觀光產業類非公務機關個人資料檔案安全維護管理辦法

中華民國 111 年 4 月 1 日交路（一）字第 11182002907 號令訂定

中華民國 114 年 11 月 12 日交授觀企字第 11420008691 號令修正

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　本辦法所稱主管機關：在中央為交通部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。

第三條　本辦法所稱非公務機關，包括下列各款：

一、觀光旅館業。

二、旅館業。

三、民宿。

四、旅行業。

五、觀光遊樂業。

本辦法所稱消費者，指以消費為目的而為交易、使用商品或接受服務者。

第四條　非公務機關保有消費者個人資料達八千筆者，應依本辦法規定，規劃、訂定、修正與執行消費者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（以下簡稱本計畫及處理方法）。

依前項規定應訂定本計畫及處理方法者，應於本辦法施行之日起六個月內完成；其於本辦法施行後，保有消費者個人資料筆數始達八千筆者，應自保有筆數達八千筆之日起六個月內完成之。

非公務機關依前二項規定完成本計畫及處理方法之訂定後，所保有之消費者個人資料筆數減少，連續二年期間所保有之筆數未達八千筆者，得停止本計畫及處理方法全部或一部之執行。但嗣後保有之消費者個人資料筆數達八千筆時，應於保有筆數達八千筆之日起三十日內，恢復本計畫及處理方法全部之執行。

前三項消費者個人資料筆數，以非公務機關累計所保有之消費者個人資料為計算基準；其未達八千筆之事實，應由非公務機關證明之。

非公務機關經主管機關要求提出本計畫及處理方法實施情形者，應於收受通知後三十日內，以書面方式提出。

第五條　非公務機關依前條規定訂定本計畫及處理方法時，應視其組織規模、特性、保有個人資料之性質及數量等事項，參酌第六條至第二十一條規定，訂定包含下列各款事項之適當安全維護管理措施；必要時，第二款各目事項得整併之：

一、非公務機關之組織規模及特性。

二、個人資料檔案之安全管理措施：

（一）配置管理之人員及相當資源。

（二）界定蒐集、處理及利用個人資料之範圍。

（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）設備安全管理、資料安全管理及人員管理措施。

（七）認知宣導及教育訓練。

（八）個人資料安全維護稽核機制。

（九）使用紀錄、軌跡資料及證據保存。

（十）個人資料安全維護之整體持續改善。

（十一）業務終止後之個人資料處理方法。

第六條　非公務機關應依其業務規模及特性，衡酌經營資源之合理分配，建立個人資料檔案安全維護管理組織，配置相當人員及資源，負責規劃、訂定、修正與執行本計畫及處理方法等相關事項。

本計畫及處理方法之訂定或修正，應經非公務機關代表人或經其授權之人員核定。

個人資料檔案安全維護管理組織，應定期就執行任務情形向

非公務機關代表人或經其授權之人員提出書面報告。

非公務機關應將訂定之安全維護計畫留存營業所在地備查；主管機關得派員檢查。

第七條　非公務機關應依個人資料保護相關法令，定期查核確認所保有之個人資料現況，界定其納入本計畫及處理方法之範圍。

第八條　非公務機關應依前條界定之個人資料範圍及其蒐集、處理、利用個人資料之流程，評估可能產生之個人資料風險，並根據風險評估之結果，訂定適當之管控機制。

第九條　非公務機關為因應消費者個人資料被竊取、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、事故發生後應受通報之對象及其通報方式。

三、事故發生後研議其矯正預防措施之機制。

前項第一款通知當事人之內容應包含個人資料外洩之事實、採取之因應措施及提供之諮詢服務專線。

非公務機關遇有消費者個人資料外洩事故，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格式通報其主管機關。如向地方主管機關通報，非公務機關並應副知中央主管機關。

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。

主管機關得知或接獲第三項通報後，得依本法第二十二條至第二十五條規定，為適當之監督管理措施。中央主管機關認有必要時，得督導地方主管機關對於非公務機關之相關機制改善情形。

