



達文西

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

國家通訊傳播委員會

通傳事業個資法遵教育訓練 及實務案例分享

- 價值1,500萬元的個資保護合規管理

達文西個資暨高科技法律事務所

王慕民 合夥律師

112年10月4日

合夥律師 王慕民



證照

- ◆ 中華民國律師(2011年~)
- ◆ BS 10012 個資管理系統主導稽核員
- ◆ Europrivacy 合格建置員

學歷

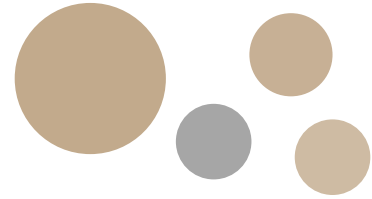
- ◆ 東吳大學 法律系在職專班科技法律組碩士
- ◆ 國立政治大學 法律系法學士

專業領域

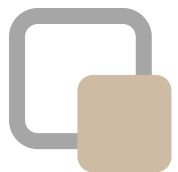
- ◆ 個資適法性查檢與矯正
- ◆ 個資管理制度建置
- ◆ 個資委外稽核
- ◆ 個資法律爭訟
- ◆ 個資法律顧問
- ◆ 個資法認知教育訓練

現任

- ◆ 達文西個資暨高科技法律事務所合夥律師



1 | 2023年個資法修正 - 違法責任有哪些？



112年3月2日-行政院「個資三箭」

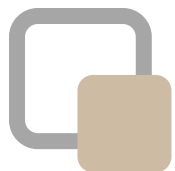
行政院第 3845 次會議

防止非公務機關個資外洩 精進措施

國家發展委員會

報告人：法制協調處楊淑玲處長

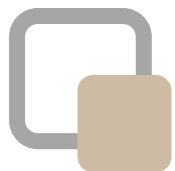
112 年 03 月 02 日



112年3月2日-行政院「個資三箭」

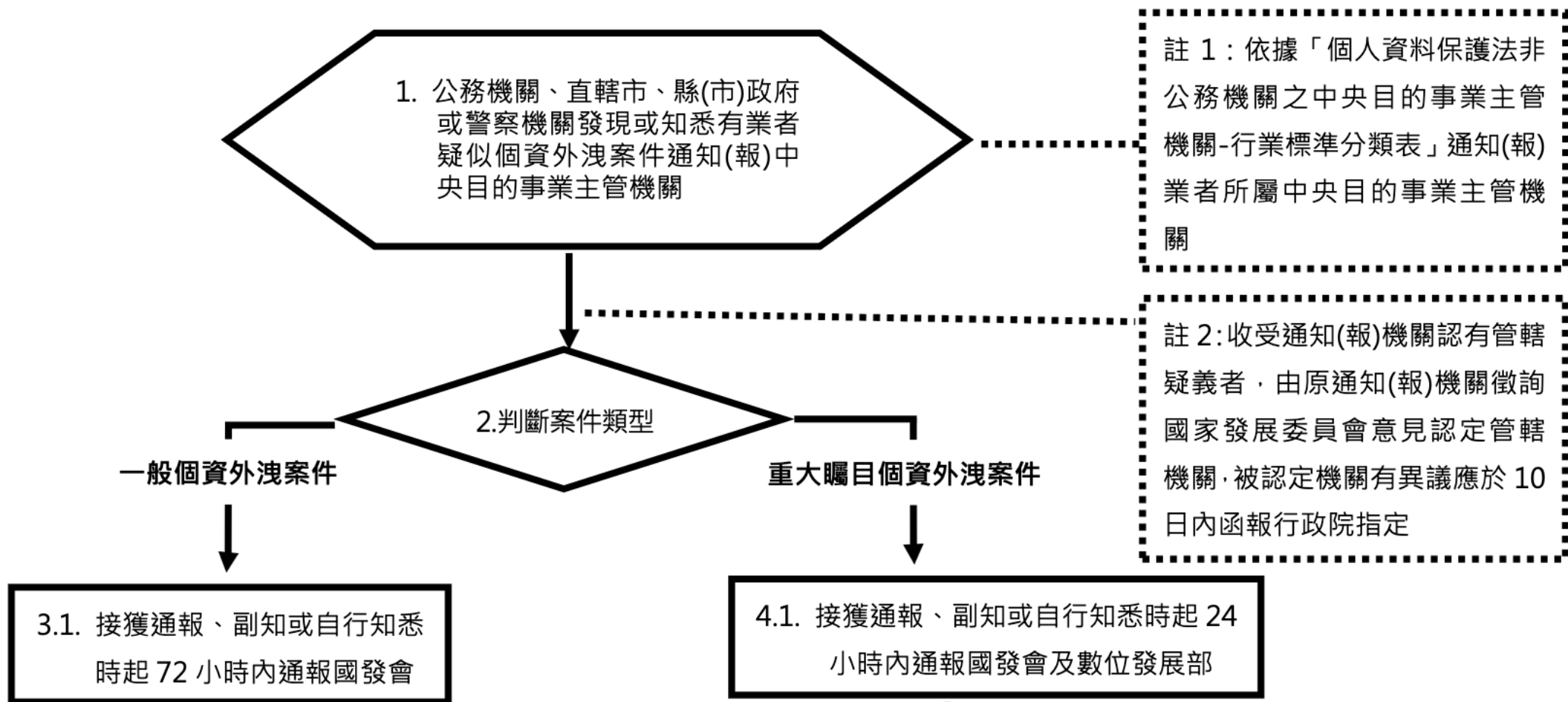


isniVoD

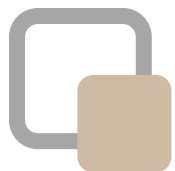


行政院及所屬各機關落實個人資料保護聯繫作業要點(112.05.29)

附件二、中央目的事業主管機關對個資外洩案件之行政調查流程圖

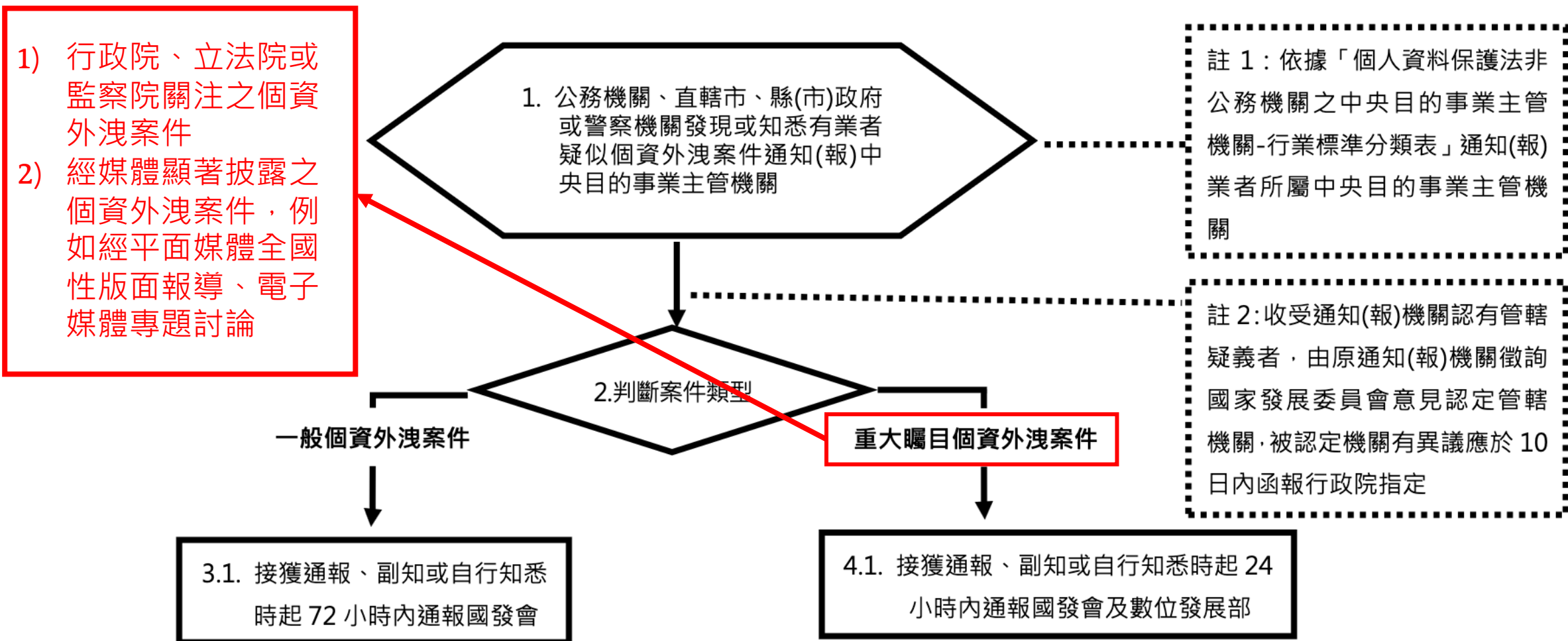


iswVod

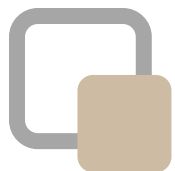


行政院及所屬各機關落實個人資料保護聯繫作業要點(112.05.29)

