

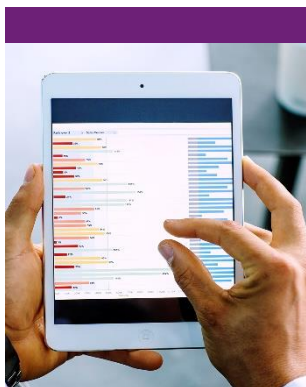
# 不動產經紀業所應知悉的 個人資料保護遵循重點

講師：KPMG 安侯企管 李冠樟

# 大綱

## 01

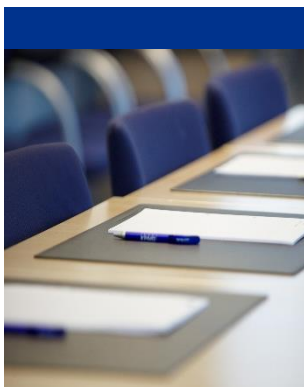
不動產經紀業  
個人資料管理  
稽核表實務做  
法說明



3

## 02

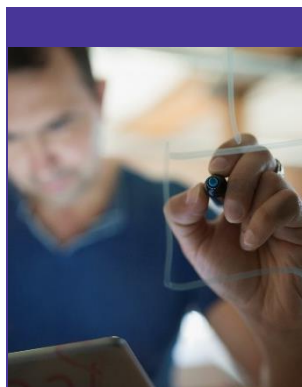
個人資料達一萬  
筆以上者應採取  
之資訊安全措施  
相關說明



13

## 03

個人資料檔案  
盤點與風險評  
估說明



20

## 04

問題與討論



50

# 1.不動產經紀業個人資料 管理稽核表實務做法說明



# 不動產經紀業個人資料管理內部自主稽核檢核表

稽核項目	依據 條文	說明
<b>一、管理人員及資源</b>		
(一)是否至少配置1名管理人員，負責規劃、訂定修正與執行個人資料檔案安全維護計畫（以下簡稱安維計畫）及業務終止後個人資料處理方法（以下簡稱處理方法）等相關事項，並定期向負責人提出報告？	第5條第1項	業者應指定至少1名管理人員並提出定期向負責人提出報告之證明文件。
(二)是否訂定個人資料保護管理政策，並公告於營業處所適當之處或網站，使其所屬人員及個人資料當事人均能知悉？	第5條第2項	業者應提供個人資料保護管理政策文件及於營業處所或網站揭示之相片或截圖。
<b>二、個人資料之範圍界定與清查</b>		
是否定期查核確認所保有之個人資料現況，並界定納入安維計畫及處理方法之範圍？	第6條	業者應提供所保有之個人資料現況、界定納入安維計畫及處理方法之範圍及定期查核紀錄。
<b>三、風險評估及管理機制</b>		
是否就所界定之個人資料範圍及其蒐集、處理、利用個人資料之流程，評估可能產生之個資風險並根據風險評估之結果，訂定適當之管控機制？	第7條	業者應提供個資風險評估及管控措施文件。

# 不動產經紀業個人資料管理內部自主稽核檢核表

稽核項目	依據 條文	說明
<b>四、事故之預防、通報及應變機制</b>		
(一) 是否已建立並執行個人資料事故之應變、通報及預防機制，包括個人資料事故發生後「應採取之各類措施」、「應受通報之對象及其通報方式」及「矯正預防措施之研議機制」？	第8條第1項	業者應提供符合規定之應變、通報及預防機制文件
(二) 所建立的應變措施，是否包含「控制當事人損害之方式」、「查明個人資料事故後通知當事人之適當方式」及「應通知當事人個人資料事故事實、所為因應措施及諮詢服務專線」？	第8條第1項	業者應提供符合規定之應變措施文件。
(三) 是否訂定並執行個人資料事故達1,000筆以上時，應於發現後72小時內，以書面通報地方主管機關，並副知內政部之機制？	第8條第2項	業者可提供相關流程規範
<b>五、個人資料蒐集、處理及利用之內部管理程序</b>		
(一) 是否告知所屬人員，執行業務蒐集、處理一般個人資料時，應檢視是否符合個人資料保護法（以下簡稱本法）第19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20條第1項但書情形？	第9條	業者可提供相關流程規範並應提供已要求所屬人員確實辦理，或依規定執行之切結文件。

# 不動產經紀業個人資料管理內部自主稽核檢核表

稽核項目	依據條文	說明
(二)蒐集個人資料時，是否遵守本法第8條及第9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？	第10條	業者可提供符合規定之相關流程規範。並應提供已要求所屬人員確實辦理或依規定執行之切結文件。
(三)是否訂定並執行利用個人資料行銷時，明確告知當事人所屬公司（商號）名稱之規範？	第 11 條 第1項	業者可提供符合規定之相關流程規範。並應提供已要求所屬人員、加盟店、直營店、聯賣業者，確實辦理或依規定執行之切結文件。
(四)是否訂定並執行加盟經營者利用個人資料行銷時應告知加盟品牌名稱及公司（商號）名稱之規範？	第 11 條 第1項	
(五)是否訂定並執行利用個人資料行銷時，提供當事人免費表示拒絕接受行銷方式之規範？	第 11 條 第2項	
(六)是否訂定並執行當事人表示拒絕接受行銷時，應立即停止利用其個人資料行銷之規範？	第 11 條 第3項	
(七)是否訂定並執行當事人表示拒絕接受行銷之日起7日內，直營店應通知總公司（商號）彙整後再周知所屬各部門之規範？	第 11 條 第4項及 第5項	
(八)是否訂定並執行當事人表示拒絕接受行銷之日起7日內，加盟店應通知內部其他業務人員，其有上傳加盟總部者，亦應併同通知加盟總部之規範？	第 11 條 第4項及 第5項	
(九)是否訂定並執行當事人表示拒絕接受行銷之日起7日內，涉有參與聯賣服務者，應通知其他聯賣業者之規範？	第 11 條 第4項及 第5項	

