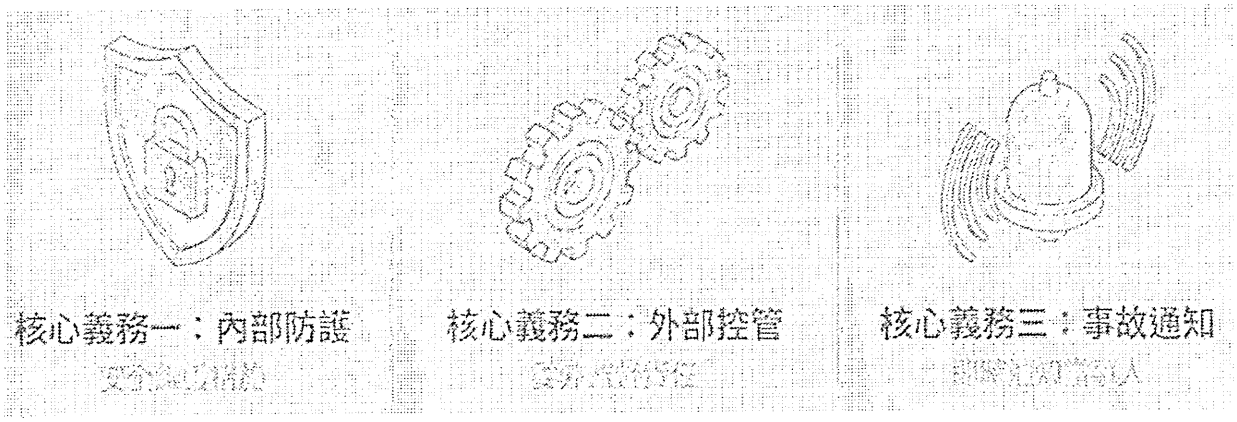
個資安維案件常見爭點之訴願決定及行政訴訟判決重點分析報告

三大核心重點



核心義務一：內部防護

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

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

個資法§12
施行細則§22

核心義務一：內部防護

◆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。

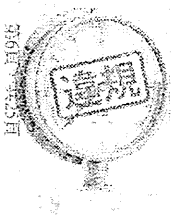
◆個資法施行細則第12條

- 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)

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。

*行政院院臺訴字第1145006174號訴願決定

爭點二
只要採購防護軟硬體，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。

採購防護軟硬體≠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」

*行政院院臺訴字第1050175635號、第1050174274號訴願決定

爭點三
賣家使用平台功能被假買家釣魚詐騙資料，平台業者是否負責？

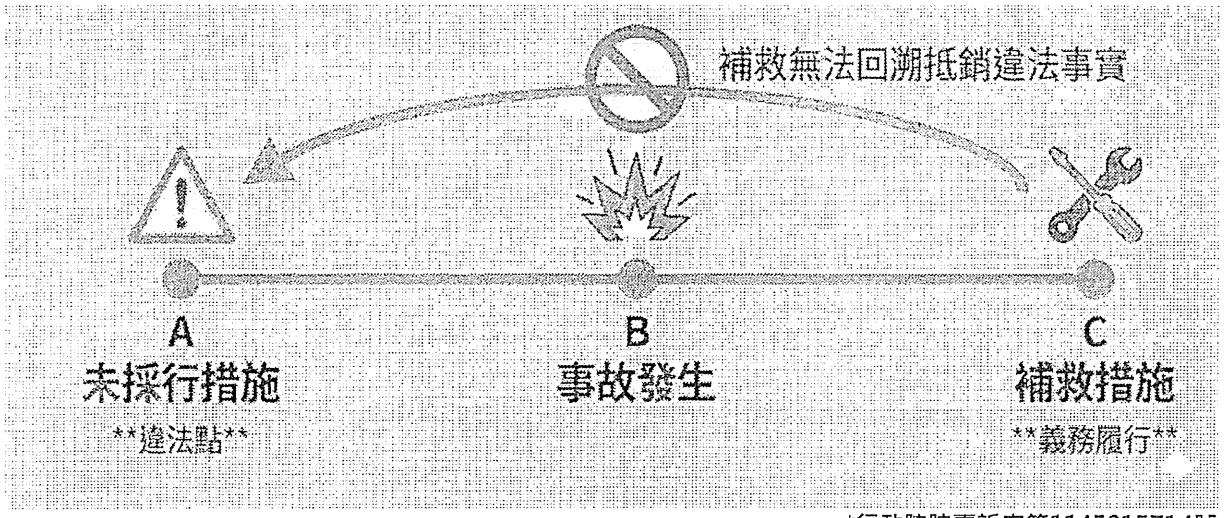
假買家向平台賣家宣稱無法下單，出示假QR Code或直接透過Line與賣家聯絡，誘騙賣家提供資料。

