參照附件 ・資料安全管理作業書 ・檢測報告	請說明定期檢視之週期，及說明如何因應系統之弱點或漏洞，並檢附佐證資料。 （非必須具備項目）
8.7 是否採行防止外部網路入侵對策，並定期更新？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司保有個資之資通訊系統已採行外部網路入侵對策。 參照附件 ・資料安全管理作業書 ・防火牆 ・防毒軟體授權證明書	請說明防止外部網路入侵對策，並檢附相關佐證。 （非必須具備項目）
8.8 是否採行非法或異常使用行為之監控及因應機制？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司保有個資之資通訊系統已採行端點偵測及應變機制。 參照附件 ・資料安全管理作業書 ・偵測系統軟體授權證明書	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。 （非必須具備項目）

稽核項目 **9** **資料安全稽核機制**
（個人資料保護法施行細則第12條第2項第9款）

稽核內容	自評結果	說明（實作建議）	備註
9.1 **是否每年定期由適當組織執行資料安全內部稽核並提出評估報告？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司每年定期安排由內稽小組執行資料安全內部稽核，並將稽核情形及結果彙整後，向個人資料管理組織提出評核報告。 參照附件 ・資料安全稽核作業書 ・評核報告	請說明稽核之頻率及執行方式，並檢附最近一次之評估報告。
9.2 **是否採取改善措施以持續改善資料安全維護？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司於稽核結束後，已依前次稽核結果發現缺失進行矯正，並持續追蹤改善成效。 參照附件 ・稽核矯正單 ・改善追蹤紀錄	請檢附檢視或修正之紀錄，並檢附稽核矯正單及追蹤紀錄。

稽核項目 **10** **使用紀錄、軌跡資料及證據保存**
（個人資料保護法施行細則第12條第2項第10款）

稽核內容	自評結果	說明（實作建議）	備註
10.1 **是否保存個人資料提供或移轉第三人之紀錄？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司向委外廠商、關係企業提供個人資料時，均有留存相關紀錄。 參照附件 ・個資移轉紀錄	是否保存個人資料提供或移轉第三人之紀錄？

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
10.2 **是否保存當事人行使個資法第三條之權利及處理過程之紀錄？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂定當事人權利行使程序，均於法定期限受理並留存相關處理過程紀錄。 參照附件 ・受理當事人權利行使作業書 ・當事人權利行使申請表 ・受理回復紀錄	請檢附當事人行使個資法第三條之權利及處理過程之紀錄。
10.3 **是否保存個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂定個資銷毀程序，電腦設備及其他儲存媒介物需經報廢審核作業，確認無個資外洩疑慮後進行銷毀並留存紀錄。 參照附件 ・資料銷毀作業書 ・報廢單 ・個資檔案刪除銷毀申請表	請檢附個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄。
10.4 **是否保存人員權限新增、變動及刪除之紀錄**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司每年定期檢視所屬人員帳號權限，並保存人員權限新增、變動及刪除之紀錄。 參照附件 ・個資系統權限申請表單 ・帳號權限審查紀錄	請檢附人員權限新增、變動及刪除之紀錄。
10.5 **是否保存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？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司於特定目的期限屆滿前保存對於消費者個人資料相關紀錄及軌跡資料。 參照附件 ・資料安全管理作業書 ・系統存取紀錄 ・軌跡資料（Log）相關日誌檔案	請說明留存之期限，並檢附近一年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。

稽核項目 **11** **個人資料安全維護之整體持續改善**

（個人資料保護法施行細則第12條第2項第11款）

稽核內容	自評結果	說明（實作建議）	備註
11.1 是否定期就個人資料安全維護議題召開會議並提出持續改善報告？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司每年定期召開個資管理會議討論，並提出持續改善報告。 參照附件 ・年度個資管理會議紀錄 ・持續改善報告	請檢附相關個人資料安全維護議題會議之紀錄。
11.2 是否訂定個人資料管理（或安全維護）辦法並定期檢視更新？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂定個人資料管理安全維護計畫，並每年定期檢視配合法規更新。 參照附件 ・個人資料管理安全維護計畫 ・修訂文件紀錄	請檢附個人資料管理（或安全維護）辦法以及完整之版本資訊，包含但不限於日期、提報人及核定人等相關資訊。

稽核項目 **12** **委託作業**

（個人資料保護法第4條、個人資料保護法施行細則第7條及第8條）

稽核內容	自評結果	說明（實作建議）	備註
12.1 委託他人蒐集、處理或利用個人資料之全部或一部時，是否要求受託人依委託人應適用之規定為之？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司涉及個資委外之業務，事前已於委託契約要求委外廠商遵守個資法規範。 參照附件 ・委外廠商清單 ・委外個資保護契約 ・委外廠商個資安全維護聲明書	請檢附個資委外之廠商清單及合約文件。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
12.2 委託他人蒐集、處理或利用個人資料之全部或一部時，是否於委託契約或相關文件明確約定適當之監督事項及方式？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司簽訂委託契約時，已於契約內容中明確約定適當之監督事項及方式。 參照附件 ・委外個資保護契約 ・委外廠商個資安全維護聲明書	請檢附個資委外之廠商清單及合約文件。
12.3 委託他人蒐集、處理或利用個人資料之全部或一部時，是否確實執行監督？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司涉及個資委外之業務，每年定期透過抽查／自評／實地方式執行監督，並做成委外稽核報告。 參照附件 ・委外稽核報告 ・委外缺失追蹤紀錄	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。
12.4 是否要求受託者僅得於委託機關指示之範圍內，蒐集、處理或利用資料？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司涉及個資委外之業務，事前已於委託契約要求受託者僅得於委託機關指示之範圍內，蒐集、處理或利用資料。 參照附件 ・委外個資保護契約 ・委外廠商個資安全維護聲明書	請檢附個資委外之廠商清單及合約文件。
12.5 是否要求受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司涉及個資委外之業務，事前已於委託契約要求受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。 參照附件 ・委外個資保護契約 ・委外廠商個資安全維護聲明書	請檢附個資委外之廠商清單及合約文件。

稽核項目 **13** **使用資通訊系統蒐集、處理或利用個人資料**

（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）

稽核內容	自評結果	說明（實作建議）	備註
13.1 **是否就使用資通訊系統蒐集、處理或利用個人資料之服務範圍取得資安或個資驗證？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司保有個人資料之資通訊系統已取得ISO 27001資安認證、TPIPAS個資管理認證。 參照附件 ・ISO證書 ・資料隱私保護標章（dp.mark）	請檢附外部稽核證書（或驗證通過證明書），例如ISO27001、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。

稽核項目 **14** **個資存放雲端之安全控管**

（個人資料保護法施行細則第12條第2項第6款）

稽核內容	自評結果	說明（實作建議）	備註
14.1 **是否確保個人資料放在雲端上的安全？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已建立雲端的存取控制權限、雲端資料加密及備份，並定期檢視及更新。 參照附件 ・雲端管理作業書 ・雲端存取紀錄	請說明如何確認Database的安全以及放在那個國家？並提出相關佐證（如雲端業者出具的證明書）。

稽核項目 **15** **發生個資事件之處理**

（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）

稽核內容	自評結果	說明（實作建議）	備註
15.1 近兩年內是否發生個人資料被竊取、洩露、竄改或其他侵害情形之個資事件？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司近兩年內有發生個資事故，發現事故時已及時通報主管機關。 參照附件 ・個人資料侵害事故通報與紀錄表	請檢附通報記錄。
15.2 是否就個資事件委請公正之第三方進行調查？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司於個資事件發生後，已委請第三方資安廠商進行調查並做成報告。 參照附件 ・事件調查報告	請檢附就個資事件聘請第三方資安廠商就事件調查之報告。
15.3 是否及時且適當的通知當事人？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司於個資事件發生後，已及時透過簡訊／電子郵件向當事人通知個資外洩及採取之因應措施。 參照附件 ・事故通知紀錄	請檢附向用戶說明事件緣由及防護措施之通知。
15.4 是否就事件的發生進行根因分析，並提出強化措施？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司於個資事件發生後，已召開事件處理會議，就本次事件的發生進行根因分析，並提出對應的強化措施。 參照附件 ・事件處理會議紀錄 ・事件處理報告 ・強化措施追蹤紀錄	請檢附事件報告、強化措施的實施情形以及相關內部會議紀錄。

稽核項目 **16** **個人資料庫之共享使用**
（個人資料保護法第8條）

稽核內容	自評結果	說明（實作建議）	備註
16.1 **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？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司與其他關係企業共享使用客戶個人資料庫，事前已明確向當事人告知法定事項及蒐集主體。 參照附件 ・個資告知聲明書	請說明具體共享之主體名稱，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。

稽核項目 **17** **國際傳輸**
（個人資料保護法第8條第1項第4款、第21條）

稽核內容	自評結果	說明（實作建議）	備註
17.1 **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 ☐ 不符合 ☐ 不適用	本公司進行個資國際傳輸前，已檢視及遵循主管機關要求。 參照附件 ・資料傳輸管理程序書	請進行說明是否有進行檢視。（中央目的事業主管機關得限制非公務機關為國際傳輸個人資料。）
17.2 **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 ☐ 不符合 ☐ 不適用	本公司進行個資國際傳輸前，已於官網公告隱私權政策，告知當事人擬傳輸之地區。 參照附件 ・個資告知聲明書 ・官網隱私權政策	請提出告知當事人之佐證紀錄。

二、零售業個資防護自評表填寫範例教學

「經濟部主管零售業者個資防護自評表」(以下簡稱本表),係為經濟部商業發展署制定,以推動零售業者(以下簡稱業者)營運之個人資料保護與管理基本防護查核,以符合「零售業個人資料檔案安全維護管理辦法」之規定要求,引導業者建立自主個人資料保護與管理。

