有關電商業者落實

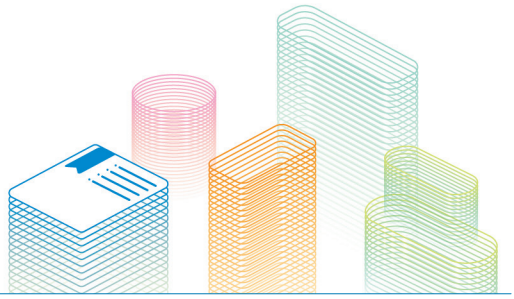
數位經濟相關產業
個人資料檔案安全維護管理辦法

參考指引

moda 數位發展部
Ministry of Digital Affairs

中華民國 113 年 12 月
執行單位 | 財團法人資訊工業策進會

目錄



壹 前言

近年來，隨著網際網路及電商產業的發展，我國電商產業的營業額持續增長。但在電商市場規模逐年擴大的同時，因交易所衍生之詐騙事件也層出不窮，像是帳號密碼被盜用、個資外洩、網路詐騙、釣魚郵件等不勝枚舉，防範網路詐騙或個資外洩已成為民眾生活關切的重點之一。為提升一般民眾的交易安全，相關平台業者或廠商開始紛紛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。

目前我國針對個資及外洩等規範，係以個人資料保護法 (以下簡稱個資法) 為主。個資法自民國 (以下同)101 年 10 月 1 日施行，並分別於 105 年 3 月 15 日、112 年 5 月 31 日經歷二次修法。因應近期國內個資外洩案件，為避免企業個資外洩遭不法集團利用，爰修正個資法第 48 條非公務機關違反安全維護義務之裁罰方式及額度，改為逕行處罰同時命改正，並提高罰鍰上限，處新臺幣 (下同) 2 萬元以上 200 萬元以下罰鍰；情節重大者，處 15 萬元以上 1,500 萬元以下罰鍰。屆期未改正者，按次處 15 萬元以上 1,500 萬元以下罰鍰。藉由本次修正裁罰方式及額度，將促使業者強化個資的資安維護作為。

我國數位發展部自 111 年 8 月 27 日正式成立，由數位發展部數位產業署作為數位經濟相關產業的中央目的事業主管機關，並於 112 年 10 月 12 日發布《數位經濟相關產業個人資料檔案安全維護管理辦法》。因此，以個人資料保護與管理之法令要求，希冀協助及引導電商業者因應法規要求與建立個資保護及管理參考，數位發展部數位產業署特委託資策會科法所，研擬《有關電商業者落實數位經濟相關產業個人資料檔案安全維護管理辦法參考指引》供業者參考以提升個資保護與資安管理能力。

本指引係參照前述數位發展部發布之《數位經濟相關產業個人資料檔案安全維護管理辦法》，並以個資法施行細則第 12 條第 2 項所列之 11 款管理事項或要求為架構，同時導入 PDCA(Plan-Do-Check-Act) 方法論，以計畫、執行、檢查、行動等方式，建立及持續改善電商業者個人資料保護與管理制度。旨在引導並鼓勵業者自主管理，國內電商業者可參考相關法遵內容，但不以此為限，以考量業者營運風險與需求，訂定符合業者本身營運需求之個人資料保護與管理制度。

表 1　個資法施行細則第 12 條第 2 項之 11 項要求

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。

資料來源 | 本研究團隊整理

貳 《數位經濟相關產業個人資料檔案安全維護管理辦法》介紹

一、立法說明

依據個資法第 27 條規定，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。

數位發展部為數位經濟相關產業之中央目的事業主管機關，為使相關業者自行或受委託蒐集、處理或利用個人資料檔案，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，爰依上開規定之授權，於 112 年 10 月 12 日訂定發布《數位經濟相關產業個人資料檔案安全維護管理辦法》(以下簡稱本辦法)，要求該等業者訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法 (以下簡稱安全維護計畫)，以加強管理、確保個人資料之安全維護。

至於經濟部於 104 年 9 月 17 日發布之《網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法》，因本辦法施行，為避免法規適用競合，將自 112 年 11 月 21 日起公告廢止。

二、本辦法適用之對象

首先敘明，本辦法第 2 條僅規定適用對象的業別，而並未設立適用本辦法的門檻條件，因此無論資本額或保有個人資料筆數多寡、公司類型，均一併適用本辦法。依據本辦法第 2 條規定，本辦法所稱數位經濟相關產業類業者 (以下簡稱業者)，指從事附表一所列行業之自然人、私法人或其他團體。參酌「行政院主計總處行業統計分類」，於本辦法附表一明定本辦法之適用對象，包含「4871 電子購物及郵購業」之「從事以網際網路方式零售商品之行業 (不含電視、廣播、電話等其他電子媒介及郵購方式)」，即本指引所稱之「電商業者」；「582 軟體出版業」；「620 電腦程式設計、諮詢及相關服務業」；「6312 資料處理、主機及網站代管服務業」之「從事代客處理資料、主機及網站代管以及相關服務之行業 (不含線上影音串流服務)」；「639 其他資訊供應服務業」；「6699 未分類其他金融輔助業」之「第三方支付服務業 (不含其他金融輔助業)」。

表 2　數位經濟相關產業類業者

行政院主計總處行業統計分類 分類編號及行業名稱	適用本辦法之行業
4871 電子購物及郵購業	從事以網際網路方式零售商品之行業 (不含電視、廣播、電話等其他電子媒介及郵購方式)
582 軟體出版業	軟體出版業
620 電腦程式設計、諮詢及相關服務業	電腦程式設計、諮詢及相關服務業
6312 資料處理、主機及網站代管服務業	從事代客處理資料、主機及網站代管以及相關服務之行業 (不含線上影音串流服務)
639 其他資訊服務業	其他資訊服務業
6699 未分類其他金融輔助業	第三方支付服務業 (不含其他金融輔助業)

資料來源 |《數位經濟相關產業個人資料檔案安全維護管理辦法》附表一

三、本辦法之規範重點

(一) 個人資料保護管理政策與安全維護計畫之訂定

業者為落實個人資料之保護，應配置管理人員及相當資源，負責個人資料保護管理政策 (以下簡稱個人資料保護政策) 之訂定及修正，與安全維護計畫之訂定、修正及執行 [1]。關於個人資料保護政策與安全維護計畫之訂定或修正，應經業者代表人或經其授權之人員核定 [2]，以確保個人資料保護的推動與執行，彰顯管理保護之責。

關於業者訂定個人資料保護政策，其內容應包括：

(1) 遵守我國個人資料保護相關法令規定。
(2) 以合理安全之方式，於特定目的範圍內，蒐集、處理及利用個人資料。
(3) 以可期待之合理安全水準技術保護其所蒐集、處理或利用之個人資料檔案。
(4) 設置聯絡窗口，供個人資料當事人行使其個人資料相關權利或提出相關申訴與諮詢。
(5) 規劃緊急應變程序，以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。
(6) 如委託蒐集、處理及利用個人資料者，應妥善監督受託業者。
(7) 持續維運安全維護計畫之義務，以確保個人資料檔案之安全 [3]。

[1] 參照本辦法第 5 條第 1 項。
[2] 參照本辦法第 5 條第 2 項。
[3] 參照本辦法第 4 條。

三、本辦法之規範重點

此係基於為使企業全體所屬人員對於個人資料之保護能有所體認並落實，故企業於訂定個人資料保護政策後，應進行對內公開周知的宣導。

而關於安全維護計畫之訂定，業者應納入第 5 條至第 17 條規定之具體內容作為實際管理程序，並應適時檢討修正[4]。又數位發展部得要求業者於指定期限內以書面方式提出安全維護計畫之實施情形[5]，亦即主管機關將依據本辦法之實際內容，對業者進行程序訂定與執行狀況之確認。而為持續改善安全維護計畫，業者應訂定整體持續改善機制，包括：

(1) 安全維護計畫及未落實執行時應採取矯正預防措施。

(2) 參酌安全維護計畫執行狀況、技術發展、業務調整及法令變化等因素，定期檢視或修正[6]。另考量業者訂定安全維護計畫需有一定時間作業，爰予以規定應於本辦法施行之日起 3 個月內完成安全維護計畫之訂定[7]，使業者於因應本辦法時有所緩衝，故應於 113 年 1 月 13 日以前訂定安全維護計畫。

(二) 應定期清查個人資料現況及評估可能風險

為使業者得有效掌握個人資料蒐集、處理或利用過程中之風險，應先界定個人資料範圍進行個人資料盤點作業，即應定期清查確認所蒐集、處理或利用之個人資料現況，以界定其納入安全維護計畫之範圍[8]。又業者對於個人資料之各項管理程序均源自於對自身風險狀況之瞭解，應進行個人資料風險評鑑作業，即應依已界定之個人資料範圍及其業務涉及個人資料蒐集、處理或利用之流程，定期評估可能產生之風險，並根據風險評估結果，採取適當安全管理措施[9]。故業者應定期清查個人資料現況，建立個人資料檔案盤點清冊與作業流程說明文件，並就此執行個人資料之風險評鑑，包含可能面臨之法律風險，且有別於一般針對個人資料風險多偏向於資安類型之評估，業者亦應注意因不當利用個人資料、未盡告知義務或未妥適提供當事人行使權利等違法風險。

(三) 個人資料事故之預防、通報及應變機制

業者為因應當事人個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故，應訂定應變、通報及預防機制[10]，以保障當事人之個人資料，預防個資外洩或資安事件發生。除了事故之控制預防機制，與因應個資法第 12 條事故通知義務外，並明定事故發生向主管機關之通報機制。即當業者遇有個人資料安全事故，將危及其正常營運或大量當事人權益者，應於知悉事故後 72 小時內依本辦法附表二填具「業者個人資料外洩通報表」向數位發展部進行通報，或通報直轄市、縣 (市) 政府時副知數位發展部[11]，以利各方能盡速採取行動降低個資外洩所帶來的損害。另此機制得採分階段通報，若企業未能於時限

[4] 參照本辦法第 3 條第 2 項。
[5] 參照本辦法第 3 條第 3 項。
[6] 參照本辦法第 17 條。
[7] 參照本辦法第 3 條第 1 項。
[8] 參照本辦法第 6 條。
[9] 參照本辦法第 7 條。
[10] 參照本辦法第 8 條第 1 項。
[11] 參照本辦法第 8 條第 2 項。

三、本辦法之規範重點

內通報者應附具延遲理由，或未能於當次提供通報事項全部資訊者應分階段提供[12]。目前台灣電腦網路危機處理暨協調中心 (以下簡稱 TWCERT/CC) 亦於數位發展部指導下，推動企業資安事件通報協處[13]，以供業者遭遇個人資料安全事故時，得以達成及時控制風險與降低當事人損害之目的。

(四) 應訂定個人資料內部管理程序

為確保個人資料之蒐集、處理或利用，符合個資法相關法令要求，業者應訂定內部管理程序，內容包括：

(1) 檢視一般個人資料與特種個人資料是否符合法定要件。
(2) 當事人拒絕行銷之處置。
(3) 當事人行使權利之處理。
(4) 個人資料正確性之維護。
(5) 個人資料之刪除等事項[14]。

又關於業者進行個人資料之國際傳輸，事前應檢視是否受數位發展部限制，並且應告知當事人其個人資料所欲國際傳輸之區域，同時對資料接收方應盡監督義務[15]。

(五) 應訂定適當之資料、人員、設備安全管理措施

針對資料之安全管理措施，業者對於個人資料之加密、備份及傳輸應採取適當安全措施[16]。若業務上有透過資通系統直接或間接蒐集、處理或利用個人資料的情形，企業應採取之措施包括：

(1) 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。
(2) 資通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。
(3) 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。
(4) 與網路相聯之資通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。
(5) 資通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。
(6) 處理個人資料之資通系統進行測試時，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。
(7) 處理個人資料之資通系統有變更時，應確保其安全性未降低。
(8) 定期檢視處理個人資料之資通系統，檢查其使用狀況及存取個人資料之情形。
(9) 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。
(10) 其他數位發展部公告之資料安全管理措施[17]。

[12] 參照本辦法第 8 條第 3 項。
[13] 〈一般資安通報線上服務〉，台灣電腦網路危機處理暨協調中心，https://www.twcert.org.tw/tw/sp-geno-guide-1.html。
[14] 參照本辦法第 9 條。
[15] 參照本辦法第 10 條。
[16] 參照本辦法第 11 條第 1 項。
[17] 參照本辦法第 11 條第 2 項。

三、本辦法之規範重點

至於針對人員應採取之安全管理措施，包括：

(1) 與所屬人員約定保密義務。
(2) 識別業務內容涉及個人資料蒐集、處理或利用之人員。
(3) 其業務特性、內容及需求，設定所屬人員接觸個人資料之權限，並定期檢視其適當性及必要性。
(4) 人員離職時，要求人員返還個人資料之載體，並刪除因執行業務而持有之個人資料[18]。

而針對存有個人資料之儲存媒介物，所應採取之設備安全管理措施，則包括：

(1) 依儲存媒介物之特性及使用方式，建置適當之保護設備或技術。
(2) 針對所屬人員保管個人資料之儲存媒介物，訂定適當之管理規範。
(3) 針對存放儲存媒介物之環境，施以適當之進出管制措施[19]。

(六) 應定期實施個人資料保護認知宣導及教育訓練

為有效落實管理制度，業者應定期對所屬人員實施個人資料保護認知宣導及教育訓練，其內容應包括：

(1) 個人資料保護相關法令之規定；
(2) 所屬人員之責任範圍；
(3) 安全維護計畫各項管理程序、機制及措施之要求[20]。

而對於代表人、負責人或第 5 條所稱管理人員，另應依其於安全維護計畫所擔負之任務及角色，定期實施必要之教育訓練[21]。另針對從事以網際網路方式供他人零售商品之平台業者，其安全維護計畫應加入事項包含：

(1) 對其平台使用者，進行適當之個人資料保護及管理之認知宣導或教育訓練；
(2) 訂定個人資料保護守則，要求平台使用者遵守 ，以督促其訂定及執行個人資料安全維護措施。

(七) 資料安全稽核與相關紀錄及證據之保存

為確保安全維護計畫之有效實施，業者應依其業務規模及特性，訂定適當之個人資料安全稽核機制，定期檢查安全維護計畫執行狀況，提出評估報告並採取改善機制[23]。即業者應以內部稽核之方式，確認安全維護計畫之落實，並為確保稽核品質，該稽核人員宜由具備管理、法制及資訊安全之人員擔任之。又業者執行安全維護計畫時，應評估其必要性，保存相關記錄至少 5 年，包括：

(1) 個人資料之蒐集、處理及利用紀錄。
(2) 自動化機器設備之軌跡資料。
(3) 落實執行安全維護計畫之證據[24]。

而當企業之業務終止後，其所蒐集、處理或利用之個人資料應銷毀、移轉、刪除、停止處理或利用，亦應留存相關紀錄至少 5 年[25]，作為企業已遵循個資法相關規定之證明。

[18] 參照本辦法第 12 條。
[19] 參照本辦法第 14 條。
[20] 參照本辦法第 13 條第 1 項。
[21] 參照本辦法第 13 條第 2 項。
[22] 參照本辦法第 13 條第 3 項。
[23] 參照本辦法第 15 條。
[24] 參照本辦法第 16 條第 1 項。
[25] 參照本辦法第 16 條第 2 項。

三、本辦法之規範重點

(八) 執行頻率分級管理

由於本辦法之適用門檻已不限於特定之公司組織型態，無論業者係屬股份有限公司、有限公司、無限公司、兩合公司、獨資或合夥，均須遵循本辦法之規定。為避免業務規模較小業者負擔過多成本，本辦法就部分安全維護措施採取執行頻率分級管理。即明定「資本額達新台幣 1 千萬元以上」或「保有個人資料筆數達 5 千筆以上者」之企業，應每 12 個月至少實施及檢討改善一次，包括界定個人資料之範圍、個人資料之風險評估、部分資料安全管理措施 (包含更新防止外部網路入侵對策、演練事故因應機制、檢測系統漏洞、存取權限控管)、認知宣導及教育訓練，以及資料安全稽核機制、整體持續改善機制等措施 [26]。

表 3　本辦法規範對象所須遵守義務比較表

《數位經濟相關產業個人資料檔案安全維護管理辦法》規範對象所須遵守義務比較表

條號	項目 (累計義務)	未符合條件者	符合條件者
§3	訂定安全維護計畫及處理方法	V	V
§4	公開個人資料保護政策內容	V	V
§5	配置管理人員及相當資源	V	V
§6	界定個人資料之範圍	V	V (每 12 個月至少執行一次)
§7	個人資料之風險評估及管理機制	V	V (每 12 個月至少執行一次)
§8	事故之預防、通報及應變機制	V	V
§9	個人資料蒐集、處理及利用之內部管理程序	V	V (§9 ⑧每 12 個月至少執行一次)
§10	國際傳輸限制、告知及監督	V	V
§11	資料安全管理措施	V	V (§11 II①、②、③、④、⑧每 12 個月至少執行一次)

