

高雄市旅行商業同業公會 (函)

公會地址：(801)高雄市前金區市中一路167號5樓
電話：(07)241-3881

受文者：全體會員旅行社

速別：最速件

密等及解密條件：普通

發文日期：中華民國104年05月29日

發文字號：高市旅行(104)本字第174號

主旨：「旅行業個人資料檔案安全維護計畫及處理辦法」，業經交通部於104年5月5日以交路(一)字第10482001664號令訂定發布，並自即日施行，檢送發布令影本(含法規條文)及「旅行社個人資料檔案安全維護計畫範本」，敬請查照。

說明：

1. 依據交通部觀光局104年5月22日觀業字第1040909259號函轉交通部104年5月5日交路(一)字第10482001661號、10482001662號、10482001663號函(副本)辦理。
2. 該局訂定之「旅行業個人資料檔案安全維護計畫及處理辦法」共21條，業經交通部104年5月5日以交路(一)字第10482001664號令訂定發布施行在案，其重點如下：
 - (1)本辦法依個人資料保護法第27條第3項訂定、適用對象為旅行業，綜合、甲種旅行業並應訂定個人資料檔案安全維護計畫，及該計畫所應包含之必要事項內容要項。(第1條至第3條)
 - (2)個人資料妥適性之確保：旅行業進行安全維護之前，應確認個人資料蒐集之特定目的、蒐集處理個人資料時應行告知義務、進行個人資料蒐集、處理及利用之限制，個人資料正確性之確保程序、旅行業委託他人進行蒐集、處理及利用時，應依相關規定辦理、利用個人資料行銷之注意事項、個人資料進行國際傳輸前應遵循事項、當事人行使權利之方式。(第4條至第11條)
 - (3)安全管理措施：旅行業指定專人或專責組織負責安全維護管理工作，並明定人員管理、資料安全管理、環境管理等措施。倘仍發生竊取、竄改、毀損、減失或洩漏等事故，應採取之機制(包括通報該局、以簡訊或書面等適當方式通知當事人，通知內容包括個人資料外洩事實、已採取之處理措施、客服電話窗口等資訊)。(第12條至第16條)

(4)安全稽核、紀錄保存及改善機制:有關旅行業個人資料之安全稽核機制、個人資料使用記錄保存及改善個人資料保護計畫等事項。

(第 17 條至第 19 條)

(五)業務終止後之措施:旅行業業務終止後對個人資料檔案應採取之措施，併與留存相關紀錄。(第 20 條)

3. 按本辦法第 2 條第 2 項規定，綜合、甲種旅行業者應於本辦法施行後 6 個月內訂定維護計畫，請會員應於 104 年 11 月 4 日前填寫旨揭範本，旨揭範本已置於該局行政資訊網(消保事項專區→旅行業→其他宣導事項)，並參考該範本訂定維護計畫執行;該局未來前往旅行業進行業務檢查時將一併檢查是否訂定旨揭維護計畫。若未於上開期限內訂定維護計畫，將依個人資料保護法第 48 條規定，經限期改正，屆期未改正者，按次處新臺幣 2 萬元以上 20 萬元以下罰鍰。

理事長

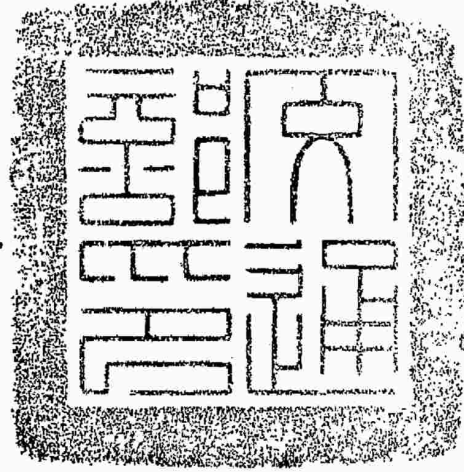
沈奉立

正本

檔 號：
保存年限：

交通部 令

發文日期：中華民國104年5月5日
發文字號：交路（一）字第10482001664號



裝



訂定發布「旅行業個人資料檔案安全維護計畫及處理辦法」，並
定自即日施行。

附「旅行業個人資料檔案安全維護計畫及處理辦法」

線

部長 陳建宇

○○旅行社(股份)有限公司個人資料檔案安全維護計畫範本

壹、旅行業之組織及規模

- 一、組織型態：股份有限公司、有限公司
- 二、代表人(負責人)：○○○
- 三、資本額：新臺幣○○○萬元整
- 四、公司編號：○○○
- 五、公司類別：(綜合、甲種)
- 六、公司地址：○○市○○區○○路(街)○段○號○○樓
- 七、員工人數：○○人

貳、個人資料檔案之安全維護管理措施(計畫內容)

一、管理人員及資源

(一) 管理人員：

- 1、配置人數：○人。(建議至少配置1名管理人員)
- 2、職責：負責規劃、訂定、修正與執行計畫或業務終止後個人資料處理方法等相關事項，並向負責人提出報告。

(二) 預算：每一年新台幣○○萬元。(包含管理人員薪資、設備費用等，依實際狀況填寫)

