數位發展部令　中華民國112年10月12日
數授產服字第1126000621號

訂定「數位經濟相關產業個人資料檔案安全維護管理辦法」。

附「數位經濟相關產業個人資料檔案安全維護管理辦法」

部　長　唐鳳

數位經濟相關產業個人資料檔案安全維護管理辦法

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。

第　二　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　三　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　四　條　業者應對內公開周知個人資料保護管理政策，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、處理或利用個人資料。

三、以可期待之合理安全水準技術保護其所蒐集、處理或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、處理或利用個人資料者，應妥善監督受託者。

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　五　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　六　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　七　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　八　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　九　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　十　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 十一 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 十二 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 十三 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 十四 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 十五 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 十六 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 十七 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 十八 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 十九 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 二十 條　本辦法自發布日施行。

本則命令之總說明及逐條說明請參閱行政院公報資訊網（https://gazette.nat.gov.tw/）。

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

<table>
<tr><td colspan="3">個人資料侵害事故通報與紀錄表</td></tr>
<tr><td>業者名稱

通報機關</td><td colspan="2">通報時間:　年　月　日　時　分
通報人:　簽名(蓋章)
職稱:
電話:
Email:
地址:</td></tr>
<tr><td>事件發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">事件發生種類</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td><td>個人資料侵害之總筆數(大約)
_____筆</td></tr>
<tr><td>□一般個人資料_____筆
□特種個人資料_____筆</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料外洩可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於知悉個人資料外洩後72小時通報</td><td colspan="2">□是　□否，理由：</td></tr>
</table>