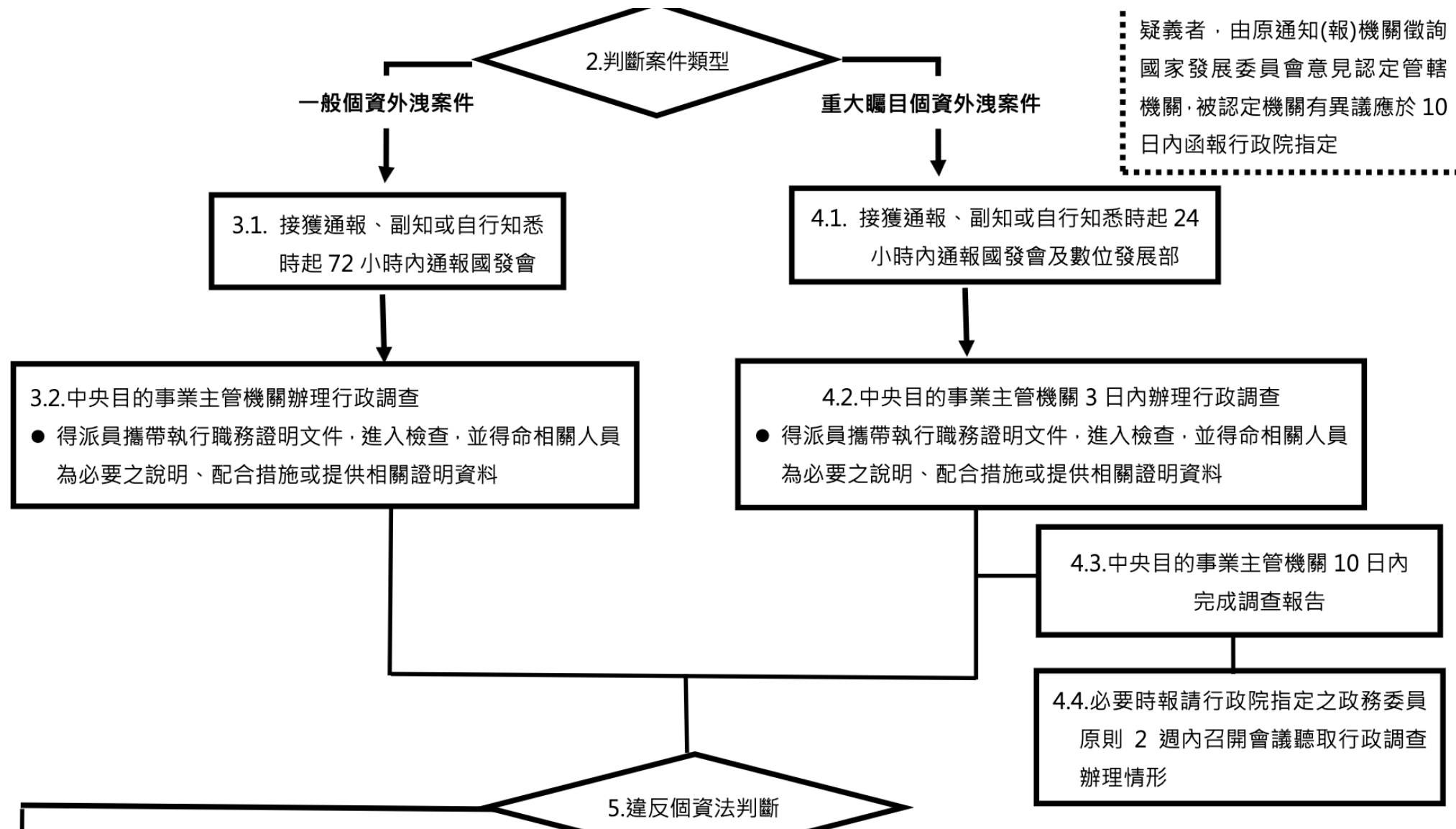
附件二、中央目的事業主管機關對個資外洩案件之行政調查流程圖

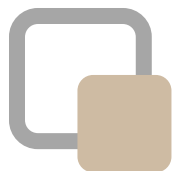


iswVod

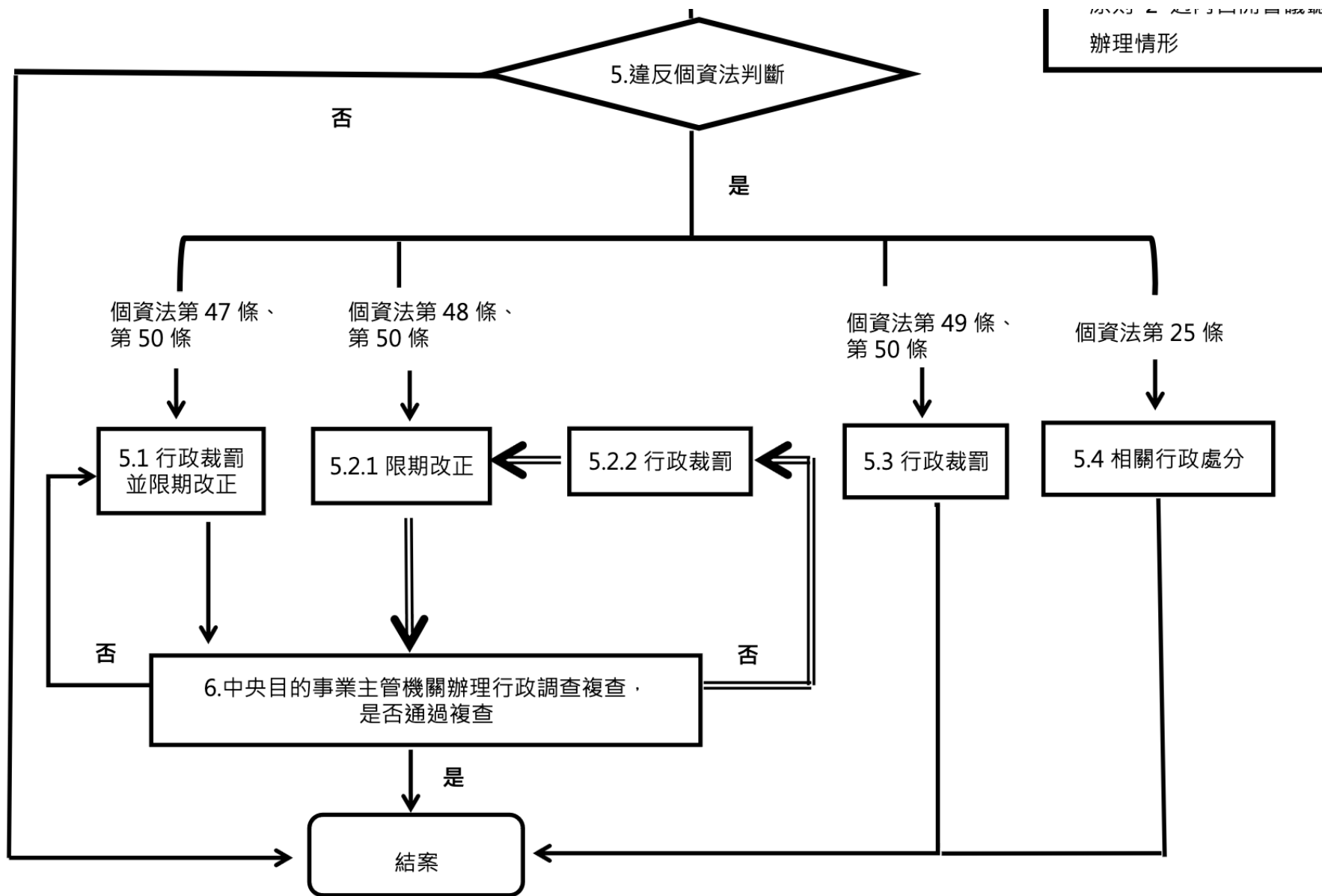


行政院及所屬各機關落實個人資料保護聯繫作業要點(112.05.29)

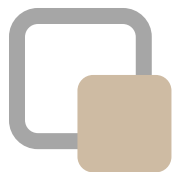




行政院及所屬各機關落實個人資料保護聯繫作業要點(112.05.29)



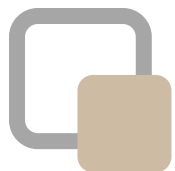
iswVod



112年3月2日-行政院「個資三箭」



isniVoD



民間企業的個資保護罰則過低？

華航個資外洩「林志玲、郭台銘」都在列？傳罰最高20萬 民航局未證實

2023-03-03 10:52 聯合報／記者周湘芸／台北即時報導



華航今年1月初收到匿名網路勒索信件，隨後有部分客戶個資被揭露於駭客網站，且名單涉航提供

+ 華航

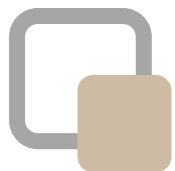
微風遭駭 90萬用戶個資外洩

2023-02-23 00:48 經濟日報／記者林海、馬瑞璿、何秀玲／台北報導

+ 資安



日前有人在駭客論壇聲稱竊得微風百貨的內部資料，微風表示，近日收到匿名網路勒索信件，第一時間立即啟動損害機制，目前內部資安團隊已完成軟體及作業系統安全性更新。記者曾學仁／攝影



重罰來了

iThome

新聞

產品&技術

專題

AI

Cloud

醫療IT

資安

研討會

社群

IT EXPLAINED

Q搜尋

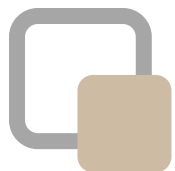
新聞

立院三讀通過個資法修法，企業外洩個資可直接開罰要求改善，最重可罰1,500萬元

個資法修正案通過後，未來企業違反安全維護義務的裁罰方式及額度將調整為，先開罰並命改正，情節嚴重者最重可罰1,500萬元。

文/ 蘇文彬 | 2023-05-16 發表

立法院今天（5/16）三讀通過個資法修正案，國發會指出，修正案加強對非公務機關違反安全維護義務，例如企業外洩個資事件，可直接開罰並限期改正，違反嚴重者最高可罰1,500萬元。另外，呼應各界要求設置獨立個資保護機關，行政院將儘速成立個資保護委員會籌備處。



個資法第48條^(112.5.16)

新個資法第48條 (112.05.16)

- i. 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期末改正者，按次處新台幣二萬元以上二十萬元以下罰鍰：
 - 一、違反第八條或第九條規定。
 - 二、違反第十條、第十一條、第十二條或第十三條規定。
 - 三、違反第二十條第二項或第三項規定。
- ii. 非公務機關違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法者，由中央目的事業主管機關或直轄市、縣（市）政府處新台幣二萬元以上二百萬元以下罰鍰，並令其限期改正，屆期末改正者，按次處新台幣十五萬元以上一千五百萬元以下罰鍰。
- iii. 非公務機關違反第二十七條第一項或未依第二項訂定個人資料處理方法，其情節重大者，處新台幣十五萬元以上一千五百萬元以下罰鍰，並令其限期改正，屆期末改正者，按次處罰。

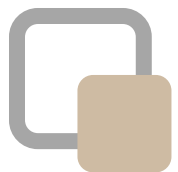
個資法第27條

第一項

非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第二項

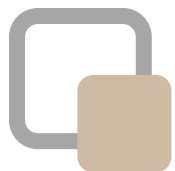
中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。



112年3月2日-行政院「個資三箭」



isniVoD



個資保護委員會來了

立法院三讀《成立個資保護委員會 企業外洩個資最重罰1500萬

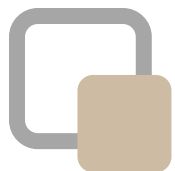
Newtalk新聞 | 政治 | 陳佩君台北市報導

發布 2023.05.16 | 14:41

 [分享](#)  [字級](#)  [追蹤](#)  [收藏](#)  [留言](#)

立法院今天三讀《個人資料保護法》修正案，《個資法》主管機關為「個人資料保護委員會」，專責監督個資問題。

國發會主委龔明鑫日前說明，個資法修法三讀通過後，最快8月可設「個人資料保護委員會」籌備處，再進行第二階段籌辦組織法等草案，預計明年送立院審核；籌備處人力初期40到50人，以專責處理個資保護事項。



個資保護委員會籌備處預計2024年1月掛牌

個資保護委員會籌備處 預計2024年1月掛牌

2023/10/2 16:55

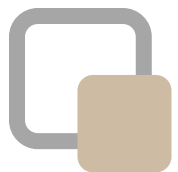


（中央社記者潘姿羽台北2日電）民進黨立委陳亭妃關切政府打詐，但法令通過後，後續進度相對緩慢，國發會主委龔明鑫今天說明，現在正進行個資法保護委員會籌備處相關工作，預計明年1月便可掛牌成立。



個人資料保護法自民國99年修正公布全文後，從未明定主管機關，行政院為落實個資保護，促進個資的合理利用，並依憲法法庭111年憲判字第13號判決所示，應建立個人資料保護獨立監督機制的意旨，因此提出個人資料保護法部分條文修正草案，明定設立個資保護委員會為個資法主管機關；草案今年5月獲立法院會三讀通過。





違反個資法 - 刑事責任

意圖為自己或第三人不法（財產）利益 或 意圖損害他人（各種）利益

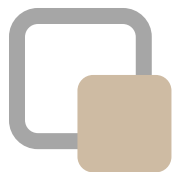
違法蒐集、處理
或利用個人資料

非法變更、刪除，或以其他非
法方法妨害個資檔案正確性

足生損害於他人

處5年以下有期徒刑，
可併科100萬元以下罰金

處5年以下有期徒刑、拘役或科或併科
100萬元以下罰金



違反個資法 - 行政責任

2萬-
20萬

- 先改再罰
- 蒐集個資沒有告知法定資訊
- 不讓當事人行使權利
- 違法行銷

5萬
-50萬

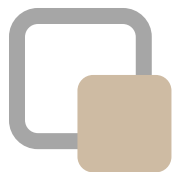
- 先罰再改
- 違法蒐集、處理、利用個人資料
- 違法國際傳輸個人資料

2萬-
1500萬

- 先罰再改
- 沒有做到適當安全維護
- 沒有訂定安全維護計畫
- 2萬 - 200萬
- 情節重大：15萬 - 1500萬

代表人
一起罰

- 企業受罰時
- 代表人、管理人、有代表權人
- 受同額罰鍰處罰
- **除非能證明盡到防止義務**



違反個資法 - 民事責任

要件

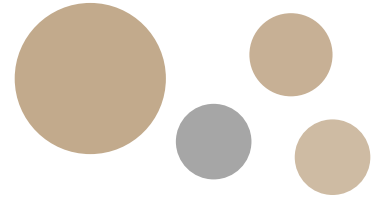
- 違反個資法規定，致個資遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。
- 除非能證明無故意或過失。