法院

1. 作為交易平台業者，為網路交易服務的提供者，不問係為建構安全交易空間以保護買賣雙方，或追求交易平台之永續經營，對於網路釣魚詐騙均有採取適當且有效之預防、通報及應機制的作為義務。
2. 仍應採取必要的「防笨措施」以防止使用者發生個資被竊取或洩漏情事。

*臺北高等行政法院 112年度訴字第889號行政判決

爭點四
事後補救能否免責？



*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**

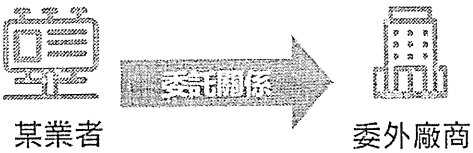
- 受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，**視同委託機關。**

◆**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)**

爭點五
業者以「未具資安專業」為由且已委外，主張免責？



某業者
訂單系統

委外廠商

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

訴願人與委外廠商間屬私法契約，惟委外廠商既係受訴願人委託而為個人資料之蒐集、處理或利用，訴願人應釐清與委外廠商之資安事件責任，明定雙方權責，並採取適當安全措施，以防止個人資料被竊取或洩漏。訴願人無資安專長，非得據以免除訴願人須採取適當安全措施以維護消費者交易個資不致外洩之理由，否則個資法第27條第1項規定將形同具文；訴願人無資安專長，可聘請資安專家補足，非僅依賴委外廠商，而不欲花費其他成本判斷委外廠商所為是否確實符合資訊安全。

1.委託契約
2.明定雙方權責
3.採取適當安全措施(監督管理)

