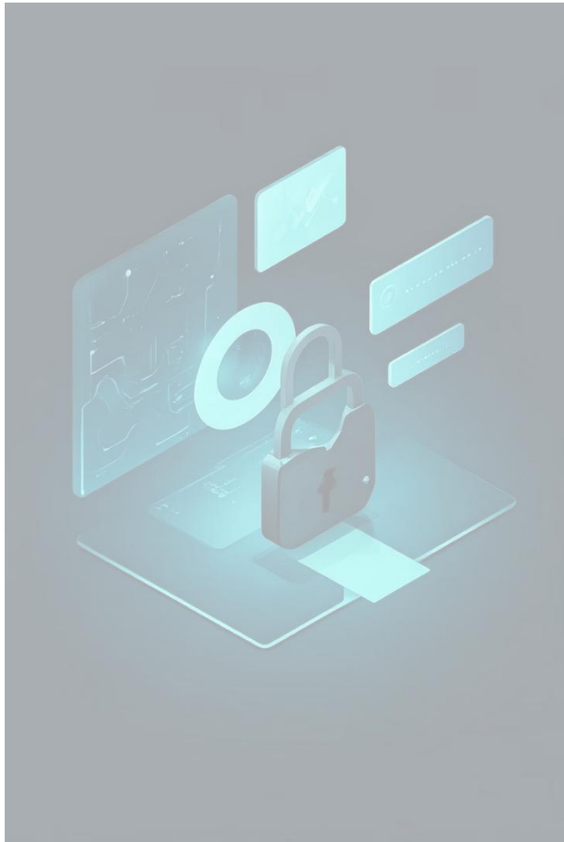
交通部觀光署115年度行政檢查計畫資安顧問服務案

季簡報

115年6月



目錄

一、共通性問題

二、個案問題分析

-觀光業者個資外洩分享

-近期事件分享

一、共通性問題

一、共通性問題

- 查核家數43家，共23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管理辦法第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43家，共35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管理辦法第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43家，6.1項共21間、6.2項共18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43家，共17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43家，共20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43家，共18間須進行改善。

查核項目	查核內容
8.認知宣導及教育訓練	8.1是否定期對實施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？

- 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管理辦法第5條第1項第2點第7條認知宣導及教育訓練。
- 請檢附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。

一、共通性問題

- 查核家數43家，共31間須進行改善。

查核項目	查核內容
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？

- 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管理辦法第5條第1項第2點第8條個人資料安全維護稽核機制。
- 資料安全稽核機制之作法建議寫在安全維護計畫中，且應包含**稽核之頻率及執行方式**，並應檢附最近一次之評估報告。

一、共通性問題

- 查核家數43家，共32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43家，共20間須進行改善。

查核項目	查核內容
11. 使用紀錄、軌跡資料及證據保存	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？

- 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，應檢附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。

一、共通性問題

- 查核家數43家，共19間須進行改善。

查核項目	查核內容
11. 使用紀錄、軌跡資料及證據保存	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？

- 依個人資料檔案清冊盤點，其存放的機器設備中，應留有軌跡資料。請檢附近一年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，提醒資料應留存五年(個資施行細則第19條第3項)。

一、共通性問題

- 查核家數43家，共25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管理辦法第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43家，共17間須進行改善。

查核項目	查核內容
13.委託作業	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

- 依據個人資料保護法施行細則第8條&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管理辦法第21條。
- 與委外廠商之合約中是否有約定個人資料適當之監督事項及方式，如每月報告、實地/書面稽核。
- 應檢附個資委外之廠商清單及合約文件。

一、共通性問題

- 查核家數43家，共22間須進行改善。

查核項目	查核內容
13.委託作業	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？

- 依據個人資料保護法施行細則第8條&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管理辦法第21條。
- 呈13.2，於合約中約定後，在履約期間的監督是否有執行。
- 請說明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。

一、共通性問題

- 查核家數43家，共18間須進行改善。

查核項目	查核內容
13.委託作業	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？

- 依據個人資料保護法施行細則第8條&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管理辦法第21條。
- 任何佐證能證明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。
- 應檢附個資委外之廠商清單及合約文件或其他地方有告知委外廠商之證明。

