旅行業個人資料檔案安全維護計畫及處理辦法

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。	本辦法訂定依據。
第二條　旅行業保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏；其為綜合旅行業及甲種旅行業者，並應訂定個人資料檔案安全維護計畫（以下簡稱維護計畫）。 前項維護計畫之訂定，綜合旅行業及甲種旅行業應於取得旅行業執照前完成；其於本辦法施行前已取得旅行業執照者，應於本辦法施行之日起六個月內完成。	一、依本法第二十七條第一項規定，「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏」，爰於本條第一項前段規定全體旅行業不分種類皆應予遵循。另依本法第二十七條第二項規定，「中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法」，爰依各種類之旅行業規模大小等，於本條第一項後段規定應訂定個人資料檔案安全維護計畫之旅行業種類。 二、現行國內旅行業依本條例第二十七條第二項規定分為綜合、甲種、乙種三類，數量分別為一百二十四家、二千二百八十八家、二百零七家，考量旅行業多為中小型企業，且多不具法律專業，爰選擇資本總額較高、經營規模較大之綜合旅行業及甲種旅行業為指定對象，須訂定個人資料檔案安全維護計畫。至於乙種旅行業雖無須訂定維護計畫，惟仍應依本條第一項前段規定，採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 三、另增列第二項，規定旅行業訂定維護計畫義務之時間，俾期明確；另就本辦法施行前已取得旅行業執照之旅行業，給予六個月作業

	時間，以完成維護計畫之訂定。
第三條　旅行業保有個人資料檔案者，得參酌第四條至第二十條規定，訂定適當之安全維護管理措施。 綜合旅行業及甲種旅行業訂定之維護計畫內容，應包括下列項目，下列項目必要時得予整併： 一、 配置管理人員及相當資源。 二、 界定個人資料之範圍並定期清查。 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、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、 資料安全稽核機制。 八、 使用紀錄、軌跡資料及證據保存。 九、 辦理個人資料認知宣導及教育訓練。 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。	一、本法施行細則第十二條就本法第二十七條第一項所定非公務機關應採行「適當之安全措施」，已規定其措施得包括之相關事項，本辦法第四條至第二十條主要即係就其所列項目進一步為具體規定，爰配合前條第一項前段所定旅行業之義務，於第一項規定提示其履行義務之方法。 二、配合前條第一項後段規定「綜合旅行業及甲種旅行業者，並應訂定個人資料檔案安全維護計畫」之義務，第二項規定其個人資料保護計畫內容應包括之項目，其具體內容則如第一項規定所述，係進一步規定於第四條至第二十條。
第四條　旅行業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。 前項清查發現有下列情形者，旅行業應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料: 一、非屬特定目的必要範圍內之個人資料。	本計畫及方法固針對個人資料安全訂定維護計畫，惟受保護之標的即個人資料檔案本身之適法性厥為前提事項，爰規定旅行業應先確認蒐集個人資料之特定目的，再依其目的之必要性，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，並於清查後予以適當處置。

二、特定目的消失或期限屆滿而無本法第十一條第三項但書之情形。	
第五條　旅行業為遵守本法第八條及第九條關於告知義務之規定，應採取下列方式： 一、 檢視蒐集、處理個人資料之特定目的。 二、 檢視蒐集、處理之個人資料，是否符合免告知之事由；其不符者，依據資料蒐集之情形，採取適當之告知方式。	旅行業應依本法第八條及第九條之規定，除免為告知之情形外，應採取適當告知方式以盡告知義務。
第六條　旅行業應檢視蒐集、處理個人資料是否符合本法第十九條規定，具有特定目的及法定要件，並檢視利用個人資料是否符合本法第二十條第一項特定目的必要範圍內利用之規定；於特定目的外利用個人資料時，應檢視是否具備法定特定目的外利用要件。	旅行業應符合本法第十九條、第二十條第一項規定於特定目的內蒐集、處理、利用個人資料，若於特定目的外利用，應檢視是否具備法定特定目的外利用要件。
第七條　旅行業於首次利用個人資料為行銷時，應提供當事人免費表示拒絕接受行銷之方式；當事人表示拒絕行銷後，應立即停止利用其個人資料行銷，並週知所屬人員。	旅行業於首次利用個人資料行銷時必須向當事人揭露拒絕接受行銷之方式，且當事人拒絕行銷後，應立即停止利用其個人資料行銷，並週知所屬人員。
第八條　旅行業為維護其所保有個人資料之正確性，應採取下列方式為之： 一、 檢視個人資料於蒐集、處理或利用過程，是否正確。 二、 當發現個人資料不正確時，適時更正或補充。 三、 個人資料正確性有爭議者，應依本法第十一條第二項規定處理。 因可歸責於旅行業之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對	一、依本法第十一條第一項規定「公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之」，旅行業為確保所保有個人資料之正確性，應採取適當方式確認並適時更正補充，爰為第一款、第二款規定。 二、個人資料正確性有爭議者，依本法第十一條第二項規定「應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須並註明其爭議或經當事人書面同意

