

交通部指定觀光產業類 手把手個資保護實作教學

李怡親 高級法律研究員

財團法人資訊工業策進會 科技法律研究所

2024

tpipas@iii.org.tw
ichinlee@iii.org.tw



Institute for Information Industry



stli

科技法律研究所
SCIENCE & TECHNOLOGY
LAW INSTITUTE



大綱

簡報 大綱

01

觀光產業個人資料檔案
安全維護自主檢查表

02

旅宿業個人資料檔案
安全維護計畫



01

觀光產業個人資料檔案 安全維護自主檢查表



修法重點、加重未採安全措施之處罰

加重未有適當安全措施處罰，取消需先限改規定

個資法第48條新增第2項、第3項規定

違反項目	舊法	新法	差異
違反告知義務、當事人權利行使、行銷規定 48條1項	先限期改正， 未改正2-20萬	先限期改正， 未改正2-20萬	不變
未採適當安全措施、 未依安維辦法辦理 新增48條第2、3項	先限期改正， 未改正2-20萬	● 2-200萬、再限改 未改正15-1500萬 ● 情節重大： 15-1500萬、再限改	罰則提高 無需先限改
代表權人兩罰規定 50條	除盡防止義務外， 受同一處分	除盡防止義務外， 受同一處分	罰則 實質提高

按行政罰法第19條，僅法定罰鍰最高3,000元以下者，方得以其情節輕微免予處罰。若主管機關認定非公務機關違反個資法第27條規定，未採取適當安全措施，則主管機關仍須依法處份。



修法重點、加強行政檢查力道

落實**執法**，加重**行政檢查**力道，



- 1) 個資外洩情形：個資類別、人數、影響程度、故意或重大過失
- 2) 安全維護措施落實情形：有無落實個資安維辦法規定、累犯
- 3) 知悉個資外洩後採行措施：有無採取降低損害行為、通報、通知、配合行政檢查
- 4) 其他：未遵循主管機關處分、因個資外洩獲益

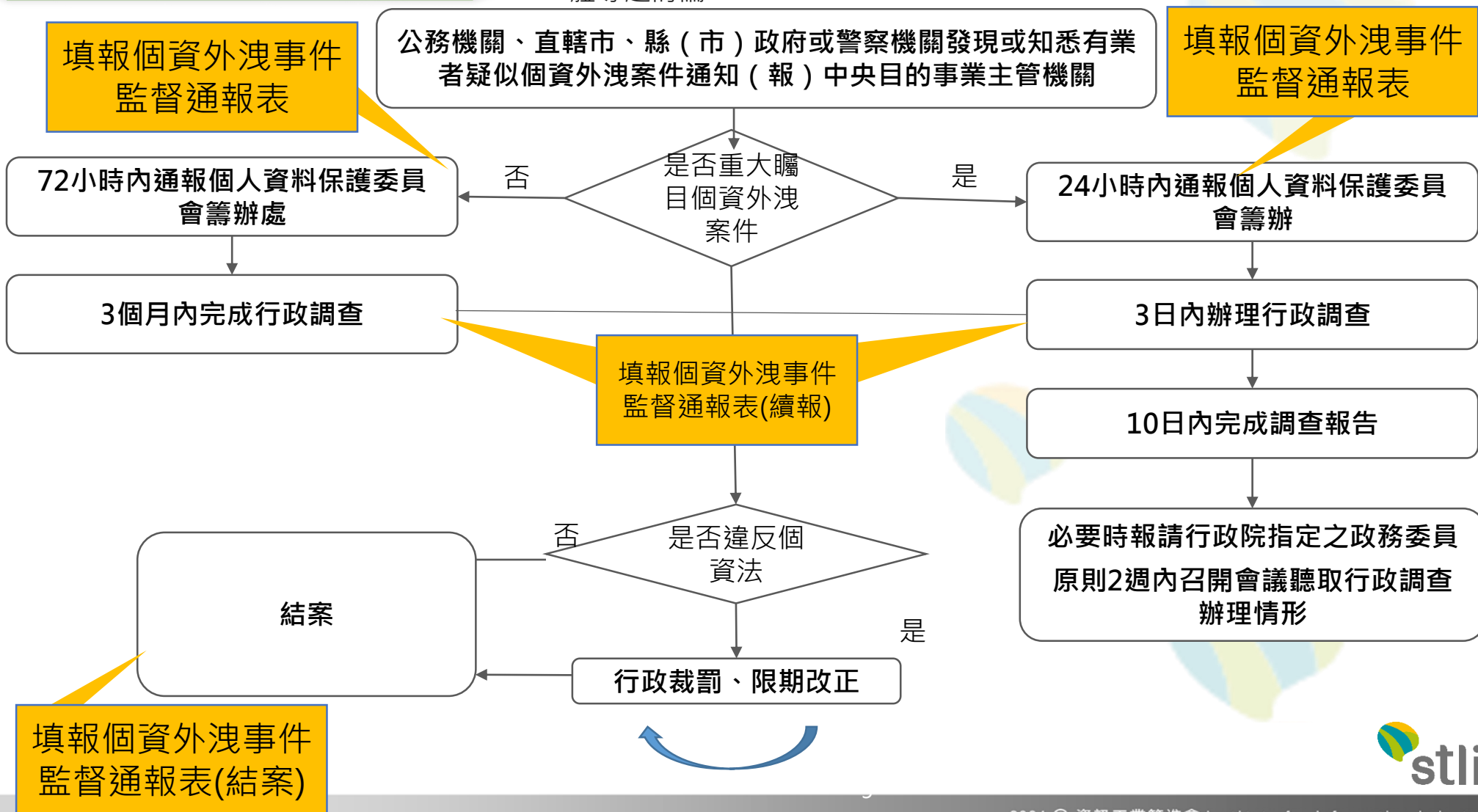


個資外洩案件之行政調查流程

依「行政院及所屬各機關落實個人資料保護聯繫作業要點」第2點第2項

行政院及所屬各機關落實個人資料保護聯繫作業要點

1. 行政院、立法院或監察院關注之個資外洩案件。
2. 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。





各部會裁罰案件統計

廠商名稱	主管機關	罰鍰 (萬)	裁罰可考量因素	備註
汽車租賃業者	交通部公路局	20	重大矚目 + 40萬筆用戶 + 未訂定安維計畫	舊法
民用航空運輸業者	交通部民航局	20	重大矚目 + 8,000筆會員 + 資料庫控管未落實	舊法
線上書城	數位部數產署	5+5	重大矚目 + 警政署通報多次+民眾接到詐騙電話 + 資料庫控管未落實	舊法
新加坡電商	數位部數產署	10+10	重大矚目 + 警政署通報多次+市佔率高、影響大 + 民眾有實際財損 + 個資盤點等多項安維措施未落實	舊法
OO百貨	經濟部商業署	20+20	重大矚目 + 90萬筆用戶個資 + 個資盤點等多項安維措施未落實	舊法
瓦斯業者	經濟部能源署	15	民眾有實際財損	
旅行社	交通部觀光署	200	重大矚目 + 民眾有實際財損 + 曾有前案	
A健身房業者	教育部體育署	140+140	重大矚目 + 警政署多次通報+民眾有實際財損	§12:20W §27:120W
B健身房業者	教育部體育署	140+140	重大矚目 + 警政署多次通報+民眾有實際財損	§12:20W §27:120W
OO數位	數位部數產署	限期改善	OO百貨之資服業 + 未落實安維措施	舊法
有線電視	數位部數產署	2+2	A健身房之資服業 + 未落實安維措施	
資訊公司	數位部數產署	2+2	高中學習歷程資服業 (8間外洩) + 未落實安維措施	
日韓商品電商	數位部數產署	2+2	警政署多次通報+民眾有實際財損 + 未落實安維措施	
網路機能服飾	數位部數產署	4+4	警政署多次通報+民眾有實際財損 + 未落實安維措施	



裁罰案例

■ 2023年 5 月數位發展部裁罰案例

A 電商平台

經數位部多次要求業者完善個人資料保護，並提出相關佐證資料以為證明，該業者在個資盤點上仍僅提供4筆盤點內容，顯有缺漏，且在風險評估分析上，對於風險值較高之流程未提供已採取矯正措施之佐證。另外，對委外廠商未落實稽核，未能提供完整的安全管控執行、稽核紀錄等具體佐證資料，無法證實業者對保有個資已採行適當之安全措施，因此依據個資法第48條第4款併第50條規定，處分業者併同其負責人罰鍰計新台幣20萬元。

B 網路書局

經數位部產業署實地行政檢查，現場已發現在帳號管理上執行未確實，另要求事後提供之補充或佐證資料，業者個資盤點資料仍不完整，且針對委外廠商監督管理未落實執行，因此依據個資法第48條第4款併第50條規定處分，業者併同其負責人罰鍰計新台幣10萬元。

■ 2023年 5 月經濟部裁罰案例

C 百貨業

經濟部辦理行政調查，經審業者函復改善情形及佐證資料，系爭個資外洩事故仍有未確實通知當事人、未明確揭示蒐集個資主體(包括本公司及其關係企業)、未採行適當個資安全維護措施(無留存自行檢查、內部稽核、銷毀等紀錄)等。因此依據個資法第48條及第50條規定處分，業者與其代表人各裁罰新台幣20萬元罰鍰。





「交通部指定觀光產業類個人資料檔案安全維護計畫及處理辦法」之規定

觀光產業個人資料檔案安全維護自主檢查表

公司名稱： ☐ 有限公司 ☐ 股份有限公司				
經營業別： <u>旅行業/觀光遊樂業/觀光旅館業/旅館業/民宿</u> (請自行圈選)				
保有個人資料筆數： <u> </u> 筆		查核日期： <u> </u> 年 <u> </u> 月 <u> </u> 日		
是否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	訂定「消費者個人資料檔案安全維護計畫」	☐ 是 ☐ 否		按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條訂定安全維護計畫。
2. 配置管理之人員及相當資源	是否設個人資料管理單位或適當組織？	☐ 是 ☐ 否		請檢附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		請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。
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		請檢附風險評估過程底稿、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	☐ 是 ☐ 否		請說明應變機制對降低、控制事故對當事人造成損害之作法。

- 檢查內容以「交通部指定觀光產業類個人資料檔案安全維護計畫及處理辦法」（下稱辦法）之規定為基準。
- 共有17項查檢項目，合計54個細項應填寫。
- 個資法第27條要求組織應有個資適當安全維護措施，適當安全維護措施內容規定於個資法施行細則第12條2項（共計11款），辦法將各該安全維護計畫所應涵蓋內容展開。
- 根據辦法第6條到第22條，並將組織內部查檢結果對應組織安維計畫第幾頁或第幾點之說明。
- 建議組織應於日常作業中留下各該條文紀錄及證據。



觀光產業個人資料檔案安全維護 自主檢查表（自評表）

公司名稱：

經營業別：

保有個人資料筆數：

是否具對外電子商務服務系統：

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
1	消費者個人資料檔案安全維護計畫	訂定「消費者個人資料檔案安全維護計畫」	是 ☐ 否 ☐	按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條訂定安全維護計畫。



