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

條文	說明
第一條　本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。	本辦法訂定之依據。
第二條　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。 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。	一、本辦法所稱網際網路零售業及網際網路零售服務平台業，分別指以網際網路方式零售商品及經營供他人零售商品之網際網路平台之業者，但考量一定規模以上之業者，其擁有之個人資料已占大宗，且考量業者之經營成本，爰本辦法將適用之範圍，限制在一定資本額以上之股份有限公司。 二、為使本部能有效管理，縱非前開一定資本額以上之股份有限公司，如其已發生個人資料外洩等事故，或本部認有加強管理之必要時，亦得指定公司或商號適用本辦法。 三、但如行業須經特許、許可或受專門管理法令規範之行業，因其已有特定之目的事業主管機關，而非本部主管，爰不適用本辦法之規定。
第三條　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。 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	一、參考中央目的事業主管機關依個人資料保護法第二十七條第三項規定訂定辦法之參考事項(以下簡稱訂定辦法之參考事項)第二點第一款之規定，非公務機關為落實個人資料保護之目的，應考量其業務規模及特性，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，負責訂定個資保護政策及安全維護計畫，爰訂定第一項。 二、為確保網際網路零售業能確實遵循個資保護政策及安全維護計畫，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，爰訂定第二項。

定之。	
第四條　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。	參考訂定辦法之參考事項第二點第一款第二目之規定，為使網際網路零售業全體所屬人員對於個人資料之保護能有所體認並落實，網際網路零售業應對內公開周知個資保護政策，爰訂定本條規定。
第五條　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。 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。 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。	一、第一項明定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。 二、參考訂定辦法之參考事項第二點第二款第二目之規定，網際網路零售業因種類、特性之不同，其所蒐集、處理或利用之個人資料範圍亦有不同，導致其所適用之個人資料保護法令也可能有所差異，為符合法令之規定，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，其中所稱個人資料保護法令，並不以本法及本法施行細則為限。又個人資料保護法令，可能因時勢變遷而有變更之可能，網際網路零售業應隨時檢視該

	法令之變動，並適時檢討修正安全維護計畫。另為使安全維護計畫符合實際需求，如有業務或環境之變動，網際網路零售業亦應適時檢討修正安全維護計畫，爰訂定第二項。 三、為利監督，本部得於必要時，要求網際網路零售業提出安全維護計畫及其相關文件，爰訂定第三項。
第六條　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。	參考本法施行細則第十二條第二項第二款及訂定辦法之參考事項第二點第二款第一目之規定，非公務機關訂定安全維護計畫，應先界定個人資料範圍，亦即定期清查保有之個人資料現況；又安全維護計畫之規劃及執行，與個人資料之蒐集、處理或利用之作業流程息息相關，爰明定網際網路零售業應建立個人資料檔案清冊及個人資料作業流程說明文件。
第七條　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。	參考本法施行細則第十二條第二項第三款及訂定辦法之參考事項第二點第三款之規定，非公務機關訂定安全維護計畫，應先就個人資料進行風險評估，爰明定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相關風險，並訂定適當之管控及因應措施。
第八條　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。	一、參考訂定辦法之參考事項第二點第四款規定訂定之。 二、為因應本法第十二條明定之業者對當事人之通知義務，事故發生時，網際網路零售業應適時以電子郵件、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，爰訂定第一項第二款。 三、如發生影響層面較廣之重大事故，除第一項前三款之規定外，網際網路零售業尚應即時依本部指定之機制進行通報，並依本部指示，公告或持

四、發生重大事故時，即時依本部指定之機制進行通報，並依本部指示，公告或持續通報事故之處理情形與避免類似事故再次發生之矯正及預防機制。 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。	續通報事故之處理情形與避免類似事故再次發生之矯正及預防機制，爰訂定第一項第四款。又關於「重大事故」之定義，參考澳洲立法例及我國金融監督管理委員會發布之金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法第六條第三項之規定，明定於第二項。
第九條　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。	一、參考訂定辦法之參考事項第三點規定訂定之。 二、配合本法施行細則第十二條第二項第五款之規定，網際網路零售業應將其個人資料蒐集、處理及利用之內部管理程序，明定於安全維護計畫中，包括：檢視個人資料之蒐集、處理或利用是否符合法定要件；當事人拒絕行銷之處置；對受託人之監督事項；遵守本部所為國際傳輸之限制；當事人行使權利之處理；個人資料正確性之維護；個人資料之刪除等事項，爰訂定第一項各款及第二項。 三、第一項第二款所稱書面同意，本法施行細則第十四條明定，依電子簽章法之規定，得以電子文件為之。 四、第一項第七款之國際傳輸，因係將當事人之個人資料傳輸至境外，故網際網路零售業應於個人資料傳輸前，特別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。 五、第一項第十款所稱「個人資料是否正確」，應依蒐集之特定目的，並考量對當事人或第三人權益之維護認定之，例如依蒐集之特定目的，當事人亦可不提供姓名而僅提供暱稱，則網際網路零售業以當事人之暱稱稱呼該當事人，不應認定其個人資料不正確；惟如與當事人間存在爭議，仍應依本法第十一條第二項規定處理

