General Data Protection Regulation（GDPR）

歐盟通用資料保護規則

—GDPR於2016年4月27日通過，於2016年5月25日生效，預計於2018年5月25日全面實施。

GDPR強化歐盟公民之下列權利：

1. Right of access （資料檢視權）；
2. Right to rectification （更正權）；
3. Right to be forgotten （被遺忘權）；
4. Right to restriction of processing（限制處理權）；
5. Right to data portability （資料可攜權）；
6. Right to object （對自動化處理之拒絕權）。

GDPR適用對象

1. 企業或組織在歐盟境內有實體營運據點的企業或組織；
2. 企業或組織雖未於歐盟境內設有營運據點，但對歐盟境內資料主體（自然人；下稱「歐盟公民」）有下列行為：
   (1) 對歐盟境內之歐盟公民提供商品或服務，無論此項商品或服務是否需要歐盟公民支付對價；
   (2) 企業或組織的商業模式有透過網路或任何方式監督歐盟公民的個人行為，包含在網路上取得網頁瀏覽者的所在地資料、網頁瀏覽歷史資料（cookies）等。

GDPR適用對象應具備條件及義務

1. 企業或組織在開始處理歐盟公民個人資料（下稱「個人資料」）之前，應提供歐盟公民下列有關個人資料影響評估之合理協助：
   (1) 對預定個人資料處理作業及處理目的作有條理的說明。
   (2) 所提供服務與相關個人資料處理作業之必要性及適當性。
   (3) 關於個人資料處理作業對歐盟公民之權利及自由所生之風險。
   (4) 解決風險的措施，包括防護機制、安全措施及機制，以確保個人數據的保護。
2. 除法律另有規定外，企業或組織就個人資料之處理限於與歐盟公民間之約定事項所用。除法律定有禁止通知之規定外，當個人資料用於約定事項以外之用途時，企業或組織在處理個人資料前，應儘速通知歐盟公民。
3. 企業或組織應考慮下列條件，提供適當且經歐盟公民檢視及同意之個人資料保護措施，以防止個人資料外洩事件：
   (1) 個人資料之性質；
   (2) 因個資外洩事件衍生的危害；
   (3) 科技發展程度；
   (4) 實施任何措施的成本。

4. 企業或組織應確保其所屬人員，及經其授權處理個人資料之其他企業或組織，就個人資料之處理限於約定事項所用。
5. 未取得歐盟公民事前書面同意，且符合下列條件者，不得將個人資料移轉至歐盟以外地區：
   (1) 就資料之傳輸設有合理防護機制。
   (2) 歐盟公民有執行資料傳輸指示的權利及有效的法律救濟。
   (3) 遵循歐盟公民所提出有關資料傳輸之合理指示。
6. 除法律另有規定，應保存個人資料外，企業或組織應依歐盟公民書面指示，刪除或返還個人資料（包含副本）。
7. 企業或組織應保存完整且正確之歐盟公民個人資訊處理紀錄及相關資訊。
8. 若企業或組織有涉及對歐盟公民的資料處理，且符合下列情形者，必須設置資料保護長（Data Protect Officer）：
   (1) 依其核心業務之性質、範圍或目的，需要進行大規模、定期且有系統地分析、蒐集個人資料；或
   (2) 涉及特種個人資料（如：種族、政治理念、宗教、哲學信仰、基因數據、生物特徵、健康、性向等）或刑事犯罪紀錄等資料之處理。
9. 企業或組織應配合歐盟公民或其指定之人對其個人資料處理活動之檢視要求（瞭解其個人資料處理活動之進行）。
10. 在企業或組織授權其他企業或組織處（下稱「次受託處理者」）理個人資料之前，應：
   (1) 以書面通知歐盟公民有關預定之次處理者及預定處理事項；
   (2) 取得歐盟公民之書面同意；
   (3) 與次受託處理者簽訂書面契約，契約內容應包含要求次處理者遵循所有 GDPR 適用對象之義務；
   (4) 在合理範圍內，提供歐盟公民有關次受託處理者之資訊。
11. 企業或組織應就次處理者之所有故意或過失行為負責。
12. 只要發生歐盟公民個人資料外洩之情事，企業或組織應於 72 小時內通報資料保護主管機關（Data Protection Authority）。

GDPR罰則

1. 如企業或組織蒐集與處理個資的流程不符規定，則最高可處 1,000 萬歐元，或前一年度全球營業總額 2%罰鍰，以較高者為準。
2. 如企業或組織違反 GDPR 規定，例如侵害個資隱私權，最高可能被處 2,000 萬歐元，或前一年度全球營業總額 4%罰鍰，視情節輕重，以較高者為準。

（資料來源： 禾同國際法律事務所, 僅供參考。）