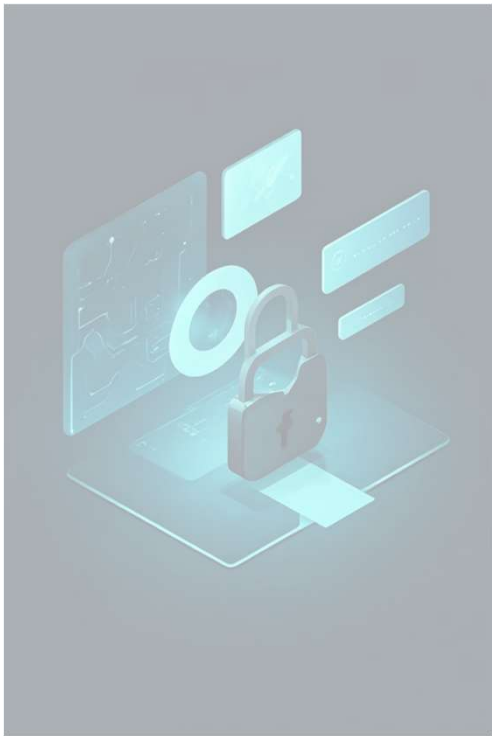
# 觀光署
# 114年度行政檢查計畫資安顧問服務案

## 季簡報

## 114年12月

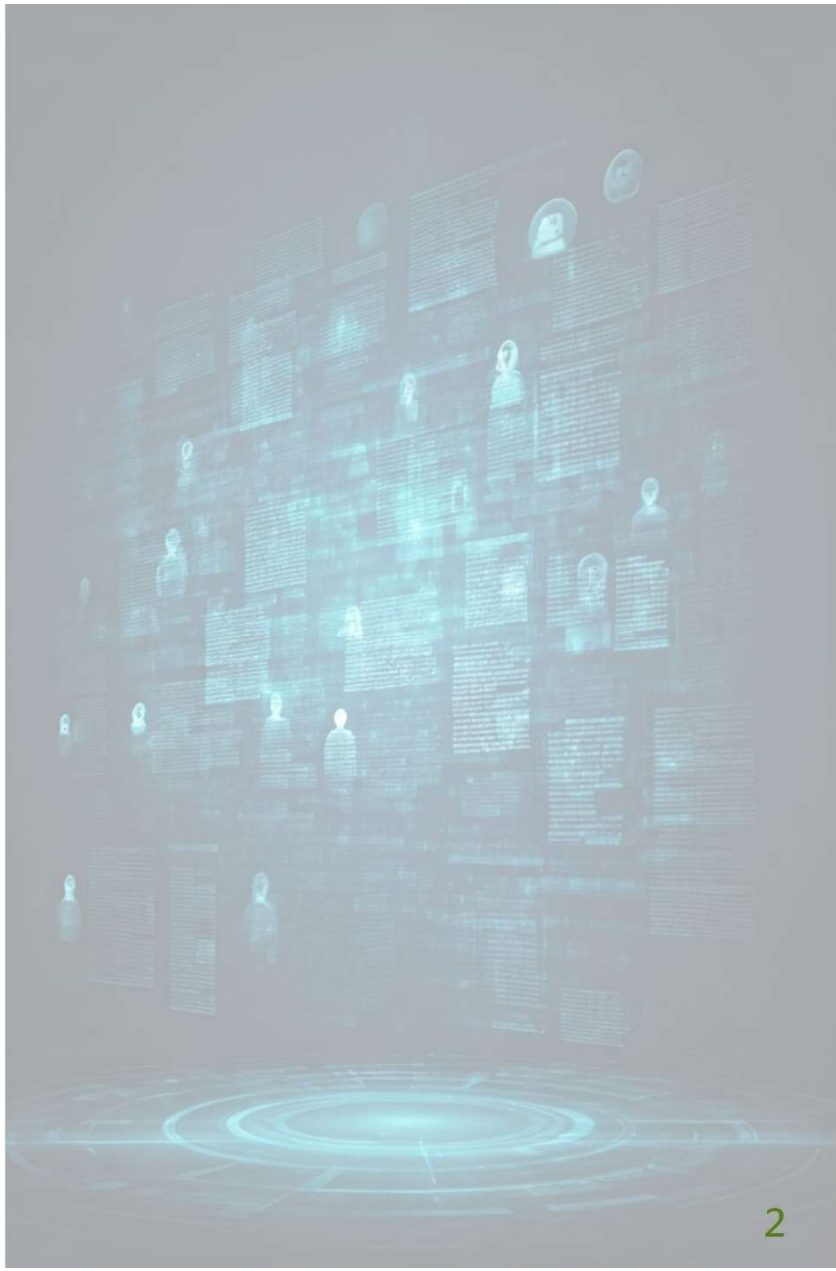


# 目錄

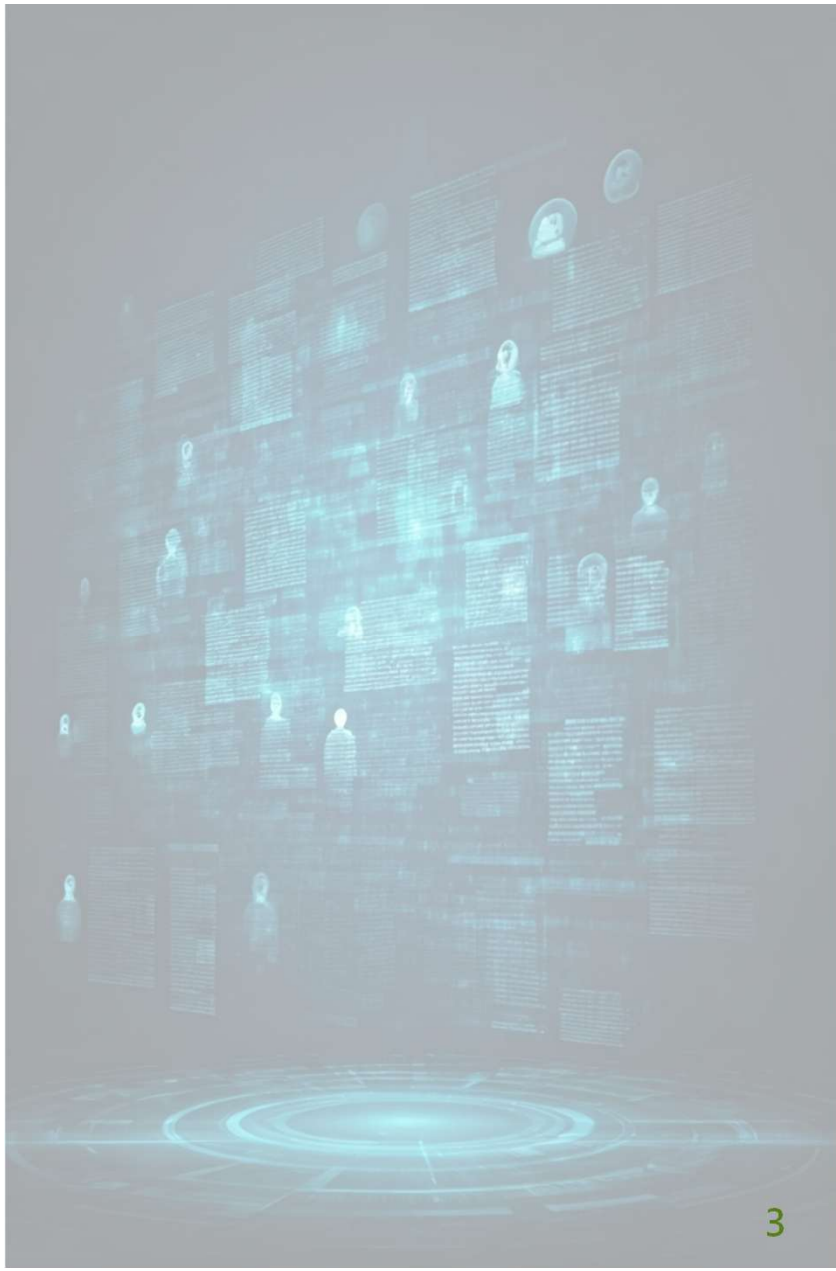
一、共通性問題

二、個案問題分析

-近期事件分享



# 一、共通性問題



# 一、共通性問題

- 已完成稽核業者名稱如下：

| 項次 | 業者名稱 |
|---|---|
| 1 | 巨大旅行社 |
| 2 | 開喜旅行社 |
| 3 | 行健旅行社 |
| 4 | 信安旅行社 |
| 5 | 吉航旅行社 |
| 6 | 加利利旅行社 |
| 7 | 清晨旅行社 |
| 8 | 友泰國際旅行社 |
| 9 | 雙向國際旅行社 |
| 10 | 找到了旅行社 |
| 11 | 高雄福華大飯店 |
| 12 | 兄弟大飯店 |
| 13 | 永業旅行社 |
| 14 | 遠雄悅來大飯店 |
| 15 | 美侖大飯店 |
| 16 | 鴻毅旅行社 |
| 17 | 耐斯王子大飯店 |
| 18 | 天海旅行社 |