目的

本表旨在提供我國零售業者以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。

使用對象

以經濟部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。

如何使用本表

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「零售業個人資料檔案安全維護管理辦法」等規範建議業者內部由負責業務之主管、法務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。

本表填寫步驟如下

1. 依序由第1題組填寫至第22題組,以本表之稽核內容為基準,並可參考「備註」欄位之說明,瞭解本稽核項目之具體內容或程序文件範例,比對業者本身現行個人資料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」)於「自評結果」欄位,並將相關證明文件、紀錄填寫於「說明」欄位。

2.「自評結果」欄位：依稽核實際狀況，參考相關佐證資料填具自評結果。

☐ 符合	☐ 不符合	☐ 不適用
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。	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。	實際作業排除稽核內容之適用。

稽核項目 **1** **個人資料檔案安全維護計畫之訂定及修正**

（零售業個人資料檔案安全維護管理辦法第4條、第6條）

稽核內容	自評結果	說明（實作建議）	備註
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。**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已於○○年○○月訂定（修正）安全維護計畫，載明法定事項。 參照附件 ・安全維護計畫	請檢附個人資料檔案安全維護計畫及相關管理文件。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
1.2 是否定期檢視及配合相關法令修正安維計畫？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司每年定期召開個資管理會議定期檢視並配合法令修正安維計畫。 參照附件 ・OO年度個資管理會議紀錄 ・安維計畫修訂文件紀錄	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。

稽核項目 **2** **配置專責人員並執行任務**

（零售業個人資料檔案安全維護管理辦法第5條）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司已指定OO部門主管擔任專責人員，負責規劃、訂定、修正、執行安全維護計畫及其他個資管理相關事項。 參照附件 ・個資管理單位組織圖 ・成員表 ・權責分工辦法	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零售業者之代表人或經其授權之人員提出報告？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司專責人員每年定期向代表人提出安全維護計畫執行報告。 參照附件 ・OO年度安全維護計畫規劃暨執行報告	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。

稽核項目 **3** **界定個人資料範圍並定期確認**
（零售業個人資料檔案安全維護管理辦法第7條第1項）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司已訂定個資盤點作業規範，並建立個資盤點清冊。 參照附件 ・個資盤點作業書 ・個資業務流程圖 ・個資盤點清冊	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 ☐ 不符合 ☐ 不適用	本公司每年定期執行個資盤點作業，確認所保有個資之變動。 參照附件 ・OO年度個資盤點清冊	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。

稽核項目 **4** **個人資料蒐集、處理及利用之內部管理程序**
（零售業個人資料檔案安全維護管理辦法第7條第2項）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司已訂定個資蒐集、處理及利用之內部管理程序。 參照附件 ・個資蒐集 ・處理及利用之內部管理程序作業書	請檢附個人資料蒐集、處理及利用之內部管理程序文件。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司每年定期執行個資盤點作業，對於無保存必要之個資進行適當處置。 參照附件 ・OO年度個資盤點清冊、處置紀錄	請檢附最近一次檢視紀錄以及相關處置紀錄。

稽核項目 5 蒐集、處理、利用作業

（零售業個人資料檔案安全維護管理辦法第8條第1項）

稽核內容	自評結果	說明（實作建議）	備註
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？ 一、本公司名稱。 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、當事人依個人資料保護法第3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？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂有個資告知聲明書，發布於本公司管網，內容已載明法定應告知事項。 參照附件 ・個資告知聲明書 ・官網隱私權政策	告知當事人之佐證紀錄。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
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？ 一、本公司名稱。 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、當事人依個人資料保護法第3條規定得行使之權利及方式。	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂有個資告知聲明書，已於首次利用前，向間接蒐集的當事人寄送電子郵件進行告知，內容已載明法定應告知事項。 參照附件 ・個資告知聲明書 ・官網隱私權政策	告知當事人之佐證紀錄。

稽核項目 6 **資料傳輸**

（零售業個人資料檔案安全維護管理辦法第8條第3項）

稽核內容	自評結果	說明（實作建議）	備註
6.1 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 ☐ 不符合 ☐ 不適用	本公司進行個資國際傳輸前，已檢視及遵循主管機關要求。 參照附件 ・資料傳輸管理程序書	請進行說明。（中央目的事業主管機關得限制非公務機關為國際傳輸個人資料。）
6.2 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 ☐ 不符合 ☐ 不適用	本公司進行個資國際傳輸前，已於官網公告隱私權政策，告知當事人擬傳輸之地區。 參照附件 ・個資告知聲明書 ・官網隱私權政策	請提出告知當事人之佐證紀錄。

稽核項目 **7** **資料安全管理**

（零售業個人資料檔案安全維護管理辦法第8條第2項及第9條第1款、第2款、第5款、第6款、第7款）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司已建立資料管理機制，並依業務需要及性質設定帳號權限。 參照附件 ・資料安全管理作業書 ・個資系統權限清單	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 ☐ 不符合 ☐ 不適用	本公司每年定期檢視所屬人員帳號權限。 參照附件 ・個資系統權限申請表單 ・帳號權限審查紀錄	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他存放媒介物時，應妥善保管個人資料之儲存媒介物？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已要求所屬人員妥善保管個資之儲存媒介物。 參照附件 ・資料安全管理作業書 ・保管紀錄	請說明並檢附資料安全管理措施。
7.4 於傳輸個人資料時，是否依不同傳輸方式（包括但不限於：實體紙本、電子郵件、網際網路、專線），採取適當之安全措施？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司針對紙本資料透過掛號方式，電子檔案透過電子郵件加密傳送，已分別採取適當安全措施。 參照附件 ・資料傳輸管理程序書 ・個資傳輸紀錄	請說明傳輸個人資料時，採取之安全措施，並檢附佐證資料。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
7.5 **有加密必要之個人資料，是否於蒐集、處理或利用時，採取適當之加密措施？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司針對涉及具有加密必要的資訊（如身份證字號、信用卡資料等），已透過SSL/TLS加密協議、AES加密算法處理。 參照附件 ・安全管理作業書 ・遮罩化處理介面或加密儲存的系統截圖	請說明對個資進行加密之方式，並檢附佐證資料。
7.6 **有備份必要之個人資料，是否有採取適當之保護措施？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司針對涉及具有備份必要的個資，已實施備份加密、存取權限控管、異地備援等管理機制。 參照附件 ・安全管理作業書 ・存取權限清單	請說明所採取之保護措施，並檢附佐證資料。

稽核項目 **8** **人員管理**
（零售業個人資料檔案安全維護管理辦法第9條第3款及第4款）

稽核內容	自評結果	說明（實作建議）	備註
8.1 **是否與所屬人員約定個人資料保管及保密義務？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已與所屬人員簽定個資保密切結書。 參照附件 ・保密切結書	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。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司要求所屬人員離職時須完成辦理交接。 參照附件 ・離職交接檢核表	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。

稽核項目 **9** **安全措施**
（零售業個人資料檔案安全維護管理辦法第10條）

稽核內容	自評結果	說明（實作建議）	備註
9.1 資通訊系統是否採行使用者身分認證機制？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司保有個資之資通訊系統已採行使用者身分確認及保護機制。 參照附件 ・資料安全管理作業書	請說明使用者身分認證機制，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 ☐ 不符合 ☐ 不適用	本公司保有個資之資通訊系統已採行個資隱碼機制。 參照附件 ・資料安全管理作業書 ・隱碼設定規則 ・系統化面截圖	請說明個人資料顯示之隱碼機制，並檢附相關佐證。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
9.3 **是否定期檢視蒐集、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，並因應系統漏洞所造成之威脅？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司針對涉及個資之電腦、相關設備或系統，每年定期執行弱點掃描、滲透測試等檢測，並針對發現之風險立即修復。 參照附件 ・資料安全管理作業書 ・檢測報告	請說明定期檢視之週期，及說明如何因應系統之弱點或漏洞，並檢附佐證資料。
9.4 **是否對於與網路相連而存有個人資料之資通訊系統，隨時更新並執行防毒軟體，及定期執行惡意程式檢測？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司為確保與網路相連的資通訊系統安全，將確保系統中的防毒軟體為最新版本，並即時更新病毒碼；亦針對系統定期執行惡意程式檢測，檢查系統中可能存在的潛在威脅，並即時處理檢測結果。 參照附件 ・資料安全管理作業書 ・防毒軟體授權書 ・檢測報告	請檢附更新與執行防毒軟體及執行惡意程式檢測之佐證。
9.5 **是否採行防止外部網路入侵對策，並定期更新？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司保有個資之資通訊系統已採行外部網路入侵對策。 參照附件 ・資料安全管理作業書 ・防火牆及防毒軟體授權證明書	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 ☐ 不符合 ☐ 不適用	本公司保有個資之資通訊系統已採行端點偵測及應變機制。 參照附件 ・資料安全管理作業書 ・偵測系統軟體授權證明書	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。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司每年定期執行個資事故演練及檢討改善。 參照附件 ・資料安全管理作業書 ・個資事故演練紀錄書	請說明使用真實個資進行測試時之相關規範，並檢附相關佐證。
9.8 **處理個人資料之資通訊系統有變更時，是否有確保其安全性未降低？**	☐ 符合 ☐ 不符合 ☐ 不適用	公司針對涉及個資之資通訊系統在進行軟硬體升級、架構調整或其他變更時，將進行風險評估，確認系統安全性不受影響或已採取補強措施，並驗證變更後系統的安全性。 參照附件 ・資料安全管理作業書 ・風險評估報告 ・驗證報告	請說明於系統變更時（例如：版本更新、作業系統更新、更換系統等），如何確保安全性未降低。
9.9 **是否有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？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司針對涉及個資之資通訊系統，每月（或每季）定期進行檢視系統是否有異常使用情形，並檢查存取紀錄是否有未經授權的存取。 參照附件 ・資料安全管理作業書 ・檢視報告 ・異常事件處理紀錄	請說明定期檢視之週期，並檢附相關佐證。
9.10 **本辦法第10條第1項各款規定之措施，是否有定期檢討改善？**	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂定資料安全管理作業程序，每年定期召開會議檢討現行的保護措施，並根據檢討結果進行必要的改善。 參照附件 ・資料安全管理作業書 ・會議紀錄 ・改善報告	請說明定期檢討之週期，並檢附相關佐證資料。