爭點六
監督委外廠商之實際作為？

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

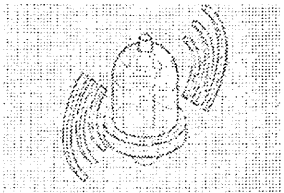
定期去查核廠商，而非僅看書面報告

*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

*行政院院臺訴字第1135019458、
第1135020662號訴願決定



核心義務三：事故通知

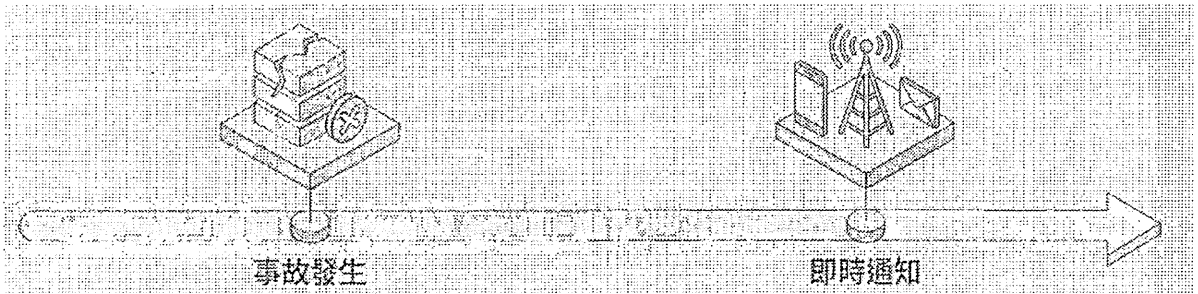
◆個資法第12條第1項

- 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。

爭點七
通知當事人之方式及內容？



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）

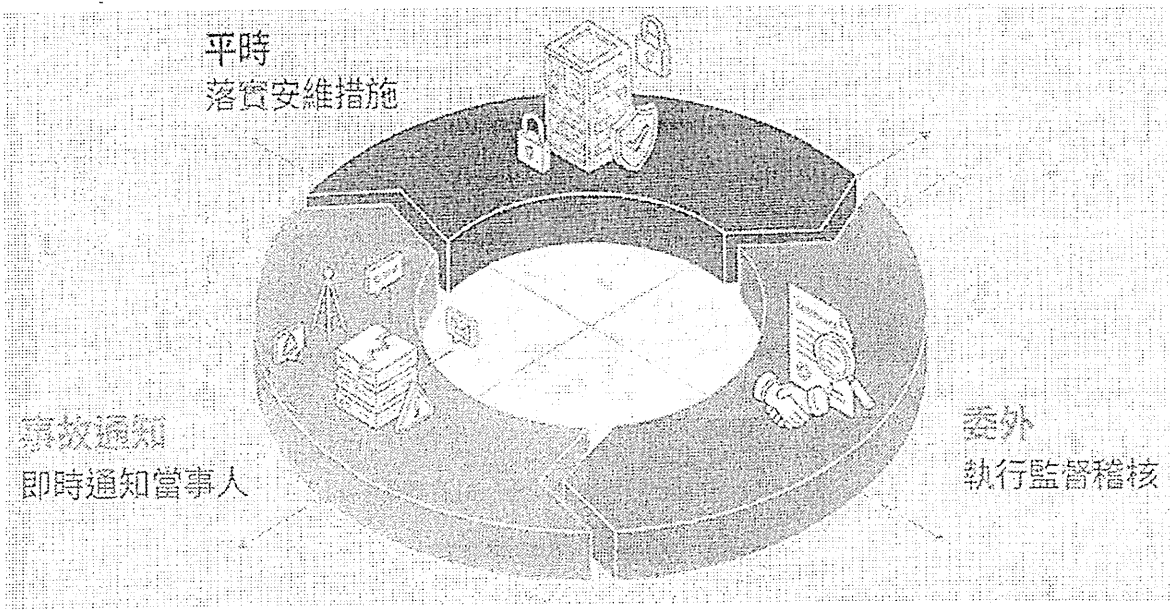
*行政院院臺訴字第1080175176號、第1100168370號訴願決定

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。

*行政院院臺訴字第1135019458號、第1135020662號訴願決定

結論與建議



114年11月11日總統公布之個人資料保護法修正重點介紹

114年個資法研修背景

憲法法庭
111年憲判字第13號判決

- **欠缺個人資料保護之獨立監督機制**，對個人資訊隱私權之保障不足，而有違憲之虞
- **至於監督機制如何設置，則屬立法形成自由**

獨立監督機制
個人資料保護委員會

- **個資會組織法：立院審議中**
- **個資法：**
  - ✓ **配合個資會職權之修正：** 已於114年11月完成，**刻正辦理相關子法法制作業**
  - ✓ **配合數位時代的法規調適：** 持續研議，籌備處與個資會接力推動

114年個資法修正草案

修正條次	修正內容
第1條之2	政策推進會議
第12條	事故通報應變及紀錄保存
第18條	個資長、公務機關安維辦法
第20條之1	非公務機關安維辦法
第21條	國際傳輸之限制權限劃一
第21條之1至之5	公務機關個資保護之監督
第22條	非公務機關事前檢查規劃
第51條之1	非公務機關監管過渡機制
第53條之1	行政救濟程序

114年個資法修正重點

二大修法主軸	相關關鍵措施
成立獨立監督機關	增訂個資事故處置義務 基礎個資檔案安維辦法
強化公務機關管理	公務機關置個資保護長 內外部稽核及檢查機制
確保監理效能穩定	六年過渡達成事權集中

