非公務機關就個人資料檔案採行適當安全措施之認定

蕭富庭*

壹、前言

依個人資料保護法第27條第1項規定，當非公務機關保有個人資料檔案，應採行適當之安全措施。如果非公務機關沒有採行適當安全措施，依照個人資料保護法第48條第2項規定，處新臺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，按次處新臺幣十五萬元以上一千五百萬元以下罰鍰。第48條第3項接著規定，其情節重大者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺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[1]。

非公務機關對於上開條文最大之問題，乃何謂「採行適當之安全措施[2]」？衍生問題有：依中央目的事業主管機關規定，訂定個人資料檔案安全維護計畫，是否屬採行適當之安全措施[3]？請外部講師講授個人資料保護法，可說是採行適當之安全措施嗎？

雖然個人資料保護法施行細則第12條第1項規定有界定個人資料保護法第27條第1項所稱適當之安全措施，是指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。個人資料保護法施行細則第12條第2項規定接著說明，前項措施，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

＊本文作者係執業律師、國立臺北大學法律學系財經法組博士生。

註1：2025年3月27日行政院會通過之個人資料保護法部分條文修正草案，本條已移列至修正條文第20條之1規定，刪除第27條規定。而修正條文第20條之1規定：「非公務機關保有個人資料檔案者，應辦理安全維護事項，防止個人資料被竊取竄改、毀損、滅失或洩漏。前項個人資料檔案安全維護事項、管理機制，應採取之措施及其他相關事項之辦法，由主管機關定之。」

註2：有學者指出：「所謂『適當之安全措施』，依個資法施行細則第12條第1項，同時亦指個資法第6條第1項但書第2款及第5款所稱『適當安全維護措施』、個資法第18條所稱『安全維護事項』、第19條第1項第2款及第27條第1項在此所稱『適當之安全措施』。由此亦可見我國現行個資法用語之紊亂。」請參照翁逸泓（2023），〈個資安全與個資保護──非公務機關之個資安全維護計畫、措施與洩漏通報〉，《當代法律》，第22期，第8頁第13註。

註3：關於金融業之個人資料保護與資料治理規範，請參照陳肇鴻（2024），〈金融機構資料治理規範架構之建構──由資訊需求與風險出發〉，《台灣法律人》，第35期，第47-62頁。

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。

然而，檢視個人資料保護法施行細則第12條規定後，在實務上仍無法確定與釐清何謂「採行適當之安全措施」，例如：適當之安全措施必須包括個人資料保護法施行細則第12條第2項規定之所有事項嗎？如果僅採行部分事項但能夠達成個人資料保護目的，是否已足？配置管理之人員及相當資源之相當資源，如何界定？非公務機關該如何進行有效風險評估？有特定範本或工具可供參考嗎？

由於實務操作中仍存諸多不確定性，本文第貳與第參部分將觀察我國司法實務判決與行政機關函釋，檢視實務上如何認定「適當之安全措施」。於第肆部分觀察新加坡個人資料保護法規定與新加坡個人資料保護委員會之執法案例，參考新加坡如何認定適當安全措施。最後為結論。

貳、我國司法實務判決之觀察

本文接下來以臺北高等行政法院高等庭112年度訴字第1396號行政判決及臺北高等行政法院高等庭112年度訴字第889號判決，探討法院如何闡釋個人資料保護法第27條第1項「應採行適當之安全措施」之內涵。

一、臺北高等行政法院高等庭112年度訴字第1396號判決

本件原告OO拍賣有限公司經營之網路拍賣平台，因警政署165反詐騙專線多次通報民眾接獲冒用該平台名義之詐騙電話，詐騙內容涉及訂單日期、商品名稱、金額、付款方式等交易個資，顯示疑有重大個資外洩之虞。警政署遂於111年至112年間先後以多次公文移送主管機關，被告數位發展部遂召開數次行政檢查與複查會議，並要求原告提出佐證資料及改善措施。惟經檢視，原告雖主張案件屬「網路釣魚詐騙」而非系統外洩，且已通知用戶及採行阻斷QR Code、惡意連結等防制機制，但仍被認為未完全符合個人資料保護法第27條第1項所定「適當安全措施」，因而被告先後於112年5月5日及5月30日作成二次限期改正處分。原告不服，認為被告認定事實錯誤、要求不明確且欠缺期待可能性，提起訴願遭駁回後，提起本件行政訴訟。

本件爭點，再於被告數位發展部因OO拍賣平台頻繁遭警政署通報涉有「網路釣魚詐騙」，進而認定原告未依個人資料保護法第27條第1項採行適當安全措施，並作成限期改正處分，該處分是否適法，即原處分有無認定事實錯誤、違反明確性及欠缺期待可能性之違法？