# 不動產經紀業個人資料管理內部自主稽核檢核表

稽核項目	依據條文	說明
(十)是否訂定並執行中央主管機關對經紀業為限制國際傳輸個人資料之命令或處分時，通知所屬人員遵循辦理之規範？	第 12 條 第1項	業者可提供符合規定之相關流程規範。並應提供已要求所屬人員確實辦理或依規定執行之切結文件。
(十一)是否訂定並執行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之規範？	第 12 條 第2項	業者可提供符合規定之相關流程規範。並另提供告知當事人之個人資料所欲國際傳輸之區域之相關證明資料。如無則免提供。
(十二)是否訂定並執行將個人資料作國際傳輸時，對資料接收方為下列事項之監督之規範 1. 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。 2. 當事人行使本法第3條所定權利之相關事項。	第 12 條 第2項	業者應提供傳輸前，提醒資料接收方受監督事項之文件。
(十三)是否訂定並執行受理當事人依本法第3條行使個資各項權利時，應提供當事人行使個資各項權利時之聯絡窗口、聯絡方式之規範？	第 13 條 第1款	業者可提供符合規定之相關流程規範或教材。並應提供已要求所屬人員確實辦理或依規定執行之切結文件。
(十四)是否訂定並執行受理當事人依本法第3條行使個資各項權利時，應驗證申請人身分為當事人本人或經授權之代理人之機制？	第 13 條 第2款	業者可提供符合規定之相關流程規範或教材。並應提供已要求所屬人員確實辦理或依規定執行之切結文件。

# 不動產經紀業個人資料管理內部自主稽核檢核表

稽核項目	依據 條文	說明
(十五)除有妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益、本公司(商號)或第三人之重大利益等情形外，是否有依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本(本法第10條但書)？同意或拒絕當事人行使權利之事由，是否於法定期限內或法定延長期限內以書面通知當事人(15/30天)？	第 13 條 第3款及 第5款	業者應提供實際案例回復文件(並檢視是否於法定期限內以書面通知或制式空白回復文件。
(十六)是否訂定並執行個人資料正確性有爭議時，應主動或依當事人之請求停止處理或利用之規範？未主動或未依當事人之請求停止處理或利用時(本法第11條第2項但書)，是否係因執行業務所必須或經當事人書面同意，並經註明其爭議？同意或拒絕當事人行使權利之事由，是否於法定期限內或法定延長期限以書面通知當事人(本法第13條：30/60天)？	第 13 條 第3款及 第5款	業者應提供當事人書面同意書、實際案例回復文件(並檢視是否於法定期限內以書面通知)或制式空白回復文件。
(十七)個人資料蒐集之特定目的消失或期限屆滿時，未主動或未依當事人之請求，刪除、停止處理或利用該個人資料時(本法第11條第3項但書)是否係因執行業務所必須或經當事人書面同意？同意或拒絕當事人行使權利之事由，是否於法定期限內或法定延長期限內以書面通知當事人(本法第13條：30/60天)？	第 13 條 第3款及 第5款	業者應提供當事人書面同意書、實際案例回復文件(並檢視是否於法定期限內以書面通知)或制式空白回復文件。
(十八)是否有訂定並執行當事人查詢、請求閱覽個人資料或製給複製本，有收取必要成本費用者，應告知當事人收費基準之規範？	第 13 條 第4款	業者可提供實際案例經當事人署名之告知文件或制式空白告知文件(含當事人簽名欄)，或經所屬人員切結執行之流程規範。
(十九)委託他人蒐集、處理或利用個人資料之全部或一部時，是否依本法施行細則第8條規定，與受託者明確約定相關監督事項及方式，並為適當之監督？	第 21 條 第1項及 第2項	業者應提供與受託者明確約定相關監督事項之文件。



# 不動產經紀業個人資料管理內部自主稽核檢核表

稽核項目	依據 條文	說明
<b>六、資料安全管理及人員管理</b>		
(一)是否依據業務需求，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？	第15條第2項 第1款	業者應提供所屬人員存取權限定期設定文件。
(二)是否檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程及其負責人員？	第15條第2項 第2款	業者應提供依業務性質制定之流程及其負責人員之規範文件。
(三)是否明定所屬人員應妥善保管個人資料之儲存媒介物並約定保管及保密義務？	第15條第2項 第3款	業者應提供與所屬人員約定儲存媒介物保管及本項約定之切結書。
(四)是否明定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，並簽訂保密切結書？	第15條第2項 第4款	業者應提供與所屬人員本項約定之切結書
(五)使用資通訊系統蒐集、處理或利用消費者個人資料達1萬筆以上時，是否採取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？	第16條第1項 第1款至第4 款	業者應提供相關機制文件。
(六)使用資通訊系統蒐集、處理或利用消費者個人資料達1萬筆以上時，是否有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，並進行定期演練及檢討改善	第16條第1項 第5款及第6 款、第2項	業者應提供相關機制文件及定期演練紀錄及檢討改善等文件。

# 不動產經紀業個人資料管理內部自主稽核檢核表

稽核項目	依據 條文	說明
<b>七、認知宣導及教育訓練</b>		
(一)是否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？	第17條	業者可提供相關宣導及教育訓練資料。
(二) 所屬人員是否均已完成訓練或取得宣導資料，並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？	第17條	業者可提供所屬人員考試成績或參訓人員名冊或切結書等。
<b>八、設備安全管理</b>		
(一)所蒐集保管之個人資料檔案，是否就存放或處理現有各種不同個人資料媒體型態（包含紙本、電腦、自動化機器或其他存放媒介物）之設備採取必要適當之安全設備或防護措施？	第 14 條 第 1 項及第2項	業者可現場展示安全設備或防護措施。例如保險櫃及安全防護或加密機制等。
(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，是否配置安全防護系統或加密機制？	第 14 條 第 2 項第2款	業者可現場展示。
(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，是否採取適當之銷毀或防範措施？	第 14 條 第 2 項第3款	業者可提供個資存放媒介物等報廢汰換或轉作其他用途時之措施或流程規範、文件。
(四) 委託他人蒐集、處理或利用個人資料之全部或一部或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，委託他人執行者，是否依個資法施行細則第8條規定，與受託者明確約定相關監督事項並為適當之監督。	第 14 條 第 2 項 第 3 款 及 第21條	業者可提供委託他人蒐集、處理或利用個人資料、或委託他人將個人資料存放媒介物執行報廢汰換或轉作其他用途時，與受託者明確約定相關監督事項之文件。