個人資料法施行細則§12 (本辦法§5)

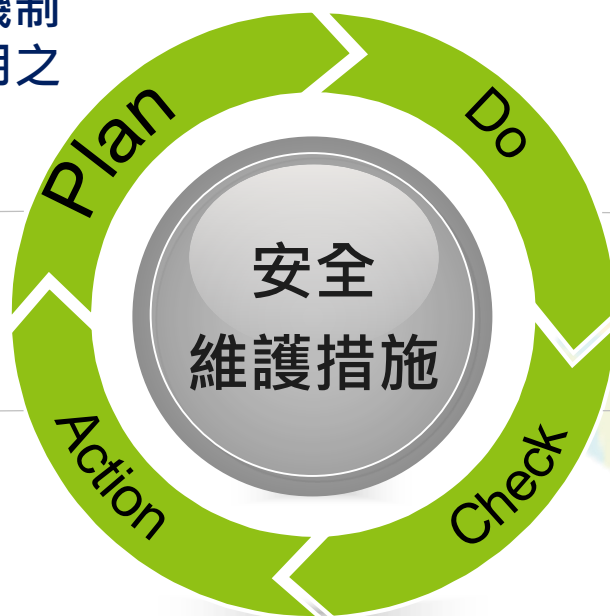
- 適當安全維護措施

Plan規劃

1. 配置管理之人員及相當資源
2. 界定個人資料之範圍
3. 個人資料之風險評估及管理機制
4. 事故之預防、通報及應變機制
5. 個人資料蒐集、處理及利用之內部管理程序

Do實施

6. 資料安全管理及人員管理
7. 認知宣導及教育訓練
8. 設備安全管理



Action行動

11. 個人資料安全維護之整體持續改善

Check檢查

9. 資料安全稽核機制
10. 使用紀錄、軌跡資料及證據保存



適當安全維護措施



配置管理
之人員及
相當資源

個人資料之
風險評估及
管理機制



個人資料蒐集、
處理及利用之
內部管理程序

認知宣導及
教育訓練



資料安全稽核
機制

個人資料安全
維護之整體持
續改善



界定個人資
料之範圍

事故之預防、
通報及應變
機制



資料安全
管理及人
員管理

設備安全管理



使用紀錄、
軌跡資料及
證據保存



配置管理 之人員及 相當資源

配置管理人員及資源

辦法條文

第六條

1. 非公務機關應依其業務規模及特性，衡酌經營資源之合理分配，建立個人資料檔案安全維護管理組織，配置相當人員及資源，負責規劃、訂定、修正與執行本計畫及處理方法等相關事項。
2. 本計畫及處理方法之訂定或修正，應經**非公務機關代表人或經其授權之人員核定**。
3. 個人資料檔案安全維護管理組織，應定期就執行任務情形向**非公務機關代表人或經其授權之人員提出書面報告**。
4. 非公務機關應將訂定之安全維護計畫留存營業所在地備查；主管機關得派員檢查。

對應安維計畫段落範例

(參考旅宿業個人資料檔案安全維護計畫 範本)

配置管理之人員及資源

一. 管理人員：

1. 配置人數：○○人(至少1名)。
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，並向代表人(經營者)或經其授權人員提出報告。

二. 稽核人員/單位：

1. 姓名/單位：○○○。(至少1名)
2. 職責：資料安全稽核機制。
 - 1) 不得與管理人員為同一人。
 - 2) 定期稽核安全維護計畫之執行情形及成效，並將稽核結果，向代表人(經營者)或經其授權人員提出報告。

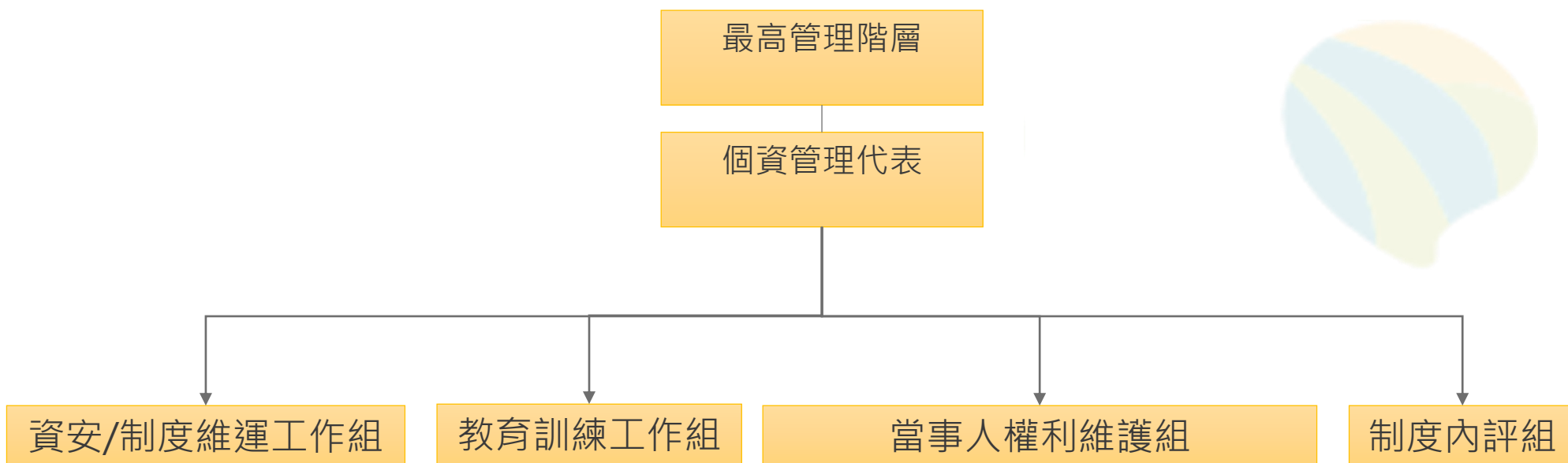
三. 預算：每年新臺幣○萬元。(包含管理人員薪資、設備費用等，依實際狀況填寫)

可提供證據參考

- 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。



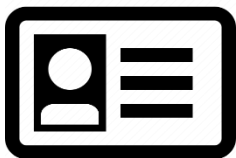
常見個資小組維運架構參考



編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
2	配置管理之人員及相當資源	是否設個人資料管理單位或適當組織？	是 ☐ 否 ☐	請檢附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



界定個人資料之範圍



界定個人資料之範圍

辦法條文

第七條
非公務機關應依個人資料保護相關法令，定期查核確認所保有之個人資料現況，界定其納入本計畫及處理方法之範圍。

對應安維計畫段落範例

蒐集、處理及利用個人資料之範圍及特定目的

- 一. 特定目的：(觀光旅館業/旅館業/民宿)管理業務、契約、類似契約或其他法律關係事務、消費者、客戶管理與服務等運用、人事管理等運用(類別：識別類、社會情況類)。
- 二. 個人資料：自然人(包含旅客、消費者、從業人員等)之姓名、出生年月日、國民身分證統一編號、護照號碼、信用卡卡號、聯絡方式及其他得以直接或間接方式識別該個人之資料。
- 三. 指定管理人員每○○日(或週、月、季、年)定期清查本公司(或民宿)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。

可提供證據參考

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。盤點表內容建議：

- 作業流程：流程步驟、行為模式(蒐集、處理、利用)
- 個資檔案名稱及類型
- 蒐集、處理、利用之特定目的
- 資料來源：內部或外部、直接、間接蒐集
- 蒐集(告知及蒐集方式)、處理(保存方式與年限暨刪除銷毀方式)、利用(傳遞對象、目的與方式)
- 委託機關(如有委託情形)

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
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 ☐	• 請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。



個人資料的定義

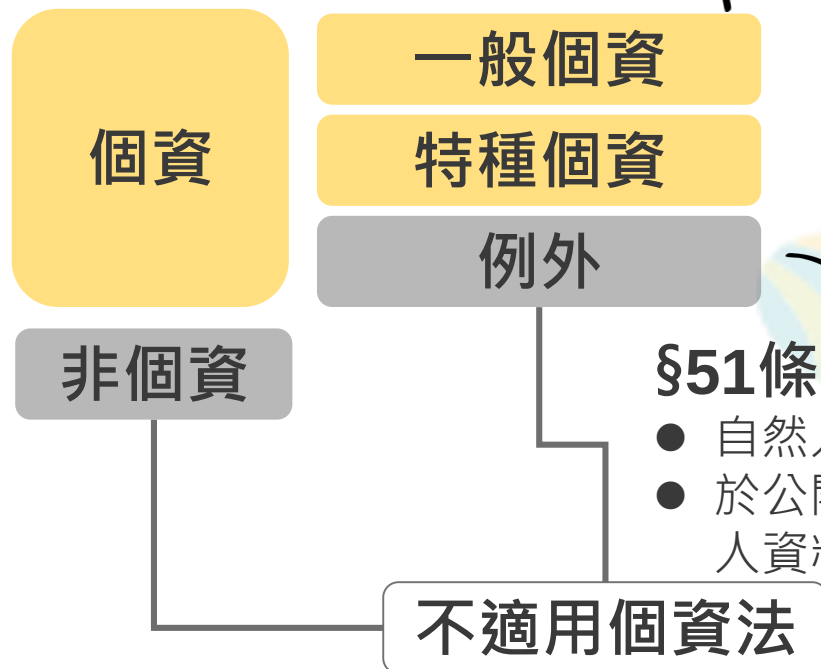
亡者資料？

§2條

自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料

§6條

有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，原則上不得蒐集、處理或利用。



§51條

- 自然人 + 單純個人或家庭活動之目的
- 於公開場所或公開活動 + 未與其他個人資料結合+影音資料。



案例解析



鄭家純 ✓

2021年5月9日 · 🌐

我猜想她現在的氣場
會是這色吧

#965326 Hex Color Code



The hexadecimal color code #965326 is a medium dark shade of orange. In the RGB color model #965326 is comprised of 58.82%

red, 32.55% green and 14.9% blue. In the HSL color space #965326 has a hue of 24° (degrees), 60% saturation and 37% lightness. This color has an approximate wavelength of 589.8 nm.