種類

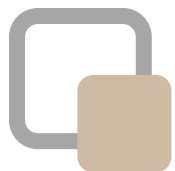
- 財產損害
- 精神損害
- 回覆名譽

範圍

- 不容易或不能證明實際損害額時，可請求法院依照侵害情節，以每人每一事件500元以上2萬元以下計算。
- 同一事件 + 多數受害人，賠償上限2億元



2 | 企業面臨的常見個資求償案例



消費者因企業個資外洩受騙請求賠償之架構

第1步

消費者應證明詐騙集團所利用之個資來自企業

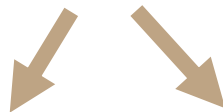
如消費者證明有



第2步

企業證明對個資外洩無故意或過失

如企業無法證明無故意過失

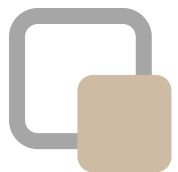


財產上損害

(個資法第28 I、III、29，民法第184條)

非財產上損害

(個資法第28 II、III、29，民法第195條)



消費者因企業個資外洩受騙請求賠償之架構

財產上損害

第3步

企業外洩個資與詐騙有無因果關係？

3-1 應由誰證明有無因果關係？

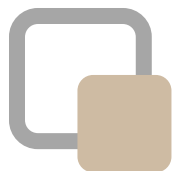
3-2 有無因果關係？

如有因果關係



第4步

與有過失比例



消費者應證明詐騙集團所利用之個資來自企業

見解1

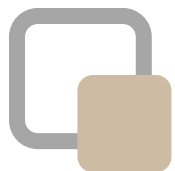
只有通聯來電紀錄，不足以證明受詐騙電話內容來自於企業。

裁判字號：臺北簡易庭 111 年度北小字第 5366 號民事判決

裁判日期：民國 112 年 01 月 31 日

裁判案由：損害賠償

)原告固提出發票、通聯記錄、兩造間對話紀錄、被告公司FB粉專與Google map評價內容、消費協商爭議處理書、被告公司網站隱私權保護章節等件影本為證，惟此並不足以證明原告通聯記錄之來電內容確為其在被告公司之訂單內容，亦難證明原告接獲所謂詐騙電話時，其個人資料即來自被告公司網站系統遭到入侵而致資料外流。而本件縱有第三人曾在被告公司FB粉專與Google map評價網頁留言關於被告公司之資料外洩，亦不足為原告之個人資料有自被告公司外洩之證明。且原告向被告購買商品後，尚經寄送過程，寄送資料之外洩是否因被告公司所致，亦屬不明，自難僅以原告主張其於購買商品後曾接獲詐騙電話可明確說出其在被告公司之訂單內容云云，即認被告有違反個人資料保護法規定而致原告個人資料有遭不法蒐集、利用等情事，是原告主張，自非可採。



消費者應證明詐騙集團所利用之個資來自企業

見解2

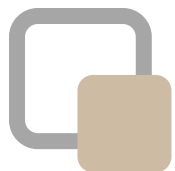
因詐騙內容與企業訂單內容不相符，故認為無法證明詐騙集團所使用之資料係來自於企業。

裁判字號：臺北簡易庭 110 年度北簡字第 904 號民事判決

裁判日期：民國 110 年 03 月 09 日

裁判案由：侵權行為損害賠償

負舉證責任。經查，原告固提出內政部警政署165全民防騙網109年10月19日至109年10月25日民眾通報高風險賣場、內政部警政署165全民防騙網109年5月11日至109年5月17日民眾通報高風險賣場、PTT、Dcard 網路貼文等件影本為證（見本院卷第35頁至第57頁），惟此並不足以證明原告遭詐騙時其個人資料即來自被告公司網站系統遭到入侵而致資料外流，況本件係超商取貨付款等情，亦據被告提出網購訂單資料影本乙份在卷可佐（見本院卷竹117頁），並為原告所不爭執（見本院卷第121頁），是原告並未在購買本件商品時使用郵局帳戶，亦難僅以原告主張其於購買商品後即收到詐騙電話云云，即認原告遭詐騙時之個人資料係來自被告公司，自無從認原告主張可採。



消費者應證明詐騙集團所利用之個資來自企業

見解2

因詐騙內容與企業訂單內容不相符，故認為無法證明詐騙集團所使用之資料係來自於企業。

裁判字號：臺北簡易庭 111 年度北簡字第 3221 號民事判決

裁判日期：民國 111 年 04 月 28 日

裁判案由：侵權行為損害賠償

顯然未經確認或證實。例如：原告於「誠品線上」網站是以台北富邦的信用卡消費(本院卷第123頁)，此點已與原告所陳稱詐騙集團掌握其交易資料且告知會自其國泰世華帳戶扣款並安排謊稱國泰世華客服人員施行詐術的事實不一致；加

以，原告於起訴狀第2頁事實與理由項下第1點陳稱，詐騙集團告知原告簽收包裹等同於在批發商同意書上簽名云云。惟實際上該包裹是由原告大樓的警衛收受並在快遞員之送件單上回蓋收發章，原告並未曾簽收任何文件(本院卷第125頁)。故詐騙集團告知原告之資訊，已與前述之紀錄不符，則詐騙集團所持有的原告個資顯然不是來自於被告，容屬有疑。更何況，現今詐騙集團犯行猖獗，可以各種手段獲取社會大眾各類網路購物資訊，作為行騙對象，故相關資料可能來自於外部詐騙份子入侵原告之個人電腦、手機、物流網站電腦系統、甚或以各種方式搜集資訊拼貼而成。故原告僅以詐騙集團提出與實際交易紀錄有多處不同之資訊，即認為被告公司有個資外洩之情事，其主張顯然仍屬臆測，亦無依據。



消費者應證明詐騙集團所利用之個資來自企業

見解3

消費者報警向警察陳述遭詐騙情節，應屬可信，且165防詐騙平台也有大量通報事件，非單一個案，因此推論消費者主張遭外洩之個人資料係來自於企業，符合經驗法則。

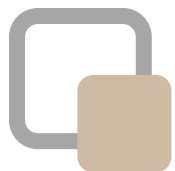
裁判字號：臺中簡易庭 110 年度中簡字第 1952 號民事判決

裁判日期：民國 111 年 12 月 23 日

裁判案由：損害賠償

見原告於遭詐騙後隨即於同日晚間即向警報案，其當下向警察陳述遭詐騙情節，自屬可信，原告前揭主張遭詐騙情節，堪認為真正。原告另主張被告未依個人資料保護法（下稱個

信用卡中心洩漏原告個資。參以刑事警察局165反詐騙諮詢專線公告之高風險賣場紀錄，被告於110年至111年間上榜43次，累計達587人受害，且原告受害相同期間，亦有相同受害者在被告粉絲頁面下留言，有新聞畫面及粉絲頁面留言截圖可佐（見本院111年度中消小25號民事判決理由欄所載），被告亦有向原告傳送反詐騙宣導簡訊，有該簡訊截圖在卷可考（見卷第53頁），可見類似利用被告保有之消費者個資進行詐騙情形眾多，並參酌前揭原告遭詐騙情節，詐騙集團假冒西堤餐廳人員正確提供原告先前消費訂單內容，原告主張詐騙集團所利用之前揭原告個人資料，係來自被告保有之原告消費個資，即與常情不悖，堪可認定為真正。被告



消費者應證明詐騙集團所利用之個資來自企業

見解3

消費者報警向警察陳述遭詐騙情節，應屬可信，且165防詐騙平台也有大量通報事件，非單一個案，因此推論消費者主張遭外洩之個人資料係來自於企業，符合經驗法則。

裁判字號：臺灣臺中地方法院 111 年度訴字第 2708 號民事判決

裁判日期：民國 112 年 03 月 15 日

裁判案由：損害賠償等

觀之上開留言內容及系爭反詐騙公告所列舉之詐騙集團手法，與原告遭詐騙之情節（詐騙集團知悉原告姓名及曾購買褲子，並要原告取消會員升級服務等）相符，是被告客戶之個人資料外洩，顯非單一個案。綜合111年1月至9月間冒用被告名義詐騙而通報之案件數高達500餘件，及被告自111年4月25日起至同年9月18日止，連續遭刑事警察局公告為「解除分期付款詐騙」類型之高風險賣場等情，**堪認**詐騙集團所利用之原告個人資料，係自被告保有之個人資料洩漏。被告空言泛稱係詐騙集團透過其他管道取得云云，要無可取。



如證明外洩資之個資來自企業，企業應證明對個資外洩無故意或過失

見解1

企業有個人資料檔案安全維護計畫，且有內部稽核報告、系統指令頁面等資料為憑，因此認定已採行合於個資法所定之安全措施，不能僅以遭駭客入侵即推論企業有違反個資法規定或管理上有缺失。

裁判字號：臺灣士林地方法院 107 年度消字第 6 號民事判決

裁判日期：民國 108 年 10 月 31 日

裁判案由：損害賠償

其次，被告公司已提出其個人資料檔案安全維護計畫（見本院卷一證物袋內），經與交通部觀光局所發布之旅行業個人資料檔案安全維護計畫範本（見本院卷二第68頁至第74頁）比對後，內容大致相符，包含個人資料處理及利用管理措施、事故預防、通報及應變機制、資料安全管理（包含員工、設備）及相關稽核機制等項目，均有明定，其中關於指定員工定期清查所保有之個人資料、設定員工不同權限以分別控管掌握之個人資料，以及輸出入個人資料時均需使用識別密碼、定期變更密碼等方式作為加密機制等，亦符合前揭旅行

業個人資料檔案安全維護計畫及處理辦法第4條第1項、第13條第1款、第14條第2款等規定，至於計畫執行層面，被告公司亦進行內部稽核、資料安全人員職業訓練，並定期變更電腦系統作業密碼等情，有被告公司向交通部觀光局提出之內部稽核報告、系統指令頁面、職業訓練等資料為憑（見本院卷一第344頁至第348頁），足見被告公司為保有所掌握之個人資料檔案，已採行合於個資法所定之安全措施。況且，兩造均不爭執本件個人資料外洩肇因於第三人入侵被告公司電腦作業系統所為之竊取行為，已如前述，益徵本件個人資料外洩並非被告公司管理不當所致，而鑑於電腦科技雖日新月異，然駭客惡意入侵電腦系統進行攻擊之事仍層出不窮，足見現今科技尚無法提供可完全防堵駭客攻擊之防護技術，自不能僅以被告公司電腦系統遭他人惡意入侵竊取資料一事，遽而推論其違反個資法規定或管理上有所疏失。



如證明外洩資之個資來自企業，企業應證明對個資外洩無故意或過失

見解2

企業所租用之機房系統與雲端服務因過久沒有更新，並未落實企業之個人資料處理作業辦法；只有進行員工資安訓練非對於客戶個人資料及訂單資料管理維護之積極作為。

裁判字號：內湖簡易庭 109 年度湖簡字第 1959 號民事判決

裁判日期：民國 110 年 05 月 31 日

裁判案由：侵權行為損害賠償

查均未能找出遭入侵的方式等語。則被告縱使訂有上開作業規範及向果核公司租用機房系統，其使用之系統歷經5年未更新，於系統遭入侵後亦無法即時發現任何異常之目標電腦及惡意程式檔案，其顯然未落實系爭個人資料處理作業辦法第16條第9項規定「對於電腦作業系統及相關應