(三) 個人資料保護管理政策：遵循個人資料保護法關於蒐集、處理及利用個人資料之規定，並確實維護與管理所保有個人資料檔案安全，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

二、個人資料之範圍

(一) 特定目的：旅行業服務、接受旅客委託代辦入、出國境及簽證手續、履行旅遊契約或類似契約或其他法律關係事務、消費者旅客管理與服務、辦理責任保險、人事管理、承攬執行接待或引導旅客觀光旅遊業務而收取報酬之導遊、領隊。(類別：識別類、社會情況類)

(二) 個人資料：本計畫所稱自然人之個人資料，除係指旅客姓名、出生年月日、國民身分證統一編號、護照號碼、聯絡方式、信用卡號外及其他得以直接或間接方式識別該個人之資料。

三、風險評估及管理機制

(一) 風險評估

- 1、經由本公司電腦下載或外部網路入侵而外洩。

- 2、經由接觸書面契約書類而外洩。
- 3、員工及第三人竊取、毀損或洩漏。
- 4、旅行社間互為傳輸時之外洩（包括分公司間傳輸、同業旅行社間傳輸）。

（二）管理機制

- 1、藉由使用者代碼、識別密碼設定及文件妥適保管。
- 2、定期進行網路資訊安全維護及控管。
- 3、電磁資料視實際需要以加密方式傳輸。
- 4、加強對員工之管制及設備之強化管理。

四、個人資料蒐集、處理及利用管理措施

（一）直接向當事人蒐集個人資料時，應明確告知以下事項：

- 1、 公司名稱。
- 2、 蒐集目的。
- 3、 個人資料之類別。
- 4、 個人資料利用之期間、地區、對象及方式。
- 5、 當事人得請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。
- 6、 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

（二）所蒐集非由當事人（或旅客）提供之個人資料，應於處理或利用前向當事人告知個人資料來源及前項應告知之事項。

（三）旅行社得為辦理本計畫之特定目的內，進行個人資料蒐集、處理、利用，於委託期限屆滿時應主動刪除或銷毀。但因法令規定（旅行業管理規則第25條第3項：「旅行業辦理旅遊業務，應製作旅客交付文件與繳費收據，分由雙方收執，並連同與旅客簽定之旅遊契約書，設置專櫃保管一年，備供查核。」）、執行業務所必須或經書面同意者，不在此限。

（四）利用個人資料為行銷時，當事人（或旅客）表示拒絕行銷後，應立即停止利用其個人資料行銷。

（五）旅客表示拒絕行銷或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料時，連絡窗口為：○○○；電話為：○○○○○○○。並將聯絡窗口及電話等資料，揭示於本公司營業處所或公司網頁。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。

（六）負責保管及處理個人資料檔案之員工，其職務有異動時，應將所保管之儲

存媒體及有關資料檔案移交，以利管理。

(七) 本公司員工如因其工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

(八) 由指定之管理員工定期清查所保有之個人資料是否符合蒐集特定目的，若有非屬特定目的必要範圍之資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置。

(九) 本公司如有委託他人（或他公司）蒐集、處理或利用個人資料時，當對受託者為適當之監督並與其明確約定相關監督事項。

（如未委託他人則可以選擇加以刪除）

(十) 所蒐集之個人資料如需作特定目的外利用，必須先行檢視是否符合規定。

(十一) 本公司因故終止業務時，原保有之個人資料，即依規定不再使用，並採銷毀、移轉或其他妥適方式處理。

五、事故之預防、通報及應變機制

(一) 預防：

- 1、本公司員工如因其工作執掌而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之。
- 2、本公司對內或對外從事個人資料傳輸時，加強管控避免外洩。
- 3、加強員工教育宣導，並嚴加管制。

(二) 通報及應變：

- 1、發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向交通部觀光局及公司負責人通報，並立即查明發生原因及責任歸屬，及依實際狀況採取必要措施。
- 2、對於個人資料遭竊取之旅客，應以適當方式通知使其知悉及本公司個人資料外洩事實、已採取之處理措施、客服電話窗口等資訊。
- 3、針對事故發生原因研議改進措施。

六、資料安全管理、員工管理及設備安全管理

(一) 資料安全管理

1、電腦存取個人資料之管控：

- (1) 個人資料檔案儲存在電腦硬式磁碟機上者，應在電腦設置識別密碼、保護程式密碼及相關安全措施。
- (2) 本公司員工如因其工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為

之，其中識別密碼並應保密，不得洩漏或與他人共用。

- (3) 個人資料檔案使用完畢應即退出，不得任其停留於電腦終端機上。
- (4) 定期進行電腦系統防毒、掃毒之必要措施。
- (5) 重要個人資料（如護照號碼、國民身分證統一編號）應另加設管控密碼，非經陳報公司主管核可，並取得密碼者，不得存取。

