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

通訊傳播事業
個資法遵教育及實務案例分享

達文西個資暨高科技法律事務所

孔德澔 律師

2024年4月17日

講者介紹

學歷

- 國立政治大學 法律學研究所公法組碩士
- 國立政治大學 法律學系學士

專業領域

- 智慧財產權法
- 個人資料保護法
- 行政訴訟
- 憲法

現任

- 達文西個資暨高科技法律事務所 律師

曾任

- 憲政時代雜誌執行編輯

證照

- 中華民國律師

個資法修正重點

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

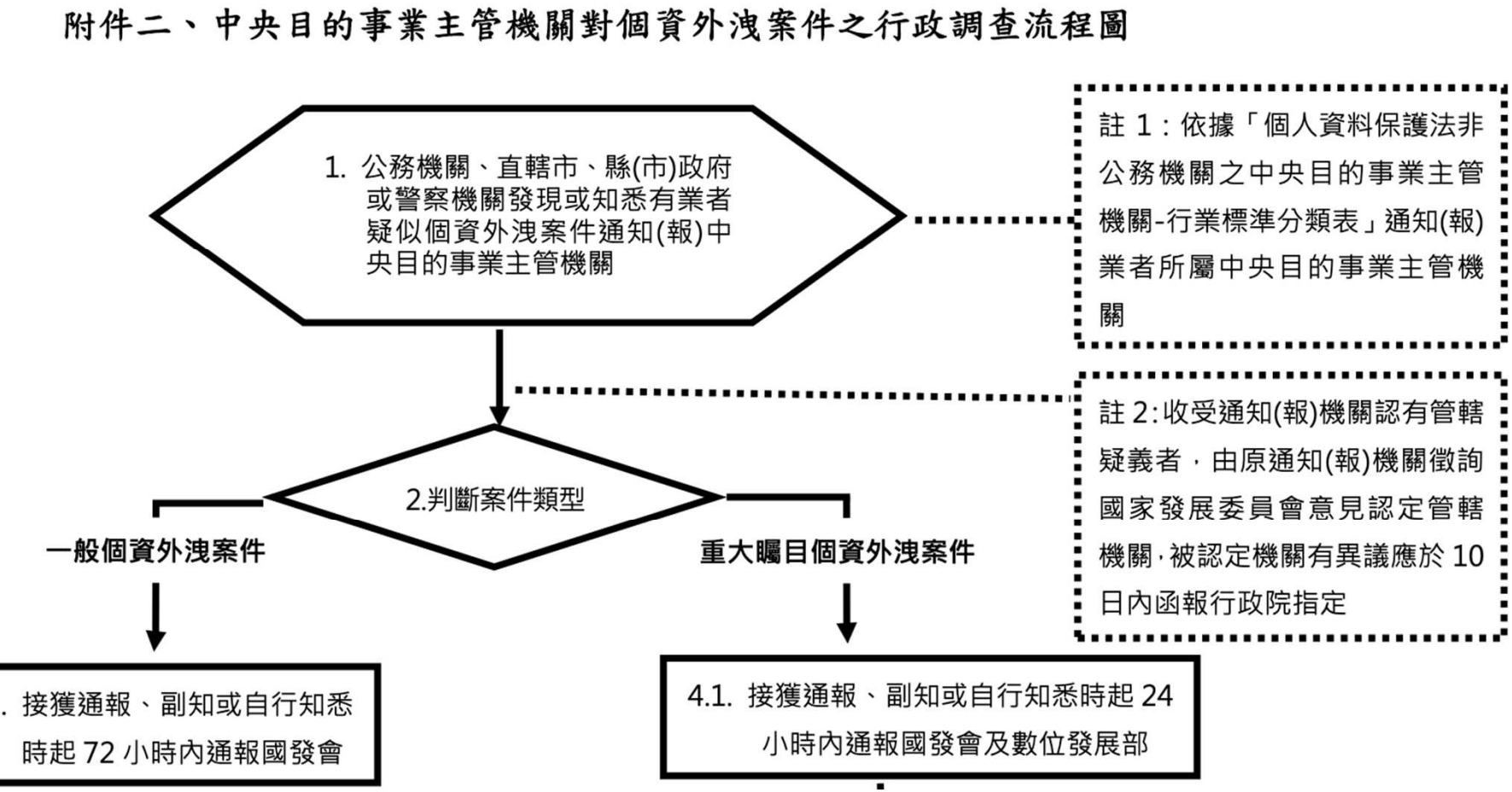
國家發展委員會

報告人：法制協調處楊淑玲處長

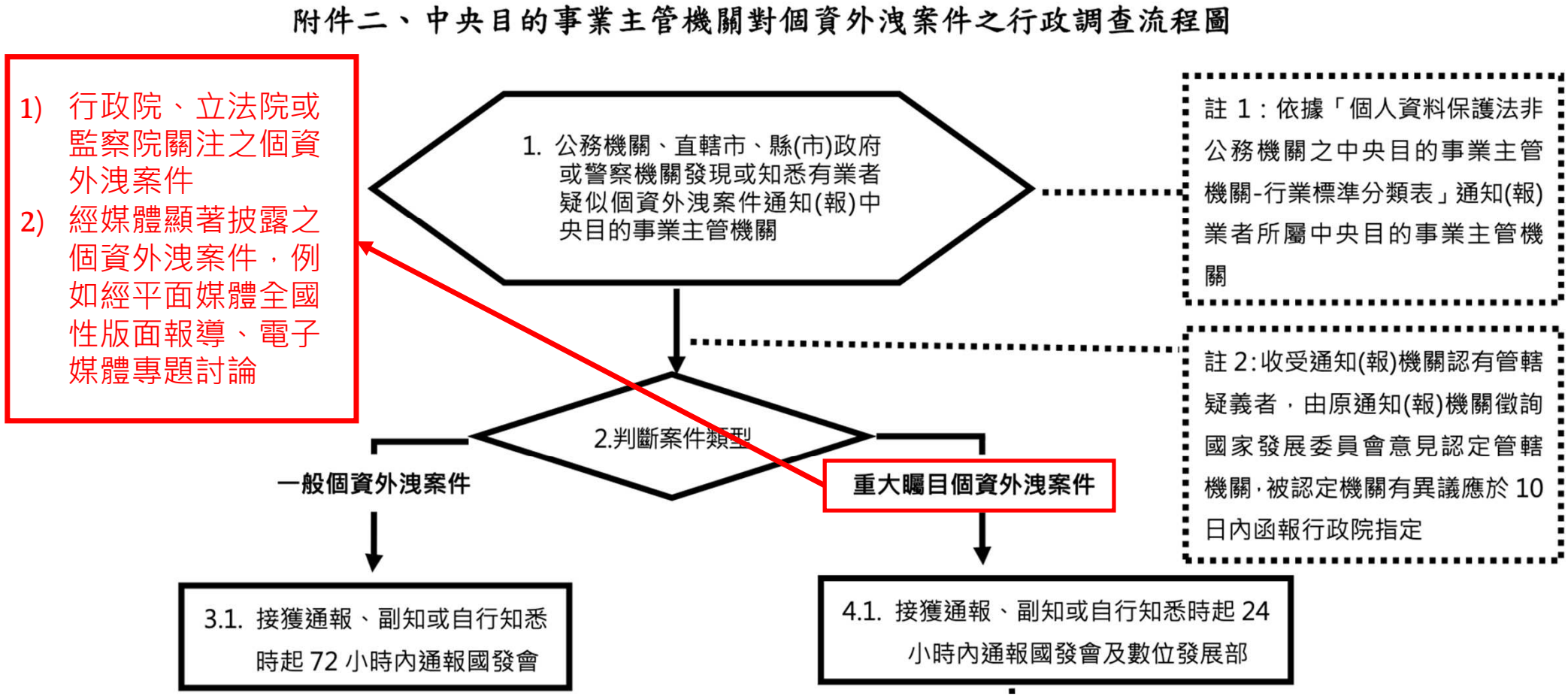
112 年 03 月 02 日

112年3月2日-行政院「個資三箭」

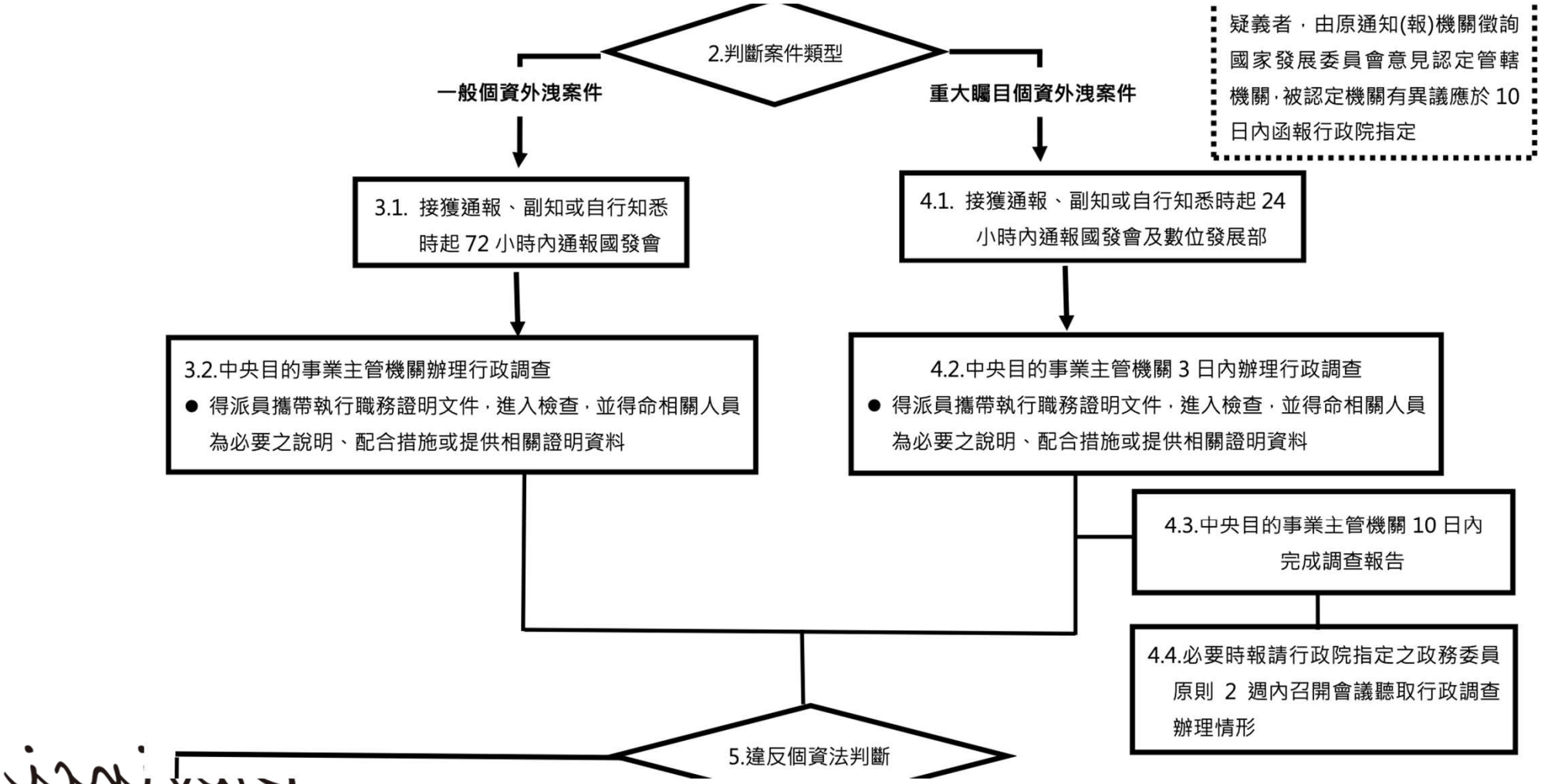
行政院及所屬各機關落實個人資料保護聯繫作業要點(112.05.29)



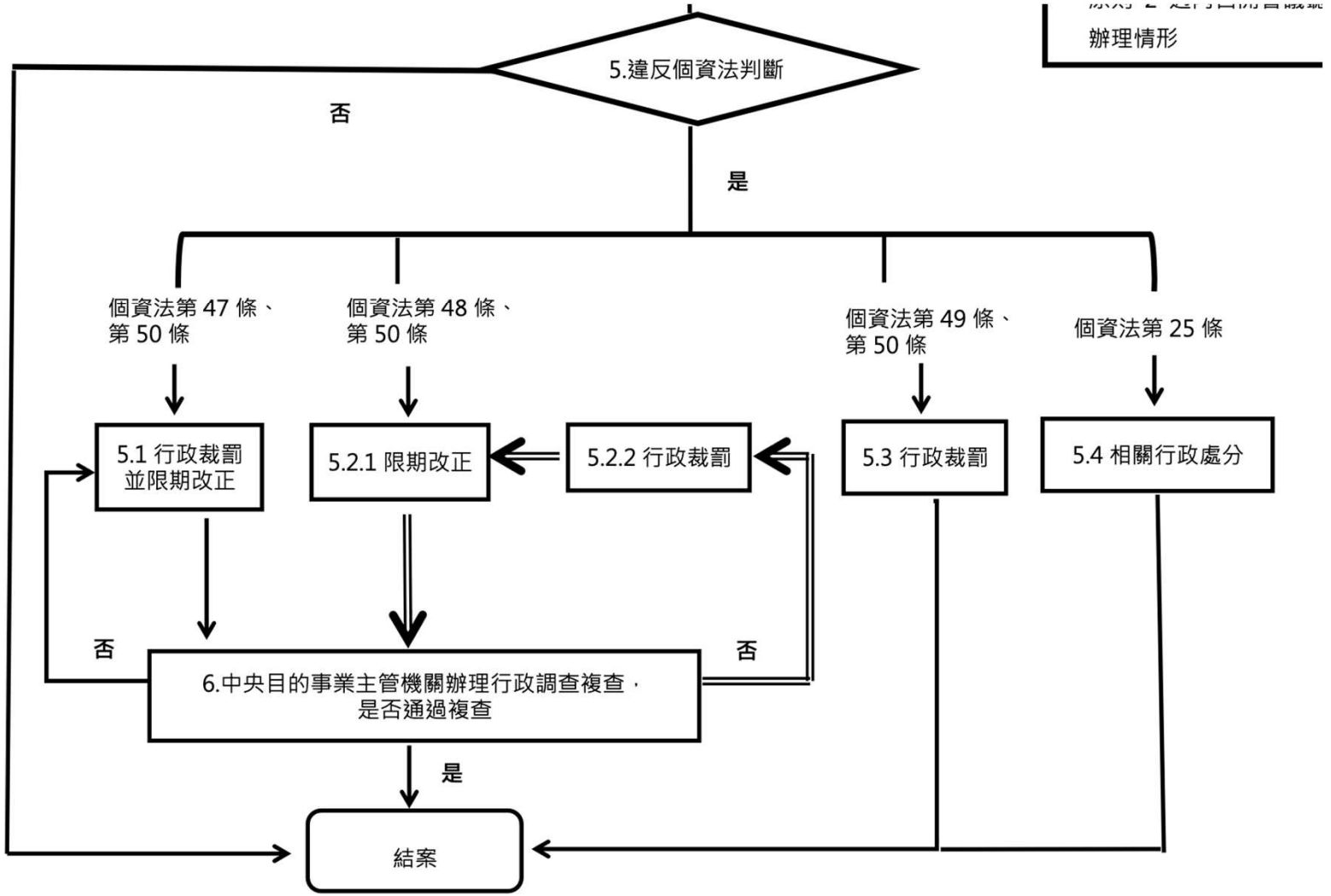
行政院及所屬各機關落實個人資料保護聯繫作業要點(112.05.29)



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



112年3月2日-行政院「個資三箭」

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 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，屆期未改正者，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，屆期未改正者，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，屆期未改正者，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。

情節重大的標準？

