調　查　報　告

壹、案　　由：邇來發生多起民間企業個人資料外洩甚至被上網兜售事件，包括雄獅旅行社股份有限公司、中華航空公司、和運租車股份有限公司和雲行動服務iRent、微風廣場實業股份有限公司等，外洩資料達數百萬筆，究原因為何？政府相關機關包含各該公司目的事業主管機關及資安專責單位對該等民間企業資安納管與平時之監督、事後之處罰是否足夠？現行相關法令是否完備？未來應處防範之道為何？均有深入瞭解之必要案。

貳、調查意見：

現今網際網路及跨境電子商務時代，如何有效管理「公務」或「非公務」機關個人資料之蒐集、處理或利用，為一大挑戰，前此個人資料保護法（下稱個資法）規定，並未明定主管機關，非公務機關採「分散式監督管理」之模式，由各中央目的事業主管機關或地方政府監督所轄事業之個人資料保護事項，至於公務機關之監管則回歸行政體系之指揮監督。是以，為落實111年8月12日憲法法庭111年憲判字第13號判決要旨，有關建立個資保護獨立監督機制之要求，個資法遂於112年5月31日修正[1]，由「個人資料保護委員會（下稱個資委員會）」

[1] 資料來源：國發會新聞稿，立法院三讀通過個資法修正案 將強化企業個資外洩罰則 並盡速設置個資保護委員會籌備處， 刊 登 日 期 ： 112 年 5 月 16 日 ， 取 自 網 址 ： https://www.ndc.gov.tw/nc_27_36901。修法有兩項重點；1.修正個資法第48條非公務機關違反安全維護義務之裁罰方式及額度，改為逕行處罰同時命改正，並提高罰鍰上限，處新臺幣（下同）2萬元以上200萬元以下罰鍰；情節重大者，處15萬元以上1,500萬元以下罰鍰。屆期未改正者，按次處15萬元以上1,500萬元以下罰鍰。藉由本次修正裁罰方式及額度，以回應各界普遍反映業者違反安全維護義務罰責過低，且先命改正後處罰之方式，無法責成業者強化個資的資安維護作為。2.增訂個資法第1條之1規定，由個資委員會擔任個資法主管機關。行政院將積極推動設置個資保護獨立監督機關，以呼應去(111)年8月12日憲法法庭第13號判決，要求3年內完成個資保護獨立監督機制之意旨，解決目前個資法分散式管理下之實務監管

擔任個資法主管機關，解決目前個資法分散式管理下之實務監管問題，並與國際趨勢接軌。

邇來發生多起個資外洩案件，引發各界高度關注，除公務機關性質之戶政、健保資料外，非公務機關包括雄獅旅行社股份有限公司（下稱雄獅公司）、中華航空股份有限公司（下稱華航公司）、和運租車股份有限公司和雲行動服務iRent（下稱和雲公司）、微風廣場實業股份有限公司（下稱微風公司）等，分別由交通部觀光署（原交通部觀光局，下稱觀光署）、交通部民用航空局（下稱民航局）、交通部公路局（原交通部公路總局，下稱公路局）、經濟部所轄管。旨揭個資外洩事件[2]，均非公務機關，即非屬資通安全管理法（下稱資安法）所稱特定非公務機關資料外洩，並非資安法規範對象，需依個資法及其中央目的事業主管機關所訂定之安全維護辦法相關規定辦理。基此，為釐清非公務機關個資外洩之經過、原因、行政檢查過程及後續複查結果，以及政府相關機關對該等民間企業資安納管、平時監督及事後處罰等，相關法令完備性與未來防範之道，爰立案調查。

本案經向交通部、經濟部、數位發展部（下稱數位部）、國家發展委員會（下稱國發會）函詢及調取相關卷證[3]，並於112年9月23日請交通部政務次長陳彥伯、經濟部商業發展署（原商業司）署長蘇文玲、數位部政務次長李懷仁、國發會副主任委員高仙桂率相關主管人員到院詢問；經彙整相關卷證資料，再參酌上開機關於本院詢問後所補充之書面說明[4]及審計部111年度中央政府總

問題，並與國際趨勢接軌。

[2]雄獅公司、華航公司、和雲公司、微風公司等4件個資外洩事件，分別以「雄獅個案」、「華航個案」、「iRent個案」、「微風個案」稱之。

[3]交通部（112年5月17日交郵字第1125006711、112年1月13日交科字第1125032945）、經濟部112年5月17日經商字第11204016790、數位部112年5月15日數位韌性字第1120008274、國發會112年6月9日發法字第1122001340號函。

[4] 國發會112年8月18日、數位部112年8月18日、經濟部112年10月19日之電子郵件補充資料。

決算審核報告等資料，茲臚列調查意見如下：

一、交通部監管「雄獅旅行社股份有限公司」、「中華航空股份有限公司」、「和運租車股份有限公司和雲行動服務iRent」，以及經濟部監管「微風廣場實業股份有限公司」個資外洩案，均已完成行政調查，函請業者限期改正在案；惟部分案件仍為觀察階段，尚未結案，交通部與經濟部允應持續督導，並觀察業者個資外洩改善情形。另，和雲公司未訂定個人資料檔案安全維護計畫長達9個月，且資料庫因不當配置導致資料曝險，本件凸顯交通部未能即時發揮監督與稽核功能，殊有不當，允應檢討策進。按消費者個資保護涉及人民權益甚鉅，主管機關有積極保障義務，行政院應督飭所屬以上開案件為鑑，重新喚醒臺灣企業對資料外洩之重視，促請業者提高個資保護意識與善盡維護責任，倘發生個資外洩事件，尤應積極查處並澈底執行違規裁罰，避免不必要之損害

