編號：499

議題研析

一、 議題：歐盟資料保護一般規則對我國個人資料保護法制及跨境經營商務（臺商）之影響研析

二、 所涉法律

個人資料保護法

三、 探討研析

（一） 歐盟個人資料保護法制發展簡介

歐洲傳統上極為重視個人隱私保護，歐洲議會及歐盟理事會 1995 年制定之「資料保護指令（Data Protection Directive)，於施行逾廿載後的 2016 年 4 月 27 日通過「歐盟資料保護一般規則(General Data Protection Regulation)」(GDPR)，並自 2018 年 5 月 25 日起施行，號稱史上最嚴格之個資法。

1995 年資料保護指令（Directive）僅係最低限度之保護規範，歐盟各會員國於該指令基礎上建立之個人資料保護制度，可能對當事人權利保護不一。而 GDPR 則屬全歐盟均可直接適用之規則(Regulation)，各會員國不需另外進行立法。惟就現行已存在保障程度不足之內國法規，必須檢視修正，以符合 GDPR 之規範，故 2016 年通過之 GDPR，給予各會員國 2 年修法緩衝期，至 2018 年始生效。GDPR 旨在提升及確保對於歐盟境內資料當事人權利保護之一致性(特別是網路活動)，並排除個人資料在歐盟境內流通之障礙。

（二） GDPR 之規範重點簡介

1. GDPR 之適用範圍(第 3 條)：不論資料管理者或資料處理者於歐盟境內是否設立分支機構,只要其在跨境提供商品或服務的過程(例如網路購物)中,有蒐集或處理歐盟居民之個人資料者，即適用 GDPR。
2. 保護客體(第 4 條)：明文規範個人資料包括位置資訊(location data)、網路識別碼(online identifier)等，亦即納入 IP 位址、GPS 定位等。
3. 當事人之權利部分：除以往之資料查詢、複製、更正及刪除權之外,更進一步賦予當事人得請求資料管理者及處理者刪除連結(第 17 條：被遺忘權，為強化網路環境之被遺忘權，將刪除權擴張至「公開個人資訊」之控管者有義務通知「刻正進行個人資料處理」之控管者刪除任何該個人資料之連結、副本或複製品)、要求以可共同操作之格式提供資料(第 20 條：資料可攜權)等權利。當事人同意必須具體、明確、受充分告知，如單純沉默、預設選項為同意，則不構成同意；個人資料之處理係以直接行銷為目的時,當事人有權在任何時間、且毋需任何費用拒絕該處理。
4. 跨境傳輸原則禁止:以保障歐盟公民個資只能在如同歐盟對隱私高度保障的地區進行利用-

(1)就歐盟境內之個人資料原則禁止跨境傳輸至歐盟以外之地區或國家。例外須符合下列情形之一者，方得為之： A.擬傳輸地區經評估具備「適當保護水平」(第 45 條) ；B.資料管理者已提供適當保護措施 (第 46 條)；C.當事人明確同意、履行契約或依當事人要求，為締約前之必要措施、基於重要公共利益之維護、為主張、行使或防禦法律上之請求權所必要、基於保護當事人之重要利益所必要、依法辦理之登記作業，而向公眾提供資訊等(第 49 條)。

(2)評估第三國個人資料保護程度充足與否時，應考量有否獨立監管機關之存在並有效運作、已否參與或簽署關於個人資料保護之國際協定或其他具法律拘束力之契約、或參與多邊或區域體系而生之義務等。第三國資料保護程度不足時，應禁止向該第三國為資料移轉(第 45 條)。此時控管者或處理者應採取適當之保護措施以彌補第三國對資料保護之欠缺，該等措施可包括利用有拘束力之企業守則（Binding Corporate Rules，BCR)、歐盟執委會採行或核准之標準資料保護條款、由監管機關授權控管者或處理者與第三國或國際組織之個人資料控管者、處理者或接收者之契約條款等(第 46 條)。

5. 資料管理者部分

(1)新增資料保護影響評估(DPIA)、資料保護長(Data Protection Officer,DPO)等制度：

於特別使用新科技之處理方式,考量該處理之本質、範圍、使用情形及目的後，認為可能導致自然人權利及自由高度風險時，控管者應於處理前，實行該處理對於個人資料保護之影響評估(第 35 條)；下列情形，應指定具資料保護法律與實踐之專業知識的資料保護官或資料保護長：A.除法院行使司法權外，由公務機關或機構執行個人資料處理處理時；B.控管者或處理者需要定期且系統性地大規模監控（regular and systematic monitoring）資料主體時；C.大規模處理特殊類型個人資料或與前科及犯罪相關之個人資料時；或 D.歐盟或會員國相關法律有明確要求時等（第 37 條至第 39 條)。

