《一般資料保護規範》
GDPR : General Data Protection Regulation

《一般資料保護規範》(英語：General Data Protection Regulation，縮寫作 GDPR；歐盟法規編號：(EU) 2016/679)，又名**《通用資料保護規則》**，是在歐盟法律中對所有歐盟個人關於資料保護和隱私的規範，涉及了歐洲境外的個人資料出口。GDPR 主要目標為取回個人對於個人資料的控制，以及為了國際商務而簡化在歐盟內的統一規範。

GDPR 取代了歐盟在 1995 年推出的歐盟個人資料《資料保護指令》(Data Protection Directive) 95/46/EC，該條例包含有關處理歐盟內部資料主體的個人可識別資訊的條款和要求，適用於與歐洲做生意的所有企業，不論實體位置何在。處理個人資料的業務流程必須在設計和預設情況下構建資料保護，這意味著個人資料必須使用假名化或匿名化進行存儲，並且預設使用盡可能最高的隱私設置，以避免公開資料未經明確同意，並且不能用於識別沒有單獨存儲附加資訊的主題。任何個人資料除非在法規規定的合法基礎上完成，否則資料控制者或處理者已經從資料所有者那裡獲得明確的選擇同意。資料所有者有權隨時撤銷此權限。

個人資料處理者必須清楚地披露任何資料收集，聲明資料處理的合法基礎和目的，保留資料的時間以及是否與任何第三方或歐盟以外的國家共享資料。用戶有權以通用格式請求處理器收集的資料的便攜式副本，並有權在特定情況下刪除其資料。 公共主管部門和以核心活動為中心定期或系統地處理個人資料的企業需要雇用資料保護官員（DPO）負責管理 GDPR 的合規性。如果資料洩露對用戶隱私產生不利影響，企業必須在 72 小時內報告任何資料洩露。

本法案在 2016 年 4 月 27 日通過，兩年的緩衝期後，在 2018 年 5 月 25 日強制執行。根據歐洲聯盟運作條約第 288 條第 2 項，因為 GDPR 屬於歐盟條例(英語：regulation；德語：Verorderung)，不是指令（英語：directive；德語：Richtlinie)，所以不需經過歐盟成員國立法轉換成各國法律，而可直接適用。隨著英國在 2019 年脫離歐盟，英國也於 2018 年 5 月 23 日御准批准了 2018 年資料保護法案 。該法案包含了相應的法規和保護措施。

GDPR 延伸歐洲資料保護法的領域至所有處理歐盟住民的境外公司。 GDPR 使通行歐盟的資料保護規章一致，因此使歐洲以外的公司能夠更容易地遵守這些規章；然而代價是嚴格的資料保護規定，且有著公司全球收益 4%或兩千萬歐元(擇高者）的高額罰款。

《一般資料保護規則》(英語：General Data Protection Regulation，縮寫作 GDPR 保護範圍：
只要是一個人所能產生出的任何資料，幾乎都被重新定義為個人資料並受到保護。
個人身份 - 電話號碼、地址、車牌等
生物特徵 - 歷資料、指紋、臉部辨識、視網膜掃描、相片等
電子紀錄 - Cookie、IP 位置、行動裝置 ID、社群網站活動紀錄

GDPR 的法規基礎有：
被遺忘權 (Right to be forgotten)：可以要求控制資料的一方，刪除所有個人資料的任何連結、副本或複製品。
取用權 (Right to Access)：可向資料控制方，尋求關於使用者本身的資料之使用方法、地點及目的等等。此外控制方也應以電子形式提供資料的副本供擁有者參考。
資料可攜權 (Right to data portability)：意思是用戶可以以通用、機器可讀的形式取得某一服務的資料，進而轉移到另外一個服務上
隱私始於設計 (Privacy by design)：組織需要採納隱私設計的架構，在最初階段就對隱私及資料保護問題進行預測及因應，並且應對裝置及應用程式實施嚴格的身分驗證及授權機制。

企業責任
知悉個資遭侵害，需 72 小時內通報與通知、個資保護影響評估、個資保護設計及預設。

影響產業
由於 GDPR 大大擴展了其涵蓋範圍，因此受到了全球的廣泛關注，因為從以往地域上的限制，轉變成為凡是向歐盟人民提供產品、服務或監測歐盟境內公民網路行為的境外企業都算。
受到影響的產業非常廣泛，影響甚大的產業有幾項:

醫療資訊
為了有效推動智慧醫療，許多病患的醫療資訊必須電子化，透過各種深度學習演

算法去訓練模型，進而達成各種需求。而電子病歷所衍生的隱私問題，在高度安全的區塊鏈技術尚未普及的情況下，雖然可以透過去識別化初步的過濾掉個人資訊，然而在以往尚無法律強制性的時期，卻也無從確實地在使用醫療資料上保障個人隱私。現在，基於 GDPR 的規定，取得醫療資料的前提是有取得病患的同意，雖然增加了一些程序，但資料安全與隱私的保障所帶來的益處，不僅能夠保障病患的基本權利，也能提升資料使用上的正當性。

網路零售

這是一個會處理大量個人可識別資訊之產業，包括跨境電商、連鎖商店、旅遊服務、餐飲，只要是替歐盟顧客服務，掌握信用卡資料、地址、基本個資，都屬於 GDPR 規範中。再加上網路服務隨之產生的資料之大，使其更首當其衝，這也正是為何 Apple 蘋果等網路服務公司 也推出了個資管理系統，以因應 GDPR 修訂。

金融

金融機構持有大量個人可識別資訊，每當涉及個資需要傳輸到境外、處理或利用到歐盟民眾個資、海外設有分行、委外業務，都可能受到影響。再加上歐盟在世界經濟中佔有第二大位，金流來往頻繁，更不用說近年區塊鏈技術的興起，資料隱私安全議題更是影響甚大。

航空運輸

航空運輸主宰當今人口移動的方式，旅客往返的機票、出入境資料也都涉及個人隱私。以台灣為例，華航、長榮兩家國營航空業者來說，目前在歐洲都有航點，不僅在海外設有辦公室，也需要頻繁處理大量旅客資料。