

收字第 145 號	
115.3. -6	
經辦人	

檔 號：

保存年限：

法務部 書函

地址：100204臺北市中正區重慶南路1段
130號

承辦人：周元華

電話：02-21910189分機2340

900

屏東縣屏東市復興路468號

受文者：屏東律師公會

發文日期：中華民國115年3月3日

發文字號：法檢決字第11504502800號

速別：普通件

密等及解密條件或保密期限：

附件：如主旨

主旨：為強化律師業之個人資料保護及資訊安全維護意識，檢附個人資料保護委員會籌備處彙整「個資安維案件常見爭點之訴願決定及行政訴訟判決重點分析報告」，請貴會參閱並轉知所屬會員知悉，以避免類此違法情形發生，請查照。

說明：依行政院115年2月4日「行政機關落實個人資料保護執行聯繫會議」決議辦理。

正本：全國律師聯合會、基隆律師公會、臺北律師公會、桃園律師公會、新竹律師公會、苗栗律師公會、臺中律師公會、彰化律師公會、南投律師公會、雲林律師公會、嘉義律師公會、臺南律師公會、高雄律師公會、屏東律師公會、宜蘭律師公會、花蓮律師公會、臺東律師公會

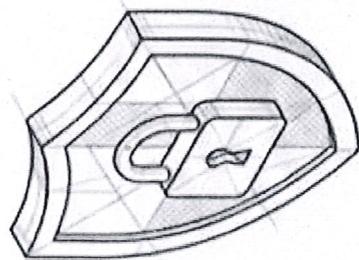
副本：個人資料保護委員會籌備處、本部檢察司

法務部



個資安維案件常見爭點之 訴願決定及行政訴訟判決 重點分析報告

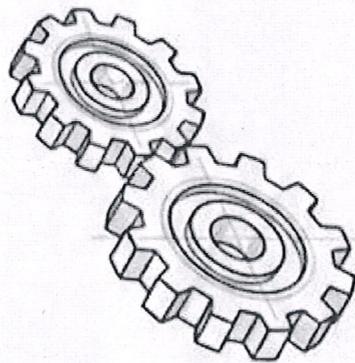
三大核心重點



核心義務一：內部防護

安全維護措施

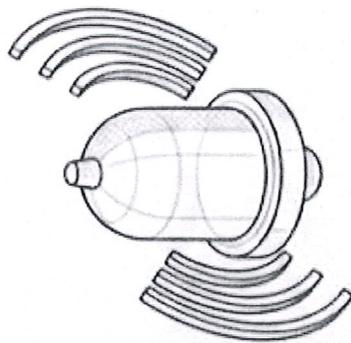
個資法§27
施行細則§12
各部會安維辦法



核心義務二：外部控管

委外監督責任

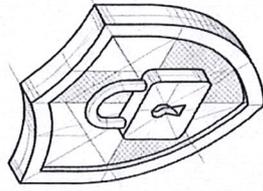
個資法§4
施行細則§7、8
各部會安維辦法



核心義務三：事故通知

即時通知當事人

個資法§12
施行細則§22



核心義務一：內部防護 安全維護措施

◆個資法第27條第1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。

◆個資法施行細則第12條

- 本法……第27條第1項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。
- 安全措施得包括下列事項，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：

- 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、軌跡資料及證據保存。
- 十一、個人資料安全維護之整體持續改善。

◆各中央目的事業主管機關所訂定之安全維護管理辦法(目前有60部)

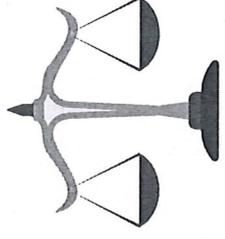


常見爭點一 未發生竊取或洩漏，即無違反規定？

違法認定

個資法第27條第1項課予非公務機關安全保管責任之緣由，目的係為阻絕個人資料遭侵害之可能性。立法目的明示課予非公務機關對所持有之個人資料安全負保管責任，而非等到實際損害發生後始得處罰。