(一)邇來發生多起個資外洩案件，除公務機關性質之戶政、健保資料、公務人員個資外，非公務機關包括雄獅公司（旅行業）、華航公司（航空事業）、和雲公司（汽車運輸業）、微風公司（百貨公司業）等，引發各界高度關注。上開個資外洩事件，均非公務機關，亦非屬資安法所稱特定非公務機關，並非資安法規範對象，需依個資法及其中央目的事業主管機關所訂定之安全維護辦法相關規定辦理，合先敘明。

(二)經查，**交通部**監管雄獅公司、華航公司、和雲公司（合稱交通部3件個資外洩案），分屬觀光產業類、民用航空事業、汽車運輸業等業別，分由觀光署、民航局、公路局所轄管，上開案件個資外洩分別於111年11月27日、112年1月4日、112年1月28日發

生，其事件發生前之資安管理相關規定與計畫，以及個資外洩之經過、原因、行政檢查過程詳后表，茲分別說明如下：

1、交通部3件個資外洩案之資安管理相關規定

（1）雄獅個案：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。

（2）華航個案：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。

（3）iRent個案：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（原名稱：汽車運輸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。

2、**針對交通部3件個資外洩案，據該部查稱**，雄獅個案遭駭客入侵所致、華航個案遭網路駭客勒贖持有其會員個資（疑105至107年間系統轉換，或異業合作時所致資料外洩）。其中，iRent個案未依相關規定制定個人資料檔案安全維護計畫，且資料庫暴露於公開網路不設防，足徵該部執行非公務機關例行性業務檢查作業，未能有效發揮監督與稽核功能，致無法及早發現業者未對消費者個資檔案安全採行適當維護計畫及處理，仍有待督促注意檢討改善在案[5]，另就本院調查發現iRent個案情形說明如后：

（1）未依行為時汽車運輸業個人資料檔案安全維護計畫及處理辦法第3條「**應訂定**消費者個人資料檔案安全維護計畫」之規定：**旨揭辦法**111

[5] 111年度中央政府總決算審核報告（第2冊）丙、拾貳、交通部主管（節錄），丙53-56。

年4月1日訂定發布，同年月29日施行[6]，迨至112年2月4日辦理行政檢查，始發現該公司並未訂定安全維護計畫，長達9個月。

（2）復依公路局於112年2月4日偕同中華資安公司及安侯顧問公司等第三方資安團隊至和雲公司進行複查，發現與「汽車運輸業個人資料檔案安全維護計畫及處理辦法」第7條、第18條、第21條等規定有違之情事，內容摘述如下：

〈1〉第7條第2款規定，業者應自事故發生或知悉時起72小時內填具個人資料侵害事故通報與紀錄表通報主管機關，副知公路局，未於時限內通報者，應附理由說明之。經檢視和雲公司個人資料侵害事故通報與紀錄表，未於個資外洩知悉後起72小時內通報，且尚未說明逾時通報原因，相關通報表單亦無權責主管(如代表人)核准紀錄。

〈2〉第18條第3項規定，業者應針對對外電子商務服務系統定期演練及檢討改善。惟查未發現對外電子商務服務系統執行「防止外部網路入侵對策」及「非法或異常使用行為之監控與因應機制」等情境之定期進行演練及檢討改善紀錄。

〈3〉第21條規定，業者應採行適當措施，採取個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據保存機制，以供必要時說明其所訂計畫之執行情況；其相關紀錄之保存期限至少為5年。經查，系統日誌原先紀錄僅留存7日，尚未發現iRent APP與iRent

[6] 111年4月1日交通部交路字第1115004382號令訂定發布全文23條(111年4月28日交通部交路字第11150056611號令發布，自111年4月29日施行)。

租賃系統日誌調整符合5年之紀錄。

（3）另據交通部查復資料及和雲公司112年2月4日聲明指出略以[7]，**和雲公司所屬雲端ELK資料庫(用於iRent App記錄應用程式Log檔之暫存資料庫)未適當阻擋外部連線，導致可能遭外部專業資訊人員使用特定工具及技巧進入查詢近3個月會員異動資料**，總計40萬108筆用戶個資存有外洩風險，坦承原初步發現並通報「近3個月內可能受影響用戶為14萬名，調整為40萬名」，全數納入對應範圍。關於事件的影響，也因資料庫曝險時間較長，爰將潛在影響用戶數量修正。是以，此情顯示和雲公司漠視全國人民個資之洩漏風險，影響層面加深加劇。

（4）**承前所述，鑑於資料庫外洩事故層出不窮[8]，尤應喚醒企業之重視，iRent資料庫因不當配置導致資料曝險，已非資安新議題，國內企業需汲取教訓，避免問題一再重演**。

3、再據交通部指稱略以，雄獅個案並無裁罰，持續觀察個資外洩改善情形是否確實執行，再行通報申請結案。經查，該公司於111年11月27日遭惡意不明人士透過網路攻擊作業系統，時隔1年再次發生，茲據該公司於112年11月20日聲明指出

[7] 摘錄交通部查復資料，摘錄附件5略以，iRent個案行政管理查核報告關於個資侵害總筆數，於112年2月1日首次通報存有外洩風險個資筆數計14萬2,509筆，經該公司後續評估風險範圍需擴大統計該資料庫於111年5月1日至112年1月28日期間之資料，爰該公司於**112年2月4日續報更正侵害筆數計40萬108筆**。

[8] 羅正漢，112年2月6日發表，iRent資料庫暴露於公開網路不設防，引發大眾關注，配置錯誤問題應受更多重視，取自：https://www.ithome.com.tw/news/155392。內容略以，再據資安業者Group-IB在西元2022年4月發布統計指出，2021年他們就發現了30.8萬筆開放在網際網路的資料庫，且2022年第1季又發現新增9.1萬個資料庫，5季下來共發現39.9萬個。至於資料庫類型上，以Redis資料庫管理系統最高（37.5%）、第二是MongoDB（31%），第三是Elastic（29%）。