稽核項目 10 認知宣導及教育訓練

（零售業個人資料檔案安全維護管理辦法第11條）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司每年定期辦理員工個資保護教育訓練。 參照附件 ・教育訓練課程講義 ・簽到表 ・測驗成績紀錄	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。

稽核項目 11 事故之預防、通報、應變及改善機制

（零售業個人資料檔案安全維護管理辦法第12條）

稽核內容	自評結果	說明（實作建議）	備註
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？ 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錄表」通報經濟部。 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。	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已訂定個資事故通報應變機制，並載明法定事項。 參照附件 ・個資事故通報應變作業書	請檢附個資事故之預防、通報及應變機制之管理文件。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司於前次事故發生時，已依個資事故通報應變機制及時處理。 參照附件 ・事故通報紀錄表	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 ☐ 不符合 ☐ 不適用	本公司於前次事故發生後，已配合主管機關調查並函報事故處理報告。 參照附件 ・事故處理報告	請檢附事故處理報告及改善措施之佐證資料。

稽核項目 **12** **設備安全管理措施**
（零售業個人資料檔案安全維護管理辦法第13條）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司針對紙本個資檔案已訂定管理程序並妥善維護管理設施。 參照附件 ・資料安全管理作業書 ・檔案室／櫃之調閱紀錄	請說明個資檔案安全保護措施及管理文件。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司針對存放電子化個資檔案之電腦設備，已訂定管理程序並配置安全防護系統。 參照附件 ・資料安全管理作業書 ・安全防護系統授權書	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 ☐ 不符合 ☐ 不適用	本公司已訂定個資銷毀程序，電腦設備及其他儲存媒介物需經報廢審核作業確認無個資外洩疑慮。 參照附件 ・資料銷毀作業書 ・報廢單	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。

稽核項目 **13** **資料安全稽核機制**

（零售業個人資料檔案安全維護管理辦法第14條）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司已指定查核人員，並每年定期進行稽核作業。 參照附件 ・稽核報告	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。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司已依前次稽核結果發現缺失進行改善。 參照附件 ・改善報告	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 ☐ 不符合 ☐ 不適用	本公司負責稽核之查核人員未兼任安全維護計畫專責業務。 參照附件 ・個資管理單位組織圖 ・成員表 ・權責分工辦法	請檢附最近一次稽核之小組成員名單。

稽核項目 **14** **使用紀錄、軌跡資料及證據保存**

（零售業個人資料檔案安全維護管理辦法第15條）

稽核內容	自評結果	說明（實作建議）	備註
14.1 是否留存個人資料使用紀錄至少5年？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司對於個資使用紀錄均留存5年。 參照附件 ・資料安全管理作業書 ・個資使用紀錄 ・調閱紀錄	請說明留存個人資料使用紀錄之作業方式，並提供留存個人資料使用紀錄至少5年的佐證。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司對於軌跡資料或其他相關之證據資料均留存5年。 參照附件 ・資料安全管理作業書 ・系統存取紀錄 ・軌跡資料（LOG）相關日誌檔案	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。

稽核項目 **15** **業務終止後，個人資料處理方法**
（零售業個人資料檔案安全維護管理辦法第16條）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司針對業務終止後，無保有必要之個資進行銷毀，並將銷毀紀錄留存5年。 參照附件 ・業務終止個資處理作業書 ・銷毀紀錄	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 ☐ 不符合 ☐ 不適用	本公司針對業務終止後，仍具保有必要之個資進行移轉，並將移轉紀錄留存5年。 參照附件 ・業務終止個資處理作業書 ・移轉紀錄	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。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司針對業務終止後，無保有必要之個資進行刪除、停止處理或利用，並將刪除紀錄留存5年。 參照附件 ・業務終止個資處理作業書 ・刪除紀錄	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。

稽核項目 **16** **個人資料安全維護之整體持續改善方案**

（零售業個人資料檔案安全維護管理辦法第17條、個人資料保護法施行細則第12條第2項第3款）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司每年定期召開個資管理會議定期檢視並配合法令修正安維計畫。 參照附件 ・年度個資管理會議紀錄 ・安維計畫修訂文件紀錄	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 ☐ 不符合 ☐ 不適用	本公司每年定期執行風險評估及風險評鑑作業。 參照附件 ・風險管理作業書 ・風險評估表 ・風險評鑑表	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。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
16.3 是否依據風險分析之結果訂定適當之管控措施？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已依據前次風險評鑑結果，針對高風險作業採取適當管控及因應措施。 參照附件 ・風險管理作業書 ・高風險回應計畫	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。

稽核項目 17 當事人權利行使

（零售業個人資料檔案安全維護管理辦法第18條）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司已訂定當事人權利行使程序。 參照附件 ・受理當事人權利行使作業書 ・當事人權利行使申請表	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 ☐ 不符合 ☐ 不適用	本公司針對當事人權利行使具有法定例外事由，向當事人通知有關拒絕理由。 參照附件 ・本年度當事人權利行使清單 ・拒絕當事人權利行使之通知信	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。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司均於法定處理期限受理當事人權利行使。 參照附件 ・受理當事人權利行使作業書 ・本年度當事人權利行使清單	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，如依個人資料保護法第14條規定酌收必要成本費用，是否進行告知？	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已告知行使查詢或請求閱覽、製給複製本，將酌收必要成本費用。 參照附件 ・受理當事人權利行使作業書 ・網站公告	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 ☐ 不符合 ☐ 不適用	本公司已提供聯絡窗口及聯絡方式供當事人權利行使。 參照附件 ・受理當事人權利行使作業書 ・網站公告	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。

稽核項目 **18** **委託作業**
（零售業個人資料檔案安全維護管理辦法第19條）

稽核內容	自評結果	說明（實作建議）	備註
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？ 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、受託者就個人資料保護法第12條第2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。 五、委託機關如對本公司有保留指示者，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。 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。 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。	☐ 符合 ☐ 不符合 ☐ 不適用	本公司與委外廠商已簽訂委外契約，並明定法定事項及監督權限。 參照附件 ・委外個資保護條款 ・委外廠商個資安全維護聲明書	請檢附個資委外之廠商清單及合約文件。

稽核內容	自評結果	說明（實作建議）	備註
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「零售業個人資料檔案安全維護管理辦法」之規定。	☐ 符合 ☐ 不符合 ☐ 不適用	本公司已於委託契約要求委外廠商遵守安維辦法之規定。 參照附件 ・委外個資保護條款 ・委外廠商個資安全維護聲明書	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 ☐ 不符合 ☐ 不適用	本公司每年定期執行委外監督作業，並做成委外稽核報告。 參照附件 ・委外監督稽核表	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。

稽核項目 19 行銷規範

（零售業個人資料檔案安全維護管理辦法第20條）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司利用個資行銷，已明確告知公司登記名稱及個資來源。 參照附件 ・個資告知聲明書	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。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司已提供客服專線，供當事人免費拒絕行銷。 參照附件 ・拒絕接受行銷公告	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 ☐ 不符合 ☐ 不適用	本公司接獲當事人表示拒絕行銷後，已立即停止利用並對內公開周知。 參照附件 ・客服處理記錄 ・行銷名單刪除紀錄	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。

稽核項目 **20** **個人資料庫之共享使用**

（個人資料保護法第8條及第9條）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司與其他關係企業共享使用客戶個人資料庫，並明確告知法定事項及蒐集主體。 參照附件 ・個資告知聲明書	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。

（續下頁）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司有使用其他關係企業之客戶個人資料庫，並明確告知法定事項及個資來源。 參照附件 ・個資告知聲明書	請檢附於處理及利用前告知當事人之佐證。

稽核項目 **21** **使用資通訊系統蒐集、處理或利用個人資料**

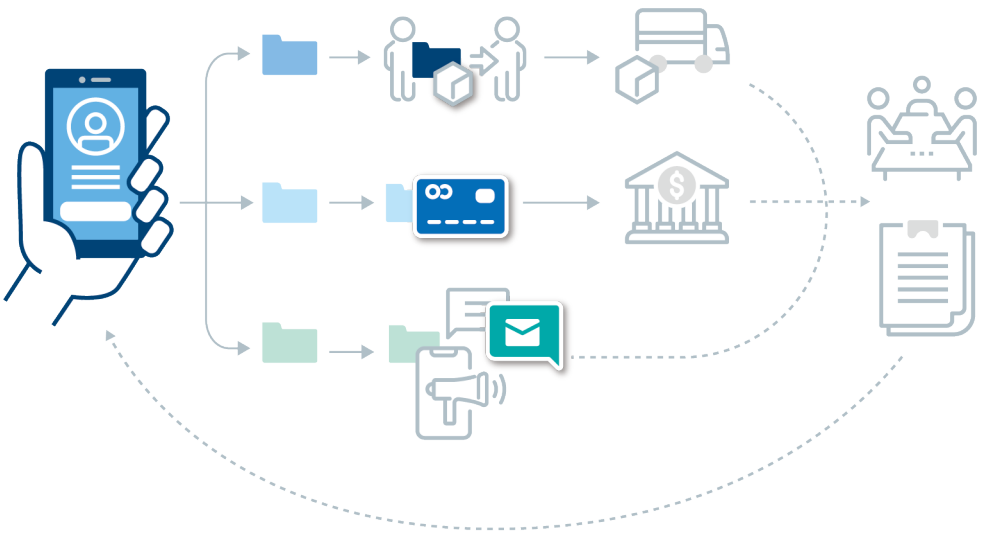
（中央目的事業主管機關依個人資料保護法第22條第1項為職權調查之事項）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司保有個資之資通訊系統已取得ISO 27001資安認證、TPIPAS個資管理認證。 參照附件 ・ISO證書 ・資料隱私保護標章（dp.mark）	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。

