從歐盟 GDPR 略窺我國個資法及子法之修正方向

蔡柏毅 / 金融聯合徵信中心 法務室

前言

歐盟《個人資料保護規則》（General Data Protection Regulation，以下簡稱GDPR）自2016年4月通過、 2018 年5月施行以來，已成為全球個資保護的新標竿。我國近年積極修訂《個人資料保護法》（以下簡稱個資法）及其子法，核心目標除回應並遵循我國憲法法庭111年憲判字第13 號判決，並強化對個資的保護及監管外，更是為了爭取歐盟的「適足性認定」（Adequacy Decision），讓台灣企業經營者能更順暢地參與歐盟乃至全球的供應鏈。

隨著「個人資料保護委員會」（以下簡稱個資會）籌備處陸續公告《個資法施行細則》修正草案及多項關鍵子法草案，台灣的個資法規體系逐漸完備。在近期公布的相關子法草案中，也可以發現 GDPR 的影響。例如：個資會籌備處最新公告的《個人資料檔案安全維護管理辦法》草案，就個人資料的安全維護建立一致性的基礎標準等。雖於陸續公告之修法總說明或修正對照表中，不一定有明言某處規範之修正係回應GDPR，惟相關脈絡仍然有跡可循。本文擬自我國個資法及相關子法修正案的對比出發，分析與GDPR間千絲萬縷的關係。

尋求「適足性認定」與資料的合法化國際傳輸

依GDPR規定，在任何情況下，向第三國或國際組織之個人資料移轉僅得於完全遵循本規則之前提下執行，唯有當控管者或處理者已遵守本規則所定關於個人資料移轉至第三國或國際組織之規範，且受本規則所定其他條款之拘束時，個人資料之移轉始得為之。第三國應確保有效而獨立之資料保護監督機制（effective independent data protection supervision）、對人權、法治與自由之基本尊重，且應提供資料主體（當事人）有效且可實現的權利，以及有效的行政與司法救濟途逕。評估第三國個人資料保護程度是否充足時，應考量是否具有一個（或以上）獨立監管機關之存在並有效運作。

2016 年美國與歐盟所簽訂的「隱私盾（Privacy Shield）協議」被歐盟法院（Court of Justice of the European Union）認為，其不足以彌補兩者之間在個人資料保護的落差，其中歐盟法院對於適足性的認定標準在於「本質上的相當（essentially equivalent）」，其意義並非要求申請國對於個人資料的保護要與歐盟一模一樣（identical）。而係要求「基本原則」、「體制設計」與「規範的具體執行」必須符合而言。

GDPR明定歐盟執委會為適當程度保護之評估時，必須特別考量下列因素，包括：1. 相關法規的完備程度，包括共通性與針對特定產業所為之立法；2. 至少有一個獨立監督管理機關，其具有適當的執法權力，以負責確保個人資料保護法規的落實、協助資料主體行使其權利並提供相關諮詢、並負責與歐盟會員國之主管機關進行合作；以及3. 締結或宣示關於個人資料保護之國際承諾等。

早期日本亦如我國修法前，採取分散監督管理之模式，除修訂相關法律（「個人情報の保護に関する法律」），於平成28（2016）年設立獨立專責機關（「個人情報保護委員會」，直屬內閣總理大臣），並已於平成31（2019）年1月通過歐盟驗證取得前揭「適足性認定」，得與歐盟地區相互進行個人資料之國際傳輸。

我國原先非公務機關的跨境傳輸限制，係由各中央目的事業主管機關分別決定，本次修正原則改由個資會統一行使，必要時得會商目的事業主管機關決定之。對非公務機關國際傳輸限制權限集中由獨立的監督管理機關決定，以此新制與歐盟洽商適足性認定，經其認定我國對於個人資料之保護係與其程度相當，則我國企業於將個人資料從歐盟境內傳輸至我國境內時，所必須支付的「總體法令遵循成本」相較於其他情形明顯較低，反之亦然。

諸如為彌補對資料保護之欠缺，包括利用有拘束力之企業守則（BCR， Binding Corporate Rules）、標準資料保護條款（SCC， Standard Contractual Clauses）或由監管機關授權並認可之標準契約條款、遵循行業共同之行為守則、取得認證機制（certification）或資料保護標章（Data Protection Seals and Marks）等方式，法令遵循成本（compliance costs）極高，而收效甚微。