[9]，疑遭駭客攻擊受損之範圍，資訊包含顧客姓名、聯絡方式、商品內容。但不包括消費者信用卡機敏性資料，後續應進行通報調查等程序，避免損害擴大；華航個案與iRent個案均有裁罰且已結案。針對上開等情，交通部允應持續督導，並觀察業者個資外洩改善情形。

表1　雄獅、華航、iRent等個資外洩事件個案之發生經過、行政檢查及裁罰情形一覽表

項次	雄獅個案	華航個案	iRent個案
類別	觀光產業類	民用航空事業	汽車運輸業
事件發生	111.11.27	112.1.4	112.1.28
個資外洩經過及原因	●雄獅公司於111年11月29日向觀光署通報，有旅客收到詐騙電話，疑似有駭客入侵該旅行社旅客聯繫資訊，觀光署於111年12月5日函請該公司妥速查明防範，並將後續處理情形函復。 ●雄獅公司111年12月21日函復該署，有關個資外洩屬遭駭客入侵所致，該公司已啟動內部資安防禦機制，並以手機簡訊針對風險範圍訂購人發出防詐騙通知；另於111年11月29日發布新聞稿聲	華航公司112年1月4日遭網路駭客勒贖持有其會員個資，並要求支付約2億元贖金，並預告將繼續揭露該公司會員個資，後陸續於駭客論壇揭露該公司計8,104筆會員加密個資(每次1,004筆)；經該公司比對揭露會員資料，有高比例與現有資料庫之資料不符，推定非近期外洩資料，可能係該公司105至107年間系統轉換，或異業合作時所造成資料外洩。	●和雲公司於112年1月28日接獲外部人士告知其資料庫個資具外洩風險，該公司即於獲報後1小時內阻斷外部連線，惟當時未通報交通部，另交通部亦未接獲數位部介入查處之相關通知。 ●公路局於112年2月1日上午接獲通知後，隨即請和雲公司提出書面說明並辦理通報作業，該局續依聯繫作業要點通報國發會及相關機關單位，並於同日下午派員至該公司行政調查。

[9] 取自：雄獅旅遊聲明，發稿日期：112年11月20日，取自：https://info.liontravel.com/category/zh-tw/notice/index。

項次	雄獅個案	華航個案	iRent個案
	明啟事及防詐騙提醒。		●公路局調查，係因和雲公司所屬雲端ELK資料庫未適當阻擋外部連線，導致可能遭外部專業資訊人員使用特定工具及技巧進入查詢近3個月會員異動資料。
行政檢查過程及後續結果	觀光署會同外部資訊安全公司前往雄獅公司現場行政檢查，並函請該公司依缺失及建議稽核報告回復（112.2.22、112.6.20）、雄獅於函復改善報告（112.4.28、112.8.22）。 備註：觀光署後續將持續追蹤該公司改善措施是否確實執行，並將改善情形通報國發會。	華航公司到民航局說明及提報改善報告（112.1.13）、行政檢查（112.2.7）、2次發函限期改正（112.2.9、112.2.18）、2次行政檢查複查（112.2.15、112.4.6）、辦理資安訪視與輔導（112.2.23）。 備註：行政檢查第2次複查，華航公司依會議結論補充並提送完整報告，行政檢查複查通過。	●公路局於112年2月1日接獲通報後派員行政調查，並發函要求限期改正。 ●公路局辦理2次複查：**112年2月4日派員複查，和雲公司未採行適當安全措施致個人資料洩漏，又未訂定個人資料檔案安全維護計畫，不符規定**；112年3月1日再複查，該公司已依限完成補正。
裁罰情形	**無裁罰紀錄**	個資法第48條裁罰華航公司新臺幣(下同)20萬元（112.3.22）	個資法第48條裁罰和雲公司20萬元（112.2.8）
結案日期	持續觀察改善情形是否確實執行，**若近期再無同案資料外洩案件發生，將通報國發會申請結案**。	112.7.5	112.7.31

日期格式：年.月.日

資料來源：整理自交通部查復資料及112年9月23日約詢簡報資料。

(三)再查，有關**經濟部**監管微風公司資安管理相關規定與計畫，以及個資外洩之經過、原因、行政檢查過程詳后表，茲說明如下：

1、訂有資訊安全管理辦法，及依該資訊安全管理辦法設有資訊安全管理/個人資料保護執行小組。

2、事故原因：112年2月22日報載微風集團用戶個資遭駭，並收到網路勒索信件。

3、資安外洩之應變作業：經內部評估後，決定立刻啟動系統緊急應變措施，先關閉系統，並公告暫停會員服務，因駭客宣稱入侵之現象，此階段為確保整體服務環境的一致性及完整性，決定立刻啟動緊急應變措施，採取全面更新系統策略，排除任何可能的不確定性因素；並以網路層的調整為主軸，依最小需求範圍之指引方針，盡可能地縮減外面IP曝光之範圍，同時擴大雲端防禦系統保護範圍，致使駭客只能進行外網攻擊，而藉由雲端防禦系統之阻擋，進而成功化解掉駭客持續對公司的報復型、暴力攻擊事件。

表2　微風個案事件發生經過、行政檢查及裁罰情形一覽表

項目	相關說明
事件發生	112.2.22
個資外洩經過及原因	微風公司用戶個資遭駭，並收到網路勒索信件，內容包含微風公司業務資料及供應商資料與90萬用戶個資等。
行政檢查過程及後續結果	經濟部、資安院、資策會、內政部警政署前往微風公司（112.2.23、112.2.24），疑係「微風數位時代股份有限公司」建置會員APP蒐集之個資遭駭、召開行政調查會議（112.4.7）、發函限期改正（112.4.17）、112年4月19日發函於同年5月8日(含)前提供第三方調查報告，該公司於同年6月8日提交資安事件調查報告。
裁罰情形	微風公司裁罰20萬元；微風公司之代表人裁罰20萬元。

