制度未竟，責任已臨：行政檢（調）查的攻防戰

李怡親*

前言：個資風險治理的臨界時刻

民國114年，是臺灣個人資料保護制度邁向重構與成熟的關鍵轉捩點。憲法法庭在111年作成的憲判字第13號判決，針對全民健康保險資料之蒐集與利用制度進行合憲性審查。該判決雖肯認《個人資料保護法》（下稱「個資法」）部分條款並不違憲，卻同時指出整體個資制度在監理機制與法制架構上存在重大違憲疑慮，並具體點出四項結構性缺陷：其一，欠缺獨立運作之個資監理機關；其二，健保資料之使用規範未符合憲法第23條之法律保留原則；其三，對資料目的外利用欠缺當事人退出之權利；其四，整體資料處理架構未建構足夠的組織與程序性保障。此為臺灣憲政史上首次對《個資法》條文作出違憲之虞的警示，並附加三年內完成法制修正的期限，亦即「憲法大限」正式到期之時。

然而，截至本文撰寫之際，與個資議題相關的三部法律，包含《個資法》、《個人資料保護委員會組織法》與《全民健康保險資料管理條例》（下稱「個資三法」）皆尚未完成立法程序。即便已有初步委員會審查與協商召集，整體進度仍停留在黨團協商階段，尚未實質通過。

在個資法制尚未完備之際，一方面實務操作規範（如去識別化標準、個資稽核人員獨立性等）未盡完善，公司難以預先完成設計隱私；另一方面，中央目的事業主管機關、個資委員會與法院未來可能在制度轉型中，出現不一致的解釋與執行標準，使公司面臨不確定的法律責任。

儘管立法進度遲滯，中央目的事業主管機關的執法力度並未因此鬆懈，反而近年來行政檢查的頻率、針對性及法律適用深度逐年提升。這不僅對公司帶來雙重風險，更突顯出將個資治理從被動應變轉向積極防範的重要性。若公司法遵策略，仍僅停留在「有告知、有同意」的最低門檻，不啻於在法制斷層之上裸奔。本文旨在探討，在當前立法未竟、憲法責任已臨的特殊時刻，公司如何從事補救轉向事前預防，並在資料創新與法遵之間，找到平衡點，將個資風險轉化為公司價值。

*本文作者係財團法人資訊工程策進會科技法律研究所專案經理

表1：個資三法立法進度

法案名稱	本年度黨團協商情況	目前進度
個人資料保護法部分條文修正草案	8/22協商[1]：第51條之1文字調整後通過，維持行政院草案6年過度規劃。	黨團協商完竣，全案照委員會決議及協商結論通過，交付院會。
個人資料保護委員會組織法草案	6/24協商[2]：提案修正設為中央二級獨立機關、7名專任委員（限連任一次）、人力上限20人。協商無共識，交院長協商。	委員會審竣，經一次黨團協商，但尚未有協商結論。（第3、10條保留）
全民健康保險資料管理條例草案	8/6協商[3]：就停止利用權例外規定限縮適用情境並增明確性，初步共識，但民眾黨團需內部討論，未能形成結論。	第一次黨團協商未就全文達成協商共識，擇期繼續審查。（第19條保留）

資料來源：本文自行製作

壹、 個人資料的風險與價值：資料經濟時代的合規轉向

一、 從附帶資訊到公司資產

數位化浪潮重塑了資料的價值曲線，也同步放大了資料風險的輪廓。從日常消費、健檢掛號、手機打卡、演算法推薦到生成式AI介面，幾乎每一位個體都在無意間生成並擴張其數位足跡。這些片段資訊被即時蒐集、分析、交叉比對，構築起一套高度依賴個資流通的現代數位經濟模式，公司與政府機關亦隨之成為資料驅動治理與經營的核心風險節點。

在這樣的營運模式中，個人資料不再僅是附帶性資訊，而是推動公司策略與價值創造的核心資產。公司透過個資應用，不僅能加速身分驗證，也能提升使用者介面的個人化程度，優化演算法推薦精準度，建構信用與風險評估模型，進而推動更具成效的產品開發與行銷決策。在AI與機器學習架構中，大量個資更作為模型訓練的原料，以提升預測力與決策效率，並逐步趨動了公司「以數據為動能」的營運引擎。

二、當數據創新遇上資料治理

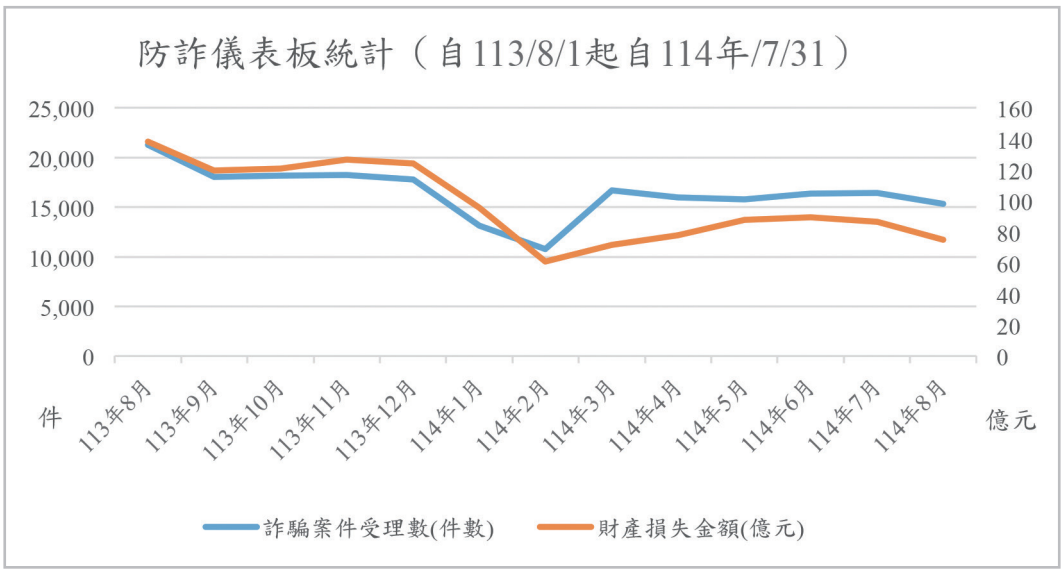
根據警政署自113年8月1日建置「打詐儀錶板」專網的統計，在短短一年內，因詐騙所造成的財損已高達約新台幣1,198億元，甚至

註1：立法院議事暨公報資訊網（114年8月22日），個人資料保護法部分條文修正草案朝野黨團協商會議紀錄，
https://ppg.ly.gov.tw/ppg/sittings/consult-among-political-parties/2025082005/details

註2：立法院議事暨公報資訊網（114年6月24日），個人資料保護委員會組織法草案朝野黨團協商會議紀錄，
https://ppg.ly.gov.tw/ppg/sittings/2025062371/details?meetingDate=114/06/24&meetingTime=11:00-12:00&departmentCode=null

註3：立法院議事暨公報資訊網，（114年8月6日），全民健康保險資料管理條例草案朝野黨團協商會議紀錄，
https://ppg.ly.gov.tw/ppg/sittings/consult-among-political-parties/2025073106/details

表2：防詐儀錶板



資料來源：本文自行製作

超過了去年國內第一大電商平台momo的年營收（新台幣1,125.6億元）[4]，顯示出詐騙與個資外洩所帶來的經濟衝擊不容小覷。

而當個資轉化為公司營運的核心驅動邏輯時，其伴隨的風險外部性亦同步擴大。一旦資料處理不當，不僅可能觸犯個資法規，更可能造成信任斷裂，進而嚴重影響顧客黏著度、品牌評價與長期商譽。在追求業務效率與法規遵循的動態平衡中，公司若在合法性、正當性與使用者信賴之間失足，其數位轉型之路將可能因信任繩索的斷裂而功敗垂成。

這種風險張力，也明確反映在國際市場觀察之中。根據 Euromonitor 發布的《2025年全球消費趨勢報告》[5]指出，信任已成為2024年全球消費者決策的核心依據。超過半數（54%）的消費者僅願意向其「完全信任的品牌」購買商品與服務，並傾向以第三方認證或制度機制驗證資訊真實性，作為購買依據。由此可見，消費者對資訊掌控與透明度的期待，正在成為影響品牌競爭力的關鍵因素。

資誠發布的《2024年消費者之聲調查》[6]亦指出，83%的受訪者認為個資保護是品牌贏得信任的首要條件，超越了產品與服務品質（79%）及價格考量（75%）。其中，雖有50% 的受訪者表示願意提供個資以換取個人化服務，但前提是「資料用途須被清楚告知」，顯示消費者對資料使用的敏感度與風險意識持續提升中，並逐步轉化為公司面對的資料治理壓力與動力。

註4：資料來自公開資訊觀測站，富邦媒（8454)於113年度營業收入為112,563,635仟元。
註5：Euromonitor International, Voice of the Consumer: Lifestyles Survey 2024, at 32 (Nov. 11, 2024).
註6：PwC, 2024 Voice of the Consumer Survey, https://www.pwc.tw/zh/news/press-release/press-20240515.html (last visited Aug. 5, 2025).

