法規名稱：(廢)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

廢止日期：民國 112 年 11 月 21 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

1 本辦法所稱網際網路零售業，指以網際網路方式零售商品，且登記資本額為新臺幣一千萬元以上之股份有限公司，或受經濟部（以下簡稱本部）指定之公司或商號。但不包括應經特許、許可或受專門管理法令規範之行業。

2 本辦法所稱網際網路零售服務平台業，指經營供他人零售商品之網際網路平台，且登記資本額為新臺幣一千萬元以上之股份有限公司，或受本部指定之公司或商號。但不包括應經特許、許可或受專門管理法令規範之行業。

第 3 條

1 網際網路零售業為符合本法、本辦法及其他相關法令之規定，應依其業務規模及特性，衡酌經營資源之合理分配，設個人資料管理單位或適當組織，並配置適當資源，負責下列事項：

一、個人資料保護管理政策（以下簡稱個資保護政策）之訂定及修正。

二、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）之訂定、修正及執行。

2 個資保護政策及安全維護計畫之訂定或修正，應由網際網路零售業之代表人或其授權之其他負責人核定之。

第 4 條

網際網路零售業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

1 第三條之安全維護計畫應納入符合第六條至第十九條規定之具體內容。

2 網際網路零售業應隨時檢視其所適用之個人資料保護法令及該法令之變動，並適時檢討修正安全維護計畫；如有業務或環境之變動，亦同。

3 本部於必要時，得要求網際網路零售業提出安全維護計畫及其相關文件，並得依本法第二十二條至第二十五條規定所賦予之職權，為適當之監督管理措施。

第 6 條

網際網路零售業應適時並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。

第 7 條

網際網路零售業應適時並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。

第 8 條

1 前條因應措施，應包括個人資料被竊取、竄改、毀損、滅失或洩漏等事故之應變機制，其內容應對下列事項為具體規定：

一、降低、控制事故對當事人造成損害之作法。

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專線與其他查詢管道。

三、避免類似事故再次發生之矯正及預防機制。

四、發生重大事故時，應自發現事故時起算七十二小時內，依附表格式，以電子郵件方式通報總機構所在地直轄市或縣（市）主管機關及副知本部，並應視案情發展適時通報處理情形，以及將整體查處過程、結果與檢討等函報總機構所在地直轄市或縣（市）主管機關並副知本部。

2 前項第四款所稱重大事故，指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及網際網路零售業正常營運或大量當事人權益之情形。

第 9 條

1 除法律另有規定外，網際網路零售業應就下列事項訂定具體程序或機制，並提出有效方式維持其運作：

一、檢視個人資料之蒐集、處理，符合本法第十九條第一項所定之法定情形及特定目的，或有其他合法事由。

二、檢視個人資料之利用，符合蒐集時之特定目的，或符合本法所定得為特定目的外利用之情形，或有其他合法事由；依當事人書面同意而為特定目的外利用者，應確認已符合本法第七條第二項有關書面同意之規定。

三、檢視已依便利當事人之適當方式，踐行本法第八條及第九條所定之告知義務；如有免為告知之情形，應確認其合法依據。

四、檢視已於首次行銷時提供當事人表示拒絕行銷之管道，並由網際網路零售業支付所需費用。

五、檢視當事人已拒絕接受行銷時，即停止利用其個人資料為行銷，並周知所屬人員或採行防範所屬人員再次行銷之措施。

六、檢視個人資料之蒐集、處理、利用與本法第五條之規定相符。

七、對個人資料進行國際傳輸前，應針對該次傳輸進行可能之影響及風險分析，並採取適當安全保護措施。

八、於特定目的消失、期限屆滿、有本法第十九條第二項所定情形，或有違反本法規定而為個人資料之蒐集、處理或利用時，應依法刪除或停止蒐集、處理、利用個人資料。

九、如於特定目的消失或期限屆滿，而未刪除、停止處理或利用個人資料時，須因執行業務所必須或經當事人書面同意。

十、檢視個人資料是否正確，有不正確或正確性有爭議者，應分別情形依本法第十一條第一項、第二項及第五項之規定辦理。

十一、關於本法第三條所列當事人權利之行使事宜：

（一）提供行使權利之方式應考量個人資料安全管理之必要性及當事人之便利性。

（二）應依適當之方式確認，或請求當事人或代為行使權利之人說明，其確為當事人本人或有權代為行使權利之人。

（三）於提供查詢或製給複製本時，得收取成本費用，但應先明確告知。

（四）應遵守本法第十三條有關處理期限之規定。

（五）於得合法拒絕權利行使或得延長處理期限之情形，應將拒絕之理由或延長之原因，以書面通知當事人。

十二、委託他人蒐集、處理或利用個人資料之全部或一部時，應有選任受託人之標準及評估機制，且應於委託契約或相關文件明確約定適當之監督方式，並確實執行。

十三、受他人委託處理個人資料之全部或一部時，如認委託機關之指示有違反本法或其他個人資料保護相關法令者，應立即通知委託機關。

2 網際網路零售業將當事人個人資料作國際傳輸者，應檢視是否受本部限制，並且告知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 10 條