[26] 參照本辦法第 18 條第 1 項。

三、本辦法之規範重點

條號	項目 (累計義務)	未符合條件者	符合條件者
§ 12	人員安全管理措施	V	V (§ 12 ③ 每 12 個月至少執行一次)
§ 13	認知宣導及教育訓練	V	V (§ 13 I、II 每 12 個月至少執行一次)
§ 14	設備安全管理措施	V	V
§ 15	資料安全稽核機制	V	V (每 12 個月至少執行一次)
§ 16	使用紀錄、軌跡資料及證據保存	V	V
§ 17	個人資料安全維護之整體持續改善	V	V (§ 17 ② 每 12 個月至少執行一次)

資料來源 | 本研究團隊整理

關於資本額之認定，業者為股份有限公司採「實收資本額」，若為有限公司、無限公司與兩合公司則採「資本總額」，於獨資或合夥方式經營之事業，為登記之資本額 [27]。而保有個人資料筆數之計算，以業者單日所保有之個人資料為認定基準；若因刪除、銷毀或其他方法致保有個人資料筆數減少，且連續 2 年期間保有個人資料筆數未達 5 千筆之業者，得不適用頻率強化管理規定；但嗣後因直接或間接蒐集而致保有個人資料筆數達 5 千筆以上者，應於保有筆數達 5 千筆以上之日起 30 日內，恢復適用頻率強化管理規定 [28]。若業者原先之資本額未達新台幣 1 千萬，係於本辦法施行後始增資達新台幣 1 千萬元以上，或因直接或間接蒐集而保有個人資料達 5 千筆以上者，則應自符合條件之日起 6 個月後，開始每 12 個月至少實施及檢討改善前項措施一次 [29]。

(九) 個人資料委外之原則與義務

當業者有受委託蒐集、處理或利用個人資料之情形，應遵循委託者之中央目的事業主管機關所定之個人資料相關法規 [30]。而當業者有委託他人蒐集、處理或利用個人資料之情形，則應對受託者依個資法施行細則第 8 條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容 [31]。

[27] 參照本辦法第 18 條第 3 項。
[28] 參照本辦法第 18 條第 4 項。
[29] 參照本辦法第 18 條第 2 項。
[30] 參照本辦法第 19 條第 1 項。
[31] 參照本辦法第 19 條第 2 項。

三、本辦法之規範重點

(十) 安維計畫常見查核缺失

2024 年數位發展部數位產業署就電子商務業、第三方支付業、遊戲業等業者之安維計畫進行查核，將查核所知有關安維計畫各條文之常見錯誤整理如下表：

表 4 安維計畫查核缺失整理

條文 / 規範內涵		常見缺失情況
第 5 條	配置管理人員及相當資源	管理人員不足、未配置資源、資源不合理
第 6 條	個資盤點	未設定執行週期、盤點不確實
第 7 條	風險評鑑	未設定執行週期、未能識別風險、未依風險設置對應管理機制
第 8 條	預防、通報及應變程序	未設置通報窗口、通報時間有誤、未建立通報流程
第 9 條	內部管理程序	未定期銷毀、告知聲明(隱私權政策)有缺漏、未提供當事人行使權利窗口、未建置維護資料正確性機制
第 10 條	國際傳輸	未告知國際傳輸有關事宜
第 11 條	資料安全管理措施	未設定執行週期、採行之資安措施未包含所有子法要求事項
第 12 條	人員管理措施	未設定執行週期、未執行權限控制及盤點、未簽保密契約
第 13 條	教育訓練	未設定差異化教育訓練
第 14 條	設備安全管理措施	漏未規定設備安全、門禁機制漏未盤點
第 15 條	稽核	未規定稽核程序、稽核人員缺乏獨立性
第 16 條	紀錄保存	保存期限設定不足五年、留存資料而非紀錄
第 17 條	持續改善	漏未規定、未識別法規更新

資料來源 | 本研究團隊整理

三、本辦法之規範重點

最常見的缺失情形屬「應明訂期限而未明訂」的情形，提醒業者於撰寫安維計畫時應該要注意法規對於期限有所要求，多數而言為至少每 12 個月須進行一次有關措施的實施。而其他各項疏失，分別論述如下：

1. 教育訓練
   (1) 第 13 條第 2 項規定業者須對所屬人員進行個人資料保護認知宣導及教育訓練，惟常見業者將資安教育訓練與個資教育訓練混為一談，應特別注意二者之差異。
   (2) 第 13 條第 2 項規定對代表人、負責人或第 5 條所稱管理人員，需要另應依其於安全維護計畫所擔負之任務及角色，定期實施必要之教育訓練。此教育訓練之內容需要與針對所屬人員之個人資料保護認知宣導及教育訓練有所不同，而常見業者漏未規定須進行本項之教育訓練。
   (3) 第 13 條第 3 項特別針對 B2B2C、C2C 這種經營可以供賣家自行上架的平台業者，需要對其平台使用者進行教育訓練及提供保護守則的規定，惟業者也可能忽略本項規定。
2. 設備安全管理措施
   因現在許多業者使用雲端服務，因而可能對於設備、實體環境之界定比以往來得模糊，因此認為無須訂定有關設備安全之管理措施，仍要提醒業者終端設備如手機、筆電或平板等設備，仍需要設立一定的管理措施。
3. 風險評鑑
   風險評鑑對於多數業者來說皆有一定難度，建議可參考本指引專篇「個人資料風險評估管理程序 (含個人資料風險評鑑表、高風險回應計畫)」來進行有關之風險評鑑程序，另需要特別注意風險評估之排程，如適用高頻率業者至少每 12 個月應進行一次風險評鑑。
4. 資料安全管理措施
   (1) 最常見問題屬適用高頻率業者未依規定至少每 12 個月進行一次有關之資安措施，除此之外較常見的屬對於資料庫的保護及人員權限有疑慮。
   (2) 建議業者可將資料庫之資料欄位進行隱碼設置、嚴謹管控管理者特權帳號、設置合理之身分認證機制、須列明密碼複雜度，並複雜度須達一定程度。
5. 內部管理程序
   常見之缺失情形屬未定期檢視個人資料蒐集之特定目的是否已消失或期限是否已屆滿，提醒業者應注意個資保存期限，並依期限執行刪除及銷毀作業。
6. 預防、通報及應變程序
   (1) 常見的錯誤為缺少通報及應變處理流程、未依法對當事人進行事故通知。
   (2) 建議業者建立通報應變處理組織及流程 SOP、並進行相關通報演練。
   (3) 若不幸發生個資事故，應依法通知當事人，包含被侵害事實、已採取之因應措施及後續處置方式。

四、常見問答

01

Q 我怎麼知道我的公司要不要訂個人資料檔案安全維護計畫 (簡稱安維辦法) ？

A 各中央目的事業主管機關會依據所管轄之產業別，制定適合該產業的安維辦法，因此只要主管機關有公布，您的公司就需要訂定「個人資料檔案安全維護計畫」(簡稱安維計畫)。另外提醒，就算主管機關未頒布安維辦法，公司仍要遵守個人資料保護法及個人資料保護法施行細則的規定。

02

Q 我有很多主管機關，我要訂很多份安維計畫嗎？

A 如果公司經營的業務比較多元，可能會同時受到多個主管機關管轄，此時可能會被多部安維辦法要求訂定安維計畫。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安維辦法規定，並且以其中較為嚴格的規定來執行。如：A 安維辦法要求每一年執行甲業務，B 安維辦法要求每半年執行甲業務，則應每半年執行一次甲業務為宜。

03

Q 界定個人資料範圍(即進行個人資料盤點)時，除消費者 / 會員資料外，是否尚包含員工、合作廠商的個資？

A 於進行個人資料盤點時，所要盤點的個人資料檔案為公司保有的所有個資，因此除消費者與客戶的個資以外，也包含從員工或是合作廠商等處蒐集到的個資，全部都應納入個人資料檔案盤點清冊中。

四、常見問答

04

Q 如何判斷個人資料的筆數？

A 在個資盤點作業時計算保有個資的數量，只須填寫大概數量即可。然而實際上個資筆數的計算可能還是須依情境而訂，由於在不同業務使用個資，其目的也當然有所不同，建議將特定目的、風險值相同或相近的資料，納入同一個資檔案進行盤點，並從自身業務流程角度出發，去定義為一筆個資。假設有 100 位會員註冊您網站的會員 (會員資料：姓名、電話、地址、出生日期)，但僅有其中 50 位會員下單購買產品，並將產品以委外配送 (寄送資料：訂單、姓名、電話、地址)。則其中會員註冊應盤點為 100 筆資料，而 50 筆訂單則因尚包括訂單資料、收款資訊和委外運送，建議另行計算為 50 筆資料，總計筆數為 150 筆。

05

Q Cookie(網路識別碼)是否屬於個人資料？

A 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》，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方式識別該個人之資料，因此 Cookie 也屬於個人資料之範圍。

06

Q 何謂個資業務終止？

A 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。

四、常見問答

07

Q 客戶可以要求我刪除他的個人資料嗎？我多久要刪除？我可以不刪除嗎？

A 消費者對於資料的刪除權是法定的權利，當消費者提出刪除資料時原則上業者應同意並刪除，且不得在合約內請消費者放棄刪除權，亦不能限制刪除權行使。
原則上企業需要在 30 日內回覆當事人刪除是否被接受，如果不能刪除需要具備相當合理的理由，如某些法規可能要求保留資料達一定年限等情形；若無特殊理由，則應該在同意當事人申請之後盡速刪除之，若因自動化排程設定資料管理週期，只要是合理的刪除期限，亦能符合刪除的規定。

08

Q 何謂個資法之「自動化機器設備」？

A 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

Q 安維辦法第 16 條的規定，是所有個人資料都要保存 5 年嗎？

A 安維辦法第 16 條的規定是指對於個人資料有利用 (使用)、銷毀、移轉和刪除個人資料相關的「紀錄」，例如 A 客服於幾月幾日幾時取用 B 客戶資料此事的紀錄保存 5 年，而非客戶的資料本身需要保存 5 年。如果是關於自動化機器設備之軌跡紀錄 (Log) 也應保存，所有紀錄至少要保留 5 年。

10

Q 何謂個資的國際傳輸(跨境傳輸)？

A 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。我國原則上允許個資國際傳輸，但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，並且務必於蒐集資料時明確告知當事人預定傳輸的個人資料範圍、類別、特定目的、期間、地區、對象及傳輸方式。

四、常見問答

11

Q 使用雲端服務是否有涉及國際傳輸？

A 如果公司所使用的雲端服務，機方非落地於本國境內，或傳輸過程中可能經過他國伺服器中轉，皆會構成個資國際傳輸情形，需要依法告知。

12

Q 何為「委外」？我有沒有「委託」？

A 只要公司不是以單獨法人進行的行為，均有涉及「委外」、「委託」。例如公司可能使用系統商開發的一站式購物網頁、透過某銀行的金流服務收款，最後透過某物流運送，就至少涉及了「系統商」、「金流商」和「物流商」三個委託行為。

13

Q 應如何落實對委外廠商的管理與監督？

A 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)：

a. 公司需要建立適當的選商程序並遵循規定招商；
b. 透過委外契約與受託公司約定監督事項相關條款 (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)；
c. 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)；
d. 請受託公司針對內部情況，對照個資法施行細則第 12 條 2 項適當安全措施，來提供「自我檢核表」，供選商企業參考。

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。

四、常見問答

14

Q 何謂個資事故？發生個資事故後應如何通知客戶或消費者？是否可以張貼防詐騙公告或廣發簡訊代替？

A 「個資事故」依照個資法第 12 條規定，指當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，白話來說就是客戶的個資外洩了。

當事故發生後，公務機關或非公務機關應查明後以適當方式通知當事人。而所謂「適當方式」解釋上可包含言詞、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的方式通知當事人。

注意，若僅以張貼防詐騙公告或廣發簡訊方式，作為對受侵害個資當事人的通知，不符合法規中所稱「以適當方式通知當事人」！

除應以適當方式通知外，在通知內容方面建議，應包含以下幾點：

a. 個人資料被侵害的事實，事故原因情形與對當事人的影響；

b. 企業對事故已採取的因應措施或處理；

c. 提供個資當事人事件窗口（查詢專線或其他查詢管道）。

以較明確文字針對受侵害之客戶或消費者，提供發生個資事故資訊及後續聯繫窗口使個資當事人知悉確認。

15

Q 如果發生個資事故該如何向主管機關進行通報？

A 若公司有「安維辦法」的適用時，須於發現事故時起 72 小時內，通報主管機關。地區性公司通報地方縣、市政府；全國性企業通報數位發展部。如向地方主管機關通報者，並應副知中央主管機關。

企業可填寫該辦法附件的個人資料侵害事故通報與紀錄表向主管機關通報。

16

Q 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？

A 依個資法第 22 條規定，行政檢查具有強制力，且企業的相關人員必須要配合提供必要的說明、配合措施或提供相關證明資料。倘若企業規避、妨礙或拒絕行政檢查，如有違反可依個資法第 49 條對其處以新臺幣 2 萬元以上 20 萬元以下罰鍰。

四、常見問答

17

Q 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？

A

a. 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。
b. 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。
c. 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)。
d. 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。

18

Q 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？

A

a. 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。
b. 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。
c. 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。
d. 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。

四、常見問答

19

Q 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？

A

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

20

Q 若公司發生機敏資訊外洩事件該如何找出問題根因？

A 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。

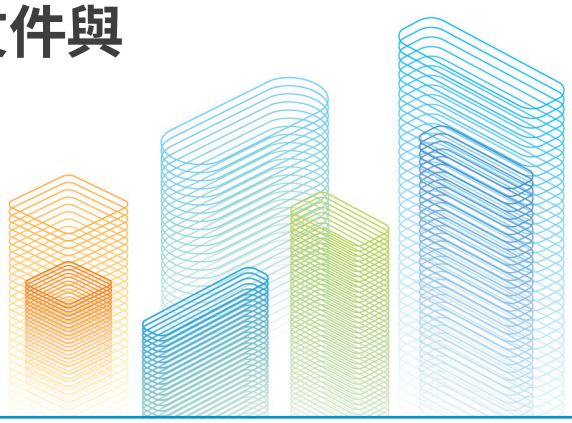
21

Q 如何降低帳戶遭到盜竊的可能性？

A

a. 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。
b. 定期更換密碼；建議每隔三個月或六個月更換一次密碼。
c. 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。
d. 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。
e. 定期檢查帳戶的登入紀錄和交易紀錄，如有任何異常活動，應立即通知服務提供者並更改密碼。
f. 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。
g. 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。

參 電商業者個資法遵文件與制度建置



為防杜個資外洩所導致詐騙，及強化消費者權益之保障，有關資料蒐集、處理或利用須知或應注意事項等，相關電商業者不宜忽略，且更應進一步搭配內部作業流程及因應作為，增強企業法令遵循之能力。基此，此一法遵參考指引係由數位發展部委請資策會科法所專業法制團隊提供，可供電商業者進行法令遵循規劃、教育訓練，或協助企業內部落實個資保護與管理等參考。

本指引計有數位發展部所管電商業者個資防護企業自評表、安全維護計畫範本、制度建置等三大部分，謹分別說明如下：

一、數位發展部所管電商業者個資防護企業自評表

透過本自評表，提供業者個人資料保護與管理之基礎要求，以協助並引導業者因應法規要求與建立個資保護與管理參考，並鼓勵業者自主管理，使其能透過本自評表，考量營運風險與需求，並訂定符合業者營運現況之個人資料保護與管理制度。而業者更可透過本表，預先規劃於保護內部個人資料安全時，所能呈現之具體紀錄、行為，亦可作為對外證明其係具備個資保護能力，並積極投入的表現。

數位發展部所管電商業者個資防護企業自評表說明

數位發展部所管電商業者個資防護企業自評表 (以下簡稱本表)，係為數位發展部數位產業署委託財團法人資訊工業策進會制定，以推動電商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

本表旨在提供我國電商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

電商業者，即行政院主計總處行業統計分類 4871 電子購物及郵購業，從事以網際網路方式零售商品之行業 (不含電視、廣播、電話等其他電子媒介及郵購方式)。

一、數位發展部所管電商業者個資防護企業自評表

如何使用本表

本表係依據主管機關於 112 年 10 月間頒佈之「數位經濟相關產業個人資料檔案安全維護管理辦法」之規定，並參照主管機關於行政檢查時提供之「數位發展部所管電商業者個資防護企業自評表」等，可協助業者依序展開個人資料保護與管理之控制措施。
填寫本表時，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：

一、 依序由第 1 題組填寫至第 11 題組，以本表之查核內容為基準，並可參考「簡述原因」欄位之說明，瞭解本查核項之具體內容或程序文件範例，比對業者本身現行個人資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」/「部分符合」/「不符合」/「不適用」欄位，並將相關證明文件、紀錄及說明填寫於填寫於「簡述原因 (並檢附佐證資料)」欄位。

二、 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「數位經濟相關產業個人資料檔案安全維護管理辦法」等規範。

自評表內容	
填表日期：_____年_____月_____日	
公司全稱	
公司登記資本額	
公司統一編號	
網站名稱	
上一年度營業額	
會員數量	
員工數量	
填寫人員／職稱 (可填寫多人)	