第十條　非公務機關所屬人員為執行業務而蒐集、處理一般個人資料時，應檢視是否符合本法第十九條之要件；利用時，應檢視是否符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合本法第二十條第一項但書情形。

第十一條　非公務機關蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。

第十二條　中央主管機關依本法第二十一條規定，對非公務機關為限制國際傳輸個人資料之命令或處分時，非公務機關應通知所屬人員遵循辦理。

非公務機關將個人資料作國際傳輸者，應檢視是否受中央主管機關限制，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：

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。

第十三條　非公務機關於個人資料當事人行使本法第三條規定之權利時，應依下列規定辦理：

一、提供聯絡窗口及聯絡方式。

二、確認為個人資料當事人本人，或經其委託者。

三、認有本法第十條但書各款、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之事由時，應附理由通知當事人。

四、有收取必要成本費用者，應告知當事人收費基準。

五、遵守本法第十三條有關處理期限之規定。

第十四條　非公務機關對所蒐集保管之個人資料檔案，應採取必要適當之安全設備或防護措施。

前項安全設備或防護措施，應包含下列事項：

一、紙本資料檔案之安全保護設施。

二、電子資料檔案存放之電腦、自動化機器相關設備、可攜式設備或儲存媒體，配置安全防護系統或加密機制。

三、存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放媒介物報廢汰換或轉作其他用

途時，應採取適當之銷毀或防範措施，避免洩漏個人資料；委託他人執行者，非公務機關對受託者之監督依本法第二十條規定辦理。

第十五條　非公務機關為確實保護個人資料之安全，應對其所屬人員採取適度管理措施。

前項管理措施，應包含下列事項：

一、依據業務需求，適度設定所屬人員不同之權限，控管其接觸個人資料之情形，並定期檢視權限內容之適當性及必要性。

二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。

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、所屬人員異動或離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂保密切結書。

第十六條　非公務機關使用資通訊系統蒐集、處理或利用消費者個人資料達八千筆，且具對外電子商務服務系統者，應採取下列資料安全管理措施：

一、使用者身分確認及保護機制。

二、個人資料顯示之隱碼機制。

三、網際網路傳輸之安全加密機制。

四、個人資料檔案與資料庫之存取控制及保護監控措施。

五、防止外部網路入侵對策。

六、非法或異常使用行為之監控及因應機制。

前項第五款及第六款所定措施，應定期演練及檢討改善。

第一項所稱電子商務，係指透過網際網路進行有關商品或服務之廣告、行銷、供應、訂購或遞送等各項商業交易活動。

第十七條　非公務機關應定期或不定期對於所屬人員施以基礎個人資

料保護認知宣導及教育訓練，使其明瞭相關法令之要求、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及措施。

第十八條　非公務機關為確保本計畫及處理方法之落實，應依其組織規模及特性，衡酌資源之合理分配，訂定個人資料安全維護稽核機制，並指定適當人員每年至少進行一次本計畫及處理方法執行情形之檢查。

前項檢查結果應向代表人提出報告，並留存相關紀錄，其保存期限至少五年。

非公務機關依第一項檢查結果發現本計畫及處理方法不符法令或有不符法令之虞者，應即改善。

第十九條　非公務機關執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。

非公務機關依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄：

一、刪除、停止處理或利用之方法、時間或地點。

二、將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間、地點，及該對象蒐集、處理或利用之合法依據。

前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。

第二十條　非公務機關應隨時參酌業務與本計畫及處理方法之執行狀況、社會輿情、技術發展及相關法規增修等因素，檢討所定本計畫及處理方法，必要時予以修正。

第二十一條　非公務機關委託他人蒐集、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為適當監督。

非公務機關為執行前項監督，應與受託者明確約定相關監督事項及方式。

第二十二條　非公務機關業務終止後，其保有之個人資料不得繼續使用，應依下列方式處理，並留存相關紀錄，其保存期限至少五年：

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。

第二十三條　本辦法自發布日施行。