法院認為，原告自111年至112年間，屢次被警政署通報疑有交易個人資料外洩，被告依法召開多次行政檢查會議並要求原告限期改正。雖然原告回覆稱已有通知受害用戶、導入阻斷QR Code與惡意連結的機制，但經複查後仍發現其對於多項指示事項與通報內容未能完整說明或補正，仍有資料不足之情

形。因此，被告依個人資料保護法第27條第1項及第48條第4款規定，作成原處分，命原告於限期內補充資料與改正措施，並明示若不履行將依個人資料保護法第48條及第50條規定裁罰。法院認定該處分並無事實認定錯誤或違法，屬合法行政處分：

「由上述始末可知，原告自111年至112年間疑似有交易個資外洩情事，經警政署分別以111年10月26日、111年11月30日、112年1月7日、112年4月7日、112年5月17日函移請經濟部及被告辦理。被告自111年8月27日成立以來，陸續於111年12月30日、112年3月15日、112年3月23日召開行政檢查會議，評核結果認為原告有待改正事項，經被告所屬數產署依行為時個資法第48條第2款或第4款規定，分別以112年1月19日、112年2月4日函通知原告限期改正，及經被告以112年4月20日函請原告提供相關佐證資料。原告雖據以112年3月21日、112年4月10日及112年4月24日函回復，或稱已通知受詐騙之用戶，或稱已採行阻斷QR Code及惡意連結機制等語，然經被告112年4月28日行政檢查會議評核結果，原告對於上開會議結論指示事項及警政署通報等相關資料之說明（本院卷2附件9、13、原證7），仍有未盡事宜，尚有待補充資料5項，因認違反個資法第27條第1項規定，依行為時個資法第48條第4款規定，以原處分1命原告於2週內補充說明或提供相關資料等改正措施，及將改善結果函復該部，函內並敘明倘未於期限內回復或經檢視改正不完全者，將依行為時個資法第48條及個資法第50條規定辦理，經核並無不合，原處分1並無原告所指認定事實錯誤之違法。」

法院認為，即便部分案件可能涉及「網路釣魚詐騙」，但由於詐騙集團所掌握之交易資訊（如買賣時間、商品名稱、金額、付款方式）並非一般人可任意取得，合理推斷這些資訊來自原告所保管之交易個人資料外洩。因此，原告身為個資控制者，依個人資料保護法第27條第1項及施行細則第12條規定，仍負有建立「預防、通報與應變機制」之義務。既然經過多次行政檢查仍發現防制措施有缺漏，導致冒名詐騙案件反覆發生，原告不得以「只是釣魚詐騙」為由卸責：

「原告雖又主張本件警政署所接獲民眾舉報之詐騙案件，性質上實為『網路釣魚詐騙』事件，並非原告洩漏用戶個資所致等語。然細觀警政署通報案件列表內容，民眾所通報接獲冒用原告系爭拍賣網站名義之詐騙電話，其交易資訊包含買賣時間、商品名稱、金額及付款方式等細節，甚至有因曾經使用原告賣場上架商品，爾後收到詐騙集團電話冒用為原告或金融機構客服，以訂單錯誤等內容，引導進行ATM相關匯款操作之情形，上開交易資訊衡情非屬一般人可任意取得，而可合理推測該等由原告所保有之交易個資遭外洩，而非純屬網路釣魚詐騙事件；縱使本件不乏亦有原告所稱，詐騙集團利用網路釣魚手法，騙取系爭拍賣網站用戶自行洩漏個資之情事，然原告身為系爭拍賣網站之提供

者，並因此保有用戶之個資檔案，其依前述個資法第27條第1項及個資法施行細則第12條之規定，就『網路釣魚詐騙』事件之發生，仍有採取適當且有效之預防、通報及應變機制的作為義務，以防止其用戶個資外洩，原告所採取之相關防制措施，既經前述被告所召開多次行政檢查及複查會議，經外部專家檢視原告歷次所提供之資料後，發現原告所採行措施仍有所缺漏，因而導致假冒系爭拍賣網站名義之詐騙案件一再發生，自難謂原告未違反個資法第27條第1項規定。是原告上開主張，並非可採。」