# 不動產經紀業個人資料管理內部自主稽核檢核表

稽核項目	依據 條文	說明
<b>九、資料安全稽核機制</b>		
(一)是否依業務規模及特性，衡酌經營資源之合理分配訂定個人資料安全維護稽核機制，並指定適當人員每半年至少進行一次安維計畫及處理方法執行情形之檢查？	第18條第1項	業者應指定適當人員並提供至少每半年1次安維計畫及處理方法執行情形之稽核紀錄。
(二)是否將檢查結果向負責人提出報告，並由公司(商號)負責人於紀錄確認。上開相關紀錄並應留存至少五年？	第18條第2項	業者可提供負責人簽名之稽核紀錄文件。
(三)檢查結果發現安維計畫及處理方法不符法令或有不符法令之虞時，是否立即改善？	第18條第3項	業者可提供不符時之改善文件，無不符之情形者免提供。經查有不符之情形者，應立即改善。
<b>十、使用紀錄、軌跡資料及證據保存</b>		
(一)是否記錄個人資料使用情況，並留存軌跡資料或相關證據。	第19條第1項	業者可提供個人資料刪除、停止處理或利用之方法、時間或地點之程序、措施等機制或文件。
(二)個人資料蒐集之特定目的消失或期限屆滿，刪除、停止處理或利用所保有之個人資料時，是否記錄個人資料之刪除、停止處理或利用之方法、時間或地點？其軌跡資料或其他相關證據及紀錄是否留存至少5年？	第19條第2項第1款及第3款	業者可提供個人資料刪除、停止處理或利用之方法、時間或地點之程序、措施等機制之文件。
(三)個人資料蒐集之特定目的消失或期限屆滿時，將停止處理或利用之個人資料移轉其他對象者，是否記錄其移轉之原因、對象、方法、時間、地點，及該對象蒐集處理或利用之合法依據等相關證據？其軌跡資料或其他相關證據及紀錄是否留存至少5年？	第19條第2項第2款及第3款	業者可提供符合規定之相關流程規範。業者可提供個人資料移轉其他對象時之措施、流程規範文件。

# 不動產經紀業個人資料管理內部自主稽核檢核表

稽核項目	依據 條文	說明
<b>十一、個人資料安全維護計畫與整體持續改善</b>		
(一)是否依公司(商號)之規模、特性、保有個人資料之性質及數量等事項，訂定適當之安維計畫？	第4條	檢視所訂之安維計畫是否適當
(二)是否隨時參酌業務及本公司所訂安維計畫及處理方法執行狀況、社會輿情、技術發展及相關法規訂修等因素，檢討所定安維計畫及處理方法，必要時予以修正？是否於規定時間內將修正後之安維計畫及處理方法報請所在地直轄市、縣(市)主管機關備查？	第 20 條 及 第 23 條	檢視安維計畫是否依相關因素進行訂修，並於規定時間內報備查。
(三)是否訂定業務終止後，所保有個資銷毀之方法、時間、地點及證明銷毀之方式；移轉時其移轉之原因對象、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；或其他刪除、停止處理或利用之方法、時間或地點；上開軌跡資料、相關證據及紀錄應至少留存五年？	第22條	業者可提供符合規定之相關流程規範。並檢視處理方法是否依規定訂定。



## 2.個人資料達一萬筆以上者應採取之資訊安全措施 相關說明

# 使用資通訊系統蒐集、處理或利用消費者個人資料達一萬筆以上者，應採取之資訊安全措施相關說明



依據內政部指定地政類非公務機關個人資料檔案安全維護管理辦法第16條規定：「非公務機關使用資通訊系統蒐集、處理或利用消費者個人資料達一萬筆以上者，應採取下列資訊安全措施：一、使用者身分確認及保護機制。二、個人資料顯示之隱碼機制。三、網際網路傳輸之安全加密機制。四、個人資料檔案及資料庫之存取控制與保護監控措施。五、防止外部網路入侵對策。六、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。」是以，公司（商號）有使用資通訊系統蒐集、處理或利用消費者個人資料達一萬筆以上之情形者，該資通訊系統應至少有上開六項資訊安全措施。

# 適當安全維護管理措施(續)




資訊系統

## 第十六條

非公務機關使用資通訊系統蒐集、處理或利用消費者個人資料達一萬筆以上者

應採取下列資訊安全措施：

- 一、使用者身分確認及保護機制。
- 二、個人資料顯示之隱碼機制。
- 三、網際網路傳輸之安全加密機制。
- 四、個人資料檔案與資料庫之存取控制及保護監控措施。
- 五、防止外部網路入侵對策。
- 六、非法或異常使用行為之監控及因應機制。

 前項第五款及第六款所定措施，應定期演練及檢討改善。

# 六大應採取之資訊安全措施

項目	資訊安全措施	實作說明
一	使用者身分確認及保護機制	系統應建立帳號管理機制，包含帳號申請、建立、修改、啟用、停用及刪除之程序，並執行身分驗證管理，如身分驗證資訊不以明文傳輸、密碼複雜度或帳號鎖定機制等。
二	個人資料顯示之隱碼機制	系統界面呈現個人資料時，應以適當且一致性之隱碼或遮罩處理，以避免過多且非必要之個人資料揭露，可參考 <b>CNS 29191</b> 「資訊技術 - 安全技術 - 部分匿名及部分去連結鑑別之要求事項」國家標準。
三	網際網路傳輸之安全加密機制	個人資料傳輸時，應採用傳輸加密機制，如採用加密傳輸通道、使用公開、國際機構驗證且未遭破解之演算法。
四	個人資料檔案及資料庫之存取控制與保護監控措施	儲存於電子媒體及資料庫之個人資料，應適當加密保護，並提供使用者識別、鑑別及身管理，並採用最小權限原則進行存取控制管理。
五	防止外部網路入侵對策	針對外部入侵之防禦，應採用適當資安控制措施建立防禦縱深，包括防毒軟體、防火牆、入侵偵測與防禦系統，及應用程式防火牆等。
六	非法或異常使用行為之監控與因應機制	針對系統或個人資料檔案之存取，應確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件，且應留存系統相關日誌紀錄並定期檢視，或設置適當監控及異常行為預警機制。