用程式之漏洞，定期安裝修補之程式」（見本院卷一第164頁）。另樂利公司固有通知被告進行年度集團郵件社交工程演練、要求被告員工執行資安防護資料、並自109年3月1日起實施被告員工兩步驟帳號驗證、檔案加密等作為，然僅可認被告對於「員工」進行之資安訓練，但無法認定上開作為係屬於對於被告之「客戶之個人資料及訂單資料」管理維護之積極作為。是以不能認被告已對於系爭網路平台記錄、保存原告之個人資料盡適當安全維護措施。被告違反個人資料保護法第27條第1項規定，堪予認定。被告辯稱其對於系爭網路平台記錄、保存原告之個人資料已盡適當安全維護措施，所辯即無足採。



倘若企業被認定違反個資法，則消費者得否請求受詐騙之財產上損失？

（一）應由消費者證明有因果關係 或 推定有因果關係應由企業推翻？

見解1

實務見解多認為應由消費者舉證有因果關係。

裁判字號：臺中簡易庭 110 年度中簡字第 1952 號民事判決

裁判日期：民國 111 年 12 月 23 日

裁判案由：損害賠償

字第481號判例意旨參照）。次按依民法第184條第1項前段規定，侵權行為之成立，須行為人因故意過失不法侵害他人權利，亦即行為人須具備歸責性、違法性，並不法行為與損害間有因果關係，始能成立，且主張侵權行為損害賠償請求權之人，對於侵權行為之成立要件應負舉證責任。就歸責事由而言，無論行為人因作為或不作為而生之侵權責任，均以

行為人負有注意義務為前提，在當事人間無一定之特殊關係（如當事人間為不相識之陌生人）之情形下，行為人對於他人並不負一般防範損害之注意義務。又就違法性而論，倘行為人所從事者為社會上一般正常之交易行為或經濟活動，除被害人能證明其具有不法性外，亦難概認為侵害行為，以維護侵權行為制度在於兼顧「權益保護」與「行為自由」之旨意（最高法院100年度台上字第328號判決意旨參照）。故本件原告依侵權行為之法律關係請求被告賠償其損害，既為被告所否認，揆諸前開最高法院判決及判例意旨，原告就被告有侵權行為之成立要件自應負舉證責任。



倘若企業被認定違反個資法，則消費者得否請求受詐騙之財產上損失？

(一) 應由消費者證明有因果關係 或 推定有因果關係應由企業推翻？

見解2

亦有判決認定企業為透過交易營利之企業經營者，對於資料被竊取與外洩風險之控制較佳，因此推定有因果關係存在，除非企業得提出確切之反證證明

裁判字號：臺南簡易庭 106 年度南簡字第 1450 號民事判決

裁判日期：民國 107 年 06 月 26 日

裁判案由：侵權行為損害賠償

，抑或因而遭被告公司人員外洩等情，惟此等事實因有於國際網絡科技浩瀚並參雜人為因素之變異而有高度舉證困難，責令被害人擔負完全之舉證責任實有不公；而被告既為以此交易營利之企業經營者，原告交付個資後即由其支配掌握，其對於個資被竊取或外洩風險之控制及分擔能力俱優於原告；抑有進者，航空業者對旅客個資之維護義務，除建立在個人資料隱私權之保護外，亦有防免旅客個資外洩致影響飛航安全等重大風險實現，是本院斟酌本件訴訟性質、兩造之舉證能力及被告違反義務之情節及風險分配之合理性，而比照我國實務就公害訴訟降低被害人因果關係舉證責任之見解，認被告行為所生之危險已有相當合理確定性，即推定有一般因果關係之存在（最高法院102年度台上字第31號判決參照），被告倘認無一般或個別因果關係存在，自應提出確切之反證證明。



倘若企業被認定違反個資法，則消費者得否請求受詐騙之財產上損失？

(二) 受詐騙與企業違反個資法間具有無因果關係？

見解1

不具因果關係：資料外流並不必然發生客戶受詐騙且受有財物損失之侵害結果，消費者財物之損失係因詐騙集團成員積極實施詐騙行為所致。

裁判字號：內湖簡易庭 109 年度湖簡字第 1959 號民事判決

裁判日期：民國 110 年 05 月 31 日

裁判案由：侵權行為損害賠償

權受損害之不可欠缺之條件。然而考量詐騙集團介入行為對損害結果之強度，遠超乎原先個人資料外洩之影響，且屬故意犯罪行為，被告亦無防止該第三人不法行為之契約或法令上義務，堪認詐騙集團對原告施以詐術之故意行為業已中斷被告過失使資料外洩結果與原告財產上損害間之因果關係。且被告於系爭網站平台首頁及購物車頁面已設



倘若企業被認定違反個資法，則消費者得否請求受詐騙之財產上損失？

(二) 受詐騙與企業違反個資法間具有無因果關係？

見解1

不具因果關係：資料外流並不必然發生客戶受詐騙且受有財物損失之侵害結果，消費者財物之損失係因詐騙集團成員積極實施詐騙行為所致。

裁判字號：臺南簡易庭 110 年度南簡字第 1745 號民事判決

裁判日期：民國 111 年 03 月 31 日

裁判案由：請求損害賠償

戶等語，**足證**詐騙集團係利用原告的疏忽及不熟悉自動櫃員機之操作而行詐騙。再者，因應多年來利用自動櫃員機的詐騙手法，各家銀行已在自動櫃員機張貼防詐騙之宣導事項，原告即應對此一詐騙技倆有所警覺，然原告因其個人疏忽而誤信詐騙集團手法，致被詐騙集團所騙。換言之，被告系爭網站平台內客戶資料之外流，固係對於原告**隱私權**之侵害，然衡諸一般情形，資料外流並不必然發生客戶受詐騙且受有財物損失之侵害結果，原告財物之損失係因詐騙集團成員積極實施詐騙行為所致。



倘若企業被認定違反個資法，則消費者得否請求受詐騙之財產上損失？

(二) 受詐騙與企業違反個資法間具有無因果關係？

見解2

具有因果關係：資料外洩與詐騙集團實施詐騙間具有因果關係。

裁判字號：臺灣臺中地方法院 111 年度訴字第 2708 號民事判決

裁判日期：民國 112 年 03 月 15 日

裁判案由：損害賠償等

2261號判決意旨參照)。本件第三人利用被告未採行適當安全措施之機會，取得被告所保有之會員個人資料（含會員購買紀錄），一般而言即係做為非法用途，而詐欺集團取得上開個人資料後，即假冒被告名義利用該個人資料以詐騙包含原告之被告會員，致原告受騙而受有損害。故被告未採行適當安全措施以防止其保有之包括原告之個人資料洩漏之行為，按諸上開一般情形，即足生原告因遭詐欺集團利用其個人資料而受騙致生損害之結果，兩者間應具有相當因果關係。是被告此節所辯，亦無足取。



倘若企業被認定違反個資法，則消費者得否請求受詐騙之財產上損失？

(二) 受詐騙與企業違反個資法間具有無因果關係？

見解2

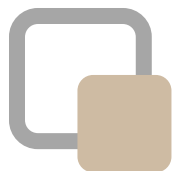
具有因果關係：資料外洩與詐騙集團實施詐騙間具有因果關係。

裁判字號：臺灣士林地方法院 107 年度簡上字第 225 號民事判決

裁判日期：民國 108 年 09 月 05 日

裁判案由：侵權行為損害賠償

，亦如前述，可見若非詐騙集團取得[]留存於系爭網站平台之個人資料，並使用該等明確、特定之個人資料以取信於[]，[]應不致於陷於錯誤而遭詐騙，堪認[]公司前揭未盡適當安全維護措施，致洩漏[]個人資料之行為，與[]遭詐騙受有25萬7,892 元損害間有相當因果關係，[]自得請求該部分財產上損害之賠償。



倘若企業被認定違反個資法，則消費者得否請求受詐騙之財產上損失？

(三) 與有過失比例

- 法院多認為消費者就受詐騙與有過失，因此可以依照過失比例減輕賠償
- 企業應負之過失比例：

見解

10%

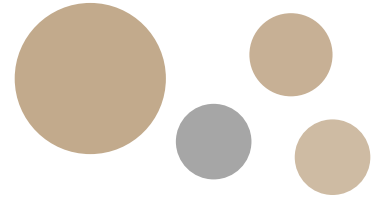
30%

70%

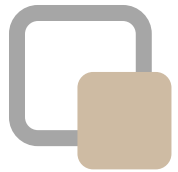
台中地院
111訴2708

台南地院
106南簡1450

士林地院
107簡上225



3 | 通傳事業的個資法合規管理



個人資料保護法

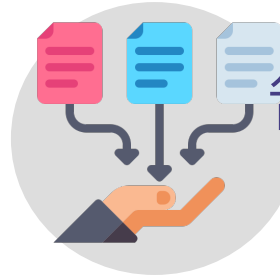
安全維護



事故通知



蒐集



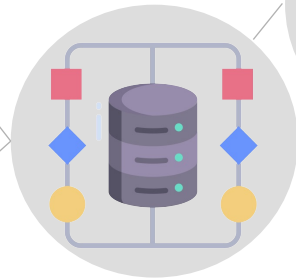
告知義務



處理



保存



刪除



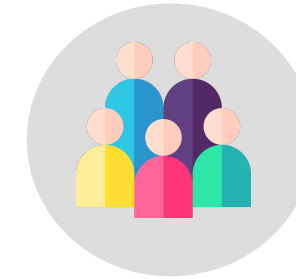
利用



國際傳輸



當事人權利



委外監督





國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法(111.07.01)



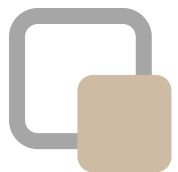
個資保護規劃



個資管理程序



稽核與改善



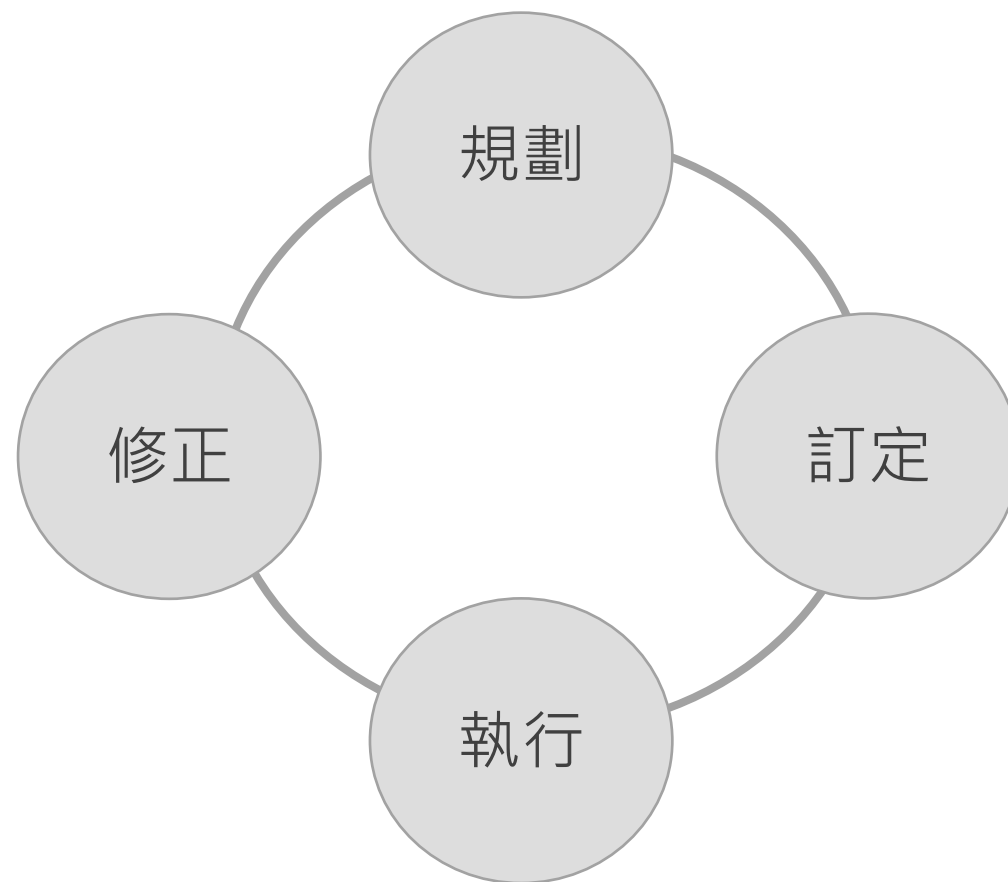
國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第3條