→ 業者未發生竊取或洩漏，不代表沒有違反規定。

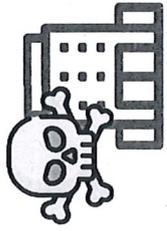


裁罰處分衡酌因素
是否竊取或洩漏僅作為
「裁罰輕重」之衡量，
而非免責依據。





常見爭點二 只要採購防護軟體，即能免責？



業者

為加強公司電腦資安等級，花費數十萬加裝正版防毒軟體，並升級為主控台模式，電腦作業軟體亦全面升級，已盡力改善資訊安全問題而非完全無作為。



訴願機關

個資法第27條第1項規定課予非公務機關應採取適當安全維護措施以防止個人資料被竊取或洩漏之義務，以確認個人資料外洩原因並採取適當之安全措施，自為訴願人之責任，資訊安全係風險值概率而非有、無之問題，必需長期投入時間與資源，始得維護資訊安全之水準，絕非單純購買軟、硬體即可防杜，要難以無資安專長、無單位可以確認個人資料外洩原因等，卸免查證其安全措施是否適當及防止個人資料外洩之責。

採購防護軟體 ≠ 合法
單純購買軟硬體不足
以主張免責。(有做但
尚未完備)

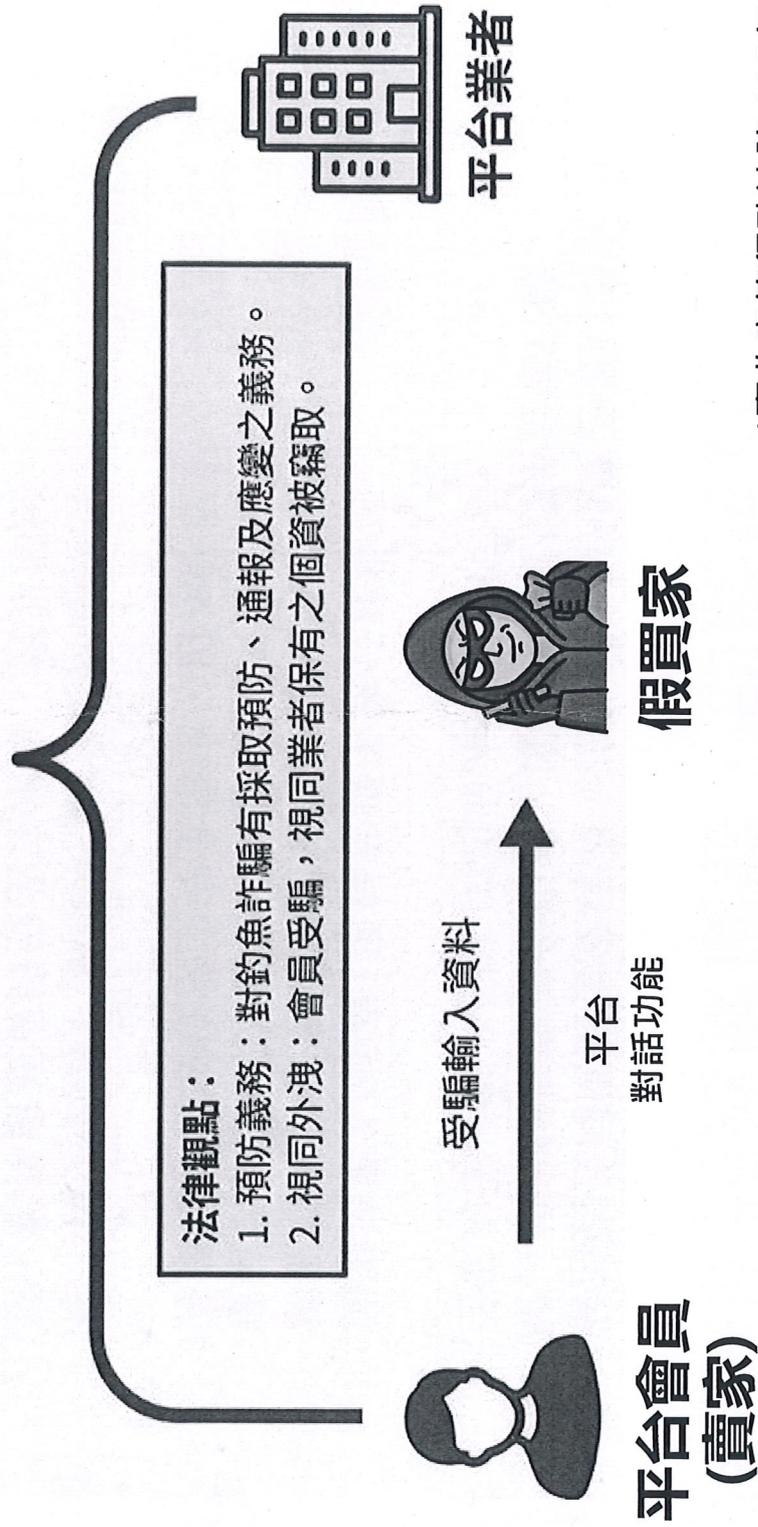
持續性要求
適當之安全措施需「長
期投入」

*行政院臺訴字第1050175635號、

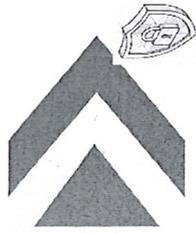
第1050174274號訴願決定



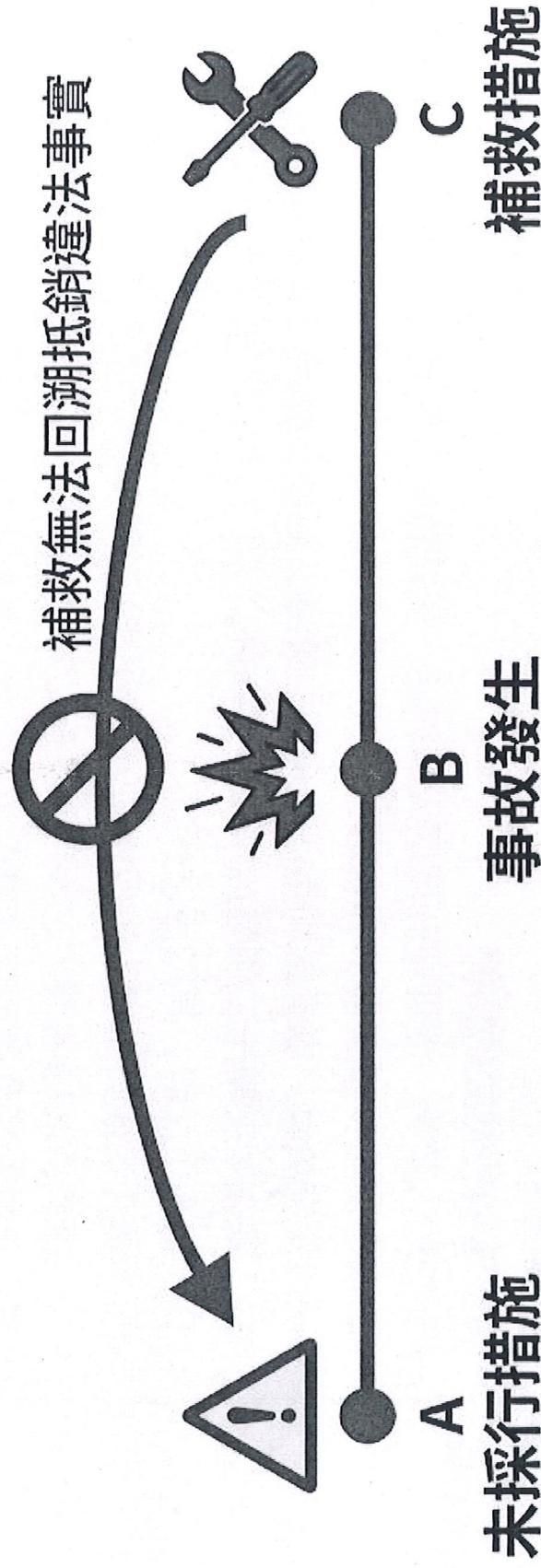
常見爭點三 會員被他人釣魚詐騙資料，業者是否負責？



* 臺北高等行政法院 112 年度訴字第 889 號、
第 1396 號判決



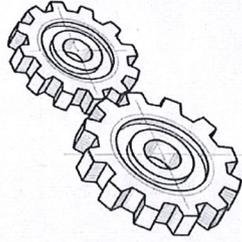
常見爭點四 事後補救能否免責？



違法點

義務履行

*行政院院臺訴字第1145015714號、