貳、 行政檢查與行政調查的法源與程序

一、 現行法之政策背景與形成脈絡

根據國家發展委員會於112年3月2日行政院第3845次會議所提出之報告，「個資保護三支箭」已成為現行修法之核心政策方向，分別為：一、設置獨立專責之個資監理機關（個資委員會籌備處（下稱「籌備處」）已於112年10月成立）；二、強化行政罰責機制；三、提升跨部會聯繫會議之功能。

在強化問責方面，若業者未依所屬產業所訂之個資安全維護辦法擬擬計畫，或未具備適當安全措施，中央目的事業主管機關得不經限期改正程序，逕行裁罰，顯示行政裁量權之擴張與執行力道之提升；在聯繫會議機能的強化，則透過行政檢查機制，落實「高風險對象強化監理」的政策。而經濟部、衛福部、交通部、金管會與數發部等與民生密切相關的中央目的事業主管機關首先擇定轄下高風險業者啟動行政檢查。

二、 行政檢查與行政調查程序解析

隨著個資法制度的重構與行政執法強化，中央目的事業主管機關對公司個資保護實務的介入程度日益加深。其中，行政檢查與行政調查機制，成為實務上評估公司於事前風險預防，及檢視合規缺口的主要手段。以下解析行政檢查與調查的法源依據、執行方式與自評表實務查檢常見缺失，以供公司參考。

（一） 法源依據

依個資法第22條第1項規定，中央目的事業中央目的事業主管機關為執行資料檔案安全維護、業務終止資料處理方式、國際傳輸限制，或其他例行性業務檢查，認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進行行政檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資

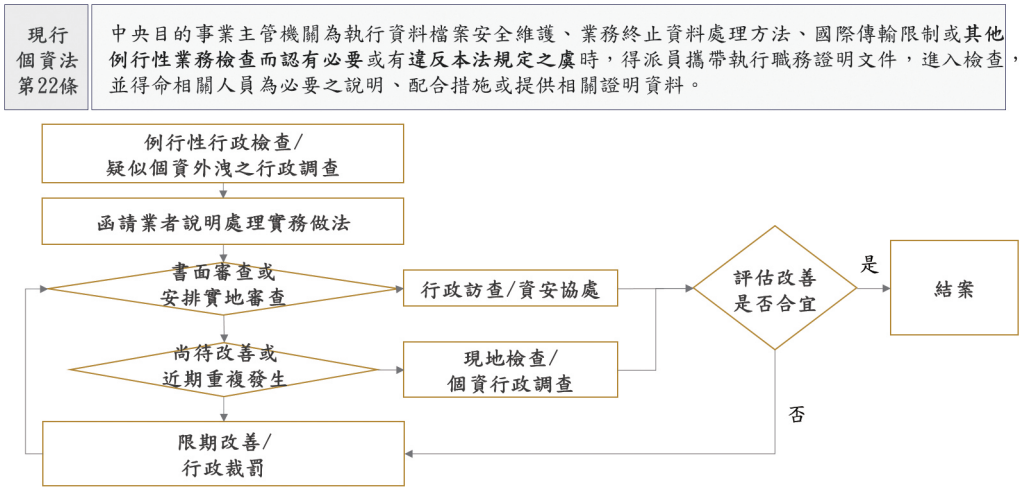


圖1：行政檢查及行政調查流程示意圖

資料來源：本文自行繪製

料。該條文奠定中央目的事業主管機關進行檢查之合法基礎，並明確區分行政檢查與行政調查所依據之情境。

（二）行政檢（調）查方式

就檢查方式而言，行政檢查主要分為「書面審查」與「現地訪查」兩類。檢查標準依各中央目的事業主管機關訂定之個資檔案安全維護辦法及各部會自評表內容進行檢查。流程上，中央目的事業主管機關會先發函給受檢公司，先由公司完成自評表並提供相關佐證文件供與初步審視後，視情形進行現地審查。現地審查執行方式依照不同中央目的事業主管機關而有所不同，檢查地點可能至業者端，亦有可能前往中央目的事業主管機關指定處所進行檢查。以經濟部或數發部為例，議程大約一至一個半小時不等，由業者就公司採行之個資安全措施簡報約半小時，再由委員提問及業者詢答。

至於行政調查，則多由具體個案引發，例如民眾陳情、媒體報導、地方政府通報或公司自主通報個資事故所觸發。實務上，公司發生個資事故後，如依法須通報，然目前除國家通訊傳播委員會（NCC）明訂通報系統與電子信箱外，其他中央目的事業主管機關普遍未建立一致通報窗口，致使公司多以首長信箱或地方政府信箱寄送通報資料。中央目的事業主管機關在接獲通報後，將發函要求公司於限期內說明案情並提出佐證資料。

此等說明及佐證內容通常包括兩個層面：其一為「事前防護」，即針對事故根因，說明業者於事發前已採取何種安全維護措施，並應參考自評表內容提供對應證據，以證明其已有「積極作為」；其二為「事後改善」，於事發後，是否於72小時內通報中央目的事業主管機關，並於合理期間通知個資當事人，說明事實與事發後擬採取之具體改善措施，並以實施該安全維護措施後，無異常軌跡或當事人申訴減少等作為佐證成效之依據。

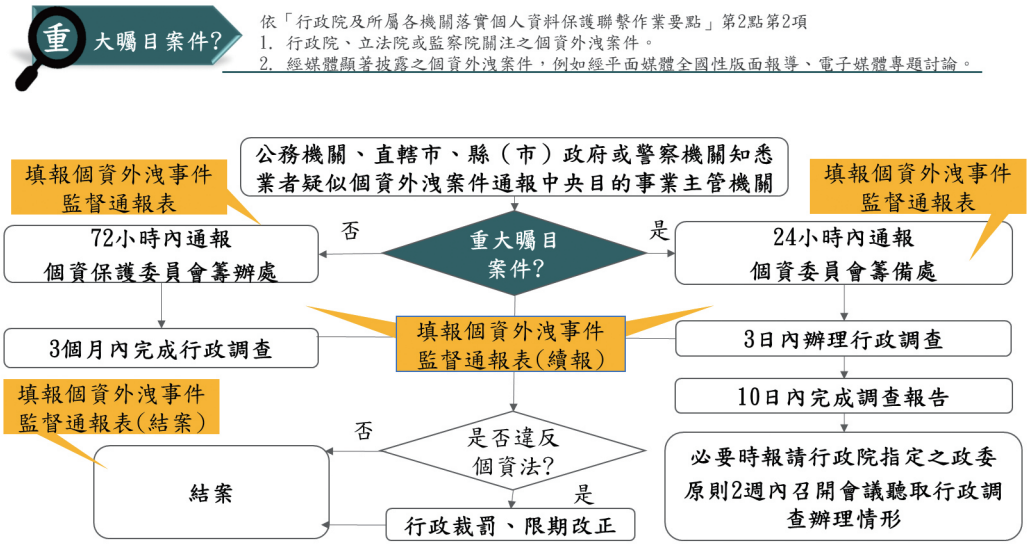


圖2：中央目的事業主管機關對個資安維案件之行政調查流程圖

資料來源：本文自行繪製

中央目的事業主管機關經初步審查公司說明後，如有必要，將召開調查會議，由業者簡報並經與委員詢答後，由審查委員釐清公司及其代表人是否已盡《個資法》及相關子法上的防止義務，以決定裁罰與否；若屬重大矚目案件，相關中央目的事業主管機關將自知悉時起 24 小時內，通報個資會籌備處及數位發展部（下簡稱「數發部」），並於三日內啟動行政調查，十日內完成調查報告。必要時，籌備處得報請行政院指定之政務委員，於兩週內召開會議，聽取行政調查辦理情形與後續處理建議。