從分散式監理到監管一元化的「獨立機關」

GDPR規定各會員國應設置至少一獨立監管機關（independent supervisory authorities），職司個人資訊隱私權之保障。各國依上開規定，多於聯邦或國家層級設置個資監管機關（Data Protection Agency或Data Protection Authority，DPA），例如法國「國家資訊與自由委員會（Commission Nationale de l'Informatique et des Libertés，CNIL）」；英國「資訊專員辦公室（Information Commissioner's Office，ICO）」等。

GDPR要求設立的個人資料保護獨立監督機關，任務包括：法規政策的制定、提升公民意識與教育、對國內以及其他國家間的協調等，同時其應擁有調查、矯正、行為指引等權力，並且得以司法作為救濟前述行為的手段。所謂「獨立」，指的是依據法律獨立行使職權、自主運作的法定地位，不受其他政府機關指揮監督，其作成之決定，除法律另有規定或司法權介入行使外，不被直接或間接影響其效力而言。

個資法自1995年制定以來，並未明定主管機關，公務機關採自律管理，於行政體系指揮監督相關業務。非公務機關則分散由各目的事業主管機關或地方政府監管所轄事業之個人資料保護事項。故公、私部門在執行個資保護的認知、措施與強度等容有不同，影響整體法制成效。GDPR 的核心要求之一是各國必須設立具備獨立地位的監督機關。我國過去採取「分散式管理」，由各目的事業主管機關各自監督、管理所屬非公務機關，導致執法標準不一且缺乏專業統籌。

我國憲法法庭於2022年8 月12 日針對「全民健康保險資料庫」一案作成民國111年憲判字第13號判決，強調資訊隱私權保障，亦應隨科技發展採行確保資料正確與安全的措施，並設置「組織上」與「程序上」的必要防護。其中，獨立的個資保護監督機制最為關鍵，其本身就代表了「組織」上的必要機制。憲法法庭判決認為由現行個資法或其他相關法律規定整體觀察，「欠缺獨立監督機制，對人民資訊隱私權之保障不足」，有違憲疑慮，要求相關機關制定或修正法律建立制度，以完善《憲法》第22 條保障人民資訊隱私權之意旨。

首先，2023 年5 月 16 日立法院三讀通過行政院提案的個資法修正案，總統於同年 5月31 日公布，新增第1 條之1，明定設置「個人資料保護委員會」為個資法主管機關，確立由獨立監督機關統籌個資保護工作；同年12 月5 日行政院成立「個資會籌備處」。隨後由個資會籌備處提經行政院院會通過之個資法修正案，於 2025 年10 月17 日經立法院三讀通過，並經總統於同年11 月11 日公布，新法施行日期則尚待行政院以命令定之，俗稱「日出」條款。

根據前揭個資法修正案，及個資會最新公告的《個人資料保護委員會組織法》草案，我國已正式確立設置個資會，其性質為中央三級獨立機關。另外在已預告的《個資法施行細則》草案中，原屬各部會的職權正逐步整合至個資會。這一轉變象徵我國個資監管體系將告別前述「球員兼裁判」的分散模式，進而轉向符合國際標準及我國《憲法》所要求的，具備專責化、獨立性的監督管理機制，未來的行政檢查與處分將更具專業化，裁罰標準也可望漸趨於一致。

從一次到位的想像，到設計逐年逐步推進的「協力機制」

鑒於個資法之「普通法」屬性，適用對象廣泛，且個資會初期各方面之資源有限，職務量能尚難以立即、有效及於全體公務機關及非公務機關之現實，本次修法採兩階段納管策

略。第一階段優先將原本全然缺乏外部監督機制的公務機關、以及目前尚無明確目的事業主管機關的非公務機關，優先由個資會進行全面監管；第二階段則對原由明確目的事業主管機關監管的非公務機關，設定過渡條款，初期維持現況，並逐步將各該機關之監管權限移轉予個資會，最終達成「個資保護監督一元化」目標。

非公務機關蒐集、處理、利用個人資料之活動態樣繁多、且整體數量龐大，並考量個資會成立初期人力與資源有限，設計為期六年的過渡機制。個資會報請行政院公告一定範圍之非公務機關，由原中央或地方目的事業主管機關暫依相關規定監管。過渡期內，個資會每兩年會商相關機關檢討公告範圍，並逐步減列。隨過渡期推進，各目的事業主管機關之監管權限將逐步移轉個資會，最終達成「監管一元化」之目標。