第1145006174號訴願決定



核心義務二：外部控管
委外監督責任

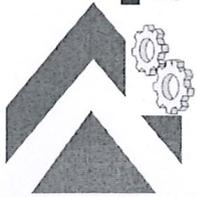
◆**個資法第4條**

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

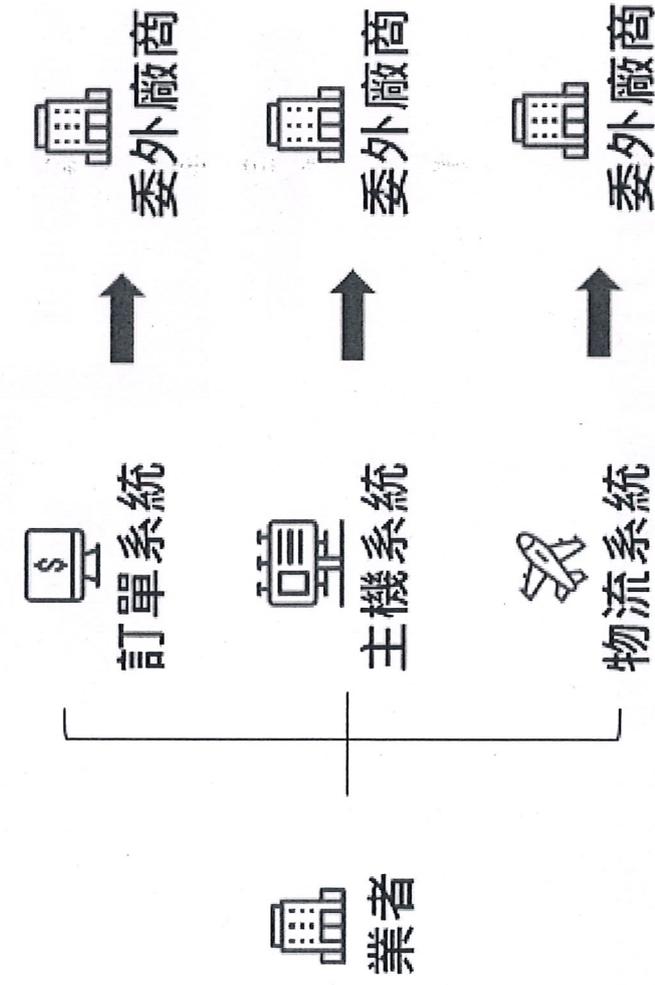
◆**個資法施行細則第8條**

- 委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為**適當之監督**。
- 前項監督至少應**包含**下列事項：
 - 一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
 - 二、受託者就第十二條第二項採取之措施。
 - 三、有複委託者，其約定之受託者。
 - 四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。
 - 五、委託機關如對受託者有保留指示者，其保留指示之事項。
 - 六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。
- 委託機關應**定期**確認受託者執行之狀況，並將確認結果記錄之。

◆**各中央目的事業主管機關所訂定之安全維護管理辦法(目前有60部)**



常見爭點五 業者以「未具資安專業」為由，主張免責？



-
1. 簽立契約
 2. 明定雙方權責
 3. 採取適當安全措施

*行政院院臺訴字第1050183642號、
第1050184074號訴願決定



常見爭點六 監督委外廠商之實際作為？

PIPC

保存紀錄

完整保留查核與
改善紀錄

*個資法施行細則第8條第3項