110.11.12檢方調查認為，雞排妹雖指控陳沂公布她的手機號碼，但：

1. 雞排妹自稱有2支電話，且被公布的電話無法收簡訊或接電話；
 2. 雞排妹也在臉書公開自己號碼，還表示歡迎大家去誠品消費可以報她的號碼享購物折扣；
- 檢察官因此認定，雞排妹並沒有因陳沂公布其手機號碼而受有任何損害，陳沂違反《個資法》罪嫌不足，因而將她不起訴。

雞排妹與陳沂直播時唸出陳沂手機前四碼，即時被當事人阻止，然而，雞排妹下線後，透過社群媒體以色碼暗示陳沂手機後六碼：

112.4.11台北地方法院判決4月有期徒刑，得易科罰金。一審依個資法判刑4月，二審改判3月，得易科罰金。

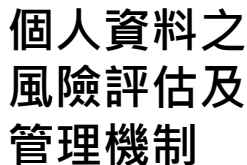
113.3.21最高法院駁回上訴定讞。



客訴管理流程個資盤點表範例

檔案編號	作業流程名稱	個資行為態樣 (可複選) 1.蒐集 2.處理 3.利用 4.國際傳輸	個人資料			直接蒐集			間接蒐集			告知義務		委託或受託		保管儲存與刪除銷燬				數量 (概數)
			檔案名稱	種類及類別	類型 1.紙本 2.電子檔 3.資料庫 4.其他	方式	特定目的	法定情形	來源	特定目的	法定情形	告知與否	免告知法定事由	有無	委託者或受託者	資料載體	儲存場所	保存期限 1.法定 2.自訂 3.其他	刪除銷燬	
1	客訴管理	蒐集處理	客服表單	姓名、電話、電子郵件、住址	電子檔資料庫	網頁蒐集	客訴管理	契約				網頁告知		無		電子檔	資料庫	兩年刪除	期限後刪除銷毀	500
2	客訴管理	蒐集處理	客服錄音檔	姓名、電話、電子郵件	電子檔資料庫	語音蒐集	客訴管理	契約				語音告知		無		電子檔	資料庫	兩年刪除	期限後刪除銷毀	400





可提供證據參考

風險評估過程底稿、風險評鑑報告及風險處理計畫。評鑑表內容建議

1. 經由本公司（或民宿）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. 旅宿業間互為傳輸時之外洩（包括分公司間傳輸、與相關業者間傳輸等）。

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. 電子資料檔案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。

- 應可產生可重複之一致、有效、可比較的方法論
- 組織應得透過開方法論分辨出資產價值，以便採取適當的避險措施

[illegible]



風險評估過程底稿及方法論

表一、xxx飯店個資價值評價表

個資價值評價			
個資來源	廠商	員工	民眾/客戶
個資敏感度	低	中	高
一般個資	低 1	2	3
財務細節	中 2	4	6
特種個資	高 3	6	9

表三、xxx飯店個資風險總評值

個資風險評鑑							
個資價值評價							
率 威 或 可 能 性	評值	低		中		高	
	低	1	2	3	4	6	9
	中	3	6	9	12	18	27
	高	5	10	15	20	30	45

表二、xxx飯店個資弱點與威脅評估標準

個資弱點與威脅	
高 5	違反個資法及相關法令，或合約要求 無相對應管理程序規制，或個資檔案無專人控管
	無安全管控措施，如紙本彌封、專人傳遞、檔案櫃上鎖，或資料加密、防火牆、防毒軟體、權限控管、滲透測試等
中 3	違反組織內部規範 有相應管理措施，但無有效執行，或無保留相關紀錄
	有安全管控措施，但偶有未確實執行
低 1	符合個資法、相關規範、合約要求及組織內部規範等 有相對應管理程序規制，且確實落實執行並保留紀錄
	有安全管控措施，且措施皆正常運作，且有保留紀錄



風險評鑑表範例

檔案名稱

風險管理措施

內部稽核狀況

客訴意見表單

放置於上鎖的資料櫃，鑰匙由該部門主管保管。若有需要調閱須經申請。

目前未查獲任何不符合事項，且都留有調閱資料文件相關完整紀錄。

客服錄音檔

電子檔存放於電腦主機機房，機房有門禁管制。機房進出皆需要有紀錄，若要調閱語音檔，須向部門主管申請。

經過稽核仍偶有未落實的情形產生，每年約為六到七件。

實例題作答區

作業流程		個人資料檔案			個資來源 (請擇一勾選)			個人資料類別 (請擇一勾選)			(查表一、填分數) 價值評值	個資弱點與 威脅評估 (查表二、擇一勾選)			(查表三、填分數) 個資風險總評值	是否評價為中風險以上	(簡答，僅高風險須填寫) 因應中、高風險之管理措施
作業流程 名稱	個資行為 模式 (可複選)	資料檔案名稱	資料檔案 型態	個人資料 之類別	廠商	員工	民眾/客	一般 資	財務 細	特種 資		低	中	高			
作業流程 名稱	1. 對外蒐集 2. 處理 3. 利用 4. 委託行為	個人資料 檔案名稱	1. 紙本 2. 電子檔 3. 作業系統資料 庫		低	中	高	低	中	高		低	中	高			
客訴處理	[蒐集]	客訴意見表單	[紙本]	中英文姓名、身分代碼、帳號、電話、email、通訊住址	[]	[]	[V]	[V]	[]	[]	[3]	[V]	[]	[]	[3]	[否]	N.A.
	[蒐集]	客服錄音檔	[電子檔]	中英文姓名、身分代碼、帳號、電話、email、通訊住址	[]	[]	[V]	[V]	[]	[]	[3]	[]	[V]	[]	[9]	[是]	落實門禁控管、進出須登記及陪同



事故之預防、通報及應變機制

事故之預防、通報及應變機制

辦法條文

第九條

1. 非公務機關為因應消費者個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故，應訂定下列應變、通報及預防機制：
 - 1) 事故發生後應採取之應變措施，包括降低、控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。
 - 2) 事故發生後應受通報之對象及其通報方式。
 - 3) 事故發生後研議其矯正預防措施之機制。
2. 非公務機關遇有消費者個人資料外洩事故，將危及其正常營運或大量當事人權益者，應於**知悉事故後七十二小時內**依附表格式通報其主管機關。如向地方主管機關通報，非公務機關並應副知中央主管機關。
3. 無法於時限內通報或無法於當次提供前項所述事項之全部資訊者，應檢附延遲理由或分階段提供。
4. 主管機關得知或接獲第二項通報後，得依本法第二十二條至第二十五條規定，為適當之監督管理措施。中央主管機關認有必要時，得督導地方主管機關對於非公務機關之相關機制改善情形。

對應安維計畫段落範例

事故之預防、通報及應變機制

(一) 預防：

1. 本公司（或民宿）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（或民宿）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，將危及正常營運或大量當事人權益，應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，並於知悉事故72小時內依附表通報目的事業主管機關(國際觀光旅館及非直轄市一般觀光旅館為交通部觀光署、直轄市一般觀光旅館為直轄市政府、旅館及民宿為各縣市政府)。
2. 對於個人資料遭竊取之當事人，應以適當方式通知使其知悉及本公司（或民宿）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、預防之措施。

可提供證據參考

- 事故應變程序文件書
- 若有發生個資事故，附上通報紀錄表，以及通知消費者之證明
- 附上根因分析或事件分析報告，預防矯正單等



觀光產業個人資料檔案安全維護 自主檢查表

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
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 ☐	請說明應變機制對降低、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 ☐	請說明應變機制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 ☐	請說明應變機制對避免類似事故再次發生之矯正及預防機制。
		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？	是 ☐ 否 ☐	請檢附事故通報文件。



觀光產業個人資料檔案安全維護 自主檢查表

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
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	是 ☐ 否 ☐	請檢附通報記錄。
		16.2是否就個資事件委請公正之第三方進行調查？	是 ☐ 否 ☐	請檢附就個資事件聘請第三方資安廠商就事件調查之報告。
		16.3是否即時且適當的通知當事人？	是 ☐ 否 ☐	請檢附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？	是 ☐ 否 ☐	請檢附事件報告、強化措施的實施情形以及相關內部會議紀錄。



個人資料侵害事故通報及紀錄表

第九條附表

個人資料侵害事故通報與紀錄表		
非公務機關名稱 通報機關	通報時間： 年 月 日 時 分 通報人： 簽名(蓋章) 職稱： 電話： Email： 地址：	
事件發生時間		
事件發生種類	☐ 竊取 ☐ 洩漏 ☐ 竄改 ☐ 毀損 ☐ 滅失 ☐ 其他侵害事故	個資侵害之總筆數(大約) ☐ 一般個資 筆 ☐ 特種個資 筆
發生原因及事件摘要		
損害狀況		
個資外洩可能結果		
擬採取之因應措施		
擬採通知當事人之時間及方式		
是否於發現個資外洩後72小時通報主管機關	☐ 是 ☐ 否，理由	

註1：各欄位資訊若尚未明確，得先填寫「不明」，並俟明確後再通報更新補充。

註2：上開72小時通報主管機關，例假日均納入時效計算。



事故演練計畫

模擬時間	對象/事件	情境敘述	演練重點
10:00 10:05	接獲事件訊息	客服中心通知有1,000筆會員個資遭上網兜售	是否正確判斷個資事故並通報權責單位
10:05 10:10	事故單位查證	部門主管查證，發現遭上網兜售的個資皆為飯店近一年的訂購會員，資訊人員判斷是否系統有異常，或有個資遭外洩之虞	事故單位查證事件發生情況並將細節與狀況通報相關單位協助查證，資訊單位(或系統服務廠商)鑑別是否有資安侵害致資料外洩
10:10 10:30	應變處理回報	各單位訊息回報並研擬後續對策 1.作業影響情況 2.事故損害情況 3.作業延誤情況 4.可能個資外洩管道 5.估算回復正常作業所需時間	確認當事人通知範圍及研擬通知當事人的方式及內容，通知內容至少包含： 1.事故發生之方式 2.已採取之因應措施 3.後續查詢與處理管道
10:45 11:00	對外通報	通報澎湖縣政府並副知交通部 建議同步向警察機關報案留底	主管機關(72hrs) 警察機關報案留存證據
11:00 11:30	事後處理 (書面)	發送email或簡訊給受影響當事人	即時通知當事人
11:30 12:00	檢討會議	判斷根因，預防再次發生	召開演練檢討會議，強化控制措施



個人資料蒐集、處理及利用之內部管理程序



個人資料蒐集、處理及利用之內部管理程序

辦法條文	對應安維計畫段落範例	可提供證據參考
第十條 非公務機關所屬人員為執行業務而蒐集、處理一般個人資料時，應檢視是否符合本法第十九條之要件；利用時，應檢視是否符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合本法第二十條第一項但書情形。	個人資料蒐集、處理及利用之內部管理措施 • 個資蒐集告知聲明（個資法§8、9） • 當事人權利行使方式及管道（個資法§3、10、11、13、14） • 拒絕行銷管道（個資法§20II、III） • 委託他人時的監督義務（個資法施行細則§8II） • 國際傳輸（個資法§21） 蒐集： 1.法定依據：個資法第19條一項各款；若有蒐集特種個資，應確認符合個資法第6條第一項各款之一 2.蒐集方法依：Email、網路平台、電話/現場/口頭、紙本等 3.告知事項：確認是否有踐行告知義務，或符合法定要項可免告知。 處理： 1.法定依據：個資法第19條一項各款 保管方式：個人電腦、儲存於資料庫/主機、存放作業區域個人櫃/抽屜、存放檔案室 2.保存期限依法定或自訂，填寫保存年限。 3.刪除/銷毀方式：說明如何刪除或銷毀，如統一刪除/銷毀、由承辦人自行刪除/銷毀。 4.內部傳送：說明對象單位（通常為內部）及用途。 利用： 1.特定目的外利用之法定依據：原則於蒐集之特定目的內利用各資，若有特定目的外，應確認為個資法第20條一項各款之何款。 2.說明利用對象機構（通常為外部）及用途。 3.資料利用方法依下列代碼進行填寫：Email、網路平台、電話/現場/口頭、傳真、紙本	• 蒐集、處理、利用之程序文件書 • 日常作業相關文件表單