項目	相關說明
結案日期	尚未結案。

日期格式：年.月.日

備註：於112年12月19日致電經濟部確認本案目前尚未結案。

資料來源：整理自經濟部查復資料及112年9月23日約詢簡報資料。

(四)綜上，交通部監管雄獅個案及經濟部監管微風個案尚未結案，其中雄獅公司繼111年11月27日遭惡意不明人士透過網路攻擊該公司作業系統，另於112年11月20日再度發生，上開機關允應持續觀察個資外洩改善情形，並依個資法暨其施行細則及監管各業別個人資料檔案安全維護計畫及處理辦法等相關規定，加強客戶個人資料保護作業，並觀察業者個資外洩改善進度。另，和雲公司未訂定個人資料檔案安全維護計畫長達9個月，且資料庫因不當配置導致資料曝險，本件凸顯交通部未能即時發揮監督與稽核功能，殊有不當，允應檢討改進。按消費者個資保護涉及人民權益甚鉅，主管機關有積極保障義務，行政院應督飭所屬藉由上開案件，重新喚醒臺灣企業對資料外洩之重視，促請業者提高個資保護意識與善盡維護責任，倘發生個資外洩事件，尤應積極查處並澈底執行違規裁罰，避免不必要之損害。

二、「個人資料保護法」於84年8月11日制定公布，非公務機關之個人資料保護事項之監管，由各業別之中央目的事業主管機關辦理，國發會僅為解釋機關；為符合111年憲法法庭宣示第13號判決意旨、國家人權行動計畫之規劃及國際趨勢，嗣112年5月31日修正公布，由「個人資料保護委員會」擔任個資法主管機關，

刻正推動組織法草案及第2階段個資法修正工作，後續允應依上開判決意旨，積極建立個資保護獨立監督機制，發揮專責機關之實質功能。另個資法並未規範個資外洩事件之通報機制，對於「應通報未通報」或「遲延通報」亦無罰則，顯仍有未盡周延之處，允宜併同檢視，強化行政機關執法權限及監督力道

(一)個資法立法架構原係採分散式管理，國發會為個資法之法律解釋機關，至於各該非公務機關之個人資料保護事項之監管，則由各業別之中央目的事業主管機關辦理；該會為符合111年憲法法庭宣示第13號判決意旨、國家人權行動計畫之規劃及國際趨勢，提高個資外洩事件相關罰則，提出個資法第1條之1、第48條、第56條修正草案，內容為：增訂由「個資委員會」擔任個資法主管機關，修正非公務機關違反安全維護義務之裁罰方式及額度，改為逕行處罰同時命改正，並提高罰鍰上限[10]，行政院於112年4月13日第3851次院會通過修正草案，經立法院於112年5月16日三讀通過，總統於112年5月31日公布，期提升對個人資料保護之重視，賦予行政機關更有效之執法權限，合先敘明。

(二)有關個資法第1條之1規定，賦予個資保護獨立監督機關設置依據之目前籌備現況與進度。**據國發會指稱略以，**「為順利推動成立個資委員會，行政院籌

[10] 資料來源：國發會新聞稿摘要略以，2項修法重點，1.修正個資法第48條非公務機關違反安全維護義務之裁罰方式及額度，改為逕行處罰同時命改正，並提高罰鍰上限，處2萬元以上200萬元以下罰鍰；情節重大者，處15萬元以上1,500萬元以下罰鍰。屆期未改正者，按次處15萬元以上1,500萬元以下罰鍰。藉由本次修正裁罰方式及額度，以回應各界普遍反映業者違反安全維護義務罰責過低，且先命改正後處罰之方式，無法責成業者強化個資的資安維護作為。2.增訂個資法第1條之1規定，由個資委員會擔任個資法主管機關。行政院將積極推動設置個資保護獨立監督機關，以呼應去(111)年8月12日憲法法庭第13號判決，要求3年內完成個資保護獨立監督機制之意旨，解決目前個資法分散式管理下之實務監管問題，並與國際趨勢接軌，取自：https://www.ndc.gov.tw/nc_27_36901。

設『個人資料保護委員會籌備處(下稱籌備處)[11]』，並於112年9月23日完成籌備處暫行組織法規之發布，其他籌備事項亦逐步依時程規劃推進中，依上開憲法法庭判決意旨，**於114年8月12日前成立**」等語。同時表示，籌備處成立後，全盤檢視個資法，規劃個資委員會之編制及其應執行之任務，以及中央、地方主管機關之合作機制，瞭解目前其對各轄管產業之監管情形與產業特性，於無違個人資料保護的核心價值下，搭配國內實務發展狀況與國際個資保護監督機關監管實務趨勢，研擬及協調我國公、私部門整體個人資料保護監管模式與未來個資委員會監管與執法架構與策略。

(三)實務上，有關個資事件與資安事件適用法令上，據國發會、數位部查稱略以，依資安法規定，資安法係為建構國家資通安全環境，賦予納管對象資安防護責任，適用對象為公務機關及特定非公務機關，而依個資法規定，著重個人法益之保護，避免人格權受侵害，並促進個人資料之合理利用，適用對象為公務機關及非公務機關。實務上，於公務機關及特定非公務機關處理之資訊，涉及以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統或相關之服務，則應適用資安法規定，因資安問題所致個資外洩事件，應優先依據該法相關規定辦理，並通報主管機關數位部資通安全署；然而，針對非公務機關個資外洩事件通報處置機制情形，據國發會查稱「個資法未明定非公務機關之通報義務，亦無通報規範及罰則」等語，顯見個資法僅強調個資之蒐集、處理及利用，避免人