查檢項目		自評內容				簡述原因 並檢附佐證資料
		符合	部分符合	不符合	不適用	
1. 人員及資源配置 (安維辦法第 3、4、5 條)						
1.1	已配置專責人員或組織管理及維護保有之個人資料。					(佐證資料如：企業組織圖，得以看出個資專責人員配置 [此段說明文字請刪除]
1.2	已配置適當資源 (如軟硬體設施及經費等) 執行個人資料保護相關事項。					(佐證資料如：軟硬體設施及經費表等)[此段說明文字請刪除]
1.3	已訂定及配合相關法令修正個人資料保護管理政策。					(佐證資料如：政策文件等)[此段說明文字請刪除]
1.4	已訂定及配合相關法令修正個人資料檔案安全維護計畫。					(佐證資料如：計畫書等) [此段說明文字請刪除]
2. 界定個人資料 (安維辦法第 6 條)						
2.1	已定義個人資料並建立盤點清冊。					(佐證資料如：個資盤點表等)[此段說明文字請刪除]
2.2	個人資料是否包含特種個資？若有，請詳述其法令依據及蒐集內容。					若未蒐集特種個資則填不適用
3. 風險評估 (安維辦法第 7 條)						
3.1	已進行風險評估。					(佐證資料如：風險評估表，可分辨出資產價值，以便採取適當的避險措施)[此段說明文字請刪除]
3.2	已進行風險評鑑。					(佐證資料如：風險評鑑表，包含風險識別與風險預估 [此段說明文字請刪除]
3.3	已針對風險進行因應。					(佐證資料如：適當之管控及因應措施、區分風險分級等)[此段說明文字請刪除]
4. 事故通報應變 (安維辦法第 8 條)						
4.1	有通報及應變程序。					(佐證資料如：通報應變程序文字等)[此段說明文字請刪除]

查檢項目		自評內容				簡述原因 並檢附佐證資料
		符合	部分符合	不符合	不適用	
4.2	事故發生時會確實通報。					當年度無事故者，4.2-4.6 應填不適用 (佐證資料如：通報單等)[此段說明文字請刪除]
4.3	事故發生後採取應變措施。					(佐證資料如：說明所採應變措施等)[此段說明文字請刪除]
4.4	於期限內通知當事人。					(佐證資料如：通知書內容等)[此段說明文字請刪除]
4.5	事後採取預防措施。					(佐證資料如：說明所採預防措施等)[此段說明文字請刪除]
4.6	自發現個資外洩事故時起算 72 小時內，填列「個人資料侵害事故通報與紀錄表」通報總機構所在地直轄 (縣) 市主管機關或本部。					(佐證資料如：通報紀錄等等)[此段說明文字請刪除]
5. 蒐集處理利用之內部管理程序 (安維辦法第 9、10、19 條)						
5.1	資料蒐集、處理應具備特定目的並具有法定要件。					(佐證資料如：資料盤點表或其他內部制度文件等)[此段說明文字請刪除]
5.2	依規定取得當事人同意 (當事人同意之情形)。					(佐證資料如：當事人同意書等)[此段說明文字請刪除]
5.3	已清楚直接或間接蒐集個人資料之適法性，如履行告知義務及時點 (未履行告知義務時，是否符合免告知之情形)。					(佐證資料如：資料盤點表、資料流程說明 (圖) 或其他內部制度文件等)[此段說明文字請刪除]
5.4	告知內容包含個資法第八條規定項目。					(佐證資料如：資料盤點表其他內部制度文件等)[此段說明文字請刪除] 若符合個資法第八條第二項或第九條免告知則填不適用
5.5	個人資料之利用，符合特定目的之範圍。					(佐證資料如：資料盤點表、資料流程說明 (圖) 或其他內部制度文件等)[此段說明文字請刪除]

查檢項目		自評內容				簡述原因 並檢附佐證資料
		符合	部分符合	不符合	不適用	
5.6	是否有國際傳輸個人資料之情形，並告知當事人。					無國際傳輸應填不適用 (佐證資料如：資料盤點表、資料流程說明 (圖) 或其他內部制度文件等)[此段說明文字請刪除]
5.7	已訂定個人資料蒐集、處理及利用目的消失或屆滿之資料銷毀、刪除程序。					(佐證資料如：銷毀、刪除錄影或截圖，足以顯示確實已刪除個資及內部有關資料刪除、銷毀之制度文件等)[此段說明文字請刪除]
5.8	有定期檢核及紀錄以確認特定目的外之利用。					(佐證資料如：資料盤點表、資料流程說明 (圖)、內部評鑑或稽核紀錄或其他內部制度文件等)[此段說明文字請刪除]
5.9	目的外利用符合法定要件。					(佐證資料如：資料盤點表、資料流程說明 (圖) 或其他內部制度文件等)[此段說明文字請刪除]
5.10	是否有利用個人資料進行行銷之情形。					(佐證資料如：資料盤點表、資料流程說明 (圖) 或其他內部制度文件等)[此段說明文字請刪除]
5.11	是否有提供個人資料予第三人之情形。					(佐證資料如：資料盤點表、資料流程說明 (圖) 或其他內部制度文件等)[此段說明文字請刪除]
5.12	若有進行委託或複委託，進行前已得內部核定 (權責主管核可) 並經委託或複委託廠商簽訂委託契約。					無委託或複委託應填不適用 (佐證資料如：複委託契約、保密協議書等)[此段說明文字請刪除]
5.13	定期對委託方或複委託方進行監督並記錄。					無委託或複委託應填不適用 (佐證資料如：契約、查核記錄或其他內部制度文件等)[此段說明文字請刪除]
5.14	具備當事人權利行使流程。					(佐證資料如：內部制度文件等)[此段說明文字請刪除]
5.15	當事人權利行使回覆情形做成紀錄供內部權責人備查。					(佐證資料如：內部制度文件、權利行使之記錄等)[此段說明文字請刪除]

查檢項目		自評內容				簡述原因 並檢附佐證資料
		符合	部分符合	不符合	不適用	
5.16	權責人員應清楚了解個人資料之使用及其保存期限。					(佐證資料如：評估機制記錄或其他內部制度文件等)[此段說明文字請刪除]
5.17	契約終止或解除，應刪除、銷毀所持有之個人資料。					(佐證資料如：契約、查核記錄或其他內部制度文件等)[此段說明文字請刪除]
5.18	契約終止或解除，應返還個人資料之載體。					(佐證資料如：契約、查核記錄或其他內部制度文件等)[此段說明文字請刪除]
5.19	員工離職時，應依規定繳回其使用或保管之資訊資產 (如個人電腦、隨身碟)。					(佐證資料如：查核記錄或其他內部制度文件等)[此段說明文字請刪除]
5.20	新承接人員應變更各系統密碼。					(佐證資料如：查核記錄或其他內部制度文件等)[此段說明文字請刪除]
6. 資料安全與人員管理 (安維辦法第 11、12 條)						
6.1	是否進行去識別化作業？					(佐證資料如：提供資料庫的結構和設計、針對個人資料的去識別化措施或資料加密截圖)[此段說明文字請刪除]
6.2	是否有資料存取控制措施？					(佐證資料如：存取權限管理、監控審核記錄等)[此段說明文字請刪除]
6.3	是否進行檔案加密？					(佐證資料如：存取權限管理、監控審核記錄等)[此段說明文字請刪除]
6.4	是否進行資料備份，並對備份資料採取適當之保護措施？					(佐證資料如：文件備份記錄等)[此段說明文字請刪除]
6.5	資料之傳送是否進行管控？					(佐證資料如：傳送過程使用安全通信協議 (例如 TLS1.2 以上)、存取權限限制等)[此段說明文字請刪除]
6.6	使用資訊系統或其他系統進行個人資料交換時，是否有採取適當保護措施？					(佐證資料如：存取控制措施 (經過授權的使用者才能使用) 或契約協議)[此段說明文字請刪除]

查檢項目		自評內容				簡述原因 並檢附佐證資料
		符合	部分符合	不符合	不適用	
6.7	是否建置防火牆、電子郵件過濾機制或其他入侵偵測設備，並定期更新及執行惡意程式檢測。					(佐證資料如：防毒軟體證明等)[此段說明文字請刪除]
6.8	是否有遠端存取控管措施？					(佐證資料如：IP 限制、使用 VPN 加密通道或雙因子認證)[此段說明文字請刪除]
6.9	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。					(佐證資料如：弱點掃描、滲透測試報告等)[此段說明文字請刪除]
6.10	保有資料者是否遵守保密協定？					(佐證資料如：保密切結書)[此段說明文字請刪除]
6.11	人員進出情形是否具體掌控？					(佐證資料如：人員進出登記簿)[此段說明文字請刪除]
7. 認知宣導與教育訓練 (安維辦法第 13 條)						
7.1	對所屬人員應實施個資保護認知宣導與教育訓練。					(佐證資料如：訓練記錄及其他內部制度文件等，應能呈現教育訓練主題、對象、頻率等資訊)[此段說明文字請刪除]
7.2	對代表人、負責人或個資管理人員依其任務及角色，定期實施教育訓練。					(佐證資料如：訓練記錄及其他內部制度文件等，應能呈現教育訓練主題、對象、頻率等資訊)[此段說明文字請刪除]
7.3	應進行課後評量。					(佐證資料如：訓練記錄或其他內部制度文件等)[此段說明文字請刪除]
7.4	應對新進人員進行教育訓練。					(佐證資料如：訓練記錄及其他內部制度文件等，應能呈現教育訓練主題、對象等資訊)[此段說明文字請刪除]
7.5	對平台使用者進行個資保護之認知宣導或教育訓練。					非經營平台應填不適用 (佐證資料如：契約、查核記錄或其他內部制度文件等)[此段說明文字請刪除]

查檢項目		自評內容				簡述原因 並檢附佐證資料
		符合	部分符合	不符合	不適用	
7.6	訂定個人資料保護守則，要求平台使用者遵守。					非經營平台應填不適用 (佐證資料如：契約、查核記錄或其他內部制度文件等)[此段說明文字請刪除]
8. 設備安全管理 (安維辦法第 14 條)						
8.1	對設備及環境應進行控管與保護。					(佐證資料如：內部制度文件等，應能呈現採取之安全管理措施項目等資訊)[此段說明文字請刪除]
8.2	應定期檢查或維護更新設備。					(佐證資料如：內部評估或稽核記錄、內部制度文件等，應能呈現採取之安全管理措施項目等資訊)[此段說明文字請刪除]
8.3	針對存放個人資料之媒體於報廢或再利用前應進行處理 (如硬碟消磁)。					(佐證資料如：執行記錄、內部評估或稽核記錄、內部制度文件等，應能呈現有效處理之結果)[此段說明文字請刪除]
9. 稽核機制 (安維辦法第 15 條)						
9.1	應訂定個人資料安全稽核機制。					(佐證資料如：稽核相關內部制度文件等，應能呈現稽核之頻率、範圍、效力及方法論等資訊)[此段說明文字請刪除]
9.2	應定期實施稽核。					(佐證資料如：內部評估或稽核記錄等，應能呈現稽核之頻率、範圍、發現或結論、改善措施及稽核採用之方法論等資訊)[此段說明文字請刪除]
10. 紀錄保存 (安維辦法第 16 條)						
10.1	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？)					(佐證資料如：紙本部分：存取及利用紀錄、調閱紀錄、軌跡資料、銷毀紀錄；或是相關日誌 (LOG) 留存)[此段說明文字請刪除]

查檢項目		自評內容				簡述原因 並檢附佐證資料
		符合	部分符合	不符合	不適用	
10.2	管理含有個人資料之資訊系統，是否已建立必要之使用紀錄、軌跡資料 (Log Files) 及證據之保存措施？					(佐證資料如：Log Files 保存，包含資訊系統使用紀錄及軌跡資料紀錄、針對儲存個人資料資料庫的存取紀錄、EDR 偵測回應紀錄、第三方鑑識分析報告)[此段說明文字請刪除]
11. 持續改善 (安維辦法第 17 條)						
11.1	應定期檢視個資保護措施。					(佐證資料如：內部制度文件、定期檢視記錄或採取之措施版次記錄等)[此段說明文字請刪除]
11.2	應針對缺失進行改善。					(佐證資料如：內部制度文件、缺失改善記錄等)[此段說明文字請刪除]
11.3	若有主管機關建議，應依主管機關所提出之建議進行改善？					若無，可填不適用 (佐證資料如：主管機關之要求及對應之處置紀錄等)[此段說明文字請刪除]

備註 | (* 以上查檢項目應適當說明或提出可足資證明之文件名稱)

二、個人資料檔案安全維護計畫(範本)

因應國內外法令規範、消費者意識抬頭、及配合政府打擊詐欺等需求，相關電商業者有必要強化個資保護與資安管理能量，除符合營運所需外，並可減少個資外洩而導致詐騙之情事。此外，透過專業法制團隊協助撰擬之參考指引(包含但不限於：業者應告知消費者事項、個資及資安應行注意事項、系統委外合約、或委外監督準則，甚至涵蓋資料跨境傳輸所需規範或需求)，除提升個資及資安管理能力外，尚將可協助廠商避免個資不當利用或提升當事人權利行使之效益。此外，業者亦可利用本參考指引，做為內部教育訓練、業務執行之參考及說明，以加強內部個資保護與管理之意識與能力。

個人資料檔案安全維護計畫(範本)

(公司名稱)個人資料檔案安全維護計畫(範本)　　僅供參考

訂定日期：中華民國　　年　　月　　日
修訂日期：中華民國　　年　　月　　日

範本僅為舉例參考，請依貴公司內部管理作業程序及實際業務情形訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法等相關事項。
灰底處說明內容請業者閱讀後刪除，底線處請業者依情況填入或選擇文字。

壹、 依據

個人資料保護法第 27 條第 3 項及數位經濟相關產業個人資料檔案安全維護管理辦法。

貳、 目的

落實個人資料檔案之安全維護及管理，防止被竊取、竄改、毀損、滅失或洩漏。

參、 組織規模及特性

一、組織型態：股份有限公司、有限公司、無限公司、兩合公司、獨資或合夥事業
二、代表人(負責人)：○○○
三、公司地址：○○縣(市)○○鄉(鎮、市、區)○○路(街)○段○號○○樓
四、員工人數：約○○人(可記載一定範圍之人數)
五、資本額：新臺幣○萬元。(股份有限公司為實收資本額，於有限公司、無限公司及兩合公司為登記之資本總額，於獨資或合夥方式經營之事業，為登記之資本額。)
六、保有個人資料數量：約○○筆(除客戶外，亦包含員工及第三方)

肆、 個人資料檔案之安全維護管理措施

一、配置管理之人員及資源

(一)管理人員：

1. 配置人數：○○人(至少 1 名)。
2. 職責：負責規劃、訂定、修正與執行本計畫及處理方法等相關事項，並每○○日(或週、月、年)向○○(請填代表人或管理組織名稱)提出報告。

(二)預算：每年新臺幣○○○元。(包含管理人員薪資、資安預算、設備費用、外部單位稽核等，可記載一定範圍之金額，請依貴公司實際狀況填寫)

二、蒐集、處理及利用個人資料之範圍及特定目的

(一)個人資料範圍界定：

1. 本公司每○○日(或週、月、年)就本公司保有之個人資料進行清查及盤點，相關程序另訂之，附件：○○○。(可參考文件"有關電商業者落實數位經濟相關產業個人資料檔案安全維護管理辦法參考指引"「三、個人資料盤點管理程序」進行)
2. 依盤點內容，指本公司蒐集、處理及利用之自然人(包含消費者、使用者、所屬人員等)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。(請依貴公司實際狀況填寫，並註明部門、個人資料使用的單位、蒐集資料之合法依據等)

(二)蒐集、處理及利用個人資料之特定目的：

行銷(040)、契約、類似契約或其他法律關係事務(069)、消費者、客戶管理與服務(090)、消費者保護(091)、網路購物及其他電子商務服務(148)、廣告或商業行為管理(152)、調查、統計與研究分析(157)。(註：個人資料範圍及特定目的，請參考個人資料保護委員會籌備處「個人資料保護法之特定目的及個人資料之類別」https://ws.pdpc.gov.tw/FS01/FilePath/3/relfile/33/554/abb677b4-3a42-445f-9ad3-c87e251f1e97.pdf，依貴公司實際情形填列，亦可填寫具體之特定目的。)

(三)個人資料範圍含有特種個人資料(如病歷、醫療、基因、性生活、健康檢查及犯罪前科)者，應檢視是否符合個資法第6條第1項但書法定情形；個人資料範圍含有一般個人資料者，應檢視是否符合個資法第19條第1項法定情形及特定目的，經當事人同意而為蒐集或處理者，並應確保符合個資法第7條第1項規定。

(四)指定管理人員每○月(或每季、每年)定期清查本公司所保有的個人資料檔案，以及其蒐集、處理和利用個人資料的作業流程，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。

三、個人資料之風險評估及管理機制

(一)風險評估

1. 本公司每○○日(或週、月、年)就本公司保有之個人資料盤點內容進行風險評估，相關程序另訂之，附件：○○○。(可參考文件"有關電商業者落實數位經濟相關產業個人資料檔案安全維護管理辦法參考指引"「四、個人資料風險評估管理程序」進行)
2. 經本公司評估之高(中)風險情形如下：
   (1) 經由本公司或各營業處所電腦下載或外部網路入侵而外洩。
   (2) 經由接觸涉有個人資料之業務書件而外洩。
   (3) 所屬人員或第三人竊取、毀損或洩漏。
   (4) 與所屬單位、業間互為傳輸時外洩(包括分公司間傳輸、與相關業者間傳輸等)。
   (5) ○○。(註：倘經評估有其他風險，請自行增列。)

