政策焦點

FOCUS

歐盟GDPR簡介與我國政府因應推動方向

國家發展委員會

壹、前言

數位經濟時代下，大數據流通與資源分享已是不可逆的趨勢，如何讓個人資料的運用發揮價值，並兼顧隱私保護，便成為重要的課題。歐盟為了讓個人資料的保護規範因應時代變遷，並建立一體適用的管理規範，在2016 年通過一般資料保護規則（General Data Protection Regulation, GDPR），並於今（2018）年 5 月 25 日全面施行，GDPR 建立了一套嚴格的個人資料保護法制架構，適用範圍更可能擴及歐盟境外的企業，因此引起各國的高度關注。

本次 GDPR 規範重點包括擴大適用範圍、加重企業責任、強化當事人權利及提高罰則金額等部分；另於個人資料國際傳輸係採取「原則禁止、例外允許」模式，

因此只有在符合 GDPR 規範的例外情形下，個人資料才能進行國際傳輸。鑑於臺歐雙邊經貿往來向來密切，GDPR 的施行勢必將廣泛影響我國在歐盟營運或對歐從事業務的企業，政府對此當積極推動相關措施，以協助企業因應 GDPR 的衝擊與影響。本文以下將簡介 GDPR 重點規範，並就政府因應措施及推動方向進行相關說明。

貳、歐盟GDPR簡介

歐盟 1995 年發布「個人資料保護指令」（Data Protection Directive）係對於個人資料保護的最低限度規範，歐盟各會員國尚須以該指令為基礎並進一步內國法化，以建立各會員國的個人資料保護法制，惟各國內國法化後可能產

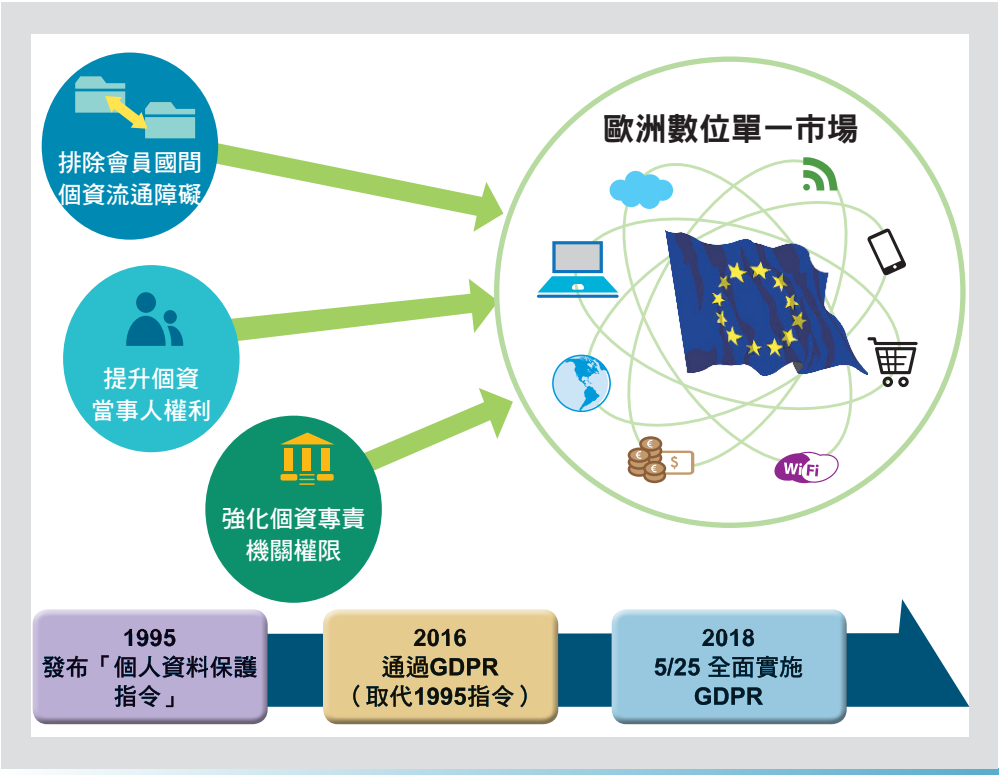

圖 1　一般資料保護規則（GDPR）背景說明

生規範上的落差，進而形成不利資料流通、阻礙經濟活動或造成不當競爭等負面影響。因此，歐盟於推動與建構數位單一市場之際，於 2016 年通過一般資料保護規則（General Data Protection Regulation, GDPR），在規範位階上將原有的「指令」（Directive）提升為「規則」（Regulation），這意味著各會員國縱使不透過內國法化的程序，仍可一體適用 GDPR 的規範，易言之，不論歐盟會員國是否將 GDPR 規定轉換成內國法，個資當事人都可以直接援引 GDPR 規定作為個資保護的主張。GDPR 經過 2 年過渡期後，已於今（2018）年 5 月 25 日全面施行，歐盟欲透過 GDPR 的實施，以達成排除會員國間個人資料流通障礙、提升個資當事人權利並強化個資專責機關權限等願景。