二、臺北高等行政法院高等庭112年度訴字第889號判決

本件起因於內政部警政署165反詐騙專線接獲民眾通報，認原告OO拍賣有限公司經營之網路平台疑有違反個人資料保護法情形，遂於111年9月13日、10月26日及11月30日先後通知被告數位發展部處理。被告於111年10月24日及11月11日發函，要求原告查明並提供佐證資料，並釐清是否依個人資料保護法第12條通知相關當事人。原告於11月8日及12月2日回函，表示經調查資訊系統並無遭駭客入侵或個資外洩情形，因而不負通知義務。嗣於111年12月30日召開行政檢查會議後，被告認為原告未踐行個人資料保護法第12條及第27條第1項規定，即未以適當方式通知當事人，亦未採取足夠安全措施，遂於112年1月19日及2月4日分別作成處分，命原告限期2個月內改正。原告不服，提起訴願遭駁回，遂提起本件行政訴訟，請求確認原處分違法。

本件爭點之一，乃關於個人資料保護法第27條第1項「適當安全措施」之範圍？被告認為，原告雖於函復中主張平台並無個資外洩情形，且已採取公告提醒、外部連結警示畫面、異常登入雙重驗證等措施。惟實際上該平台仍持續發生大量個資外洩事件，並長期列居警政署165專線公布之高風險賣場，顯示其所稱措施不足以有效防護個資安全。另依個人資料保護法施行細則第12條第2項，非公務機關應具備盤點清冊、風險評鑑表、事故通報、教育訓練、稽核報告等佐證，然原告均未提出。因此，雙方爭執：被告基於通報結果與平台實際風險，認定原告違反個人資料保護法第27條第1項規定，進而命其限期改正，是否屬適法之行政處分？

依判決所載，當前社會，電信與網路科技之蓬勃發展固然帶來便利，但同時也衍生許多利用此類工具進行之不法行為。尤其是詐欺犯罪，藉由電話、簡訊或網路平台廣泛散播，不僅侵害財產安全，更常伴隨個人資料外洩之風險。此類犯罪往往跨境發生，受害人數眾多，造成社會重大不安與信任危機，因此如何從源頭阻斷訊息傳遞，成為各國共同努力之方向。

而要有效遏止此等犯罪，僅靠司法或警察機關並不足夠，必須仰賴公私協力，讓電信業者、網路平台扮演積極角色，例如確認訊息發送者的真實身分、阻擋惡意訊息來源繼續擴散等。此外，為了保障人民的隱私與資訊安全，非公務機關在蒐集與利用個人資料時，亦負有採取安全措施之責任。此處「適當之安全措施」雖屬不確定法律概念，但仍

可透過風險分析、管控措施、事故應變與後續預防機制等環節具體化，正如判決所揭示：

「伴隨電信、網路科技發展，以電信通訊或網路作為實施工具之犯罪行為，尤其是詐欺犯罪大量發生，各國莫不戮力偵辦防止電信詐騙、網路詐騙，從源頭攔阻詐騙訊息藉由電信通訊傳遞，即為其中要者。而攔阻詐騙訊息循電信通訊或網路傳遞，即需藉由公私協力方式，使民間業者承擔如核對確認發送訊息者身分、阻截詐騙或惡意訊息來源繼續發送等任務。又為防止個人資料被竊取、竄改、毀損、滅失或洩漏，非公務機關應採行適當之安全措施，個資法第27條第1項定有明文。所謂『適當之安全措施』雖屬不確定法律概念，惟依據非公務機關規模、特性、取得保有個人資料之性質及數量等因素，評估個人資料蒐集、處理、利用的流程，藉以分析可能產生的風險，並根據風險分析結果，訂定適當管控措施，實施後且應滾動檢討，就（疑似）發生個資被竊取或洩漏情形，採取應變措施以控制損害，查明事故狀況並以適當方式通知當事人，且應研議預防機制防止類似事故再次發生等，均應屬之。」

因此，非公務機關之平台經營者並非僅提供技術性之交易撮合工具，而係承擔維繫市場信賴與交易安全之核心角色。基此，平台業者除應遵循個人資料保護法第27條所揭示之安全維護義務外，尚負有積極建構安全交易空間之責任。尤其在「網路釣魚詐騙」頻仍發生的情境下，平台業者是否具備有效之預防、通報及應變機制，直接關乎消費者權益保障與平台永續經營之正當性。法院因此不再僅從形式合規檢視平台之作為，而是實質檢驗其所採措施是否足以達成防堵效果：