1、個資外洩情形

- 是否包含特種個資
- 受影響者數量
- 外洩對當事人之影響
- 外洩是否因故意或重大過失

2、安全維護措施的落實情形

- 有無依本法第二十七條第三項所定辦法規定，採取安全維護措施。
- 是否曾因未盡個人資料安全維護義務，而有發生個人資料外洩情事

情節重大的標準？

3、知悉個人資料外洩後採行措施

- 有無採取降低當事人損害之行為。
- 有無依規定主動通報主管機關。
- 有無規避、妨礙或拒絕主管機關調查之情事。
- 有無以適當方式通知當事人。

4、其他

- 是否遵循主管機關依本法規定就同一個人資料外洩案件所為之相關處分。
- 是否因該個人資料外洩獲有直接或間接之利益。

112年3月2日-行政院「個資三箭」

個資保護委員會來了

立院三讀》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掛牌(2024.12.5)

【個人資料保護委員會籌備處揭牌】個資保護邁向新階段

個資法法律責任

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 - 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。

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

- 組織受罰時
- **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**

通傳事業的個資法合規管理

個人資料的識別性

識別性

連結

挑出

推測

姓名、出生年月日、身分證號、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

其他得以直接或間接方式識別該個人之資料

須與其他資料對照、組合、連結等，始能識別該特定之個人

個人資料保護法

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

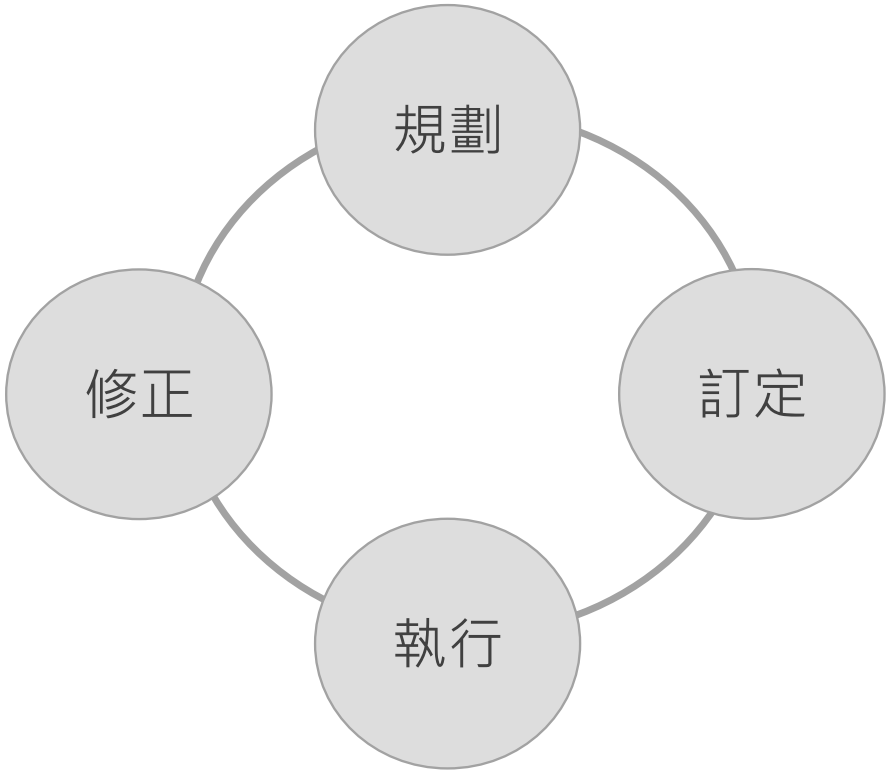
國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法 - 第3條