修正重點說明 - 關鍵措施1

優先成立獨立監督機關

關鍵措施

1. 增訂個資事故處置義務
修正條文第12條

事故處置

- 新增通報、應變及紀錄留存等義務
- 由個資會受理事故通報
- 另有子法
- 業者違反通報等義務，有行政罰

修正重點比對

Before

- 僅有通知義務(1項)
- 通報義務僅存在於各部會所定個資檔案安全維護辦法(非公務機關)
- 通知要件：違法+查明後

After

- 處置義務：通知、通報、應變、紀錄留存(4項)
- 通報要件：子法將規範一定通報範圍，避免無實益通報
- 通知要件：知悉事故後均須通知

修正重點說明 - 關鍵措施1(續)

1. 增訂個資事故處置義務

基於獨立監督機關之地位
統一受理，減少認定爭議

個資會

轉報

基於上級監督機關之地位
一併了解事態

上級或監督機關

通報

符合一定
通報範圍

目的事業主管機關

併報

公務機關

非公務機關

1.不論事故情節，**均有應變及紀錄留存義務**
2.違反相關義務且未配合個資會要求改正者，得**公布機關名稱**及違法情形

發生個資事故

通知

個資當事人

1.不論事故情節，**均有應變及紀錄留存義務**
2.違反通知義務：**先令限改再處罰**
3.違反通報、應變或紀錄留存義務：**直接處罰**

修正重點說明 - 關鍵措施2

優先成立獨立監督機關

關鍵措施

2. 建立個資保護之統一解釋
修正條文第18條、第20條之1

法律效果

- 由個資會訂定共通版本
- 日後稽核、檢查、裁處之基準

修正重點比對

Before

- 授權部會針對特定業別訂定安維辦法
- 對公務機關僅在施行細則要求訂定內部規定(要點)

After

- 原則：所有公、私部門均有個資會所定共通基礎辦法之適用→因適用對象廣泛，必須有差異化管理機制
- 例外：特定業別安維辦法在過渡期間繼續有效，管制標準須等於或高於共通版

修正重點說明 - 關鍵措施3、4

優先強化公務機關管理

關鍵措施

3.公務機關之個資保護長
修正條文第18條

法律效果

- 由機關首長指派人員兼任
- 統籌規劃、督導考核機關個資管理事務
- 應配給適當人力及資源
- 職掌、職能條件、訓練等另有子法

4.內外部稽核及檢查機制
修正條文第21條之1至之4

因應施行

- 應向上級(監督)機關提報個資保護管理情形
- 應督導及稽核所屬(監督)機關
- 個資會全面納管，有權稽核及行政檢查
- 提報管理情形、稽核機制等另有子法
- 違法未配合改正，個資會將對外公布以示譴責

修正重點說明 - 關鍵措施3、4(續)

3.公務機關置個資保護長
4.內外部稽核及檢查機制

上級、監督機關固有職務監督體系

依據個資會之規劃，收受下級或受監督機關提報之個資保護管理情形、改善報告，督導、稽核所屬或所監督機關，且一併接受事故通報

公務機關個資保護事務內部監督機制

個資保護長團隊、法定專人

內部個資安全維護規範

個資會

1. 日常監管：
   1) 收受無上級/監督機關者之實施情形、改善報告
   2) 收受左列上級/監督機關之稽核(改善)結果
   3) 對各級公務機關均有稽核權

2. 違法或事故監管：
   1) 受理事故通報
   2) 發動檢查及下令改正

修正重點說明 - 關鍵措施5(完)

優先確保監理效能穩定

關鍵措施

5.六年過渡適用等相關事項

修正條文第51條之1

*因應個資會成立初期監管非公務機關之量能問題

過渡機制

- 個資會先行納管無明確目的事業主管機關者
- 有明確目的事業主管機關者，暫維持監管現況，得依個資法發動檢查(含事前)及裁處
- 對於目的事業主管機關所為處分不服者，原則向個資會提起訴願，以利統一見解

由行政院公告：下列非公務機關或業務活動之個資保護事務(暫)由原目的事業主管機關繼續監管
甲、乙、丙、丁、戊...
A、B、C、D、E...

*已初步完成盤點及磋商

每2年檢討，逐步減少
甲、乙、丙、丁、戊...
A、B、C、D、E...

個資會成立6年後完成權限變動