「惟原告做為網路拍賣平台，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、通報及應變機制的作為義務。查被告自接獲警政署通報起，先後於111年10月24日、11月11日發函要求原告查明妥處並提供相關佐證資料，原告回函雖說明個資可能外洩原因、對當事人之通知、事故後續處理作為及採行之個資安全措施等，惟觀諸警政署通報結果，第1次通報（統計期間為111年7月30日至8月28日）被害件數為65件，第2次通報（統計期間為111年9月17日至10月16日）被害件數為324件，第3次通報（統計期間為111年10月25日至11月24日）被害件數則達538件，呈現遞增趨勢，顯示原告所採行措施尚未發生阻止或減少詐騙案件發生的效果。迄被告於111年12月30日召開行政檢查會議，經原告出席說明後，被告評核結果認定原告涉有違反個資法第48條規定，應限期改正2個月，另建議原告「買賣家聊天功能應阻斷導向外部連結及封鎖QR Code圖片，應主動針對聊天內容之特定文字封鎖，如『簽署』、『協定』、『金流』、『添加客服』、『系統通知』、『凍結』……」，原告則於原處分作成後以112年3月21日函通知被告稱已透過電子郵件通知用戶、且已採行阻斷QR Code及惡意連結之機制

等功能，而被告於本院審理時亦稱『……經被告的要求及原告進行、提供相關保障措施後，原告經營的拍賣平台上受詐騙的情形已有減少……經過原告之改善，就詐騙事件也產生了防堵的效果，數量已經大幅下降……』等語，可認被告所建議之「阻斷外部連結、封鎖QR Code」確為有效方法。衡諸上情，並考量遭詐騙之賣家，顯然認為詐騙者佯裝買家出示前述結帳失敗、系統通知等訊息確為原告之「官方通知」，亦不瞭解該訊息所含QR Code或LineApp係導向外部連結，原告作為交易平台業者，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。本院因此沿襲既有判決前例（本院112年度訴字第1396號）立場，支持被告所認上述賣家受騙類型亦該當原告所保有個人資料被竊取或洩漏之見解。……可知原告確實未依被告上開函文說明，以『非防詐騙宣導等預防性通知』之適當方式通知當事人其個資被侵害之事實及已採取之因應措施等。至於其他防止個資被竊取或洩漏之安全措施，在確實阻斷外部連結及封鎖QR Code前，復未生實際效果，亦如前述，則被告以原告違反個資法第12條、第27條第1項規定，分別以原處分1、原處分2命原告限期改正，於法尚無違誤。」

三、小結

觀察上開判決，法院就個人資料保護法第27條第1項「適當之安全措施」之解釋，不僅止於形式上是否制定政策文件或單純宣導，而是以實際維護安全效果作為檢驗標準。

首先，法院強調「適當安全措施」屬不確定法律概念，應依業者規模、特性、所保有個人資料之性質與數量，透過風險分析、管控措施、事故應變與預防機制加以具體化。即非公務機關若僅以公告提醒、雙重驗證或例行安全措施主張合乎個人資料保護法第27條第1項規定，卻無法有效阻止外洩與詐騙案件發生，即難謂符合「適當安全措施」之要求。

其次，法院指出，平台經營者並非單純之技術中介者，而是承擔維繫市場信賴與交易安全之核心角色。尤其在網路釣魚詐騙頻仍的情境下，業者仍應負責建立有效之預防、通報與應變機制。即便部分事件係因用戶受騙自行洩漏，若涉及的交易資訊屬於平台保有之個資，仍可推論平台在安全維護上有不足之處。

再者，兩案均確認主管機關要求非公務機關限期改正、補充資料及導入具體技術措施（如阻斷外部連結、封鎖QR Code）的處分，並無逾越法律授權。法院認為此等作法正是將「適當安全措施」之不確定法律概念，透過檢查與改善要求落實為可具體操作之標準。

參、我國行政機關函釋之觀察

本文觀察之行政機關函釋，為法務部函釋、國家發展委員會函釋與個人資料保護委員會籌備處之函釋。原本依個人資料保護法第53條與第55條規定，法務部應會同中央目的事業主管機關訂定特定目的及個人資料類別，提供公務機關及非公務機關參考使用。

以及個人資料保護法施行細則，由法務部定之。因此，關於個人資料保護法之解釋，原先由法務部為之。後於2019年，法務部與國家發展委員會公告個人資料保護法及個人資料保護法施行細則相關條文涉及原管轄機關為法務部者，變更為國家發展委員會[4]。

之後個人資料保護法於112年5月31日增訂之第1條之1規定，明定個人資料保護法之主管機關為個人資料保護委員會。依個人資料保護法第1條之1第2項規定，自個人資料保護委員會成立之日起，個人資料保護法所列屬中央目的事業主管機關、直轄市、縣（市）政府及第53條、第55條所列機關之權責事項，由個人資料保護委員會管轄。為配合個人資料保護委員會籌備處暫行組織規程第2條第3款、個人資料保護委員會籌備處辦事細則第5條第2款等規定之施行，公告部分個人資料保護法及個人資料保護法施行細則相關權責事項，由國家發展委員會改為個人資料保護委員會籌備處管轄[5]。是關於個人資料保護法之解釋，目前由個人資料保護委員會籌備處為之。