第1項

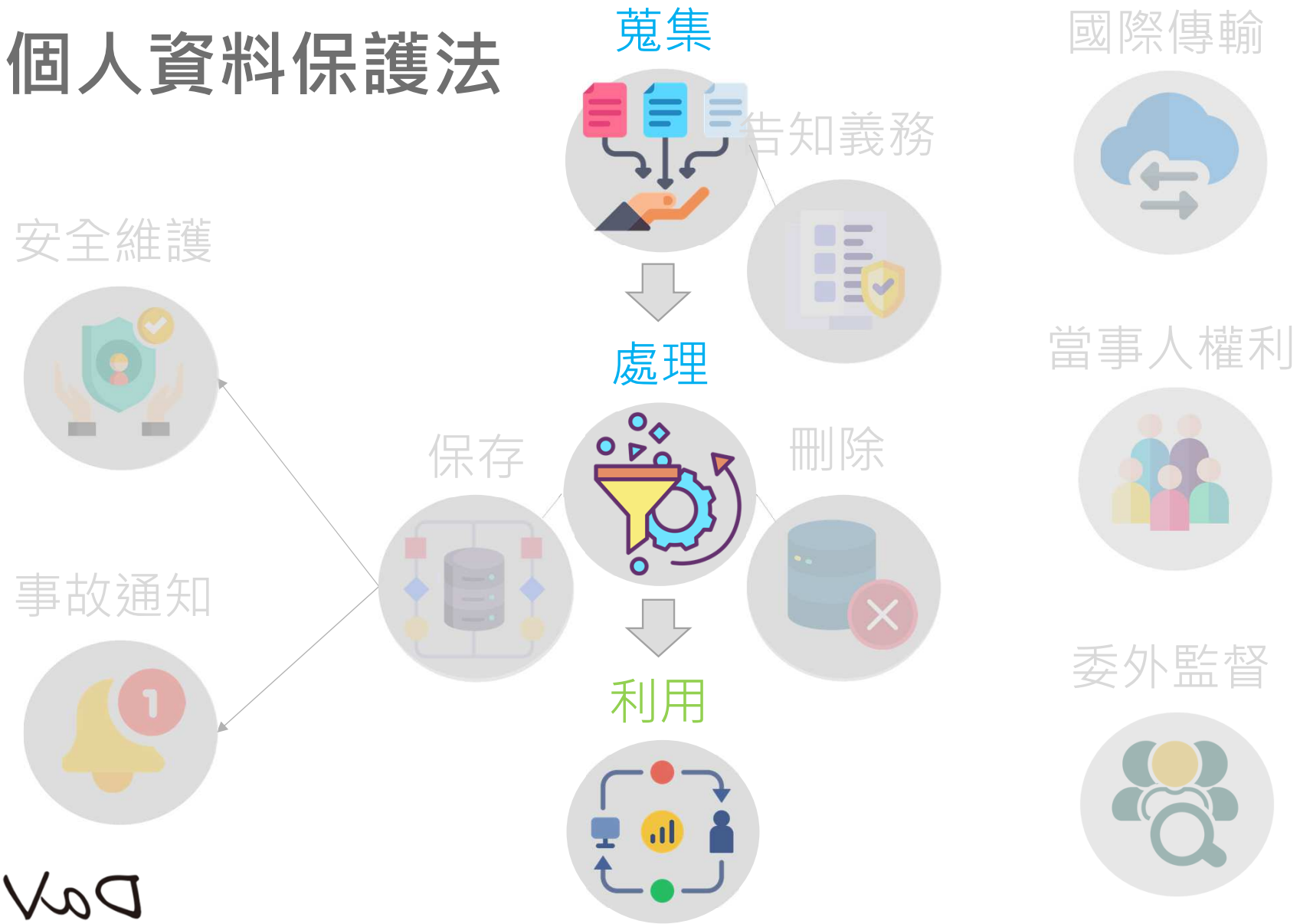
業者應依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，以規劃、訂定、修正與執行其個人資料檔案安全維護計畫及業務終止後個人資料處理方法。

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



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：

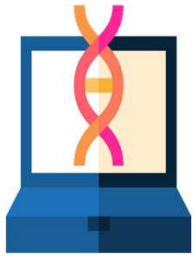
- 外部利用
- 內部利用
- 對當事人

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(知情同意)

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

西班牙-銀行違法使用個資遭罰3百萬歐元

GDPR fine: AEDP issues €3M fine to Caixabank Spain

26/10/2021 in Banking Industry, GDPR, GDPR fines

On **21 October 2021**, the Spanish data protection authority (AEPD) issued a **decision to fine Caixabank** Payments & Consumer EFC, EP, S.A.U., **€3 million** for unlawful processing of personal data and violation of **Article 6** of the **General Data Protection Regulation** (**GDPR**).

Following the complaint from the individual, AEPD conducted an investigation against Caixabank back in 2019.

The investigation uncovered that Cixabank requested information about the individual from the solvency file, even though the individual had no ongoing contracts with the bank.

The individual was also included in the **bank's marketing campaigns** for a pre-granted credit, without **proper consent** and without providing adequate information about the data processing, including profiling, or the **legal basis** used to carry out such processing.

- 金融客戶在2014年已經與銀行終止契約，雙方**沒有任何契約存在**。
- 直到2019年，客戶發現該銀行仍在取得客戶關於償債能力的資料。
- 且銀行將該客戶放在信用卡行銷活動的名單中，向客戶行銷，事先**沒有取得客戶同意**，也沒有向客戶揭露GDPR規定應告知的資訊。
- 銀行表示是內部疏失。
- 主管機關裁罰300萬歐元，並要求銀行在6個月內取得「行銷同意」。

(https://dataprivacymanager.net/gdpr-fine-3-million-to-caixabank-spain-spain/)

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

- 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。

拒絕時

- 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）。

拒絕後

國發會：拒絕商業行銷指引(112.06.13)

行銷時

- 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。

拒絕時

- 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。

拒絕後

國發會：拒絕商業行銷指引(112.06.13)

行銷時

拒絕時

拒絕後

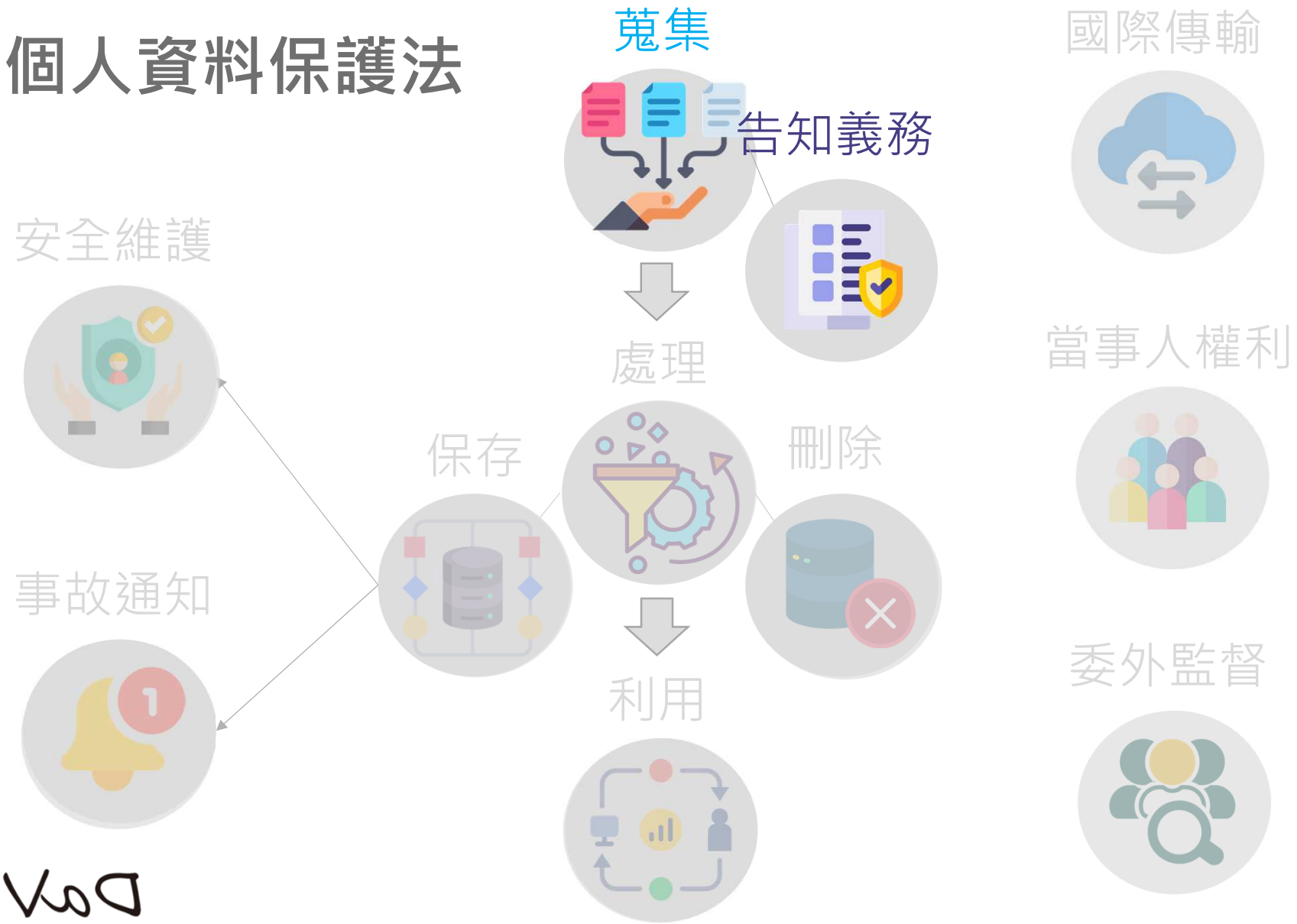
- 應記錄、更新及彙整當事人拒絕商業行銷之意思表示，並回覆當事人已收到其拒絕行銷之通知；另依本法第二十七條第一項及同法施行細則第十二條規定，採行適當之安全措施。
- 非公務機關應儘速周知所屬人員或受委託者，依本法第二十條第二項意旨，停止對該當事人進行商業行銷。