(二)管理機制

本公司每○○日(或週、月、年)依風險評鑑之風險結果，制訂因應風險所必要之管理措施，包含：

1. 適度設定所屬人員權限，加強使用者代碼、識別密碼之控管及妥適保管文件。
2. 每○○日(或週、月、年)進行網路資訊安全維護及控管。
3. 電子檔案資料視實際需要以加密方式傳輸。

4. 加強對所屬人員及設備之管理。
5. ○○。(註：可依貴公司實際情形自行增列。)

四、 事故之預防、通報及應變機制

(一) 預防：

1. 指定專人辦理安全維護事項，防止本公司保有之個人資料被竊取、竄改、毀損、滅失或洩漏。(請業者將預防有關措施略為舉例，若為資安面之控制措施，可於七 (二) 資料安全管理措施詳述)
2. 本公司保有之個人資料檔案，限承辦人員使用或存取，使用或存取範圍限與其本身業務相關，且存取檔案時須鍵入其個人之使用者代碼及識別密碼。非承辦人員參閱、使用或存取相關個人資料檔案或書件時，應經負責人或經授權之管理人員同意，並留存申請授權與管理人員同意紀錄。
3. 存有個人資料之儲存媒體 (含可攜式媒體)，視必要性採取適當之加密機制；存有個人資料之紙本文件於不使用或下班時，遵守桌面淨空，置於抽屜或儲櫃並上鎖。
4. 存有個人資料之紙本及存放媒介物於報廢汰換或轉作其他用途前，確實刪除資料或格式化，或採物理方式破壞、銷毀，並留存相關銷毀稽核紀錄。
5. 電腦系統安裝防毒軟體並○○ (應明定時間) 更新病毒碼，避免惡意程式與系統漏洞對作業系統之威脅。
6. 對內或對外從事個人資料傳輸時，加強管控避免外洩，並留存相關紀錄。
7. 加強所屬人員教育宣導，並嚴加管制並留存相關紀錄。
8. ○○。(註：可依貴公司實際情形自行增列。)

(二) 通報及應變：

1. 發現個人資料遭竊取、竄改、毀損、滅失或洩漏等安全事故時，即時向○○ (請填負責人或管理組織名稱) 通報。發生個人資料安全事故將危及正常營運或大量當事人權益者，自發現時起 72 小時內，以數位經濟相關產業個人資料檔案安全維護管理辦法之附表二「業者個人資料外洩通報表」通報○○ (全國性公司請填：數位發展部；地方性公司請填：○○縣 / 市政府並副知數位發展部)。
2. 發生個人資料安全事故時，儘速以適當方式通知當事人事故發生之事實、已採取之處理措施以及本公司窗口電話等資訊。窗口資訊：○○○○○○○○○○
3. 發生個人資料安全事故後，針對事故發生原因研議改進措施。
4. ○○。(註：可依貴公司實際情形自行增列。)

五、 個人資料蒐集、處理及利用之內部管理措施

(一) 所屬人員直接向當事人蒐集個人資料時，明確告知當事人以下事項：

1. 本公司名稱。
2. 蒐集目的。
3. 個人資料之類別。(註：可參考個人資料保護委員會籌備處「個人資料保護法之特定目的及個人資料之類別」https://ws.pdpc.gov.tw/FS01/FilePath/3/relfile/33/554/abb677b4-3a42-445f-9ad3-c87e251f1e97.pdf 。)
4. 個人資料利用之期間、地區、對象及方式。
5. 當事人得向本公司請求閱覽、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)利用個人資料為行銷時，當事人表示拒絕行銷後，立即停止利用其個人資料行銷，並將拒絕情形通報本公司彙整後周知所屬各部門及員工。

(四)由指定的管理人員每○月(或每季、每年)清查所保有的個人資料，以確保其符合相關法定要求及特定目的。如果發現資料不再符合法定要求或超出特定目的必要範圍，或在特定目的消失、期限屆滿、契約完成履行、解除或終止後，除非法律規定、業務執行必須或經當事人書面同意，應主動刪除或銷毀該等個人資料，並留存相關紀錄。

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

(六)為維護個人資料之正確性，本公司應主動或依當事人之請求更正或補充之；當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。因可歸責於本公司之事由，未為更正或補充之個資，應於更正或補充後，通知曾提供利用之對象。

(七)本公司委託他人或其他公司蒐集、處理或利用個人資料時，應簽訂委託契約並明確約定其內容，每○月對受託者為適當之監督，並留存相關紀錄。(註：留存相關紀錄指委外合約之修訂、實際監督證據或要求受委託者填具之自評表等。)

(八)數位發展部對網際網路零售業為限制國際傳輸個人資料之命令或處分時，本公司應通知所屬人員遵循辦理。所屬人員將個人資料進行國際傳輸時，應檢視是否受數位發展部限制，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督：

1. 預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。
2. 當事人行使個資法第 3 條所定權利之相關事項。

(九)○○。(註：可依貴公司實際情形自行增列。)

六、 當事人權利行使

當事人或其法定代理人向本公司表示拒絕提供，或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料時，採取下列方式辦理：

(一)提供聯絡窗口：○○○；及聯絡方式：○○○○○○。以上聯絡資訊公告於本公司營業處所或網頁(有網站或其他適當處所者，請增列網站首頁及其他適當地點)。

(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)有個資法第 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，併附理由通知當事人或其法定代理人。

(四)遵守個資法第 13 條處理期限之規定。

(五)當事人查詢或請求閱覽個人資料或製給複製本者，依個資法第 14 條規定得酌收必要成本費用。

七、 設備安全管理、資料安全管理及人員管理措施

(一)設備安全管理

1. 指派專人管理建置個人資料之電腦、自動化機器相關設備、可攜式設備，應定期清點、保養維護，並應注意資料之備份及設備防竊、未經授權攜出等相關安全措施。
2. 建置個人資料之個人電腦，禁止直接作為公眾查詢之前端工具。
3. 應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。
4. 電腦、自動化機器或其他存放媒介物需報廢汰換或轉作其他用途時，本公司負責人或營業處所主管應檢視該設備所儲存之個人資料是否確實刪除、銷毀。委託他人執行者，當對受託者為適當之監督並與其明確約定相關監督事項及方式。

5. 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。
6. 電腦設備報廢或不使用時，確實刪除電腦硬體設備中所儲存之個人資料檔案。
7. ○○○。(註：可依貴公司實際情形自行增列。)

(二) 資料安全管理

1. 資通訊系統存取個人資料之管控：
   (1) 個人資料檔案存放的電腦、自動化機器相關設備或可攜式設備，應設置識別密碼、保護程式密碼、安全防護系統、加密機制及其他相關安全措施。
   (2) 前項安全措施應每月 (或每週、每年) 檢測一次，以避免或降低系統漏洞遭利用或潛在威脅。
   (3) 個人資料檔案使用完畢應即退出或關閉檔案，不得任其停留於電腦螢幕上。
   (4) 建置防火牆、電子郵件過濾機制或其他入侵偵測設備以防止外部網路入侵對策，並每周 / 月進行更新。
   (5) 每○○日 (週、月) 進行電腦系統防毒、掃毒之必要措施，並確保系統穩定性後執行系統更新。
   (6) 重要個人資料應另加設管控密碼，其帳號及密碼須符合一定之複雜度 (請列明複雜度要求)。並定期更換密碼，非經陳報本公司 (商業) 負責人、各營業處所主管或經指定之管理人員核可，並取得密碼者，不得存取。
   (7) 所屬人員非經本公司○○ (請填負責人、管理組織或其他經授權之人員，依貴公司實際情形填寫) 核可，不得任意存取本公司保有之個人資料檔案。
   (8) 本公司應每○週 (或每月) 對所有保有的個人資料檔案進行備份。其中屬重要個人資料者其備份應異地存放，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。
   (9) 本公司蒐集、處理或利用個人資料達○○筆以上時，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 個字以〇標示)、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) (下列擇一)
      □ 本公司不使用真實個人資料進行資通系統測試。
      □ 本公司應避免使用真實個人資料進行資通系統進行測試，若有因測試所必需而使用真實個人資料進行資通系統測試時，應遵守下列規範：○○○○○○○○。
   (11) 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。
   (12) 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。
   (13) 本公司將資料傳輸或儲存於○○○○○○○○提供之雲端服務，並採取○○○○○○○○等 (請填寫如加密、去識別化、權限控制等實際採行之措施) 適當的安全機制。
   (14) ○○。(註：可依貴公司實際情形自行增列。)
2. 紙本資料之保管：
   (1) 本公司保有個人資料存在於紙本者，應存放於公文櫃內並上鎖，非經公司負責人、營業處所主管或經指定之管理人員同意，不得任意複製、拍攝或影印。

(2) 儲存個人資料紙本之保管箱或檔案室內，應設置防火裝置及防竊措施。儲存個人資料之電腦主機系統應設置防火牆，降低外部入侵風險。主機置放之機房應設置門禁、監視錄影及防火設備。

(3) 對於記載個人資料之紙本丟棄時，應先以碎紙設備進行處理。

(4) ○○(註：可依貴公司實際情形自行增列。)

(三) 人員管理

1. 依業務需求適度設定所屬人員 (例如主管、非主管人員) 不同之權限，以控管其個人資料蒐集、處理及利用之情形，並每○月檢視權限之適當性及必要性。
2. 本公司所屬人員使用電腦設備蒐集、處理、利用個人資料，應以專屬帳號密碼登入電腦系統，存取個人資料檔案權限應與所職掌業務相符。專屬帳號密碼均應保密，不得洩漏或與他人共用。
3. 所屬人員應每○週 (或每月、每年) 變更一次登錄電腦的識別密碼，並在變更密碼後才能繼續使用電腦。
4. 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。
5. 本公司與所屬人員間之勞務、承攬及委任契約均列入保密條款及相關之違約罰則，以確保其遵守對於個人資料內容之保密義務 (含契約終止後)。
6. 因業務需要而須利用非權限範圍之特定個人資料者，應事前提出申請，經業務主管人員同意後開放權限利用。
7. 負責個人資料檔案管理人員於職務異動時，應將保管之檔案資料移交，接辦人員應另行設定密碼。
8. 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。
9. ○○。(註：可依貴公司實際情形自行增列。)

八、 認知宣導及教育訓練

(一) 本公司所屬人員每年計有○人參與相關單位辦理之個人資料保護法宣導或數位學習教育訓練至少○小時，以促使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。前述宣導及教育訓練內容應有包含主管機關重要規定的宣導 (如相關辦法、函釋、安維計畫等)，並應留存教育訓練實施紀錄 (例如：簽到表、測驗結果等文件)。

(二) 對於負責人、管理人員應依其於本計畫所擔負之任務及角色，每○月 (年) 實施必要之教育訓練。(需為進階課程)

(三) 對其平台使用者，透過網頁 (有網站或其他適當處所者，請增列網址及其他適當地點) 進行適當之個人資料保護及管理之認知宣導或教育訓練，並訂定個人資料保護守則，要求平台使用者遵守。

(註：此處「平台」特指 B2B2C 或 C2C 型態，提供非平台經營者得上架商品或提供服務之平台，如無經營此類型平台者，得自行刪減本項。)

(四) ○○。(註：可依貴公司實際情形自行增列。)

九、 個人資料安全維護稽核機制

(一) 本公司每○月 (或年) 至少乙次辦理個人資料檔案安全維護稽核，檢查本公司執行本計畫之狀況，將檢查結果作成稽核報告，並向負責人 (或管理組織) 提出，且經其簽名確認。

(二)針對檢查結果不符合或潛在不符合之事項，應規劃改善與預防措施，並確保相關措施之執行。執行改善與預防措施時，應依下列事項辦理：

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

(三)○○。(註：可依貴公司實際情形自行增列。)

十、 使用紀錄、軌跡資料及證據保存

(一)本公司執行本計畫時，應評估其必要性，保存個人資料之蒐集、處理或利用紀錄，及自動化機器設備之軌跡資料(電腦設備或其他相關之證據資料須加以保存並製作備份保存於適當處所以供備查)、落實執行安全維護計畫之證據，並至少留存5年。

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

(三)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，依貴公司實際情形填寫)核可，不得任意取出。

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

十一、 個人資料安全維護之整體持續改善

(一)針對個資安全稽核結果不符合法令之虞者，規劃矯正與預防措施。

(二)本公司將參酌本計畫執行狀況、技術發展、業務調整及法令修正等因素，定期檢討本計畫是否合宜，必要時予以修正。

十二、 業務終止後之個人資料處理方法

本公司業務終止後，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，並留存相關紀錄至少5年：

(一)銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

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

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

三、制度建置

(一) 個人資料盤點管理程序(含個人資料盤點表)

依個資法施行細則第 12 條第 2 項第 2 款「界定個人資料之範圍」及本辦法第 6 條之規定，具體要求業者應定期清查確認所蒐集、處理或利用之個人資料現況，界定納入安全維護計畫之範圍。故電商相關業者應適度掌握內部所保有的個資，此一程序主要可協助業者對於內部個資蒐集、處理及利用之現況有所瞭解，並藉由程序內之個人資料盤點表，完整清點單位所保有之個人資料檔案，並留存相關紀錄，且透過盤點程序，亦能使業者查核所保有個人資料檔案之適法性，以減少違法之風險。

1. 目的：業者為了遵循個人資料保護法之相關法律規定，針對個人資料蒐集、處理及利用之現況瞭解，得參考以下說明內容建置個人資料盤點管理程序。
2. 範圍：凡本公司涉及個人資料蒐集、處理、利用、委託及國際傳輸作業等相關流程及單位均屬之。
3. 權責：
   3.1 個人資料盤點：各單位個資保護專人。
   3.2 個人資料盤點審核：各單位主管、管理代表。
4. 定義：
   個人資料相關之定義 (依個人資料保護法第 2 條之定義)：
   4.1 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。
   4.2 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。
   4.3 蒐集：指以任何方式取得個人資料。
   4.4 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。
   4.5 利用：指將蒐集之個人資料為處理以外之使用。
5. 作業內容：
   5.1 確認個人資料盤點時機：為確保本公司蒐集、處理及利用個人資料的管理符合個人資料保護法之要求，並降低本公司潛在的風險，應依下列時機進行盤點：
      5.1.1 各單位應自動進行個人資料盤點：
         5.1.1.1 個人資料保護法規、命令或目的事業主管機關函令之變更或發佈，而有其必要時；
         5.1.1.2 當本公司因增加新的業務範圍、項目，而產出或變更個人資料蒐集、處理及利用之情形。
      5.1.2 個人資料保護管理執行小組應於下列時機開會討論進行個人資料盤點：
         5.1.2.1 每年定期檢視本公司個人資料風險之評估作業時；
         5.1.2.2 當本公司發生個資事故，需重新檢視個人資料防護作業時。

5.2 個人資料檔案盤點方法：

5.2.1 盤點時應包括各項業務、活動，在正常、異常及緊急與意外狀況等操作所產生之個人資料檔案使用狀況，包括相關流程中輸入(來源)與輸出(產出)之內容，避免遺漏，並將結果登錄於「個人資料盤點表」。

5.2.2 盤點項目依下列填寫重點執行：

5.2.2.1 流程 / 檔案編號：依 5.2.3 規定執行編碼。

5.2.2.2 作業流程：依涉及之個人資料業務行為進行填寫，須將涉及個人資料之流程步驟完整填寫於「作業流程」，再將各步驟之「個人資料行為模式」，依下列代號填入 (可複選)：1. 蒐集；2. 處理；3. 利用；4. 委託行為。

5.2.2.3 個人資料檔案：

1. 填入該步驟涉及之「資料檔案名稱」，並依下列代號，填入其「資料檔案類型」：1. 紙本；2. 電子檔；3. 作業系統資料庫。
2. 如同一資料於作業流程中會產生兩種以上資料檔案類型，則需另以一列表示其作業流程內容。

5.2.2.4 特定目的、法定情形與個人資料之類別：

1. 特定目的依個人資料保護委員會籌備處公告之「個人資料保護法之特定目的及個人資料之類別」之代碼進行填寫。
2. 法定情形依個資法第 19 條蒐集、處理個人資料之法定情形填寫，並應檢附理由或說明。
3. 個人資料類別依個人資料保護委員會籌備處公告之「個人資料保護法之特定目的及個人資料之類別」(附表一) 之代碼進行填寫。

5.2.2.5 資料來源：依下列代碼進行填寫：

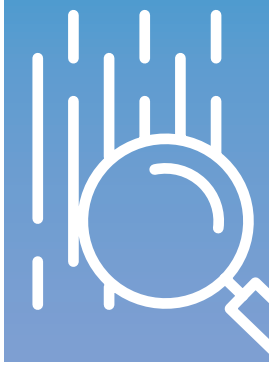
1. 直接向當事人蒐集；
2. 內部單位提供 (註明來源 _____)；
3. 外部間接蒐集 (註明來源 _____)；