本文以下先將法務部函釋、國家發展委員會函釋與個人資料保護委員會籌備處之函釋分為三類：

一、僅指引應採行適當安全措施

以下函釋僅指引非公務機關保有個人資料檔案，依法必須採行適當之安全措施，避免個人資料被竊取、竄改、毀損、滅失或洩漏：

（一）法務部法律字第10100244810號書函

（節錄）：「末按本法第27條第1項規定：『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。』故公司仍應採行適當之安全措施，並要求所屬員工遵循該公司個人資料檔案安全規範，以免違反上開規定，併予敘明。」

（二）法務部法律字第10203504830號函

（節錄）：「惟請貴署及金融機構依本法第18條及第27條第1項之規定，指定專人辦理個人資料之安全維護事項，或採行適當之安全措施，以防止義務人個人資料被竊取、竄改、毀損、滅失或洩漏，併此敘明。」

（三）法務部法律字第10303503260號函

（節錄）：「農會應依本法第27條第1項及本法施行細則第12條第2項規定，應採行適當之安全措施，防止所保有個人資料檔案被竊取、竄改、毀損、滅失或洩漏，包含建立查核控管機制；貴會基於農會之中央目的事業主管機關，亦應依本法第22條至27條規定，監督管理農會妥善執行個人資料保護業務，併此敘明。」

二、關於非公務機關擬定個人資料檔案安全維護計畫

以下函釋說明中央目的事業主管機關得要求非公務機關擬定個人資料檔案安全維護計

註4：法務部法律字第10803500010號公告、國家發展委員會發法字第1080080004A號公告。
註5：國家發展委員會發法字第1122002856號公告。

畫或處理方法，而個人資料檔案安全維護計畫辦法，宜請審酌產業規模、特性及其保有個人資料之性質與數量等因素。

（一）法務部法律字第1000008403號書函（節錄）：「故有關非公務機關訂定個人資料檔案安全維護計畫及處理方法之標準等相關事項之辦法，依法應由中央目的事業主管機關制訂之。又上開個人資料檔案安全維護計畫應包含資料（含電子資料及紙本）之處理流程、資料保存、維護、稽核、風險管理等事項，應非僅限人員之保密事項，併此敘明。」

（二）法務部法律字第10403507160號函（節錄）：「中央目的事業主管機關在指定應訂定個人資料檔案安全維護計畫等之非公務機關並訂定相關規範時，宜審酌「非公務機關之規模、特性」及「非公務機關保有個人資料之性質及數量」等事項，本於權責依實際需要訂定之，並未限於僅應針對通案情形指定行業並訂定相關辦法，且中央銀行業已指定「票據交換所」訂定個人資料檔案安全維護計畫，並已訂定「票據交換所個人資料檔案安全維護計畫標準辦法」。準此，是否指定郵政業（依來函所述，實質上為○○郵政股份有限公司）訂定個人資料檔案安全維護計畫並訂定相關辦法，宜請審酌郵政業之規模、特性及其保有個人資料之性質與數量等因素，本於權責決定之。」

（三）法務部法律字第10403503590號函（節錄）：「按中央目的事業主管機關就所管非公務機關所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之標準等相關事項之辦法（以下簡稱安全維護標準辦法），倘規範非公務機關就個人資料外洩事件通報目的事業主管機關之機制，因其係促使目的事業主管機關及早瞭解個人資料外洩事件，適時協助非公務機關採取適當之應變措施，以控制事故對當事人之損害，屬執行個人資料保護之細節性事項，雖因而對非公務機關產生不便或輕微影響，惟未限制其自由權利，非屬法律保留範圍，並無違反法律保留原則之問題。」

三、關於適當安全措施之內涵與標準

以下函釋說明如何判斷「適當之安全措施」，並強調應依比例原則與個案具體情況決定：

（一）法務部法律字第10203503430號書函（節錄）：「1.按公務機關及非公務機關皆有義務應參酌本法施行細則第12條所列事項，並衡酌所欲達成之個人資料保護目的及所涉及個人資料特性，辦理安全維護事項採行適當之安全措施（本法第18條、第27條規定參照），以防止個人資料被竊取、竄改、毀損、滅失或洩漏，依不同具體個案情況，採取不同技術上及組織上之措施，本法並無硬性規定需一律採行紙本加印浮水印或加密等措施，始可謂符合本法規定。2.至於公務機關利用網路填報系統受理非公務機關申報涉及個人資料事項，因該網路填報

系統係由公務機關所設置，自應由公務機關依本法上開規定就該系統採行適當安全維護措施。惟非公務機關為維護其所提供個人資料之安全性，於提供個人資料予公務機關時，仍可參酌本法上開規定審慎採行安全維護措施，並與公務機關洽商共同採行適當之安全措施。」