[11]籌備處已於112年12月5日成立，行政院長表示：人員編制為39人，未來會增加到89位。

格權受侵害，並促進個人資料之合理利用，由該法所列章節可知（按：第1章總則、第2章與3章公務機關對個人資料之蒐集、處理及利用、第4章損害賠償及團體訴訟、第5章罰則、第6章附則），並無訂定個資外洩相關通報機制，實務上任由各目的事業主管機關自行認定，且對未通報或延遲通報行為亦無罰則與處置，茲說明如后[12]：

1、資通安全事件者，得依循各該機關按資安法第14條第1項及第2項規定所設置之通報及應變機制，於知悉資通安全事件時，辦理通報上級機關或監督機關，並應通報主管機關等事宜；非資通安全事件者，因個資法條文並無訂定非公務機關應通報及應變機制之一致標準規範，當事件發生時，未能即時採取緊急警示與危機處理等相關措施，以有效縮短處理應變時間，及儘速降低對民眾損害程度，恐致損害賠償風險驟增。又，個資法第47條至第49條之行政罰鍰，僅涵蓋非公務機關違反該法有關蒐集、處理及利用個資等相關罰則規定。

2、再查，「行政院及所屬各機關落實個人資料保護聯繫作業要點」，尚無法源依據可就非公務機關若有延遲通報行為，訂定相關處罰機制，無法即時防制違規再犯。

(四)再據相關文獻學者指出[13]，我國現制缺乏個資保護專責機關與獨立監管機制，存在「有違憲疑慮」、「無從回應社會對於重大事故發生後應嚴格執法之期待」、「組織、人員、財務、功能方面獨立性不足」、

[12] 111年度中央政府總決算審核報告（第2冊）丙、貳、行政院主管（節錄），丙53-56。

[13] 資料來源：蔡柏毅（民112）。我國設置個資保護專責機關與獨立監管機制之芻議。***金融聯合徵信。42***，45-46。

「權責不清」、「利害衝突」、「主管機關事權不分」「無從與歐盟地區及先進國家直接進行合規的個人資料國際傳輸」、「法令遵循成本過度提高」等種種問題，現階段刻正推動組織法草案及第2階段個資法修正工作，對於能否解決前開問題尚待觀察，盼未來個資委員會成立後，藉由法律、資安、資訊、資料等跨領域專家對於專業、技術的熟稔，運用歷年累積之實務經驗，追求在「釐清問題」與「解決問題」方面，針對未來層出不窮的各種個資疑難問題提出因應，保持重要政策之持續與延續性，避免短期或偏狹的利益考量，主動介入，積極監督，發揮個資保護專責機關的實質功能，俾符國發會所稱「有明確規範整併權限為專責機關之重要意義，達到事權統一，提升執法效能」之設立目的與功能，並可確保個資之蒐集、利用符合相關法令之規定，增強個資蒐用之合法性與可信度，避免其受到濫用或不當洩漏。

(五)綜上，「個人資料保護法」於84年8月11日制定公布，非公務機關之個人資料保護事項之監管，由各業別之中央目的事業主管機關辦理，國發會僅為解釋機關；為符合111年憲法法庭宣示第13號判決意旨、國家人權行動計畫之規劃及國際趨勢，嗣112年5月31日修正公布，由「個人資料保護委員會」擔任個資法主管機關，刻正推動組織法草案及第2階段個資法修正工作，後續允應依上開判決意旨，積極建立個資保護獨立監督機制，發揮專責機關之實質功能。另個資法並未規範個資外洩事件之通報機制，對於「應通報未通報」或「遲延通報」亦無罰則，顯仍有未盡周延之處，允宜併同檢視，強化行政機關執法權限及監督力道。

三、依「行政院及所屬各機關落實個人資料保護聯繫作業要點」規定，個資外洩案件均應於規定時間內填列「監督通報紀錄表」通報，倘屬重大矚目案件：「知悉後24小時內通報、3日內進行行政調查，調查後10日內完成調查報告」，另將具有高風險者優先列入年度檢查對象，加強對非公務機關個人資料保護之監管，落實非公務機關個人資料檔案之安全維護，允應持續督導並澈底執行；惟「重大矚目案件」、「高風險者」尚乏明確標準，亦無「改正期限」天數、次數限制，任憑各部會自行裁量，亟待政府整體正視及全般審慎評估，避免導致業者質疑公平性

(一)行政院為防止非公務機關違反個人資料檔案安全維護義務，加強所屬中央目的事業主管機關對非公務機關個人資料保護之監管，以落實非公務機關個人資料檔案之安全維護，特於110年8月11日訂定「行政院及所屬各機關落實個人資料保護聯繫作業要點」(下稱聯繫作業要點)，復於112年5月29日修正[14]，聯繫作業要點載明，行政院得召開行政機關落實個人資料保護執行聯繫會議(下稱聯繫會議)，執行相關任務，包含：1.研議中央目的事業主管機關依個資法第27條第3項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（下稱安全維護辦法）應予規定之相關事項。2.統籌個資外洩案件之監督通報。3.就重大矚目之個資外洩案件管轄權爭議，確認管轄機關，及該案件行政調查之協調。4.其他個人資料侵害案件之跨部會協調聯繫事務。其所稱「重大矚目」之個資外洩案件範圍，1.行政院、立法院或監察院