5.2.2.6 蒐集：

1. 蒐集方法依下列代碼進行填寫：1.Email；2. 網路平台；3. 電話 / 現場 / 口頭；4. 傳真；5. 紙本送達；6. 其他。
2. 告知事項：確認是否有踐行告知義務，或符合法定要項可免告知。
3. 如該個人資料流程未有蒐集行為，則該欄位以斜線表示。

5.2.2.7 處理：

1. 保管方式依下列代碼進行填寫：1. 儲存個人電腦；2. 儲存於資料庫 / 主機；3. 存放作業區域個人櫃 / 抽屜；4. 存放檔案室；5. 其他。
2. 保存期限依法定要求填寫，如無法定要求，則填寫自訂保存年限。
3. 刪除 / 銷毀方式，依目前執行方式填寫：1. 統一刪除 / 銷毀；2. 由承辦人自行刪除 / 銷毀；3. 目前無刪除 / 銷毀。
4. 內部傳送：說明對象單位及用途。
5. 如該個人資料流程未有處理行為，則該欄位以 N/A 表示。



5.2.2.8 利用：

1. 說明對象機構及用途，如該個人資料流程未有利用行為，則該欄位以 N/A 表示。
2. 資料利用方法依下列代碼進行填寫：1.Email；2. 網路平台；3. 電話 / 現場 / 口頭；4. 傳真；5. 紙本送達；6. 其他。

5.2.2.9 委託：說明於本業務流程中，將全部或部分業務委託之受託機關名稱。

5.2.3 個人資料檔案編號：(作業流程編號)-(檔案流水編號)

編號：XXXX – XX . XX

(單位代號)-(作業流程編號)(檔案流水編號)

1. 單位代號：依本公司規定之單位代號。
2. 作業流程編號：「個人資料盤點表」上所排列之流程序列，01、02...。
3. 檔案流水編號：個人資料檔案之流水編號 01、02...。

5.3 「個人資料盤點表」完成後，須交單位主管及管理代表審核後存查。

5.4 「個人資料盤點表」完成後，再依「個人資料風險評估管理程序」進行風險識別及評估。

6. 相關文件：

6.1 個人資料風險評估管理程序

7. 使用表單：

7.1 個人資料盤點表

個人資料盤點表(範例)

流程 / 檔案編號	作業流程			個人資料檔案		保有之特定目的、法定情形與個人資料之類別			資料來源	蒐集		處理				利用		委託
	作業流程名稱	流程步驟	個資行為模式 (可複選)	資料檔案名稱	資料檔案類型	特定目的 (必填)※附表一	法定情形 (需附理由說明)	個人資料之類別 ※附表一		蒐集方法	告知事項	保管		刪除 / 銷毀	內部傳送	傳遞		委託機關
												保管方式	保存期限			傳遞對象及目的	傳遞方式	
說明各單位流程編號：(單位代號)-(作業流程編號). (檔案流水編)	作業流程	流程步驟	1. 蒐集 2. 處理 3. 利用 4. 委託行為	個人資料檔案名稱 (表單、應用程式，或 ISO 單號)	1. 紙本 2. 電子檔 3. 作業系統資料庫	◎依該個人資料蒐集、處理或利用流程之特定目的			1. 內部 (註明來源 ____) 2. 外部 (註明來源 ____) 3. 直接向當事人蒐集 4. 間接蒐集 (註明來源____)	1. Email 2. 網路平台 3. 電話 / 現場 / 口頭 4. 傳真 5. 紙本送達 6. 其他____	1. 有告知 (說明告知方式、內容 ____) 2. 免告知 (說明原因____) 3. 目前尚無告知	1. 儲存個人電腦 2. 儲存於資料庫 / 主機 3. 存放作業區域個人櫃 / 抽屜 4. 存放檔案室 5. 其他____	1. 法定保存期限 (____) 2. 自訂保存期限 (____) 3. 無保存期限	1. 統一銷毀 2. 由承辦人自行銷毀 3. 目前無銷毀	1. 國內 (說明對象單位及用途 ____) 2. 國外 (說明對象單位、國家及用途	1. 國內 (說明對象機構及用途 ____) 2. 國外 (說明對象機構、國家及用途 ____)	1. Email 2. 網路平台 3. 電話 / 現場 / 口頭 4. 傳真 5. 紙本送達 6. 其他____	請註明受託機關名稱

管理代表：　　單位主管：　　單位個資保護專人：

三、制度建置

(二) 個人資料風險評估管理程序(含個人資料風險評鑑表、高風險回應計畫)

依個資法施行細則第 12 條第 2 項第 3 款「個人資料之風險評估及管理機制」及本辦法第 7 條之規定，要求業者應依已界定之個人資料範圍及其業務涉及個人資料蒐集、處理或利用之流程，定期評估可能產生之風險，並根據風險評估結果，採行適當之安全措施。而本程序可協助業者藉由盤點程序所完成之盤點表內容，界定個人資料檔案之風險值，並透過風險回應措施，有效的採取安全維護措施及應變機制，以降低個資事故發生的可能性。

個人資料風險評估管理程序

1. 目的：業者為了遵循個人資料保護法之相關法律規定，針對個人資料之可能面臨之威脅、弱點及風險之識別及管理，得參考以下說明內容建置個人資料風險評估管理程序。
2. 範圍：凡本公司涉及個人資料蒐集、處理、利用之流程及單位均屬之。
3. 權責：
   3.1 風險評估作業：各單位個資保護管理專人。
   3.2 高風險回應：各單位個資保護管理專人、單位主管。
   3.3 風險處置追蹤：管理代表。
   3.4 風險評估作業審核：管理代表。
4. 定義：無。
5. 作業內容：
   5.1 各單位依「個人資料盤點管理程序」所盤點之個人資料相關業務流程，依其流程 / 檔案編號、作業流程；個人資料檔案及個人資料之類別填入「個人資料風險評估表」中。
   5.2 風險評鑑標準：
   5.2.1 個人資料價值評值：

重要性等級	個人資料類別
重要 (高)	含有特種個人資料如有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料； 個人資料類別代碼：個人資料類別項目 C一一一：健康紀錄。 C一一二：性生活。 C一一三：種族或血統來源。 C一一六：犯罪嫌疑資料。 C〇六六：健康與安全紀錄。

<table>
<tr><td>敏感 (中)</td><td>個人銀行帳戶及其他財務資訊；<table>
<tr><td>C〇〇二</td><td>識別財務者。</td></tr>
<tr><td>C〇〇三</td><td>政府資料中之辨識者。</td></tr>
<tr><td>C〇三二</td><td>財產。</td></tr>
<tr><td>C〇八一</td><td>收入、所得、資產與投資。</td></tr>
<tr><td>C〇八二</td><td>負債與支出。</td></tr>
<tr><td>C〇八三</td><td>信用評等。</td></tr>
<tr><td>C〇八四</td><td>貸款。</td></tr>
<tr><td>C〇八五</td><td>外匯交易紀錄。</td></tr>
<tr><td>C〇八六</td><td>票據信用。</td></tr>
<tr><td>C〇八七</td><td>津貼、福利、贈款。</td></tr>
<tr><td>C〇八八</td><td>保險細節。</td></tr>
<tr><td>C〇八九</td><td>社會保險給付、就養給付及其他退休給付。</td></tr>
<tr><td>C〇九一</td><td>資料主體所取得財貨或服務。</td></tr>
<tr><td>C〇九二</td><td>資料主體提供之財貨或服務。</td></tr>
<tr><td>C〇九三</td><td>財務交易。</td></tr>
<tr><td>C〇九四</td><td>賠償。</td></tr>
</table></td></tr>
<tr><td>一般 (低)</td><td>含有一般個人資料如姓名、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、職業等「個人資料保護法」定義之具唯一性 / 可以直接識別出當事人之個人資料 (唯一性個人資料：相片、指紋、ID、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼)；
非屬特種個人資料及財務細節之其他個人資料均屬之。<table>
<tr><td>C〇〇一</td><td>識別類</td></tr>
<tr><td>C〇一一 ~ C〇一四</td><td>特徵類</td></tr>
<tr><td>C〇二一 ~ C〇二四</td><td>家庭情形</td></tr>
<tr><td>C〇三一 ~ C〇四一</td><td>社會情況</td></tr>
<tr><td>C〇五一 ~ C〇五八</td><td>教育、考選、技術或其他專業</td></tr>
<tr><td>C〇六一 ~ C〇七三</td><td>受僱情形</td></tr>
<tr><td>C一〇一 ~ C一〇三</td><td>商業資訊</td></tr>
<tr><td>C一三一 ~ C一三四</td><td>其他各類資訊</td></tr>
</table></td></tr>
</table>

評值	個人資料屬性
高	民眾 / 客戶
中	內部員工
低	廠商

個人資料價值矩陣表				
個人資料來源		供應商	員工	民眾 / 客戶
個人資料類別		低	中	高
一般	低	低	低	中
敏感	中	低	中	高
重要	高	中	高	高

5.2.2 個人資料行為評價：

弱點等級	個人資料行為模式
高	委託外部廠商執行個人資料蒐集、處理或利用
中	個人資料蒐集、利用
低	個人資料內部處理

5.2.3 個資弱點與威脅評估：

個資弱點對照表	
	個資弱點
高	違反個資法及相關法令，或合約要求
	無相對應管理程序規制，或個資檔案無專人控管
	無安全管控措施，如紙本彌封、專人傳遞、檔案櫃上鎖，或資料加密、防火牆、防毒軟體、權限控管、滲透測試等
中	違反組織內部規範
	有相應管理措施，但無有效執行，或無保留相關紀錄
	有安全管控措施，但未確實執行
低	符合個資法、相關規範、合約要求及組織內部規範等
	有相對應管理程序規制，且確實落實執行並保留相關紀錄
	有安全管控措施，且措施皆正常運作，且有保留相關紀錄

威脅發生頻率或可能性	
高	每年 5 件以上
中	每年 5 件以下
低	未曾發生

個資弱點與威脅評值矩陣表

個資弱點與威脅評值

	威脅發生頻率或可能性			
個資弱點	評值	低	中	高
	低	低	低	中
	中	低	中	高
	高	中	高	高

5.2.4 個人資料風險總評值矩陣圖

個資風險總評值

個人資料行為評估	個人資料價值								
	低			中			高		
	個人資料事件發生頻率								
	低	中	高	低	中	高	低	中	高
低	1	2	3	2	3	4	3	4	5
中	2	3	4	3	4	5	4	5	6
高	3	4	5	4	5	6	5	6	7

5.3 風險評估資料審查：

5.3.1 彙總資料並依個人資料風險總評值矩陣圖，確認各項得分，並由推行小組及管理代表決議擬定不可接受風險值 (高風險)。

5.3.2 個人資料保護管理推行小組每年至少應重新審查個人資料檔案價值、威脅、弱點、處理基準值。

5.4 風險回應：

5.4.1 各單位個資保護專人應將不可接受風險值 (高風險) 之個人資料檔案彙整到「高風險回應計畫」進行個人資料安全控制措施之確認。

5.4.2 專人並應於回應計畫中填具「目前採取控制措施確認」欄位，以確認目前單位針對該高風險個人資料檔案所採取之管控措施，如目前無任何管控措施則寫「無」。

5.4.3 專人並應與單位主管討論後，決定改善措施並填具於「採取加強控制措施」，並於欄位中說明預計改善完成日期，俾便有效降低高風險並利於追蹤確認。

5.4.4 管理代表應定期追蹤確認改善情形，並將改善建議填具於「追蹤後建議」欄位，如已無須進一步追蹤，可填寫「已結案」。

5.4.5 針對不可接受風險值 (高風險) 之個人資料檔案，於執行改善加強控制措施後，如仍無法降低個資風險，但經管審會議決議後，可接納此風險，並持續控管之。

5.5 「個人資料風險評鑑表」及「高風險回應計畫」須交單位個資保護專人及單位主管簽核後，交本公司管理代表存查。

6. 相關文件：

6.1 個人資料盤點管理程序

7. 使用表單：

7.1 個人資料盤點表

7.2 個人資料風險評鑑表

7.3 高風險回應計畫

個人資料風險評鑑表(範例)

流程 / 檔案編號	作業流程			個人資料檔案			個資來源			個人資料類別			價值評值	個資行為評估			個資行為評價	個資弱點與威脅評估			個資風險總評值	高風險(以◎標註)
	作業流程名稱	流程步驟	個資行為模式(可複選)	資料檔案名稱	資料檔案型態(可複選)	個人資料之類別	廠商	員工	民眾 / 客戶	一般個資	財務細節	特種個資		個人資料內部處理	個人資料外部蒐集、利用	委託外部廠商執行個資蒐集、處理或利用		低	中	高		
說明各單位流程編號：(單位代號)-(作業流程編號)	作業流程	流程步驟	1. 對外蒐集 2. 處理 3. 利用 4. 委託行為	個人資料檔案名稱(表單、應用程式，或ISO 單號)	1. 紙本 2. 電子檔 3. 作業系統資料庫		低	中	高	低	中	高		低	中	高						

管理代表：　　單位主管：　　單位個資保護專人：

高風險回應計畫(範例)

流程/檔案編號	作業流程			個人資料檔案			價值評值	個資行為評價	個資弱點與威脅評估	個資風險總評值	目前採取控制措施確認	採取加強控制措施	採取措施追蹤日期	剩餘個資風險總評值	追蹤後建議	追蹤確認人
	作業流程名稱	流程步驟	個資行為模式	資料檔案名稱	資料檔案型態	個人資料類別										

管理代表：　　單位主管：　　單位個資保護專人：

(三) 個人資料事故緊急應變處理程序(含個人資料事故通報與處理單及事故應變通報清冊)

依個資法施行細則第 12 條第 2 項第 4 款「個人資料之風險評估及管理機制」及本辦法第 8 條之規定，要求業者為因應當事人個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故，應訂定下列應變、通報及預防機制，以降低當事人損害。而本程序提供業者規劃應變措施的參考，如應變組織、通報清單暨通報辦法、事件預防、損害抑止，以及事故發生原因矯正追蹤等內容，希望透過業者預先規劃應變措施，以減少當事人損失，並降低事故對其造成之損害。

個人資料事故緊急應變處理程序

1. 目的：業者為確保於個人資料事故發生時，能迅速依程序進行通報，並採取必要之應變措施與建立事故預防機制，以降低事故所造成之損害，得參考以下說明內容建置個人資料事故緊急應變處理程序。
2. 範圍：本公司各單位於作業時發現個人資料事故之因應、通報、處置及改善作業。
3. 權責：
   - 3.1 事故緊急應變通報：全公司同仁。
   - 3.2 受理事故緊急應變通報：事故單位個人資料保護管理專人。
   - 3.3 事故緊急應變執行內容擬定：事故單位個人資料保護管理專人及單位主管。
   - 3.4 事故緊急應變執行內容核准：管理代表及個人資料保護推行小組。
   - 3.5 事故緊急應變內容執行:事故單位個人資料保護管理專人及單位主管。
   - 3.6 事故緊急應變執行結果確認：管理代表及個人資料保護推行小組。
4. 定義：無。
5. 作業內容：
   - 5.1 事故通報作業：
     - 5.1.1 各單位同仁如發現有個人資料安全事故發生或接獲其他單位同仁通知個人資料安全事故時，應立即向單位個人資料保護管理專人反應，由專人填寫「個人資料事故通報與處理單」，並進行通報。
     - 5.1.2 事故通報說明：
       - 5.1.2.1 專人應通報個人資料保護推行小組及管理代表，並依據本程序 5.2 至 5.5，進行事故應變與處理，並填寫「事故應變通報清冊」，以保留紀錄。
       - 5.1.2.2 專人應將本程序 5.2 至 5.5 之處理內容紀錄，填寫「業者個人資料外洩通報表」向目的事業主管機關通報，或視情況向檢警機關報案。
       - 5.1.2.3 通報對象：數位發展部；電話：02-23808390；信箱：www-mailbox.adi.gov.tw。
       - 5.1.2.4 通報內容：事件發生種類、外洩大略筆數、發生原因及事件摘要、採取的因應措施、通知當事人的時間和方法。
       - 5.1.2.5 如有必要，專人得通報專家、學者、輔導顧問或技術人員等，以協助辨識、排除或解決個人資料事故。

5.2 事件處理：

5.2.1 對外發言：

5.2.1.1 如個人資料事故或遇到個人資料事故需對媒體或外部團體說明時，個人資料保護推行小組應討論個人資料事故發生原因與擬採取之因應措施，並指定小組成員一人為聯絡窗口統一對外發言。

5.2.1.2 如需通知個人資料事故，應以適當方式通知個人資料事故當事人，所謂適當方式包含即時以言詞、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。