第1項

業者應依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，以規劃、訂定、修正與執行其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。

第2項

本計畫及處理方法之訂定或修正，應經非公務機關負責人或法定代理人簽署





個人資料保護法

安全維護



事故通知



蒐集



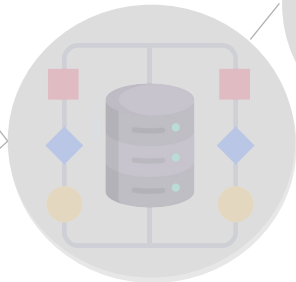
告知義務



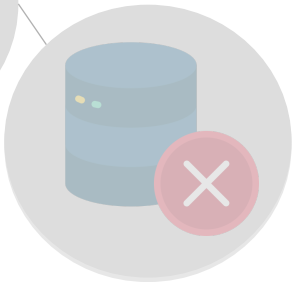
處理



保存



刪除



利用



國際傳輸



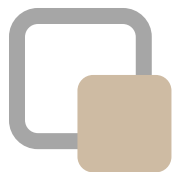
當事人權利



委外監督



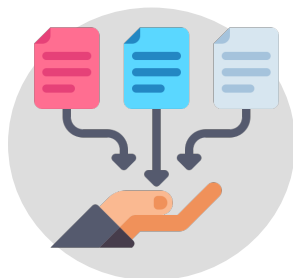
Da Vinci



蒐集、處理與利用

誠實信用、正當合理
具備**特定目的**，不超過目的**必要範圍**

蒐集



以任何方式取得

處理



為建立或利用個人資料檔案：

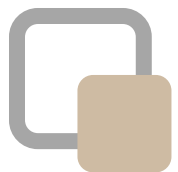
記錄、輸入、儲存、
編輯、更正、複製、
檢索、刪除、輸出、
連結或內部傳送

利用



處理以外的使用：

- 外部利用
- 內部利用
- 對當事人



蒐集、處理與利用特種個資

特種個資



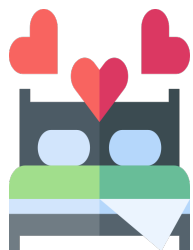
病歷



醫療



基因



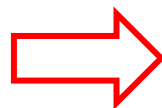
性生活



健康檢查



犯罪前科



原則禁止蒐集、處理、利用，除非：

法律明文規定

公務機關執行法定職務 /
非公務機關履行法定義務

當事人自行公開/已合法公開

公務或學術機關為醫療、衛生、犯
罪而研究+無識別性

協助公務機關執行法定職務

經當事人書面同意



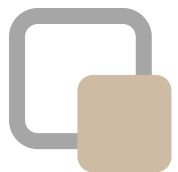
國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第5條

業者應就下列事項，訂定個人資料之管理程序

第1款 -

蒐集、處理或利用之個人資料包含本法第六條所定特種個人資料者，檢視其特定目的及是否符合相關法令之要件。

- 依據清查出的個資業務流程，檢視個人資料保護法各項規範的符合性
- 包含下列項目：
 - ❑ 蒐集、處理、利用特種個資的法律依據
 - ❑ 蒐集資料不超過達成目的所須範圍
 - ❑ 法定資訊揭露的完整程度
 - ❑ 當事人同意有效性
 - ❑ 利用個資符合蒐集目的
 - ❑ 保存期限符合法律規定
 - ❑ 委外監督措施
 - ❑ 安全維護義務等



蒐集、處理與利用一般個資

蒐集個資的特定目的



蒐集、處理一般個資的法律依據

法律明文規定

契約/類似契約關係

當事人自行/合法公開

學術機構研究+無識別性

當事人同意 (知情同意)

增進公共利益

一般可得來源

對當事人權益無侵害

利用一般個資：在蒐集目的必要範圍內

例外

法律明文規定

為增進公共利益所必要

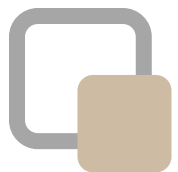
為免除當事人生命、身體、自由、財產危險

為防止他人權益之重大危害

為公益做統計/學術研究+無識別性

當事人同意(明確告知目的、範圍及同意與否的影響)

有利於當事人權益



國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第5條

業者應就下列事項，訂定個人資料之管理程序

第3款 -

檢視個人資料之蒐集、處理，是否符合本法第十九條規定，具有特定目的及法定情形；其經當事人同意者，並應確保符合本法第七條第一項規定。

個人資料保護法第7條第1項

.....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。



國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第5條

業者應就下列事項，訂定個人資料之管理程序

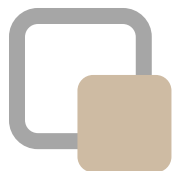
第4款 -

檢視個人資料之利用，是否符合蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否符合法定情形，經**當事人同意**者，並應確保符合本法第七條第二項規定。

個人資料保護法第7條第2項

.....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。

- 依據清查出的個資業務流程，檢視個人資料保護法各項規範的符合性
- 包含下列項目：
 - ☐ 蒐集、處理個資的法律依據
 - ☐ 蒐集資料不超過達成目的所須範圍
 - ☐ 法定資訊揭露的完整程度
 - ☐ 當事人同意有效性
 - ☐ 利用個資符合蒐集目的
 - ☐ 保存期限符合法律規定
 - ☐ 委外監督措施
 - ☐ 安全維護義務等



利用個資行銷規定

- 首次行銷，要提供當事人免費拒絕的方式
- 當事人可隨時拒絕行銷，企業應立即停止行銷

利用一般個資：蒐集目的必要範圍內

例外

法律明文規定

為增進公共利益所必要

為免除當事人生命、身體、自由、財產危險

為防止他人權益之重大危害

為公益做統計/學術研究+無識別性

當事人同意(明確告知目的、範圍及同意與否的影響)

有利於當事人權益



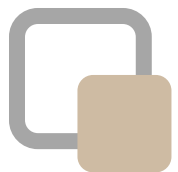
國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第5條

業者應就下列事項，訂定個人資料之管理程序

第5款 -

利用個人資料為行銷，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。

- 建立拒絕行銷管道
- 確認前端人員接收拒絕行銷資訊後，可於系統註記，或依照其他內部流程有效更新可行銷名單
- 定期維護可行銷名單



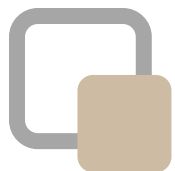
國發會：拒絕商業行銷指引(112.06.13)

行銷時

拒絕時

拒絕後

- 對當事人進行商業行銷時，於首次及後續行銷時須主動表明其名稱。
- 首次進行商業行銷時，應提供當事人免費、快速、容易表達之簡便方式以拒絕接受上開行銷，例如：免付費電話或簡訊、電子郵件地址、企業網站客戶服務網址、於應用程式（APP）內取消行銷資訊等。
- 首次利用合法蒐集之個人資料，對當事人依本法第二十條第三項規定進行商業行銷後，於其行使同條第二項規定之拒絕權利前，而非公務機關續行對當事人行銷時，仍宜以清楚易懂、置於醒目位置且容易取得之方式，持續揭示便利當事人拒絕接受商業行銷相關方式之資訊（例如：於企業網站公佈）。



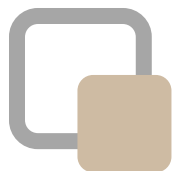
國發會：拒絕商業行銷指引(112.06.13)

行銷時

拒絕時

拒絕後

- 當事人對非公務機關利用其個人資料為商業行銷時，有權不附理由，隨時、任意地表示拒絕，且不以該機關為首次商業行銷時為限。
- 應尊重當事人拒絕商業行銷之意思，按其拒絕行銷之意願及範圍停止行銷；其後非經當事人再為通知或更改其意願前，不得再為行銷。
- 本法第二十條第三項雖規範非公務機關須提供當事人拒絕接受行銷之方式，惟未限制當事人僅得以上開方式行使拒絕權，非公務機關不得以當事人未依所提供之方式為由，拒絕停止對當事人商業行銷。



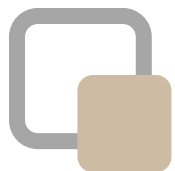
國發會：拒絕商業行銷指引(112.06.13)

行銷時

拒絕時

拒絕後

- 應記錄、更新及彙整當事人拒絕商業行銷之意思表示，並回覆當事人已收到其拒絕行銷之通知；另依本法第二十七條第一項及同法施行細則第十二條規定，採行適當之安全措施。
- 非公務機關應儘速周知所屬人員或受委託者，依本法第二十條第二項意旨，停止對該當事人進行商業行銷。



國發會：拒絕商業行銷指引(112.06.13)

委託商業行銷

- 如非公務機關委託他人向當事人進行商業行銷，應採取適當之監督措施（例如於雙方契約中納入對應約款），確保受託者履行該非公務機關所適用之本法第二十條第二項及第三項規定（另參照本法施行細則第七條及第八條），以處理當事人拒絕商業行銷之相關事宜。



個人資料保護法

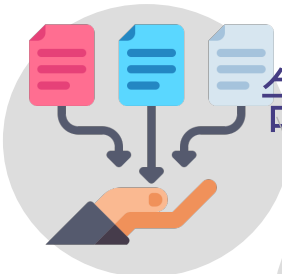
安全維護



事故通知



蒐集



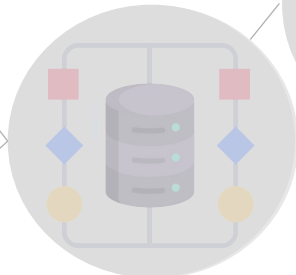
告知義務



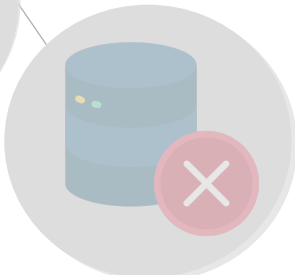
處理



保存



刪除



利用



國際傳輸



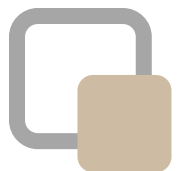
當事人權利



委外監督

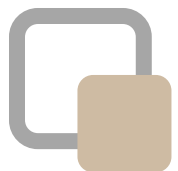


Da Vinci



告知義務 (隱私權政策、個資告知聲明)

個資來源	直接蒐集(來自當事人)	間接蒐集(來自第三方或公開資料)
告知時機	蒐集前/時	處理或利用時/首次對當事人利用時
告知內容	蒐集機關名稱	
	蒐集個資目的	
	蒐集個資類別	
	利用個資的期間、地區、對象、方式	
	當事人權利及行使方式	
	得自由選擇提供時， 不提供的影響	個資來源