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



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

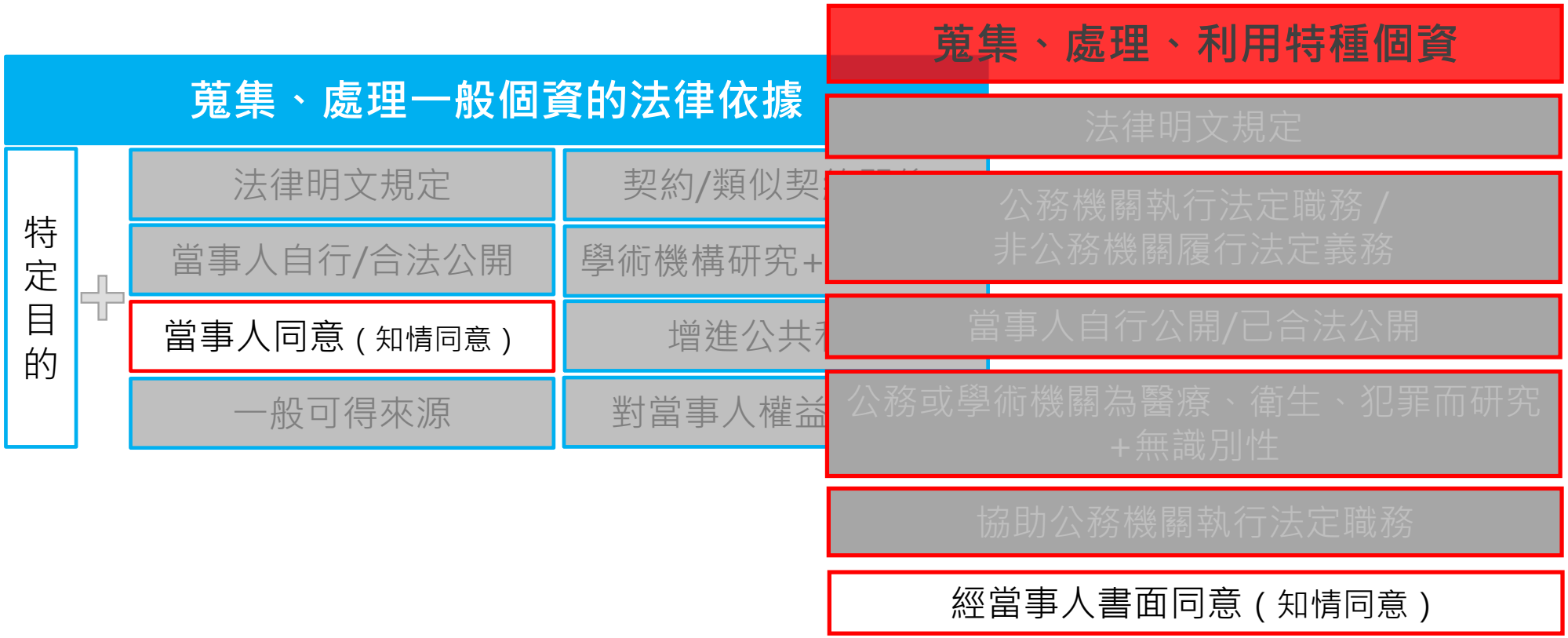
業者應就下列事項，訂定個人資料之管理程序

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。

- 依據清查出取得個資的管道，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

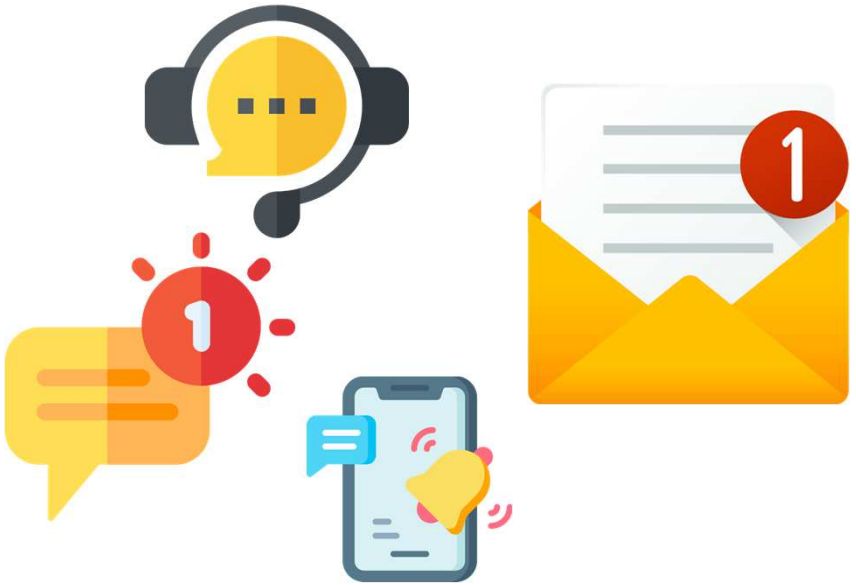
合法告知才能有效同意


蒐集、處理一般個資的法律依據
特定目的
法律明文規定
當事人自行/合法公開
當事人同意（知情同意）
一般可得來源
契約/類似契
學術機構研究+
增進公共
對當事人權益
蒐集、處理、利用特種個資
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（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。



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

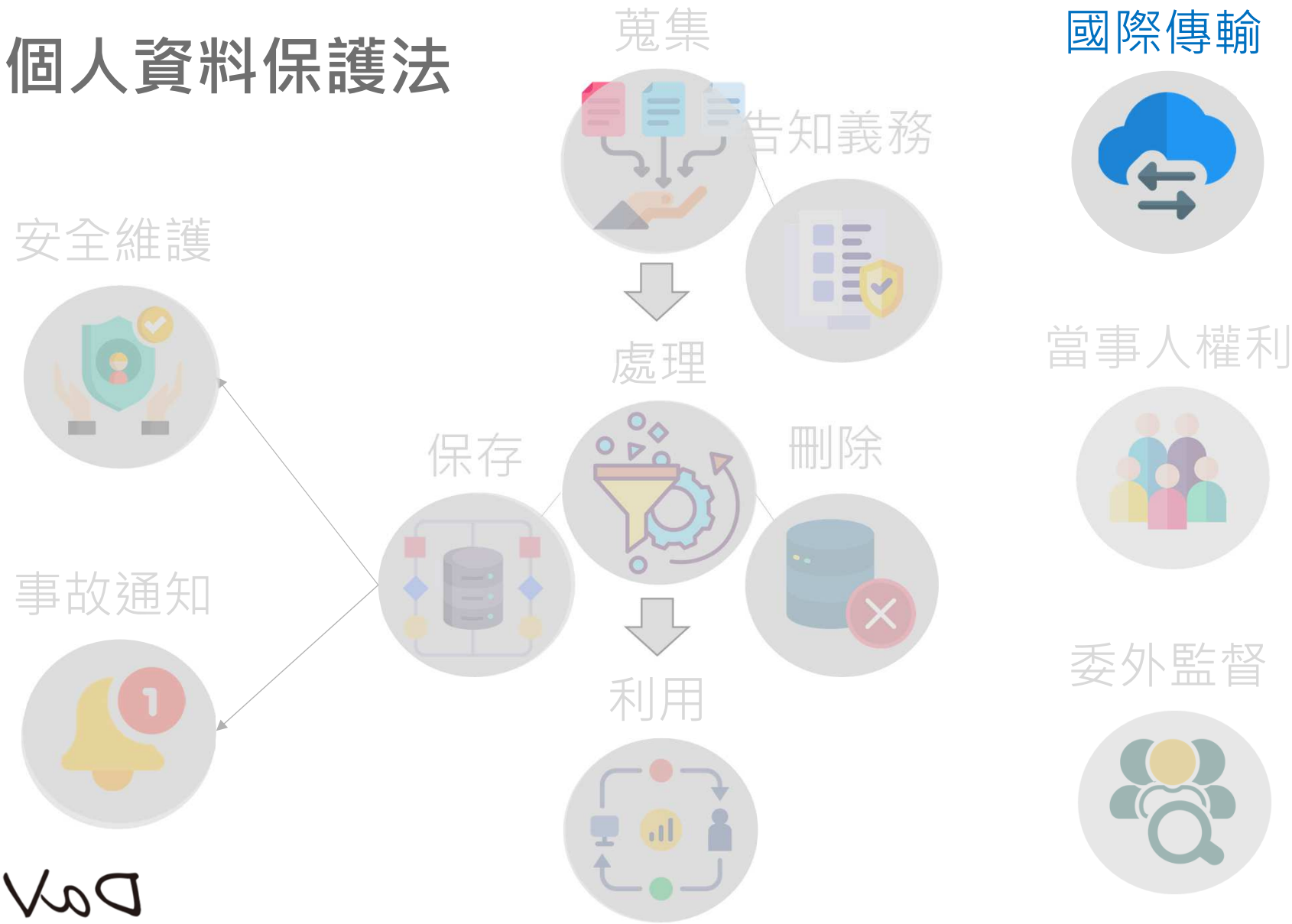
第2款 -

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



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。

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

個人資料的保存期限

個資法第11條	例外
特定目的消失/違反個資法	法令規定或契約約定保存期限
主動或依當事人請求	刪除將侵害當事人利益
刪除、停止處理或利用	不能刪除之正當事由
	當事人書面同意