象。	者，不在此限」，爰為第三款規定。 三、配合本法第十一條第一項所定維護旅行業所保有個人資料正確性義務，同條第五項另規定「因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知其曾提供利用之對象」，鑒於其違反者，依本法第四十八條第二款有處罰規定，爰於第二項併予增列規定，俾期業者注意遵守，並維護其曾提供利用該個人資料之正確性。
第九條　旅行業委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託人依本法施行細則第八條規定為適當之監督，並明確約定相關監督事項與方式。	本法施行細則第八條規定「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。 前項監督至少應包含下列事項：……。」，爰配合並引用前揭施行細則條次，規定旅行業委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託人為適當監督，避免違反本法相關規定。
第十條　旅行業進行個人資料國際傳輸前，應檢視有無交通部依本法第二十一條規定為限制國際傳輸之命令或處分，並應遵循之。	本法二十一條規定「非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：一、涉及國家重大利益。二、國際條約或協定有特別規定。三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。四、以迂迴方法向第三國（地區）傳輸個人資料規避本法」，依發展觀光條例第三條及第二十六條規定，旅行業之中央目的事業主管機關為交通部，爰規定旅行業進行個人資料國際傳輸前，應確認交通部是否依前揭規定而有所限制，並應予以遵循。
第十一條　旅行業為提供資料當事人行使本法第三條所定權利，應採取下列方式為之：	本法第三條規定當事人就其個人資料可行使查詢、閱覽、製給複本、補充更正、要求停止蒐集、處理、利用、刪除

一、確認是否為個人資料之本人，或經其委託授權者。 二、提供當事人行使權利之方式，並遵守本法第十三條有關處理期限之規定。 三、告知是否酌收必要成本費用。 四、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行使權利之事由者，應附理由通知當事人。	之權利，惟為避免個人資料不當外洩，自應確認其是否有行使權利之資格，爰為第一款規定；另配合本法第十條但書、第十一條第二項及第三項但書、第十三條及第十四條，就得拒絕當事人事由、處理期限及得酌收必要成本費用等有所規範，爰於第二款至第四款一併規定旅行業應採取之方式。
第十二條　旅行業就個人資料檔案安全維護管理，應指定專人或建立專責組織，並配置相當資源。 前項專人或專責組織之任務如下： 一、 規劃、訂定、修正與執行維護計畫及業務終止後個人資料處理方法等相關事項，並定期向旅行業負責人報告。 二、 訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。 三、 定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。	為有效訂定及執行個資檔案安全維護管理，旅行業應指定專人或建立專責組織，定期向旅行業負責人報告個資安全狀況。又專人或專責組織除負責個人資料檔案安全維護計畫相關事項，亦須對所屬人員進行教育訓練，使其明瞭個人資料保護法相關規定、所屬人員之責任範圍。
第十三條　旅行業應採取下列人員管理措施： 一、 依據蒐集、處理及利用個人資料個別作業之需要，適度設定所屬人員不同之權限並控管其接觸個人資料。 二、 檢視各相關業務流程涉及蒐集、處理及利用個人資料之負	旅行業應訂定從事個人資料業務之人員管理措施，諸如設定不同權限、簽訂保密條款、離職或完成受指派工作後應將個人資料交接，亦不得加以複製使用。