徵諸GDPR及國際趨勢，個資保護專責機關實質上是集「適用」、「解釋」、「監督」、「糾正」、「協調」、「檢查」、「裁罰」、「申訴」、「建議」、「宣導」等全方位、多元綜合功能之獨立機關。以我國多起重大個資外洩案件為例，主管機關除在案發前施以「監督」、「糾正」、「檢查」，案發後「適用」相關法律規範予以「裁罰」之外，必須多管齊下，持續提高對社會大眾的「宣導」，進一步提供受害者相關協助案件的調查、釐清事實，接受其有關的「申訴」，後續與相關機關進行「協調」，提出改善「建議」等等，方有所成。

個資保護在執行層面上由專責機關逐步統一事權，無論「事前」行政檢查的實施、個資侵害防護措施與能力的提升；「事中」精進個案通報與監督程序；「事後」執法的落實與強化等措施；「平時」對於個資保護觀念的推行、教育與宣導、及個資保護意識的喚醒（awareness raising）等等，在在需要專責機關加以推動，並專注有效解決個資保護的各種爭議問題，衡平「個資保護」及「合理利用」兩大公益目的，堪稱個資保護的「基礎建設」（infrastructure）。

更透明化的「通知義務」與「通報義務」

個人資料之蒐集、處理、利用通常發生在當事人實際能夠控制的範圍之外，其本質即易於被侵害，諸如所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等情形，統稱「個資事故」（data breach）。若資料之控管者或處理者刻意隱匿事故的發生，當事人則無從得知其個資被侵害，而無從及時彌補或防止損害繼續擴大，對當事人權益形成危害。另一方面，有監督管理權限的主管機關如未獲得通報，則無法及時獲悉，並按其影響程度進行適切之調查及協助，除影響監理效能外，亦可能導致事故機關之忽視及怠於處理，僅能在事後進行裁罰，而無法從源頭降低個資事件的負面影響，顯然不利我國個人資料保護之落實。因此使主管機關得以儘先獲悉事件之發生，並採取必要之監督管理作為，具有高度之公益性與規制性，為GDPR資訊透明（transparent information）原則及我國《憲法》保障人民「資訊隱私權」的體現。

個資法修正前原已有之「通知當事人」義務規定維持，但刪除「違反本法規定」及「查明後」之前提，使其適用之範圍更為明確、監管密度更提昇。簡言之，於事故發生後，即應依法定之內容、方式、時限，通知受影響者。此舉可使當事人得及早知悉事故，並自行評估其權益受損之程度，即時進行補救，而無須待確認「是否已違法」或資料蒐集（處理、利用）者「是否已查明」，使可能受影響之當事人得以知悉及應變之時間點提前。

近期個資會預告的《個人資料事故通知通報及應變辦法》草案，參考 GDPR 之規定，將通報主管機關與應變的相關義務載明於個資法中，明定非公務機關在知悉發生個資事故後，必須於 72 小時內以適當方式個別通知當事人；另於個資事故涉及特種個資、所保有或受影響之個人資料達一定筆數以上者，應於 72 小時內向主管機關完成通報。對當事人之通知於符合特定情形時，得斟酌技術之可行性及隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之，以確保當事人受到通知。此舉大幅限縮了危機處理緩衝期，要求資料控管者及處理者建立更即時的內部偵測機制，誠為當事人權益保障之關鍵。

個資事故發生後，首先應視事故規模、態樣及可能之影響範圍，依蒐集、處理、利用資料的目的與範圍進行分析調查，確認個資侵害的態樣，研判本次侵害的影響程度與風險高低後，採行適當之應變機制或措施，避免損害擴大，據以通報監管機關及通知受影響之當事人，並留存相關紀錄。公務機關須同步通報上級、監督機關或法定機關；非公務機關則於通報後，由個資會轉知其目的事業主管機關，以兼顧效率與資訊之完整性。

有關違反通知義務或通報義務之責任部分，分述如下：

- 違反通知義務（包含「通知內容」、「通知方式」及「應變措施」）採「先令限期改正，如逾期尚未改正，再予處罰」模式。
- 違反通報義務（除前述內容、方式、時限、措施外，尚包括「紀錄保存」）則採「如有違反，得直接處罰，並同時責令限期改正」模式。

通報義務攸關風險控管與主管機關即時反應可能性，而通知義務則著重當事人及時獲悉個人資料事故之發生，以自主維護其權益，兩者立法目的不同，因此採差異化規範，逐步強化對主管機關與當事人的通報與通知義務，提高資訊透明度，縮短應變時間。