總結而言，行政檢查與調查機制，已由過往的「事後查核」逐步轉型為強調「風險預防」的合規工具，其制度設計亦日益精緻、具體。公司應於平時即建立完善的紀錄軌跡，並建構事故預防與應變機制，俾於發生個資事件時，能即時提出具體之個資安全維護措施及執行紀錄，展現足以因應風險之治理能力，進而提升回應速度與營運韌性，降低裁罰風險，同時維繫品牌信任與市場聲譽。

（三） 自評表查檢項目與常見缺失

隨著我國個人資料保護法修法進程推進，主管機關對於非公務機關個資防護義務的要求已逐漸具體化。如將《個資法施行細則》第12條第2項所規定11項「適當安全維護措施」，轉化成自評表的具體查驗標準。換言之，公司不僅需在書面上建立完整的個資檔案安全維護計畫，更必須回應自評表各項安全維護措施，且須提出足以證明計畫已落實運作之紀錄與證據。以下將就自評表各項目所要求之具體證據，與常見誤區進行說明：

1. 配置管理人員及資源

在「配置管理人員及資源」方面，檢查重點已從單純的專責人員指派，進一步關注其是否具備充分資源與組織支持。業者通常需提供內部組織架構圖、專責人員任命文件與職掌說明，以及經費預算表，藉以展現此一制度並非流於形式，而能在組織層級落實。相對而言，若僅以形式上設置而欠缺實質職權，往往會被認定為「有計畫無執行」。

2.界定個人資料範圍

個資檔案盤點清冊可協助公司盤點涉及個資蒐用之流程，如個資盤點欄位設計可檢視：①蒐集、處理與利用之特定目的與類別；②蒐用個資所適用的法定要件；③履行告知之義務；④個資檔案存放的位置及是否留有備份檔；⑤流程是否委外；⑥特定目的外利用；⑦國際傳輸等議題，並了解⑧該流程約莫存有多少筆個資，以協助公司釐清個資法上之權利與義務。

在實務檢查中，主管機關往往要求公司出具個資檔案盤點清冊或資料流向圖，以確保個資蒐用符合《個資法》第5條「最小化蒐集原則」。若欄位設計失當，將無法看出公司蒐用個資於其生命週期中是否合規；若盤點個資流程不確實，常有缺漏，亦將影響後續「風險評估與管理機制」之正確性。

3.風險評估及管理機制與事故預防、通報及應變

在「風險評估及管理機制」與「事故

預防、通報及應變」方面，行政檢查展現出其「風險導向」的核心精神。主管機關已不再滿足於公司單純宣稱「我們重視您的個資安全」，而是要求公司須建立一套「一致、有效、可比較」的風險評估方法論，並依據該方法論，反映個資盤點中各流程的風險值，進而回應前述第一款「人員及資源配置」的要求，將資源精準投入於關鍵環節，確實將剩餘風險有效降至公司可接受的最大風險值，以更有效率與效果防範個資事故的發生。

在事故應變部分，則區分公司近期是否曾發生個資事故，自評項目亦有不同義務。若公司未曾發生個資外洩，仍應具備完整的通報流程程序文件、平時確實執行事故演練並留存紀錄，以證明其應變機制並非紙上談兵，而能於事件發生時即時啟動；若曾發生個資外洩事故，則須檢附通知當事人與通報主管機關之紀錄[7]。前者有助於資料主體釐清事故發生的事實，避免因資訊不透明而造成二次傷害；後者則有助於主管機關即時掌握事故動向，進行必要的監督與協助。

4.蒐集、處理及利用之內部管理程序

蒐集、處理與利用為個人資料生命週期的核心環節。公司除應提交內部個資管理規範及程序文件外，亦須全面檢視其合規性。其中，「委外監督」更是實務檢查中的重點項目，不僅考驗公司在議約談判上的能力，更著重於公司是否能有效發揮監督功能。公司不得以「外包」作為責任切割之理由，而應透過契約條款與監督實作，確保委外廠商同樣遵循個資保護標準，並納入持續性的監督與稽核機制。

具體而言，公司應於「選商階段」，將委外廠商之個資保護能力納入評估條件之一；在「履約期間」，執行實質且有效的監督作業[8]；於「契約關係終止後」，要求委外廠商提供所有專案涉及之個資已完成安全返還或刪除之證明。此一流程有助於確保委外廠商於整個合作期間皆受制於個資保護標準，落實公司對個資安全的責任。

註7：通報對象為中央目的事業主管機關，或直轄市、縣（市）政府。若公司適用各該產業訂定之個人資料檔案安全維護管理辦法，則須於知悉事故後72小時內依業者個資外洩通報表完成通報。目前除國家通訊傳播委員會（NCC）設有專門通報管道（https://pdin.ncc.gov.tw/ISRS/Account/Login ）外，公司可通報予縣市政府1999陳情系統，或其中央主管機關之首長信箱。

註8：實務上，公司可透過以下三個階段，對委外廠商進行實質且有效的監督：

- 選商階段：要求廠商提供PIMS（個人資料管理系統）或ISMS（資訊安全管理系統）等相關個資或資安標章，作為其具備合規能力的證明。
- 履約階段：在契約面上，應建立完整的委外廠商清單，並於委外契約中納入符合《個資法施行細則》第8條第2項各款規定的條文；在實務操作上，則應落實定期監督，例如定期前往廠商處進行稽核，或要求廠商填寫自評表等。
- 結案階段：應要求廠商將因委外案所取得的個資確實返還、刪除或銷毀，並可透過簽具切結書、提供照片或影片等方式，作為佐證。

5.個資三管：資安管理、人員管理與設備管理

「資料安全管理及人員管理」與「設備安全管理」則關注於技術與管理的雙軌落實。主管機關通常要求檢附存取權限設定表、密碼與加密政策、人員離職交接清冊，以及資訊設備安全管理規範、防火牆與防毒紀錄，以及機敏環境如機房等出入管制名冊。

6.認知宣導及教育訓練

根據網路安全公司Mimecast訪問全球超過1,100名資安人員所彙整的《The State of Human Risk》發現[9]，大多的資料外洩來自於人為錯誤，並超出技術或系統上的缺失。因此，在教育訓練提供員工個資及資安意識的自評項目，主管機關在檢查中，會要求公司提供教育訓練教材、課程簽到表與測驗紀錄，以確保公司已實際執行教育訓練計畫，並將個資法相關觀念內化於全體員工。

在實作上，最難操作的在於如何對「全體員工」進行有效的教育訓練，包含派遣人力等都要考量，而非僅存在於法務部門或資訊部門的專業知識。從組織治理的角度來看，這一要求旨在將個資保護轉化為「組織文化」的一環，而非僅少數專責人員的功課。

7.資料安全稽核與使用紀錄與軌跡資料及證據保存

即便公司已建立完善的內部控制措施，在當前的技術環境下，資料外洩的風險仍無法完全歸零。因此，公司在資安防禦上，除了事前預防，更應著重於事故發生後的應變與復原韌性。當主管機關主動或被動介入個資行政調查時，其重點將鎖定在事故的根本原因分析，以及公司應變措施的可稽核性（auditability）。

正如法諺所云：「舉證之所在，敗訴之所在。」這意指在訴訟或行政調查中，無法提出有力證據的一方，將面臨極高的敗訴風險。因此，公司必須建立持續性的資料安全稽核機制。這不僅包含日常營運中對存取日誌、操作紀錄與軌跡資料的完整保存，作為事故發生後釐清責任歸屬的核心依據；更應透過年度稽核計畫、稽核報告與追蹤改善計畫，向主管機關證明個資治理並非一次