（二）法務部法律字第10403512200號書函（節錄）：「故本件來函所詢疑義，倘係A君翻閱B協會工作人員C君所保管收據明細時，趁C君不備而竊取D君之個人資料者，則應就個案事實調查B協會對於所保有之個人資料檔案是否已採行適當之安全措施，以及C君有無故意過失。」

（三）法務部法律字第10503502080號函（節錄）：「非公務機關依中央目的事業主管機關訂定之安全維護標準辦法訂定其安全維護計畫或處理方法後，未依其計畫或方法所定事項履行者，其目的事業主管機關應依個案具體情形審酌該非公務機關有無違反個資法第27條第1項規定，亦即其所違反之行為是否構成未採行適當安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏之情形；若是，自可依個資法第48條第4款規定論處。」

（四）法務部法律字第10603503880號函（節錄）：「本件○○雜誌寄送電子郵件未以密件副本方式為之，致揭露部分報名者電子郵件地址資料之行為，是否違反個資法第27條第1項『應採行適當之安全措施』及第5條『比例原則』之規定，仍應視本件個案中，對所蒐集之個人資料，其內部管理程序、管理機制、管理人員配置、認知宣導、設備安全管理、資料安全稽核機制等措施是否適當採行，由貴部基於目的事業主管機關之職權綜合判斷審酌之。」

（五）法務部法律字第10703512270號書函（節錄）：「準此，非公務機關依中央目的事業主管機關訂定之安全維護標準辦法訂定其安全維護計畫或處理方法後，未依其計畫或方法所定事項履行者，其目的事業主管機關應依個案具體情形審酌該非公務機關有無違反個資法第27條第1項規定，亦即其所違反之行為是否構成未採行適當安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏之情形；若是，自可依個資法第48條第4款規定論處。」

（六）國家發展委員會發法字第1090015912號（節錄）：「○○公司表示已採行門禁管理、教育訓練、資料存取管理及勞動契約相關罰則等措施，仍無法避免客服人員透過來電顯示自行記下號碼並洩漏至外部行銷網站之行為，則○○公司是否仍有違反個資法第27條第1項『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』之規定？按個資法第27條第1項所稱『適當安全措施』，依同法施行細則第12條規定，包括配置管理之人員及相當資源、資料安全管理及人員管理、設備安全管理、資料安全稽核機制等。有關○○公司主張已盡安

全措施是否有違個資法第27條第1項規定一節，事涉事實認定，應由貴會本於權責審認。」

（七）個人資料保護委員會籌備處個資籌法字第1140000195號：「查本案電子郵件未以密件副本方式而揭露消費者電子郵件地址資料之行為，是否違反個資法第27條第1項『應採行適當之安全措施』一節，仍應視個案中就上開事項所採行各項具體措施之內容，綜合判斷是否達到足以防止個人資料被竊取、竄改、毀損、滅失或洩漏之程度，惟此屬於具體個案事實之認定，建請貴局賡續本於職權調查釐清。」

四、小結

觀察上述函釋可知，我國行政機關對於個人資料保護法第27條規定之適當安全措施，早期法務部函釋多屬重申性與指引性，強調非公務機關依法必須採行適當安全措施，並要求建立內部規範或指定專責人員，以符合法定義務。其目的在於提醒義務人遵守基本要求，但對適當安全措施之具體內涵著墨有限。

其次，部分函釋強調中央目的事業主管機關得依產業特性、資料類型與規模，要求非公務機關訂定計畫與處理方法。此顯示行政機關透過授權規定，逐步建立行業別安全維護計畫，並將個人資料外洩通報、應變措施納入計畫範疇，以加強事前與事後控管。

回到本文探討之核心，即採行適當安全措施之認定，函釋多次強調應依比例原則及具體情況而定，避免僵化要求特定技術或形式，而是透過內部管理程序、資源配置、教育訓練、設備安全管理與稽核機制等要素，綜合判斷是否符合適當安全措施之要求[6]。此見解雖有助於兼顧產業差異，但同時也導致非公務機關實務上不易掌握具體標準，非公務機關是否已採取保護個人資料之適當安全措施，仍存在不確定性。

肆、新加坡案例之參考

新加坡於2012年制定新加坡個人資料保護法（Personal Data Protection Act, PDPA），並由新加坡個人資料保護委員會（Personal Data Protection Commission, PDPC）負責執法[7]。新加坡個人資料保護委員會在執法實務上，經由諮詢指南說明安全措施之內容[8]，亦透過每個裁罰案例逐步建構適當安全措施之具體內涵。以下摘選三件案例，藉以說明新加坡個人資料保護委員會在不同個案情況下對新加