| 項次 | 業者名稱 |
|---|---|
| 19 | 國聯大飯店 |
| 20 | 亞都麗緻大飯店 |
| 21 | 旅遊家旅行社 |
| 22 | 永信旅行社 |
| 23 | 新竹喜來登大飯店(西館) |
| 24 | 豐邑喜來登大飯店(東館) |
| 25 | 和逸飯店桃園青埔館 |
| 26 | 礁溪老爺酒店 |
| 27 | 蘭城晶英酒店 |
| 28 | 大眾旅行社 |
| 29 | 名人堂花園大飯店 |
| 30 | 馬雅花台灣旅行社 |
| 31 | 美麗信花園酒店 |
| 32 | 名生旅行社 |
| 33 | 世邦旅行社 |
| 34 | 鼎運旅行社 |

| 項次 | 業者名稱 |
|---|---|
| 35 | 洋明旅行社 |
| 36 | 何時旅行社 |
| 37 | 樺一旅行社 |
| 38 | 金環球旅行社 |
| 39 | 亞柏國際旅行社 |
| 40 | 名冠旅行社 |
| 41 | 永利旅行社 |
| 42 | 義大世界 |
| 43 | 麗寶樂園 |
| 44 | 雲仙樂園 |
| 45 | 遠雄海洋公園 |
| 46 | 怡園渡假村 |
| 47 | 東勢林場遊樂區 |
| 48 | 杉林溪森林生態渡假園區 |
| 49 | 九九峰動物樂園 |
| 50 | 九族文化村 |

| 項次 | 業者名稱 |
|---|---|
| 51 | 綠舞莊園日式主題遊樂區 |
| 52 | 珂境旅行社 |
| 53 | 汎佳旅行社 |
| 54 | 百威旅行社 |
| 55 | 尊榮國際旅行社 |
| 56 | 飛行家旅行社 |
| 57 | 高豐旅行社 |
| 58 | 迎家國際旅行社 |
| 59 | 愛玩樂旅行社 |
| 60 | 小叮噹科學主題樂園 |
| 61 | 六福村主題遊樂園 |
| 62 | 柳營尖山埤渡假村 |
| 63 | 頑皮世界 |
| 64 | 劍湖山世界 |
| 65 | 小人國主題樂園 |
| 66 | 野柳海洋世界 |
| 67 | 尚順育樂世界 |

# 一、共通性問題

- 已完成本案共67家業者稽核，應稽核家數共67家業者。
- 針對超過33家業者(比率超過約50%)應改善之題項，納入後續共通性問題進行改善建議說明。

# 一、共通性問題

- 查核家數67家，共42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？ |

- 業者應製作「 個人資料檔案清冊」及個人資料作業流程說明文件，並經公司內部權責主管核定(核定紀錄也要留存)，其個人資料之範圍界定之作法建議寫在「安全維護計畫」中。(詳細作法可參考經濟部「個資作業手冊」https://www.moea.gov.tw/mns/colr/content/SubMenu.aspx?menu_id=7783)。

註：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。

# 一、共通性問題

- 查核家數67家，共52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？ |

- 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。(詳細作法可參考經濟部「個資作業手冊」https://www.moea.gov.tw/mns/colr/content/SubMenu.aspx?menu_id=7783)


註：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。

# 一、共通性問題

- 查核家數67家，共34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 | 5.4是否就個資事件之重大事故定義，及重大事故之通報流程為何？ |

- 業者應規劃**個資事故應變機制**，機制中包含個資事件之重大事故定義，及重大事故之通報流程。
- 業者可參考行政院及所屬各機關落實個人資料保護聯繫作業要點(113/5/15)
  - 本要點所定重大矚目之個資外洩案件，其範圍如下：
    - (一) 本院、立法院或監察院關注之個資外洩案件。
    - (二) 經媒體顯著披露之個資外洩案件，例如經平面媒體全國性版面報導、電子媒體專題討論。

# 一、共通性問題

- 查核家數67家，共37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**。

註：依據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(§15)訂定。

# 一、共通性問題

- 查核家數67家，共35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？ |

- 業者應保留對所屬人員之**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
  - 各項個人資料保護相關作業程序。