個人資料的蒐集處理或利用要件彙整

非公務機關利用	非公務機關蒐集處理	特種資料
法律明文規定	法律明文規定	法律明文規定
為增進公共利益所必要。		公務機關執行法定職務或非公務機關履行法定義務必要範圍內
為免除當事人之生命、身體、自由或財產上之危險		為協助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
經當事人同意	經當事人同意	經當事人 書面 同意*
有利於當事人權益	對當事人權益無侵害。	當事人自行公開或其他已合法公開之個人資料
	當事人自行公開或其他已合法公開之個人資料	
公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人	學術研究機構基於公共利益為統計或學術研究而有必要	公務機關或學術研究機構基於 醫療、衛生或犯罪預防 之目的，為統計或學術研究而有必要
	與當事人有契約或類似契約關係	已採取適當之安全措施
為防止他人權益之重大危害	為增進公共利益所必要	但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。
	個人資料取自於一般可得之來源	

事前或事後有適當安全維護措施

*但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限



蒐集住宿旅客資料之法令規定整理

- Q：住宿業者可否要求登記、影印旅客的身分證資料嗎？
- A：可以，依據「觀光旅館業管理規則 § 19」、「旅館業管理規則 § 23」以及「民宿管理辦法 § 28」中，均有規定住宿業者必須登記每日住宿旅客資料，且保存期間為六個月之規定。
- 為確保交易及旅客住宿安全，因此住宿業者確實可以要求登記、影印身分證資料，然而依照個人資料保護法 § 19 法律要求的規定，但業者須基於**確保交易及旅客住宿安全的特定目的**

法規	內容
觀光旅館業管理規則 § 19	• 觀光旅館業應登記每日住宿旅客資料；其保存期間為半年。 • 前項旅客登記資料之蒐集、處理及利用，並應符合個人資料保護法相關規定。
旅館業管理規則 § 23	• 旅館業應將每日住宿旅客資料登記；其保存期間為半年。 • 前項旅客登記資料之蒐集、處理及利用，並應符合個人資料保護法相關規定。
民宿管理辦法 § 28	• 民宿經營者應將每日住宿旅客資料登記；其保存期間為六個月。 • 前項旅客登記資料之蒐集、處理及利用，並應符合個人資料保護法相關規定。



當事人之「同意」

■ 個人資料保護法§7

- ◆ 第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。
- ◆ 第十六條第七款、第二十條第一項第六款所稱同意，指當事人經蒐集者**明確告知特定目的外之其他利用目的、範圍及同意與否**對其權益之影響後，**單獨所為之意思表示**。
- ◆ 公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意。
- ◆ 蒐集者就本法所稱經當事人同意之事實，應負舉證責任。





個人資料蒐集時之告知義務

告知義務

辦法條文

第十一條

非公務機關蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。

對應安維計畫段落範例

所屬人員直接向當事人蒐集個人資料時，明確告知當事人以下事項：

1. 本公司名稱。
2. 蒐集目的。
3. 個人資料之類別。(註：可參考法務部「個人資料保護法之特定目的及個人資料之類別」)
4. 個人資料利用之期間、地區、對象及方式。
5. 當事人得向本公司請求閱覽、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，以及如不提供對其權益之影響。

可提供證據參考

- 個資告知聲明或隱私政策
- 當事人同意書
- 個資盤點表

	直接蒐集時之告知義務	間接蒐集時之告知義務
法源依據	個人資料保護法§8	個人資料保護法§9
告知時機	直接蒐集	間接蒐集
告知內容	(1)蒐集機關名稱 (2)蒐集目的 (3)個資類別 (4)利用地區、期間對象與方式 (5)當事人權利行使之方式 (6)得自由提供時，不提供對當事人權益之影響 (7)間接蒐集時之資料來源 (若為間接蒐集始適用)	
例外規定	• 法律規定得免告知 • 係機關執行法定職務或履行法定義務所必要 • 告知將妨害法定職務執行 • 告知將妨害公共利益 • 當事人明知應告知之內容 • 蒐集非基於營利之目的且對當事人無不利影響	• 有左列情形 • 當事人自行公開或已合法公開之個資 • 不能向當事人或其法定代理人為告知 • 基於公共利益為統計或學術研究之目的而有必要等 • 大眾傳播業者基於新聞報導之公益目的而蒐集個資



觀光產業個人資料檔案安全維護 自主檢查表（自評表）

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
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 ☐	• 請檢附最新個資盤點資料，確認皆已識別保有依據。
		6.2個人資料之利用，是否符合特定目的之範圍？	是 ☐ 否 ☐	
		6.3是否有目的外之利用？目的外利用是否符合法定要件	是 ☐ 否 ☐	• 請說明機關所蒐集之個資是否具有目的外之利用情形。如有目的外利用，請說明其符合之法定要件。
		6.4是否依規定取得當事人同意（當事人同意之情形）？	是 ☐ 否 ☐	• 請說明蒐集個資並取得當事人同意之情形。
		6.5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）？	是 ☐ 否 ☐	• 請檢附告知事項。



觀光產業個人資料檔案安全維護 自主檢查表（自評表）

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
6	蒐集、處理 利用作業	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？如需費用是由機關支付所需費用？	是 ☐ 否 ☐	• 請說明提供當事人拒絕行銷之方式
		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 ☐	• 請說明是否有當事人拒絕接受行銷以及作業流程。



個人資料蒐集告知聲明

請您詳細填寫以下資料！* 為必填欄位

會員姓名：	姓 名	*	電子郵件：		*
設定密碼：		*	確認密碼：		*
請使用8個字元以上混合使用數字和英文字大小寫的密碼			請再次輸入密碼		
會員稱謂：	先生	*	所在國籍：	臺灣	
出生日期：	yyyy-mm-dd		所在縣市：	臺北市	
綁定本飯店LINE@會員帳號,詳填此欄位可獲得專屬通知。			身分證號：	☒	*
行動電話：	e.g. +886 912345678	*	護照證號：	☐	*
(您的個人資料僅供飯店使用)			住房備註：		

☐ 會員電子報 ☐ 好康優惠券
☐ 我已閱讀並同意遵守會員規範。*

請勾選我已閱讀並同意遵守會員規範。

留下同意軌跡

XXX飯店（下稱「本公司」）依個人資料保護法（下稱「個資法」）第8條第1項規定，向台端告知下列事項，請台端詳閱：

一、蒐集、處理及利用之特定目的

基於行銷、訂位及提供賓客服務之範圍內蒐集、處理或使用個人資料並透過整合資料即時發送餐飲住宿等相關資訊、活動邀請及行銷業務等訊息使用，以之作為後續服務提供之依據。

二、蒐集之個人資料類別：

姓名、所在國籍、所在縣市、身分證統一編號、護照號碼、電子郵件帳號、聯絡方式、性別、出生日期等，詳XXX飯店訂房網頁面、訂房契約書或業務相關文件等內容。



個人資料蒐集告知聲明

三、個人資料利用之期間、地區、對象及方式

(4) 個資期間地區對象方式

(一) 期間：在上述取得您個人資料目的之存續期間內，本公司將藉由您已提供之上述資料，在上述目的範圍內，提供您本公司之相關服務或優惠訊息。

(二) 地區：本公司將恪遵個人資料保護相關法規，密切依循法規資訊安全的執行要領，於中華民國領域內管理、保護、處理、使用您的個人資料，並基於提供您本集團之住宿及餐飲服務，本公司位於美國之總公司，亦可能提供您國際中文版外的服務或優惠訊息。

(三) 對象：本公司將恪遵個人資料保護相關法規來管理、保護、處理、使用您的個人資料，且您的個人資料將僅限於本集團總公司、本公司與其旗下餐廳及本集團指定合作廠商，於提供您服務或優惠訊息時使用，除法律另有規定，或經過您的事前書面同意外，本公司絕不會向任何其他第三人揭露或供其使用。

(四) 方式：本公司將依您提供個人資料之目的，以符合法令之自動化及人工方式管理、保護、處理、使用您的各類資料，於取得您的書面同意前，絕不會將您的個人資料進行超乎上述目的的使用。



個人資料蒐集告知聲明

四、台端對個人資料得行使之權利及方式

(5) 當事人權利行使

依個資法第3條規定，台端就本公司保有台端之個人資料得行使下列權利：

（一）依個人資料保護法之規定，您可向本公司提出下列要求：

1. 得向本公司查詢、請求閱覽或請求製給複製本，本公司依法得酌收必要成本費用。
2. 得向本公司請求補充或更正，惟依法台端應為適當之釋明。
3. 得向本公司請求停止蒐集、處理或利用及請求刪除，惟依法本公司因執行業務所必須者，得不依台端請求為之。

（二）行使權利之方式：

本公司將秉持對您個人資料保護的重視，依法律及上述原則管理、保護、處理、使用您的個人資料，如您對我們有任何指教，或要行使前述的權利，請撥打本公司的聯絡電0800123123，或將您的需求郵寄至本公司的電子郵件信箱:OOO@XXX.com

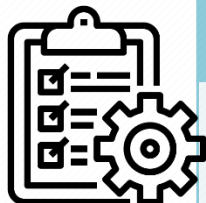
五、台端不提供個人資料所致權益之影響

(6) 對當事人權益的影響

您可自由選擇是否提供您的個人資料，但您選擇不提供或不完全提供時，本公司將可能無法提供您上述取得您個人資料目的之相關服務。



個資蒐集、處理及利用之合法要件



國際傳輸

辦法條文	對應安維計畫段落範例	可提供證據參考
第十二條 1. 中央主管機關依本法第二十一條規定，對非公務機關為限制國際傳輸個人資料之命令或處分時，非公務機關應通知所屬人員遵循辦理。 2. 非公務機關將個人資料作國際傳輸者，應檢視是否受中央主管機關限制，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督： 一. 預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。 二. 當事人行使本法第三條所定權利之相關事項。	國際傳輸： 法定依據：依據個資法第21條，先行確認該產業是否受國際傳輸之限制。目前觀光產業未受限制，但仍應確認： - 交通部對業者為限制國際傳輸個人資料之命令或處分時，本公司應通知所屬人員遵循辦理。 - 所屬人員將個人資料進行國際傳輸時，應檢視是否受交通部限制，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督： - 預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。 - 當事人行使個資法第3條所定權利之相關事項。	- 是否有國際傳輸之情形 - 若有是否告知傳輸地區、對象 - 是否使用雲端服務，若有應確認資料庫落地之國家，並提出相關佐證(如雲端業者出具的證明書)以證明安全性。

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
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 ☐	請說明如何確認Database的安全以及放在那個國家？並提出相關佐證(如雲端業者出具的證明書)