註6：此部分如同有學者認為：「具體上，所應採取安全維護措施之寬嚴程度，常須視資料的敏感性、業務營運規模與性質及所面臨風險類型而定。資料越具識別性或敏感性，隱私安全管制措施應更嚴謹。」翁清坤（2003），〈個人資料之去識別化與再識別化風險：法律之觀點〉，《國立臺灣大學法學論叢》，第52卷第3期，第711頁。

註7：達文西個資暨高科技法律事務所（2023），《歐盟、南韓、新加坡個人資料保護法對於違反安全維護義務之行政處罰規定》，國家發展委員會委託報告，第3-4頁。

註8：何念修（2019），〈個資保護「適當之安全措施」──以新加坡個資法之技術措施建議為比較對象〉，《科技法律透析》，第31卷第1期，第58頁。

坡個人資料保護法第24條規定之適用與解釋。

一、新加坡電信案

關於新加坡個人資料保護委員會之2017年新加坡電信案件，涉及新加坡電信（Singtel）所委託之外包服務商Tech Mahindra，於進行ONEPASS系統維護時，因更新程式碼中遺漏必要條件，導致有用戶資料錯誤覆蓋約27,800名用戶之個人資料，導致其他用戶可以在MySingtel行動應用程式（MySingtel Application）以及MyBill（mybill.singtel.com）和MyAccount（myaccount.singtel.com）入口網站上看到受影響客戶之個人資料[9]。

新加坡個人資料保護委員會認定Tech Mahindra雖係受新加坡電信委託，但其作為新加坡個人資料保護法之資料中介者（data intermediary），仍負有第24條保護義務（protection obligation），應採取適當安全措施[10]。然Tech Mahindra未遵守內部標準作業程序，亦未先於測試環境驗證，或實施多層審核，致使大量資料被錯誤覆蓋、資料庫編碼問題，造成用戶可以看到其他用戶之個人資料，因而違反新加坡個人資料保護法。最終，新加坡個人資料保護委員會裁處Tech Mahindra新幣1萬元罰鍰。

相較之下，新加坡個人資料保護委員會認為新加坡電信已採取適當安全措施。新加坡與Tech Mahindra簽訂契約，要求Tech Mahindra遵守新加坡個人資料保護法與資訊安全政策，並設有測試環境、滲透測試與現場審查。新加坡個人資料保護委員會因此認定新加坡電信已採取適當措施，並未違反新加坡個人資料保護法。

本案彰顯新加坡個人資料保護委員會對適當安全措施之要求：一方面強調資料中介者本身須直接承擔責任，不得僅以「受委託」為由規避；另一方面，也肯認若資料控管者在契約、監督與制度設計上已落實適當安全措施，則可免於違法。

二、新加坡DPL案

本案事實為：DPL為華僑銀行（OCBC Bank）之資料中介者，受託負責客戶帳單之印製與寄送。然而，在作業過程中，DPL未依內部標準作業程序進行，導致部分帳單被錯誤送達至非授權之收件人，洩漏客戶之個人資料[11]。

註9：Singapore Personal Data Protection Commission, *Re Singapore Telecommunications Ltd. & Another* (Tech Mahindra), Grounds of Decision (Apr. 6, 2017), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/grounds-of-decision---tech-mahindra---060417.pdf (last visited Sept. 3, 2025).

註10：Personal Data Protection Act 2012 §24: "An organisation must protect personal data in its ossession or under its control by making reasonable security arrangements to prevent-(a) unauthorised ccess, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b)the loss of any storage medium or device on which personal data is stored."

註11：Singapore Personal Data Protection Commission, Re Data Processing Ltd., Grounds of Decision (June 20, 2017), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/grounds-of-decision---datapost---200617.pdf (last visited Sept. 3, 2025).

新加坡個人資料保護委員會認定，DPL作為資料中介者，雖然係依華僑銀行委託處理個資，但依新加坡個人資料保護法第24條規定，仍應負適當安全措施之義務。換言之，資料中介者與資料控管者同樣應確保其所持或管理之個人資料免於未經授權之存取、使用或洩漏。由於DPL未能在列印及寄送程序中設置有效檢查與驗證機制，致使錯誤發生，顯然未盡適當安全措施。

新加坡個人資料保護委員會考量到受影響客戶有限，且DPL已採取補救措施，包括加強內部審核流程與職員教育訓練，最終處以新幣3千元罰鍰。

三、新加坡消費者協會案

2024年7月，新加坡個人資料保護委員會認為新加坡消費者協會（Consumers' Association of Singapore, CASE）於兩次個人資料洩漏事件中違反新加坡個人資料保護法第24條與第12條(a)規定，處以新幣2萬元罰鍰[12]。

