一、歐盟一般資料保護規章簡介

(一) 歐盟個人資料保護法規原為「1995 年資料保護指令」（Data Protection Directive[1]）。該指令並不直接適用於歐盟會員國，而是由會員國依據該指令之規範訂定國內法律並據以執行。該指令於 1995 年生效，為因應科技與網路之快速發展、全球化等外在環境變化，以及為消除各會員國法規差異以追求歐盟數位單一市場（Digital Single Market）目標，歐盟執委會於 2009 年開始推動修法，以強化及調和歐盟境內資料保護法規。

(二) 歐盟執委會隨後於 2012 年 1 月提出「一般資料保護規章」（General Data Protection Regulation[2]，簡稱 GDPR）草案，以取代 1995 年資料保護指令。與 1995 年資料保護指令不同的

1 Directive 95/46/EC
2 Regulation (EU) 2016/679

是，GDPR 將可直接適用歐盟全境，不須經過「轉換」成歐盟會員國國內法的程序。歐盟在 GDPR 中保留了 1995 年資料保護指令的基本架構與核心原則，但希望藉由 GDPR 改進現有個人隱私保護法律架構，達到調和並簡化境內資料保護規範以追求數位單一市場的目標、強化個人對自身資料的掌控能力、強化主管機關監理能力等目的。這些改變，一方面加強對個人隱私的保護，另一方面也讓企業更容易遵循相關法規。經過歐盟執委會、歐盟部長理事會與歐洲議會三方協商，歐盟已於 2016 年 4 月完成 GDPR 立法程序並於 5 月生效。*為讓政府及民間部門得以因應新法生效的改變，歐盟在 GDPR 中設定 2 年緩衝期，將於 2018 年 5 月 25 日起正式施行*。

(三) GDPR 主要涵蓋資料當事人的權利、資料控制者與處理者的義務、個資跨境傳輸、政府的監理體制、救濟措施等面向，內容大略包含：

1. **基本原則**：包括個資之處理對於資料當事人應合法、公平且透明；個資之蒐集應基於特定、明確且正當之目的；蒐集之個資應適當、相關且限於與目的有關者；蒐集之個資應準確、保持更新，錯誤資料應予刪除或修正；個資儲存時間不

長於為達處理目的所必須；處理方式須確保個資受適當安全保護（第 5 條）。

2. **當事人同意：**包括個資之蒐集、處理、利用須經資料當事人明確同意；以書面請求同意必須與其他事項區隔且淺顯易懂；*當事人可隨時撤銷其同意*（第 6~8 條）。

3. **當事人之權利：**包括當事人有權向資料控制者查詢、閱覽及複製其個資；當事人有權要求更正、刪除其個資；當事人有權限制其個資之處理；資料控制者有義務通知資料接收者相關更動；當事人有權將其資料自一資料控制者移轉到另一資料控制者而不受限制；當事人有權對其資料被基於公益、公權力或資料控制者合法權益目的之處理（包括自動化剖析 profiling）提出異議（第 15~21 條）。

4. **資料控制者與處理者之義務：**包括資料控制者應就資料蒐集者的資訊、蒐集資料的事由、當事人權益等資訊，以淺顯易懂、免費的方式告知當事人；資料控制者須採取相關技術與組織內部措施以確保個資處理合乎相關規範；歐盟境外資料控制者與處理者處理歐盟居民個資，應在歐盟境內指定代表人；資料控制者僅能委託能確保合乎相關規範之處理者，且

資料處理者處理資料應受合約規範；資料控制者應保留資料處理活動之紀錄；資料控制者與處理者應與主管機關合作；資料控指者與處理者應採行適當之技術（如去連結化或加密）以確保個資安全性；*若發生個資外洩事故，必須於 72 小時內通報主管機關，情節嚴重者需通知當事人*；資料控制者應進行資料保護風險影響評估；資料控制者與處理者核心業務涉及需定期、系統性、大規模監測當事人之資料處理時需設立資料保護專員；主管機管應鼓勵行為準則（code of conduct）之創設，產業協會可推出行為準則供資料控制者與處理者採行以符合 GDPR 規範；主管機關應鼓勵認證機制（certification mechanism）之創設，資料控制者與處理者可申請認證以顯示符合 GDPR 規範（第 12~14、24~43 條）。