[14] 110年8月11日行政院院授發協字第1102001106號函訂定、112年5月29日行政院院授發協字第1122001174號函修正。

關注之個資外洩案件。2.經媒體顯著披露之個資外洩案件，例如經平面媒體全國性版面報導、電子媒體專題討論。此外，**對於行政檢查部分**，中央目的事業主管機關應於每年1月底前擬定依個資法第22條第1項規定辦理之行政檢查計畫送國發會，並於提報聯繫會議後，確實執行，亦應評估所管非公務機關之個資外洩風險，將其中具有高風險者優先列入年度行政檢查對象（所謂高風險者，得參考第6點各款情形[15]及發生個資外洩事件之次數等因素綜合考量）；**有關通報部分**，中央目的事業主管機關接獲非公務機關通報或副知，或非因通報或副知而自行知悉個資外洩案件，經確認屬該機關管轄後，應於接獲通報、副知或知悉時起72小時內，填列監督通報紀錄表，通報國發會。但個資外洩案件屬重大矚目者，於知悉後24小時內通報國發會及數位部，並偕同數位部於3日內進行行政調查，提供專業分析與鑑識技術協助，跨部會合作提升行政調查能量；且應於調查後10日內完成調查報告；必要時國發會得報請行政院2週內召開會議，由行政院政務委員主持，聽取行政調查辦理情形（參照聯繫作業要點第2點、第4點、第7點、第8點），先予敘明。

(二)復查，聯繫作業要點優先針對高風險業者，強化例行性的行政查核，立意良善，然據國發會、數位部、經濟部、交通部對於有關「高風險業者」認定未盡一致：

1、國發會：依據聯繫作業要點第4點及第6點規定，

[15] 1.非公務機關之規模、特性。2.保有個人資料之數量或性質。3.與民眾日常生活關係密切程度。4.個資外洩衝擊層面廣泛程度。5.個資外洩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。6.個人資料存取環境。7.個人資料傳輸之工具及方法。8.國際傳輸之頻率。

由中央目的事業主管機關評估非公務機關發生個資外洩事件之次數、非公務機關之規模與特性、保有個人資料之數量或性質、與民眾日常生活關係密切程度、個資外洩衝擊層面廣泛程度、個資外洩將造成當事人身心危害與社會地位受損或衍生財務危機等重大影響、個人資料存取環境、個人資料傳輸之工具及方法、國際傳輸之頻率等因素綜合考量，判斷是否為高風險業者。

2、數位部：針對12個月內發生2次以上個資外洩之高風險業者。

3、經濟部：依聯繫作業要點第6點各款情形，包含業者之規模、特性；保有個人資料之數量或性質；與民眾日常生活關係密切程度；個資外洩衝擊層面廣泛程度；個資外洩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；個人資料存取環境；個人資料傳輸之工具及方法；國際傳輸之頻率，並斟酌業者之行業型態及規模(資本額)、保有個人資料數量、發生個資外洩次數、曾因個資外洩受主管機關行政檢查之情形，及發生個資外洩業者所屬集團之其他業者等因素，據以擇定行政檢查之對象。

4、交通部：各業別屬性差異，分如下：

（1）觀光產業類：觀光署針對重大矚目案件、警政署165反詐騙諮詢專線所列高風險事業，或接獲外洩之通報次數達2次，且筆數超過200筆之觀光產業業者列為必要檢查案件。

（2）汽車運輸業：當年度曾發生重大矚目之個資外洩案件者或保有個人資料之數量較多(1萬筆以上)且與民眾日常生活關係密切(寄送貨物)之較具規模汽車路線貨運業者。

（3）民用航空事業：民航局針對112年發生個資外洩事件之業者優先辦理行政檢查。

5、渠等於本院約詢時分別表示：數位部李懷仁次長「依據警政署之通報系統，通報次數較高，密切注意」；經濟部商業發展署（原商業司）蘇文玲署長「小型業者執行行政檢查成本較高，以個資筆數較多者為先」；交通部陳彥伯次長「先從民航局、觀光署開始，因為家數較多，原則上是高風險或個資數較多者優先」等語。

(三)另查，國發會雖稱，各部會近期對於重大矚目案件，已強化案件通報程序，惟重大矚目案件定義依聯繫作業要點乃指，行政院、立法院或監察院關注之個資外洩案件，或經媒體顯著披露之個資外洩案件，倘不屬前開機關關注或媒體揭露者，是否就形同「一般案件」處理。易言之，當個資外洩發生時，各目的事業主管機關對重大矚目案件認定標準不同，均視個案予以判斷，一般案件與重大矚目案件在通報程序上有所不同（詳下表），包含通報時間、通報機關、行政檢查及完成調查報告，恐致案件通報程序未臻完備，影響處理時效、耽誤處置作為。

表3　一般案件與重大矚目案件定義、行政措施及處置時效一覽表

項目	一般案件	重大矚目案件
定義	-	1.立法院或監察院關注之個資外洩案件。 2.**經媒體顯著披露之個資外洩案件**。
通報時間	72小時內	24小時內
通報機關	國發會	國發會及數位部
行政檢查	個資外洩案件之後續行政措施及處置情形，按季通報國發會。	3日內
調查報告		調查後10日內

資料來源：本調查自行彙製。

(四)再查，個資法第48條「限期改正」之規定，其中第1項規定，非公務機關有相關情事之一者[16]，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2萬元以上20萬元以下罰鍰。究此，**國發會指稱略以**，「實務上，個資外洩案件樣態多元且複雜，無法訂定一致之改正期限規範，仍應由目的事業主管機關依具體個案中，違反義務之非公務機關動機、行為或系統模式、事故影響程度、人數等實際情況彈性調整，裁量判斷合理之改正期限」。另參本院約詢時數位部李懷仁次長指稱，「如果是破壞到技術層面如：核心系統，可能需要2-3年，不知弱點爰無法訂定法律」、「無法定一個具體的期限」、「一般製造業與金融業之核心系統，嚴謹程度不同，如類似案件，應該會有類似期限可依循」等語，茲以國發會提供112年相關個案處理情形說明，其給予改正天數最短1天，最長32天，以交通部監管案件之其中2例，改正天數分別為1天與1個月，顯見其模糊性太高，恐致民間業者質疑公平性。甚且，該會提供7件個案中，有5件為「未依限改正予以裁罰」等情，益徵機關給予之改正期間與業者實務執行上存有落差。另就數位部3個案進行說明，數位部個資外洩之處理過程含「函請業者補充說明、查明案情並說明、召開行政檢查會議、複查會議、限期改正、現地檢查」等，來回數十回，最後才進行開罰，尚乏明確標準下，限期改正的次數不一，1次至4次不等，且前次改正時間離下次改正時間約16日至3個月不等，難謂妥適。