在執行的細節上，GDPR有較多細緻的設計可資參考，如：受個資事故影響的當事人為複數的情形，原則上仍應個別通知，除非個別通知涉及不符比例的勞費（disproportionate effort）。通知內容應清楚、透明，使用平易清晰之用語，並應單獨遞送，不得與其他例行性的帳單、廣告、或動態等合併提供。

從明定「去識別化」定義，到更具體化的「安全維護義務」

GDPR於前言及本文中均強調對於個人資料應用「假名化（pseudonymisation）技術」，可有效降低風險，並可協助資料控管者及處理者履行其保護個人資料之義務。「假名

化」係指個人資料經適當處理後，在不使用額外資訊時，不再得以識別特定當事人，且該額外資料已被分開存放，並以技術上及組織上的（technical and organisational）措施，確保該個人資料無法或不再可識別特定當事人。

我國個資法雖未使用「假名化」一辭，概念上仍得透過解釋我國個資法第2 條第4 款規定「編輯」之處理行為，包含「假名化」，如運用各種技術予以去識別化，而依其呈現方式，仍保有額外資訊得間接識別該特定個人者（參照法務部105 年 8 月 4 日法律字第10503510730 號函意旨）。

在 2026 年 1 月預告的《個資法施行細則》草案中，針對「無從識別特定當事人」的定義進行了重大修正。草案第 17 條參酌憲法法庭 111 年憲判字第 13 號判決（健保資料庫案），明定係指「運用當時可用之技術方法，已無法直接辨識特定自然人」。此處的「當時可用之技術方法」為不確定概念，可參照酌採前述GDPR有關「假名化」、或稱「去識別化」（de-identification）的技術上安全維護措施之內涵。

《個資法施行細則》這次修正明確了過往對「匿名化」與「去識別化」定義的模糊地帶，「匿名資料」不適用規則保護，明確化技術定義則有助於研發與大數據（巨量資料）的應用，但也提醒我們：資訊安全與個人資料保護管理之間，權益保障核心雖有所差異，但安全保障之整體組織及技術層面仍有相當交集。資料保護是一場動態的技術賽跑，現有的去識別化技術若隨科技進步而變得可還原，仍可能重新落入個資法規範的規制之內。

過去我國各不同產業的「安全維護辦法」內容差異頗大，造成跨產業經營企業的困擾。除《個人資料檔案安全維護管理辦法》草案所定人員、設備及場域等安全管理及稽核機制之外，可採用的相關安全維護機制尚有：

- 定期稽核與技術防護： 要求具備一定規模的業者，或處理敏感或大量個資的業者，必須落實加密、匿名化，並定期進行參照GDPR的資料保護影響評估（DPIA， Data Protection Impact Assessment）。
- 導入「隱私設計」（Privacy by Design and by Default）： 在新產品或服務開發初期，即納入近似GDPR的遵循評估程序，避免事後高昂的修改成本。
- 檢視資料相關委外處理契約條款： 重新檢視委託者與受託者間的個資安全責任歸屬，並以契約條款予以明確化。例如個資事故發生時，受託者應於知悉時立即通知事故機關，並保存通知紀錄。

從「指定專人」到設置「個資保護長」

無人則不足以成事，公務機關或一定規模之非公務機關應有具備個人資料保護專業之成員，或具備此等輔助機能之組織角色，始足以因應個人資料保護所涉廣泛性、高度變化性的實務運作問題。對於規模較大、所保有之個資檔案數量較多、職務或業務複雜度高、及所屬監管對象或分支機構繁多者，尤然。

個資法第18條要求公務機關應指定「專人」辦理安全維護事項及個人資料檔案安全維護事項，其設置目的旨在辦理安全維護計

畫、提供諮詢，與個資保護長（DPO， data protection officer）負責「監督資料控制者或資料處理者之法規遵循」，有功能上與性質上的差異。

換言之，公務機關治理由「被動保管責任」轉向「主動治理責任」，建立持續改進的管理模式。公務機關須由首長指派一定職級以上之適當人員兼任個資長，配置適當人力及資源，並接受相關訓練或取得證照、證書。個資長統籌督導本機關與所屬或所監督公務機關落實個資保護，為內部監理核心。