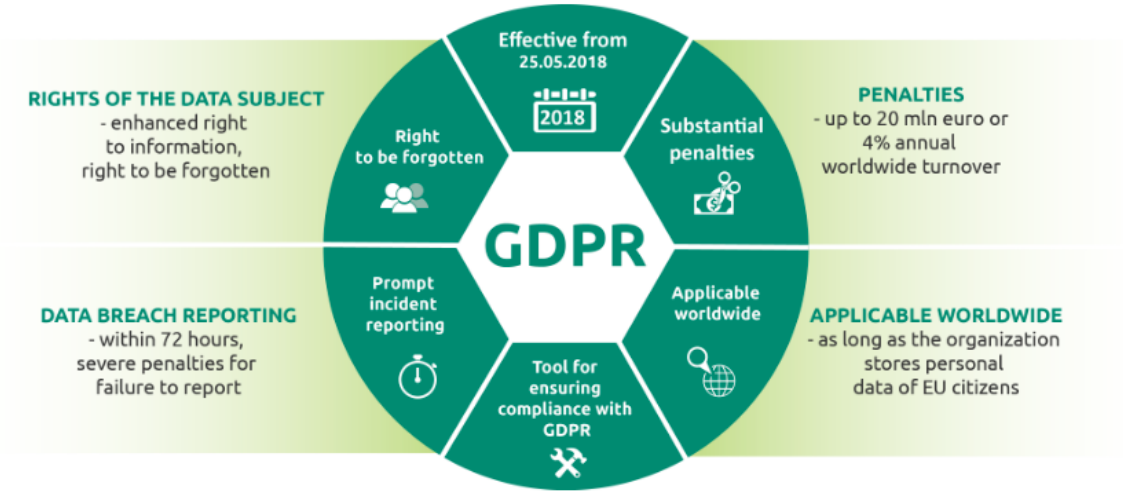
5. **跨境傳輸個資之規範**：對於歐盟居民個人資料傳輸至第三國，歐盟採有條件允許（原則禁止、例外允許），包含：(1) 由歐盟認可第三國對個資保護程度跟歐盟水準相當的適足性認定（adequacy decision）；(2) 資料控制者與處理者間簽訂歐盟執委會公布之標準資料保護條款（standard data protection clauses，或稱標準契約條款，standard contractual clauses）；

(3) 適用同一集團企業或合作進行經濟活動的不同集團內企業，且經主管機關核准的企業拘束規則（binding corporate rules）；(4) 歐盟資料控制者或處理者採行行為準則，搭配第三國之資料控制者或處理者具法律效力且可執行之承諾；(5) 歐盟資料控制者或處理者經過認證，搭配第三國之資料控制者或處理者具法律效力且可執行之承諾；(6) 部分排除適用（derogation），指的是某些情況下，雖然無法確保個資被傳輸到第三國續受完善保護，但仍可傳輸，例如當事人明確同意且已被告知相關風險情況下，可將其個資傳輸至第三國等（第 44~49 條）。

6. **政府組織與監理：**包括歐盟各會員國資料保護監理主管機關之職權與獨立性；各主管機關應協同合作以確保法規施行之一致性；歐洲資料保護委員會之設立等（第 51~76 條）。

7. **救濟措施與罰則：**當事人若認為其個資遭受侵害，可向主管機關提出控訴，若不滿主管機關處理結果，則可對主管機關決議提出司法訴訟；當事人可對資料控制者與處理者提出司法訴訟；當事人應就其損害，自資料控制者與處理者獲得補償；主管機關對於違反 GDPR 者除進行稽核即要求修正外，