當事人權利行使及刪除銷毀個資

當事人權利行使

辦法條文

對應安維計畫段落範例

可提供證據參考

第十三條

非公務機關於個人資料當事人行使本法第三條規定之權利時，應依下列規定辦理：

- 一. 提供聯絡窗口及聯絡方式。
- 二. 確認為個人資料當事人本人，或經其委託者。
- 三. 認有本法第十條但書各款、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之事由時，應附理由通知當事人。
- 四. 有收取必要成本費用者，應告知當事人收費基準。
- 五. 遵守本法第十三條有關處理期限之規定。

當事人權利行使

1. 當事人向本公司行使當事人權利時，聯絡窗口為：○○○；聯絡電話：○○○。以上聯絡資訊公告於本公司營業處所或網頁。
2. 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。
3. 由指定之管理人員每○月(或季、年)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，除因法令規定、執行業務所必須或經當事人書面同意者，主動刪除或銷毀其個人資料，並留存相關紀錄。
4. 當本公司保有之個人資料利用期限屆滿時，除因法令規定、執行業務所必須或經當事人書面同意者外，將主動刪除或銷毀其個人資料，並留存相關紀錄。

- 當事人權利行使作業程序書及管道
- 內部制度文件及實際質性作法
- 當事人權利行使之紀錄，及通知當事人及曾經利用者之證據
- 刪除銷毀記錄（時間、地區、對象、方式）
- 執行記錄、內部評估或稽核記錄

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
11	使用紀錄資料軌跡及證據保存	11.1 是否保存個人資料提供或移轉第三人之紀錄？	是□ 否□	• 是否保存個人資料提供或移轉第三人之紀錄？
		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□	• 請檢附當事人行使個資法第三條之權利及處理過程之紀錄。



設備安全管理



設備安全管理

辦法條文

第十四條

非公務機關對所蒐集保管之個人資料檔案，應採取必要適當之安全設備或防護措施。前項安全設備或防護措施，應包含下列事項：

- 一. **紙本資料**檔案之安全保護設施。
- 二. **電子資料**檔案存放之電腦、自動化機器相關設備、可攜式設備或儲存媒體，配置安全防護系統或加密機制。
- 三. 存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放**媒介物報廢汰換或轉作其他用途時**，應採取適當之銷毀或防範措施，避免洩漏個人資料；**委託他人執行者**，非公務機關對受託者之監督依本法第二十條規定辦理。

對應安維計畫段落範例

設備安全

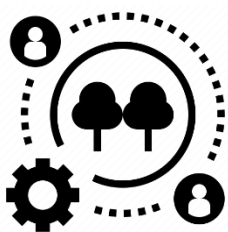
1. 指派專人管理建置個人資料之電腦、自動化機器相關設備、可攜式設備，應定期清點、保養維護，並應注意資料之備份及設備防竊、未經授權攜出等相關安全措施。
2. 應指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經單位主管同意並作成紀錄不得攜帶外出或拷貝複製。
3. 本公司保有之個人資料檔案每○週(月)備份。重要個人資料備份應異地存放，並應建置防止個人資料遭竊取、竄改、損毀、滅失或洩漏等事故之機制。
4. 電腦、自動化機器或其他存放媒介物需報廢汰換或轉作其他用途時，並應檢視該設備所儲存之個人資料是否確實刪除、銷毀。委託他人執行者，當對受託者為適當之監督並與其明確約定相關監督事項及方式。
5. 更新或維修電腦設備時，應指定專人在場，確保個人資料之安全及防止個人資料外洩。
6. 電腦設備報廢或不使用時，確實刪除電腦硬體設備中所儲存之個資檔案。

可提供證據參考

- 設備管理程序文件
- 消防、監控設備稽核及維護紀錄
- 執行記錄、內部評估或稽核記錄



人員管理



人員管理

辦法條文

第十五條

非公務機關為確實保護個人資料之安全，應對其所屬人員採取適度管理措施。

前項管理措施，應包含下列事項：

- 一. 依據業務需求，適度設定所屬人員不同之權限，控管其接觸個人資料之情形，並定期檢視權限內容之適當性及必要性。
- 二. 檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。
- 三. 要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。
- 四. 所屬人員異動或離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂保密切結書。

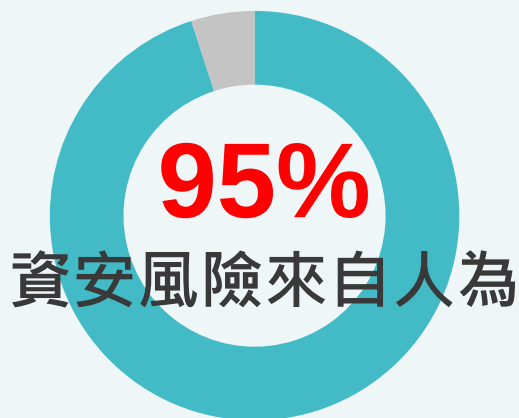
對應安維計畫段落範例

人員管理

1. 選任監督：本公司聘用人員時，應進行適當篩選。
2. 保密契約：本公司與人員簽訂僱傭或委任契約時，應一併簽訂個人資料相關保密契約，並確保於人員離職或職務變動後適當期間內仍負有保密義務。
3. 教育訓練：本公司定教育訓練計畫，並訂定評量機制。

可提供證據參考

- 聘僱契約
- 保密契約
- 教育訓練紀錄
- 執行記錄、內部評估或稽核記錄

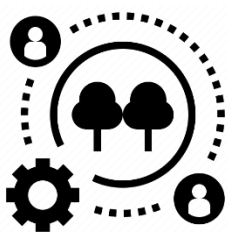


根據世界經濟論壇「全球風險報告」資安風險，有95%資安相關議題根因乃人為所致。

- 風險來自於人員、設備、行為模式
- 政策推動與實際意願，內部與外部之配合



資料安全管理



資料安全管理

辦法條文

第十六條

- 業者因執行業務以資通訊系統蒐集、處理或利用個人資料時，應採行下列資訊安全措施：
 - 使用者身分確認及保護機制。
 - 個人資料顯示之隱碼機制。
 - 網際網路傳輸之安全加密機制。
 - 個人資料檔案及資料庫之存取控制與保护措施。
 - 防止外部網路入侵對策。
 - 非法或異常使用行為之監控與因應機制。
- 前項第五款及第六款所定措施，應定期演練及檢討改善。
- 第一項所稱電子商務，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。

對應安維計畫段落範例

資安管理

- 個資檔案存放之電腦、自動化機器設備或可攜式設備，應設置識別密碼、保護程式密碼、安全防护系統、加密機制或相關安全措施。
- 儲存個人資料紙本之保管箱或檔案室內，應存放於辜文貴並上鎖，丟棄時應使用碎紙設備。
- 除非經指定之管理人員核可，不得存取。
- 所屬人員非經核可，不得任意複製個資檔案。
- 針對不同性質個資儲存媒介物，有適當防範措施，及報廢機制。
- 本公司蒐集、處理或利用個人資料達○○筆以上時，設置使用者身分確認、個資顯示之隱碼機制。
- 防止外部網路入侵對策及非法或異常使用行為之監控及因應機制。

可提供證據參考

- 資料安全管理作業程序書
- 存取權限管理、監控審核記錄
- 傳送過程使用安全通信協議（如TLS1.2以上）、存取權限制
- 備份機制
- 儲存個資媒介物報廢機制
- 防毒軟體
- IP限制、使用VPN加密通道或雙因子認證
- 弱點掃描、滲透測試報告



資料安全稽核機制



資料安全 稽核機制

辦法條文

第十八條

1. 非公務機關為確保本計畫及處理方法之落實，應依其組織規模及特性，衡酌資源之合理分配，訂定個人資料安全維護稽核機制，並指定適當人員**每年至少進行一次**本計畫及處理方法執行情形之檢查。
2. 前項檢查結果應向代表人提出報告，並留存相關紀錄，**其保存期限至少五年**。
3. 非公務機關依第一項檢查結果發現本計畫及處理方法不符法令或有不符法令之虞者，應即改善。

對應安維計畫段落範例

個資稽核機制

1. 本公司（或民宿）每年至少辦理**1次**個人資料安全維護稽核，檢查是否落實本計畫規範事項，針對檢查結果不合法令及潛在不符合之風險，應即改善，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) 紀錄檢查情形及結果。
2. 前項檢查結果應載入稽核報告中，由公司代表人（或民宿經營者）或經其授權人員簽名確認，並留存相關紀錄至少**5年**。

可提供證據參考

- 稽核相關內部制度文件等，應能呈現稽核之頻率、範圍、效力及方法論
- 內部評估報告或稽核記錄
- 提報專責人員之會議紀錄
- 預防矯正計畫
- 改善落實追蹤





觀光產業個人資料檔案安全維護 自主檢查表（自評表）

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
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 ☐	請檢附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。
		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 ☐	請檢附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 ☐	請檢附所屬人員清單(正職、短期約僱)及所簽署之保密切結書。
		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人資料？	是 ☐ 否 ☐	
		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 ☐	請說明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或網路共用資料夾，是否進行加密或遮蔽？並檢附查核結果。
		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 ☐	說明機關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？並請相關佐證。
		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 ☐	請說明資料備份機制，並檢附規範制度文件。



觀光產業個人資料檔案安全維護 自主檢查表（自評表）

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
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 ☐	• 請說明對存放儲存媒介物之環境相關消防、監控、進出入等控管措施，並檢附相關照片。
		• 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？	是 ☐ 否 ☐	• 請確認是否定期檢查或維護更新設備？並請檢附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 ☐	• 請檢附消防、監控設備等維護紀錄
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 ☐	• 請說明稽核之頻率及執行方式，並檢附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 ☐	• 請檢附檢視或修正之紀錄，並檢附稽核矯正單及追蹤紀錄。
17	個人資料庫之共享使用	• 17.1是否有其他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？	是 ☐ 否 ☐	請說明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。另檢附告知當事人之佐證。
		• 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？	是 ☐ 否 ☐	請檢附於處理及利用前告知當事人之佐證。



觀光產業個人資料檔案安全維護 自主檢查表（自評表）

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
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 ☐	建議依「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16條所列項目稽核。 - 使用者身分確認及保護機制 - 個人資料顯示之隱碼機制 - 網際網路傳輸之安全加密機制 - 個人資料檔案與資料庫之存取控制及保護監控措施 - 防止外部網路入侵對策 - 非法或異常使用行為之監控及因應機制
		14.2是否採行個人資料顯示之隱碼機制？	是 ☐ 否 ☐	
		14.3是否採行網際網路傳輸之安全加密機制？	是 ☐ 否 ☐	
		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 ☐	
		14.5是否採行防止外部網路入侵對策？	是 ☐ 否 ☐	
		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 ☐	
		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 ☐	