註9：Mimecast, The State of Human Risk (2025), https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/（最後瀏覽日：2025年8月28日）。

註10：以「計畫──執行──檢查──行動（Plan-Do-Check-Act），PDCA方法論」為基礎。建構滾動式個資管理流程：

(1)計畫：建立個人資料保護管理政策、目標及相關程序。

(2) 執行：個人資料管理制度之實施。

(3)檢查：依據個人資料保護管理之政策、目標及要求，評估與監督流程及其軌跡，並將結果回報給公司管理階層加以審查。

(4)行動：採取措施，以持續改善個人資料管理制度之績效。

性作業，而是一個持續檢討與精進的滾動式改善過程。

8.持續改善機制

最後，「持續改善機制」將整體合規置於動態治理的架構下。主管機關通常要求公司檢附 PDCA[10]循環紀錄，如管理審查會議紀錄、稽核報告與追蹤改善計畫，以確保個資保護措施能隨業務變動與技術發展不斷調整。這一要求，實則將個資保護納入公司長期治理的核心環節，而不再是靜態的法規遵循。

以下就「經濟部主管商業服務業者個資防護自評表」為例，說明行政檢查自評項目常見缺失。

三、實務案例解析：從行政裁處看風險誤區

我國各部會對行政裁處的資訊揭露多仍有限。除數發部[11]與金管會[12]透過新聞稿或專區公告外，其餘僅能自上市櫃公司因重大資安事件於公開資訊觀測站發布之重訊略知一二。然而，此類資訊內容零散且不完整，難以呈現行政檢查與裁處的核心重點，亦使業界在合規實務上缺乏具體可資借鏡的案例。

表3：商業服務業者個資防護自評表及常見缺失

稽核項目	稽核內容	常見缺失
1.配置管理之人員及相當資源（個人資料保護法施行細則第12條第2項第1款）	1.1是否設個人資料管理單位或適當組織？	公司在進行自評時，常因組織規模或人力限制將個資代表或管理人員的職務外包予律師或會計師事務所，或由集團母公司的個資代表兼任。然而，依據個資保護規範，公司內部應至少指派一名專責人員，以因應日常業務中產生的個資處理需求。
2.界定個人資料之範圍（個人資料保護法施行細則第12條第2項第2款）	2.1是否每年定期清查其所保有之個人資料檔案及其蒐集、處理或利用個人資料之作業流程，據以建立個人資料檔案清冊及個人資料作業流程說明文件？	• **盤點不確實**：僅部分部門填寫，或遺漏新業務、臨時性專案之個資。 • **誤判個資範圍**：忽略如會員編號、客服錄音檔、員工/供應商個資等可間接識別的資料。 • **個資欄位設定失當**：未能有效連結至個資生命週期的風險節點。 • **蒐集、處理、利用**：未能掌握生命週期應盡義務，及辨別蒐用個資之法定要件。 • **保存與銷毀**：保存期限設定不當、存放位置不安全、無備份或備援，或未確實屆期刪除。 • **計算個資筆數**：個資筆數應以每一特定目的所蒐用之人數為計算，若邏輯錯誤恐影響風險評估的準確性。

註11：在數位發展部「斥詐人生」專區中，可查詢電商業因個資行政調查而遭受行政處分之紀錄。

註12：金管會依「金融監督管理委員會處理違反金融法令重大裁罰措施之對外公布說明辦法」第2條規定辦理。

稽核項目	稽核內容	常見缺失
3.個人資料之風險評估及管理機制（個人資料保護法施行細則第12條第2項第3款）	3.1是否每年定期評估其因蒐集、處理或利用個人資料可能面臨的法律或其他風險，並訂定適當之管控及因應措施？	・**方法論量測不足**：缺乏量化指標，無法有效衡量與比較風險。 ・**高風險控制不力**：管理階層未設定可接受的最高風險值，也未針對高風險項目制定並執行預防或矯正計畫。 ・**風險情境掌握度低**：公司未能充分設想個資流程中的潛在風險情境，導致事故發生時缺乏應對策略。
4.事故之預防、通報及應變機制（個人資料保護法施行細則第12條第2項第4款）	4.1個資事故應變機制是否包含降低、控制事故對當事人造成損害之作法及因應措施？	・**個資通報機制之實務缺失**：個資通報機制不應只是一份標準作業程序（SOP）。應注意以下實務環節： ・**辨識能力不足**：同仁無法區分個資「事故」與「事件」，延誤通報。
	4.2個資事故應變機制是否包含適時以電子郵件、簡訊、電話或其他便利當事人知悉之適當方式通知當事人個人資料被侵害之事實與已採取之因應措施，及後續供當事人查詢之專線與其他查詢管道？	・**通知內容不合規**：僅發布籠統的「防詐騙」公告，內容不僅不合規，也未能有效保護當事人。 ・**通知未以個別告知為原則**：應事先評估並確認個資主體的聯絡方式，同時考量通知方式的成本，除非能證明通知成本過鉅，始得以公告方式為之。 ・**通報延遲**：未能在法定期限內（72小時）通報主管機關。 ・**預防與矯正**：缺乏明確的預防矯正SOP。這導致事故發生時，無法即時啟動有效措施，也未能確實執行矯正計畫，阻斷風險擴大。
	4.3個資事故應變機制，是否包含避免類似事故再次發生之矯正及預防機制？	
	4.4是否就個資事件通報，其通報流程為何？	
5.蒐集、處理、利用作業（個人資料保護法施行細則第12條第2項第5款）	5.1資料蒐集、處理是否具備特定目的並具有法定要件？	缺乏特定目的、未落實告知義務、不符合法定要件，或未遵循個資最小化原則。
	5.2個人資料之利用，是否符合特定目的之範圍？	超出告知範圍利用個資，或不符合特定目的外利用的法定要件。
	5.3是否有目的外之利用？目的外利用是否符合法定要件？	
	5.4是否依規定取得當事人同意（當事人同意之情形）？	・**同意時點不符**：公司在個資蒐集之後，才補行告知及取得同意。 ・**同意形式不當**：採用預設同意或包裹式同意，未提供當事人自主選擇權，特別是未能針對特定目的外利用設計單獨的同意選項。 ・**同意軌跡不足**：未能留下有效的同意紀錄或軌跡，如同意的時間、方式等。
	5.5是否履行告知義務（未履行告知義務時，是否符合免告知之情形）？	**告知內容不足**：告知內容未充分依照個資法第八條或第九條告知： ・**名稱**：若有集團共享同一份告知聲明，應明確揭示。

稽核項目	稽核內容	常見缺失
		・**特定目的與類別**：蒐集之目的與蒐集目的和實際狀況不符，未能符合最小化蒐集原則。 ・**期間、地區、對象、方式**：說明過於籠統，未檢視是否與其他廠商分享個資、是否涉及國際傳輸。 ・**當事人權利行使說明不足**：未明確提供當事人權利行使說明（如身份驗證方式是否接受代理人行使），或說明若不提供個資，可能對於當事人有何不利之影響（如無法提供完整的服務）。
	5.6是否已於首次行銷時提供當事人表示拒絕行銷之管道？如需費用是由機關支付所需費用？	未具備免費拒絕行銷管道，或窗口不明。
	5.7是否依當事人拒絕接受行銷之要求，立即停止利用其個人資料為行銷，並週知所屬人員或採行防範所屬人員再次行銷之措施	・**拒絕行銷要求處理延遲**：負責窗口或客服未能即時回應當事人的拒絕行銷要求。 ・**系統註記不及時**：即使當事人已明確拒絕，公司後端系統未能及時更新或註記，導致仍持續對其進行行銷。 ・**共享個資廠商未獲通知**：公司未能將當事人拒絕行銷的意願，即時於系統上註記，或通知所有共享其個資的合作廠商，致當事人持續收到不同管道的行銷資訊。
6.資料安全管理及人員管理（個人資料保護法施行細則第12條第2項第6款）	6.1是否識別業務內容涉及個人資料蒐集、處理或利用之人員？	未遵循個資法第五條「**個資最小化原則**」，且未定期對人員的權限進行審查與調整，如員工轉調、離職、長假、留職停薪等，其權限未隨之調整。
	6.2是否依其業務特性、內容及需求，設定所屬人員接觸消費者個人資料之權限，並定期檢視其適當性及必要性？	未對個資存取進行有效管控，如未定期刪除或停用已逾期或長期閒置的帳號。特別是委外建置的系統，經常發生委外廠商共用權限，且在契約結束後未將帳號刪除。
	6.3是否與所屬人員約定保密義務？	與員工簽訂雇傭或委任契約時，未簽署與個資相關的保密契約，或未規定在人員離職或職務變動後，仍於適當期間內負有保密義務。
	6.4是否要求人員離職時，返還保有消費者個人資料之載體，並刪除因執行業務而持有之消費者個人資料？	・**實體載體未回收**：人員離職時，並未要求其返還保有個資的紙本文件、筆記型電腦、隨身碟或行動硬碟等載體，可能導致離職員工將客戶資料帶離公司。 ・**未留存佐證紀錄**：即使有執行相關程序，但未要求離職人員簽署切結書，或留存刪除、銷毀的證明文件，以供佐證。