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	之。 六、委託他人蒐集、處理或利用個人資料之全部或一部時，依本法施行細則第八條第一項至第三項之規定，應對受託者為適當之監督，故第一項第十二款明定，網際網路零售業委託他人蒐集、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。 七、受他人委託處理個人資料之全部或一部時，依本法施行細則第八條第四項之規定，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，爰訂定第一項第十三款。

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。 本部依本法第二十一條規定就國際傳輸個人資料定有相關限制者，其相關限制應納入前項之程序或機制。	
第十條 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。	網際網路零售業所保有之個人資料，大部分應屬消費者之個人資料，如其有消費者個人資料保護機制，應適時提醒消費者，並為適當之公告，以利消費者使用。
第十一條　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。	一、參考訂定辦法之參考事項第四點規定訂定之。 二、對於個人資料之保護，除於組織面給予整體規劃，及法令遵循程序之設計外，尚應考慮安全管理措施之部分，而如何規劃安全管理措施，則應綜合考量網際網路零售業之業務性質、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；安全管理措施可分為人員管理、作業管理、設備管理及技術管理之不同要求，分別明定於第十二條至第十五條。
第十二條　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	一、參考訂定辦法之參考事項第四點第二款規定訂定之。 二、人員管理首先應確認蒐集、處理及利用個人資料之相關業務流程之負責人員，方可確認管理之範圍，爰訂

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。	定第一款。 三、為免個人資料遭受不必要之接觸，網際網路零售業應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，爰訂定第二款。 四、網際網路零售業應要求所屬人員負相關之保密義務，以防止個人資料遭所屬人員洩漏，爰訂定第三款。
第十三條 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。	一、參考訂定辦法之參考事項第四點第一款規定訂定之。 二、網際網路零售業應訂定個人資料儲存媒體使用規範並確實執行之，以避免個人資料儲存媒體遭不當存取或利用，爰訂定第一款。 三、為免個人資料外洩，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，爰訂定第二款。 四、為免個人資料外洩，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，爰訂定第三款。 五、第四款所稱傳輸個人資料時應有適當安全之防護機制，除加密機制外，包括但不限確保資料收受者正確之確認機制，以避免資料傳輸錯誤。 六、為確保網際網路零售業業務之運作及個人資料當事人之權益，針對重要之個人資料，應採取適當之備份機制，並比照原件保護之，爰訂定第五款。
第十四條 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。	一、參考訂定辦法之參考事項第四點第三款規定訂定之。 二、在設備安全管理方面，網際網路零售業應針對不同之作業內容及作業

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。	環境，實施必要之安全環境管制；妥善維護並控管蒐集、處理或利用個人資料過程中所使用之實體設備；並建置必要之保護設備或技術，以維持設備之基本安全。
第十五條　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。	網際網路零售業若利用電腦或相關設備蒐集、處理或利用個人資料時，針對相關電腦系統技術，亦應有相應之管理措施，本條即臚列相關之技術安全管理措施，並明定網際網路零售業應予採用。
第十六條　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。	參考訂定辦法之參考事項第二點第五款之規定，為使安全維護計畫相關管理程序能落實執行，網際網路零售業之所屬人員，均應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，尤其就代表人、負責人或第三條所稱管理單位或適當組織之人員，更應使其明瞭其於安全維護計畫中所擔負之任務及角色，爰明定網際網路零售業應每年定期實施認知宣導及教育訓練之規定。
第十七條　網際網路零售業於業務之一	一、參考訂定辦法之參考事項第四點第

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。 前項之移轉，應採取合法且適當之方式為之。	四款規定訂定之。 二、網際網路零售業於業務一部或全部終止時，原則上應刪除、銷毀或停止處理、利用相關之個人資料。如將相關個人資料移轉第三人，應先確認該第三人依法有權蒐集該個人資料，爰訂定第一項。 三、第一項之移轉，應採取合法且適當之方式進行，以免移轉過程中資料外洩，爰訂定第二項。
第十八條　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。	一、參考訂定辦法之參考事項第五點第一款、第三款規定訂定之。 二、安全維護計畫之規劃是否妥適，及其執行是否確實，應由依第三條所設之個人資料管理單位或適當組織進行內部稽核，該稽核之結果，應用以檢討修正個資保護政策、安全維護計畫及規劃相關改善措施。另為確保稽核品質，該稽核人員宜由具備管理、法制及資訊安全之人員擔任之。
第十九條　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。	一、參考訂定辦法之參考事項第五點第二款規定訂定之。 二、網際網路零售業為證明已落實安全維護計畫，並釐清個人資料於蒐集、處理或利用過程中的相關權責，應就個人資料使用情況、軌跡資料等留存相關紀錄。爰配合本法施行細則第十二條第二項第十款規定，明定網際網路零售業應於安全維護計畫中，訂定相關紀錄、證據之保存機制並徹底落實。

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。	
第二十條　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。	為確保個人資料保護之成果，除將第三條至第十九條之規定準用於網際網路零售服務平台業之外，尚應促使網際網路零售服務平台使用者一併配合，爰明定網際網路零售服務平台業之安全維護計畫，應加入對平台使用者進行認知宣導或教育訓練等內容，並要求平台使用者遵守其所訂定之個人資料保護守則。又本條所稱平台使用者，並不以第二條第一項所稱網際網路零售業為限，尚包含登記資本額及組織型態不符第二條第一項規定之業者乃至消費者等，併予說明。
第二十一條　本辦法自發布日施行。	本辦法之施行日期。