註：依據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(§17)訂定。

# 一、共通性問題

- 查核家數67家，共52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？ |

- 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**，業者應提供最近一次之評估報告。

註：依據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(§18)訂定。

# 一、共通性問題

- 查核家數67家，共42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**。


註：依據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(§18)訂定。

# 一、共通性問題

- 查核家數67家，共37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？ |

- 業者於「個人資料檔案清冊」盤點資料若有進行刪除、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」，可參考下頁範本。

註：依據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(§19)訂定。

# 一、共通性問題

- 查核家數67家，共37間須進行改善。

## 紀錄應包含之關鍵要素

範本

| 要素 | 說明 | 範例 |
| --- | --- | --- |
| **銷毀/停止原因** | 說明為何進行此操作。 | 蒐集目的已達成、契約屆滿、當事人要求行使刪除權。 |
| **銷毀/處理方法** | 物理銷毀或數位刪除的具體技術。 | 碎紙機（縱橫碎）、低階格式化、數位抹除、實體硬碟鑽孔。 |
| **執行時間** | 精確到日期與小時。 | 2026年1月19日 14:30。 |
| **執行地點** | 實體地點或系統路徑。 | 台北總部3樓檔案室、雲端資料庫（AWS S3 特定 Bucket）。 |
| **執行人與監驗人** | 確認操作的責任歸屬。 | 資訊部陳專員執行，資安官林經理監驗。 |

# 一、共通性問題

- 查核家數67家，共36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？ |

- 應檢附相關個人資料安全維護議題會議記錄。

註：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。

# 一、共通性問題

- 查核家數67家，共33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？ |

- 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。

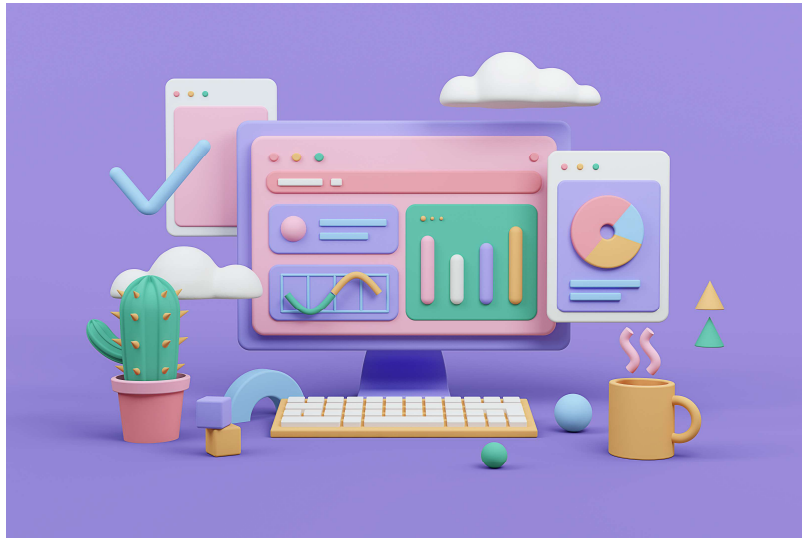
註：依據個人資料保護法施行細則第8條&交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第21條。