資料去識別化佐證

	ID	GENDER	NAME	DOB	SSID	CCNUM	CC_V
1	262	f	曾**	(null)	F2*****439	****-****-****-4999	MM/YY
2	263	f	黃**	(null)	E2*****352	(null)	MM/YY
3	264	m	忠**	(null)	B1*****888	****-****-****-9861	MM/YY
4	265	f	蔡**	1989/MM/DD	C2*****795	****-****-****-2047	MM/YY
5	266	f	張**	(null)	H2*****900	****-****-****-6810	MM/YY
6	267	(null)	李**	(null)	R1*****434	(null)	MM/YY
7	268	(null)	吳**	(null)	V1*****041	****-****-****-1690	MM/YY
8	269	(null)	楊**	(null)	Y1*****475	****-****-****-6005	MM/YY
9	270	(null)	張**	(null)	L1*****512	(null)	MM/YY
10	271	(null)	鄭**	(null)	P1*****556	****-****-****-8111	MM/YY
11	272	(null)	吳**	(null)	N1*****942	****-****-****-2739	MM/YY
12	273	(null)	黃**	(null)	F1*****534	(null)	MM/YY
13	274	(null)	楊**	(null)	C1*****306	****-****-****-7360	MM/YY
14	275	f	林**	1981/MM/DD	E2*****165	****-****-****-9016	MM/YY
15	276	f	洪**	1984/MM/DD	L2*****885	****-****-****-1048	MM/YY

資料來源：經濟部商業發展署行政檢查前業者應備事項宣導與指引



人員進出機房登記表

人員進出機房登記表					
文件編號	KSVS-D-019		機密等級	限閱	版次 1.0

紀錄編號：

填表日期： 年 月 日

日期 (民國年月日)	進出機房時間		進入機房人員 簽 名	進出事由	攜出入物品	陪同人員 簽 名
	進入	離去				
				☐ 定期巡檢 ☐ 其他 ☐ 設備維護或設定 備註事項：_____		
				☐ 定期巡檢 ☐ 其他 ☐ 設備維護或設定 備註事項：_____		
				☐ 定期巡檢 ☐ 其他 ☐ 設備維護或設定 備註事項：_____		
				☐ 定期巡檢 ☐ 其他 ☐ 設備維護或設定 備註事項：_____		
				☐ 定期巡檢 ☐ 其他 ☐ 設備維護或設定 備註事項：_____		
				☐ 定期巡檢 ☐ 其他 ☐ 設備維護或設定 備註事項：_____		

資料來源：經濟部商業發展署行政檢查前業者應備事項宣導與指引



伺服器OS更新紀錄範例

Windows Updates History Viewer					
檔案(F) 編輯(E) 檢視(V) 選項(O) 說明(H)					
Windows Updates History Viewer					
標題	描述	KB 號碼	安裝日期	更新作業	作業結果
2020-10 適用於 x64 ...	安裝此更新可解決 Wind...	KB4580419	2020/11/9 下午 0...	安裝	成功
Microsoft Defender ...	這個套件將會更新 Micr...	KB4052623	2020/11/8 下午 0...	安裝	成功
Microsoft Defender ...	這個套件將會更新 Micr...	KB4052623	2020/11/7 下午 0...	安裝	失敗
Microsoft Defender ...	這個套件將會更新 Micr...	KB4052623	2020/11/7 下午 0...	安裝	已中止
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/10/27 上午 ...	安裝	成功
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/10/28 上午 ...	安裝	成功
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/10/28 下午 ...	安裝	成功
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/10/29 上午 ...	安裝	成功
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/10/29 下午 ...	安裝	成功
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/11/1 下午 0...	安裝	成功
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/10/30 下午 ...	安裝	成功
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/11/2 下午 0...	安裝	成功
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/11/2 下午 1...	安裝	成功
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/11/3 上午 0...	安裝	成功
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/10/30 下午 ...	安裝	成功
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/11/4 上午 0...	安裝	成功
Microsoft Defender ...	請安裝此更新來修訂用...	KB2267602	2020/11/5 下午 0...	安裝	成功
26 個項目，已選定 1 個項目		10.0.19041.488	NirSoft Freeware. https://www.nirsoft.net		

資料來源：經濟部商業發展署行政檢查前業者應備事項宣導與指引



個資媒體消磁佐證範例

消磁服務證明書

證書編號：20101005-XX

此致XXXX機關：

有限公司於中華民國 年X月X日，於貴公司營運據點（地址：台北市XX路XX號X樓）協助貴公司消磁硬碟XX顆以及磁帶XX卷，消磁媒體數量共計XX樣。詳細消磁媒體記錄如附件，以茲證明。

附件項目如下：

1. 消磁服務日期
2. 消磁服務人員名單
3. 消磁媒體清冊共XX頁XXX項
4. 消磁服務過程錄影影像檔案
5. 貴公司驗收記錄



資料來源：經濟部商業發展署行政檢查前業者應備事項宣導與指引



認知宣導及教育訓練

認知宣導及教育訓練

辦法條文	對應安維計畫段落範例	可提供證據參考
第十七條 非公務機關應定期或不定期對於所屬人員施以基礎個人資料保護認知宣導及教育訓練，使其明瞭相關法令之要求、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及措施。	認知宣導及教育訓練 1. 本公司（或民宿）每年應定期或不定期對員工施以基礎個人資料保護認知宣導及教育訓練至少○小時，使員工明瞭個人資料保護相關法令、責任範圍及個人資料保護事項之機制、程序及措施；對於新進員工應給予特別指導，以利遵循相關規定。 2. 前述教育宣導及訓練應留存紀錄(例如：簽名冊等文件)。	• 教育訓練簡報 • 各項相關課程簽到表(需含授課日期) • 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。

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
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？	是 ☐ 否 ☐	• 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。



教育訓練證明

澎湖縣觀光產業個人資料檔案安全維護自主檢查表教學簽到單

日期：2024年12月10日

地點：澎湖科技大學

時間：10:00 AM - 12:00 AM

標號	單位	職稱	姓名	簽名

交通部指定觀光產業類 手把手個資保護實作教學

李怡親 高級法律研究員

財團法人資訊工業策進會 科技法律研究所

2024



科技法律研究所
SCIENCE & TECHNOLOGY
LAW INSTITUTE





使用紀錄、軌跡資料及證據保存



使用紀錄、 軌跡資料及 證據保存

辦法條文	對應安維計畫段落範例	可提供證據參考
第十九條 1. 非公務機關執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。 2. 非公務機關依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄： 一、刪除、停止處理或利用之方法、時間或地點。 二、將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間、地點，及該對象蒐集、處理或利用之合法依據。 3. 前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。	使用紀錄、軌跡資料及證據保存 本公司（或民宿）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(或民宿)如何保存，例如：個人資料使用查詢紀錄、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。)	- 紙本：存取及利用紀錄、調閱紀錄、軌跡資料、銷毀紀錄； - 電子檔：相關日誌(LOG)留存 - Log Files保存，包含資訊系統使用紀錄及軌跡資料紀錄、針對儲存個人資料資料庫的存取紀錄、EDR偵測回應紀錄、第三方鑑識分析報告



觀光產業個人資料檔案安全維護 自主檢查表（自評表）

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
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 ☐	• 是否保存個人資料提供或移轉第三人之紀錄？
		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 ☐	• 請檢附當事人行使個資法第三條之權利及處理過程之紀錄。
		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 ☐	• 請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。
		11.4 是否保存人員權限新增、變動及刪除之紀錄？	是 ☐ 否 ☐	• 請檢附人員權限新增、變動及刪除之紀錄。
		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 ☐	• 請說明留存之期限，並檢附最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。



個人資料刪除（銷毀）申請單

申請刪除(銷毀)內容			
申請人 / 工號	儲存媒體	單位	
資料名稱 / 數量 (範圍)	☐ 紙本資料 ☐ 電子檔案 ☐ 其他		
資料名稱 / 數量 (範圍)	資料名稱： 政府計畫別： 數量(範圍)：		
銷毀或刪除原因	☐ 蒐集目的消滅 (補充說明: _____) ☐ 當事人請求 (補充說明: _____) ☐ 保存期限到期 (補充說明: _____) ☐ 其他 (補充說明: _____)		
儲存地點或系統			
預計銷毀或刪除日期 / 時間	_____年_____月_____日 / _____時_____分		
計畫銷毀或刪除方式	☐ 碎紙 ☐ 焚毀 ☐ 消磁 ☐ 電子檔刪除 ☐ 其他：_____		
申請單位主管 (簽章)			
刪除(銷毀)執行結果			
執行結果	☐ 已完成	完成日期: 年 月 日 時 分	
	☐ 未完成	說明:	
	其他:		
銷毀或刪除資料執行人 (簽章)		見證人員 (簽章)	



業務終止

業務終止

辦法條文	對應安維計畫段落範例	可提供證據參考
第二十二條 非公務機關業務終止後，其保有之個人資料不得繼續使用，應依下列方式處理，並留存相關紀錄，其保存期限<u>至少五年</u>： 一. 銷毀：銷毀之方法、時間、地點及證明銷毀之方式。 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。 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。	業務終止 本公司業務終止後，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5年： （一）銷毀：銷毀之方法、時間、地點及證明銷毀之方式。 （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。 （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。	- 業務終止以及刪除銷毀、移轉或停止處理利用之管理程序文件 - 執行記錄、內部評估或稽核記錄





案例探討-委外系統商

● 案例：高院112年度上字656號判決

事實概要

- 麗禧公司提供消費者線上訂購溫泉券之購買系統，該系統由墨攻公司進行建置、維護與管理。消費者以其個資使用系爭訂購系統購買溫泉券，嗣接獲詐騙電話，遭訛詐轉出99,987元。
- 消費者依個資法第29條第1項、第2項、民法第184條第1項前段、第2項、民法第185條規定，請求麗禧公司、墨攻公司連帶給付財產上損害99,987元、非財產上損害2萬元。

判決要旨

- 被上訴人麗禧公司、墨攻公司應分別給付上訴人新臺幣2萬元。
- 詐騙集團所用個資為訂購系統所外洩，應由被上訴人（企業）舉證其就上訴人個資外洩乙事，並無違反個資法之故意或過失。
- 未見外洩前之管理維護系爭訂購系統行為，相關措施均屬訂購系統遭竊取個資後所為，不足證明被上訴人就個資外洩前，就訂購系統有何管理維護，及已盡採取**適當安全措施之責**。
- 數發部雖認被上訴人平時維護措施尚稱妥適、應變措施尚屬合宜、改善措施亦稱合理；觀光局雖認麗禧公司對墨攻公司之監督尚符個資法規定。**惟行政調查程序與司法訴訟程序不同，其認定對法院無拘束力。**
- 上訴人之財產損失係詐騙集團所致，與被上訴人之過失行為**無因果關係**。
- 被上訴人侵害上訴人**隱私權、個資自主權**，致其個資為詐騙集團利用，上訴人因此耗費時間心力申訴之過程煎熬，並需持續擔心個資遭他人使用，受有精神上痛苦，故應賠償上訴人非財產上損害即慰撫金2萬元，核屬適當。。