# 使用者身分確認及保護機制

1. 實務上常建立已加密之安全通道(如HTTPS 與 VPN 等)保護傳輸資料之機密性。
2. 密碼長度至少8個字元以上、大小寫英文與數字及特殊符號4取3、密碼每90天需變更一次、變更3次內之密碼不得重複、5次不正確的登入嘗試須鎖定帳號15分鐘

## 使用公開、國際機構驗證且未遭破解之演算法

SSL V3 及TLS1.0 皆已被視為安全性不足，若無相容性問題，建議停用。110年3月，RFC 8996 標準[10]正式棄用TLS1.0 及TLS1.1。對IE、Edge、Chrome、Safari 及Firefox 而言，目前皆建議網站採用TLS 1.2，而網頁連線也以TLS 1.2 為主。另外，加密協定所使用的演算法(Ciphers)亦有安全考量，如RC2、RC4、DES及3DES 等加密演算法已遭破解，建議可改用AES 與RSA 等尚未遭破解之加密演算法。

# 非法或異常使用行為之監控與因應機制

- ✓ 實務上建議可包含(但不限於)以下系統事件：
  - 管理者行為(如調整系統組態、異動系統帳號等)
  - 身分驗證失敗(如帳號登入失敗、觸發帳戶鎖定等)
  - 存取資源失敗(如頁面失效、資料庫連線失敗等)
  - 功能錯誤(如系統功能無法使用、帳戶無法登入等)
  - 重要資料異動(如存取個人資料或機敏性資料等)
  - 重要操作行為(如變更個人密碼、金融轉帳交易等)
  
- ✓ 建議資通系統日誌留存期限應至少保留**6個月**

# 3.個人資料檔案盤點與風險 評估說明



# 個人資料盤點清冊欄位說明

## • 應用步驟：

1. 製作「個人資料盤點清冊」
2. 盤點與建立「個人資料檔案基本資訊」與「資料流」
3. 審視與分析「個人資料項目」、「其它可識別個資」與個資保存項目

個資作業流程識別			個人資料檔案基本資訊									資料流						
編號	主流程名稱	子流程名稱	個人資料檔案名稱	檔案型態	當事人	保有依據	特定目的	個人資料類別	§17對外公告	主管單位	保有單位	組織身分	組織身分補充欄位	資訊來源	蒐集者	蒐集介面	是否告知	組織內部提供者

資料流					個人資料項目(Y:必填欄位/O:選填欄位/N:無該欄位)																	
組織內部接收者	委外廠商	供應者	第三方	國際傳輸	姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	職業	聯絡方式	財務情況	病歷	醫療	基因	性生活	健康檢查	犯罪前科

其它可識別個資		保護方式	保存					備註	盤點單位名稱	
其他直接識別	其他間接識別	控制措施	儲存位置	複本、備份或異地備援位置	法定保存期限	自訂保存期限	刪除或銷毀方式		子部門名稱	部門名稱

# 盤點實務概述 - 「個資作業流程識別」

個資作業流程識別				個人資料檔案基本資訊									資料流					
編號	主流程名稱	子流程名稱	個人資料檔案名稱	檔案型態	當事人	保有依據	特定目的	個人資料類別	§17對外公告	主管單位	保有單位	組織身分	組織身分補充欄位	資訊來源	蒐集者	蒐集介面	是否告知	組織內部提供者

## • 業務或服務作業流程

- **編號**：自定序號。
- **主流程名稱**：可參考單位的部門職責內容、業務項目、服務目錄、日常作業流程等方式，列出主要的服務項目或作業流程類別。
- **子流程名稱**：前項服務項目或作業流程類別之內容，若包含一項以上之服務細項或細部作業，可再個別區分成單一項目。
- **個人資料檔案名稱**：命名可供單位識別之個人資料檔案名稱。

# 盤點實務概述 - 「個人資料檔案基本資訊」(1/4)

個資作業流程識別			個人資料檔案基本資訊									資料流						
編號	主流程名稱	子流程名稱	個人資料檔案名稱	檔案型態	當事人	保有依據	特定目的	個人資料類別	§17對外公告	主管單位	保有單位	組織身分	組織身分補充欄位	資訊來源	蒐集者	蒐集介面	是否告知	組織內部提供者

## • 個人資料檔案基本資訊

- 檔案型態：可分為1.紙本類、2.電子類、3.電子檔-可攜式媒體、4.系統資料庫，不同檔案型態分開列。
- 當事人：組織所蒐集個資的對象，例如：客戶/消費者(自然人)、法人之負責人、法人之聯絡人、廠商之相關人員、正職員工/聘僱員工/派遣員工、其他人員(不在上述定義中之人員，如利害關係人等)。
- 保有依據：是否有蒐集個資的法定合法基礎，或是組織自定之保有依據。
- 特定目的：參考法務部公告之「個人資料保護法之特定目的及個人資料之類別」，可複選。
- 個人資料類別：參考法務部公告之「個人資料保護法之特定目的及個人資料之類別」，可複選。

# 個資檔案的型態

## 紙本類

申請書、表單、報表、盤點表、契約及檢附文件等紙本檔案。



## 電子檔-可攜式媒體

數位形式文件如保存於可攜式媒體。



## 電子類

文書處理檔案、掃描檔、照片檔、影像檔及錄音檔等電子檔案。



## 系統資料庫

指個人資料僅保存於資訊系統內，未另外列印成紙本或另存成電子檔案。

# 盤點實務概述 - 「個人資料檔案基本資訊」(2/4)

個資作業流程識別			個人資料檔案基本資訊										資料流					
編號	主流程名稱	子流程名稱	個人資料檔案名稱	檔案型態	當事人	保有依據	特定目的	個人資料類別	§17對外公告	主管單位	保有單位	組織身分	組織身分補充欄位	資訊來源	蒐集者	蒐集介面	是否告知	組織內部提供者