稽核項目	稽核內容	常見缺失
	6.5消費者個人資料有加密之必要者，於蒐集、處理或利用時，是否採取適當之加密措施？	• **未能根據資料的敏感度與風險級別採取適當的加密措施**：機敏個資未加密或加密強度不足；資料庫、異地備援或備份檔未加密；以及離線裝置中的個資未加密等。一旦資料被竊取，未經加密或遮蔽的個資將完全暴露。 • **金鑰管理不當**：加密金鑰未受到妥善保護，如將金鑰與加密資料儲存在同一處，或金鑰未定期更換。
	6.6傳輸消費者個人資料時，是否依不同傳輸方式，採取適當之安全措施？	• **未以加密方式傳輸敏感性資料**：未採用HTTPS等安全傳輸協定，或所使用的協定版本已過時或存在漏洞，致敏感個資在傳輸過程中遭攔截或竊取。 • **未檢查憑證來源**：在使用加密連線時，未確實檢查伺服器憑證的合法性與有效性，可能造成「中間人攻擊」的風險。
	6.7消費者個人資料有備份之必要者，是否對備份資料採取適當之保護措施？	• **未加密或加密強度不足**：常見備份檔未加密，或密碼從未變更。 • **實體或存取控制不當**：未對存放備份資料的儲存裝置（如硬碟、磁帶）或雲端空間設定實體或存取權限。 • **異地備援資料未受保護**：實體安全、環境控制或網路存取權限不足。 • **備份資料未定期檢視與銷毀**：過期或不再需要的備份檔持續留存，增加外洩風險。
7.認知宣導及教育訓練（個人資料保護法施行細則第12條第2項第7款）	7.1是否定期對實施所屬人員之個人資料保護與管理認知宣傳及教育訓練？所屬人員是否明瞭上課內容？	• **未涵蓋所有員工**：如高階主管、派遣人員及工讀生。 • **內容僅限於資安部分**：缺乏與《個資法》或個資管理實務相關的課程。 • **課程內容未即時更新**：課程未留意相關法規變動，或因應技術、主管機關函釋及實務見解調整。
8.設備安全管理措施（個人資料保護法施行細則第12條第2項第8款）	8.1是否依據作業內容及環境之不同，實施必要之安全環境管制？	• **未落實實體門禁管控**：未設置門禁系統或相關管制措施，導致非授權人員可隨意進出存放個資的管制區域。 • **環境監控不足**：未對機房或重要儲存區進行環境監控，如缺乏溫濕度控管、煙霧、漏水警報系統，或消防設備。
	8.2是否妥善維護並控管個人資料蒐集、處理或利用過程中所使用之實體設備？	• **設備未定期清點或維護**：未建立設備清單，或未定期對電腦、伺服器、印表機等設備進行維護與盤點，導致設備遺失或故障。 • **機敏個資未設專用設備**：處理機敏個資，與一般辦公設備共用。

稽核項目	稽核內容	常見缺失
	8.3是否針對不同作業環境，建置必要之保護設備或技術？	・**防火牆及入侵偵測系統配置不當**：未依據不同作業環境（如開發、測試、正式環境）設定適當的防火牆規則，或未建置入侵偵測/防禦系統，以偵測並阻擋惡意攻擊。 ・**網路隔離不足**：處理機敏個資的網路環境未與一般辦公網路進行隔離。
9.資料安全稽核機制（個人資料保護法施行細則第12條第2項第9款）	9.1是否每年定期由適當組織執行資料安全內部稽核並提出評估報告？	・**未定期執行稽核**：未建立年度內部稽核計畫，或未定期執行個資內部稽核。 ・**稽核報告流於形式**：均回覆符合，未附上相關佐證，致未能真實發現個資管理缺失。 ・**無獨立的稽核人員**：負責稽核的人員缺乏經驗、獨立與客觀性。
	9.2是否採取改善措施以持續改善資料安全維護？	・**改善措施未落實**：缺失未被有效追蹤，且未在預定時間內完成改善。且未分配權責人員定期追蹤、執行、確認成效。 ・**缺乏預防矯正機制**：未將個資事故、稽核缺失等，納入其個資安全維護計畫中進行持續改善與優化。
10.使用紀錄、軌跡資料及證據保存（個人資料保護法施行細則第12條第2項第10款）	10.1是否保存個人資料提供或移轉第三人之紀錄？	**無移轉紀錄**：將個資提供給委外廠商或合作夥伴時，未保存詳細紀錄，例如移轉的時間、對象、目的及內容。
	10.2是否保存當事人行使個資法第三條之權利及處理過程之紀錄？	**未保存當事人權利行使紀錄**：未明確區分與個資無關的客訴，或為當事人權利行使的案件，致雖有處理，仍未保存完整的申請單、處理過程及回覆紀錄，或超過個資法第13條規定的保存期限。
	10.3是否保存個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄？	**資料銷毀無紀錄**：未定期盤點並銷毀已逾保存期限的個資，或即使已執行銷毀，也未留下銷毀的原因、方法、時間及地點等書面紀錄。
	10.4是否保存人員權限新增、變動及刪除之紀錄	**未保留權限異動軌跡**：缺乏人員權限變動（如新增、刪除、調整）的紀錄，致無法追溯何人、何時、因何原因被賦予或移除特定權限。
	10.5是否保存消費者個人資料之蒐集、處理及利用紀錄，以及自動化機器設備之軌跡資料？	**缺乏軌跡資料**：未完整保存個資蒐集、處理及利用的系統軌跡資料，或軌跡資料的保存時間不足（如有適用產業個資辦法時，未能將紀錄留存五年）。
11.個人資料安全維護之整體持續改善（個人資料保護法施行細則第12條第2項第11款）	11.1是否定期就個人資料安全維護議題召開會議並提出持續改善報告？	**未定期召開會議**：未建立定期召開個資安全會議的制度，或會議流於形式，缺乏實質的議題討論與決策。
	11.2是否訂定個人資料管理（或安全維護）辦法並定期檢視更新？	**辦法未訂定或未更新**：未根據法規要求訂定個人資料管理辦法，或僅參考範本，而發生「說、寫、做」不一致的情形。或雖已訂定安維計畫，但未隨法規變動或內部環境變化而定期檢視與更新。