可處罰鍰；對於部分違法情事如資料控制者違反其認證義務或認證機構違反其義務，最高罰鍰可達 1,000 萬歐元或其全球營業額之 2%，*另對於部分違法情事如違反個資處理基本原則、傳輸個資至第三國等，最高罰鍰可達 2,000 萬歐元或其全球營業額之 4%（第 77~84 條）*。



二、對我國企業可能影響

(一) GDPR 生效，對於在歐洲設有分公司、子公司的我國廠商，將會產生直接衝擊。不只是因為這些歐洲分支機構需要遵守 GDPR 在當事人權利及資料控制者與處理者（亦即企業）的義務之規範，這些跨國企業，不論是運輸業、金融服務業、旅遊

業、網路服務業（例如社群網路、搜尋引擎、手機應用軟體開發或營運商）、科技業（如 3C 產品製造業者），或是從事電子商務的企業，在運作上，關聯企業之間或需進行個資傳輸，在這種情況下，除了提高對個資處理的安全水準以維護商譽，更需要注意涉及個資傳輸到歐盟境外第三國的規範，例如訂定企業拘束規則，以避免遭受高額罰鍰。

(二) 然而，即使是在歐洲未設有分支機構的我國企業，也必須注意 GDPR 的相關規範。依據 GDPR 規定，只要涉及針對歐盟居民個資的蒐集、處理、利用（以歐盟市場為目標），無論目的是為提供商品或服務，或是監控歐洲居民的行為，即使資料控制者或處理者不在歐洲境內，都必須遵循 GDPR 的規範[3]。因此，業務中涉及處理歐盟居民個資的企業，也必須確保自己可以符合 GDPR 中對於企業在蒐集、處理及利用個資上的各項義務。此外，我國的企業為了取得歐盟居民個資，若要進行個資的跨國傳輸，同樣需特別注意涉及個資傳輸到歐盟境外第三國的規範，例如與歐盟的企業對手依標準資料保護條款訂定企

3 舉例而言：一間臺灣企業，雖然未在羅馬尼亞設有據點，但針對羅馬尼亞消費者設立羅馬尼亞文的網站，便會被視為以「歐盟（此例為羅馬尼亞）市場為目標」。然而，一家歐盟境外企業持有歐盟居民個資，不會因此自動成為 GDPR 適用對象。例如一名德國人來臺工作，在一家本地銀行開戶，留下個人資料。此種情況下，這家臺灣的銀行不會因此落入 GDPR 適用範圍。這家銀行是否落入 GDPR 的適用範圍，仍須視該銀行是否有針對歐盟市場的業務行為而定。

業，確保歐盟居民的個資跨國傳輸可合法、正常的進行，而不會影響業務。

三、因應方式

(一) 歐盟十分重視個人的隱私權益，認為這屬於基本人權之一。GDPR 的多數規範沿用自 1995 年資料保護指令，已經歷 20 年以上的實務運作，因此在我國企業與歐盟企業或民眾商務往來已十分密切的情況下，對於個人資料保護的相關規範，大概都已不會太陌生。不過，GDPR 相較於 1995 年資料保護指令，仍有不少差異，*除了擴大適用範圍，涵蓋處理歐盟居民個資的境外企業，也增強了對當事人權利及企業義務的規範，例如加強對當事人同意的規定、增加當事人要求刪除其個資的權利（被遺忘權）、強化企業告知當事人資訊的規定、企業發生個資外洩事件之通報義務等。*加上隨著業務拓展而需要更大量的資料跨國傳輸可說是當前全球化的商業環境下不可避免的趨勢，因此，對於企業而言，面對 GDPR 即將生效，建議除了尋求法律專家瞭解 GDPR 規範，也宜開始評估企業業務是否包含對歐盟居民個資之處理而落入 GDPR 的管轄範圍，以及相關作業方式與管理措施是否符合 GDPR 規範。評估面向可包含企