[16] 相關情事之一者：1.違反第8條或第9條規定。2.違反第10條、第11條、第12條或第13條規定。3.違反第20條第2項或第5項規定。

(五)綜上，依「行政院及所屬各機關落實個人資料保護聯繫作業要點」規定，個資外洩案件均應於規定時間內填列「監督通報紀錄表」通報，倘屬重大矚目案件：「知悉後24小時內通報、3日內進行行政調查，應於調查後10日內完成調查報告」，另將具有高風險者優先列入年度檢查對象，加強對非公務機關個人資料保護之監管，落實非公務機關個人資料檔案之安全維護，允應持續督導並澈底執行；惟個資外洩案件樣態多元且複雜，「重大矚目案件」、「高風險者」尚乏明確標準，亦無「改正期限」天數、次數限制，任憑各部會自行裁量，亟待政府整體正視及全般審慎評估，避免導致業者質疑公平性。

四、數位發展部為綜合性電商（無店面零售業）之主管機關，111年8月27日至112年8月底止，接獲內政部警政署通報個資疑似外洩案件計53家業者，尚未結案者占五成；又僅依該署通報案件啟動行政檢查程序，結案亦以「是否再獲通報」作為判斷依據，迄今尚無整體系統性規劃處理方式，行事有欠積極，殊有未洽。又其監管「蝦皮購物、旋轉拍賣、生活市集」個資外洩，111年至112年受騙人次達3,500餘人次，高達95%之受害者多為賣家，係屬詐騙集團全新隨機詐騙手法，上開等情均應積極研謀對策並加強宣導。另，該部推行「隱碼機制」，運用數位工具提升電商資安防護能力，保護民眾個人資訊不外流，目前已有3家導入，為減少個資外流、降低詐騙發生率，允應賡續輔導業者積極辦理

(一)數位部依個資法第27條第3項規定訂定「數位經濟相

關產業個人資料檔案安全維護管理辦法」[17]略以，上開管理辦法所稱數位經濟相關產業，指從事相關行業之自然人、私法人或其他團體，依行政院主計總處行業統計行業名稱及分類編號，包括：1.電子購物及郵購業（4871）、2.軟體出版業（582）、3.電腦程序設計、諮詢及相關服務業（620）、4.資料處理、主機及網站代管服務業（6312）、5.其他資訊服務業（639）、6.未分類其他金融輔助業（6699）。是以，數位部為綜合性電商（無店面零售業）的主管機關，據該部查復稱，收到疑似個資外洩通報（含警政署165通報），均發函要求業者查明個資外洩事故根因及說明其後續改善措施，並輔導業者進行落實法令遵循及內部管理的改善，協助業者打造健全之資安防護、落實資安管理，合先敘明。

(二)據數位部復稱，所主管無店面零售，收到疑似個資外洩通報有相關處置作為；然而，該部僅對警政署通報個資外洩案件啟動行政檢查程序，結案也以「有無接獲警政署通報」為判斷依據，且多以書面審查為主（72%），行政調查占少數（28%），迄今尚未結案者占五成[18]，茲摘述111年8月27日至112年8月底止，該部接獲疑似個資外洩通報之處理情形如下：

1、接獲個案數：53家(121家次)，其中26家已結案、11家尚在觀察期、16家尚待補正。

2、行政調查部分：針對重大案件、多次通報、遲未回應、回應措施不足業者共15家，啟動行政調查

[17] 數位部112年10月12日數授產服字第1126000621號令訂定發布「數位經濟相關產業個人資料檔案安全維護管理辦法」，全文20條；自發布日施行。

[18] 計算式：(53-26) /53=50.94%【未結/總數=未結%】。

作業，已辦理17次行政調查，其中3家已結案、5家尚在觀察期、7家尚待補正。調查結果函請業者限期改正(善)共8家(含違反個資法規定裁罰2家)，業者均依限提出改善計畫。

3、書面審查部分：共38家，經法律及資安專家以書面審查業者回應說明，其中23家已結案、6家尚在觀察期、9家尚待補正。

表4　數位部監管無店面零售收到疑似個資外洩通報之相關處置作為

單位：家

	合計	待補正	觀察期	結案	限期改正	裁罰
行政調查	15	7	5	3	8	2
書面審查	38	9	6	23	-	-
總計	**53**	**16**	**11**	**26**	**8**	**2**

註：結案原因為業者已落實所提改善措施，且未再接獲警政署通報。

資料來源：數位部約詢時簡報、書面說明資料。

(三)隨著科技越趨發達，帶動電商產業蓬勃發展（謂：跨境電商[19]），除在國內進行網路交易，更能不受地域限制，橫跨各國進行貨物販售，不僅擴大銷售市場，亦增進企業能見度。復據數位部查復表示，近年網路購物風氣盛行，蝦皮購物、旋轉拍賣、生活市集（下稱3家平台電商），屢有疑似個資外洩事件而引發詐騙情事，業者因業務性質蒐集大量個資，易衍生個資外洩風險，調查指出蝦皮購物與旋轉拍賣，有高達九成五受害者是賣家，打破以往買家受騙之框架，說明如下：

1、犯罪集團假扮為普通買家(下稱假買家)，透過電

[19] 跨境電商的全名為跨境電子商務（Cross Border E-Commerce）：在定義上，與跨境零售相似，皆是藉由不同關境的交易主體，透過電子商務（網路平台）完成進出口貿易中展示、洽談、金流交易等環節，再藉由跨境物流送達商品，完成商品交付的國際商業活動。簡單來說，是指一種「發生地點在網路上」的國際貿易，即從國外網路平台下單，把所需物品買回來的過程。

