觀光產業個人資料檔案安全維護自主檢查表 115.1.5版

公司名稱：	□有限公司 □股份有限公司
經營業別：旅行業/觀光遊樂業/觀光旅館業/旅館業/民宿（請自行圈選）	
保有個人資料筆數： 筆	檢查日期： 年 月 日
具對外電子商務服務系統：□是 □否	

檢查項目	檢查內容	檢查結果	說明	備註
1.消費者個人資料檔案安全維護計畫	是否訂定「消費者個人資料檔案安全維護計畫」	□是 □否 □不適用		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法（§4&§5）訂定。
2.配置管理之人員及相當資源	是否設有個人資料管理單位或適當組織？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§6)訂定。 可確認個資管理單位組織圖、分工及相關辦法，並提出個資窗口所協助之各項個資保護工作事項，如：參與會議、盤點及風險評鑑工作、事件處理等。
3.界定個人資料之範圍	是否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？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§7)訂定。 可確認個人資料檔案清冊及個人資料作業流程說明文件，並經權責主管核定之紀錄。

4.個人資料之風險評估及管理機制	是否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？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§8)訂定。 可確認風險評估過程底稿、風險評鑑報告及風險處理計畫。
5. 事故之預防、通報及應變機制	5.1個資事故應變機制是否包含降低、控制事故對當事人造成損害之作法？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§9)訂定。 可確認個資事故應變機制，機制中有說明是否有對降低、控制事故對當事人造成損害之作法。
	5.2個資事故應變機制，是否包含適時以電子郵件、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？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§9)訂定。 可確認個資事故應變機制，機制中有說明對通知當事人之作法。
	5.3個資事故應變機制，是否包含避免類似事故再次發生之矯正及預防機制？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§9)訂定。 可確認個資事故應變機制，機制中對避免類似事故再次發生之矯正及預防

				機制。
6. 蒐集、處理、利用作業	6.1資料蒐集、處理是否具備特定目的並具有法定要件？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§10)訂定。 可確認最新個資盤點資料，確認皆已識別個資蒐集、處理之保有依據。
	6.2個人資料之利用，是否符合特定目的之範圍？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§10)訂定。 可確認最新個資盤點資料，確認皆已識別個資的利用為符合特定目的範圍。
	6.3是否有目的外之利用？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§10)訂定。 確認公司已有確認所蒐集之個資是否具有目的外之利用情形。
	6.3.1目的外利用是否符合法定要件？	若6.3勾選勾選「是」請續填 □是 □否		如有目的外利用，應有其符合之法定要件。
	6.4是否履行告知義務？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§11)訂定。 可確認告知說明/同意書或相關佐

				證。 業者大部分應為對客戶直接蒐集個資。
	6.4.1未履行告知義務時，是否符合免告知之情形？	若6.4勾選勾選「否」請續填 □是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§11)訂定。 免告知可參考個資法第8條第2項。
	6.5是否依規定取得當事人同意（當事人同意之情形）？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§11)訂定。 可確認蒐集客戶個資取得當事人同意之情形，並確認告知同意書或相關佐證，有些業者會使用國內外旅遊定型化契約，稽核員應確認契約中的說明是否與現有方式相符。
	6.6是否已於首次行銷時提供當事人表示拒絕行銷之管道？如需費用是由公司支付所需費用？	□是 □否		依照個資法第20條第3項，可確認當事人拒絕行銷之方式，例如，提供免付費電話、免費回郵等。
	6.7是否依當事人拒絕接受行銷之要求，立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？	□是 □否		依照個資法第20條第2項，可確認當事人拒絕接受行銷後公司的作業流程，以防範所屬人員再次行銷之措施。

7.資料安全管理及人員管理	7.1是否識別業務內容涉及個人資料蒐集、處理或利用之人員？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§15)訂定。 可確認個資管理單位組織圖、分工及相關辦法，以及個人資料檔案清冊（確認接觸個資之人員）。
	7.2是否依其業務特性、內容及需求，設定所屬人員接觸消費者個人資料之權限，並定期檢視其適當性及必要性？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§15)訂定。 依個人資料檔案清冊盤點，了解接觸個資之人員，針對資料夾、系統權限進行帳號權限清查，可確認個資資料夾、個資系統權限申請表單以及帳號權限審查紀錄。
	7.3是否與所屬人員約定保密義務？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§15)訂定。 可確認所屬人員清單（正職、短期約僱）及所簽署之保密切結書，應包含個資保密等條款。
	7.4是否要求人員離職時，返還保有消費者個人資料之載體，並刪除因執行業務而持有之消費者個	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§15)訂定。 可確認所屬人員清單（正職、短期約