責人員。 三、 要求所屬人員負有保密義務。 四、 所屬人員離職或完成受指派工作後，應將其執行業務所持有之個人資料辦理交接，亦不得私自持有複製物而繼續使用該個人資料。	
第十四條　旅行業應採取下列資料安全管理措施： 一、 運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，應訂定使用可攜式設備或儲存媒體之規範。 二、 針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，應採取適當之加密機制。 三、 作業過程有備份個人資料之需要時，應比照原件，依本法規定予以保護。 四、 存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物於報廢或轉作其他用途時，應採適當防範措施以避免洩漏個人資料；其委託他人執行者，準用第九條規定辦理。	旅行業應對個人資料採取適當之資料安全管理措施，例如加密、個人資料報廢或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料。
第十五條　旅行業針對保存個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦或自動化機器設備等媒介物之環境，應採取下列環境管理措施： 一、 依據作業內容之不同，實施適宜之進出管制方式。 二、 所屬人員應妥善保管個人資料之媒介物。 三、 針對不同媒介物存在之環境，適度建置空調、消防、防鼠	旅行業針對保存個人資料之媒介物環境管理措施得採取進出管制措施，所屬人員應妥善保管媒介物，且對媒介物提供適度保護設備或技術。

除蟲等保護設備或技術。	
第十六條　旅行業為因應所保有之個人資料發生被竊取、竄改、損毀、滅失或洩漏等事故，應採取下列機制： 一、 採取適當之應變措施，以控制並降低事故對當事人之損害，並通報交通部觀光局。 二、 查明事故之狀況並依本法第十二條規定以適當方式通知當事人，並告知已採取之因應措施。 三、 檢討缺失並研擬預防機制，避免類似事故再次發生。	本法施行細則第十二條第二項第四款規定「事故之預防、通報及應變機制」為本法第二十七條第一項所稱適當之安全措施之一。旅行業有個人資料被竊取、竄改、損毀、滅失或洩漏等事故發生者，應採取適當應變措施降低對當事人之損害，並通知當事人，嗣後亦需研議預防機制以避免事故再次發生，爰參考法務部所定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辦法之參考事項第二點第四款，為本條規定。
第十七條　旅行業應訂定個人資料安全稽核機制，定期或不定期查察第十二條所定專人或專責組織是否落實執行所定計畫等相關事項，並列入專人或專責組織成員之考績。	旅行業應訂定個人資料檔案安全稽核機制，並定期或不定期查察專人或專責組織是否落實執行。
第十八條　旅行業應採行適當措施，採取個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據保存機制，以供必要時說明其所定維護計畫之執行情況；其相關紀錄之保存期限，至少為五年。	旅行業應留存個人資料使用紀錄等保存證據機制，以供證明確有實施所定計畫。另為明確其責任，並兼顧查考必要，爰於後段規定其相關紀錄之保存年限。
第十九條　旅行業宜參酌執行業務現況、社會輿情、技術發展、法令變化等因素，檢視所定維護計畫是否合宜，必要時予以修正。	旅行業應參酌相關因素，檢視所定計畫是否合宜，必要時予以修正。
第二十條　旅行業業務終止後，其保有之個人資料應依下列方式處理及記錄；其紀錄並應至少保存五年： 一、銷毀者，記錄其方法、時間、地點及證明銷毀之方式。 二、移轉者，記錄其原因、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。	旅行業於業務終止後，包括依旅行業管理規則第五十九條規定旅行業受交通部觀光局廢止旅行業執照、自行解散等，對個人資料之處理方式，得採取銷毀、移轉或其他刪除、停止處理、利用個人資料之措施，並保存相關紀錄至少五年，以供必要時之稽核。

三、其他刪除、停止處理或利用個人資料者，記錄其方法、時間或地點。	
第二十一條　本辦法施行日期，由交通部定之。	本辦法之施行日期，考量相關配套措施作業時程，爰規定由交通部另定之。