5.2.1.3 通知個人資料事故之當事人，通知內容應包含個人資料被侵害之事實及採取之因應措施並提供後續查詢與處理管道。

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

5.2.2 事故辨識作業：

5.2.2.1 事故單位個人資料保護管理專人應依「個人資料事故通報與處理單」進行事故處理。

5.2.2.2 事故單位個人資料保護管理專人應將辨識結果記錄在「個人資料事故通報與處理單」之中。

5.2.2.3 辨識工作完成前，應儘可能避免系統重新開機或變更個人資料相關紀錄流程，以保全完整證據。若系統必須重新開機，則應於重新開機前保留系統稽核紀錄檔案。

5.3 事故抑制作業：

5.3.1 事故單位個人資料保護管理專人應依個人資料安全事故辨識結果，針對異常狀況採取緊急抑制措施，並將抑制方法記錄在「個人資料事故通報與處理單」。

5.3.2 緊急抑制措施應以隔離或停止事故發生之作業、設備、系統、環境及存取權限或連線為原則。

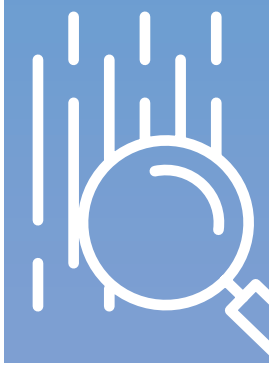
5.4 事故排除作業：

5.4.1 事故單位個人資料保護管理專人應依個人資料安全事故發生之原因，進行事故排除作業。

5.4.2 為避免事故排除作業造成重要資料或鑑識證據之遺失，應於事故排除作業前完成重要設定檔、資料與鑑識紀錄檔之備份。

5.4.3 備份作業完成後，應確認備份資料之有效性與可用性，以避免備份失敗導致資料毀損。

5.4.4 事故排除作業除需移除個人資料安全事故原因外，應依事故發生原因加強防護，並進行矯正及加強防護的措施，作為往後個人資料安全日常管理的參考，以避免相同事故再次發生。



5.5 事故應變執行內容核准、結果確認：

5.5.1 個人資料事故之事故單位個人資料保護管理專人及單位主管擬定執行內容 (事故辨識作業、事故抑制、排除作業) 向權責單位報告核准，並於執行完畢後，由權責單位進行執行結果確認。

5.6 事故檢討與學習：

5.6.1 個人資料安全事故處理過程應由事故單位個人資料保護管理專人填寫「個人資料事故通報與處理單」，並保存所有事故分析及處理紀錄。

5.6.2 個人資料安全事故發生後，應提報個人資料管理審查會議，討論是否修訂相關安全政策與規範，以防止事故再次發生。

5.6.3 個人資料安全事故處理結果，在無牽涉個人隱私與業務機密之情況，應定期彙整並公告於內部網站，描述事故發生原因、過程、處理方式、改善與注意事項等，作為內部個人資料宣導及事故預防之參考資訊。

6. 相關文件：無

6.1 附件：非公務機關發生個資事故時對個資當事人通知

7. 使用表單：

7.1 個人資料事故通報與處理單

7.2 業者個人資料外洩通報表

7.3 事故應變通報清冊

附件：非公務機關發生個資事故時對個資當事人通知(範例)

(1) 標準範例

親愛的消費者 / 會員您好：

非常抱歉，近期(公司或網站名稱)因(原因)發生個人資料外洩事故，您的資料包含在此次事故範圍內，且已有消費者接獲詐騙訊息(若無則刪除)。提醒您，詐騙集團通常於週末或下班時間以(手法)誆騙消費者。如接獲疑似詐騙電話，請不要聽從指示操作 ATM 或提供任何個人資料，並立即通報 165 警政署反詐騙專線。

針對這次事件，本公司已採取 (請詳述 1. 立即止損方式及 2. 後續改善措施)，未來也會持續加強資訊安全與個人資料保護管理，以降低消費者個資被侵害之風險。

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

(公司名稱) 敬上

(2) 事故發生於較久以前

親愛的消費者 / 會員您好：

非常抱歉，(公司或網站名稱)曾於(業者掌握的事發期間或警政署來函所載之區間)因(原因)發生個人資料外洩事故，您的資料包含在此次事故範圍內，且已有消費者接獲詐騙訊息(若無則刪除)。提醒您，詐騙集團通常於週末或下班時間以(手法)誆騙消費者。如接獲疑似詐騙電話，請不要聽從指示操作 ATM 或提供任何個人資料，並立即通報 165 警政署反詐騙專線。

針對這次事件，本公司已(請詳述 1. 立即止損方式及 2. 後續改善措施)，且於近期未再接收到相關通報(請向警政機關確認，若有則刪除)。本公司未來也會持續加強資訊安全與個人資料保護管理，以降低消費者個資被侵害之風險。

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

(公司名稱) 敬上

(3) 事故發生原因不明

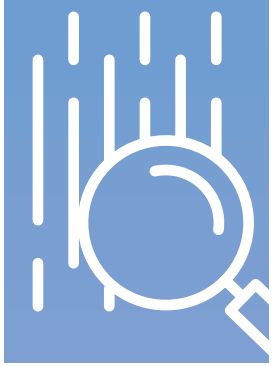
親愛的消費者 / 會員您好：

非常抱歉，(公司或網站名稱)發生個人資料外洩事故，您的資料包含在此次事故範圍內，且已有消費者接獲詐騙訊息(若無則刪除)。提醒您，詐騙集團通常於週末或下班時間以(手法)誆騙消費者。如接獲疑似詐騙電話，請不要聽從指示操作 ATM 或提供任何個人資料，並立即通報 165 警政署反詐騙專線。

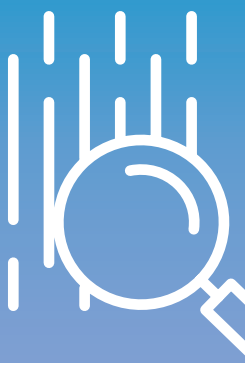
針對這次事件，本公司已(立即止損方式)並對(請列舉公司調查之系統 / 資料庫等)進行相關調查，並針對所有可能發生事故之系統及流程採行(後續改善措施)，且於近期未再接收到相關通報(請向警政機關確認，若有則刪除)。本公司未來也會持續加強資訊安全與個人資料保護管理，以降低消費者個資被侵害之風險。

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

(公司名稱) 敬上



三、制度建置



(4) 事故肇因源於委外廠商

親愛的消費者 / 會員您好：

非常抱歉，(公司或網站名稱)因(資訊系統廠商／委外物流業者，詳述原因)而導致本公司會員／訂單資料發生個人資料外洩事故，您的資料包含在此次事故範圍內，且已有消費者接獲詐騙訊息(若無則刪除)。提醒您，詐騙集團通常於週末或下班時間以(手法)誆騙消費者。如接獲疑似詐騙電話，請不要聽從指示操作 ATM 或提供任何個人資料，並立即通報 165 警政署反詐騙專線。

針對這次事件，本公司已(請詳述 1. 立即止損方式及 2. 針對委外廠商採取之後續改善措施)，且於近期未再接收到相關通報(請向警政機關確認，若有則刪除)。本公司未來也會持續加強資訊安全與個人資料保護管理，並加強對委外廠商之監督，以降低消費者個資被侵害之風險。

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

(公司名稱) 敬上

個人資料事故通報與處理單(範例)

編號：　　填表日期：　　年　　月　　日

事故通報來源	☐ 民眾 ☐外部機構 / _____ 必填) ☐ 內部通知單位人員：_____ 部 _____ 人員
通報人	事故單位
	姓名
	聯絡電話
	電子郵件
發生時間	年　月　日　時　分
事故說明	
個人資料檔案事故辨識作業	事故所涉及個人資料檔案影響評估 (如檔案種類、檔案數量、檔案內容描述)
	受影響業務 / 系統 (如：售票系統、購物網站等)
	可能造成當事人損失之評估說明 (如：遭到詐騙、被騷擾等)

事故抑制、排除作業：包含內、外部處理過及處理時間 (如：已採取或擬取應變措施，並於何時完成)

事故應變通報清冊(範例)

編號	通報單位	承辦人	聯絡電話	傳真	電子郵件	地址
1	數位發展部		02-23808390		www-mailbox.adi.gov.tw	

三、制度建置

(四) 個人資料委外處理管理程序(含個人資料業務委外契約範例)

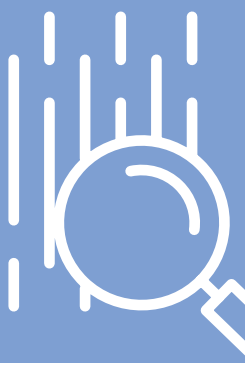
依本辦法第 19 條第 2 項之規定，具體要求業者委託他人蒐集、處理或利用個人資料者，應對受託者依個資法施行細則第 8 條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。而本程序可做為業者對委外廠商執行個資業務時監督管理的參考辦法，並於程序中提供委外契約範例，並可讓業者透過使用「數位發展部所管電商業者個資防護企業自評表」，瞭解委外廠商對於個人資料保護與管理的程度，以落實監督管理之責。

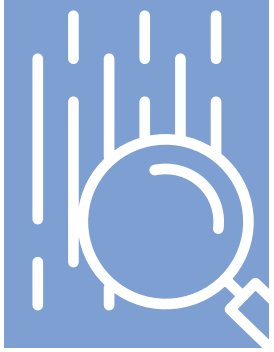
有關本指引內所提示的各項義務，原則上係作為電商業者自我檢視之用途。若業者當公司有發生個資外洩事故，致民眾受到不法侵害時，業者是否有違反個人資料保護相關法令之情形，決定應承擔之法律責任，仍須視個案具體事實認定之。

個人資料委外處理管理程序

1. 目的：業者為確保公司業務委外作業之個人資料安全，並能符合內部作業流程要求，得參考以下說明內容建置個人資料委外處理管理程序。
2. 範圍：凡本公司委外作業涉及個人資料蒐集、處理或利用者均屬之。
3. 權責：
   3.1 委託單位：擬定個人資料相關之委外服務之規格、契約內容、保密協議以及適當安全維護措施要求，並於契約期間內負責委外廠商相關管理作業事項。

4. 定義：
   4.1 委託單位：本公司將全部或部分業務委託另一機關或個人之業務承辦單位
   4.2 受託單位：指接受本公司委託單位之委託，而代為執行本公司個人資料之蒐集、處理或利用相關業務之另一機關或個人。
5. 作業內容：
   5.1 受託單位遴選
      5.1.1 委託單位於簽訂委外契約前，應進行受託單位之遴選。
      5.1.2 遴選之內容除服務品質、產品製程效率等之外，尚應就受託單位之個人資料保護與管理能力，納入評核項目如下列擇一：
         5.1.2.1 受託機關就受委託業務業有導入個人資料保護與管理制度(如臺灣個人資料保護與管理制度(TPIPAS)驗證，並持續維持其驗證有效性)。
         5.1.2.2 受託機關內部就受託業務業有導入個人資料保護管理制度，並能提出相關文件資料佐證。
         5.1.2.3 受託機關填具「數位發展部所管電商業者個資防護企業自評表」。
      5.1.3 於綜合評估受託機關於業務及個人資料保護之能力後，由委託機關擇選合適廠商，簽訂「個人資料業務委外契約」，要求受託單位人員於契約規定期間所知悉之業務資訊，應遵守「個人資料保護法」及本公司相關規定，且不得對外透露，並應視情況要求受託單位或其人員簽署保密協議書。
   5.2 受託單位監督：
      5.2.1 選擇受託對象時，應將受託單位之個人資料安全維護措施辦理情形列為單位之評選項目，包含但不限於下列項目：
         5.2.1.1 配置管理之人員及相當資源
         5.2.1.2 界定個人資料之範圍
         5.2.1.3 個人資料之風險評估及管理機制
         5.2.1.4 事故之預防、通報及應變機制
         5.2.1.5 個人資料蒐集、處理及利用之內部管理程序
         5.2.1.6 資料安全管理及人員管理
         5.2.1.7 認知宣導及教育訓練
         5.2.1.8 設備安全管理
         5.2.1.9 資料安全稽核機制
         5.2.1.10使用紀錄、軌跡資料及證據保存
         5.2.1.11個人資料安全維護之整體持續改善
      5.2.2 監督方式：
         5.2.2.1 由受託單位主動提具如 5.1.2 所指之相關證書、證明文件、資料，或配合填具「數位發展部所管電商業者個資防護企業自評表」。
         5.2.2.2 由委託單位執行對受託單位之監督評核，如現場查核、電話訪查，要求提供書面證明等。





5.2.3 委託單位定期確認受託者頻率：

5.2.3.1 委託契約時間半年以下者：委託單位定期確認受託者執行之狀況，如於選擇受託單位時，已將受託者之個人資料安全維護措施辦理情形列為單位之評選項目，可免執行定期確認。

5.2.3.2 委託契約時間半年以上、1 年以下者：定期確認受託者頻率不可少於 1 次。

5.2.3.3 委託契約時間 1 年以上者：定期確認受託者頻率每年不可少於 2 次。

5.3 服務變更管理：受託單位所提供之服務內容有變動時，依照變動程度，進行變更契約或重新簽定時，依本公司契約簽定作業規定處理，並確保契約內容符合相關個人資料保護與管理之要求。

6. 相關文件：

6.1 附件：個人資料業務委外契約

7. 使用表單：

7.1 數位發展部所管電商業者個資防護企業自評表

附件：個人資料業務委外契約 (範例)

個人資料業務委外契約 (範例)

立約人

甲方： XXX 公司 (委託方)

乙方：_____ (受託方)

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

第一條、個人資料告知條款

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

第二條、個人資料之定義、委託範圍

(一) 本約之個人資料其蒐集、處理及利用行為，悉遵照個資法等相關法規之定義。

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

1. 個人資料之特定目的：
2. 個人資料之類別：
3. 個人資料之範圍：
4. 個人資料之利用期間：

第三條、執行_____業務關於個人資料防護之約定

(一) 乙方應視公司規模、營運狀況採取下列措施：
1. 配置管理之人員及相當資源。
2. 界定個人資料之範圍。
3. 個人資料之風險評估及管理機制。
4. 事故之預防、通報及應變機制。
5. 個人資料蒐集、處理及利用之內部管理程序。
6. 資料安全管理及人員管理。
7. 認知宣導及教育訓練。
8. 設備安全管理。
9. 資料安全稽核機制。
10. 使用紀錄、軌跡資料及證據保存。
11. 個人資料安全維護之整體持續改善。

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

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

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

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

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

第四條、保留指揮監督事項

甲方保留指揮監督事項如下：

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

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

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

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

(五) 個人資料之清冊其內容應包括交付各種紙本及電子形式之個人資料。

第五條、複委託

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

第六條、保密協議

(一) 乙方因履行甲方委託契約所取得或知悉甲方之個人資料，應負保密義務。
(二) 本約所稱之個人資料，係指甲方所擁有之個人資料，或依法律及契約應由乙方負保密義務之個人資料，不論其係以口頭、書面或電子紀錄等任何形式呈現，除經甲方事先書面同意、甲方自行公開或其他法律另有規定之情況外，乙方及所屬人員均應負保密義務，絕不洩漏、販售、交付或以其他方式予甲方以外之第三人知悉 (但經甲方指定之第三人不在此限)、持有或利用，亦不得自行複製、留存而為契約目的以外之利用。
(三) 乙方應簽署保密切結書予甲方，若乙方所屬人員有違反本約有關保密義務之行為，視為乙方之違約行為。

第七條、委託個人資料之稽核

(一) 乙方應依個人資料保護相關法規就受甲方委託之業務定期(每____個月)記錄及稽核，並配合甲方之稽核業務，依甲方之指示提供相關文件，不得拒絕。
(二) 乙方為處理委託事務而須處理或利用甲方所蒐集之個人資料時，乙方應遵守個人資料法之相關規定，同時對於甲方所制 (訂) 定相關標準作業程序，乙方亦應遵守之。甲方認有必要時，並得隨時於本約委託事務之範圍內進行檢查，乙方不得拒絕。
(三) 乙方及其所屬人員之行為若違反個人資料法相關規定或甲方制 (訂) 定之相關標準作業程序蒐集、處理及利用個人資料，進而造成個人資料被竊取、洩漏、竄改或其他侵害者，乙方應立即通知甲方(通知事項包含查明原因及採行之補救措施)，且依甲方之指示方式及指示內容通知個人資料之當事人。
(四) 甲方若有相當之事實發現乙方及其所屬人員可能涉及違反本約或個人資料保護相關法令規定之行為時，乙方應盡最大努力協助甲方調查，提供所有必要之資料，並為各項必要之配合行為。
(五) 若違反個人資料法係由乙方、乙方所屬人員或複委託廠商之行為所致者，乙方應協助甲方對外說明，並於所有訴訟程序中，協助甲方舉證已盡相關之個人資料防護義務。

第八條、違約賠償

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

1. 違反本契約第 3 條關於個人資料防護之約定。
2. 違反本契約第 4 條甲方保留指揮監督事項之約定。
3. 違反本契約第 5 條複委託之約定。
4. 違反本契約第 6 條保密義務之約定。
5. 違反本契約第 7 條稽核之約定，經通知限期改善而未改善完成者。

第九條、契約解除

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

簽約人

甲方：XXX 公司　　乙方：
代表人：　　代表人：
地址：　　地址：

中華民國　　年　　月　　日

肆 結論與建議

一、因應個人資料保護與管理之多元化工具

(一) 臺灣個人資料保護與管理制度(Taiwan Personal Information Protection and Administration System, TPIPAS)

臺灣個人資料保護與管理制度「Taiwan Personal Information Protection and Administration System (TPIPAS)」[32] 是我國唯一由政府推動的個人資料管理制度(Personal Information Management System, PIMS)，我國頂尖智庫財團法人資訊工業策進會科技法律研究所擔任 TPIPAS 維運機構，由專業團隊負責其維運與持續追蹤國內外隱私保護趨勢接軌。

TPIPAS 的設計是基於我國個人資料保護法、OECD、APEC、GDPR 對於個人資料保護要求之重要原則，並結合「個資法遵要求」、「組織管理流程」與「政府認證標章」，從法律面、管理面與程序面確保組織有充分、適當的管理與控制程序，能夠足以符合國內個人資料保護法之最佳法遵實務要求，更有助於達成保護個人資料之目的，組織導入 TPIPAS 可增強客戶、消費者等利害關係人對於組織個人資料管理能力的信心。

(二) 資訊安全管理系統與個人資訊管理系統國際標準

ISO/IEC 27001 資訊安全管理系統(Information Security Management System)是目前國際上最多企業組織遵循的資訊安全管理系統，企業組織可透過 ISO/IEC 27001 建置符合需求的資訊安全控制措施，以達成一定水準的資安防護能力 [33]。

ISO/IEC 27701 個人資訊管理系統(Privacy Information Management System)是建立在 ISO/IEC 27001 之上，在資訊安全擴充及強化個人資料隱私要求和控制措施的管理系統，並整合 ISO 27001、ISO27002、ISO 29100 等實務做法 [34]。

[32] 臺灣個人資料保護與管理制度(TPIPAS)，https://www.tpipas.org.tw/。

[33] ISO/IEC 27701 隱私資訊管理 個人資訊保護的當責與信任，BSI，https://www.bsigroup.com/zh-TW/iso-27701/(最後瀏覽日：2023/08/26)。

[34] ISO/IEC 27701:2019 Security techniques-Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management-Requirements and guidelines, ISO, https://www.iso.org/standard/71670.html (last visited Aug. 26, 2023).