	人資料？			僱）及所簽署之保密切結書或離職單，應包含返還保有消費者個人資料之載體，並刪除因執行業務而持有之消費者個人資料之資訊。
	7.5消費者個人資料有加密之必要者，於蒐集、處理或利用時，是否採取適當之加密措施？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§14)訂定。 依個人資料檔案清冊盤點，確認個人資料檔案位置，針對其存放地點的安全性進行說明，包含： 1.針對個資電子檔案之控管規範，例如將個人資料檔案置於公用電腦、網路共用資料夾或系統中，是否進行加密或遮蔽，並確認查核結果。 2.針對紙本的資料是否安全存放，並確認查核結果。
	7.6傳輸消費者個人資料時，是否依不同傳輸方式，採取適當之安全措施？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§16)訂定。 可確認對外傳送個資檔案之相關規範，檢附規範制度文件。例如以電子郵件傳送敏感之個

				資檔案時，是否採加密機制，並可確認相關佐證。
	7.7消費者個人資料有備份之必要者，是否對備份資料採取適當之保護措施？	□是 □否		可確認資料備份機制相關規範制度文件。
8.認知宣導及教育訓練	8.1是否定期實施對所屬人員之個人資料保護與管理認知宣導及教育訓練？所屬人員是否明瞭上課內容？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§17)訂定。 可確認對所屬人員之教育訓練簡報、各項相關課程簽到表（需含授課日期）及課後評量結果。 上課內容應包含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。
9.設備安全管理措施	9.1是否依據作業內容及環境之不同，實施必要之安全環境管制？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§14)訂定。 可確認對存放儲存媒介物（放置個人資料的系統主機、辦公室）之環境相關消防、監控、進出入等控管措施，並確認相關證明。
	9.2是否妥善維護並控管個人資料蒐集、處理或利	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理

	用過程中所使用之實體設備？			辦法(§14)訂定。可確認是否定期檢查或維護更新設備，如系統主機、防火牆、個人電腦等，並可確認有定期檢查及維護紀錄。
	9.3是否針對不同作業環境，建置必要之保護設備或技術？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§14)訂定。可確認消防、監控設備（如防火牆）等管理/維護紀錄。
10.資料安全稽核機制	10.1是否每年定期由適當組織執行資料安全內部稽核並提出評估報告？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§18)訂定。確認資料安全稽核機制之作法，且應包含稽核之頻率及執行方式，並確認最近一次之評估報告。
	10.2是否採取改善措施以持續改善資料安全維護？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§18)訂定。確認持續改善之作法，可確認檢視或修正之紀錄，如矯正單/追蹤紀錄。
11.使用紀錄、軌跡資料及證據保存	11.1是否保存個人資料提供或移轉第三人之紀錄？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§18)訂定。

				若有保存個人資料提供或移轉第三人，應留有紀錄/合約規範。 若無則不適用。
	11.2是否保存當事人行使個資法第三條之權利及處理過程之紀錄？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§13)訂定。 確認當事人行使個資法第3條之權利及處理過程，若過去有發生過可確認相關紀錄，若無發生可確認目前之權利行使管道，如有個人資料當事人權利行使申請書。
	11.3是否保存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？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§19)訂定。 依個人資料檔案清冊盤點，清冊上的資料若有進行刪除、停止處理、利用或銷毀，可確認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。 如電子檔案銷毀、紙本檔案碎紙等之執行紀錄，登記在個人資料銷毀紀錄表。

	11.4是否保存人員權限新增、變動及刪除之紀錄？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§15)訂定。 可確認人員權限新增、變動及刪除之紀錄，如帳號異動申請表。
	11.5是否保存消費者個人資料之蒐集、處理及利用紀錄，以及自動化機器設備之軌跡資料？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§19)訂定。 依個人資料檔案清冊盤點，其存放的機器設備，應留有軌跡資料。可確認近一年消費者個人資料之蒐集、處理及利用紀錄（紙本&電子），以及自動化機器設備之軌跡資料，提醒資料應留存五年。
12.個人資料安全維護之整體持續改善	12.1是否定期就個人資料安全維護議題召開會議並提出持續改善報告？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§5)訂定。 可確認相關個人資料安全維護議題會議之紀錄。
	12.2是否訂定個人資料管理（或安全維護）辦法並定期檢視更新？	□是 □否		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§20)訂定。 可確認個人資料管理或安全維護辦法以及完整之版本資訊（安全維護計

				畫），包含但不限於日期、提報人及核定人等相關資訊。
13.委託作業	13.1委託他人蒐集、處理或利用個人資料之全部或一部時，是否要求受託人依委託人應適用之規定為之？	□是 □否 □不適用		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§21)訂定。 合約中是否有個資相關條款。可確認個資委外之廠商清單及合約文件。
	13.2委託他人蒐集、處理或利用個人資料之全部或一部時，是否於委託契約或相關文件明確約定適當之監督事項及方式？	□是 □否 □不適用		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§21)訂定。 合約中是否有約定個人資料適當之監督事項及方式，符合個人資料保護法施行細則第8條第2項之要求。可確認個資委外之廠商清單及合約文件。
	13.3委託他人蒐集、處理或利用個人資料之全部或一部時，是否確實執行監督？	□是 □否 □不適用		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§21)訂定。 承上，是否有進行執行。可確認對委外廠商之監督方式或檢附委外稽核報告以及稽核缺失追蹤情形。
	13.4是否要求受託者僅得於委託機關指示之範圍內，蒐集、處理	□是 □否 □不適用		依據個人資料保護法施行細則第8條第4項之要求。 合約中是否有相關