實際查核

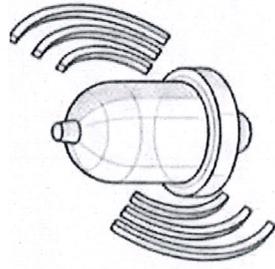
定期去查核廠商，
而非僅看書面報告

*行政院臺訴字第1125021518號、
第1135019458號訴願決定

合約規範

訂定有監督條款之
合約

*行政院臺訴字第1135019458、
第1135020662號訴願決定



核心義務三：事故通知

即時通知當事人

◆個資法第12條第1項

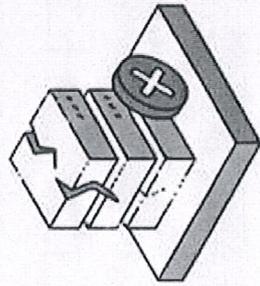
- 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

◆個資法施行細則第22條

- 本法第十二條所稱**適當方式通知**，指即時以言詞、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。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。
- 依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。



常見爭點七 通知當事人之方式及內容？



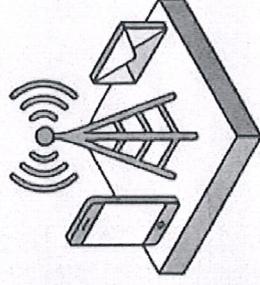
事故發生

通知內容

- 被侵害之事實
- 已採取之因應措施

(注意：不得僅發送一般性防詐騙提醒)

*行政院臺訴字第1080175176號、
第1100168370號訴願決定



即時通知

通知方式

- 應個別通知
- 以言詞、書面、電話、簡訊、電子郵件等
- 需費過鉅時得以網際網路、新聞媒體等其他適當公開方式。

*行政院臺訴字第1135019458號、
第1135020662號訴願決定



結論與建議