西班牙-銀行違法使用個資遭罰3百萬歐元

GDPR fine: AEDP issues €3M fine to Caixabank Spain

26/10/2021 in Banking Industry, GDPR, GDPR fines

On **21 October 2021**, the Spanish data protection authority (AEPD) issued a **decision to fine Caixabank** Payments & Consumer EFC, EP, S.A.U., **€3 million** for unlawful processing of personal data and violation of **Article 6** of the **General Data Protection Regulation** (**GDPR**).

Following the complaint from the individual, AEPD conducted an investigation against Caixabank back in 2019.

The investigation uncovered that Cixabank requested information about the individual from the solvency file, even though the individual had no ongoing contracts with the bank.

The individual was also included in the **bank's marketing campaigns** for a pre-granted credit, without **proper consent** and without providing adequate information about the data processing, including profiling, or the **legal basis** used to carry out such processing.

- 金融客戶在2014年已經與銀行終止契約，雙方**沒有任何契約存在**。
- 直到2019年，客戶發現該銀行仍在取得客戶關於償債能力的資料。
- 且銀行將該客戶放在信用卡行銷活動的名單中，向客戶行銷，事先沒有取得客戶同意，也沒有向客戶揭露GDPR規定應告知的資訊。
- 銀行表示是內部疏失。
- 主管機關裁罰300萬歐元，並要求銀行在6個月內取得「行銷同意」。

(https://dataprivacymanager.net/gdpr-fine-3-million-to-caixabank-spain-spain/)

丹麥-銀行未依法刪除個資遭罰130萬歐元

GDPR fine: Danske Bank fined €1.3 million over non-compliant data deletion processes

08/04/2022 in Blog, GDPR fines

On **April 5,** The Danish Data Protection Agency (**Datatilsynet**) reported Danske Bank to the police and issued a **€1.3 million (DKK 10 million)** fine for not being able to demonstrate a compliant data deletion process along with the violation of **Art. 5 (2) GDPR**.

In November 2020, Datatilsynet initiated the investigation after the Bank itself stated that they have **identified a problem with personal data deletion** and processing of personal data that was no longer necessary for the business purposes of the Bank.

- 銀行未明文化以政策規定內部的個人資料儲存與刪除規則，也無法舉證如何在「不再需要個人資料後」，刪除超過400個系統內的上百萬名當事人的個人資料。
- 主管機關裁罰130萬歐元

(https://dataprivacymanager.net/gdpr-fine-danske-bank-fined-e1-3-million-for-non-compliant-data-deletion/)