告知義務 - 例外免除

個資來源	直接蒐集(來自當事人)	間接蒐集(來自第三方或公開資料)
例外免除告知義務	依法律規定得免告知	
	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	
	非基於營利之目的+對當事人顯無不利影響	
		當事人自行公開 or 已合法公開
		不能向當事人or法定代理人告知
		公益目的+統計、學術+無從識別
		大眾傳播業+新聞報導+公益目的



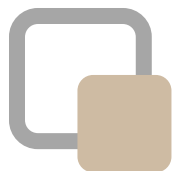
國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第5條

業者應就下列事項，訂定個人資料之管理程序

第2款 -

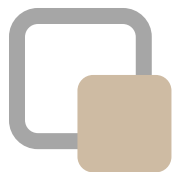
檢視個人資料之蒐集、處理或利用，是否符合
免為告知之事由，及告知之內容、方式是否合
法妥適。

- 依據清查取得個資的管道，區分直接蒐集或間接蒐集個資
- 檢視告知內容的法規符合性
- 訂定內部程序管理落實



合法告知才能有效同意

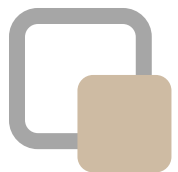
蒐集、處理一般個資的法律依據				蒐集、處理、利用特種個資	
特定目的	+	法律明文規定	契約/類似契約關係	法律明文規定	
		當事人自行/合法公開	學術機構研究+	公務機關執行法定職務 / 非公務機關履行法定義務	
		當事人同意 (知情同意)	增進公共利益	當事人自行公開/已合法公開	
		一般可得來源	對當事人權益	公務或學術機關為醫療、衛生、犯罪而研究 + 無識別性	
				協助公務機關執行法定職務	
				經當事人書面同意 (知情同意)	



告知方式

個人資料保護法施行細則第16條
依本法第八條、第九條及第五十四條
所定告知之方式，得以**言詞、書面、
電話、簡訊、電子郵件、傳真、
電子文件**或其他足以使當事人知悉
或可得知悉之方式為之。





告知方式

個人資料保護法施行細則第16條

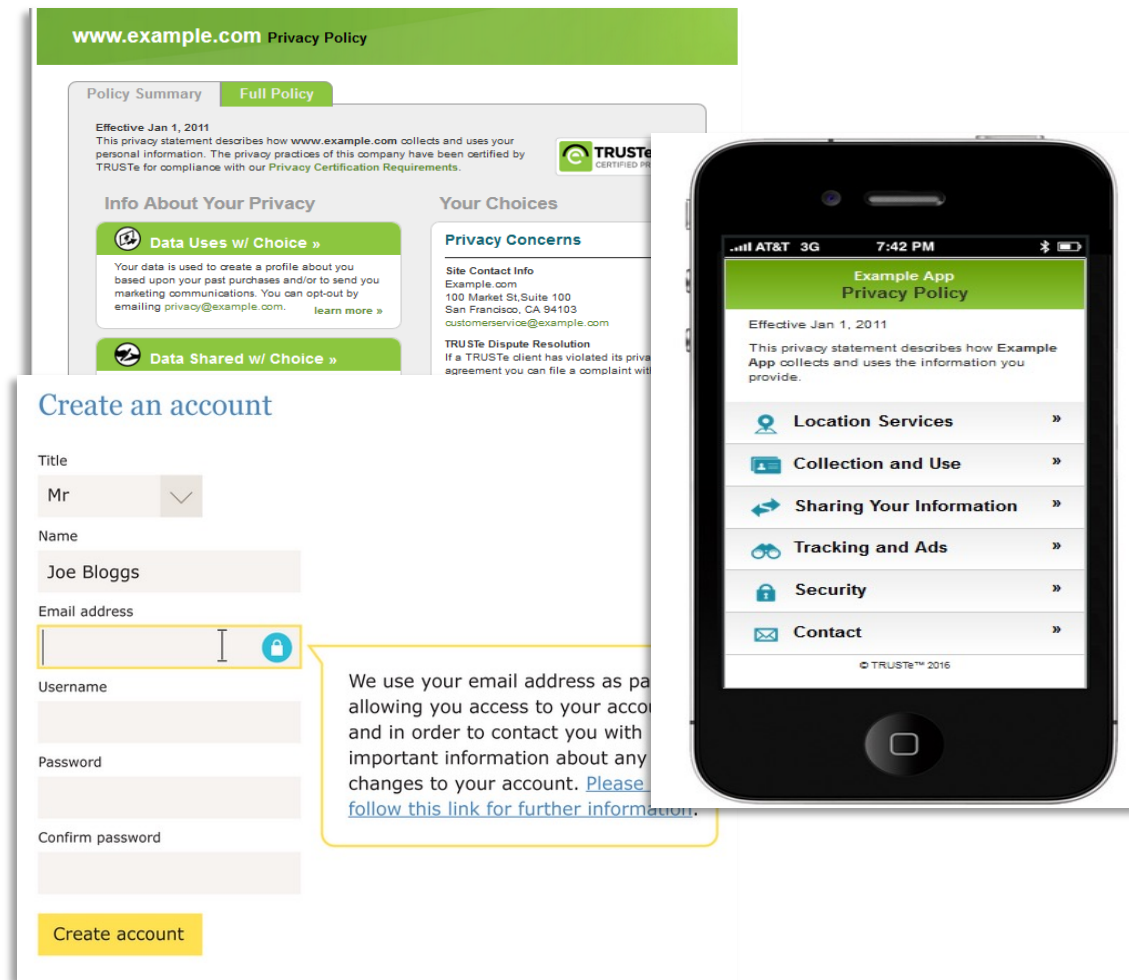
依本法第八條、第九條及第五十四條

所定告知之方式，得以言詞、書面、

電話、簡訊、電子郵件、傳真、

電子文件或其他足以使當事人知悉

或可得知悉之方式為之。





國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第5條

業者應就下列事項，訂定個人資料之管理程序

第2款 -

檢視個人資料之蒐集、處理或利用，是否符合
免為告知之事由，及告知之內容、方式是否合
法妥適。

國發會108年3月12日
發法字第1082000384號函

- 教材業者以贈品利誘學童提供個人資料，
須踐行告知義務
- 如其告知對象無法充分了解其個人資料之
後續利用，則未能符合規定
- 業者之告知方式應符合學童之**年齡、生活
經驗及理解能力**，以**容易理解、清楚簡單
之語言或文字**為之，並使該學童得以充分
瞭解其個人資料之後續利用



國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第5條

業者應就下列事項，訂定個人資料之管理程序

第2款 -

檢視個人資料之蒐集、處理或利用，是否符合
免為告知之事由，及告知之內容、方式是否合
法妥適。

法務部102年6月11日
法律字第10203503280號函

- 「符合個人資料相關法令以自動化機器或
其他非自動化之利用方式」之個人資料利
用方式，內容過於模糊、概括，應予修正，
使當事人明確知悉利用方式為何。



個人資料保護法

安全維護



事故通知



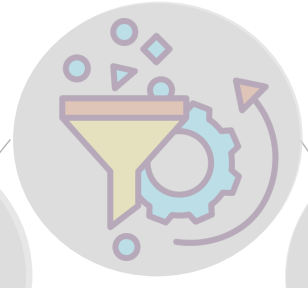
蒐集



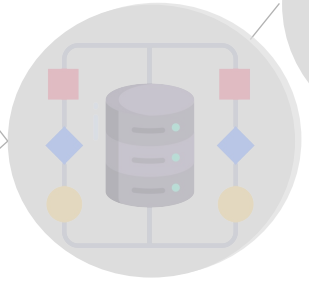
告知義務



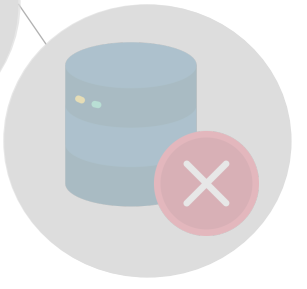
處理



保存



刪除



利用



國際傳輸



當事人權利



委外監督



Da Vinci



主管機關可限制個人資料傳輸境外

個人資料保護法第21條

有下列情形之一，中央目的事業主管機關得限制之：

- 1) 涉及國家重大利益。
- 2) 國際條約或協定有特別規定。
- 3) 接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。
- 4) 以迂迴方法向第三國（地區）傳輸個人資料規避本法。



upmedia.mg

https://www.upmedia.mg/news_info

文化部禁止台灣《蘋果日報》洩個資「不得跨境資料傳輸」

2021年12月21日 — 香港法院指派清算（盤）人處理台灣《蘋果日報》相關資產，由於擔憂資料轉移可能造成個資外流，**文化部**對此去函限制「不得**跨境傳輸**所保有的所有個人 ...」



ltn.com.tw

<https://news.ltn.com.tw/news/politics/breakingnews>

民團：文化部應一併禁止壹週刊跨境傳輸個資- 政治 - 自由時報

2021年12月27日 — 經濟民主連合及民進黨立委范雲等人今日在立法院召開記者會呼籲，除了台灣蘋果日報，**文化部**應一併發函已停刊的「壹週刊」**禁止跨境傳輸**個資。

<https://news.ltn.com.tw/news/politics/breakingnews>

台灣《蘋果日報》跨境傳輸個資？經民連籲檢方與文化部追查 ...

2022年9月7日 — 經民連研究員歐翎韶指出，**文化部**去年12月20日以函令限制台灣《蘋果日報》「不得**跨境資料傳輸**」，然而，香港商人黃浩9月在港媒專訪中透露，壹傳媒在英美仍 ...

isniVoD



國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第5條

業者應就下列事項，訂定個人資料之管理程序

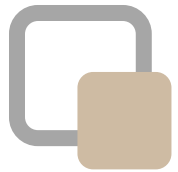
第7款 -

進行個人資料國際傳輸前，檢視是否受本會相關法令限制並遵循之。

例如：

母公司在境外，台灣子公司傳輸個人資料時 / 委託廠商在境外，台灣公司傳輸個人資料時 -

- 檢視中央主管機關有無限制傳輸
- 向當事人告知傳輸區域、對象



個人資料保護法

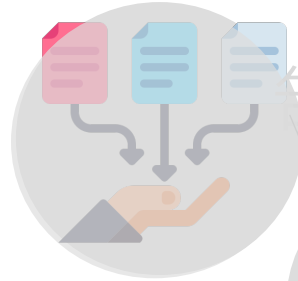
安全維護



事故通知



蒐集



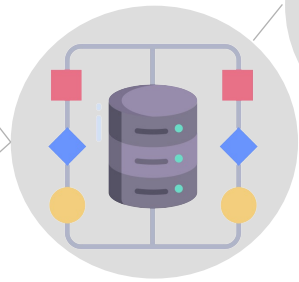
告知義務



處理



保存



刪除



利用



國際傳輸

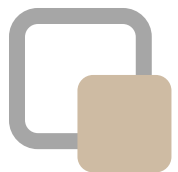


當事人權利



委外監督





個人資料的保存期限

個資法第11條

特定目的消失/違反個資法



主動或依當事人請求



刪除、停止處理或利用

例外

法令規定或契約約定保存期限

刪除將侵害當事人利益

不能刪除之正當事由

當事人書面同意





國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第5條

業者應就下列事項，訂定個人資料之管理程序

第10款 -

檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應依本法第十一條第三項規定辦理。

- 執行個資清查時，一併評估各類個人資料檔案的保存期限
- 識別紙本、電子檔與系統內資料
- 如有正當理由無法刪除，應以技術方式停止處理、利用，例如：
 - ❑ 紙本歸檔封存
 - ❑ 電子檔移至他處保存
 - ❑ 系統內資料加密、遮蔽或使同仁無從存取