委託機關定義及監督責任彙整

定義（個資法§4）

受公務機關或非公務機關委託蒐集、處理或利用個人資料者，
於本法適用範圍內，**視同委託機關**。

監督責任（細則§8）

委託機關應定期確認受託者執行狀況，並將確認結果記錄

預定蒐集、處理或利用個資之**範圍、類別、特定目的及期間**

受託者的**適當安全維護措施**

有**複委託**者，其約定之受託者

受託者違法時應**通知**或採行之**補救措施**

委託者**保留指示**之事項

關係終止或解除時，個資之**返還**或**刪除**

定期**確認**執行狀況與**記錄**結果

有無委外

監督方式

持續管理



個資委外之適當監督責任



個人資料委外議題

辦法條文	對應安維計畫段落範例	可提供證據參考
第二十一條 1. 非公務機關<u>委託他人蒐集、處理或利用個人資料之全部或一部時</u>，應依本法施行細則第八條規定為<u>適當監督</u>。 2. 非公務機關為執行前項監督，應與受託者<u>明確約定</u>相關監督事項及方式。	委外作業 本公司（或民宿）委託他人蒐集、處理或利用個人資料之全部或一部時，應依個人資料保護法施行細則第八條規定對受託人為適當之監督，並於委託契約或相關文件中，明確約定其內容，以及採取下列方式辦理： 1. 選擇受託人前，應確認需要委外的範圍，並以適當評估方式選擇具適當 個資安全維護能力的受託人。 2. 應與受託人締結委託契約，要求受託人依本公司（或民宿）應適用之個 資管理規定執行契約。 3. 於委託契約或相關文件明確約定適當之監督事項及方式。 4. 要求受託者僅得於本公司（或民宿）指示之範圍內，蒐集、處理或利用 個人資料。 5. 要求受託者認本公司（或民宿）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，應立即通知本公司（或民宿），並於契約中訂定委外廠商於知悉資通或個資安全事件情況時，應即向本公司（或民宿）權責人員或通報窗口，以指定之方式進行通報。 6. 對受託者應定期查核受託者執行之狀況，並將確認結果記錄之。(如委外查核報告以及查核缺失追蹤情形) 7. 委託關係終止或解除時，受託者應將個人資料載體之返還或將個人資料 刪除。	• 選商標準 • 契約、查核記錄或其他內部制度文件 • 複委託契約、保密協議書 • 刪除銷毀或返回個資切結書



觀光產業個人資料檔案安全維護 自主檢查表（自評表）

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
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 ☐	請檢附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 ☐	
		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 ☐	- 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 - 請檢附個資委外之廠商清單及合約文件。
		13.4是否要求受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料？	是 ☐ 否 ☐	
		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 ☐	



委外契約範例（僅供參考）

立約人 甲方：XXX 公司（委託方） 乙方：（受託方）

甲方委託乙方執行業務，就個人資料之蒐集、處理或利用行為，雙方同意遵守下列條款，並以本約視為原委託契約之一部分，本約未規範之部分悉依原契約之內容執行：

第一條、個人資料告知條款：

為遵守個人資料保護法（以下簡稱個資法）之規定，乙方如有受甲方委託代為蒐集個人資料之行為，應依個資法第8、第9條規定，履行告知義務，或於首次利用個人資料時為告知，告知之書面內容應由甲方提供。

第二條、個人資料之定義、委託範圍：

個人資料之定義、委託範圍

（一）本約之個人資料其蒐集、處理及利用行為，遵照個資法等相關法規之定義。

（二）甲方委託乙方執行業務涉及有關個人資料蒐集、處理及利用範圍如下：

1. 個人資料之特定目的：

2. 個人資料之類別：

3. 個人資料之範圍：

4. 個人資料之利用期間：

通知及補救

受委託人認為委託人之指示有違反個人資料保護法、其他法律或其法規命令者，應停止蒐集、處理或利用該個人資料並立即敘明理由通知委託人。

□委託人保留指示之事項：（若有保留指示事項，請填入內容，如稽核權、底稿交付權、當事人權利行使之義務、協助答辯權）

保留指示

第三條、安全管理措施：

（一）乙方應視公司規模、營運狀況採取下列措施：

（個資法施行細則12條第二項各款）

適當安全管理措施

第四條、複委託：

複委託

乙方若需將甲方委託之業務複委託其他廠商時，須經甲方事前書面同意。甲方若同意乙方得以複委託方式提供服務，乙方仍負有依照本約規定履行之責任，複委託廠商因執行業務而造成甲方之損害時，乙方與複委託單位應對甲方之損害負連帶賠償之責(包括但不限於訴訟費用及律師費用等)。

第五條、履約中或本合作終止時資料的刪除或返還義務：

關係終止返還義務

（一）受委託人於履行本合作期間，依本合作規定，經委託人書面同意轉讓本合作全部或一部予他廠商時，如有將個人資料移轉予受讓契約之廠商時，應作成相關記錄並提供予委託人備查，包括移轉之原因、移轉之對象（即受讓本合作之廠商）、移轉對象得保有該項個人資料檔案之依據及證明、移轉之方法、時間、地點等。

（二）受委託人就履行本合作而蒐集、處理、利用之個人資料返還委託人或予以刪除、銷毀後，應出具返還、刪除或銷毀聲明書予委託人。

第六條、保密協議：

乙方因履行甲方委託契約所取得或知悉甲方之個人資料，應負保密義務。

第七條、定期確認

定期確認及記錄

（一）委託人得針對受委託人的個人資料安全管理措施實施情形進行確認，並將確認結果記錄之；必要時，得派員進行實地訪查或委託專業人員進行查核，受委託人應予配合。

（二）委託人於訪查或查核後，認有缺失，得以書面敘明理由限期請受委託人改善，受委託人應予配合。

第七條、損害賠償及遲延履約責任

受委託人執行本合作業務有違反個人資料保護法、個人資料保護法施行細則之情事，致當事人個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。



受託者之選擇-自評表

管理重點

判斷個資有無
委外處理等

選擇委外監督方式
，簽約或實地查核

後續處置及內
部管理機制

委外廠商查核之表單設計（例示）

查核項目	查核內容	查核結果	說明
(若著眼於安全維護，細則12條要求的11款事項就將成為查核重點)		☐ 符合 ☐ 不符合 ☐ 不適用	
		☐ 符合 ☐ 不符合 ☐ 不適用	
		☐ 符合 ☐ 不符合 ☐ 不適用	
		☐ 符合 ☐ 不符合 ☐ 不適用	
		☐ 符合 ☐ 不符合 ☐ 不適用	



個人資料安全維護之整體持續改善



個人資料安全維護之整體持續改善

辦法條文

第二十條

非公務機關應隨時參酌業務與本計畫及處理方法之執行狀況、社會輿情、技術發展及相關法規增修等因素，檢討所定本計畫及處理方法，必要時予以修正。

對應安維計畫段落範例

持續改善

1. 本公司（或民宿）將隨時參酌業務及依據計畫執行狀況，注意相關社會輿情、技術發展、法令修正或其他因素，檢視所定安全維護計畫之合宜性，並予必要之修正。
2. 針對個資安全稽核結果有不符法令之虞者，規劃改善與預防措施並納入安全維護計畫。

可提供證據參考

- 內部制度文件、定期檢視記錄或採取之措施版次記錄
- 會議記錄

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
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 ☐	請檢附相關個人資料安全維護議題會議之記錄。
		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 ☐	請檢附個人資料管理(或安全維護)辦法以及完整之版本資訊，包含但不限於日期、提報人及核定人等相關資訊。



管理審查會議討論議題範例

● 輸入議題:

- 一. 先前管理階層審查之矯正預防措施
- 二. 可能影響系統之變動
- 三. 法規變更之風險
- 四. 來自利害相關者之回饋
- 五. 可用於組織以改進個人資料保護與管理績效與有效性之技術、產品或程序
- 六. 個人資料保護與管理稽核與審查之結果
- 七. 個資當事人申訴案件處理情形
- 八. 個資事故緊急應變案件處理情形
- 九. 有效性測量的結果
- 十. 改進之各項建議

● 輸出項目

- 一. 影響個人資料保護程序與控制措施之必要時的修改包括下列事項之變更：
 - ◆ (1)各項營運要求
 - ◆ (2)各項個資保護要求
 - ◆ (3)影響既有各項營運要求之營運過程
 - ◆ (4)法律或法規各項要求
 - ◆ (5)契約的各項義務
 - ◆ (6)風險等級及/或風險接受準則
- 二. 風險評鑑與風險處理計畫之更新
- 三. 矯正預防之改善
- 四. 資源需求
- 五. 控制措施的有效性如何量測之改進



02

旅宿業個人資料檔案 安全維護計畫



觀光產業個資安維辦法對照

作業程序	交通部指定觀光產業類個資安維辦法	所需文件
人員及資源配置	6	組織架構圖
清查個人資料檔案	7	個資盤點表 作業流程圖
風險評估作業程序	8	風險評鑑表
事故之預防、通報及應變作業程序	9	事故通報、通知紀錄
個人資料蒐集、處理或利用作業程序	10	安全維護計畫 程序文件書 表單(如告知聲明、個資同意書、同意行銷軌跡、當事人權利申請書、教育訓練簽到表、資安管理紀錄、保密切結、系統維護、刪除銷毀申請單、委外契約、內評報告、業務終止資料移轉刪除銷毀紀錄、會議紀錄等證據) 以及執行紀錄
個資蒐集之告知義務程序	11	
國際傳輸程序	12	
受理當事人權利行使之作業程序	13	
個資安全管理作業程序	14(設備/資安)、15(人員)、16(資通系統)	
認知宣導及教育訓練作業程序	17	
個資稽核程序	18	
使用紀錄、軌跡資料及證據保存作業程序	19	
持續改善作業程序	20	
委託監督作業程序	21	
業務終止個人資料處理作業程序	22	



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

● 適用範圍（本辦法§3）

◆ 本辦法所稱非公務機關包括下列各款：

- 觀光旅館業 □ 旅行業
- 旅遊業 □ 觀光遊樂業
- 民宿

● 應訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法（本辦法§4）

◆ 非公務機關保有消費者個人資料達八千筆者，應依本辦法規定，規劃、訂定、修正與執行消費者個人資料檔案安全維護計畫及業務終止後個人資料處理方法。

小提示：為明確旅宿業應訂定「個人資料檔案安全維護計畫」之對象，交通部觀光署函文各縣市政府依一般旅館平均住用率約45%為基準，以半年個資可達8,000筆以上推估，原則客房達100間(含)以上旅宿業應依前揭規定訂定個人資料檔案安全維護計畫，並可作為辦理旅宿業個資事前「行政檢查」對象之參考並作為執行個資行政檢查之參考依據。

個資筆數未達8,000筆者，尚無須制訂安全維護計畫。惟業者無論保有個資筆數是否達8,000筆(或客房數100間(含)以上)，每年至少1次務必確實執行「觀光產業個人資料檔案安全維護自主檢查表」。



個人資料筆數的估算方式

- 估算個人資料筆數時，我們以**每一自然人之每一蒐集特定目的**來計算。這樣可以更精確地了解資料的蒐集、處理、利用情況。
- 讓我們來看看以下例子：黃小明到安九拉大寶貝酒店住宿，留下以下資料：