稽核項目 **22** **個人資料庫之共享使用**

（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款及第9款）

稽核內容	自評結果	說明（實作建議）	備註
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 ☐ 不符合 ☐ 不適用	本公司已建立雲端的存取控制權限、雲端資料加密及備份，並定期檢視及更新。 參照附件 ・雲端管理作業手冊 ・雲端存取紀錄	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



伍、淺談社交工程防範對個人資料保護之重要性

2022年9月，某知名公司之電商平台，因外包商約聘員工個人裝置遭到偽造訊息社交工程攻擊成功，感染惡意程式，致其帳密外流，駭客自地下網站購得後順利登入網站平台，並進入公司其他內部系統，癱瘓系統運作及導致部分個人資料遭到竊取。

上述案例駭客藉由透過典型的社交攻擊手法，不當竊取個資機敏資料，並造成公司運作損害。社交工程係透過操控人性弱點來獲取敏感訊息，其破壞力不容小覷。因此，了解什麼是社交工程、如何預防社交工程以及如何通過社交工程演練來加強防護，對於保護個人資料具有極其重要的意義。

何謂社交工程

社交工程（Social Engineering）是指攻擊者利用人性的弱點，透過心理操控來獲取機密訊息或進行其他惡意活動的一種攻擊方式。與傳統的技術攻擊不同，社交工程主要依賴於欺騙、誤導和操縱受害者，而非攻擊技術系統本身。

常見的社交工程手法

釣魚攻擊（Phishing）

攻擊者通過偽裝成可信的機構或個人，發送看似合法的電子郵件或訊息，誘使受害者點擊惡意連結或提供敏感訊息。

冒充身份（Pretexting）

攻擊者偽裝成某個可信的人物或機構，編造一個合理的故事，欺騙受害者透露機密訊息。

語音詐騙（Vishing）

使用電話進行的釣魚攻擊，攻擊者假冒合法機構或個人，透過電話誘騙受害者提供敏感訊息。

垃圾訊息（Spam）

攻擊者通過大量發送垃圾郵件，嘗試從中尋找容易上當的受害者，進行訊息收集或散播惡意軟體。

如何預防社交工程

防範社交工程攻擊需要綜合採取技術和管理措施，提升個人及組織的安全意識和應對能力。

1. 提高安全意識

（1）定期培訓

企業和個人應定期參加資訊安全培訓，了解最新的社交工程攻擊手段和防範措施，提升自我防護能力。

（2）安全宣導

透過公司內部公告、宣導教材和安全講座，提醒員工注意各種社交工程攻擊的風險，並教導如何識別和應對。

2. 技術防護措施

（1）電子郵件過濾

使用先進的電子郵件過濾技術，攔截釣魚郵件和垃圾郵件，減少員工接觸到這些攻擊的機會。

（2）多因素認證（MFA）

啟用多因素認證，提高帳戶安全性，即使攻擊者獲得了密碼，也難以進入系統。

（3）安全更新

定期更新系統和應用程式的安全補丁，修補已知漏洞，防止攻擊者利用技術手段輔助社交工程攻擊。

3. 管理和制度措施

（1）資訊分類和控制

將公司內部的資訊按重要性分類，限制敏感資訊的存取權限，確保只有經授權的人員才能存取關鍵數據資料。

（2）事件應對流程

制定明確的安全事件應對流程，當發現可疑行為時，員工知道如何報告和處理，降低攻擊成功的可能性。

4. 社交工程演練

社交工程演練是一種有效的防護措施，通過模擬真實的攻擊場景，測試員工對社交工程攻擊的應對能力，從而提升整體防護水平。

（1）演練的重要性

A. 實戰檢驗

透過演練，能夠檢驗員工對各類社交工程攻擊的辨識和應對能力，找出防護中的薄弱環節。

B. 提高警覺性

經過演練的員工，對社交工程攻擊有更高的警覺性，能夠在真實情況下更有效地防範攻擊。

C. 改進安全措施

演練後的總結和回饋，有助於改進現有的安全政策和措施，提升整體安全防護水平。

（2）演練的實施

A. 制定演練計劃

針對不同類型的社交工程攻擊，制定詳細的演練計劃，包括目標、方法和預期結果。

B. 模擬攻擊場景

創造真實的攻擊場景，例如釣魚郵件、冒充電話等，模擬真實的攻擊手法，測試員工的反應。

C. 評估和回饋

演練結束後，對演練過程進行評估，總結員工的表現，並提供具體的改進建議和培訓內容。

D. 持續改進

根據演練結果，持續改進安全策略和措施，並定期進行演練，確保員工保持高水平的警覺性和應對能力。

結論

社交工程攻擊利用人性的弱點，透過心理操控來獲取敏感訊息，其威脅不容忽視。藉由提高安全意識、採取技術和管理措施，以及定期進行社交工程演練，能夠有效防範此類攻擊，保護個人資料的安全。綜合運用多種防護手段，零售業者和個人可以建立一個全面的安全防護體系，確保在面對日益複雜的社交工程攻擊時，能夠有效保護敏感資訊，維護企業的聲譽和信任。

陸、資訊安全技術對於個人資料保護的關鍵作用

2023年10月，某自動化設備設計、銷售供應商因駭客利用網路設備裝置韌體漏洞，透過VPN連線執行遠端主機桌面連線軟體，藉由高權限帳號在各主機展開橫向攻擊，進行程式安裝、刪除Log紀錄，並將檔案加密進行勒索，導致公司業務無法正常運作。

上述案例駭客藉由設備安全漏洞未進行定期即時修補，進而有機會發動一連串資安攻擊事件，不但使公司業務癱瘓，更可能導致客戶資料被不當竊取。在數位化時代，資訊安全技術的發展變得尤為重要。隨著網路技術的不斷進步，個人資料的外洩風險也不斷增加。台灣在這方面也不例外，隨著網路使用者數量的增長，保障個人資料安全的需求也日益迫切。本文將從使用者端防護、網路閘道防護、伺服器防護以及軟體開發防護四個面向，探討資訊安全技術對於個人資料保護的重要性。

一、使用者端防護

使用者端防護是資訊安全的第一道防線，因為大部分的安全漏洞都源於使用者自身的疏忽或誤操作。以下幾個方面的防護措施可以有效提升使用者端的安全性：

1. 高強度密碼管理

高強度密碼是保護個人資料的基本措施之一。使用者應該選擇包含大小寫字母、數字和特殊符號的複雜密碼，並避免使用與個人資料相關的簡單密碼。此外，定期更換密碼並避免

在多個網站使用相同的密碼也非常重要。密碼管理工具可以幫助使用者生成並管理高強度密碼，進一步提升密碼安全性。

2. 雙因子驗證

雙因子驗證（Two-Factor Authentication, 2FA）是一種增加帳號安全性的有效措施。透過要求使用者在輸入密碼後，再提供另一層驗證（如簡訊驗證碼或APP生成的驗證碼），可以有效減少帳號被盜的風險。許多網站和應用程式現在都提供雙因子驗證功能，使用者應該積極開啟此功能。

3. 防毒軟體

防毒軟體能夠偵測並移除惡意軟體，保護使用者的電腦不受病毒、木馬和間諜軟體的侵害。現代防毒軟體通常還包含防火牆功能，能夠監控並阻止可疑的網路活動。定期更新防毒軟體並進行全盤掃描是保持使用者端安全的關鍵。

4. 教育與意識提升

使用者的安全意識是防護個人資料的重要一環。定期參加安全培訓，了解最新的網路詐騙手法及防範措施，可以幫助使用者更好地應對潛在的威脅。學會識別釣魚郵件、避免點擊可疑連結，以及妥善處理敏感資訊，都是提升個人資料保護的重要手段。

二、網路閘道防護

網路閘道是連接內部網路與外部網路的樞紐，也是企業和個人資料安全的第二道防線。透過強化網路閘道的防護措施，可以有效阻止外部威脅進入內部網路。

1. 防火牆

防火牆是保護網路閘道的基本設備，通過過濾進出網路的流量來防止未經授權的存取。現代防火牆通常具有深度封包檢測（Deep Packet Inspection, DPI）功能，可以檢查封包內容，識別並阻擋潛在的威脅。配置嚴格的防火牆規則，並定期更新防火牆軟體，是確保網路閘道安全的關鍵。

2. 入侵偵測與防禦系統

入侵偵測系統（Intrusion Detection System, IDS）和入侵防禦系統（Intrusion Prevention System, IPS）能夠監控網路流量，識別並阻止可疑的活動。IDS通常用於偵測並報告潛在的入侵行為，而IPS則可以主動阻止這些行為。透過結合使用這兩種系統，可以提供更加全面的網路防護。

3. VPN（虛擬私人網路）

VPN技術可以加密網路通信，保護使用者的數據免受攔截和竊聽。在使用公共Wi-Fi或遠端連線工作時，VPN能夠提供額外的安全保護。選擇可靠的VPN服務供應商，並配置高強度加密方式，是保障通信安全的有效措施。