(2)明定資料控管者負相關舉證責任：須證明當事人知悉同意之事實及範圍及須證明其已遵守個人資料處理之一般原則(目的限制原則、資料蒐集最少原則、正確性原則、完整及保密原則等)。

6. 資料外洩通報義務與提高處罰額度：

資料控管者一旦發現侵害個資事件，應於發現後 72 小時內向監管機關通報(第 33 條)，遲延通報造成資料當事人損害，應負損害賠償責任(第 82 條)。第 83 條規定，違反者，最高得處以 2 千萬歐元或該企業之前一會計年度總營收 4%之罰鍰。

（三） 我國(臺商)因應 GDPR 之困境

我國缺乏單一個資主管機關，作為統一協調的窗口，亦尚未與歐盟進行協商 GDPR 的安全適足性認定問題。

其次，各產業個資保護水準不一，金管會對金融業個資處理的要求嚴格程度，就比其他產業要求更嚴格。GDPR 罰則很高，但臺灣個資法相對寬鬆，許多企業缺乏因應 GDPR 的誘因，普遍觀望。

末者，我國對於跨國傳送個資採取原則不禁止，例外情形才限制的作法，相較於歐盟原則禁止的規定，顯得過度寬鬆，加上沒有明確的資料保護機制，使得歐盟認定，我國在個資跨境傳輸的風險較大，因而不在歐盟允許跨境傳輸的名單中。在今年 5 月 25 日 GDPR 正式實施後，國內企業想將擁有的歐盟民眾個資，進行跨境傳輸（例如轉移到其他國家，或從其他國家回傳國內）的行為，需符合 GDPR 例外允許跨國傳輸之情形，或是讓使用者自行上傳（使用者自己把資料上傳到其他國家），否則都可能違反 GDPR。

四、 建議事項

（一）適時檢討修正個人資料保護法，以與時俱進

1995 年歐盟資料保護指令為我國個人資料保護法之重要參考立法資料，而當 GDPR 高度提升個資保護之規格及嚴密度後，我國個資法法制之規範密度即呈現相當落差。

GDPR 明確賦予當事人被遺忘權、資料可攜權，並要求資料管理者於一定情形下須進行個人資料保護之影響評估，根據該評估結果採取適當之資料保護措施,及設置資料保護長等機制,另對跨境傳輸採取原則禁止之規範方式，課予資料外洩時之通報主管機關義務與提高處罰額度等規範，均為目前我國現行個資法所未及處。GDPR 諸多高規格之規定，實務如何運作，雖尚待歐盟資料保護小組持續訂定相關細節規範予以補充，但我國仍需密切觀察，適時檢討修正個人資料保護法，以與時俱進，因應所需。

(二)臺商與歐盟進行(跨境)商務活動之法遵成本提高，應預先因應

GDPR 已於今年 5 月 25 日上路，不論企業所在地是否位於歐盟,只要會蒐集、處理或利用到歐盟居民之個資(含網路識別碼),均有適用。為因應 GDPR 新法,Twitter、Apple、Google、LINE 等國際企業，早前亦陸續修改其隱私政策。今年 3 月，臉書(facebook)約 8700 萬用戶的個資,遭英國數據分析公司「劍橋分析」存取使用，執行長薩克柏出面道歉，為個資外洩事件親赴歐盟議會聽證會。微軟更耗費 1 年多時間，全部重新檢視其提供雲端服務之線上合約，以確保符合 GDPR 規範，可見影響甚鉅。

詳言之,GDPR 規範要求之當事人同意,必須是具體、明確、正面肯定及受充分告知的同意，如資料處理有多個目的，全部目的均須取得同意，而如當事人只是單純沉默，或是電子選項預設為同意，均不構成同意，故上述跨國業者方積極在 GDPR 上路前，更新其隱私權保護政策，並請當事人同意；另 GDPR 賦予當事人資料可攜權，未來網際網路資料服務業者應提供使用者可將所儲存之個人資料以通用格式存取，並提供給其他業

者之服務；此外，業者尚需支出個人資料保護之影響評估、資料保護長、跨境傳輸等法規範遵循成本，跨國臺商的法遵成本將大幅提高，應預先因應。

據報載，國發會分析，對國內金融、航空及電子商務等 3 類產業影響最大。業者處理歐盟民眾個資時，只要發生未在 72 小時內通報非法處理或外洩、未執行個資保護風險評估、未設資料保護長、違法向第三國傳輸個資等違規行為，最高可罰 2 千萬歐元（約 7 億多元台幣）或全球上一個會計年度總營收 4%之鉅額罰金，對臺商與歐盟進行(跨境)商務活動之影響不容小覷。

撰稿人：方華香