黃小明，40歲，電話0912345678，身分證A112233445

- ✓ 用於「餐廳訂位」之特定目的：算一筆個人資料
- ✓ 用於「會員註冊」之特定目的，同時用於「旅館住宿」之特定目的，算兩筆個人資料



交通部指定觀光產業類個資檔案安全維護計畫

〇〇公司個人資料檔案安全維護計畫

訂定(或修訂)日期：中華民國〇〇〇年〇〇月〇〇日

壹、組織及規模

一、旅宿類別：☐ (國際/一般)觀光旅館 ☐ 旅館 ☐ 民宿

二、旅宿名稱：

三、代表人：經營者姓名

四、地址：

五、員工數：〇〇人(註：可概略記載，例如：約〇〇人)

蓋公司印鑑章

蓋代表人 印鑑章

貳、個人資料檔案安全維護管理措施

一、依據：

個人資料保護法第27條第3項及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條規定辦理。

二、個人資料檔案安全維護計畫之訂定及修正

(一)訂定目的：為防止個人資料被竊取、竄改、毀損、滅失或洩漏，爰訂定「個人資料檔案安全維護計畫」(下稱本計畫)，本旅宿業員工應依本計畫辦理個人資料檔案安全管理及維護事宜。

(二)本計畫將參酌業務規模及特性，衡酌經營資源之合理分配等因素，檢視其合宜性，並經負責人或其授權人員於核定後予以修正。

交通部指定觀光產業類個資檔案安全維護計畫

三、專責人員及資源配置

(一)管理人員：

1.配置人數：○。(至少1名)

2.職責：

(1)規劃、訂定、修正、執行安全維護計畫及其他相關事項。

(2)定期(每年至少1次)就執行前開任務情形向代表人（經營者）或經其授權人員提出書面報告。

(二)稽核人員/單位：

1.姓名/單位：○○○。(至少1名)

2.職責：資料安全稽核機制

(1)不得與專責人員為同一人。

(2)定期稽核安全維護計畫之執行情形及成效，並將稽核結果，向代表人或經其授權之人員提出報告。

(三)預算：每年新臺幣○○○元。（包含管理薪資、設備費用等，可記載一定範圍之金額，依實際狀況填寫）



交通部指定觀光產業類個資檔案安全維護計畫

四、個人資料之範圍及項目

(一)特定目的：(觀光旅館業/旅館業/民宿)管理業務、契約、類似契約或其他法律關係事務、消費者、客戶管理與服務等運用、人事管理等運用(類別：識別類、社會情況類)。

(二)個人資料：自然人(包含旅客、消費者、從業人員等)之姓名、出生年月日、國民身分證統一編號、護照號碼、信用卡卡號、聯絡方式及其他得以直接或間接方式識別該個人之資料。

(三)指定管理人員每○○日(或週、月、季、**年**)**定期清查**本公司(或民宿)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**。

五、個人資料之範圍及項目

(一)風險評估

1. 經由本公司(或民宿)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. 旅宿業間互為傳輸時之外洩(包括分公司間傳輸、與相關業者間傳輸等)。

(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. 電子資料檔案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。

交通部指定觀光產業類個資檔案安全維護計畫

六、個人資料蒐集、處理及利用之內部管理程序

(一)直接向當事人蒐集個人資料時，應明確告知當事人以下事項：

1. 公司(或民宿)名稱。
2. 蒐集目的。
3. 個人資料之類別。(註：可參考法務部「個人資料保護法之特定目的及個人資料之類別」<https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=f1010631>。)
4. 個人資料利用之期間、地區、對象及方式。
5. 當事人得向本公司(或法人)請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或删除其個人資料。
6. 當事人得自由選擇提供個人資料，以及如不提供對其權益之影響。

(二)所蒐集之個人資料非由當事人提供者，應於處理或利用前，向當事人告知其個人資料來源及前項應告知之事項，若當事人表示拒絕提供，應立即停止處理、利用其個人資料。

(三)本公司（或民宿）為辦理本計畫之特定目的，得進行個人資料蒐集、處理、利用，於**特定目的消失或委託期限屆滿時應主動刪除或銷毀**。但因法令(如觀光旅館業管理規則/旅館業管理規則/民宿管理規則等)規定、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，當事人表示拒絕行銷後，應立即停止利用其個人資料行銷。如需作**特定目的外利用**，得先行檢視是否符合個人資料保護法第20條第1項但書之規定。

交通部指定觀光產業類個資檔案安全維護計畫

(五)當事人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，聯絡窗口：○○○(需為執行業務人員)；電話：○○○○○○○，並將聯絡資訊揭示於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。當事人請求答覆查詢、提供閱覽個人資料或製給複製本時，如有收取必要成本費用者，應主動告知收費基準。上述申請程序，應依個人資料保護法第13條規定於處理期限內辦理完成。

(六)負責保管及處理個人資料檔案之員工，其職務有異動或離職時，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(或民宿)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(或民宿)如委託他人蒐集、處理或利用個人資料時，應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，必須先行檢視是否合法令規定。

(十一)本公司(或民宿)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。

交通部指定觀光產業類個資檔案安全維護計畫

七、事故之預防、通報及應變機制

(一)預防：

1. 本公司（或民宿）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（或民宿）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，將危及正常營運或大量當事人權益，應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，並於知悉事故72小時內依附表通報目的事業主管機關(國際觀光旅館及非直轄市一般觀光旅館為交通部觀光署、直轄市一般觀光旅館為直轄市政府、旅館及民宿為各縣市政府)。
2. 對於個人資料遭竊取之當事人，應以適當方式通知使其知悉及本公司（或民宿）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、預防之措施。

交通部指定觀光產業類個資檔案安全維護計畫

八、設備安全管理、資料安全管理及人員管理措施

(一)設備安全管理(註：如無，則免敘明)

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. 本公司(或民宿)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(或民宿)之個人資料檔案應定期備份(如：每二週)。
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，本公司代表人(或民宿經營者)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。
7. 更新或維修電腦設備時，應指定專人在場，確保個人資料之安全及防止個人資料外洩。



交通部指定觀光產業類個資檔案安全維護計畫

八、設備安全管理、資料安全管理及人員管理措施

(二)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（或民宿）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，非經陳報本公司（或民宿）○○(請填公司代表人、民宿經營者或其他經授權之人員，依實際情形填寫)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，員工非經本公司（或民宿）○○(請填公司代表人、民宿經營者或其他經授權之人員，依實際情形填寫)同意不得任意複製或影印。
- 2) 儲存個人資料紙本之保管箱或檔案室內，應設置防火裝置及防竊措施。儲存個人資料之電腦主機系統應設置防火牆，降低外部入侵風險。主機置放之機房應設置門禁、監視錄影及防火設備。
- 3) 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。

交通部指定觀光產業類個資檔案安全維護計畫

八、設備安全管理、資料安全管理及人員管理措施

(三)人員管理

1. 本公司（或民宿）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，並定期檢視權限之適當性及必要性。
2. 所屬員工每○天/週/月(需低於90日、12週或3個月)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. 本公司（或民宿）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；簽訂勞務契約亦列入保密條款及相關之違約罰則，以確保執行業務期間對於個人資料內容之保密義務。
4. 員工或為旅宿業執行業務者與公司(或民宿)終止契約時，應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，不得私自複製、留存並在外繼續使用，並應簽訂保密切結書。

九、認知宣導及教育訓練

- (一)本公司（或民宿）每年應定期或不定期對員工施以基礎個人資料保護認知宣導及教育訓練至少○小時，使員工明瞭個人資料保護相關法令、責任範圍及個人資料保護事項之機制、程序及措施；對於新進員工應給予特別指導，以利遵循相關規定。
- (二)前述教育宣導及訓練應留存紀錄(例如：簽名冊等文件)。

交通部指定觀光產業類個資檔案安全維護計畫

十、個人資料安全維護稽核機制

(一)本公司（或民宿）每年至少辦理1次個人資料安全維護稽核，檢查是否落實本計畫規範事項，針對檢查結果不合法令及潛在不符合之風險，應即改善，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. 紀錄檢查情形及結果。

(二)前項檢查結果應載入稽核報告中，由公司代表人（或民宿經營者）或經其授權人員簽名確認，並留存相關紀錄至少5年。

十一、使用記錄、軌跡資料及證據保存

本公司（或民宿）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(或民宿)如何保存，例如：個人資料使用查詢紀錄、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。）

十二、個人資料安全維護之整體持續改善方案

(一)本公司（或民宿）將隨時參酌業務及依據計畫執行狀況，注意相關社會輿情、技術發展、法令修正或其他因素，檢視所定安全維護計畫之合宜性，並予必要之修正。

(二)針對個資安全稽核結果有不合法令之虞者，規劃改善與預防措施並納入安全維護計畫。

交通部指定觀光產業類個資檔案安全維護計畫

十三、業務終止後之個人資料處理方法

本公司（或民宿）業務終止後，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5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；儲存於電腦磁碟及其他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：(請自行填寫)

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)：

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○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、時間或地點請自行填寫)：

交通部指定觀光產業類個資檔案安全維護計畫

十四、委託作業（如未委託他人則可以選擇加以刪除）

本公司（或民宿）委託他人蒐集、處理或利用個人資料之全部或一部時，應依個人資料保護法施行細則第八條規定對受託人為適當之監督，並於委託契約或相關文件中，明確約定其內容，以及採取下列方式辦理：

- 一. 選擇受託人前，應確認需要委外的範圍，並以適當評估方式選擇具適當個資安全維護能力的受託人。
- 二. 應與受託人締結委託契約，要求受託人依本公司（或民宿）應適用之個資管理規定執行契約。
- 三. 於委託契約或相關文件明確約定適當之監督事項及方式。
- 四. 要求受託者僅得於本公司（或民宿）指示之範圍內，蒐集、處理或利用個人資料。
- 五. 要求受託者認本公司（或民宿）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，應立即通知本公司（或民宿），並於契約中訂定委外廠商於知悉資通或個資安全事件情況時，應即向本公司（或民宿）權責人員或通報窗口，以指定之方式進行通報。
- 六. 對受託者應定期查核受託者執行之狀況，並將確認結果記錄之。（如委外查核報告以及查核缺失追蹤情形）
- 七. 委託關係終止或解除時，受託者應將個人資料載體之返還或將個人資料刪除。



總複習-有效性量測

重點複習

- 個資法核心三動詞為：_____、_____、_____。
- 個資管理制度的方法論為：_____、_____、_____、_____。
- 同意是由個資的_____來舉證。
- 觀光產業保有消費者個資達_____者，應訂定安維計畫。
- 特種個資原則上不得蒐集、處理、利用，除非取得個資當事人_____的同意。
- 2023年修正個資法，最高罰鍰金額為：_____。
- 公司應提供當事人首次_____拒絕行銷的管道。
- 委託方需要對受託方進行適當之_____義務。



“ 如有任何疑問 歡迎與我們聯繫



Phone

專線服務：(02) 6631-1069



Email

TIIPAS信箱：tpipas@iii.org.tw



TIIPAS官網



<https://www.tpipas.org.tw/>