業業務或服務是否涉及蒐集、處理及利用歐盟居民的個資、企業內部管理、個資處理程序、資訊安全與監控措施、緊急應變措施等實務做法與 GDPR 規範的符合性。

(二) 對我國企業影響最大的層面，應為歐盟居民個資是否能夠順利的跨國傳輸；如果不能順利傳輸，對某些業別而言將對其經營歐盟市場造成不利影響。在此方面，GDPR 維持跟現行 1995 年資料保護指令一樣的原則，也就是原則上禁止歐盟居民的個人資料傳輸到境外的第三國，除非有「安全措施」確保相關個資的安全無虞。這些安全措施就是本文第一大項第(三)段第 5 點所提到的適足性認定、標準資料保護條款、企業拘束規則、行為準則等。這些安全措施中，適足性認定屬於政府間的措施，由第三國政府與歐盟合作，促使歐盟認定某一第三國的個資保護規範跟歐盟水準相當，如此一來，歐盟與該第三國間對於個資的跨境傳輸，便不受任何限制。*目前歐盟只對 12 個地區或國家[4]做出適足性認定，臺灣尚非其中之一*，因此現階段我國企業可以透過下列方式跨境傳輸歐盟居民個資：

1. **企業拘束規則**：適用於跨國企業。企業拘束規則類似於企業

4 安道爾、阿根廷、加拿大（部分）、法羅群島、根西、以色列、曼島、澤西、紐西蘭、瑞士、烏拉圭、美國（部分）。另歐盟正就韓國、日本評估中，預計在 2018 年內完成評估，給予適足性認定。

內部的行為準則，允許在歐盟設有據點的跨國企業將歐盟居民的個資傳輸到歐盟境外且未獲適足性認定之第三國。企業拘束規則必須包含個資保護之原則、有效的手段，並且須具備法律拘束力。企業在擬定企業拘束規則後，必須送交歐盟28個會員國之一的個資保護主管機關進行跨歐盟的採認程序。

2. **標準資料保護條款**：受歐盟企業委託進行資料處理的我國企業可使用。在歐盟的資料控制者將歐盟居民的個資傳給歐盟境外且未獲適足性認定之第三國之資料控制者或處理者時，歐盟執委會擬定3種不同版本的標準資料保護條款，明列相關資料保護的權利義務，供企業簽署，透過契約的拘束力，確保第三國企業善盡個資保護之責。其中2種版本供歐盟資料控制者與第三國資料控制者間使用，1種版本供歐盟資料控制者與第三國資料處理者間使用。

3. 至於**行為準則**與**認證機制**，目前歐盟尚在研擬具體規範中。

(三) 除了上述安全措施，GDPR中關於**部分排除適用**的條款，允許在某些情況下，即使缺乏安全措施，同樣可以進行跨境個資傳輸，例如：在當事人被告知風險並明確表示同意時；為當事人

執行或完成合約所必須時；為重要公眾利益所必須時；為進行法律訴訟所必須時；當事人無法表示同意情況下，為維護其重要利益所必須時等。

四、我國政府的努力

(一) 我國政府重視個人隱私保護，於 2010 年修訂通過個人資料保護法，並於 2015 年再度修訂，以提高對個人隱私的保護水準。目前我政府已與歐盟就彼此個人資料跨國傳輸法制展開初步技術性對話，以探討未來推動獲得歐盟適足性認定的可能性，並邀請歐盟主管官員訪臺，與相關單位交流，為 GDPR 生效做好準備。我政府將持續與歐盟維持順暢溝通，以確保 GDPR 生效不會對我國企業在歐盟的業務造成不當的阻礙。

(二) 除此之外，我政府已提出加入 APEC「跨境隱私保護規則體系（Cross Border Privacy Rules System，CBPR）的申請，盼藉此進一步推動我企業提高對個資之保護水準，與國際制度接軌。

五、有用的連結

(一) 歐盟執委會司法總署針對 GDPR 修法之說明網站（英文）

(二) 歐盟執委會司法總署針對中小企業之說明網站（英文）

(三) GDPR 法規全文（英文）

(四) 歐盟執委會司法總署對企業拘束規則之說明（英文）

(五) 歐盟執委會對標準資料保護條款之說明（英文）

(六) 各歐盟會員國個資保護主管機關（英文）