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：

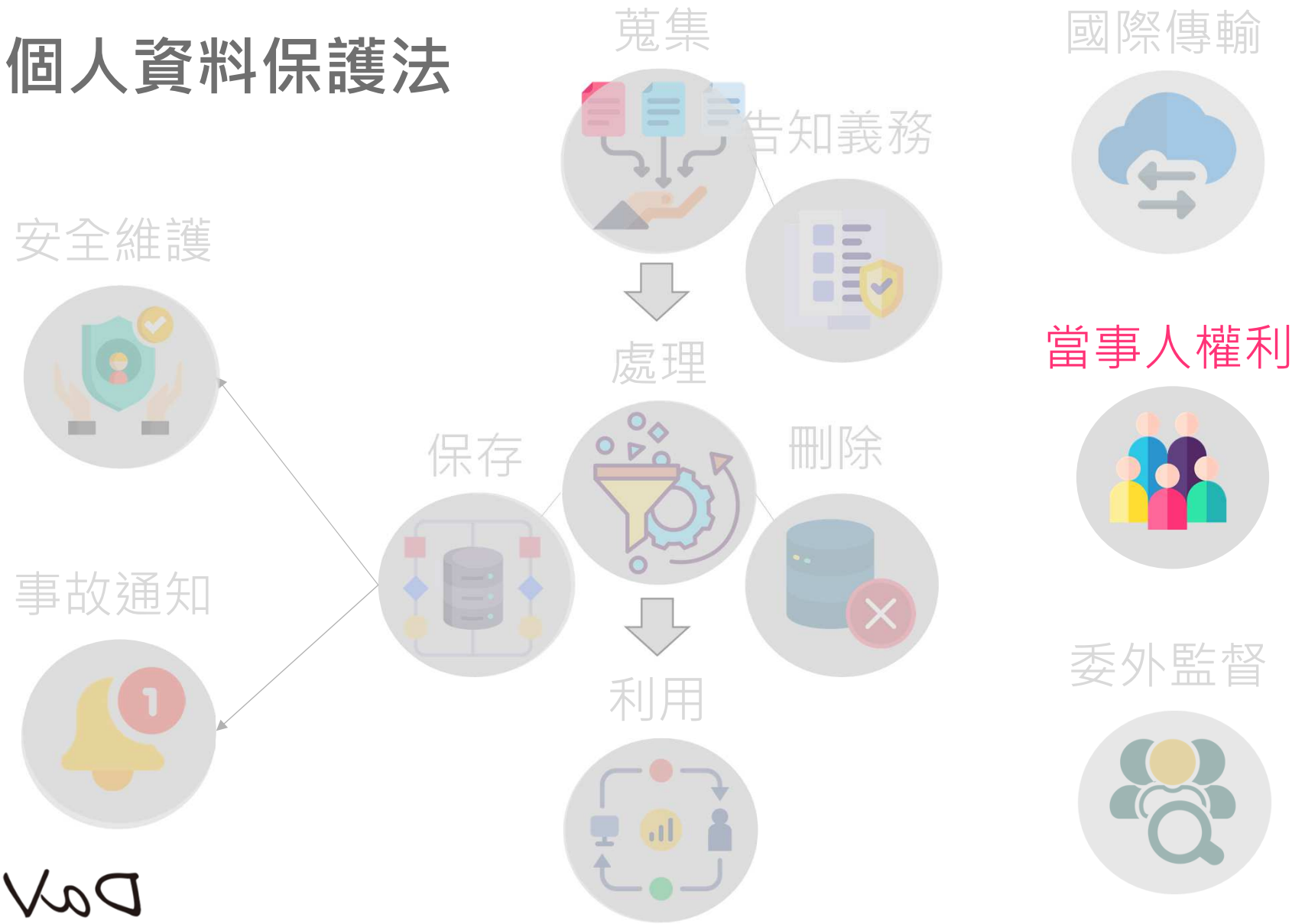
第2款 -

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



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

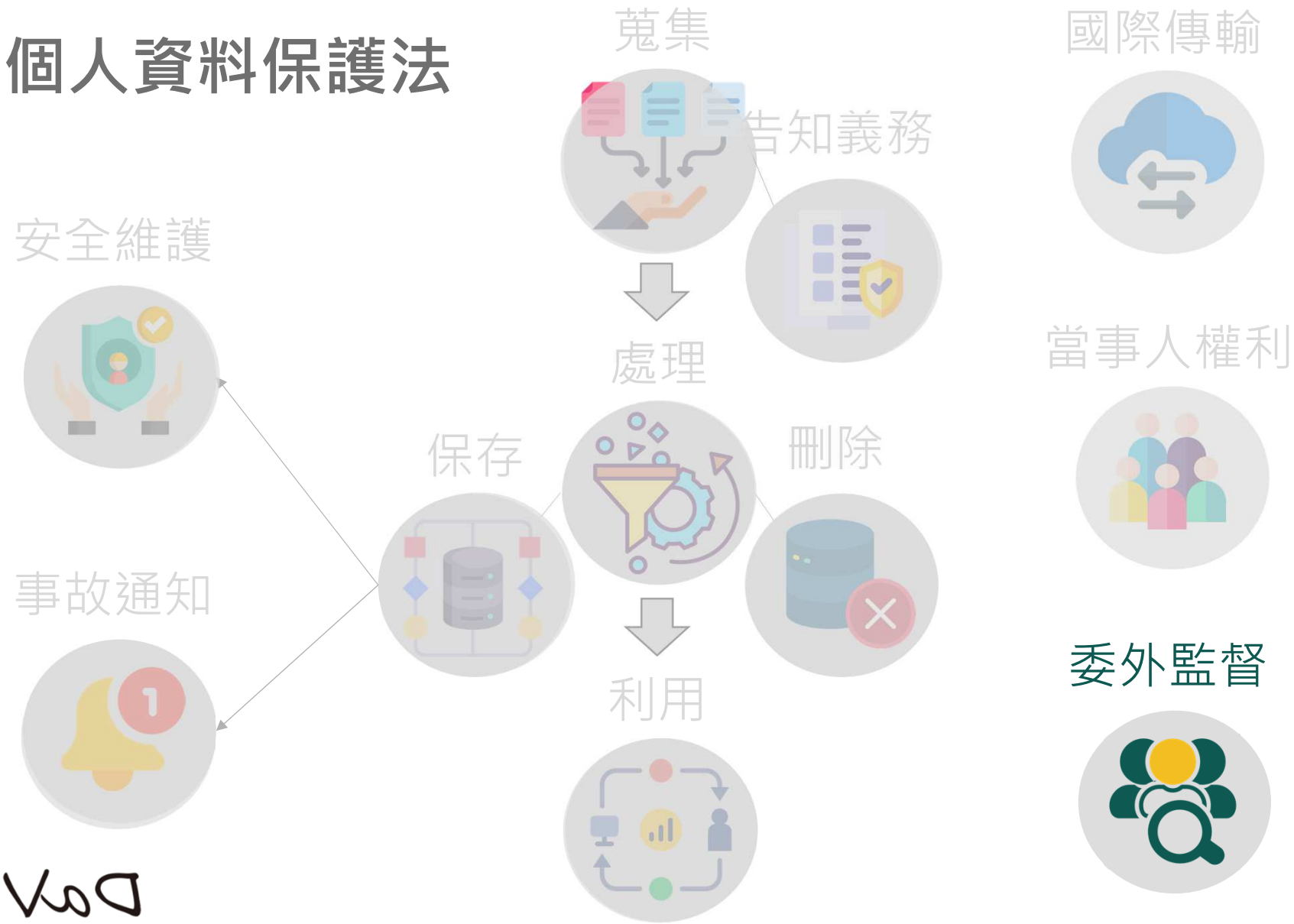
② 提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項

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



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

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。

委外廠商責任由委託機關負責

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。

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

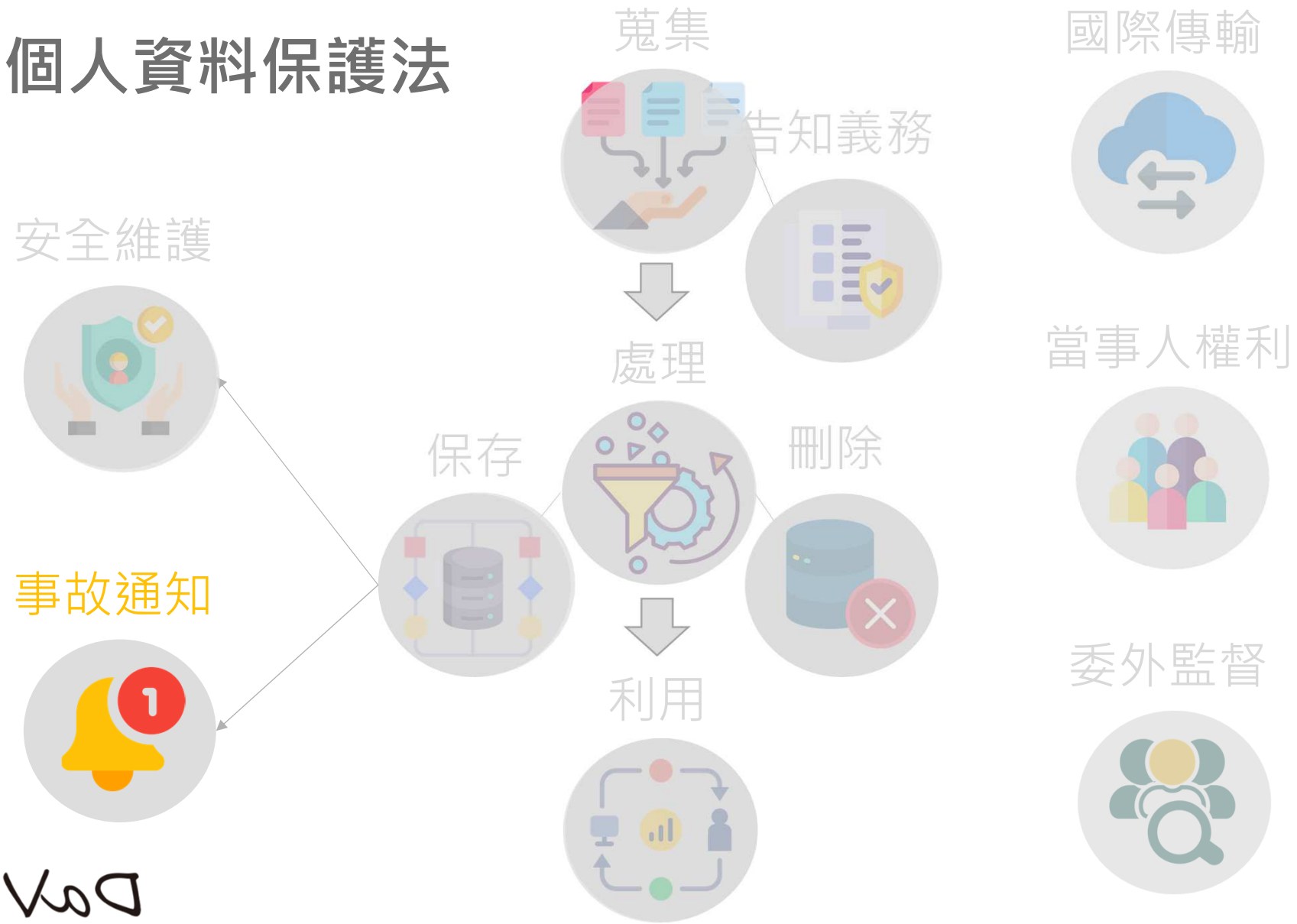
事中—執行監督

- 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

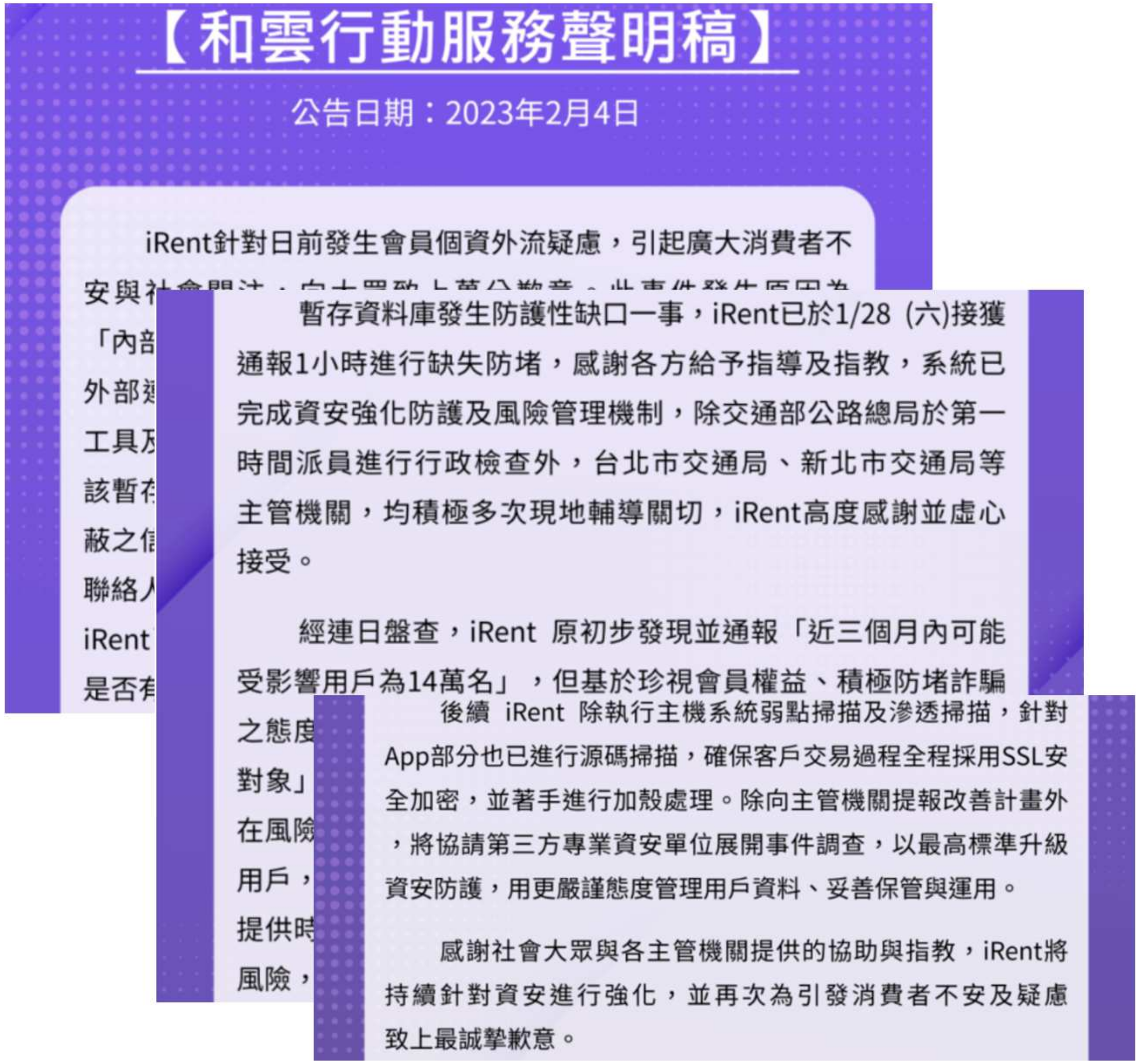
- 資料返還
- 資料銷毀
- 資料遷移？
- 你被廠商「鎖定」了嗎？

個人資料保護法



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


【和雲行動服務聲明稿】

公告日期：2023年2月4日

iRent針對日前發生會員個資外流疑慮，引起廣大消費者不

暫存資料庫發生防護性缺口一事，iRent已於1/28 (六)接獲通報1小時進行缺失防堵，感謝各方給予指導及指教，系統已完成資安強化防護及風險管理機制，除交通部公路總局於第一時間派員進行行政檢查外，台北市交通局、新北市交通局等主管機關，均積極多次現地輔導關切，iRent高度感謝並虛心接受。