稽核項目	稽核內容	常見缺失
12.委託作業（個人資料保護法第4條、個人資料保護法施行細則第7條及第8條）	12.1委託他人蒐集、處理或利用個人資料之全部或一部時，是否要求受託人依委託人應適用之規定為之？	・**未能辨別何謂委外行為**：對委外關係認知不足，導致未執行應有的監督與管理。「委外」不僅限於簽訂正式合約、將蒐集、處理、利用個資的工作交付他人的情況皆屬之。
	12.2委託他人蒐集、處理或利用個人資料之全部或一部時，是否於委託契約或相關文件明確約定適當之監督事項及方式？	・**契約未明確規範**：委外契約或相關文件中，未明確約定受託廠商應遵守的個資法規，或未詳列應執行的監督事項及方式。 ・**未落實有效監督**：雖然在契約中有約定監督條款，但可能因磋商談判能力落差，致未定期進行實質稽核或要求廠商回報，導致監督流於形式。 ・**未限制資料處理範圍**：未要求受託者僅能在委託人指示範圍內蒐集、處理或利用資料，且未要求受託者在發現違法情形時，應立即通知委託人。
	12.3委託他人蒐集、處理或利用個人資料之全部或一部時，是否確實執行監督？	
	12.4是否要求受託者僅得於委託機關指示之範圍內，蒐集、處理或利用資料？	
	12.5是否要求受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關？	
13.使用資通訊系統蒐集、處理或利用個人資料（中央目的事業主管機關依個人資料保護法第22條第1項為職權調查之事項）	13.1是否就使用資通訊系統蒐集、處理或利用個人資料之服務範圍取得資安或個資驗證？	雖非強制要求通過ISMS或PIMS認證，或取得證書，惟公司可透過投資個資及資安驗證，證明其安全管理能力，與配置相當資源的決心。
14.個資存放雲端之安全控管（中央目的事業主管機關依個人資料保護法第22條第1項為職權調查之事項）	14.1是否確保個人資料放在雲端上的安全？	・**雲端個資未盤點**：未對儲存在雲端上的個資進行全面盤點，未能進行風險評估及有效管控。 ・**國際傳輸風險**：未考慮資料儲存地的法規與政治風險，例如將個資儲存在位於中、港、澳的雲端服務，可能涉及個資法第21條的國際傳輸限制，或無法提供明確的地端國家資訊。 ・**責任歸屬不明確**：與雲端服務供應商之間，對於資料保護的責任歸屬未於契約上明確規定，一旦發生資安事件，恐產生爭議。

稽核項目	稽核內容	常見缺失
		・**未採取適當安全措施**：未啟用或設定雲端平台安全功能，如資料加密、存取權限控管與日誌審核等功能。其中，存取權限控管缺失為最常見的風險點之一： ・**公開的儲存空間**：將含有敏感資料的儲存槽權限設為公開。 ・**不安全的API**： API認證不足或配置錯誤，致允許未經授權的存取。
15.發生個資事件之處理（中央目的事業主管機關依個人資料保護法第22條第1項為職權調查之事項）	15.1近兩年內是否發生個人資料被竊取、洩露、竄改或其他侵害情形之個資事件？	・**事件應變計畫不完整**：缺乏完整的應變計畫，導致在個資事件發生時，不清楚應通知當事人的範圍、內容及方式。 ・**未及時通報**：未能及時將事件通報給主管機關，且通報時間超過72小時，或未能向合適的聯絡窗口通報。 ・**未及時以適當內容通知消費者**：未針對「個別」受影響消費者發送通知，或發送內容未包含發生的事實、採取的因應措施與諮詢窗口，而僅發送「防詐提醒」。 ・**未委託第三方調查**：針對影響重大的個資事件，組織未考慮委託公正的第三方進行調查，以確保調查的客觀性與全面性。 ・**未進行根因分析**：無法提出有效的強化措施，避免類似事件再次發生。
	15.2是否就個資事件委請公正之第三方進行調查？	
	15.3是否及時且適當的通知當事人？	
	15.4是否就事件的發生進行根因分析，並提出強化措施？	
16.個人資料庫之共享使用（個人資料保護法第8條）	16.1是否有其他關係公司或主體共享使用本公司所蒐集之客戶個人資料庫？	・**資料庫共享未告知**：常見於與關係企業、委外廠商或合作夥伴共享資料庫時，未進行充分告知。 ・**責任歸屬不明確**：各關係企業之間的權責劃分不清，或個資管理能力不一，一旦發生個資外洩，難以釐清責任。 ・**未記錄資料流向**：缺乏完整的資料流向紀錄，追溯個資共享之對象、時間及目的，致資料使用透明度不足。

資料來源：經濟部主管商業服務業者個資防護自評表
註：常見缺失為作者依照個資稽核經驗所撰

本文以下統整數發部首波裁罰案例，分析企業在行政檢查過程中常見的風險誤區；並進而檢視金管會近十年重大個資相關裁罰，以及交通部所屬產業之裁罰案例，探討不同業別個資外洩的成因與各部會在裁罰上的差異。

（一）數發部裁罰案例

表4：數發部首波裁罰案例[13]

裁罰主體	主要缺失	裁罰結果[14]
蝦皮購物	1.個資盤點：僅提供4筆盤點內容，顯有缺漏 2.風險評估與管理：高風險流程未見矯正措施 3.委外監督未落實：台灣蝦皮委託新加坡蝦皮公司進行個資保護稽核，惟於108年後都未執行稽核與紀錄報告	依修法前《個資法》第48條第4款及第50條，處分業者及其負責人罰鍰各10萬元[15]
誠品生活	1.資安措施：多個帳號久未檢視及管理上執行未確實。 2.委外監督未落實：未見對委外廠商執行實地資安稽核之紀錄	同上述法條依據，業者併同其負責人罰鍰各5萬元[16]
旋轉拍賣	1.資安措施：應強化防詐及登入機制，如對話視窗，屬於業者具有主控權之場域，卻疏於採行有效阻斷QR code及惡意連結之機制功能[17] 2.委外監督未落實：對委外廠商實際執行稽核未有相關稽核紀錄 3.未及時通知個資當事人：發生疑似個資事故，卻未踐行《個資法》第12條規定以適當方式通知當事人	限期補正（兩月內改正），未裁罰[18]

資料來源：數發部新聞稿[19]

上述數發部裁罰三案中，電商業者普遍在「個資盤點完整性」、「風險評估與預防矯正措施」及「委外稽核落實度」方面仍存在缺失。尤其在「委外監督」的落實度上，關鍵在於企業是否能正確識別委外關係，對委外廠商是否進行充分的實質監督，並留存可

註13：數位發展部數位產業署(112年5月30日)，有關蝦皮、誠品生活及旋轉拍賣涉及個資外洩事件數位發展部查處說明，
https://moda.gov.tw/ADI/news/latest-news/5273。

註14：以下幣別皆為新台幣。

註15：依據112年5月30日數授產經字第1124000495號函，誠品生活股份有限公司違反個人資料保護法第27條第1項規定，依同法第48條及第50條規定處公司及代表人罰鍰各新臺幣5萬元整並令限期改正。

註16：依據112年5月30日數授產經字第1120004109號函，新加坡商蝦皮娛樂電商有限公司違反個人資料保護法第27條第1項規定，依同法第48條及第50條規定處公司及代表人罰鍰各新臺幣10萬元整並令限期改正。

註17：數位發展部訴願決定書，數位訴決字第1120004449號，
https://www-api.moda.gov.tw/File/Get/moda/zh-tw/urhu2wxNHsT77XT；數位發展部訴願決定書，數位訴決字第1120005038號，
https://www-api.moda.gov.tw/File/Get/moda/zh-tw/zIyIWNzVYssj4PV。

註18：112年1月19日數授產經字第1124000044號函、112年2月4日數授產經字第11240000661號函，均限期原告於文到之次日起2個月內改正，並將改正結果逕復數位發展部。

註19：數位發展部(112.5.30）有關蝦皮、誠品生活及旋轉拍賣涉及個資外洩事數位發展部查處說明，平臺經濟組，
https://moda.gov.tw/ADI/news/latest-news/5273 。