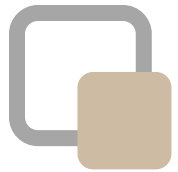
國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第6條

就下列事項，訂定相關紀錄、證據保存機制：

第2款 -

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留存之下列紀錄：

- ① 刪除、停止處理或利用之方法、時間
- ② 將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。



個人資料保護法

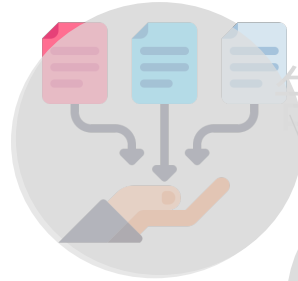
安全維護



事故通知



蒐集



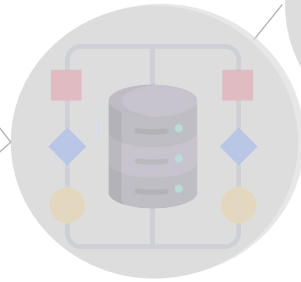
告知義務



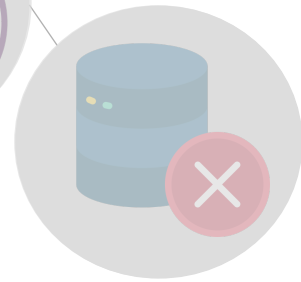
處理



保存



刪除



利用



國際傳輸



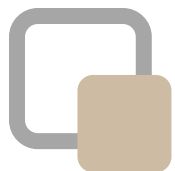
當事人權利



委外監督



Da Vinci



當事人權利

	權利內容	例外拒絕/限制	
近用權	查詢、閱覽、複製	妨害國安、外交、軍事、經濟	妨害公務機關執行法定職務
		妨害機關或第三人重大利益	
更正權	補充、更正	正確性有爭議時，停止處理、利用，除非： 執行業務所必須，或經書面同意並註明爭議	
拒絕權	停止處理、利用/刪除 (目的消失、期限屆滿、違法蒐集)	法令規定保存期限	刪除將侵害當事人利益
		不能刪除之正當事由	當事人書面同意



國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第5條

業者應就下列事項，訂定個人資料之管理程序

第8款 -

當事人行使本法第三條所定權利之相關事項：

- ① 當事人身分之確認
- ② 提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項
- ③ 對當事人請求之審查方式，並遵守本法有關處理期限之規定
- ④ 有本法所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。

- 建立當事人權利行使機制，確認單一或專責受理窗口
- 訂定程序管理當事人權利行使流程
- 宣導與訓練



個人資料保護法

安全維護



事故通知



蒐集



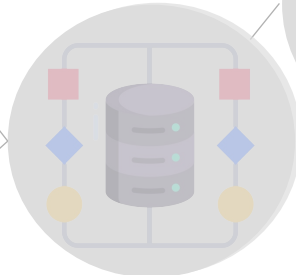
告知義務



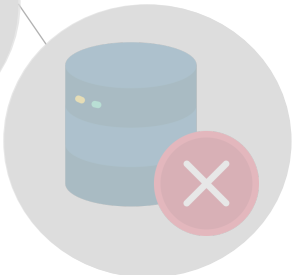
處理



保存



刪除



利用



國際傳輸



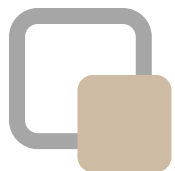
當事人權利



委外監督



Da Vinci



委外廠商責任由委託機關負責



電腦王阿達

13k 人追蹤

☆ 追蹤

日本社福承包人員醉倒後弄丟了一個存放了 **46** 萬位市民個資的隨身碟



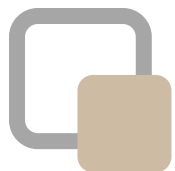
2022年6月25日 週六 下午8:32

LINE

BBC 網站在報導中引述了日本當地的報導，表示這位不具名的承包人員在下班前將這份隨身碟收到了自己的公事包中，並前往了位於大阪市西北方的尼崎市，他在當地的居酒屋喝了數個小時的酒，最終在離開後直接醉倒在路邊。當他終於酒醒後，他發現了這個重要的隨身碟早已連同自己的公事包一起不翼而飛。

尼崎市政府當局在公開聲明中表示這份隨身碟中除了包含著全體市民的名字、出生日期以及地址等基本資料之外，還記錄了許多更加機密的資訊，像是稅務細節、銀行帳號以及受社會安全局保護的家庭資訊，都是可能侵犯個人隱私的重要資訊。不過值得慶幸的是，尼崎市政府證實了存放在隨身碟中的個人資料都有進行額外的加密保護，並以一個密碼鎖上，同時也強調到目前為止還沒有出現任何試圖存取這些重要資訊的跡象或記錄。

isniVoD



委外廠商責任由委託機關負責



焦點 最新 熱門 娛樂時尚 生活 社會 財經地產 國際 政治 體育 吃喝玩樂 3C車市 蘋評理 火線

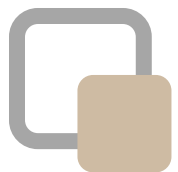
誰弄丟日本尼崎市46萬人個資USB？「外包的外包的外包公司」惹禍

據日本電視台28日報導，接受尼崎市委託協助發放津貼的雲端服務公司「BIPROGY」，在當地時間26日晚間公告表示，弄丟USB隨身碟的不是我們的外包公司員工，而是外包公司再外包的公司員工。

報導指，尼崎市委託雲端服務公司「BIPROGY」協助發放紓困金，但BIPROGY未經尼崎市許可，將業務發包給另一間公司（簡稱A公司），但沒想到這間A公司又將業務偷偷發包給另外一間公司（簡稱B公司），也就是說一項業務就層層轉包3次，弄丟USB隨身碟的並非一開始外傳的尼崎市員工，而是B公司的員工。

目前尼崎市預定向BIPROGY要求損債賠償，實際賠償內容仍未定。

isniVoD



委外監督

個資法委外監督

個資範圍、類別、目的、期間

受託者應採行的適當安全維護

複委託之受託者約定

受託者違法應通知事項及補救

委託者保留指示之事項

結束後個資之返還與刪除

定期確認執行狀況+記錄結果

資安管理法委外監督

完善資安管理措施或第三方驗證

配置專業人員

複委託與否、範圍、安全措施

涉及國安的適任性查核、管制出境

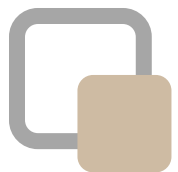
安全性檢測證明、授權證明

違法應通知及補救

結束後資料返還與刪除

其他資通安全相關措施

定期或知悉事件時執行稽核或確認



國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第5條

業者應就下列事項，訂定個人資料之管理程序

第6款 -

委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。

個資法委外監督

個資範圍、類別、目的、期間

受託者應採行的適當安全維護

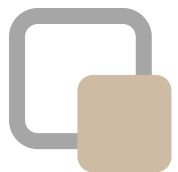
複委託之受託者約定

受託者違法應通知事項及補救

委託者保留指示之事項

結束後個資之返還與刪除

定期確認執行狀況+記錄結果



委外監督可以怎麼做



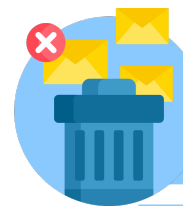
事前—明確約定

- 委託目的、類別、範圍、期間
- 權利&義務
- 安全措施
- 補救&通知事項
- 退場機制



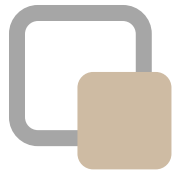
事中—執行監督

- 低強度
—廠商自評
- 中強度
—機關提出項目，廠商提出符合性
- 高強度
—機關執行稽核



事後—退場機制

- 資料返還
- 資料銷毀
- 資料遷移？
- 你被廠商「鎖定」了嗎？



個人資料保護法

安全維護



事故通知



蒐集



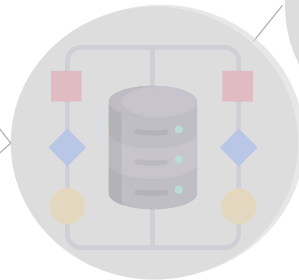
告知義務



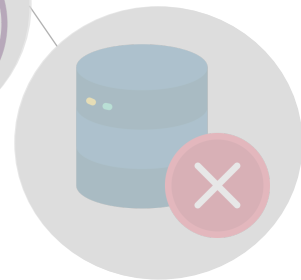
處理



保存



刪除



利用



國際傳輸

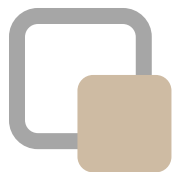


當事人權利



委外監督





個資事故發生有通知義務

個資法第12條 - 事故通知當事人

機關違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害者

應查明後即時以適當方式通知當事人

言詞、書面、電話、簡訊、電子郵件...

原則主動通知 / 例外被動公告

被侵害之事實 / 已採取的因應措施



國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第4條

第1項

非公務機關為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱事故），應訂定下列應變、通報及改善機制：

- 1) 事故發生後應採取之應變措施，包括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，其改善措施之研議機制。

個資法第12條 - 事故通知當事人

機關違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害者

應查明後即時以適當方式通知當事人

言詞、書面、電話、簡訊、電子郵件...

原則主動通知 / 例外被動公告

被侵害之事實 / 已採取的因應措施

應經取得相關認證資格之機構，進行整體診斷及檢視



國家通訊傳播委員會指定非公務機關 個人資料檔案安全維護辦法 - 第4條

第2項

非公務機關遇有**重大個人資料事故**者，應於知悉後一小時內**通報本會**，並於七十二小時內依附表格式，續行通報本會。但非公務機關接獲本會或有關機關通報發生事故時，應於四十八小時內，依附表格式通報本會。

重大個人資料事故：

- ① 危及業者正常營運之虞
- ② 造成當事人權益重大損害之虞
- ③ 逾越改正期限未改正且洩漏個資筆數160筆以上

第四條 附表

個人資料侵害事故通報紀錄表		
非公務機關名稱	通報時間： 年 月 日 時 分	
	通報人：	
	職稱：	
	電話：	
	電子郵件：	
	事故地址：	
事故發生時間		
事故發生種類	☐ 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
發生原因及事故摘要		
損害狀況		
個資侵害可能結果		
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之時限內通報	初報：重大個人資料事故知悉後一小時內 ☐ 是 ☐ 否，理由：_____	
	續報：重大個人資料事故知悉後七十二小時內 ☐ 是 ☐ 否，理由：_____	
	接獲機關通報後：四十八小時內 ☐ 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：有關通報本會方式及管道等相關資訊，另揭露於本會官網。