第一個事件為新加坡消費者協會官方郵件帳號（online-submission@case.org.sg、mediator1@case.org.sg）遭不明第三方入侵，從受影響帳號發出誘騙釣魚郵件，共發出約5,205封，波及4,945名收件人。部分受害者點擊郵件所附連結並被盜取銀行存款。第二個事件則是調查第一事件時，發生多起釣魚郵件，內容顯示消費者原先所投訴之案件細節，顯示新加坡消費者協會系統之個人資料洩漏。調查指出該事件可能發生於新加坡消費者協會與新舊資訊服務供應商間進行資料遷移過程中，使12,218名消費者個人資料面臨洩漏之風險。

新加坡個人資料保護委員會調查認定新加坡消費者協會違反新加坡個人資料保護法第24條規定，其理由：第一，新加坡消費者協會未落實堅實密碼政策（robust password policy），如存在密碼複雜度不足、未系統強制執行、帳號密碼長達四年未更替等重大漏洞，導致帳號易受攻擊。第二，新加坡消費者協會與資訊服務供應商之契約欠缺明確資訊安全責任條款（clear security responsibilities），尤其在資料遷移期間安全機制不足，導致資料外洩風險未被控管。第三，新加坡消費者協會長達五年未進行正式資安教育訓練，缺乏專責意識與應變能力。第四，新加坡消費者協會無文件化之資訊與通訊技術政策，也未建立登入資訊監控、日誌系統與稽核機制，無法及早偵測異常活動。新加坡個人資料保護委員會強調「僅僅依賴員工勤勉執行任務並非適當安全措施，組織需要採取積極主動步驟來保護個人資料。」

四、小結

觀察上述新加坡個人資料保護委員會案例，可知：首先，新加坡個人資料保護委員會明確強調資料中介者並非單純受託人，而

註12：Singapore Personal Data Protection Commission, Breach of the Protection and Accountability Obligations by Consumers' Association of Singapore (July 9, 2024), https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/commissions-decisions/gd_consumers-association-of-singapore_09072024.pdf (last visited Sept. 3, 2025).

是受新加坡個人資料保護法規範之主體，同樣負有第24條規定之保護義務，不得僅以依指示行事或受託行事作為免責理由。

其次，新加坡個人資料保護委員會對適當安全措施之要求具有技術性與組織性雙重面向，如要求有效檢查與驗證機制、密碼政策、契約安全責任、員工訓練與監控稽核等制度性設計。再者，新加坡個人保護委員會裁罰展現比例原則與風險基礎。在DPL案僅處以新幣3千元罰鍰，反映受影響範圍有限且補救措施即時；對新加坡消費者協會處以新幣2萬元罰鍰，理由在於組織長期未落實制度性措施，導致系統性風險擴大。

整體而言，新加坡個人資料保護委員會案件均具體說明適當安全措施所指為何，透過具體案例不斷累積與細緻化何謂適當安全措施，使之不僅停留在抽象概念，而能逐步形成具體可遵循操作規範[13]。

伍、結論

我國個人資料保護法第27條第1項規定所謂「適當之安全措施」，在於能否真正降低風險並產生實質效果，而非僅止於制定書面計畫或單次教育訓練。我國高等行政法院判決已明確指出，主管機關得依通報資料與實際風險要求非公務機關導入具體措施，並實際檢視成效。縱使涉及網路釣魚，但若所涉交易資訊來自非公務機關保有之個人資料，非公務機關仍負建立保護、通報與應變機制義務，根據風險分析結果，訂定適當管控措施，實施後且應滾動檢討，就發生個人資料被竊取或洩漏情形，應採取應變措施以控制損害。觀察我國行政函釋，早期僅止於重申義務與要求設置專責人員，但隨著實務進展，已強調比例原則與個案判斷，關鍵在於非公務機關能否提出盤點清冊、風險評鑑、事故紀錄、教育訓練與稽核報告等佐證資料，以確保非公務機關採行適當安全措施。

觀察新加坡個人資料保護委員會案例，調查核心圍繞在安全措施之有效性，並依比例原則與具體個案情況判斷是否符合適當安全措施。更重要的是，新加坡個人資料保護委員會每一件行政裁罰均公開理由，藉由公開化與累積案例，逐步形塑可預測標準，讓受規範者得以遵循。此種案例導向與公開化，對於我國主管機關未來在「適當安全措施」之判斷與規範上，具有重要參考價值，也有助於兼顧不同規模業者差異同時，提升個人資料保護之彈性與預期可能性。

註13：何念修，前揭註8，第61頁。