一、共通性問題

- 查核家數43家，共19間須進行改善。

查核項目	查核內容
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	14.7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？

- 應針對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作業。
- 應檢附系統演練紀錄，紀錄中包含演練檢討。

一、共通性問題

- 查核家數43家，共21間須進行改善。

查核項目	查核內容
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	14.8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？

- 確認是否完成技術性檢測（弱點掃描、滲透測試），並針對檢測完成後之結果進行追蹤修補。

二、個案問題分析
-觀光業者個資外洩說明
-近期事件分享

觀光業者A旅行社個資外洩說明

觀光業者A旅行社個資外洩原因及後續處理情形

觀光業者A旅行社個資外洩說明-事件說明

- 經訪查為離職人員蔡〇珊，於115年3月31日業務交接離職後對未完成訂單之部分人員(王〇馨、陳〇福、陳〇帆、彭〇敏、俞〇邑及譚〇婷等六人)(陳〇帆為陳〇福與彭〇敏之女、俞〇邑(未成年)為譚〇婷之女)之護照影本資料透過蔡員與客戶Line群組記事本方式留存與管理，造成客戶對此處理方式欠妥而要求僅有管理權限之蔡員刪除檔案後，才能提供護照影本資料進行後續處理，旅行社知悉後聯繫蔡員協助處理資料移交與刪除未果，旅行社於115年4月7日寄送存證信函催告，消極拒收至使信件於115年5月7日遭〇〇郵政退回，此次查核確認發現為消費執行上的程序問題。

觀光業者A旅行社個資外洩說明-後續可精進之作為

行政作業處理改善：

- 發生消費問題後單位立即調整人員離職個人資料歸還與銷毀保密切結相關要求。
- 落實人員離職作業前之業務交接，避免類似案件發生。
- 評估敏感資料透過個人與客戶line群組保存之問題。

其他建議強化部分

- 規劃作業系統Windows 10更新：
  - 建議停止使用已停止系統安全更新與技術支援之作業系統，避免安全疑慮。
- 個資盤點範圍完整性：
  - 建議納入同樣有蒐集會員個資之官網。
- 技術性檢測之範圍：
  - 建議將官網納入定期弱點掃描之範圍。