網際網路零售業如有保護消費者個人資料之機制，應適時提醒消費者應用，並為適當之公告。

第 11 條

網際網路零售業應考量業務性質、個人資料存取環境、個人資料傳輸之工具與方法及個人資料之種類、數量等因素，採取適當之人員、作業、設備及技術之安全管理措施。

第 12 條

前條之人員安全管理措施，應包括下列事項：

一、確認蒐集、處理及利用個人資料之相關業務流程之負責人員。

二、依據執行業務之必要，設定所屬人員關於個人資料蒐集、處理或利用，及接觸個人資料儲存媒體之相關權限，定期檢視權限設定內容之必要性，並控管接觸個人資料之情形。

三、與所屬人員約定保密義務。

第 13 條

第十一條之作業安全管理措施，應包括下列事項：

一、訂定個人資料儲存媒體使用規範並確實執行之。

二、個人資料儲存媒體於廢棄或轉作其他用途前，應以適當方式銷毀或確實刪除該媒體中所儲存之個人資料。委託他人執行上開行為時，準用第九條第十二款之規定，應為適當之監督。

三、蒐集、處理或利用個人資料時，如有加密或遮蔽之必要，應採取適當之加密或遮蔽機制。

四、傳輸個人資料時，應有適當安全之防護機制。

五、依據所保有個人資料之重要性，採取適當之備份機制，並比照原件保護之。

第 14 條

第十一條之設備安全管理措施，應包括下列事項。

一、依據作業內容及環境之不同，實施必要之安全環境管制。

二、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。

三、針對不同作業環境，建置必要之保護設備或技術。

第 15 條

第十一條之技術安全管理措施，應包括下列事項：

一、採取適當之安全機制，避免用以蒐集、處理或利用個人資料之電腦、相關設備或系統遭受無權限之存取，包括但不限就個人資料之存取權限，設定必要之控管機制，並定期確認控管機制之有效性。

二、定期確認蒐集、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，包括但不限採取適當之安全機制，因應惡意程式及系統漏洞所造成之威脅。

三、進行軟硬體測試時，應避免使用實際個人資料。如確有使用實際個人資料之必要時，應明確規定其使用之程序及安全管理方式。

四、定期檢查使用於蒐集、處理或利用個人資料之電腦、相關設備或系統之使用狀況及個人資料存取之情形。

第 16 條

網際網路零售業應每年定期實施所屬人員之個人資料保護與管理認知宣導及教育訓練，使其明瞭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；對代表人、負責人或第三條所稱管理單位或適當組織之人員，另應依其於安全維護計畫所擔負之任務及角

色，每年定期實施必要之教育訓練。

第 17 條

1 網際網路零售業於業務之一部或全部終止時，應刪除、銷毀或停止處理、利用相關之個人資料。如將相關之個人資料移轉第三人，於移轉前，應確認該第三人依法有權蒐集該個人資料。

2 前項之移轉，應採取合法且適當之方式為之。

第 18 條

網際網路零售業應每年定期由第三條所設之個人資料管理單位或適當組織執行安全維護計畫之內部稽核，提出評估報告，並採取下列改善措施：

一、修正個資保護政策及安全維護計畫。

二、評估報告中有不符合法令或有違法之虞者，應規劃並採取相關改善及預防措施。

第 19 條

網際網路零售業執行安全維護計畫，除其他法令另有規定外，應留存下列紀錄或證據：

一、個人資料提供或移轉第三人之紀錄，該紀錄應包括提供或移轉之對象、依據、原因、方法、時間及地點等資訊。

二、確認個人資料正確性及補充、更正之紀錄。

三、當事人行使本法第三條之權利及處理過程之紀錄。

四、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。

五、存取個人資料系統之紀錄。

六、資料備份及確認其有效性之紀錄。

七、人員權限新增、變動及刪除之紀錄。

八、因應事故發生所採取行為之紀錄。

九、定期檢查處理個人資料之資訊系統之紀錄。

十、認知宣導及教育訓練之紀錄。

十一、稽核及改善安全維護計畫之紀錄。

十二、其他必要紀錄或證據。

第 20 條

網際網路零售服務平台業，準用第三條至第十九條之規定，其安全維護計畫，並應加入下列事項：

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 21 條

本辦法自發布日施行。