# 一、共通性問題

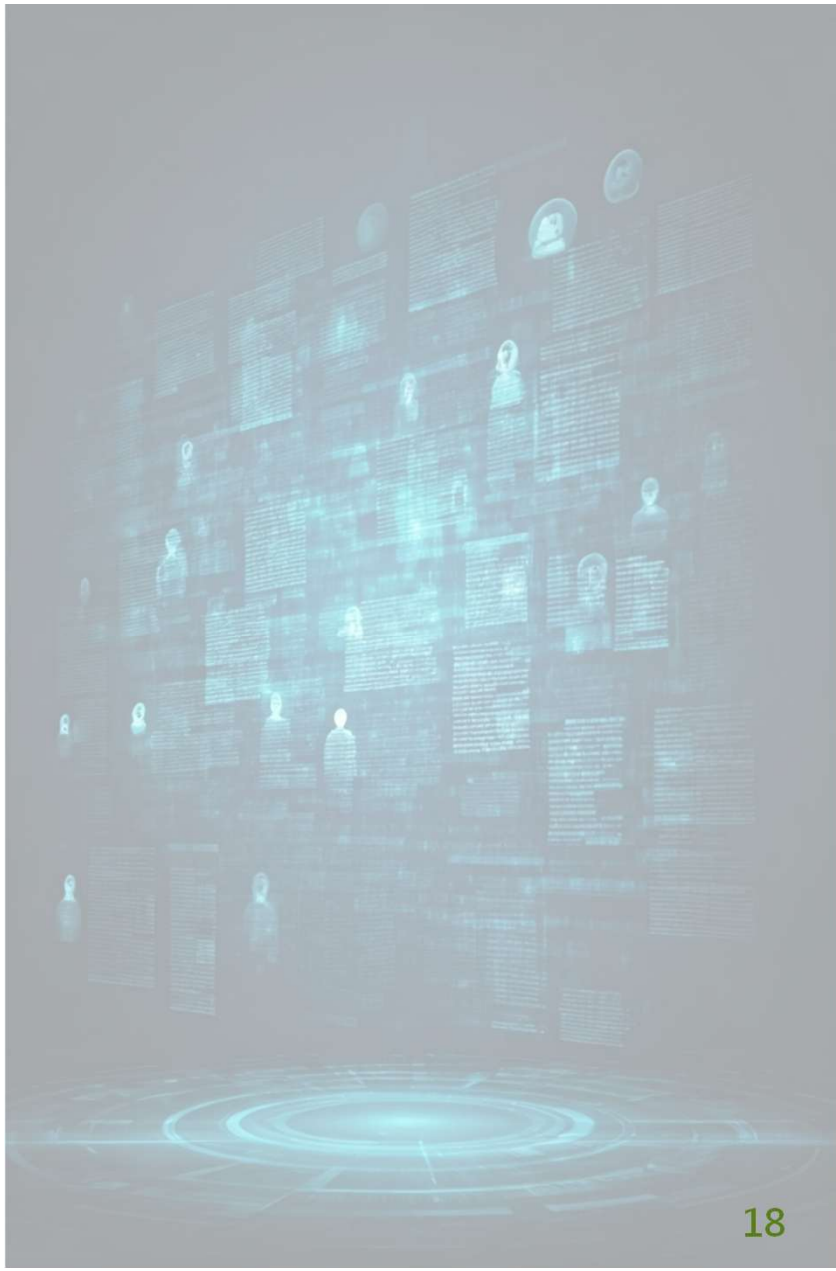
- 查核家數67家，共53間須進行改善。

| 查核項目 | 查核內容 |
| --- | --- |
| 18.其他 | 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？ |

- 應確認是否完成**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
## -近期事件分享



# 近期事件分享

本季業者未有發生個資外洩。
蒐集9-12月國內外備受關注的重大個資外洩事件，

# A公司
# 9月的網路攻擊事件
# 造成顧客、員工近200萬人個資外洩

針對事故發生的經過，A公司在9月29日早上7:00發現系統中斷、檔案被加密，11:00資安團隊切斷網路以隔離資料中心，避免災害擴大。調查發現，攻擊者是經由集團某臺網路設備，駭入資料中心，並同時植入勒索軟體，加密了多臺使用中的伺服器和數臺工作站電腦上的資料。因此，該公司推測，儲存在伺服器和工作站電腦的個資可能外洩。目前駭客尚未公開這批資料。

可能被洩露資訊的包括客戶、該公司聯絡過的外部人士、員工（包括退休員工）及其家屬。其中客戶是指曾聯絡過A公司，以及公司客服中心的顧客，外部人士則是A公司曾以Telegram訊息賀或慰問的人士，總人數約167萬。員工及員工家屬受影響人數約27萬。外洩的資料類型包括姓名、地址、電話，以及電子郵件信箱，有的還包括性別及出生日期。該公司強調，外洩資料未包含信用卡資訊。

# B媒體與D集團通報遭Oracle EBS零時差攻擊 個資外洩近萬人受害

B媒體與D集團向多州主管機關通報，旗下使用的企業資源規畫系統Oracle E-Business Suite（Oracle EBS）遭零時差弱點攻擊。駭客在2025年8月9日至14日期間利用尚未修補的弱點入侵後端系統，竊取儲存在其中的個人資料。D集團向緬因州檢察長辦公室通報的資料顯示，本次事件共影響9,479名個人，其中包含4名緬因州居民。

依D集團向主管機關與受影響對象的說明，公司在9月29日發現Oracle EBS環境出現異常活動，隨後在外部資安團隊協助下展開調查，並於10月31日完成調查，確認未授權第三方曾在8月中旬存取系統並複製含有個人資料的檔案，之後依各州規定完成通報。