商平台提供的訊息功能私訊給正常賣家，佯稱「想購買賣場內商品，但無法結帳，因電商平台顯示該賣家之賣場未完成金融認證」。

（1）假買家提供假冒成電商平台之假網址或QR CODE，請正常賣家去完成金融認證。

（2）正常賣家誤信為真，點選假買家提供之假網址，通常該假網址都會使正常賣家加入詐騙集團的line好友，並又佯稱其為電商平台客服，要求正常賣家應進行金融認證，並要求正常賣家提供姓名、電話及常用金融機構名稱等。

（3）詐騙集團即假冒金融機構致電正常賣家，要求其使用網路銀行操作轉帳，正常賣家誤以為是金融機構認證程序，多次轉帳導致受騙。

2、據數位部指稱略以，消費者被詐騙細部報案資料進行分析顯示，95%[20]為賣家遭詐騙，買家遭詐騙占5%[21]，個案處理情形彙整詳下表。

表5　數位部監管3家平台電商個資外洩案之發生經過與處理情形

	蝦皮購物	旋轉拍賣	生活市集
通報次數[3]/行政調查	7次(1,198人受騙)/5次	8次（1,960人受騙）/5次	8次（389人受騙）/3次
裁罰依據及內容	未符合個資法第27條第1項應採行適當之安全措施，依個資法第48條第4款及第50條，業者併同其負責人處合計20萬元罰鍰；命限期改正及提出改善措施。	無	無

備註：統計自數位部111年8月至112年8月期間警政署接獲受害者通報人數。

資料來源：整理自數位部112年9月23日約詢簡報資料。

[20] 收到假買家傳訊說無法下標，並傳送提供連結網址，受害者連結並輸入驗證銀行名稱，接到假銀行客服來電要求配合驗證、綁定等話術要求依指示網路轉帳，受害者依指定操作受騙。

[21] 收到假客服告知訂單扣款有誤等，要求提供登載銀行及會有銀行客服處理，稍後假銀行客服來電，受害者依指示操作轉帳受騙。

3、又查，數位部對3家平台電商辦理行政檢查、函請業者限期改正、函請業者補充說明在案，惟對蝦皮購物裁罰，未對旋轉拍賣、生活市集裁罰之原因如下：

（1）旋轉拍賣：接獲通報後，即函請業者說明妥處；數位部於111年12月30日、112年3月15日、3月23日、4月28日、8月23日辦理5次行政檢查，並於112年1月19日、2月4日、112年5月5日、5月30日函請業者限期改正，再於112年6月30日函請業者補充說明，業者均配合回復說明，並提供相關佐證資料，經審查委員檢視業者已採行適當的安全措施，故給予觀察改善期。

（2）生活市集：接獲通報後，即函請業者說明妥處；數位部於111年12月30日、112年5月8日、7月4日辦理3次行政檢查，並於112年5月23日函請業者限期改正，再於112年7月21日函請業者補充說明，業者均配合回復，並提供相關佐證資料，且自7月之行政調查後，165接獲民眾通報案件數逐步趨緩（由最高峰115人調降為14人），經委員討論決議每季定期查核。

(四)再查，數位部擬訂定參考指引供業者參考，使業者了解如何執行個資安全維護措施及資安保護措施，提醒業者蒐集個資時應遵守個資法「最小化原則」。此外，為鼓勵電商業者導入物流隱碼技術，運用數位工具提升電商業者資安防護能力，保護民眾在電商物流配送過程中，個人的電話號碼資訊不外流，減少詐騙發生的可能性，提出「隱碼機制」，即一般電商業者收到訂單後，透過物流士配送貨物，並在宅配單上印載訂單收貨人的聯絡電話號碼，以供物流士聯繫訂單收貨人收件；導入隱碼機

制後，電商業者將原訂單收貨人的聯絡電話號碼轉換為代碼，宅配單上同步進行隱碼處理，物流士則透過隱碼服務平台撥通總機加上撥接代碼，轉接給訂單收貨人，避免民眾電話號碼從物流端外洩，截至112年9月底，已有3家電商業者（FriDay購物、momo、博客來）導入隱碼機制，2家電商業者（東森、PChome）進行場域驗證，3家電商業者（酷澎、蝦皮及Yahoo）洽談規劃評估中。

(五)綜上，數位部為綜合性電商（無店面零售業）之主管機關，111年8月27日至112年8月底止，接獲內政部警政署通報個資疑似外洩案件計53家業者，尚未結案者占五成；又僅依該署通報案件啟動行政檢查程序，結案亦以「是否再獲通報」作為判斷依據，迄今尚無整體系統性規劃處理方式，行事有欠積極，殊有未洽。又其監管「蝦皮購物、旋轉拍賣、生活市集」個資外洩，111年至112年受騙人次達3,500餘人次，高達95%之受害者多為賣家，係屬詐騙集團全新隨機詐騙手法，上開等情均應積極研謀對策並加強宣導。另，該部推行「隱碼機制」，運用數位工具提升電商資安防護能力，保護民眾個人資訊不外流，目前已有3家導入，為減少個資外流、降低詐騙發生率，允應賡續輔導業者積極辦理。

參、處理辦法：

一、調查意見一，函請行政院督飭所屬確實檢討改進見復。

二、調查意見二、三，函請行政院研處見復。

三、調查意見四，函請數位發展部確實檢討改進見復。

四、檢附派查函及相關附件，送請交通及採購委員會處理。

調查委員：王麗珍

葉宜津

賴鼎銘

中　　華　　民　　國　　113　　年　　1　　月　　9　　日