供佐證的稽核紀錄。絕非僅簽署保密契約即可，而是具體可證明實際執行與監督的過程，以確保個資安全義務得以落實。

（二） 金融業重大裁罰案例

金融業因處理個資數量龐大且高度敏感，一直是主管機關裁罰的重點。以下整理與個資管理缺失相關的重大裁罰案例：

表5：金管會重大裁罰案例

裁罰主體	主要缺失	裁罰結果
中國信託銀行	權限控管不足、索引檔外洩	於102年8月22日，依《銀行法》第129條第7款規定，核處400萬元罰鍰
國泰世華銀行	離職員工將客戶個人資料下載至私人外接儲存裝置	於103年1月29日，依《銀行法》第129條第7款規定，核處300萬元罰鍰
國際康健人壽	所訂「個人資料保護政策與規範」，未將個人資料保護納入公司內部控制制度	於103年10月27日，依《保險法》第171條之1第4項規定，與「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」（下稱「金管會個資安維辦法」）第13條，核處罰鍰60萬元
新光銀行暨子公司	跨業行銷濫用個資	於105年12月27日，依《金融控股公司法》第43條第2項及第60條第13款規定，核處200萬元罰鍰
臺灣產物保險	・事故演練不足，且發生員工以個人通訊軟體將因公務取得之個資外洩予第三人； ・弱點掃描及滲透測試作業範圍尚欠完備、又未對漏洞修補及追蹤處理未訂定作業規範	於108年6月3日，因核與《個資法》第27條第2項及同條第3項授權訂定之「金管會個資安維辦法」第10條第3項規定不符，依修法前《個資法》第48條4款予以限期改正
富士達保險經紀人	公司網站無個資告知聲明，且於蒐集及傳輸時，未採取適當加密措施	於109年9月18日，因核與《個資法》第8條及第27條第1項規定不符，依照修法前第48條4款予以限期改正
家樂福保險經紀人	逾越蒐集會員資料之「特定目的」，將會員個資提供予人壽公司作保險招攬使用，卻未明確告知會員，並取得單獨同意	於110年6月11日，因核與《個資法》第7條第2項、第19條第1項及第20條第1項規定不符，依《個資法》第47條規定，核處罰鍰15萬元整
友邦人壽	未建立確認個資取得適法性之檢核機制，且當事人拒絕行銷時，未有立即註記	於110年12月30日，依《保險法》第149條第1項規定予以糾正
福灣財產保險代理人	未經當事人同意取得其保固維修汽車所蒐集個資，並供予產物保險公司進行報價	於111年1月5日，因同時違反《個資法》第19條第1項、第20條第1項、《保險法》第165條第3項規定，以一事不二罰原則，依《保險法》第167條之3規定，核處限期1個月改正，併處罰鍰30萬元整
富昇保險代理人	未經當事人同意為個資蒐集、處理及為「特定目的外」利用	於111年3月16日，因核與《個資法》第7條第2項、第19條第1項第5款及第20條第1項第6款規定不符，依第47條規定，核處罰鍰15萬元整

裁罰主體	主要缺失	裁罰結果
凱基商業銀行	針對客戶行使當事人更正或補充個資時，未確實執行身分確認機制	於111年5月5日，因違反《銀行法》第45條之1第1項及該條授權訂定之「金融控股公司及銀行業內部控制及稽核制度實施辦法」（下稱「內控內稽辦法」）第3條及第8條第3項規定，爰依《銀行法》第129條第7款規定，核處600萬元罰鍰
上海商銀	・未建立個人電腦管理者權限及可攜式設備控管相關規範； ・未能依內部規範留存使用個資軌跡； ・未落實作業系統上線前及更新時，資安監控軟體之測試，且資安監控軟體派送至工作站後未能確認其執行結果	於112年11月28日，因違反《銀行法》第45條之1第1項及該條授權訂定之「內控內稽辦法」第3條及第8條第1項規定，爰依《銀行法》第129條第7款規定，核處1,000萬元罰鍰
台灣人壽	理賠人員與覆核人員互相出借密碼，且未建立帳號登入IP檢核機制，致內部人員可任意變更保戶聯絡資訊與通知設定，進而偽造理賠案件	於114年2月20日，依《保險法》第148條之3第1項授權訂定之「內控內稽辦法」第5條第1項第3款規定不符，考量該缺失為業者自行查核發現，經酌減後，依《保險法》第171條之1第4項規定，核處罰鍰420萬元整
台新銀行	因未建立完善的系統異動測試及跨系統檢核機制，致地址資料異常長期未發現並誤寄催收信函；另未落實委外督導與錯誤核驗，導致帳單姓名與交易明細錯置	於114年5月8日，依《銀行法》第45條之1第1項、第3項及其分別授權訂定之「內控內稽辦法」第3條第1項、第8條第1項及委外辦法第6條第1項規定，依《銀行法》第129條第7款規定，核處600萬元罰鍰
國泰世華銀行	・未完善建立信用卡客服作業之控管機制，致使客服人員得逕自變更客戶手機、電子郵件及通訊地址，並偽辦掛失補發信用卡，造成通知失效與寄送異常； ・信用卡影像調閱系統查詢條件過於寬鬆，僅憑姓名即可取得申請書資料	於114年8月11日，因違反《銀行法》第45條之1第1項及該條授權訂定之「內控內稽辦法」第3條第1項及第8條第1項規定，爰依《銀行法》第129條第7款規定，核處1,200萬元罰鍰

資料來源：金管會重大裁罰案件

金管會的重大裁罰案例顯示，雖有依據《個資法》及相關規定進行裁罰，但此類案件仍屬少數。大部分銀行保險業針對個資管理缺失的裁罰，仍是基於《銀行法》或《保險法》中關於內部控制缺失的規定，因此裁罰金額較高。分析以上案例，可歸納為以下內控缺失：

1. **人員控管與權限設定：**

銀行與保險業常見內部介面權限設置不當，致內部人員得以逕自修改匯款帳號、聯絡地址及簡訊通知設定，進而衍生盜刷或詐領保險的案例層出不窮。

2. **跨系統調整與資料處理失當：**

金融機構將帳單列印、封裝或資料處理等作業交由第三方辦理，惟因委外廠商設備異常或流程控管不全，發生帳單

而誤寄他人之情形；另雖於契約已約定個資及資安義務，卻未建立持續抽檢、驗證及異常回報機制，使監督責任流於形式。

3. **資安防護與演練不足：**

未針對駭客入侵或內部人員異常使用情境進行實際資安演練，漏洞掃描與修補追蹤亦不完整。

4. **未經同意之目的外利用與違法行銷：**

將客戶資料用於特定目的外利用，如行銷或集團跨業推廣，而未明確告知或取得當事人單獨的同意。

（三）交通部裁罰案例

交通部三起個資外洩案件，分屬觀光署、民航局及公路局所轄管。其共通原因在於未依其所屬產業個資子法規定[23]，建立並落實個人資料檔案安全維護計畫，亦未採取足以防範資料庫風險的資安措施。此等疏漏導致資料庫暴露於外部威脅之下，最終造成消費者個資外洩，甚至有國人資料遭兜售於暗網。

綜上，雖然現行各部會具備例行性檢查與行政調查權限，然而，我國個資規範仍以事後追究與調查為主，且現行《個資法》並未針對業者知悉疑似個資外洩卻未自主通報的罰則，導致主管機關介入多屬被動，凸顯修法之必要與急迫性。

表6：交通部裁罰案例（112年重大矚目案）

裁罰主體	主要缺失	裁罰結果
雄獅旅行社	個資防護措施不足，導致駭客入侵內部系統，取得旅客聯繫資訊	112年上半年行政檢查後雖無裁罰，但持續追蹤改善狀況；後於112年11月20日再次遭受網路駭客攻擊，經查違反個資法第27條第1項，依現行個資法第48條第2項裁罰200萬元[20]
華航	業者遭駭客勒贖，外洩會員個資共8,104筆；研判可能源自系統轉換或異業合作	依修法前個資法第48條裁罰20萬元
iRent和雲公司	外部通報資料庫具外洩風險，惟未依規定即時通報主管機關	依修法前個資法第48條裁罰20萬元[21]

資料來源：監察院調查報告[22]

註20：交通部於113年1月12日以交授觀業字第1133000076號函，就雄獅於112年11月20日遭受網路駭客攻擊案件裁罰。

註21：交通部於重新審查後，於112年10月5日以交授公運字第1120120041A號函，撤銷先前112年2月8日交授公字第1120015562A號函所為之新臺幣20萬元裁罰決定。

註22：監察院（113年1月18日）發布《個資外洩案調查報告》（字號：113交調0001），https://www.cy.gov.tw/CyBsBoxContent.aspx?n=133&s=28586。