## • 個人資料檔案基本資訊

- **個人資料類別**：參考法務部公告之「個人資料保護法之特定目的及個人資料之類別」，可複選。
- **對外公告**：依據組織內部已規範的對外公告屬性，判斷所盤點的個人資料檔案，是否須對外公告。(如由個資當事人提供之資料或其可申請/查閱之資料應填「Y」；若為內部作業自行產生者則填「N」)
- **主管單位**：各業務主管部門或個資檔案之規劃部門(負責制定該個人資料檔案項目與欄位之部門)。  

**個資法施行細則第5條**  
個人資料檔案，包括備份檔案。
- **保有單位**：主要負責保存管理該個人資料檔案項目之部門。

# 範例

個資作業流程識別			個人資料檔案基本資訊								
編號	主流程名稱	子流程名稱	個人資料檔案名稱	檔案型態	當事人	保有依據	特定目的	個人資料類別	§17對外公告	主管單位	保有單位
1	客服作業	客訴	客服錄音檔	電子檔(錄音檔)	客戶(賣方)	契約	○九○消費者、客戶管理與服務	C○○一 辨識個人者 C○三一 住家及設施 C○三二 財產	Y	客服部	業務部/ 客服部



# 盤點實務概述 - 「個人資料檔案基本資訊」(3/4)

## 個人資料保護法之特定目的 (摘錄)

代號 特定目的項目

〇〇三 入出國及移民

〇〇四 土地行政

〇一五 戶政

〇二三 民政

〇二七 立法或立法諮詢

〇三二 刑案資料管理

〇三九 行政裁罰、行政調查

〇四二 兵役、替代役行政

〇四五 災害防救行政

一五七 調查、統計與研究分析

=====

〇〇二 人事管理(包含甄選、離職及所屬員工基本資訊、現職、學經歷、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、差勤、福利措施、褫奪公權、特殊查核或其他人事措施)

〇一四 公職人員財產申報、利益衝突迴避及政治獻金業務

〇七七 訂位、住宿登記與購票業務

一〇九 教育或訓練行政

一〇七 採購與供應管理

# 盤點實務概述 - 「個人資料檔案基本資訊」(4/4)

## 個人資料之類別 (摘錄)

### 代 號 識別類：

C〇〇一 辨識個人者。

例如：姓名、職稱、住址、工作地址、以前地址、住家電話號碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊及戶籍地址、相片、指紋、電子郵遞地址、電子簽章、憑證卡序號、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及其他任何可辨識資料本人者等。

C〇〇三 政府資料中之辨識者。

例如：身分證統一編號、統一證號、稅籍編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等。

---

### 代 號 特徵類：

C〇一一 個人描述。

例如：年齡、性別、出生年月日、出生地、國籍、聲音等。

C〇一二 身體描述。

例如：身高、體重、血型等。

---

### 代 號 家庭情況：

C〇二一 家庭情形。

例如：結婚有無、配偶或同居人之姓名、前配偶或同居人之姓名、結婚之日期、子女之人數等。

C〇二二 婚姻之歷史。

例如：前次婚姻或同居、離婚或分居等細節及相關人之姓名等。

# 盤點實務概述 - 「資料流」

個資作業流程識別			個人資料檔案基本資訊									資料流						
編號	主流程名稱	子流程名稱	個人資料檔案名稱	檔案型態	當事人	保有依據	特定目的	個人資料類別	§17對外公告	主管單位	保有單位	組織身分	組織身分補充欄位	資訊來源	蒐集者	蒐集介面	是否告知	組織內部提供者

## • 資料流

- **組織身分**：依照盤點單位對該個人資料檔案之角色，選取"資料控制者"、"資料處理者"或"共同資料控制者"。
  - 資料控制者：可決定個人資料處理之目的與方法之自然人或法人、公務組織、辦事處或其他機構。
  - 資料處理者：代控制者處理個人資料之自然人或法人、公務組織、辦事處或其他機構。
  - 共同資料控制者：兩個或兩個以上資料控制者共同決定處理之目的及方式
- 若組織身分為資料處理者，請於組織身分補充欄位填寫該資料控制者之組織名稱。
- 若組織身分為共同資料控制者，請於組織身分補充欄位填寫另一共同資料控制者之組織名稱。

# 盤點實務概述 - 「資料流」(1/2)

個資作業流程識別			個人資料檔案基本資訊									資料流						
編號	主流程名稱	子流程名稱	個人資料檔案名稱	檔案型態	當事人	保有依據	特定目的	個人資料類別	§17對外公告	主管單位	保有單位	組織身分	組織身分補充欄位	資訊來源	蒐集者	蒐集介面	是否告知	組織內部提供者

## • 資料流

- **資訊來源(蒐集方式)**: 可分為**直接蒐集**、**間接蒐集**或**直接及間接蒐集**等方式。
- **蒐集者**：組織內負責蒐集該個人資料檔案的單位、人員或系統。
- **蒐集介面**：蒐集個人資料的作業型式(如：服務櫃臺、傳真、郵寄、網路...等)，可複選。→若從系統查詢後下載或輸出，可填寫「OO系統輸出」。
- **是否需告知**：如個人資料檔案為直接向當事人蒐集，請判斷是否符合個資法第8條所規定之免告知情形。
  - ✓ 依法律規定得免告知。
  - ✓ 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。
  - ✓ 告知將妨害公務機關執行法定職務。
  - ✓ 告知將妨害公共利益。
  - ✓ 當事人明知應告知之內容。
  - ✓ 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。

# 盤點實務概述 - 「資料流」(2/2)

資料流						個人資料項目(Y:必填欄位/O:選填欄位/N:無該欄位)												
組織內部提供者	組織內部接收者	委外廠商	供應者	第三方	國際傳輸	姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	教育	職業	聯絡方式	財務情況