觀光業者B旅行社個資外洩說明

觀光業者B旅行社個資外洩原因及後續處理情形

觀光業者B旅行社個資外洩說明-事件說明

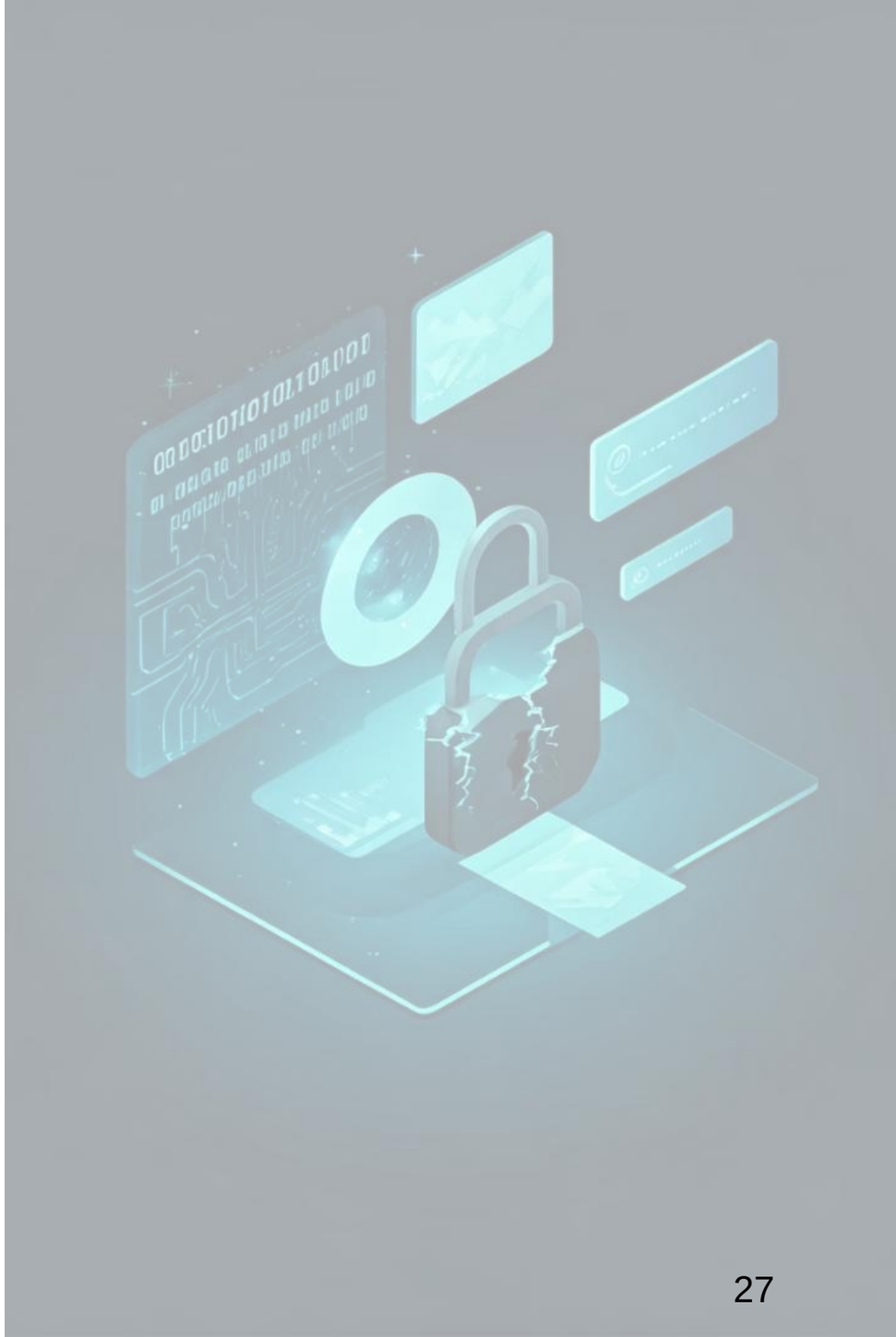
- 經訪查係前員工夏〇，於在職期間115年2月23日未經授權，冒用該公司其他員工帳號登入嘉明湖步道申請系統，並擅自攜出該公司內部行政機密資料，公司於115年4月28日進行勞資調解期間，夏〇公然釋出多項未經許可、擅自攜出之公司內部敏感性文件，已違反該公司資訊安全管理規範、員工保密切結及營業秘密。**此次查核確認為員工使用者帳號遭冒用及敏感性文件遭攜出，屬制度與管理執行上的程序問題。**

觀光業者B旅行社個資外洩說明-後續可精進之作為

- 定期執行帳號權限清查：
  - 確認同仁所擁有各系統或資料夾之帳號，其角色及權限配置妥適性。
- 密碼原則設定：
  - 針對有使用之系統，宜請同仁定期變更密碼，並強化密碼設定長度、複雜度等安全性原則。
- 資料分類分級：
  - 建議針對資料進行分類分級，並採取相對應存取控制，針對敏感性資料之存取，建議保有授權存取、紀錄之留存。
- 設備安全性更新：
  - 建議針對防火牆定期更新，並保留相關更新紀錄。