註23：觀光署訂有「交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法」供觀光產業類（各旅行業者）遵循；民航局訂有「民用航空事業個人資料檔案安全維護計畫及處理辦法」供民用航空事業遵循；公路局訂有「汽車運輸業與計程車客運服務業個人資料檔案安全維護計畫及處理辦法」供汽車運輸業遵循。

參、個資防護新篇章：本階段修法動向與對產業之影響

一、 個資法的新佈局：未來修法之動向與調整

為回應111年憲判字第13號判決，籌備處於113年12月發布預告草案，內容涵蓋四大制度主軸：包括監管權限移轉之過渡條款、增設個資保護長（Data Protection Officer, DPO）制度、個資事故通報與應變義務，以及風險導向行政檢查之法源依據。惟114年3月27日行政院通過之新版本草案，部分制度設計出現調整：例如，限縮DPO制度之適用對象為公務機關，並將情報機關排除於可受稽核之範疇；對於非公務機關，則刪除高風險行業優先行政檢查之條文規劃。

儘管草案內容有所變動，現行制度仍透過《行政院及所屬各機關落實個人資料保護聯繫作業要點》延續對高風險產業之監理精神。主管機關於擬定年度行政檢查計畫時，仍將高風險業者[24]列為優先對象，明確風險導向監理模式之延續與制度化。修法後母法亦明定，未履行通報義務者，將處以新臺幣二萬元至二十萬元罰鍰，主管機關無須再透過間接適用《個資法施行細則》第12條第2項第4款，或依《個資法》第27條第2項授權所訂定之《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》中關於違反事故通報義務，來作為裁罰依據。

二、 兩階段修法第一步：本階段修法對於非公務機關的影響

本次修法對非公務機關最具實質影響之條文，為《個資法》草案第12條及第48條之修正。依修正草案規定，公務機關與非公務機關於發生個人資料外洩等事故時，除須採行適當之應變措施、保存事故紀錄，並依一定條件啟動通報程序外，亦應依事故樣態通知當事人。此一修法方向，標誌著過往多僅存於《個資法施行細則》與產業個資辦法的事故應變機制，已正式提升為具法律拘束力之法定義務，並明確公司於個資事故發生時的「通報」中央目的事業主管機關與「通知」當事人之雙重責任。

其中，通報義務之設計，係為協助主管機關即時掌握重大風險事故，並進行後續行政處置。配合第個資法12條通報義務的明文

註24：高風險者，得參考《行政院及所屬各機關落實個人資料保護聯繫作業要點》第六點各款情形及發生個資安維案件之次數等因素綜合考量:
(一)非公務機關之規模、特性。
(二)保有個人資料之數量或性質。
(三)與民眾日常生活關係密切程度。
(四)個資安維案件衝擊層面廣泛程度。
(五)個資安維案件將造成當事人身心危害、社會地位受損或衍生財務危機等重大影響。
(六)個人資料存取環境。
(七)個人資料傳輸之工具及方法。
(八)國際傳輸之頻率。

化，草案亦修訂第48條第1項，非公務機關違反個資事故通報應變措施 紀錄保存等義務者，則新增第二項處罰規定，毋庸先令其限期改正，即可逕予處罰二萬元至二十萬元之罰鍰，希冀提升公司對資訊安全事故之風險意識，並強化了個資治理從被動應變邁向積極防範之法遵架構。

此外，根據籌備處的說明[25]，為因應我國逐步邁向個人資料保護監理一元化之制度願景，本次修法亦於第51條之1中，增訂權限移轉之過渡條款。在未來六年之過渡期間，已有有明確目的事業主管機關之私部門，其個資保護事務仍暫由原中央目的事業主管機關或直轄市、縣（市）政府繼續監管，俟時機成熟後，再分階段將該監管權限逐步轉移予個資會。對於公務機關以及目前尚未明確劃分中央目的事業主管機關之業別（如金融租賃業），優先由個資委員會納入管理範圍，

表 7：各目的事業主管機關個人資料檔案安全維護辦法

主管機關	業別	辦法數
文化部	電影事業	1
數位部	數位經濟相關產業（包含：電子購物及郵購業 、軟體出版業 、電腦程式設計、諮詢及相關服務業、資料處理、主機及網站代管服務業、其他資訊服務業，以及其他資訊服務業 ）	1
經濟部	零售業、製造業及技術服務業、自來水事業、電業及公用天然氣事業、著作權集體管理團體	5
金管會	指定非公務機關（金融控股、銀行、證券、期貨、保險、電子支付、其他經金管會公告之金融服務業-指定外籍移工匯兌公司、財團法人）	1
通傳會	電信事業、用戶數達三千戶以上之提供網際網路接取服務之設置未使用電信資源之公眾電信網路者、有線廣播電視、電視、訂戶數達三千戶以上之直播衛星廣播電視服務事業、經營國內新聞台或購物頻道事業、電信消費爭議處理機構及其他公告通傳事業等八類	1
交通部	郵政業、交通部指定氣象產業類（氣象、海象預報業）、汽車運輸業與計程車業、民用航空事業、交通部指定非公務機關（觀光旅館業、旅館業、民宿、旅行業、觀光遊樂業）、停車場經營業、船舶運送業	7
教育部	短期補習班、私立兒童課後照顧服務中心、私立專科以上學校及私立學術研究機構、私立高級中等以下學校及幼兒園、運動彩券業、海外臺灣學校及大陸地區臺商學校	6
內政部	交友服務業、殯葬服務業、營建類非公務機關、移民業務機構、祭祀團體、政黨及全國性民政財團法人、宗教團體、地政類非公務機關、合作及人民團體類非公務機關、警政類非公務機關	10
勞動部	私立職業訓練機構、人力供應業、人力仲介業	3
衛福部	社會福利財團法人、醫院、精神復健機構、私立長期照顧服務機構、護理機構、社會福利機構、中藥批發零售業、化粧品批發零售業、醫療器材批發零售業、西藥批發零售業、非輻射電子醫療器材設備製造業、食品業	12
財政部	報關業、保稅倉庫物流中心、記帳士與記帳及報稅代理人、菸酒事業、公益彩券發行機構	5
公平會	多層次傳銷業	1
工程會	工程技術顧問業	1
核安會	游離輻射設備製造業	1
中央銀行	票據交換所	1
農委會	農藥販賣業、農業金融	2
陸委會	大陸委員會指定非公務機關	1
僑委會	僑務委員會指定特定非公務機關	1
合計		60

資料來源：本文自行繪製

註25：根據行政院第3945號決議，討論(二)個資法部分條文修正草案，個人資料保護法部分條文修正草案總說明，以及簡報歸納，網址：https://www.ey.gov.tw/Page/9277F759E41CCD91/747cda78-926f-4205-99b3-1a735fc1b97b。

填補監理真空帶。

三、 結語：制度縫隙與未來展望

本次修法雖然回應了111年憲判字第13號判決成立獨立專責機構的要求，並逐步建構通報、應變及監理權限移轉等制度，但仍留有未竟之處。首先，在六年過渡期間內，個資委員會、中央目的事業主管機關與地方政府可能形成重複性監管衝突。其次，若未來個資保護長制度若擴大至指定非公務機關，則個人資料保護長及稽核人員之職掌、職能條件、訓練、獎勵與獨立性，乃至是否得外聘或由集團母公司支援，其勞僱關係與責任歸屬等規定均仍付闕如。此外，罰則之解釋與行政檢查的力度與裁罰標準不一下，亦可能在明確性與公平性上引發爭議，皆為主管機關在個資法制修法之際，不可忽視的挑戰。

而值得期待的是，本次修法所揭示的「個資防護新篇章」，不只是法條文字的更新，更是將我國個資治理推向主動防範、風險導向的全新階段。個資保護不再只是應付檢查的義務，而應是企業內部制度主動設計出的結果。只有當「信任」成為企業經營邏輯的一部分，資料經濟才能穩健落地，進而轉化為長期競爭力。

隨著修法推進與獨立專責機構的運作，若能在制度設計上補足上述缺口，將使業者得以在個資保護機制完善的前提下，真正發揮數位足跡價值化的潛力，不僅能為消費者提供更具價值的服務，同時亦能提升資訊防護力，營造安心消費的環境。