## • 資料流

- 組織內部提供者：資料來源的內部單位；如無請以N/A表示。
- 組織內部接收者：資料交付出去的內部單位；如無請以N/A表示。
- 委外廠商：與該個資檔案之蒐集、處理及利用流程有關，且會接觸到個資內容之委外機構或人員，可複選。
- 供應者：與該個資檔案之蒐集、處理及利用流程有關，但不會接觸到個資內容之委外機構或人員(如：郵局、倉儲業者等)，可複選。
- 第三方：該個資檔案於組織外進行傳送的相關利害關係人對象與方式(如：人工傳送、公文袋、E-mail、網路共享、USB隨身碟、其他行動裝置...等)，可複選。
- 國際傳輸：該個資檔案會進行跨國(境)之傳輸，若無可空白，若有請註明傳輸之對象(地區)與方式，可複選。

# 範例

資料流											
組織身分	組織身分補充欄位	資訊來源(蒐集方式)	蒐集者	蒐集介面	是否需要告知	組織內部提供者	組織內部接收者	委外廠商	供應者	第三方	國際傳輸
資料控制者	N/A	直接蒐集	客服專員	客戶服務系統(CRM)	是	無	業務部	無	無	無	無



# 盤點實務概述 - 「個人資料項目」

個人資料項目(Y:必填欄位/O:選填欄位/N:無該欄位)

姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	職業	聯絡方式	財務情況	病歷	醫療	基因	性生活	健康檢查	犯罪前科
Y	O	N															

## • 個人資料項目

- 依據該對應之個人資料檔案項目內容，勾選所含有的個人資料欄位 (Y：代表必要填寫欄位，O：代表可選擇性填寫欄位，N：代表無此欄位)。
- 確認是否有包括特種個人資料欄位之蒐集。
- 檢視目前所蒐集之個人資料欄位內容，是否為處理和利用該個人資料檔案項目的特定目的所必須？
- 蒐集保有的個人資料欄位愈多 = 個資管理上的潛在風險愈高。
- 發掘未來個資保護與管理的改善機會點。

# 盤點實務概述 - 「其他可識別個資」、「保護方式」

其它可識別個資		保護方式	保存					備註	盤點單位名稱	
其他直接識別	其他間接識別	控制措施	儲存位置	複本、備份或異地備援位置	法定保存期限	自訂保存期限	刪除或銷毀方式		司/處/室名稱	科/室/組名稱

## • 其他可識別個資

- **其它直接識別**：雖然不在現有的個資欄位清單上，但屬於可以直接辨識該自然人之個資，不需與其它相關資料做連結、比對或參照，例如當事人的簽名、相片等均屬於此類。→本欄位若填Y，請在備註補充說明。
- **其它間接識別**：在個人資料檔案中可能只含有無法直接識別出特定當事人的個人資料，但可以經由組織內其他資料來源進行資料比對、連結或參照的方式，找出當事人的身分，則此資料就屬於可以間接方式識別該個人的資料，例如車號。→本欄位若填Y，請在備註補充說明。

## • 保護方式

- **控制措施**：依據法令法規或其他要求或考量，該個人資料檔案是否已落實其他控制措施處理(請參照個資管理控制措施表之內容選取填寫)，若無請填寫無。

# 個資管理控制措施表

項目	說明
門禁管理(上鎖、上保全)	機房、檔案室、庫房等設施(不含一般辦公室)需有鑰匙或保全卡方可進入
檔案櫃上鎖	將個資檔案存放於上鎖的檔案櫃
密封郵寄	實體郵件以密封的方式郵寄
登入系統需使用自然人憑證	登入系統時需使用自然人憑證
檔案加密	對電子檔、資料庫之資料、E-mail附件等檔案加密
傳輸加密	以SSL、IPSec、金鑰等方式加密傳輸
權限控管	系統(不含公文系統)、網站、共用資料夾設定權限分級
資料遮罩、隱碼	對個資進行遮罩，如:將身份證遮蔽為A12345XXXX、姓名遮蔽為王○明等
SOC監控	設有SOC監控機制
IDS/IPS偵測	設有IDS/IPS偵測機制
特定作業限制IP位址	特定的系統作業僅有特定的IP可以執行
定期抽查或清點個資檔案數正確性	於每週、每月、每年等週期，定期抽查個資檔案的數量或內容
與委外廠商簽訂保密契約	與委外廠商簽訂保密契約
稽核委外廠商	定期或不定期對委外廠商進行安全性稽核
其他	需說明其他控制措施是什麼項目

# 盤點實務概述 - 「保存」

其它可識別個資		保護方式	保存					備註	盤點單位名稱	
其他直接識別	其他間接識別	控制措施	儲存位置	複本、備份或異地備援位置	法定保存期限	自訂保存期限	刪除或銷毀方式		司/處/室名稱	科/室/組名稱

## • 保存

- **儲存位置**：該個人資料檔案之法定保存地點(如：辦公室檔案櫃、個人抽屜、電腦機房主機、資料庫主機...等)，可複選。  
✓ 若有自行保管情形，記得誠實撰寫，如：個人抽屜、個人電腦。
- **複本或備份或異地備援位置**：該個人資料檔案若有建立複本或備份或異地備援之保存地點，可複選。
- **法定保存期限**：若該個人資料檔案有法定保存期限(如：依據組織共通性檔案保存年限基準或其他法規，3年、7年...等)，請說明法令依據名稱與年限，若無請填寫無。
- **自訂保存期限**：該個人資料檔案組織自訂之保存期限，請列出內部規章名稱，若無請填寫無。
- **刪除或銷毀方式**：該個人資料檔案當要進行刪除或銷毀時，所須依據的作業手冊、程序、準則、表單...等，或執行方式簡略說明。

# 為何要進行個資風險評鑑 - 個資遭受侵害的衝擊性

Q：哪個名單較敏感？

名單	
姓名	分機
葉大雄	1234
王一生	1235
林至凌	1236
。	
。	
。	
。	
。	
。	
以上合計共10筆	



名單	
姓名	分機
王一生	0001
張小明	0002
葉大雄	0003
。	
。	
。	
。	
。	
。	
以上合計共1000筆	

個資數量的差異

# 為何要進行個資風險評鑑 - 個資遭受侵害的衝擊性

Q：哪個名單較敏感？



## 大樂透中獎名單

姓名	電話	地址
謝一元	09...	臺北..
張大明	09...	新北..
葉大雄	09...	高雄..