# E公司旗下IT供應商系統遭駭
# 車主個資被竊

E公司旗下IT供應商日前公告，
今年稍早內部系統遭駭，影響車主駕照及社會安全碼等個資。

經過調查，判斷駭客活動期間為今年2月22日到3月2日。至於受影響的資料，在緬因州提報的資料說明包括個人名字和社會安全碼。而在提交的官方報告中，透露外洩資料除了全名和社會安全碼外，還包含駕照資料。

# G協會遭網攻外洩會員資料

G協會近日公告內部會員管理軟體遭到網路攻擊，致使為數不詳的會員姓名、電子郵件等資料外洩。

G協會透過官網的聲明指出，其用於各俱樂部行政管理、特別是會員（被授權者）登記管理的軟體遭到「網路惡意行為及資料竊取」。

# 9-12月發生之個資外洩事件預防建議

| 身分與存取管理 | 網路與系統防護 | 監控、偵測與事故通報 | 資料面控管與加密 |
|---|---|---|---|
| •對內部帳號（含離職員工、約聘與外包）強制採用多因子驗證，並將高權限帳號與一般作業帳號分離，避免像部分事件中被利用身分驗證弱點即可批次存取數千萬筆紀錄。<br>•建立「最低必要權限」與定期權限審查流程，尤其是能接觸大量個資的系統與資料庫，並對跨國 / 跨實體公司之管理帳號做嚴格控管與稽核紀錄。 | •分段與隔離關鍵系統與備援環境，重要伺服器與資料庫不得與辦公區同網域，萬一如朝日酒廠案般有多台工作站遭植入勒索程式時，能限制橫向移動範圍。<br>•強化端點防護與弱點管理，例行修補 VPN、邊界設備與伺服器漏洞，搭配**端點偵測與回應(EDR)與延伸偵測與回應(XDR)**[註]偵測異常加密、檔案大量存取或外連行為，降低勒索與外洩成功率。 | •設定對「大量查詢或匯出客戶與員工資料」「非工作時間或異常地理位置登入」「單帳號短時間內遍歷多系統」等情境的即時告警，縮短未授權存取被發現的時間。<br>•建立明確的資安事件分級與通報流程，事前擬好對主管機關與客戶溝通的標準內容，避免像多起事件一樣，攻擊自數月前發生，卻延遲許久才對外說明，引發信任危機與罰則風險。 | •針對大量個資資料庫，實施欄位層級加密與雜湊，並將明文資料與金鑰分離保存，就算遭到未授權存取也降低直接濫用風險。<br>•對備份與日誌同樣視為「含個資資產」管理，採用存取控制與加密，避免攻擊者在入侵後透過備份或集中日誌伺服器批量取得個資。 |

**註：**
EDR (端點偵測與回應) 著重於保護「端點」（如電腦、伺服器）
XDR (延伸偵測與回應) 則更全面，它會整合來自多個來源（如端點、網路、雲端、電子郵件）的數據進行關聯分析，提供更廣闊的視角來偵測和回應威脅。

# 9-12月發生之個資外洩事件預防建議

| 備援、勒索防範與營運持續 | 員工與外部利害關係人管理 | 治理與法遵 |
| --- | --- | --- |
| •規劃離線或不可變備份（immutable backup）-無法在預設保留期限內被修改、加密或刪除的資料副本，並定期演練還原，確保在伺服器與工作站大規模加密時仍可快速恢復關鍵服務，減少被迫支付贖金或以「資料外洩」作為談判籌碼。<br>•在供應鏈與關係企業間簽訂資訊安全與個資條款，將備援、通報與配合調查義務寫入，避免母公司或海外據點發生外洩時，子公司（如台灣分公司）資訊落後或難以掌握影響範圍。 | •對員工與外包定期進行社交工程、釣魚郵件演練與教育，特別是有權操作客戶資料、維運伺服器或管理雲端帳號的人員，以降低內鬼與被釣魚的風險。<br>•對客戶與員工建立「事故後」的標準通知模板，例如提醒警惕詐騙電話、釣魚簡訊與假冒客服要求補資料等，這在實際外洩事件後，可大幅降低二次被害情形。 | •依據 ISO 27001 / 27701 或當地個資法，將「跨境資料流通」「委外處理」「高風險系統變更」納入正式風險評估與控管，明確界定責任歸屬與通報時點，以避免事件發生後才互踢皮球。<br>•定期進行第三方滲透測試與紅隊演練，檢驗身分驗證、網路隔離與日誌監控等機制是否足以偵測與阻擋實務中的攻擊手法，並將發現納入年度改善計畫。 |