4. Web應用防火牆

Web應用防火牆（Web Application Firewall, WAF）專門用於保護Web應用程式免受各類攻擊，如SQL注入、跨站腳本攻擊（XSS）等。WAF能夠過濾和監控HTTP請求，識別並阻止惡意流量，從而保護Web應用程式及其背後的個人資料安全。

三、伺服器防護

伺服器是存儲和處理大量個人資料的核心設備，因此對其進行嚴格的防護是確保資料安全的關鍵。

1. 伺服器硬體防護

伺服器的物理安全是防護的基礎。應將伺服器安置在受控的數據中心，並採取嚴格的訪問控制措施，如生物識別、門禁系統等。此外，伺服器應配備不斷電系統（UPS），以確保在電力中斷時仍能正常運行，避免數據損失。

2. 操作系統安全

伺服器操作系統的安全性直接影響到整體的資訊安全。應定期更新操作系統，修補安全漏洞，並移除不必要的服務和應用程式。配置嚴格的權限管理，確保只有授權使用者才能存取伺服器上的敏感資料。

3. 資料加密

對存儲在伺服器上的個人資料進行加密，可以有效防止資料外洩。選擇高強度加密演算法，並確保加密金鑰的安全存儲，是保障資料安全的關鍵。除了靜態資料加密（Data-at-Rest Encryption），也應考慮對傳輸中的資料進行加密（Data-in-Transit Encryption）。

4. 定期備份與恢復計畫

定期備份資料並制定完善的復原計畫，可以在資料遭受破壞或滅失時，迅速復原系統運行。備份資料應存儲在安全的異地位置，並定期進行回復測試，以確保備份的有效性。

四、軟體開發防護

軟體開發過程中的安全防護同樣至關重要，因為軟體漏洞可能成為攻擊者入侵系統的切入點。

1. 安全程式碼開發

在開發軟體時，應遵循安全程式碼開發，如避免使用不安全的函數、檢查輸入有效性、使用參數化查詢防止SQL注入等。安全程式碼開發可以減少軟體漏洞，提高整體安全性。

2. 安全測試

在軟體開發過程中，應涵蓋多樣的安全測試，包括靜態程式碼分析（Static Code Analysis）、動態程式碼分析（Dynamic Code Analysis）和滲透測試（Penetration Testing）。這些測試可以幫助發現並修復潛在的安全漏洞，提升軟體的安全性。

3. 持續整合與持續交付（CI／CD）

持續整合與持續交付（CI／CD）流程能夠自動化軟體開發、測試和部署過程，確保每次程式碼變更都經過嚴格的測試。透過在CI／CD管道中加入安全測試，可以及時發現並修復安全漏洞，提高軟體交付的安全性。

4. 教育訓練

開發團隊的安全意識和技能直接影響軟體的安全性。定期進行教育訓練，了解最新的安全威脅和防範措施，並培養安全程式碼撰寫習慣，可以有效提升開發團隊的安全水準。

結論

資訊安全技術對於個人資料保護的關鍵作用不容忽視。從使用者端防護、網路閘道防護、伺服器防護到軟體開發防護，每一個環節都至關重要。隨著網路威脅的不斷演變，我們必須持續提升安全技術和意識，才能更好地保護個人資料的安全。在台灣，隨著政府和企業對資訊安全的重視程度不斷提高，相信未來的個人資料保護將會更加完善和可靠。

柒、如何確保伺服器設備安全以強化個資保護

2022年12月，某VPN設備廠商因其產品存在重大安全漏洞，導致全球近五萬台VPN設備登入資訊遭到非法竊取，同時國內部分零售業者及協助業者開發維運之系統廠商，因採用該設備，未即時更新廠商提供之安全漏洞修補程式，導致遭受駭客攻擊。

上述案例係駭客藉由伺服器設備安全漏洞未修補韌體程式，進而展開攻擊，造成資安及個資外洩事件。在數位化的商業環境中，零售業者（例如百貨公司、超市和網購平台）都依賴伺服器來管理、儲存和處理大量的顧客資料，包括姓名、地址、聯絡方式及支付資訊等。伺服器的安全性直接關係到這些敏感資料的保護，一旦發生安全漏洞或資料外洩，不僅會對顧客造成損失，也會嚴重損害企業的聲譽和信任。因此，零售業者必須採取多層次的伺服器安全措施，來確保顧客資料的保護。本文將探討如何透過伺服器的各種防護措施，來加強個資保護。

一、強化伺服器的安全配置

1. 安全配置管理

伺服器的安全配置是保護資料的基礎。零售業者應該採取以下措施：

- **禁用不必要的服務和端口：**關閉所有不必要的服務和端口，只保留必要的運行服務，減少攻擊面。
- **最小權限原則：**設定伺服器使用者和應用程式的權限時，遵循最小權限原則，即僅賦予執行其職責所需的最小權限，防止因權限過大導致的安全風險。

2. 定期更新和補丁管理

- **及時更新補丁：**伺服器操作系統和應用程式經常會發佈安全補丁，用來修補已知的漏洞。企業應制定定期更新計劃，及時安裝這些補丁，以防止攻擊者利用已知漏洞入侵系統。
- **自動更新工具：**利用自動更新工具，確保伺服器在有新補丁發佈時能夠及時更新。

二、資料加密及保護

1. 資料加密

- **靜態資料加密：**對存儲在伺服器上的敏感資料進行加密。這樣，即使硬碟被盜或伺服器被非法存取，攻擊者也無法讀取加密的資料。
- **傳輸資料加密：**使用TLS／SSL協議對網絡傳輸中的資料進行加密，確保數據在傳輸過程中的機密性和完整性。

2. 金鑰管理

- **安全存儲金鑰：**金鑰是加密系統的核心，必須妥善保管。使用硬體安全模組（HSM）或金鑰管理服務來存儲和管理金鑰。
- **定期更換金鑰：**制定金鑰輪替策略，定期更換加密金鑰，以增加資料的安全性。

三、存取控制和監控

1. 存取控制

- **多因素認證（MFA）：**除了使用者名和密碼之外，還需提供其他認證方式，如動態密碼（OTP）或生物識別，以加強系統的安全性。
- **角色基礎存取控制（RBAC）：**根據使用者的職責分配適當的權限，確保每個使用者只能存取其工作所需的最小數量的資料和資源。

2. 日誌監控

- **詳細日誌記錄：**記錄所有的存取和操作行為，包括登入嘗試、資料存取和修改操作等。
- **實時監控和警報：**使用安全資訊和事件管理（SIEM）系統，實時監控日誌，及時發現異常行為，並設置警報機制，在發生異常時迅速通知相關人員進行處理。

四、災害復原和備份

1. 定期備份

- **資料備份策略：**制定並執行定期備份策略，確保所有重要資料都有備份，包括完整備份和差異備份。
- **異地備份：**將備份資料存儲在異地，以防止本地災害（如火災、洪水等）導致數據同時遺失。

2. 災害復原計劃

- **制定應急預案：**制定詳細的災害復原計劃，包括責任分工、操作流程和聯絡方式，確保在發生災害時能夠迅速恢復業務運行。
- **定期演練：**定期進行資料復原測試，檢查備份資料的可用性和復原過程的有效性，確保災害發生時能夠迅速恢復。

五、應用程式和軟體安全

1. 安全程式碼開發

- **安全程式碼標準：**制定並遵循安全程式碼標準，確保開發過程中避免常見的安全漏洞，如SQL注入和跨站腳本攻擊（XSS）。
- **程式碼審查：**進行程式碼審查，確保所有程式碼在上線之前經過嚴格的安全檢查，及時發現和修復潛在的漏洞。

2. 持續安全測試

- **靜態程式碼分析：**使用靜態程式碼分析工具檢查程式碼中的安全漏洞，確保程式碼的安全性。
- **動態應用測試：**在運行環境中測試應用程式，模擬真實攻擊，檢查安全性。
- **滲透測試：**聘請專業的安全測試人員進行滲透測試，發現並修復應用程式中的高危險漏洞，確保系統的整體安全。

六、實體安全和環境控制

1. 實體安全

- **存取控制：**限制對伺服器和資料中心的存取，只有授權人員才能進入。使用門禁系統、生物識別技術等手段加強安全。
- **監視器監控：**在伺服器和資料中心安裝監視器監控系統，隨時監控存取情況，並記錄所有進出人員的活動。

2. 環境控制

- **溫度和濕度控制：**伺服器對溫度和濕度有嚴格要求，應配置專業的空調設備，保持適當的運行環境。
- **電力保護：**配置不斷電系統（UPS）和備用發電機，確保在斷電時伺服器能夠正常運行，不會因為電力中斷導致數據遺失或損壞。

七、供應鏈及第三方管理

1. 供應商安全評估

- **安全認證：**選擇通過ISO 27001、PCI DSS等國際安全認證的供應商，確保其具備合格的安全管理能力。
- **安全評估：**對供應商進行安全評估，檢查其安全政策、措施及實作，確保其符合自身的安全要求。

2. 合約管理及持續監控

- **安全條款：**在與供應商的合約中明確規定安全責任和義務，包括資料保護要求及違約責任。
- **持續監控：**定期審查供應商的安全措施，確保其持續符合合約要求和安全標準。

結論

在數位時代，零售業者面臨著嚴峻的資訊安全挑戰。透過強化伺服器的安全配置、資料加密及保護、存取控制和監控、災害復原和備份、應用程式和軟體安全、實體安全和環境控制以及供應鏈及第三方管理，零售業者可以建立一個多層次的資訊設備安全防護體系，有效保障顧客的個人資料安全。在不斷變化的安全環境中，零售業者需要持續改進和更新其安全策略，確保能夠及時應對新興的安全威脅，保護顧客的個人資料，維護企業的聲譽和信任。透過這些措施，零售業者不僅能夠防止個資外洩，還能夠提升顧客對其品牌的信任度，進而促進業務的長遠發展。