- 。
- 。
- 。
- 。
- 。

以上合計共10筆

## 染疫名單

姓名	電話	地址
王一生	09...	臺北..
張小明	09...	新北..
葉大雄	09...	台中..

- 。
- 。
- 。
- 。
- 。

以上合計共10筆

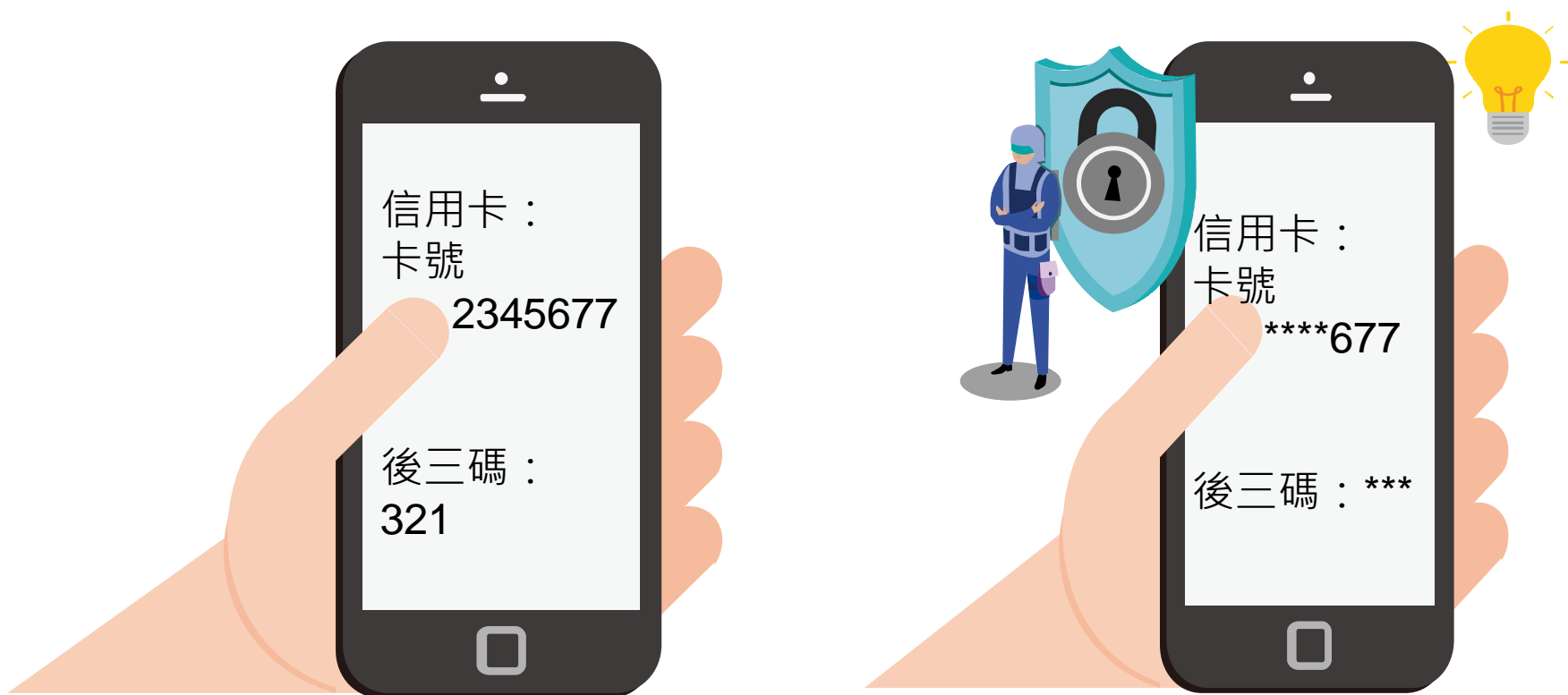
個資代表的意義  
不同



# 為何要進行個資風險評鑑 - 個資遭受侵害的衝擊性

Q：哪個較安全？

A：有適當保護措施與無適當保護措施的個資檔案，面臨的風險不相同



## 2. 個人資料保護法施行細則

### 第12條

公務機關應當針對個人資料實施適當的安全維護措施包含下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：



### 說明

- 一. 配置管理之人員及相當資源。
- 二. 界定個人資料之範圍。
- 三. 個人資料之風險評估及管理機制。**
- 四. 事故之預防、通報及應變機制。
- 五. 個人資料蒐集、處理及利用之內部管理程序。
- 六. 資料安全管理及人員管理。
- 七. 認知宣導及教育訓練。
- 八. 設備安全管理。
- 九. 資料安全稽核機制。
- 十. 使用紀錄、軌跡資料及證據保。
- 十一. 個人資料安全維護之整體持續改善。

# 個資流程衝擊分析表 八大構面



- 1 PII識別性個人識別資訊
- 2 個資數量
- 3 特種個資及自訂敏感性個資之項目數
- 4 個資存取方式
- 5 使用情境
- 6 個資檔案之存放位置
- 7 損害組織信譽
- 8 個資當事人隱私衝擊

➤ 衝擊值 = 衝擊構面值之總和

# 個資流程衝擊分析表 (1/3)

衝擊構面評分參考表：衝擊值= 所有衝擊構面之評分加總(8-40)

衝擊構面	評分(等級)		
	5	3	1
PII識別性	直接識別	間接識別	不易間接識別 (個資項目已遮罩)
個資數量 (取流程中數量最多之檔案為判斷依據)	大於100,000筆	50,000~100,000筆	小於50,000筆
敏感資料/保護機密性的義務	特種個資3種以上	特種個資1~2種	無特種個資

# 個資流程衝擊分析表 (2/3)

衝擊構面評分參考表(續)：衝擊值= 所有衝擊構面之評分加總(8-40)

衝擊構面	評分(等級)		
	5	3	1
個資存取方式	允許由組織外部連線存取個資；或允許攜離組織於外部使用	允許由未隔離外網之內部網路存取個資；或資料僅由個人保存，未集中保管	僅允許由隔離外網之內部網路存取個資；或個資存放於具調閱登記之檔案庫房
使用情境	使用全自動化方式，對當事人資料進行剖析、分析或判斷(automated decision-making)。	使用允許人工介入之半自動化方式，對當事人資料進行剖析、分析或判斷。	使用人工方式對當事人資料進行剖析、分析或判斷(automated decision-making)。
個資存取與存放位置	個資存取單位6個(含)以上或個資存放位置6處(含)	個資存取單位3~5個(含)或個資存放位置3~5處(含)	個資存取單位1~2個(含)或個資存放位置1~2處(含)