	或利用個人資料？			條款：僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。可確認個資委外之廠商清單及合約文件。
	13.5是否要求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？	□是 □否 □不適用		依據個人資料保護法施行細則第8條第4項之要求。 可確認個資委外之廠商清單及合約文件或其他地方有指示委外廠商之證明。
14.使用資通訊系統蒐集、處理或利用個人資料-消費者個人資料達8千筆，且具對外電子商務服務系統者	14.1是否採行使用者身分確認及保護機制？（基準日：○年○月○日，下同）	□是 □否 □不適用		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§16)訂定。 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。 帳號皆能辨識使用者，可確認帳號權限清查紀錄單。
	14.2是否採行個人資料顯示之隱碼機制？	□是 □否 □不適用		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§16)訂定。 系統之個人資料顯示之隱碼機制，可確認相關佐證紀錄。
	14.3是否採行網際網路傳輸之安	□是 □否		依據觀光產業類非公務機關個人資料

	全加密機制？	□不適用		檔案安全維護管理辦法(§16)訂定。應確認網際網路傳輸之安全加密機制，可確認相關佐證紀錄。
	14.4是否採行個人資料檔案及資料庫之存取控制與保護監控措施？	□是 □否 □不適用		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§16)訂定。如能看到個人資料之權限是否進行限縮，可確認帳號權限清查紀錄單，要能看出哪些帳號能看到完整個資。
	14.5是否採行防止外部網路入侵對策？	□是 □否 □不適用		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§16)訂定。
	14.6是否採行非法或異常使用行為之監控與因應機制？	□是 □否 □不適用		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§16)訂定。確認非法或異常使用行為之監控與因應機制。
	14.7前2項之防止外部網路入侵對策及非法或異常使用行為之監控與因應機制，是否定期演練及檢討改善？	□是 □否 □不適用		依據觀光產業類非公務機關個人資料檔案安全維護管理辦法(§16)訂定。確認防止外部網路入侵對策及非法或異常使用行為之監控與因應機制進行演練或檢討，如針對系統進行演練作業或對防火牆政策

				進行檢討等。
	14.8有存放個人資料之系統或伺服器是否已完成技術性檢測（弱點掃描、滲透測試），並針對檢測結果進行追蹤？	□是 □否 □不適用		
15.個資存放雲端之安全控管	15.1是否確保個人資料放在雲端上的安全？	□是 □否		若有放於雲端，應確認 Database 的安全以及放在那個國家，並確認相關佐證（如雲端業者出具的證明書）。若無則不適用。
16.發生個資事件之處理	16.1近兩年內是否發生個人資料被竊取、洩漏、竄改或其他侵害情形之個資事件？	□曾於兩年內發生個資事件。 □未有發生個資事件。		若是，請提供通報記錄等相關佐證。
	16.2是否就個資事件委請公正之第三方進行調查？	□於發生個資事件後，有委請公正之第三方進行調查。 □未有發生個資事件。		如就個資事件聘請第三方資安廠商調查並出具報告。
	16.3是否即時且適當的通知當事人？	□於發生個資事件後，有即時且適當的通知當事人。 □未有發生個資事件。		如向用戶說明事件緣由及防護措施之通知。
	16.4是否就事件的發生進行根因分析，並提出強化措施？	□於發生個資事件後，有就事件的發生進行根因分析，並提出強化措施。 □未有發生個資事件。		如事件報告、強化措施的實施情形以及相關內部會議紀錄。
17.個人資料庫	17.1是否有其他	□未有個人資料庫共享。		若是，請說明具體

之共享使用	關係企業或主體共享使用本公司所蒐集之客戶個人資料庫？	□有個人資料庫共享，並有確認具體共享使用之主體名稱，以及共享使用之原因及安全控管措施，且另確認告知當事人之佐證。	共享使用之主體名稱，以及共享使用之原因及安全控管措施。另有告知當事人之佐證。
	17.2是否使用其他關係企業或主體所蒐集之客戶個人資料庫加以處理及利用？	□未有使用其他組織個人資料庫。 □有使用其他組織個人資料庫，且有於處理及利用前告知當事人。	若是，有於處理及利用前告知當事人之佐證。
18.其他			
本公司保證所填資料及檢附文件均為真實，如有不實，願負一切法律責任。			
公司（經營業者）簽章：			

備註：各公司應依個人資料保護法及觀光產業類非公務機關個人資料檔案安全維護管理辦法落實個資保護機制，故不限於本表所列項目。