捌、應如何進行資訊系統防護以避免個資外洩

2024年5月，某電腦硬體設備生產商，因其對外服務之網站平台程式存在資安漏洞，導致駭客透過安全性漏洞直接下達指令對資料庫進行備份後竊走包含集團業務資料、公司及供應商資料與50萬用戶個資。

上述案例駭客藉由應用軟體程式安全漏洞未進行檢測及修補，進而展開攻擊，造成資安及個資外洩事件。隨著電子商務的蓬勃發展和數位支付的普及，零售業者面臨的資訊安全威脅日益嚴峻。根據台灣資安專家的觀點，零售業者應該採取全方位的資訊系統防護措施，以確保顧客的個人資料不被外洩。本文將從風險評估、安全策略、使用者端防護、網路安全、伺服器與資料庫防護、軟體開發與應用防護、第三方服務管理以及應急預案與事故處理等多個層面，詳細探討零售業者應如何進行資訊系統防護。

一、風險評估與安全策略

1. 風險評估

風險評估是資訊安全管理的基礎。零售業者應首先對其資訊系統進行全面的風險評估，識別可能的安全漏洞和威脅來源。這包括硬體、軟體、網路架構以及人員操作等方面。風險評估應考慮到內部和外部的潛在威脅，如內部員工的疏忽或惡意行為、外部駭客的攻擊等。

2. 制定安全策略

根據風險評估結果，零售業者應制定一套完整的資訊安全策略。這些策略應包括資料存取控制、資料加密、系統更新和備份等方面的內容。資訊安全策略應該明確員工的職責和操作規範，並定期進行審查和更新，以應對不斷變化的安全威脅。

二、使用者端防護

1. 高強度密碼策略

零售業者應要求員工和顧客使用高強度密碼，包括大小寫字母、數字和特殊符號，並定期更換密碼。使用弱密碼是造成資料外洩的一大因素，因此，高強度密碼策略可以大幅降低密碼被破解的風險。

2. 雙重驗證

雙因子驗證（2FA）是一種增加帳號安全性的有效措施。對於需要處理敏感資料的帳號，零售業者應強制啟用雙因子驗證。這樣，即使密碼被盜，攻擊者也無法輕易進入系統。

3. 防毒軟體與防火牆

安裝並定期更新防毒軟體，可以有效防止惡意軟體入侵。此外，啟用防火牆可以阻止未經授權的連接和資料傳輸。這些措施能夠為使用者端提供基本的安全防護。

4. 教育與意識提升

員工是資訊安全的重要一環。零售業者應定期進行安全意識培訓，提高員工對釣魚郵件、社交工程攻擊等常見安全威脅的認識，並教導他們正確處理敏感資料的方法。這樣可以有效減少因人為操作失誤而導致的安全事故。

三、網路安全

1. 網路隔離

將內部網路與外部網路進行隔離，可以有效減少攻擊者通過外部網路入侵內部系統的風險。零售業者應將銷售系統、財務系統和其他關鍵系統分離，並使用虛擬區域網路（VLAN）來控制內部網路的存取。

2. VPN（虛擬私人網路）

對於遠端工作者或需要遠程存取內部系統的員工，應使用VPN技術加密網路通信，防止資料在傳輸過程中被攔截和竊聽。選擇可靠的VPN服務供應商，並配置強加密方式，是保障通信安全的有效措施。

3. 入侵偵測與防禦系統

入侵偵測系統（IDS）和入侵防禦系統（IPS）能夠監控網路流量，識別並阻止可疑的活動。IDS可以報告潛在的入侵行為，而IPS則能主動阻止這些行為。結合使用這兩種系統，可以提供更加全面的網路防護。

四、伺服器與資料庫防護

1. 伺服器安全配置

伺服器的安全配置至關重要。應定期更新伺服器操作系統和應用程式，修補已知漏洞。配置嚴格的權限管理，確保只有授權使用者才能存取伺服器上的敏感資料。此外，應移除不必要的服務和應用程式，以減少潛在被攻擊的可能性。

2. 資料加密

對存儲在伺服器和資料庫中的個人資料進行加密，可以有效防止資料外洩。選擇強加密算法，並確保加密密鑰的安全存儲，是保障資料安全的關鍵。靜態資料加密和傳輸中資料加密同樣重要，應同時實施以確保全面的資料保護。

3. 定期備份與恢復計畫

定期備份資料並制定完善的恢復計畫，可以在資料遭受破壞或遺失時，迅速恢復系統運行。備份資料應存儲在安全的異地位置，並定期進行恢復測試，以確保備份的有效性。

五、軟體開發與應用防護

1. 安全編碼實踐

在開發軟體時，應遵循安全編碼實踐，如避免使用不安全的函數、檢查輸入有效性、使用參數化查詢防止SQL注入等。這些措施可以減少軟體漏洞，提高整體安全性。

2. 安全測試

在軟體開發過程中，應進行多層次的安全測試，包括靜態代碼分析、動態代碼分析和滲透測試。這些測試可以幫助發現並修復潛在的安全漏洞，提升軟體的安全性。

3. 持續集成與持續交付（CI／CD）

持續集成與持續交付（CI／CD）流程能夠自動化軟體開發、測試和部署過程，確保每次代碼變更都經過嚴格的測試。通過在CI／CD管道中加入安全測試，可以及時發現並修復安全漏洞，提高軟體交付的安全性。

4. API安全

許多零售業者會通過API與第三方系統進行資料交換。因此，API的安全性至關重要。應採用安全的認證和授權機制，如OAuth，並對API請求進行輸入驗證和傳輸限制，防止惡意攻擊。

六、第三方服務管理

1. 供應商評估

零售業者在選擇第三方服務供應商時，應進行嚴格的安全評估。確保供應商具有完善的資訊安全管理體系，並能提供足夠的安全保障措施。簽訂服務合約時，應明確各方在資訊安全方面的責任和義務。

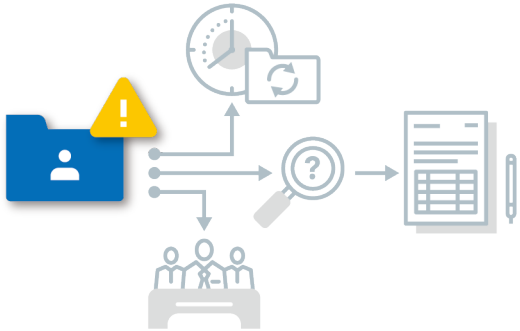
2. 監控與審查

對第三方服務的使用情況進行定期監控和審查，確保其符合安全政策和標準。發現問題時，應及時與供應商溝通並採取相應措施，確保資料的安全性。

七、事故通報應變程序與事故處理

1. 事故通報應變程序

制定詳細的事故通報應變程序，明確在發生資料外洩或其他安全事故時的處理流程和責任分工。事故通報應變措施應包括事故報告、事故當下之處理、資料恢復和事故調查等內容。



2. 定期演練

定期進行事故通報應變措施演練，檢視事故通報應變措施的可行性和有效性。透過演練，發現和改進文件措施中的不足，確保在真正發生事故時能夠迅速反應，將損失降到最低。

結論

零售業者面臨的資訊安全挑戰日益嚴峻，但只要採取全面的防護措施，從風險評估、安全策略、使用者端防護、網路安全、伺服器與資料庫防護、軟體開發與應用防護、第三方服務管理以及事故通報應變程序與事故處理等多個層面進行強化，就能有效避免個資外洩，提升消費者的信任。隨著資訊技術的發展和安全威脅的不斷演變，零售業者必須持續提升安全技術和意識，才能在激烈的市場競爭中立於不敗之地。

第2部分

個資手冊問與答QA

01 如何判斷公司是否適用零售業個人資料檔案安全維護管理辦法？

公司的營業模式是從事零售，且經營實體店面或先經營實體店面再增加網路銷售，資本額達新臺幣1,000萬以上，並有蒐集消費者（客人）個資或可取得交易對象個資，即適用零售業個人資料檔案安全維護管理辦法的規範。

關於從事零售的標準，公司可確認稅籍登記營業項目是否有：471至486（475除外）其中之一，或商工登記營業項目是否有：F201至F210（F208除外）其中之一、F301、F399。

02 如何制定一份個資安全維護計畫以符合所有法規，包含個資法與主管機關制定的個人資料檔案安全維護管理辦法等？

承第1題，如果公司經營的業務比較多元，有可能會同時適用多種個人資料檔案安全維護管理辦法，而且多數的管理辦法會要求公司制定「個人資料檔案安全維護計畫」（簡稱安維計畫），公司可以只制定一部安維計畫來因應所有的管理辦法，但要注意安維計畫的內容必須涵蓋所有規定，或對於同一事項採取較嚴格的規範。

03 界定個人資料範圍（個人資料盤點）時，除消費者／會員外，是否包含員工、合作廠商的個資？是否應進行風險評鑑？

進行個人資料盤點時，所盤點的個人資料檔案為公司保有的「全部」個資，因此除消費者與客戶的個資以外，也包含從員工或合作廠商等處蒐集到的個資，皆應納入盤點。同時，應對保有的個人資料進行風險評鑑，以找出風險點並降低至公司可接受範圍，方能落實適當風險管控措施。

上述表單及內容可至**經濟部商業發展署網站—個資保護專區**，或掃描右側QR碼前往下載參考。

經濟部商業發展署
個資保護專區

04 如何判斷個人資料的筆數？

承第3題，在個資盤點時，雖然只需填寫大概數量，但作為風險評估的基準，許多企業對如何計算個資數量有誤解。以下透過例子來說明：

假設有100位消費者加入某企業的會員，會員資料包含姓名、電話、地址、出生日期。這其中有50人購買商品，並填寫寄送資料（包含姓名、電話、地址），商品交由委外物流廠商配送。

