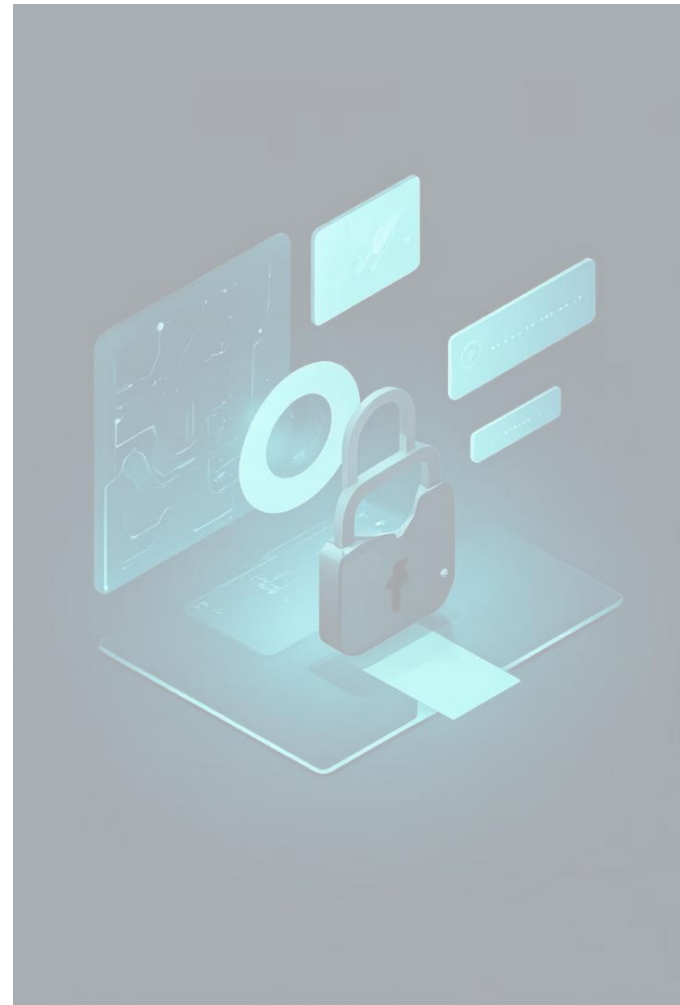




觀光署-115年度行政檢查計畫資安顧問服務案

季簡報

115年3月



一、共通性問題

- 查核家數3家，共3間須進行改善。

查核項目	查核內容
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？

- 依照交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第5條第1項第2點第2條界定蒐集、處理及利用個人資料之範圍。
- 業者應檢附「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，其個人資料之範圍界定之作法建議寫在安全維護計畫中。
- 可參考經濟部個資作業手冊
(https://www.moea.gov.tw/mns/colr/content/SubMenu.aspx?menu_id=7783)。

一、共通性問題

- 查核家數3家，共2間須進行改善。

查核項目	查核內容
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？

- 依照交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第5條第1項第2點第3條個人資料之風險評估及管理機制。
- 應檢附風險評估過程底稿、「風險評鑑報告」及「風險處理計畫」，其風險評估及管理機制作法建議寫在安全維護計畫中。
- 可參考經濟部個資作業手冊
(https://www.moea.gov.tw/mns/colr/content/SubMenu.aspx?menu_id=7783)。

一、共通性問題

- 查核家數3家，共2間須進行改善。

查核項目	查核內容
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？

- 依照交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第5條第1項第2點第4條事故之預防、通報及應變機制。
- 請提供個資事故應變機制，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。(規劃)。

一、共通性問題

- 查核家數3家，共2間須進行改善。

查核項目	查核內容
5.事故之預防、通報及應變機制	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？

- 請提供個資事故應變機制，機制中有說明對**通知當事人之作法**。(事故發生時)

一、共通性問題

- 查核家數3家，共2間須進行改善。

查核項目	查核內容
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？
	6.2個人資料之利用，是否符合特定目的之範圍？