對非公務機關而言，雖現階段尚未強制設置個資長，但監管權限逐步整合後，民間對個資保護作業之法遵要求勢必提升，尤其採取事前法遵檢查等措施，促使企業主動檢視並導入預防性個資保護機制（如「隱私保護始於設計」等），以降低違規受罰的風險。

值得一提的是，GDPR對於個資保護長的職責、功能與獨立性有明確的規範，堪為我國法制設計上參考，諸如：個資保護長應有權直接向最高管理階層報告；確保其得以適當、且及時的，涉入所有有關個人資料保護之相關業務，並免於因執行職務而被解任、或處罰。

從象徵性處罰，到具嚇阻力的裁罰，再到事前的預防檢查

GDPR 施行之初最令全球企業敬畏驚懼的，不外乎是其高達全球年營業額 4% 或 2，000 萬歐元的罰鍰。我國 2023 年修正個資法第 48 條，將非公務機關未盡安全維護義務且情節重大者，罰鍰上限由 20 萬元大幅調升至 1，500 萬元，並得按次連續處罰，加重個人資料蒐集者或持有者之責任，促使其重視並加強投入成本、技術及人力及合理資源之分配，以遵守個資安全維護義務，維護個人資料檔案之安全。

這種「重罰＋強制執行」的組合，與 GDPR 的裁罰與透明化邏輯，促使將隱私風險視為一種財務風險。若違法成本遠低於合規成本，法規將形同虛設。這股「重罰化」的趨勢，參照並回應了 GDPR 的懲罰性邏輯，使資料控管者及處理者與利用者，不得不將個資防護納入核心的經營策略考量內容。

此外個資會認為非公務機關雖尚無疑似違法情事，但「有違反個資法之虞」或「為檢視其落實本法情形而認有必要」時，得進行行政檢查，包括：「通知陳述意見」、「要求提供資料」，以及「實地檢查」等等，必要時得與目的事業主管機關之其他檢查一併行使。個資會得扣留或複製資料，必要時以最小損害方式強制為之，非公務機關無正當理由不得規避、妨礙或拒絕。檢查時並得引進外界資訊、電信、法律等專業人員協助，必要時亦可請目的事業主管機關或地方政府協助。另考量非公務機關對個人資料之蒐集、處理、利用及管理，依其業務性質、營運模式或科技運用而有相當差異，發生事故風險之高低及影響程度亦不一，前揭檢查除針對已有違法跡證者外，應建立差異化管理機制，妥適決定發動檢查之對象、次序及頻率，以符比例原則。

基於「有權利、必有救濟」之法理，不服個資會行政處分者，與其他獨立機關一致，得直接向高等行政法院提起行政訴訟。過渡期間並設計雙軌救濟管道，亦即原處分機關為「部會或地方政府」時，向個資會提起訴願；如原處分機關為獨立機關（個資會）時，則免經訴願程序，得逕提起行政訴訟，以符獨立機關特性。透過訴願案件之受理，由個資會對於目的事業主管機關就具體個案之處分或決定進行適法性及妥適性審查 ，以構築實質有效之獨立監督機制。

結語

我國目前的修法方向走在接軌國際趨勢的路上。然而，法規的生命在於落實執行，未來「個資會」正式成立，並逐年完成主管權限事務的整合後，能否如同歐盟各監督機關般，展現應有的「韌性」與「獨立性」，並在「保護隱私」與「促進資料運用」兩者間取得動態平衡，將是我國資料治理（Data Governance）與數位轉型成敗的關鍵。不應將更嚴格的制度視為監管的壓力與成本，而應藉此契機轉化為進入國際市場的競爭優勢，加速建立與歐盟、與世界對等且可信賴的法制架構。

而就我國個資法修正尚未觸及之「資料可攜權（data portability）」、「自動化數位剖析（profiling）許可權」、「個人資料對於蒐集或處理目的不再需要者之刪除權（被遺忘權）」等其他諸多修法議題，當由正式成立之個資會以本法主管機關之地位，賡續進行通盤修正研議及立法政策決定，仍有機會納入整體個資保護法制中予以明確規範。

參考文獻：

1. 李世德，<GDPR與我國個人資料保護法之比較分析>，《台灣經濟論衡》，16卷3期，2018年9月。
2. 李世德，<個資法上路前關鍵解讀>，《台灣經濟論衡》，23卷4期，2025年12月。
3. 廖淑君，<論我國因應GDPR施行之措施——以個人資料之跨境傳輸為核心議題>，商業法律與財金期刊，3卷1期，2020年12月。