GDPR 重點規範說明如下：

一、擴大適用範圍

在適用範圍上，無論個資控管者（data controller）或受託處理者[1]（data processor），只要符合下列三種情形之一且處理個人資料，就須受 GDPR 的規範：

(一) 在歐盟境內[2]設立據點，且無論處理個資的行為是否發生在歐盟境內；或

[1] 我國個人資料保護法將個資的使用區分為蒐集、處理及利用等行為態樣，而 GDPR 則統稱為「processing」，本文於此統一使用「處理」的用語，其定義可觀諸 GDPR 第 4 條第 2 項規定「不論是否透過自動化方式，對個人資料或個人資料檔案執行任何操作或系列操作，例如蒐集、記錄、組織、結構化、儲存、改編或變更、檢索、查閱、使用、傳輸揭露、傳播或以其他方式使之得以調整或組合、限制、刪除或銷毀」。

[2] GDPR 適用範圍為歐洲經濟區 (European Economic Area)，因此除歐盟成員國外，尚包含冰島、列支敦斯登及挪威。

(二) 在歐盟境內未設立據點，但對歐盟境內當事人提供商品或服務；或

(三) 在歐盟境內未設立據點，但監控歐盟境內當事人於歐盟內的行為。

二、擴大個人資料定義

個人資料可區分為「一般個人資料」與「特種個人資料」。一般個人資料是指「有關識別或可得識別個資當事人的任何資訊」，而所謂「可得識別個資當事人」是指得以直接或間接地識別該個資當事人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該當事人的身體、生理、基因、心理、經濟、文化或社會地位等具體因素等。另在 GDPR 立法前言（Recital）更說明包含透過網路 IP 位址、瀏覽紀錄產生的數位軌跡並得追蹤識別特定當事人身分等皆屬之；特種個人資料是指「揭露人種、血統、政治意見、宗教、哲學信仰、工會身分、基因、生物特徵、健康相關、性生活與性傾向等資料」，且原則上禁止處理。

三、明確當事人同意

倘透過個資當事人同意而取得個人資料者，該「同意」必須是由個資當事人自由提供、具體、知情及明確同意，而單純沉默、預設選項為同意或當事人不為表示的情形，皆不該當為同意；且若個人資料的處理具有多重目的，應就全部目的取得同意。另應注意在個資當事人撤回同意方面，須提供如同給予同意一樣容易的方式使其撤回同意。

四、加重企業責任

(一) 書面委託歐盟境內代表

非設立於歐盟境內，但對於歐盟境內當事人提供商品或服務或監控其行

為者，除偶然性的處理或公務機關外，均應以書面委託歐盟境內的代理人作為代表，受理主管機關或個資當事人提出的要求。

(二) 個人資料保護設計及預設

應考量現有技術、執行成本及處理個人資料行為的性質、範圍、內容、目的及對當事人權益所生的不同風險等，在技術上及組織上納入隱私保護措施，以確保個人資料處理符合 GDPR 要求並保護個資當事人的權利。

(三) 個人資料侵害事故通報與通知

發生個人資料侵害事故，應於知悉後 72 小時內通報當地個人資料主管機關；若對個資當事人的權益有重大危害之虞，亦應通知該當事人。

(四) 個人資料保護影響評估

個人資料處理可能造成個資當事人高度風險者，應於處理前執行個人資料保護影響評估，尤其是大規模的個人特質評估、處理特殊類型或犯罪個人資料、監控公共領域者。

(五) 指定個人資料保護長

公務機關處理個人資料、或處理個人資料之核心業務涉及大規模監控個資當事人、或大規模處理特種個人資料與犯罪個人資料的情形，應指定個人資料保護長。因此企業是否應設置個人資料保護長，並非依據企業的規模大小，而是應視企業本身所涉及的業務而定。

(六) 紀錄個資處理責任

員工人數在 250 人以上的企業或組織，應負責維護資料處理活動之紀錄，惟員工人數低於 250 人的企業或組織，如係經常性處理個人資料或涉及處理特種或犯罪個人資料者，仍有該責任的適用。

五、強化當事人權利

(一) 拒絕權

倘處理個人資料的依據為「基於公共利益」或「基於正當利益」時，個資當事人有權依具體情形，隨時拒絕該等個人資料之處理，包含對個資當事人進行剖析（profiling）的行為。另倘係為直接行銷之目的而處理個人資料時，該個資當事人有權隨時拒絕為行銷而處理其個人資料，包括拒絕與該直接行銷有關範圍內的剖析行為。