- 請檢附最新個資盤點資料，確認皆已識別個資的利用為符合特定目的範圍。

一、共通性問題

- 查核家數3家，共3間須進行改善。

查核項目	查核內容
6.蒐集、處理、利用作業	6.4是否履行告知義務（未履行告知義務時，是否符合免告知之情形）？
	6.4.1未履行告知義務時，是否符合免告知之情形？

- 應檢附告知同意書範本或已執行之告知內容。
- 免告知可參考個資法第8條第2項：
 - 一、依法律規定得免告知。
 - 二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
 - 三、告知將妨害公務機關執行法定職務。
 - 四、告知將妨害公共利益。
 - 五、當事人明知應告知之內容。
 - 六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

一、共通性問題

- 查核家數3家，共3間須進行改善。

查核項目	查核內容
6.蒐集、處理、利用作業	6.5是否依規定取得當事人同意（當事人同意之情形）？

- 應說明蒐集客戶個資並取得當事人同意之情形，並檢附告知同意書範本。

一、共通性問題

- 查核家數3家，共3間須進行改善。

查核項目	查核內容
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？

- 依照交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第5條第1項第2點第6條資料安全管理及人員管理措施。
- 請檢附個資管理單位組織圖、分工及相關辦法(可放於安全維護計畫中)，以及個人資料檔案清冊(可看到是誰碰到個資)。

一、共通性問題

- 查核家數3家，共2間須進行改善。

查核項目	查核內容
7. 資料安全管理及人員管理	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？

- 依個人資料檔案清冊盤點，了解是誰會碰到個資，針對資料夾、系統權限進行帳號權限清查，應檢附個資資料夾、個資系統權限申請表單以及帳號權限審查紀錄。

一、共通性問題

- 查核家數3家，共2間須進行改善。

查核項目	查核內容
7. 資料安全管理及人員管理	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？

- 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？並檢附查核結果。
 - 2.針對**紙本的資料**是否進行上鎖櫃中存放？並檢附查核結果。

一、共通性問題

- 查核家數3家，共2間須進行改善。

查核項目	查核內容
7. 資料安全管理及人員管理	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？

- 請說明對外傳送個資檔案之相關規範，檢附規範制度文件，作法建議寫在安全維護計畫中。例如以電子郵件傳送敏感之個資檔案時，是否採加密機制？並請提供相關佐證。

一、共通性問題

- 查核家數3家，共2間須進行改善。

查核項目	查核內容
7. 資料安全管理及人員管理	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？

- 請說明資料備份機制，並檢附規範制度文件，作法建議寫在安全維護計畫中。

一、共通性問題

- 查核家數3家，共3間須進行改善。

查核項目	查核內容
9. 設備安全管理措施	9.2是否妥善維護並控管個人資料蒐集、處理或利用過程中所使用之實體設備？

- 請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？並請檢附定期檢查及維護紀錄。
- 確認針對存放個資主機其作業系統是否EOS。

一、共通性問題

- 查核家數3家，共2間須進行改善。

查核項目	查核內容
9. 設備安全管理措施	9.3是否針對不同作業環境，建置必要之保護設備或技術？

- 請檢附消防、監控設備(如防火牆)等管理/維護紀錄。

一、共通性問題

- 查核家數3家，共2間須進行改善。

查核項目	查核內容
10. 資料安全稽核機制	10.2是否採取改善措施以持續改善資料安全維護？

- 持續改善之作法建議寫在安全維護計畫中，應檢附檢視或修正之紀錄，如矯正單/追蹤紀錄。

一、共通性問題

- 查核家數3家，共2間須進行改善。

查核項目	查核內容
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？

- 依照交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第5條第1項第2點10條個人資料安全維護之整體持續改善。
- 應檢附相關個人資料安全維護議題會議之紀錄。

一、共通性問題

- 查核家數3家，共2間須進行改善。

查核項目	查核內容
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？

- 合約中是否有個資相關條款。
- 請檢附個資委外之廠商清單及合約文件。