2、紙本資料之保管：

- (1) 對於各類委託書、契約書件（含個人資料表）應存放於公文櫃內並上鎖，員工非經公司負責人或營業處所主管同意不得任意複製或影印。
- (2) 對於記載個人資料之紙本丟棄時，應先以碎紙設備進行處理。

（二）員工管理

- 1、本公司依業務需求，得適度設定所屬員工（例如主管、非主管員工）不同之權限，以控管其個人資料之情形。
- 2、本公司員工每○天（週、月）應變更識別密碼1次，並於變更識別密碼後始可繼續使用電腦。
- 3、員工或承攬執行接待或引導旅客觀光旅遊業務而收取報酬之導遊、領隊。與公司終止僱傭、委任、承攬等契約時，將立即取消其使用者代碼（帳號）及識別密碼。其所持有之個人資料應辦理交接，不得在外繼續使用，並簽訂保密切結書（如在任職時之相關勞務契約已有所約定時，亦屬之）。
- 4、本公司員工應妥善保管個人資料之儲存媒介物，執行業務時依個人資料保護法規定蒐集、處理及利用個人資料。
- 5、本公司與員工所簽訂之相關勞務契約或承攬契約均列入保密條款及相關之違約罰則，以確保其遵守對於個人資料內容之保密義務（含契約終止後）。

（三）設備安全管理

- 1、建置個人資料之有關電腦設備，資料保有單位應定期保養維護，於保養維護或更新設備時，並應注意資料之備份及相關安全措施。
- 2、建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。
- 3、公司應指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經單位主管同意並作成紀錄不得攜帶外出或拷貝複製。
- 4、本公司之旅客個人資料檔案應定期（例如：每二週）備份。
- 5、重要個人資料備份應異地存放，並應建置防止個人資料遭竊取、竄改、損毀、滅失或洩漏等事故之機制。
- 6、電腦、自動化機器或其他存放媒介物需報廢汰換或轉作其他用途時，本公司負責人或營業處所主管應檢視該設備所儲存之個人資料是否確實刪除。

七、資料安全稽核機制

(一) 本公司定期(每年至少 1 次)辦理個人資料檔案安全維護稽核，查察本公司是否落實本計畫規範事項，針對查察結果不符合事項及潛在不符合之風險，應規劃改善措施，並確保相關措施之執行。執行改善與預防措施時，應依下項事項辦理：

- 1、確認不符合事項之內容及發生原因。
- 2、提出改善及預防措施方案。
- 3、紀錄查察情形及結果。

(二) 前項查察情形及結果應載入稽核報告中，由公司負責人簽名確認。

八、使用記錄、軌跡資料及證據保存

本公司建置個人資料之電腦，其個人資料使用查詢紀錄，每年需將該紀錄檔備份並設定密碼，另亦將儲存該紀錄之儲存媒介物保存於適當處所以供備查。

(註：本項請依實際情形說明公司如何保存，例如：個人資料使用查詢紀錄、自動化機器設備之軌跡資料(電腦設備或其他相關之證據資料須加以保存並製作備份保存於適當處所，以供必要時說明其所訂計畫之執行情況。)

九、認知宣導及教育訓練

- (一) 本公司每年派遣員工○人參與交通部觀光局辦理進行個人資料保護法基礎教育宣導及數位學習教育訓練至少○小時，使員工知悉應遵守之規定。前述教育宣導及訓練應留存紀錄(例如：簽名冊等文件)
- (二) 對於新進員工應特別給予指導，務使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

十、個人資料安全維護之整體持續改善

- (一) 本公司將隨時依據計畫執行狀況，注意相關技術發展及法令修正等事項，檢討本計畫是否合宜，並予必要之修正。
- (二) 針對個資安全稽核結果不合法令之虞者，規劃改善與預防措施。

十一、業務終止後之個人資料處理方法

本公司結束營業後，所保有之個人資料不得繼續使用，並依實際情形採下列方式處理，並留存相關紀錄至少五年(請勾選或填寫下列事項)：

(一) 銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

書面個人資料已送碎紙機絞碎。

儲存於電腦磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物之個人資料已格式化刪除資料或以物理方式破壞其功能，如折斷光碟片，擊毀硬碟等。

其他：(請自行填寫)

以上行為請拍照存證(照片需印日期並揭露地點)或錄影存證(影片需有

日期並揭露地點)。

(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。

移轉之原因：

業務需求

其他 (請自行填寫)：

移轉之對象：○○旅行社股份有限公司

移轉之方法：

紙本傳遞。

以電腦磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物傳遞。

其他 (請自行填寫)：

移轉之時間 (請自行填寫)：中華民國 000 年 00 月 00 日

移轉之地點 (請自行填寫)：

受移轉對象得保有該項個人資料之合法依據：依據個人資料保護法第 00 條規定…。

(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。

其他刪除、停止處理或利用之方法 (請自行填寫)：

其他刪除、停止處理或利用之時間 (請自行填寫)：

其他刪除、停止處理或利用之地點 (請自行填寫)：