(二) 更正權

個資當事人有權請求資料控管者即時更正不正確的個人資料，且慮及個人資料處理之目的，個資當事人有權請求補充其有欠缺的個人資料。

(三) 刪除權（被遺忘權）

在符合特定情形[3]下，個資當事人有權請求，且資料控管者亦有義務即時刪除個人資料或連結。

(四) 個人資料可攜權

在符合特定情形[4]下，個資當事人有權要求以「結構的」、「普遍使用的」、「機器可讀的」形式，接收其原提供予個資控管者的個人資料，並有權傳輸予其他控管者。

[3] 包括 (1) 對於原本蒐集或處理個人資料之目的已無必要、(2) 個資當事人撤回同意，且無其他法律依據、(3) 個資當事人依 GDPR 規定對處理個人資料行為表示反對、(4) 個人資料遭違法處理、(5) 個資控管者依法律規定有義務刪除個人資料、(6) 個資控管者對兒少提供資訊社會服務等情形。

[4] 包括 (1) 個資控管者處理個人資料的法律依據為「當事人同意」或「與當事人有契約關係」、(2) 個資控管者以自動化方式處理個人資料等情形。

六、個人資料國際傳輸

採取「原則禁止、例外允許」的模式，亦即只有符合例外規定的情形，始得進行個人資料的國際傳輸。而例外情形包括：

(一) 國家或地區取得適足性認定（adequacy decision）；或

(二) 企業自主採行符合規範的適當保護措施，例如：標準個人資料保護契約條款（Standard Contractual Clauses, SCC）、拘束性企業規則（Binding Corporate Rules, BCR）、行為守則（Codes of Conduct, CoC）、取得特定認證（Certification）等方式；或

(三) 符合其他例外情形，例如：

1. 告知個資當事人可能的風險後，取得當事人明確同意；

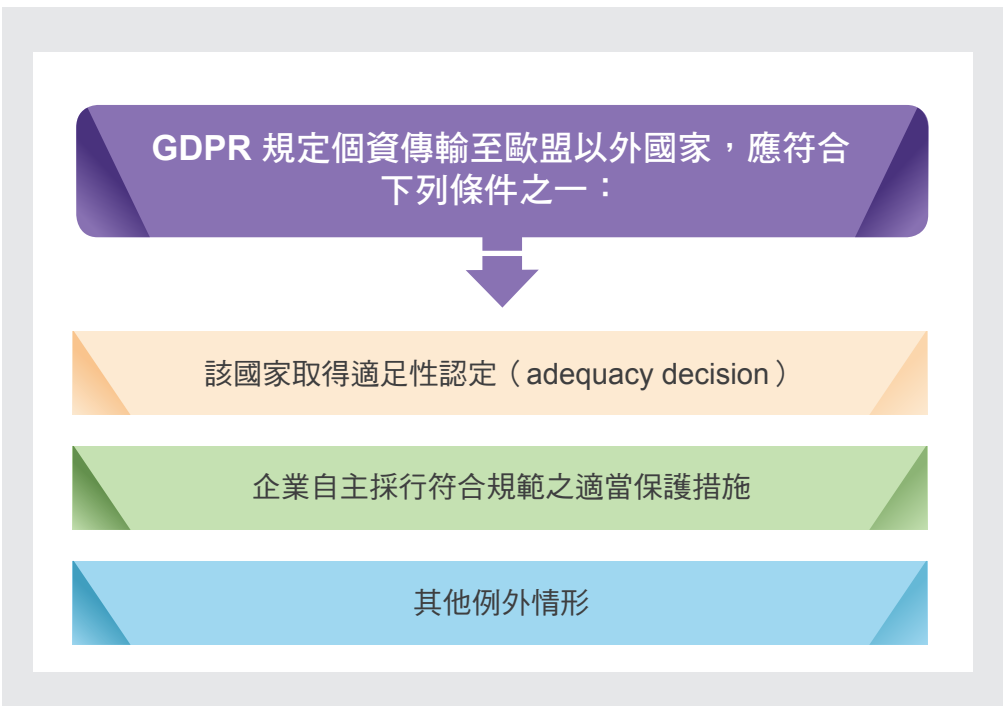

圖 2　例外允許國際傳輸之情形

2. 因執行契約所必要；

3. 基於公共利益的重要原因；

4. 個資當事人無法為同意的表示，但移轉該個人資料對保護其重要利益實屬必要等情形；

惟應注意的是，上述其他例外允許國際傳輸的情形，適用前提為少量、偶發性的國際傳輸事件。

七、提高罰則金額

依不同的違法行為區分，最高可處以 1,000 萬歐元或（如為企業）全球營業總額 2%的行政罰鍰；或最高 2,000 萬歐元或（如為企業）全球營業總額 4%之行政罰鍰。