近期事件分享

蒐集4-6月國內外備受關注的重大個資外洩事件。



C股份有限公司個資外洩事件

事件時間

2026年4月偵測到資訊系統異常。

影響範圍

臺灣客戶會員、公司員工

外洩資料

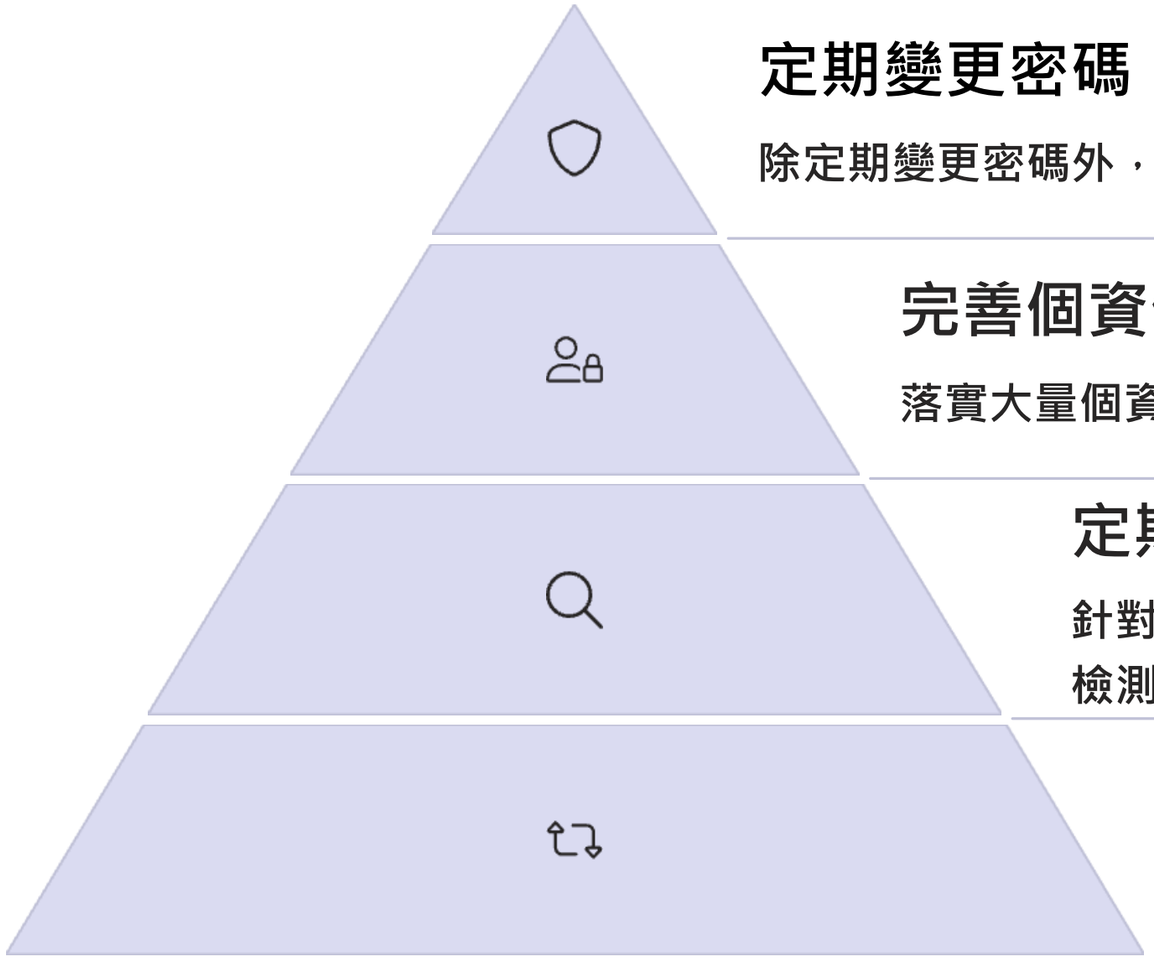
姓名、電子郵件地址等會員資料、部分員工的護照資訊與財務資訊。

社會影響

尚未公開受影響的具體人數。

參考連結： https://www.ithome.com.tw/news/176271

針對4-6月資料外洩事件之資安防護建議



定期變更密碼

除定期變更密碼外，也應注意密碼設定之強度及複雜度。

完善個資保護

落實大量個資資料庫加密與欄位層級加密與雜湊、對備份與日誌採存取控制及

定期執行技術性檢測及漏洞修補

針對存放個資之伺服器、系統等，定期執行弱點掃描、滲透測試等技術
檢測結果進行漏洞修補。

備援、勒索防範與營運持續

規劃離線或不可變備份(immutable backup)-無法在預設保留期
副本，並定期演練還原，確保在伺服器與工作站大規模加密時仍