- **常見誤解：**

  有些企業會將每位會員填寫的4個個資項目（姓名、電話、地址、出生日期）拆開來算，得出400筆個資；或是將會員資料和物流寄送資料合併，認為只需計算100筆個資。這些方式無法反映真實保有的個資數量，容易影響風險評估。

- **正確方式：**

  由於不同業務使用個資的目的不同，應根據特定目的及風險值相同或相近的資料來盤點。從業務流程角度出發，定義「一筆個資」。**即使資料重複使用，只要是不同業務流程或不同特定目的，應視為不同筆個資。**

  在這個例子中，100位消費者的會員資料是基於「加入會員」的特定目的蒐集的，因此應計算為100筆個資；另外，50位消費者購買商品並填寫寄送資料，基於「商品寄送」的特定目的，這50筆資料也應獨立計算。因此，企業目前保有的總個資數量應為150筆，而物流公司則保有50筆個資。

建議企業採用這種計算方式，能更準確反映實際保有的個資數量，並有助於個資管理和風險評估的精確性。

05 Cookie（網路識別碼）是否屬於個人資料？

依據國家發展委員會發布之《GDPR與我國個人資保護法之重點分析比較》（出自109年9月台灣經濟論衡第16卷第3期），其中關於個人資料定義之說明提及，我國個人資料保護法第2條對於個人資料之規範為得以直接或間接接方式識別該個人之資料，因此**Cookie也屬於個人資料之範圍**。

06 何謂個資業務終止？

我國個人資料保護法中所稱的業務終止，係指**業者因結束業務經營、交易完成、特定目的消失、契約或法令規定期限屆滿之情況。**因此企業於業務終止後，亦即個人資料蒐集之特定目的消失或期限屆滿後，原則上應依個人資料保護法第11條第3項之規定刪除、銷毀、停止處理或利用，但個資當事人往往無從知悉實際情況，為避免不必要的糾紛，建議業者應依照同條第2項規定，因業務終止而刪除其所蒐集、處理或利用的個人資料，留存相關紀錄；因業務終止而將個人資料移轉予他人者，應記錄其原因、對象、方法、時間、地點及受移轉對象得蒐集該個人資料之合法依據。原則上仍回歸特定目的實現或是期限屆至為根本規定。

07 消費者可否要求更正或刪除其個人資料，依據為何？企業確認要刪除消費者個資時，預計刪除的具體時間為何？

企業有義務確保個人資料的正確性，因此更正或補充個人資料是消費者的基本權利。**當消費者要求「停止蒐集、處理、利用或刪除」其個人資料時，企業應尊重這些要求，原則上應滿足，且不得事先放棄或限制這些權利。**除非有特定目的消失、期限到期、業務結束或資料蒐集違法等情況，企業應迅速刪除個人資料，並提供適當管道讓消費者行使這項權利。

根據「零售業個人資料檔案安全維護管理辦法」第7條第2項，企業應訂定內部管理程序，確保資料的蒐集、處理與利用符合特定目的及法定要件，並在目的消失或無保存必要時，應依個人資料保護法第11條第3項規定將資料刪除或適當處理。

由於個人資料型態與儲存方式各異，刪除期限會因資料處理狀況有所不同。企業需考量業務需求，但不應延長刪除時間超過必要之期間。若企業有自動化管理系統設定了合理的資料刪除週期，也能符合相關規定。

08 何謂自動化機器設備？

自動化機器設備是指能以自動化方式處理資料之設備，例如電腦、伺服器、資訊系統、通訊系統或雲端系統等。

09 有何與個人資料相關的紀錄需要保存，應該保存多久？

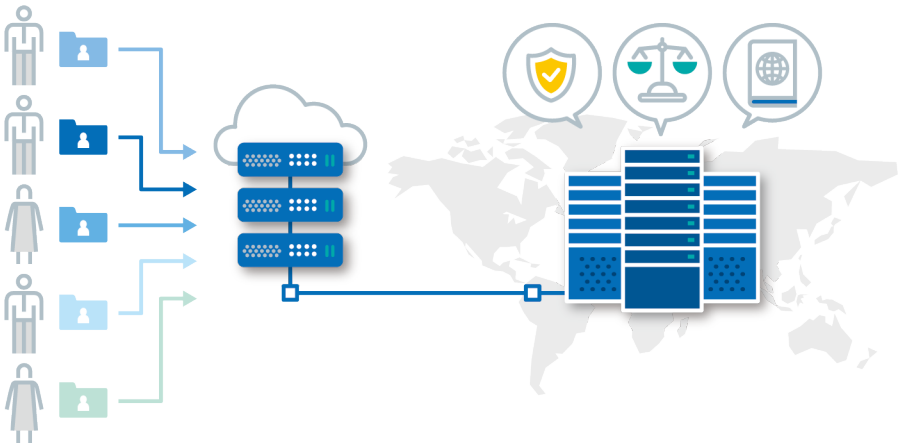
依據我國個資法施行細則第12條第2項第10款規定，使用紀錄、軌跡資料及證據保存，應與所欲達成之個人資料保護目的間，具有適當比例為原則。另外若企業適用經濟部所訂《零售業個人資料檔案安全維護管理辦法》，依據該辦法第15條及第16條的規定，自動化機器設備之軌跡紀錄（Log）及利用（使用）、銷毀、移轉和刪除個人資料都應保留相關紀錄，且**所有紀錄至少要保留五年。**

10 何謂個資國際傳輸（跨境傳輸）？

依據《個人資料保護法》第2條對於用詞之定義，國際傳輸是指將個人資料作跨境的處理或利用，例如將個人資料傳輸給位於其他國家、地區的個人或企業。按照《個人資料保護法》第21條之意旨，我國非公務機關原則上允許個人資料的國際傳輸，但例外中央目的事業主管機關得以下列各款原因限制之，於涉及國家重大利益、國際條約或協定有特別規定、接受國對於個人資料之保護未有完善法規，恐會損害個資當事人權益、以迂迴方法向第三國（地區）傳輸個人資料規避我國個資法等。同時，仍應留意產業別的主管機關是否有禁止國際傳輸的國家或地區，並且於蒐集資料時明確告知當事人。

11 使用雲端服務是否有涉及國際傳輸？

如果有公司有使用雲端傳輸或儲存個人資料，並且雲端服務提供者是將實體機房建置於境外，則會構成將個資進行國際傳輸。



12 如何有效管理與監督委外廠商？

實務上常見情形，例如A公司將商品運送服務委託B物流公司，並將消費者的姓名、電話號碼及地址資料提供予B物流公司。然而委外廠商有諸多不確定因素（例如管理制度、人事或作業流程等），較容易有風險發生，因此在委託他人蒐集、處理或利用個人資料時，委託機關應依個人資料保護法施行細則第8條規定對受託者為適當的監督。而監督可分為事前與事後，有若干可注意重點如下：

• 事前監督（選商前）

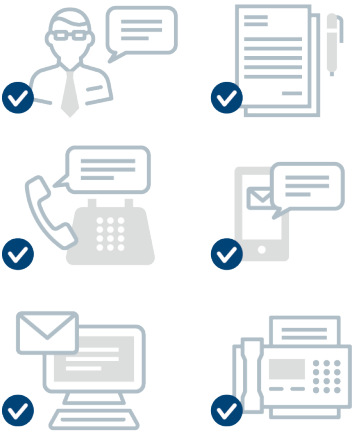
1. 建立適當的選商程序並遵循；
2. 透過委外契約與受託公司約定個資監督事項相關條款（應注意針對營業秘密等保密條款，並不屬於對個人資料有管理維護或監督的約定）；
3. 要求委外廠商取得公正第三方認證（例如導入臺灣個人資料保護與管理制度TPIPAS，並通過第三方公正驗證後，取得政府頒發的資料隱私保護標章dp.mark）；
4. 請受託公司針對內部情況提供自我檢核表，應確認有符合第8條第2項各款。

dp.mark 資料隱私保護標章

• 事後監督（選商後）

公司應依照雙方契約進行確實、定期且有效的監督，具體方式可採用現場稽核、書面審查或提供有效的公正第三方認證（例如有效的資料隱私保護標章等證明）等方式，作為確實有效的監督方法。縱使不幸發生個資事故，亦得以釐清責任歸屬。

13 何謂個資事故，發生個資事故後應如何通知客戶或消費者，是否可以寄發防詐騙簡訊或網站公告代替？



根據《個資法》第12條規定，當公務機關或企業違反法規，導致個人資料被竊取、洩漏、竄改或其他侵害，必須查明後以適當方式通知當事人。這裡所說的「適當方式」可以包括**口頭、書面、電話、簡訊、電子郵件、傳真等，或任何能讓當事人知悉的方式。**

- **不合適的通知方式：**

  單純張貼公告或廣發內容不具體清楚簡訊來通知受侵害的當事人，並不符合個資法上適當方式的要求。

企業應該個別通知當事人，最好用簡訊或電子郵件，並且在通知內容中包含以下重點：

1. 個資受侵害的事實、事故原因及對當事人的影響。
2. 企業已採取的因應措施或處理方式。
3. 提供當事人查詢事件的聯繫窗口（如查詢專線或其他管道）。

這樣的通知方式可以讓受侵害的客戶或消費者更清楚了解事情發生的經過，並知道該如何應對。雖然這可能會增加企業的負擔，但讓當事人早點知悉資料外洩的情況，能幫助他們防範後續風險，像是避免被詐騙，從而降低企業可能面臨的賠償風險。