叁、我國政府因應推動方向

歐盟為我國第一大外資來源與第五大貿易夥伴，臺歐雙邊經貿往來向來密切，GDPR 的施行勢必將廣泛影響我國在歐盟營運或對歐從事業務的企業，面對 GDPR 的施行，我國當不能置身事外；而歐盟的個人資料保護法規向為各國個人資料保護法之立法典範，我國《個人資料保護法》（以下簡稱《個資法》）歷次修法亦多有參照其規範，對此，政府除持續關注 GDPR 的規定及後續施行概況外，於 GDPR 因應措施及推動方向，更應積極整合各部會辦理相關事宜。

國家發展委員會（下稱國發會）已透過成立個人資料保護專案辦公室、辦理與歐盟洽談適足性認定事宜、官網設置 GDPR 專區，並舉辦 GDPR 研討

會及多場宣導說明會等措施，以協助公、私部門因應 GDPR 可能帶來的衝擊與影響。分述如下：

一、成立「個人資料保護專案辦公室」

由於我國個人資料保護體系在監督機制上未設單一主管機關，而係採分散式管理，由非公務機關所屬之中央目的事業主管機關或直轄市、縣（市）政府為監督機關，因此面對 GDPR 全面施行，我國亟需一單位作為部會間協調整合的平臺，以統籌辦理相關因應事宜。國發會奉行政院指示，於今（107）年 7 月 4 日正式成立「個人資料保護專案辦公室」（以下簡稱個資辦公室），並自今年 7 月 25 日起，我國《個資法》的法律主政機關由法務部移交國發會職掌，一方面積極整合各部會辦理因應 GDPR 相關事宜，並向歐盟申請適足性認定，另方面協調整合並加強各部會落實執行《個資法》的一致性。未來個資辦公室亦將視歐盟國際傳輸適足性認定諮商進程，持續研議個人資料保護相關因應對策。

二、辦理與歐盟洽談適足性認定事宜

為協助我國企業與歐盟間得以自由進行個人資料國際傳輸，國發會陳主委已於今年 5 月底率團拜訪歐盟，正式表達我方申請適足性認定的意願，國發會隨即展開適足性認定的準備工作。目前個資辦公室刻依歐盟建議，參照 GDPR 規定、歐盟適足性認定參考文件[5]與歐盟法院判決[6]等資料，撰擬我國個人資料保護整體架構之自我評估報告，並召開多次專家諮詢會議討論適足性評估工作，以期後續與歐盟順利展開技術性對話，進而取得歐盟認可我國對個人資料保護具適足程度。

---

[5] Article 29 Working Party，Adequacy Referential，WP 254 rev.01

[6] 歐盟法院 SCHREMS 案判決。

三、官網設置GDPR專區

國發會已於官網設置 GDPR 專區（圖 3），提供 GDPR 簡介、導讀、法規翻譯、歐洲資料保護委員會（EDPB）採認之 GDPR 相關解釋文件、GDPR 與我國《個資法》重點比較分析以及相關部會諮詢窗口等，並將適時更新文件，以提供各界參考運用。

圖 3　國發會官網設置 GDPR 專區

四、舉辦GDPR研討會及多場宣導說明會

為提升公、私部門對於 GDPR 的瞭解，國發會於今年 8 月舉辦中央及地方機關之 GDPR 研討會，並於 9 月舉辦北、中、南區 GDPR 企業宣導說明會，邀請相關部會分享 GDPR 因應作為以及專家學者進行專題演講，分別就政府面與產業面說明 GDPR 因應及調適方向，並透過綜合座談釐清各界對 GDPR 的相關疑義。

肆、結語

隨著數位經濟的科技發展以及全球化的影響，人類的生活步調逐漸發生變化，尤其是網際網路的普及、快速的資訊傳輸與大數據運用，為生活帶來許多便利，同時也產生相應的風險與挑戰，其中隱私權與個人資料的保護，儼然成為國際上面臨的重要議題。而當企業面對號稱史上最嚴格的 GDPR，或許擔心違反 GDPR 可能被處高額罰鍰、亦或害怕未遵守 GDPR 可能對其商譽造成影響，政府宜積極協助與輔導企業瞭解與掌握 GDPR，以有所因應，除整體落實個人資料的保護外，並避免造成不必要的恐慌。

有鑑於此，在政府協助企業因應 GDPR 方面，除有賴各中央目的事業主管機關就其所轄產業提供相關輔導與諮詢外，同時為補足我國目前個資保護採取的分散式管理機制所缺乏的協調與整合功能，政府亦已成立「個人資料保護專案辦公室」，以統籌各部會辦理 GDPR 因應相關事宜，並將持續與歐盟洽談國際傳輸適足性認定，未來亦配合推展進程適時檢討我國《個資法》。