經連日盤查，iRent 原初步發現並通報「近三個月內可能受影響用戶為14萬名」，但基於珍視會員權益、積極防堵詐騙

後續 iRent 除執行主機系統弱點掃描及滲透掃描，針對App部分也已進行源碼掃描，確保客戶交易過程全程採用SSL安全加密，並著手進行加殼處理。除向主管機關提報改善計畫外，將協請第三方專業資安單位展開事件調查，以最高標準升級資安防護，用更嚴謹態度管理用戶資料、妥善保管與運用。

感謝社會大眾與各主管機關提供的協助與指教，iRent將持續針對資安進行強化，並再次為引發消費者不安及疑慮致上最誠摯歉意。

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

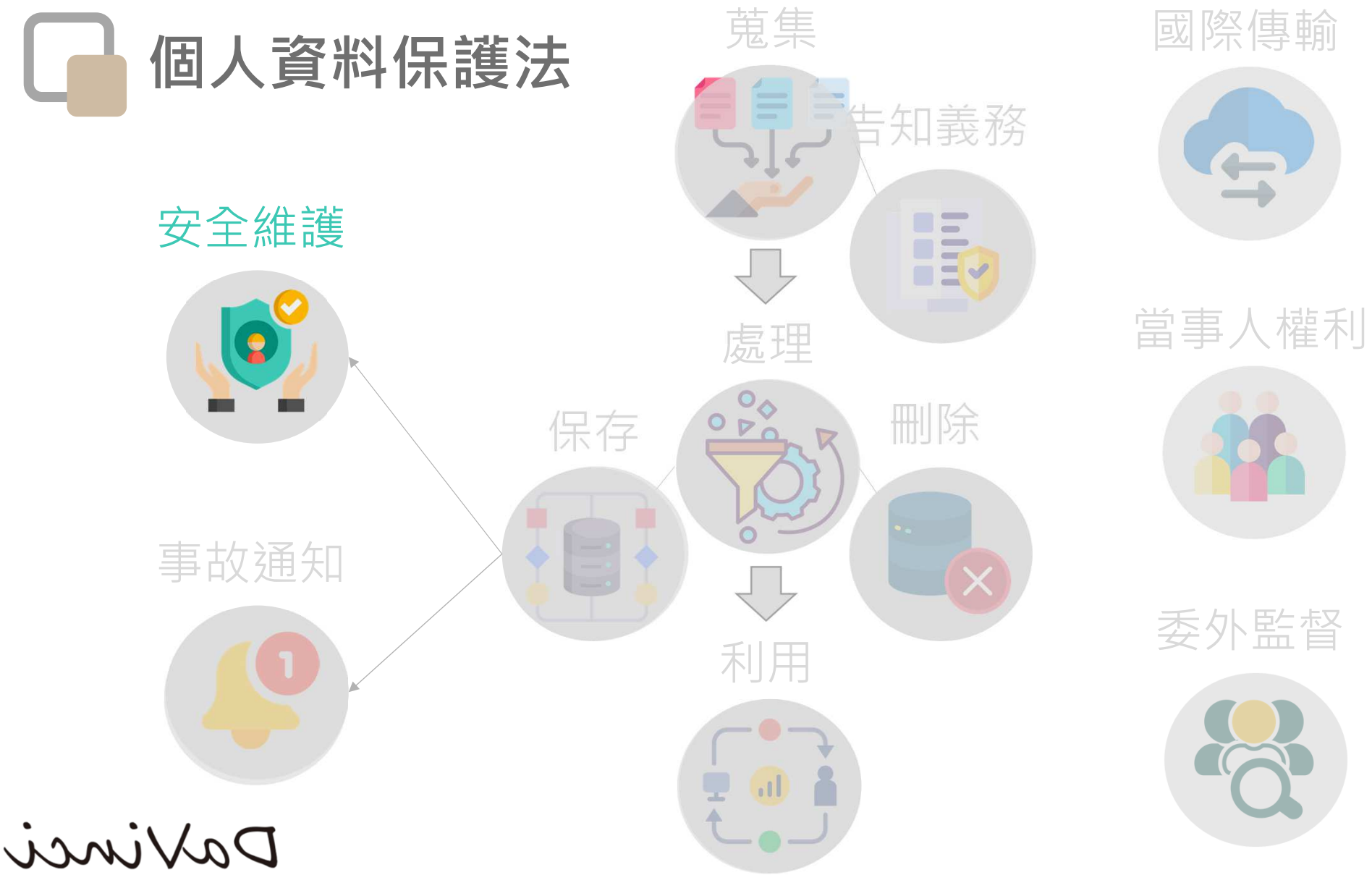
第四條 附表

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	

安全維護事項有哪些可做 - 執行面

桌面淨空

為防止未經授權之存取，同仁應於下班或長時間離開座位時，遵守桌面淨空政策

文件、設備上鎖

密級以上之文件與可攜式資訊設備存放於櫥櫃並上鎖，避免資料外洩

留意不明人員

同仁於安全區域（資訊機房）與辦公室內需隨時注意身分不明或可疑的人員

安全維護事項有哪些可做 - 執行面

環境監管

儲存敏感個人資料，或大量個人資料數量處所應具有人員監管或門禁管理

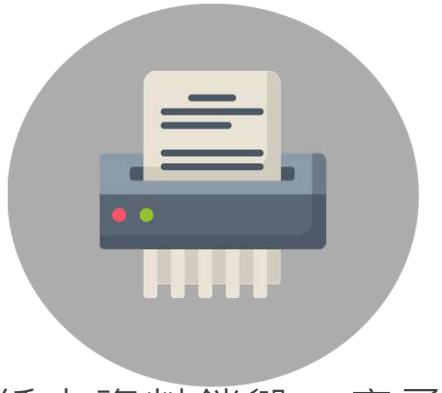
設備管理

公共使用之影印機、印表機、傳真機等含有機敏資料之輸出，應儘快取回避免遭他人取得

送修安全

資訊設備送修前，應將硬碟拆除

安全維護事項有哪些可做 - 執行面



紙本資料銷毀，應予以絞碎或其他無法還原之方式

刪除 / 移轉 / 銷毀

硬碟內部再利用，必須確認硬碟資料刪除

硬碟資料刪除 \ 銷毀，須使用資料覆寫技術或實體破壞

委外銷毀

資料銷毀若委託外部單位執行，須確認銷毀作業無法回復資料

安全維護事項有哪些可做 - 執行面

可攜式電腦與儲存媒體管理

重要資料應注意存放於安全處所，並指定專人保管以避免遺失或遭竊

可攜式儲存媒體儲存敏感或大量個資檔案時，應具密碼開啟機制

委外運送

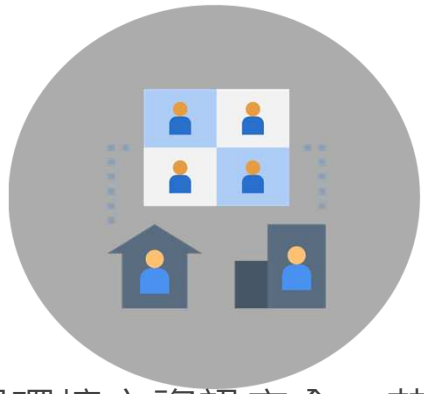
如委由外部單位運送，應選擇具有信譽之廠商

彌封、當面送達並簽收或資料內容加密保護

安全維護事項有哪些可做 - 執行面

存取控制

未經授權，不得存取業務範圍外之資訊資產或個人資料檔案



使用環境之資訊安全，若遠端連線使用，應以安全連線方式，如限制來源IP、VPN、加密或設備辨識等

安全維護事項有哪些可做 - 執行面

個人電腦管理

禁止使用或下載未經授權或與業務無關之軟體

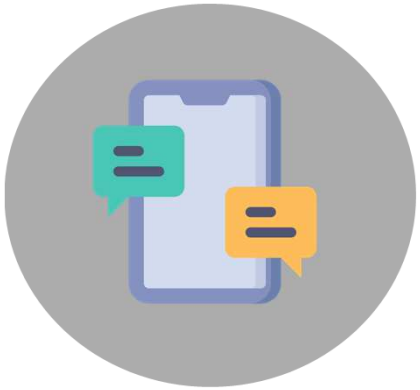
作業系統更新，必要的應用軟體更新；安裝防毒軟體 + 更新

設定開機登入帳號密碼，啟動螢幕保護並以密碼鎖定

個資存於共用資料夾，具帳號密碼管控存取；人員異動即時更新

安全維護事項有哪些可做 - 執行面

個人行為管理



除非必要，不在通訊軟體（尤其是多人群組）傳輸個資檔案

傳輸檔案前，依照資料重要性評估密碼保護措施

傳輸檔案前，再次檢查收件對象

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。

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28Ⅰ、Ⅲ、29，民法第184條)