個人資料保護法

安全維護



事故通知



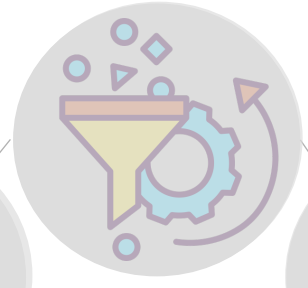
蒐集



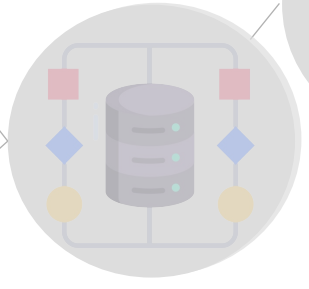
告知義務



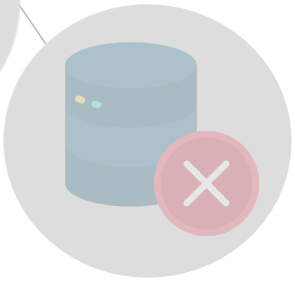
處理



保存



刪除



利用



國際傳輸



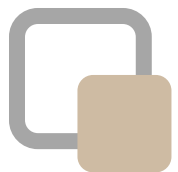
當事人權利



委外監督



Da Vinci



安全維護事項有哪些可做

個資管理PIMS

組織資源配置

界定個資範圍

風險評估機制

通報應變機制

內部管理程序

資安人員管理

認知教育訓練

設備安全管理

安全稽核機制

資料紀錄保存

計畫持續改善

資安管理ISMS

資安管理政策

資訊資產管理

風險評鑑管理

實體安全管理

通信作業管理

存取控制管理

系統開發管理

委外業務管理

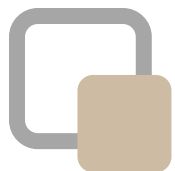
資安事件管理

業務持續管理

內部稽核管理

矯正改善管理

人員安全與教育訓練



實務作法 - 訂定個資管理、安全維護計畫

個人資料檔案安全維護計畫

- 1 目的：
 - 1.1 為確保[]個人資料檔案管理之安全，並強化對個人資料之保護能力，防止個資外洩事件發生，達成持續改善之目標。
- 2 適用範圍：
 - 2.1 本會承辦相關個人資料作業均適用之。
- 3 權責：
 - 3.1 個資暨資訊安全組織：
 - 3.1.1 個資暨資訊安全長：由資訊發展處處長擔任。
 - 3.1.1.1 個資暨資訊安全管理制度相關重大事項之審核或決議。
 - 3.1.1.2 跨部門之資源協調。
 - 3.1.2 個資暨資訊安全委員：由資訊發展處處長指派，參與管理審查會議，提供相關決策與指導。
 - 3.1.3 個資暨資訊安全官(或稱為個資暨資訊安全執秘)：由本會資訊安全業務主管擔任或由個資暨資訊安全長指派擔任。
 - 3.1.3.1 管控資訊安全政策與相關措施的執行。

個資保護與資訊安全管理制度_A1_個資保護與資訊安全管理政策(原 ISMS 編號 A1)_(draft v1.0)
個資保護與資訊安全管理制度_A2_個資保護與資訊安全管理指導綱要(原 ISMS 編號 A2)_(draft v1.0)
個資保護與資訊安全管理制度_A3_全景作業指導綱要(原 ISMS 編號 A3)_(draft v1.0)
個資保護與資訊安全管理制度_B1_個資保護與資安管理組織程序書(原 ISMS 編號 B1)_(draft v1.0)
個資保護與資訊安全管理制度_B2_文件管理程序書_(draft v1.0)
個資保護與資訊安全管理制度_B3_法規盤點程序書(draft v1.0)
個資保護與資訊安全管理制度_B4_個人資料清查程序書_(draft v1.0)
個資保護與資訊安全管理制度_B5_資訊資產管理程序書(原 ISMS 編號 B2)_(draft v1.0)
個資保護與資訊安全管理制度_B6_風險評鑑管理程序書(原 ISMS 編號 B3)_(draft v1.0)
個資保護與資訊安全管理制度_B7_個人資料安全事件管理程序書_(draft v1.0)
個資保護與資訊安全管理制度_B8_資訊安全事件管理程序書(原 ISMS 編號 B10)_(draft v1.0)
個資保護與資訊安全管理制度_B9_個人資料蒐集、處理與利用管理程序書_(draft v1.0)
個資保護與資訊安全管理制度_B10_當事人權利行使程序書_(draft v1.0)
個資保護與資訊安全管理制度_B11_實體與環境安全管理程序書(原 ISMS 編號 B5)_(draft v1.0)
個資保護與資訊安全管理制度_B12_人員安全與教育訓練程序書(原 ISMS 編號 B4)_(draft v1.0)
個資保護與資訊安全管理制度_B13_通信與作業管理程序書(原 ISMS 編號 B6)_(draft v1.0)
個資保護與資訊安全管理制度_B14_存取控制管理程序書(原 ISMS 編號 B7)_(draft v1.0)
個資保護與資訊安全管理制度_B15_系統開發與維護管理程序書(原 ISMS 編號 B8)_(draft v1.0)
個資保護與資訊安全管理制度_B16_個資保護與資安內部稽核管理程序書(原 ISMS 編號 B12)_(draft v1.0)
個資保護與資訊安全管理制度_B17_矯正管理程序書(原 ISMS 編號 B13)_(draft v1.0)
個資保護與資訊安全管理制度_B18_委外管理程序書(原 ISMS 編號 B9)_(draft v1.0)
個資保護與資訊安全管理制度_B19_業務持續運作管理程序書(原 ISMS 編號 B11)_(draft v1.0)
個資保護與資訊安全管理制度_B20_個資保護與資安績效管理程序書(原 ISMS 編號 B14)_(draft v1.0)



個資盤點是第一步，找出個人資料才能有效管理

自立晚報

政院疏忽 審計部查出實聯制檔案未銷毀

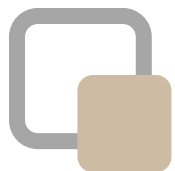


2023年2月12日 週日 下午10:58



【記者蘇旺台台北報導】審計部11日指出，防疫期間政府實施簡訊實聯制，查核發現部分防疫個資檔案未落實執行外部稽核作業，確認已刪除或銷毀，有洩漏或不當使用風險；函請行政院改善後皆已刪除，確保民眾隱私。

審計部指出，111年5月查核發現，通傳會在查訪電信業者辦理簡訊實聯制資料刪除過程，未檢核原始檔案、備份伺服器及電子郵件等資料儲存點，且部分防疫機關透過非公務環境登入疫調輔助平台，導致相關個資檔案散落在非公務電腦或行動裝置，或在實聯制措施退場後，仍持續下載運用。



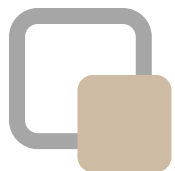
動態業務盤點更確實

業務辦理流程

與該個資檔案相關的作業流程，包含個資如何取得及如何利用、內部流動到何單位，以及由內部何單位保存等。

檔案型態

該個資檔案之形態，包括紙本類、電子類、可攜式媒體內之電子檔，以及系統資料庫。



動態業務盤點更確實

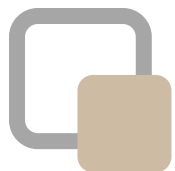
個資來源

與取得該個資之來源，包括是否直接向當事人蒐集及其方式與管道（例如當事人填寫紙本繳交、以Email寄給承辦人、郵寄、線上填寫等），或間接蒐集及其來源（例如與其他機關系統勾稽取得、他人提供等）

內部單位與外部機關

機關內部蒐集、處理或利用該個資之各單位，包括個資在機關內各單位間之流動狀況。

該個資是否提供予外部機關蒐集、處理或利用。



動態業務盤點更確實

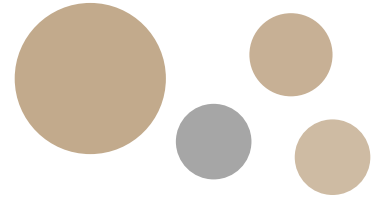
委外情形

是否委託其他公務或非公務機關蒐集、處理或利用該個資，以及受託機關接觸個資之情形。

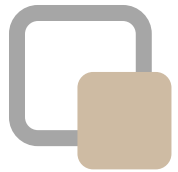
保管方式與保存期限

該個資檔案之保管方式，例如紙本保存於承辦人抽屜或機關檔案室，電子檔保存於承辦人電腦或機關系統資料庫等。

個資檔案是否有法定或自定之保存期限，例如依檔案法確定之保存年限。



4 | 結論



個人資料保護法

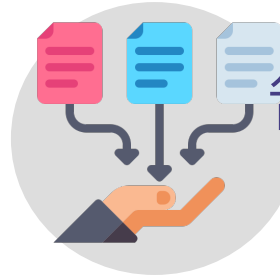
安全維護



事故通知



蒐集



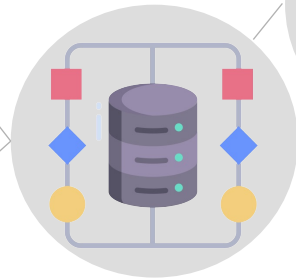
告知義務



處理



保存



刪除



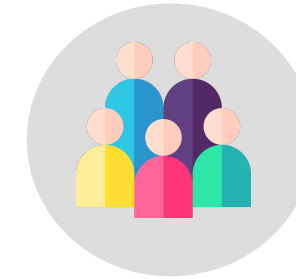
利用



國際傳輸



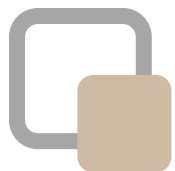
當事人權利



委外監督



DaVinci



建議：上下循環的個資保護合規管理

個人資料保護法第27條

第一項

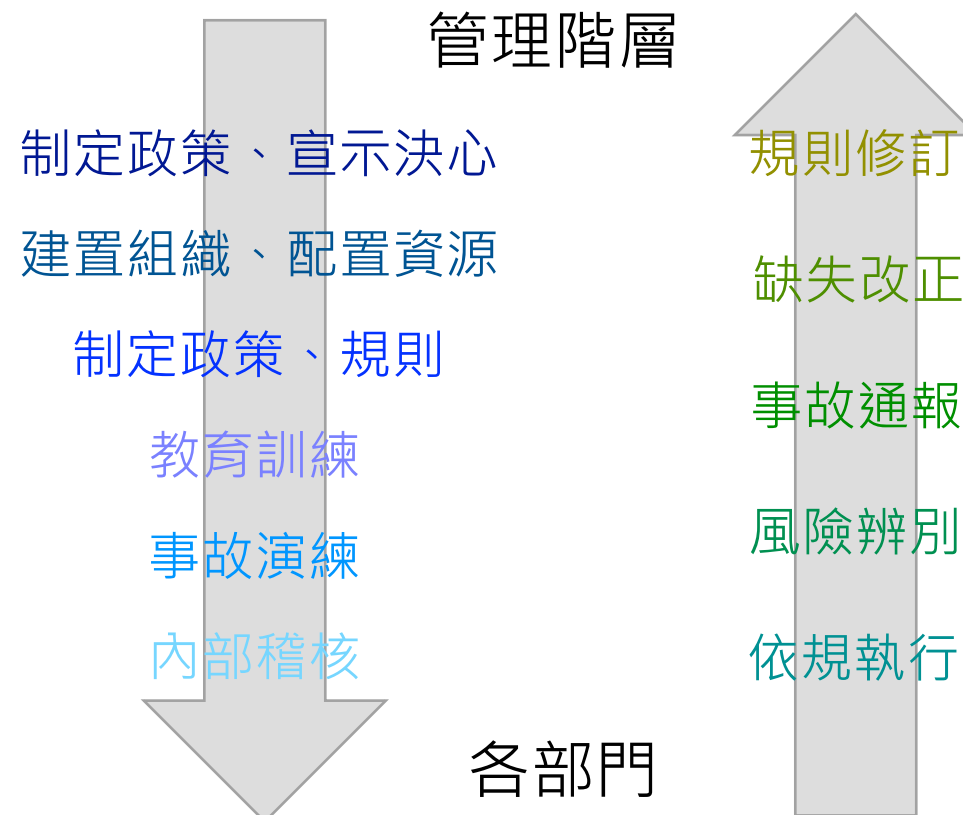
非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

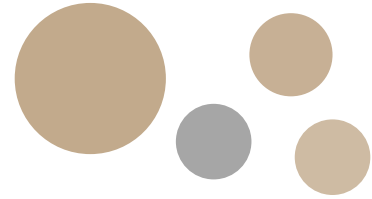
第二項

中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

NCC

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法





謝謝聆聽

THANKS FOR YOUR ATTENTION



王慕民律師

達文西個資暨高科技法律事務所

10045 臺北市中正區衡陽路51號6樓之9

TEL : 02-2367-0902