# 個資流程衝擊分析表 (3/3)

衝擊構面評分參考表(續)：衝擊值= 所有衝擊構面之評分加總(8-40)

衝擊構面	評分(等級)		
	5	3	1
損害組織信譽	若作業發生個資外洩事故，將導致組織形象、信譽受到非常嚴重損害，如：主管機關進行裁罰、國際性媒體報導負面新聞、民眾提起法律訴訟等情形。	若作業發生個資外洩事故，將導致組織形象、信譽受到嚴重損害，如：主管機關彈劾、糾舉或糾正、全國性媒體3日內(含)報導負面新聞、民眾至組織抗議或陳情等情形。	若作業發生個資外洩事故，將導致組織形象、信譽受到輕微損害，如：主管機關發函要求改善、1日內區域性媒體報導負面新聞、民眾電話或Email抱怨等情形。
個資當事人隱私衝擊	洩漏資訊，對個資當事人生命、財產造成影響，如：勒索、綁架、詐騙。	洩漏資訊，對個資當事人已有顯著影響，如：遭受騷擾、具名行銷。	洩漏資訊，造成個資當事人不愉快，未有其他實際損失



# 課程研討

Q：以下情況應如何評分？

衝擊構面	評分(等級)		
	5	3	1
PII識別性	直接識別	間接識別	不易間接識別 (個資項目已遮罩)
個資數量	大於100,000筆	50,000~100,000筆	小於50,000筆
敏感資料/ 保護機密性的 義務	特種個資3種以上	特種個資1~2種	無特種個資
個資存取方式	允許由組織外部連線存取個資； 或允許攜離組織於外部使用	允許由未隔離外網之內部網路存取個資； 或資料僅由個人保存，未集中保管	僅允許由隔離外網之內部網路存取個資； 或個資存放於具調閱登記之檔案庫房
使用情境	使用全自動化方式，對當事人資料進行剖析、分析或判斷 (automated decision-making)。	使用允許人工介入之半自動化方式，對當事人資料進行剖析、分析或判斷。	使用人工方式對當事人資料進行剖析、分析或判斷 (automated decision-making)。
個資存取與存放位置	個資存取單位6個(含)以上或個資存放位置6處(含)	個資存取單位3~5個(含)或個資存放位置3~5處(含)	個資存取單位1~2個(含)或個資存放位置1~2處(含)

# 個資流程風險評估表 (1/2)

作業流程名稱		潛在風險事件			衝擊值	風險事件發生可能性構面			風險事件發生的可能性	風險值
主流程名稱	子流程名稱	風險大分類	風險子分類	個資潛在風險事件		控制措施	稽核發現	經驗值	取控制措施、稽核發現及經驗值各自評分後取最大值。	風險值=個資作業流程衝擊值×風險事件發生可能性

- **風險分類、潛在風險事件**：依風險識別作業中「個資作業流程風險情境表」之識別結果帶入
- **衝擊值**：即「個資作業流程衝擊分析表」各構面衝擊評估值之總和
- **風險事件發生可能性**：依據已識別的風險情境，並針對個別個資潛在風險事件評估其發生可能性
- **風險值 = 個資作業流程衝擊值 × 風險事件發生可能性**

# 個資流程風險評估表 (2/2)

範例(僅為範例不代表作業與實際評估情況)：

主作業 流程名稱	子流程名 稱	潛在風險事件			衝擊值	風險事 件發生 可能性	風險值
		風險 主分 類	風險子 分類	個資潛在風險事件			
OO作業 流程	OO作業 流程	紙本 類	傳遞	紙本文件於內部傳遞、處理過程中，未適當簽收/點收或進行適當保護(備註)，致使個資遭遺失、窺伺、外洩或遭其他侵害。	11	3	33
教育訓 練	教育訓 練報名	電子 類	傳輸	個人資料更正或異動時，未有對應之紀錄(備註)，或紀錄未保存得宜及未適當保護，致使個資流程紀錄不完整。	9	3	27
OOO專 案資料	委外專 案管理 資料	處理 者作 業類	約定	組織與處理者明文約定中未明確規範，當資料逾保存期限或契約終止時，有關個人資料之銷毀、交還原組織或其他處理方式(備註)，致使個資外洩或受到不當處置。	18	5	90

# 個資作業流程風險評估表

## 風險事件發生可能性評分表

風險事件發生可能性構面				風險事件發生可能性
評分(等級)	控制措施	稽核發現	經驗值(主觀預期/內部經驗/業界經驗)	
5	控管嚴謹度低，例如：該風險情境無任何控制措施。	過去一年內，已2次內/外部稽核發現缺失者；或是內/外部稽核發現缺失，且尚未改正者。	發生可能性高；或是平均每季發生1次以上。	取控制措施、稽核發現及經驗值各自評分後取最大值
3	控管嚴謹度中等，例如：單一風險情境至少有1項控制措施。	過去一年內，內部或外部稽核發現缺失者。	發生可能性中等；或是平均每年發生1次以上但低於3次(含)。	
1	控管嚴謹度高，例如：單一風險情境有2項(含)以上之控制措施。	過去一年內，未曾被開過缺失者。	發生可能性低或無；或是平均每1~5年發生1次以下、或從未發生過。	
0	不適用	不適用	不適用	

# 九大風險情境說明


作業流程名稱		潛在風險事件			衝擊值	風險事件發生可能性構面			風險事件發生可能性	備註
主流程名稱	子流程名稱	風險大分類	風險子分類	個資潛在風險事件		控制措施	稽核發現	經驗值		



1. 紙本類



2. 電子類



3. 電子檔-可攜式媒體



4. 系統資料庫



5. 處理者作業類



6. 告知類



7. 控制者及處理者責任



8. 共同控制者責任



9. 跨境風險



# 感謝聆聽 問題與討論