非財產上損害

(個資法第28Ⅱ、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，惟此等事實因有於網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[redacted]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[redacted]，[redacted]應不致於陷於錯誤而遭詐騙，堪認[redacted]公司前揭未盡適當安全維護措施，致洩漏[redacted]個人資料之行為，與[redacted]遭詐騙受有25萬7,892 元損害間有相當因果關係，[redacted]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？

（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[redacted]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[redacted]，[redacted]應不致於陷於錯誤而遭詐騙，堪認[redacted]公司前揭未盡適當安全維護措施，致洩漏[redacted]個人資料之行為，與[redacted]遭詐騙受有25萬7,892 元損害間有相當因果關係，[redacted]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

見解

- 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：

企業是否有過失應如何認定？

見解1	做到以下事情，不算有過失： 1. 做好硬體的定期弱點檢測 2. 進行相關安全維護措施 3. 於個資外洩發生後對消費者通報

裁判字號： 臺灣臺北地方法院 111 年度 訴字第 5578 號 判決

裁判案由： 損害賠償等

裁判日期： 民國 112 年 03 月 20 日

Hewlett Packard Enterprise之掃弱報告存卷為憑（見本院卷第215至222頁），且亦已於110年11月5日取得系統敏感資料數位簽章認證（見本院卷第223至224頁），並由[redacted]再於偵測異常IP侵入後，隨即於同月18日至同月19日委請訴外人精誠科技股份有限公司進行滲透測試服務，以國際標準之OWASP（Open web Application Security Project）、OSSTMM（Open Source Security Testing Methodology Manual）以檢測網際網路弱點，並僅於主機服務掃描時，查覺1項中風險弱點並警示注意，其於就網站服務滲透均無發現異常等情，有精誠科技整合股份有限公司提供予[redacted]之滲透測試報告書存卷為憑（見本院卷第289至304頁），足見[redacted]所使用由被告墨攻公司建置管理之系爭訂購系統，已於事情盡其可能防堵外部入侵，並於事後查覺異常IP侵入之數日內已再度為弱點檢測。

企業是否有過失應如何認定？

見解1	做到以下事情，不算有過失： 1. 做好硬體的定期弱點檢測 2. 進行相關安全維護措施 3. 於個資外洩發生後對消費者通報

頁）；另數位發展部數位產業署112年1月13日之回函，亦以：平時[redacted]已有相關資料維護措施：包括已強制廠商登入位置綁定、AES256加密機制針對廠商帳號密料、多重伺服器分散資料管理、資料庫與程式分開存放、主機帳密權限控管與RSA私鑰管理、限定防火牆規則僅特定IP及帳號密碼始得進入、Linux主機使用防毒體ClamAV、辦公室環境以ESET防毒軟體監控，以及伺服器安裝關貿網路EDR端點防護、訂定個資及資安政策文件等；事發時已採取因應措施：包含立即向檢警單位報案、於110年8月31日及11月16日以emai通知遭個資外洩之旅宿業者客戶與官方網站宣導消費者資安觀念等。事後採取改善措施：包含強制客戶加入Email驗證、實施一次性動態密碼(OTP)能、鎖定IP且強制客戶登入皆須要驗證IP、Fortify全系統弱點偵測掃描、公司電腦全面安裝關貿網路EDR端點防護、110年11月修補後透過精誠資訊進行網頁弱掃測試、111年9月14日透過nessus進行主機掃描、取得ISO 27001資訊安全管理證書等情（見本院卷第265至267頁），亦徵被告已於事情、事後均本於防止系爭訂購系統之用戶個資被竊之相關措施，自難認原告個資外洩一事係因被告之過失行為所致。

企業是否有過失應如何認定？

見解1	做到以下事情，不算有過失： 1. 做好硬體的定期弱點檢測 2. 進行相關安全維護措施 3. 於個資外洩發生後對消費者通報

(3)又關於非公務機關之用戶個資遭竊取之通報義務，依據前開個資法第12條係以「非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害」為前提，故非公務機關倘並無違反個資法之規定，本即與該通知義務之前提不合，則本件被告既如前開認定，並無因過失違反個資法之情節，自無庸負擔該通報義務；更遑論[redacted]之官方網站首頁，實早於110年8月28日，即於原告最後一次使用系爭訂購系統訂購溫泉票之110年11月3日前，已有「貼心提醒 防範詐騙公告」之公告（見本院卷第205至211頁），且該公告已記載詐騙手法包括「謊稱為飯店系統遭駭客入侵，訂單被改為團體訂單會遭到扣款，並再次謊稱為銀行人員要求解除款項，以及操作銀行轉帳」之內容（見本院卷第207頁），自已透過上開合理方式警示用戶即原告。另兩造均不爭執[redacted]亦曾再於111年1月5日、111年1月8日、111年1月12日、111年1月19日、111年2月21日持續接獲[redacted]之防詐騙簡訊等情，已如前述，自難認被告有何違反個資法第12條、個資法施行細則第22條之違反通報義務之情形。

企業是否有過失應如何認定？

見解2	1. 安全維護措施要看是否有確實落實 2. 行政機關的調查結果不拘束法院 3. 如有委外蒐集處理利用行為，應確保有落實監督之責任

裁判字號： 臺灣高等法院 112 年度 上字第 656 號 判決

裁判案由： 損害賠償等

裁判日期： 民國 113 年 01 月 30 日

頁就ClamAV應用程式之介紹；被上證15 [redacted]資訊安全管理政策、被上證16：[redacted]個人資料保護管理政策（見本院卷一第343至355頁），均屬抽象之管理規範，非就系爭訂購系統所為之具體維護措施；被證8：關貿EDR雲服務交貨確認表、被證9：關貿網路EDR端點防護說明、被證10：「精誠全盤滲透報告」、「墨攻滲透報告書 210.241.131.226Nessus」、「墨攻滲透測試報告書」、被上證19：[redacted]就XSS攻擊提出之改善方式（見原審卷第235至257頁，本院卷一第361頁），均屬110年11月16日系爭訂購系統資料庫遭駭客侵入竊取個資後所為，亦未見與[redacted]就個資外洩前之管理維護系爭訂購系統行為，有何關聯性。是以被上訴人所提上開資料，均無法證明[redacted]就其管理維護之系爭訂購系統所保有之上訴人個資，已盡採取適當安全措施之責，被上訴人上開抗辯，即無足取。上訴人主張[redacted]就其系爭個資外洩而遭詐騙集團不法利用，有違反個資法第27條第1項規定之疏失，洵屬可採。

企業是否有過失應如何認定？

見解2	1. 安全維護措施要看是否有確實落實 2. 行政機關的調查結果不拘束法院 3. 如有委外蒐集處理利用行為，應確保有落實監督之責任

(2)至數發部112年1月13日函固認:「本署檢視前揭所復內容暨佐證資料，認為[redacted]之平時維護措施尚稱妥適，亦於110年8月及11月事件發生時之應變措施尚屬合宜，並持續精進其個資安全管理措施，且已依照本署要求補充相關佐證資料，該公司之改善措施亦尚稱合理。」(見本院卷一第266頁)，惟數發部之調查程序與訴訟事件程序不同，且其認定並無拘束本院之效力，被上訴人抗辯應援引數發部上開函文及112年7月28日函檢送之相關資料為有利被上訴人之認定云云，亦非可取。

企業是否有過失應如何認定？

見解2	1. 安全維護措施要看是否有確實落實 2. 行政機關的調查結果不拘束法院 3. 如有委外蒐集處理利用行為，應確保有落實監督之責任

3.被上訴人抗辯麗禧公司委由[redacted]開發電子票證業務並管理客戶資料，已盡其選任及監督義務云云。惟查，系爭訂購系統之消費者個資係存放於[redacted]，上訴人之系爭個資確曾輸入系爭訂購系統使用，且會保留於該系統中，[redacted]就其所保有之上訴人系爭個資，即應採行適當之安全措施，防止其個資被竊取或洩漏，則[redacted]委由[redacted]管理維護系爭訂購系統，亦應對[redacted]為適當監督，而被上訴人所提被上證17：墨攻公司官方網站首頁、被上證18：墨攻公司擁有多項專利（見本院卷一第357、359頁），均為[redacted]之單方資料，無法據以證明[redacted]於上訴人系爭個資遭竊外洩前，已就[redacted]管理維護系爭訂購系統，為適當監督之行為，被上訴人上開抗辯，不足採信。是上訴人主張[redacted]就其系爭個資外洩而遭詐騙集團不法利用，有違反個資法第27條第1項規定之疏失，亦屬可採。至交通部觀光局111年12月9日回函固認：「...[redacted]於個資外洩前後皆採行相關因應措施及處置，除於事前曾要求[redacted]加強個資防護措施...加強飯店本身各項個資安全防護機制且持續進行改善，尚符個人資料保護法相關規定...」（見原審卷第142頁），並於「主管機關就個資外洩事件判斷是否違反個資法」部分，調查結果表示「否」（見原審卷第151至152頁），惟交通部觀光局之調查程序與訴訟事件程序不同，且其認定並無拘束本院之效力，無從據為有利被上訴人之認定。

謝謝聆聽

THANKS FOR YOUR ATTENTION

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

孔德澔律師

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