法規名稱：零售業個人資料檔案安全維護管理辦法
修正日期：民國 113 年 11 月 13 日

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

1 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。

2 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

1 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。

2 業者於傳輸個人資料時，應採取避免洩漏之必要保護措施。

3 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

1 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。

2 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

1 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。

2 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。

3 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。

4 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

1 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。

2 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。

3 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

1 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。

2 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

1 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。

2 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

1 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。

2 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

1 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。

2 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

1 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。

2 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。