(三) 英國標準個人資料管理系統

BS 10012 英國標準個人資訊管理系統由英國標準協會基於 OECD、APEC 及英國資料保護法對於個人資訊管理制定而來。BS 10012 與其他國際標準一致，定義個人資訊管理系統的要求。標準的設計確保有充分、適當的控制措施，並有助於保護個人資訊、增強包括客戶、當事人等利害關係人對於組織在個人資訊管理上的信心。標準採用過程方法來建立、施行、運作、監控、審查、維護及改善組織的個人資訊管理系統 (PIMS)，企業 / 組織藉由導入及驗證 BS 10012，可呈現組織個資管理之積極與主動性。

表 4 各項管理系統標準分析比較表

制度	TPIPAS	ISO 27001 & ISO 27701	BS 10012
性質	個人資訊管理系統(PIMS)	資訊安全管理系統(ISMS)	個人資訊管理系統(PIMS)
主導單位	我國數位發展部	國際標準組織	英國標準協會
特色	唯一依照我國個人資料保護法為基礎設計，並可銜接 CBPR 國際要求	首個全球資訊安全管理的國際標準，包括：ISO27001、ISO27002、ISO29100	僅適用英國境內，主要依循 GDPR 設計
所涉法令	我國個人資料保護法	無法律基礎	英國資料保護法、GDPR
資安要求	選擇與個資有高度關連項目要求	以 ISO 27001 為基礎，需納入 27001 的各項控制項	確保機密性、完整性及可用性
應用分析	較利於法遵分析與檢核，易於應對個資行政檢查等主管機關要求	對於資訊安全人員操作較為便利，符合資安系統操作習慣	以國際(歐盟)法遵為主
適合對象	以法遵要求為主的組織	以資安為基礎，兼及個資保護的組織	有較多機會對「在歐盟的個資實體」提供商品或服務之組織

資料來源 | 本研究團隊整理

一、因應個人資料保護與管理之多元化工具

(四) TWCERT/CC

「台灣電腦網路危機處理暨協調中心(TWCERT/CC)」在數位發展部指導下，協處企業資安事件通報、通報產品資安漏洞、惡意檔案檢測服務，並蒐集及共享國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間的資安情資，以及舉辦資安推廣宣導活動等，其提供之資訊對於提升我國網際網路零售業者資安聯防能量及網路安全極有參考價值。

因此，鼓勵電商業者至「台灣電腦網路危機處理暨協調中心(TWCERT/CC)」網站首頁 ，申請加入「台灣 CERT/CSIRT 聯盟」會員，便於接收國內資安事件情資分享，強化資安自我防禦能量。

二、結語

為配合憲法法庭 111 年憲判字第 13 號憲法判決意旨要求建立個資保護之獨立監督機制，並為防範近年詐騙案件頻傳，避免企業將個人資料外洩遭不法集團利用，我國個資法歷經行政院於 112 年 5 月 31 日公布修正條文，除第 48 條非公務機關違反安全維護義務之處罰條文自公布日施行，其餘條文之施行日待行政院訂之。

本次修法增訂第 1 之 1 條，增設個人資料保護委員會擔任本法之獨立專責主管機關，將原屬於各中央目的事業主管機關或地方政府及國家發展委員會等權責事項，均改由個人資料保護委員會管轄。又修正第 48 條規定大幅提高罰則，主管機關對於非公務機關未採行適當之安全措施，或未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，將得逕予處罰並限期改正，處新臺幣 2 萬元以上 200 萬元以下罰鍰，屆期未改善將按次處 15 萬元以上 1500 萬元以下罰鍰；若違反義務屬於情節重大者，逕處新臺幣 15 萬元以上 1500 萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰。

為落實個資保護與管理，實務上我國業者多透過提供必要資源、建立管理制度或訂定 SOP，確保符合相關法令要求。本辦法之規範已包含非公務機關之個人資料保護之規劃，個人資料之管理程序及措施，個人資料之安全稽核、紀錄保存及持續改善機制等，對於企業或組織落實個資法可提供具體之參考，本指引也已參採相關法令規範之菁華，可協助電商業者對於個資保護與管理有初步的理解及操作能力。

[35] 台灣電腦網路危機處理暨協調中心(TWCERT/CC)，https://www.twcert.org.tw/tw/mp-1.html (最後瀏覽日：2023/08/26)。

伍 附錄

一、 個人資料保護法

名　　稱：個人資料保護法
修正日期：民國 112 年 5 月 31 日
沿　　革：

1. 中華民國八十四年八月十一日總統(84)華總(一)義字第 5960 號令制定公布全文 45 條。
2. 中華民國九十九年五月二十六日總統華總一義字第 09900125121 號令修正公布名稱及全文 56 條；施行日期，由行政院定之，但現行條文第 19 ～ 22、43 條之刪除，自公布日施行(原名稱：電腦處理個人資料保護法)。
   中華民國一百零一年九月二十一日行政院院臺法字第 1010056845 號令發布除第 6、54 條條文外，其餘條文定自一百零一年十月一日施行。
3. 中華民國一百零四年十二月三十日總統華總一義字第 10400152861 號令修正公布第 6 ～ 8、11、15、16、19、20、41、45、53、54 條條文；施行日期，由行政院定之。
   中華民國一百零五年二月二十五日行政院院臺法字第 105015428 號令發布定自一百零五年三月十五日施行。
   中華民國一百零八年一月十日法務部法律字第 10803500010 號、國家發展委員會發法字第 1080080004A 號會銜公告第 53 條、第 55 條所列屬「法務部」之權責事項，改由「國家發展委員會」管轄。
4. 中華民國一百十二年五月三十一日總統華總一經字第 1200045441 號令修正公布第 48、56 條條文；並增訂第 1-1 條條文；第 1-1 條條文施行日期，由行政院定之。

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。
依法律規定得免告知。
一、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。
二、告知將妨害公務機關執行法定職務。
三、告知將妨害公共利益。
四、當事人明知應告知之內容。
五、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。

二、 個人資料保護法施行細則

名　　稱：個人資料保護法施行細則
修正日期：民國 105 年 3 月 2 日
沿　　革：

1. 中華民國八十五年五月一日法務部(85)法令字第 10259 號令訂定發布全文 46 條。
2. 中華民國一百零一年九月二十六日法務部法令字第 10103107360 號令修正發布名稱及全文 33 條；並自一百零一年十月一日施行(原名稱：電腦處理個人資料保護法施行細則)。
3. 中華民國一百零五年三月二日法務部法令字第 10503502120 號令修正發布第 9 ～ 15、17、18 條條文；並自一百零五年三月十五日施行。

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　本法第六條第一項第一款、第八條第二項第一款、第十六條第一項第一款、第十九條第一項第一款、第二十條第一項第一款所稱法律，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。

三、 個人資料保護法之特定目的及個人資料之類別

個人資料保護法之特定目的

代號	特定目的項目
○○一	人身保險
○○二	人事管理 (包含甄選、離職及所屬員工基本資訊、現職、學經歷、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、差勤、福利措施、褫奪公權、特殊查核或其他人事措施)
○○三	入出國及移民
○○四	土地行政
○○五	工程技術服務業之管理
○○六	工業行政
○○七	不動產服務
○○八	中小企業及其他產業之輔導
○○九	中央銀行監理業務
○一○	公立與私立慈善機構管理
○一一	公共造產業務
○一二	公共衛生或傳染病防治
○一三	公共關係
○一四	公職人員財產申報、利益衝突迴避及政治獻金業務
○一五	戶政
○一六	文化行政
○一七	文化資產管理
○一八	水利、農田水利行政
○一九	火災預防與控制、消防行政
○二○	代理與仲介業務
○二一	外交及領事事務
○二二	外匯業務
○二三	民政
○二四	民意調查
○二五	犯罪預防、刑事偵查、執行、矯正、保護處分、犯罪被害人保護或更生保護事務
○二六	生態保育
○二七	立法或立法諮詢
○二八	交通及公共建設行政
○二九	公民營 (辦) 交通運輸、公共運輸及公共建設
○三○	仲裁

代號	特定目的項目
○三一	全民健康保險、勞工保險、農民保險、國民年金保險或其他社會保險
○三二	刑案資料管理
○三三	多層次傳銷經營
○三四	多層次傳銷監管
○三五	存款保險
○三六	存款與匯款
○三七	有價證券與有價證券持有人登記
○三八	行政執行
○三九	行政裁罰、行政調查
○四○	行銷 (包含金控共同行銷業務)
○四一	住宅行政
○四二	兵役、替代役行政
○四三	志工管理
○四四	投資管理
○四五	災害防救行政
○四六	供水與排水服務
○四七	兩岸暨港澳事務
○四八	券幣行政
○四九	宗教、非營利組織業務
○五○	放射性物料管理
○五一	林業、農業、動植物防疫檢疫、農村再生及土石流防災管理
○五二	法人或團體對股東、會員 (含股東、會員指派之代表)、董事、監察人、理事、監事或其他成員名冊之內部管理
○五三	法制行政
○五四	法律服務
○五五	法院執行業務
○五六	法院審判業務
○五七	社會行政
○五八	社會服務或社會工作
○五九	金融服務業依法令規定及金融監理需要，所為之蒐集處理及利用
○六○	金融爭議處理
○六一	金融監督、管理與檢查
○六二	青年發展行政
○六三	非公務機關依法定義務所進行個人資料之蒐集處理及利用
○六四	保健醫療服務
○六五	保險經紀、代理、公證業務
○六六	保險監理
○六七	信用卡、現金卡、轉帳卡或電子票證業務
○六八	信託業務
○六九	契約、類似契約或其他法律關係事務
○七○	客家行政
○七一	建築管理、都市更新、國民住宅事務
○七二	政令宣導
○七三	政府資訊公開、檔案管理及應用
○七四	政府福利金或救濟金給付行政
○七五	科技行政

代號	特定目的項目
○七六	科學工業園區、農業科技園區、文化創業園區、生物科技園區或其他園區管理行政
○七七	訂位、住宿登記與購票業務
○七八	計畫、管制考核與其他研考管理
○七九	飛航事故調查
○八○	食品、藥政管理
○八一	個人資料之合法交易業務
○八二	借款戶與存款戶存借作業綜合管理
○八三	原住民行政
○八四	捐供血服務
○八五	旅外國人急難救助
○八六	核子事故應變
○八七	核能安全管理
○八八	核貸與授信業務
○八九	海洋行政
○九○	消費者、客戶管理與服務
○九一	消費者保護
○九二	畜牧行政
○九三	財產保險
○九四	財產管理
○九五	財稅行政
○九六	退除役官兵輔導管理及其眷屬服務照顧
○九七	退撫基金或退休金管理
○九八	商業與技術資訊

代號	特定目的項目
○九九	國內外交流業務
一○○	國家安全行政、安全查核、反情報調查
一○一	國家經濟發展業務
一○二	國家賠償行政
一○三	專門職業及技術人員之管理、懲戒與救濟
一○四	帳務管理及債權交易業務
一○五	彩券業務
一○六	授信業務
一○七	採購與供應管理
一○八	救護車服務
一○九	教育或訓練行政
一一○	產學合作
一一一	票券業務
一一二	票據交換業務
一一三	陳情、請願、檢舉案件處理
一一四	勞工行政
一一五	博物館、美術館、紀念館或其他公、私營造物業務
一一六	場所進出安全管理
一一七	就業安置、規劃與管理
一一八	智慧財產權、光碟管理及其他相關行政
一一九	發照與登記
一二○	稅務行政
一二一	華僑資料管理

代號	特定目的項目
一二二	訴願及行政救濟
一二三	貿易推廣及管理
一二四	鄉鎮市調解
一二五	傳播行政與管理
一二六	債權整貼現及收買業務
一二七	募款 (包含公益勸募)
一二八	廉政行政
一二九	會計與相關服務
一三〇	會議管理
一三一	經營郵政業務郵政儲匯保險業務
一三二	經營傳播業務
一三三	經營電信業務與電信加值網路業務
一三四	試務、銓敘、保訓行政
一三五	資 (通) 訊服務
一三六	資 (通) 訊與資料庫管理
一三七	資通安全與管理
一三八	農產品交易
一三九	農產品推廣資訊
一四〇	農糧行政
一四一	遊說業務行政
一四二	運動、競技活動
一四三	運動休閒業務
一四四	電信及傳播監理
一四五	僱用與服務管理

代號	特定目的項目
一四六	圖書館、出版品管理
一四七	漁業行政
一四八	網路購物及其他電子商務服務
一四九	蒙藏行政
一五〇	輔助性與後勤支援管理
一五一	審計、監察調查及其他監察業務
一五二	廣告或商業行為管理
一五三	影視、音樂與媒體管理
一五四	徵信
一五五	標準、檢驗、度量衡行政
一五六	衛生行政
一五七	調查、統計與研究分析
一五八	學生(員)(含畢、結業生) 資料管理
一五九	學術研究
一六〇	憑證業務管理
一六一	輻射防護
一六二	選民服務管理
一六三	選舉、罷免及公民投票行政
一六四	營建業之行政管理
一六五	環境保護
一六六	證券、期貨、證券投資信託及顧問相關業務
一六七	警政
一六八	護照、簽證及文件證明處理

代號	特定目的項目
一六九	體育行政
一七〇	觀光行政、觀光旅館業、旅館業、旅行業、觀光遊樂業及民宿經營管理業務
一七一	其他中央政府機關暨所屬機關構內部單位管理、公共事務監督、行政協助及相關業務
一七二	其他公共部門 (包括行政法人、政府捐助財團法人及其他公法人) 執行相關業務
一七三	其他公務機關對目的事業之監督管理
一七四	其他司法行政

代號	特定目的項目
一七五	其他地方政府機關暨所屬機關構內部單位管理、公共事務監督、行政協助及相關業務
一七六	其他自然人基於正當性目的所進行個人資料之蒐集處理及利用
一七七	其他金融管理業務
一七八	其他財政收入
一七九	其他財政服務
一八〇	其他經營公共事業 (例如 : 自來水、瓦斯等) 業務
一八一	其他經營合於營業登記項目或組織章程所定之業務
一八二	其他諮詢與顧問服務

個人資料保護法之個人資料之類別

代號	識別類	例如
C〇〇一	辨識個人者	姓名、職稱、住址、工作地址、以前地址、住家電話號碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊及戶籍地址、相片、指紋、電子郵遞地址、電子簽章、憑證卡序號、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及其他任何可辨識資料本人者等。
C〇〇二	辨識財務者	金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號碼、保險單號碼、個人之其他號碼或帳戶等。
C〇〇三	政府資料中之辨識者	身分證統一編號、統一證號、稅籍編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等。

代號	特徵類	例如
C〇一一	個人描述	年齡、性別、出生年月日、出生地、國籍、聲音等。
C〇一二	身體描述	身高、體重、血型等。
C〇一三	習慣	抽煙、喝酒等。
C〇一四	個性	個性等之評述意見

代號	家庭情形	例如
C〇二一	家庭情形	結婚有無、配偶或同居人之姓名、前配偶或同居人之姓名、結婚之日期、子女之人數等。
C〇二二	婚姻之歷史	前次婚姻或同居、離婚或分居等細節及相關人之姓名等。
C〇二三	家庭其他成員之細節	子女、受扶養人、家庭其他成員或親屬、父母、同居人及旅居國外及大陸人民親屬等。
C〇二四	其他社會關係	朋友、同事及其他除家庭以外之關係等。