14 如果發生個資事故該如何向主管機關進行通報？

發生個資事故後，雖然個人資料保護法對未通報並沒有明確罰則，但仍可作為處罰的裁量依據（根據法務部104年3月30日法律字第10403503590號函釋）。當企業發生個資外洩時，主管機關應根據個資法第27條、第48條，考量是否違規，不會僅因未通報就直接處罰。

然而，企業有適用「零售業個人資料檔案安全維護管理辦法」者，必須按照該辦法第12條規定，**在發現事故後72小時內通報主管機關，並採取措施減少對當事人的損害。**通報方式是填寫通報紀錄表，可以提交到商業發展署的首長信箱。如果向地方主管機關通報，還需通知中央主管機關，才是合於法規的通報。另外，單純的資安事件，因無個人資料外洩，並非個資事故而無須通報。

15 政府機關至公司進行個資或資安保護措施的查核，意即行政檢查時，業者是否有配合檢查的義務？

根據個資法第22條第1項規定，當中央主管機關或地方政府需要進行「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「其他例行業務檢查」，或有懷疑違反個資法時，可以派員攜帶證件進入企業檢查，並要求相關人員提供說明、配合措施或相關證明資料。因這類檢查具有強制力，根據第22條第2項，**主管機關可以扣留或複製涉及證據的個人資料或檔案，並可要求所有人、持有人或保管人提供或交付資料。**如果無正當理由拒絕或抗拒，主管機關可以採取對企業權益損害最小的方式強制執行。

企業或相關人員不得逃避、阻礙或拒絕檢查，違者依第49條可處以2萬至20萬元罰鍰。此外，檢查時主管機關可以率領資訊、電信或法律等專業人員參與。若企業擔心商業機密或個人資料外洩，這些參與檢查的專業人員與公務員一樣依法負有保密義務，不得洩漏檢查過程中知悉的資料。

16 員工個人電腦及其使用環境如何做好資安防護，以避免資安事件發生？

- **啟用個人防火牆**

  適當阻擋對外的Port，以防止未知的程式（例如惡意程式）由內對外的直接連線要求。

- **安裝啟用防毒軟體**

  防範病毒入侵、防範惡意軟體入侵電腦、防止行動裝置，被安裝惡意程式、減少被引導至釣魚網站和安全漏洞攻擊網站的風險、遠離垃圾郵件及詐騙訊息。

- **定期作業系統／應用程式更新**

  諸如Windows Update（OS）、Office Update（文書處理軟體）、Edge／Chrome安全性設定（Web瀏覽器）、Outlook安全性設定（收／發信軟體）。

- **使用最低權限**

  以Windows作業系統為例，將使用者帳號設為「Users」權限，而不授予Administrators、Power Users群組權限。以預防使用者開啟文件、瀏覽網頁時遭惡意程式攻擊入侵，惡意程式如要常駐在電腦中時，會因權限不足無法運作。

17 伺服器應該做好那些重要的保護措施，以提升資安防護能量？

- **進行日誌稽核管理**

  建置Log Server，收集單位內各主機日誌，以作為事件查詢與分析及保存證據之用途。

- **執行弱點掃描**

  利用弱點掃描工具，找出系統安全弱點，提供改善建議，協助企業修補安全漏洞，降低遭受入侵風險。

- **進行帳號管理與盤查**

  建立作業流程，管控帳號及密碼使用，並定期檢視盤查作業系統中帳號，以防止閒置帳號所帶來的風險。

- **定期作業系統、防毒軟體、安裝之應用程式更新作業**

  以防範病毒及惡意程式入侵並避免暴露於資安漏洞風險中。

18 防範郵件社交工程所帶來的資安風險，我們可以做哪些事防範？

- 安裝防毒、防詐騙軟體
- 關閉預覽信件功能
- 設定不自動下載圖檔
- 不要亂點未知連結
- 確認消息來源、寄件者及內容
- 不隨意開啟附件檔
- 使用數位簽章
- 不隨意轉傳未查證資訊
- 設定不自動傳送讀信回條
- 定期執行社交工程演練及演練檢討

19 若公司發生機敏資訊外洩事件該如何找出問體根因？

可以透過Log紀錄，初步排查出洩漏資料的漏洞；公司一般如果有開啟對外的資訊服務，會保有Access Log、Firewall Log及Database Log，這三項Log紀錄分別可以分析出外部的異常存取、內部的異常存取及資料庫的異常存取，透過這些Log紀錄即可循線追查到疏漏的資安風險，並進行改善。

20 如何降低帳戶遭到盜竊的可能性？

- **使用強大的密碼**

  選擇長度足夠、複雜度高的密碼，包括大小寫字母、數字和特殊符號的組合。避免使用容易猜測的密碼，如個人資訊、常用單字等。

- **定期更換密碼**

  建議每隔三個月或六個月更換一次密碼。

- **多因素驗證要求**

  在登錄時提供兩種或更多的身份驗證資訊，例如電子郵件和簡訊驗證碼，以提高帳戶的安全性。

- **不明寄件人的郵件，不要點擊附件或提供個人資訊**

  當收到可疑郵件時，應該直接與相關機構聯繫，進行確認。

- **定期檢查帳戶的登入紀錄和交易記錄**

  如有任何異常活動，應立即通知服務提供者並更改密碼。

- **保護個人設備免受惡意軟體和攻擊**

  包括定期更新作業系統和應用程式、安裝防病毒軟體、不點擊可疑連結等。

- **提高用戶對資安的認識**

  宣導識別和應對釣魚攻擊、保護密碼安全等。

附錄

附錄一、個人資料保護法

第一章 總則

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。

第 1-1 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 2 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 3 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 4 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 5 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 6 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 7 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 8 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 9 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 10 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 11 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 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。

第 13 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 14 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 15 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 16 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 17 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 18 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 19 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 20 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 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：

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 22 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 23 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 24 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 25 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、 沒入或命銷燬違法蒐集之個人資料。

四、 公布非公務機關之違法情形，及其姓名或名稱與負責人。

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 26 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 27 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 28 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 29 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 30 條

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

第 31 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 32 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 33 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 34 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 35 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 36 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 37 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 38 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 39 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 40 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 41 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 42 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 43 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 44 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 45 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 46 條

犯本章之罪，其他法律有較重處罰規定者，從其規定。

第 47 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 48 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 49 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 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。

第六章 附則

第 51 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 52 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 53 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 54 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 55 條

本法施行細則，由法務部定之。

第 56 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。

附錄二、個人資料保護法施行細則

第 1 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 2 條

本法所稱個人，指現生存之自然人。

第 3 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 4 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 5 條

本法第二條第二款所定個人資料檔案，包括備份檔案。

第 6 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 7 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 8 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 9 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 10 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 11 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 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。

第 13 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 14 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 15 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 16 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 17 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 18 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 19 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 20 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 21 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 22 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 23 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 24 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 25 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 26 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 27 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 28 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 29 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 30 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 31 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 32 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 33 條

本細則施行日期，由法務部定之。

附錄三、
零售業個人資料檔案安全維護管理辦法

第 1 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 2 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 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。

第 4 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 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。

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：

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 7 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 8 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 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：

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 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：

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 11 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 12 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 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：

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 14 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 15 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 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：

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 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。

第 18 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 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 20 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，應明確告知當事人業者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 21 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 22 條

本辦法自發布日施行。

附錄四、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）
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. 蒐集、處理或利用個人資料之電腦相關設備或系統設備，應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。
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，應依不同傳輸方式，採取適當之安全措施，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）進行演練更新及提出檢討改善報告。
11. 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。
12. 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。
13. 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。
14. 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。
15. 資通訊系統與網路相連存有個人資料者，應隨時更新並執行防毒軟體，及定期執行惡意程式檢測。
16. 對於存有個人資料之資通訊系統，設定異常存取資料行為之監控及定期演練因應機制。

（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商業發展署通報，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；紙本資料檔案之安全保護設施及管理程序。

（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）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。

（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）稽核個人資料安全維護計畫之執行情形及成效，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（包括自動化機器設備之軌跡資料或其他相關之證據資料），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。

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。

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、委託作業監督

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（詳下頁）

<table>
<tr><th colspan="4">個人資料侵害事故通報及記錄表</th></tr>
<tr><td rowspan="6">事業名稱：
_____

通報機關：
_____</td><td colspan="3">通報時間：　　年　　月　　日　　時　　分</td></tr>
<tr><td colspan="3">通報人：　　簽名（蓋章）</td></tr>
<tr><td colspan="3">職稱：</td></tr>
<tr><td colspan="3">電話：</td></tr>
<tr><td colspan="3">Email：</td></tr>
<tr><td colspan="3">地址：</td></tr>
<tr><td>事件發生時間</td><td colspan="3"></td></tr>
<tr><td rowspan="6">事件發生種類</td><td colspan="2">☐ 竊取</td><td rowspan="6">個資侵害之總筆數（大約）：
_____

☐ 一般個資
☐ 特種個資</td></tr>
<tr><td colspan="2">☐ 洩漏</td></tr>
<tr><td colspan="2">☐ 竄改</td></tr>
<tr><td colspan="2">☐ 毀損</td></tr>
<tr><td colspan="2">☐ 滅失</td></tr>
<tr><td colspan="2">☐ 其他侵害事故：</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="3"></td></tr>
<tr><td>損害狀況</td><td colspan="3"></td></tr>
<tr><td>個資侵害可能結果</td><td colspan="3"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="3"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="3"></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="3">☐ 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：

PERSONAL DATA PROTECTION MANUAL FOR BUSINESS SERVICES INDUSTRY

指導單位：經濟部商業發展署 Administration of Commerce, MOEA

執行單位：財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY

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

經濟部 商業發展署廣告

出版日期：113年11月