代號	社會情況	例如
C〇三一	住家及設施	住所地址、設備之種類、所有或承租、住用之期間、租金或稅率及其他花費在房屋上之支出、房屋之種類、價值及所有人之姓名等。
C〇三二	財產	所有或具有其他權利之動產或不動產等。
C〇三三	移民情形	護照、工作許可文件、居留證明文件、住居或旅行限制、入境之條件及其他相關細節等。
C〇三四	旅行及其他遷徙細節	過去之遷徙、旅行細節、外國護照、居留證明文件及工作證照及工作證等相關細節等。
C〇三五	休閒活動及興趣	嗜好、運動及其他興趣等。
C〇三六	生活格調	使用消費品之種類及服務之細節、個人或家庭之消費模式等。
C〇三七	慈善機構或其他團體之會員資格	俱樂部或其他志願團體或持有參與者紀錄之單位等。
C〇三八	職業	學校校長、民意代表或其他各種職業等。
C〇三九	執照或其他許可	駕駛執照、行車執照、自衛槍枝使用執照、釣魚執照等。
C〇四〇	意外或其他事故及有關情形	意外事件之主體、損害或傷害之性質、當事人及證人等。
C〇四一	法院、檢察署或其他審判機關或其他程序	關於資料主體之訴訟及民事或刑事等相關資料等。

代號	教育、考選、技術或其他專業	例如
C〇五一	學校紀錄	大學、專科或其他學校等。
C〇五二	資格或技術	學歷資格、專業技術、特別執照 (如飛機駕駛執照等)、政府職訓機構學習過程、國家考試、考試成績或其他訓練紀錄等。
C〇五三	職業團體會員資格	會員資格類別、會員資格紀錄、參加之紀錄等。
C〇五四	職業專長	專家、學者、顧問等。
C〇五五	委員會之會員資格	委員會之詳細情形、工作小組及會員資格因專業技術而產生之情形等。
C〇五六	著作	書籍、文章、報告、視聽出版品及其他著作等。
C〇五七	學生 (員)、應考人紀錄	學習過程、相關資格、考試訓練考核及成績、評分評語或其他學習或考試紀錄等。
C〇五八	委員工作紀錄	委員參加命題、閱卷、審查、口試及其他試務工作情形紀錄。

代號	受僱情形	例如
C〇六一	現行之受僱情形	僱主、工作職稱、工作描述、等級、受僱日期、工時、工作地點、產業特性、受僱之條件及期間、與現行僱主有關之以前責任與經驗等。
C〇六二	僱用經過	日期、受僱方式、介紹、僱用期間等。
C〇六三	離職經過	離職之日期、離職之原因、離職之通知及條件等。
C〇六四	工作經驗	以前之僱主、以前之工作、失業之期間及軍中服役情形等。
C〇六五	工作、差勤紀錄	上、下班時間及事假、病假、休假、娩假各項請假紀錄在職紀錄或未上班之理由、考績紀錄、獎懲紀錄、褫奪公權資料等。
C〇六六	健康與安全紀錄	職業疾病、安全、意外紀錄、急救資格、旅外急難救助資訊等。
C〇六七	工會及員工之會員資格	會員資格之詳情、在工會之職務等。
C〇六八	薪資與預扣款	薪水、工資、佣金、紅利、費用、零用金、福利、借款、繳稅情形、年金之扣繳、工會之會費、工作之基本工資或工資付款之方式、加薪之日期等。
C〇六九	受僱人所持有之財產	交付予受僱人之汽車、工具、書籍或其他設備等。
C〇七〇	工作管理之細節	現行義務與責任、工作計畫、成本、用人費率、工作分配與期間、工作或特定工作所花費之時間等。

代號	受僱情形	例如
C〇七一	工作之評估細節	工作表現與潛力之評估等。
C〇七二	受訓紀錄	工作必須之訓練與已接受之訓練，已具有之資格或技術等。
C〇七三	安全細節	密碼、安全號碼與授權等級等。

代號	財務細節	例如
C〇八一	收入、所得、資產與投資	收入、總所得、賺得之收入、賺得之所得、資產、儲蓄、開始日期與到期日、投資收入、投資所得、資產費用等。
C〇八二	負債與支出	支出總額、租金支出、貸款支出、本票等信用工具支出等。
C〇八三	信用評等	信用等級、財務狀況與等級、收入狀況與等級等。
C〇八四	貸款	貸款類別、貸款契約金額、貸款餘額、初貸日、到期日、應付利息、付款紀錄、擔保之細節等
C〇八五	外匯交易紀錄	
C〇八六	票據信用	票存款、基本資料、退票資料、拒絕往來資料等。
C〇八七	津貼、福利、贈款	
C〇八八	保險細節	保險種類、保險範圍、保險金額、保險期間、到期日、保險費、保險給付等。
C〇八九	社會保險給付、就養給付及其他退休給付	生效日期、付出與收入之金額、受益人等。
C〇九一	資料主體所取得之財貨或服務	貨物或服務之有關細節、資料主體之貸款或僱用等有關細節等。
C〇九二	資料主體提供之財貨或服務	貨物或服務之有關細節等。
C〇九三	財務交易	收付金額、信用額度、保證人、支付方式、往來紀錄、保證金或其他擔保等。
C〇九四	賠償	受請求賠償之細節、數額等。

代號	商業資訊	例如
C一〇一	資料主體之商業活動	商業種類、提供或使用之財貨或服務、商業契約等。
C一〇二	約定或契約	關於交易、商業、法律或其他契約、代理等。
C一〇三	與營業有關之執照	執照之有無、市場交易者之執照、貨車駕駛之執照等。

代號	健康與其他	例如
C一一一	健康紀錄	醫療報告、治療與診斷紀錄、檢驗結果、身心障礙種類、等級、有效期間、身心障礙手冊證號及聯絡人等。
C一一二	性生活	
C一一三	種族或血統來源	去氧核糖核酸資料等。
C一一四	交通違規之確定裁判及行政處分	裁判及行政處分之內容、其他與肇事有關之事項等。
C一一五	其他裁判及行政處分	裁判及行政處分之內容、其他相關事項等。
C一一六	犯罪嫌疑資料	作案之情節、通緝資料、與已知之犯罪者交往、化名、足資證明之證據等。
C一一七	政治意見	政治上見解、選舉政見等。
C一一八	政治團體之成員	政黨黨員或擔任之工作等。
C一一九	對利益團體之支持	係利益團體或其他組織之會員、支持者等。
C一二〇	宗教信仰	
C一二一	其他信仰	

代號	其他各類資訊	例如
C一三一	書面文件之檢索	未經自動化機器處理之書面文件之索引或代號等。
C一三二	未分類之資料	無法歸類之信件、檔案、報告或電子郵件等。
C一三三	輻射劑量資料	人員或建築之輻射劑量資料等。
C一三四	國家情報工作資料	國家情報工作法、國家情報人員安全查核辦法等有關資料。

四、 數位經濟相關產業個人資料檔案安全維護管理辦法

名　　稱：數位經濟相關產業個人資料檔案安全維護管理辦法
修正日期：民國 112 年 10 月 12 日
沿　　革：
中華民國一百十二年十月十二日數位發展部數授產服字第 1126000621 號令訂定發布全文 20 條；並自發布日施行並增訂

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　本辦法所稱數位經濟相關產業(以下簡稱業者)，指從事附表一所列行業之自然人、私法人或其他團體。

第 3 條　業者應於本辦法施行之日起三個月內完成個人資料檔案安全維護計畫及業務終止後個人資料處理方法(以下簡稱安全維護計畫)之規劃及訂定。
安全維護計畫應納入符合第五條至第十七條規定之具體內容。
業者應依其所訂定之安全維護計畫執行之。數位發展部(以下簡稱本部)得要求業者提出安全維護計畫之實施情形，業者應於指定期限內，以書面方式提出。

第 4 條　業者應對內公開周知個資保護政策，使所屬人員明確瞭解及遵循，其內容應包括下列事項之說明：
一、遵守我國個人資料保護相關法令規定。
二、以合理安全之方式，於特定目的範圍內，蒐集、處理及利用個人資料。
三、以可期待之合理安全水準技術保護其所蒐集、處理、利用之個人資料檔案。
四、設置聯絡窗口，供個人資料當事人行使其個人資料相關權利或提出相關申訴與諮詢。
五、規劃緊急應變程序，以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。
六、如委託蒐集、處理及利用個人資料者，應妥善監督受託人。
七、持續維運安全維護計畫之義務，以確保個人資料檔案之安全。

第 5 條　業者應依其業務規模及特性，衡酌經營資源之合理分配，配置管理人員及相當資源，負責下列事項：
一、個人資料保護管理政策之訂定及修正。
二、安全維護計畫之訂定、修正及執行。
個人資料保護管理政策、安全維護計畫之訂定或修正，應經業者之代表人或其授權人員核定。

第 6 條　業者應定期清查確認所蒐集、處理或利用之個人資料現況，界定納入安全維護計畫之範圍。

第 7 條　業者應依已界定之個人資料範圍及其業務涉及個人資料蒐集、處理或利用之流程，定期評估可能產生之風險，並根據風險評估結果，採行適當之安全措施。

第 8 條　業者為因應當事人個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故，應訂定下列應變、通報及預防機制：

一、事故發生後應採取之應變措施，包括降低、控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。

二、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，通知當事人事故之發生與處理情形，及後續供當事人查詢之電話專線或其他適當管道。

三、事故發生後研議其矯正預防措施之機制。

業者遇有個人資料安全事故，將危及其正常營運或大量當事人權益者，應於知悉事故後七十二小時內依附表二格式通報本部，或通報直轄市、縣(市)政府時副知本部。

無法於時限內通報或無法於當次提供前項所述事項之全部資訊者，應檢附延遲理由或分階段提供。

本部或直轄市、縣(市)政府接獲第二項通報後，得依本法第二十二條至第二十五條規定為適當之處理。

第 9 條　業者應訂定下列事項之內部管理程序：

一、蒐集、處理或利用有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料者，檢視是否符合本法第六條第一項但書所定情形。

二、檢視個人資料蒐集或處理，是否符合本法第十九條第一項所定法定情形及特定目的；經當事人同意而為蒐集或處理者，並應確保符合本法第七條第一項規定。

三、檢視個人資料之利用，是否符合蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否符合本法第二十條第一項但書所定情形；經當事人同意而為特定目的外之利用者，並應確保符合本法第七條第二項規定。

四、檢視個人資料之蒐集是否符合本法第八條第二項或第九條第二項得免為告知之事由；無得免為告知之事由者，並應確保符合本法第八條第一項或第九條第一項規定。

五、利用個人資料行銷而當事人表示拒絕接受行銷者，確保符合本法第二十條第二項及第三項規定。

六、當事人行使本法第三條所定權利之相關事項：

(一) 提供當事人行使權利之方式。

(二) 確認當事人或其代理人之身分。

(三) 檢視是否符合本法第十條但書、第十一條第二項但書及第十一條第三項但書所定得拒絕其請求之事由。

(四) 依前目規定拒絕當事人行使權利者，應附理由通知當事人。

(五) 就當事人請求為准駁決定及延長決定期間之程序，並應確保符合本法第十三條規定。

(六) 當事人請求更正或補充其個人資料者，其應釋明之事項。

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

七、維護個人資料正確性之機制；個人資料正確性有爭議者，並應確保符合本法第十一條第一項、第二項及第五項規定。

八、定期檢視個人資料蒐集之特定目的是否已消失或期限是否已屆滿；其特定目的消失或期限屆滿者，並應確保符合本法第十一條第三項規定。

第 10 條 業者將個人資料作國際傳輸者，應檢視是否受本部依本法第二十一條所為之限制，並且告知當事人其個人資料所欲國際傳輸之區域，同時對資料接收方為下列事項之監督：

一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。

二、當事人行使本法第三條所定權利之相關事項。

第 11 條 業者應採取下列資料安全管理措施：

一、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。

二、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。

三、傳輸個人資料時，應依不同傳輸方式，採取適當之安全措施。

業者以資通系統直接或間接蒐集、處理或利用個人資料時，除前項要求外，應採取下列資料安全管理措施：

一、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。

二、資通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。

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、資通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。

六、處理個人資料之資通系統進行測試時，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。

七、處理個人資料之資通系統有變更時，應確保其安全性未降低。

八、定期檢視處理個人資料之資通系統，檢查其使用狀況及存取個人資料之情形。

九、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。

十、其他本部公告之資料安全管理措施。

第 12 條 業者應採取下列人員管理措施：

一、與所屬人員約定保密義務。

二、識別業務內容涉及個人資料蒐集、處理或利用之人員。

三、依其業務特性、內容及需求，設定所屬人員接觸個人資料之權限，並定期檢視其適當性及必要性。

四、人員離職時，要求人員返還個人資料之載體，並刪除因執行業務而持有之個人資料。

第 13 條 業者應定期對所屬人員，實施下列個人資料保護認知宣導及教育訓練：

一、個人資料保護相關法令之規定。

二、所屬人員之責任範圍。

三、安全維護計畫各項管理程序、機制及措施之要求。

業者對代表人、負責人或第五條所稱管理人員，另應依其於安全維護計畫所擔負之任務及角色，定期實施必要之教育訓練。

從事以網際網路方式供他人零售商品之平台業者，其安全維護計畫，應加入下列事項：

一、對其平台使用者，進行適當之個人資料保護及管理之認知宣導或教育訓練。

二、訂定個人資料保護守則，要求平台使用者遵守。

第 14 條　業者應對存有個人資料之儲存媒介物，採取下列設備安全管理措施：

一、依儲存媒介物之特性及使用方式，建置適當之保護設備或技術。

二、針對所屬人員保管個人資料之儲存媒介物，訂定適當之管理規範。

三、針對存放儲存媒介物之環境，施以適當之進出管制措施。

第 15 條　業者應訂定個人資料安全稽核機制，定期檢查安全維護計畫執行狀況，並作成評估報告；如有缺失，應予改善。

第 16 條　業者執行安全維護計畫時，應評估其必要性，保存下列紀錄至少五年：

一、個人資料之蒐集、處理或利用紀錄。

二、自動化機器設備之軌跡資料。

三、落實執行安全維護計畫之證據。

業者於業務終止後，其所蒐集、處理或利用之個人資料應依下列方式處理，並留存下列紀錄至少五年：

一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

二、移轉：移轉之原因、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。

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

第 17 條　業者應訂定下列整體持續改善機制：

一、安全維護計畫未落實執行時應採取矯正預防措施。

二、參酌安全維護計畫執行狀況、技術發展、業務調整及法令變化等因素，定期檢視或修正。

第 18 條　業者之資本額為新臺幣一千萬元以上或保有個人資料筆數達五千筆以上者，於安全維護計畫訂定後，第六條、第七條、第九條第八款、第十一條第二項第一款至第四款、第八款、第十二條第三款、第十三條第一項、第二項、第十五條及前條第二款之措施，應每十二個月至少實施及檢討改善一次。

業者之資本額於本辦法施行後始增資達新臺幣一千萬元以上，或因直接或間接蒐集而保有個人資料達五千筆以上者，應自符合條件之日起六個月後，每十二個月至少實施及檢討改善前項措施一次。

前二項所定資本額，於股份有限公司為實收資本額，於有限公司、無限公司及兩合公司為登記之資本總額，於獨資或合夥方式經營之事業，為登記之資本額。

因刪除、銷毀或其他方法致保有個人資料筆數減少，且連續二年期間保有個人資料筆數未達五千筆之業者，得不適用第一項規定。但嗣後因直接或間接蒐集而致保有個人資料筆數達五千筆以上者，應於保有筆數達五千筆以上之日起三十日內，恢復適用第一項規定。保有個人資料筆數之計算，以業者單日所保有之個人資料為認定基準。

第 19 條　業者受委託蒐集、處理或利用個人資料者，應遵循委託者之中央目的事業主管機關所定之個人資料相關法規。

業者委託他人蒐集、處理或利用個人資料者，應對受託者依本法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。

第 20 條　本辦法自發布日施行。

附表一

行政院主計總處行業統計分類 分類編號及行業名稱	適用本辦法之行業
4871 電子購物及郵購業	從事以網際網路方式零售商品之行業 (不含電視、廣播、電話等其他電子媒介及郵購方式)
582 軟體出版業	軟體出版業
620 電腦程式設計、諮詢及相關服務業	電腦程式設計、諮詢及相關服務業
6312 資料處理、主機及網站代管服務業	從事代客處理資料、主機及網站代管以及相關服務之行業 (不含線上影音串流服務)
639 其他資訊服務業	其他資訊服務業
6699 未分類其他金融輔助業	第三方支付服務業 (不含其他金融輔助業)

附表二 業者個人資料外洩通報表

個人資料侵害事故通報與紀錄表

<table>
<tr><td rowspan="3">業者名稱</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 rowspan="3">通報機關</td><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>事件發生種類</td><td>□竊取
□竄改
□滅失</td><td>□洩漏
□毀損
□其他侵害事故</td><td>個資侵害之總筆數 (大約)_____筆
□一般個資_____筆
□特種個資_____筆</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>個資外洩可能結果</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>是否於發生個資外洩後 72 小時通報</td><td colspan="3">□是　　□否，理由：</td></tr>
</table>

MEMO

MEMO

財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY