

其他

[歐盟]

GDPR 上路企業應注意避免踩雷

歐盟通用資料保護規則 (General Data Protection Regulation, GDPR) 於 2018 年 5 月 25 日開始實施，該規定於 2016 年 4 月 27 日通過歐盟議會批准，該法旨在保障歐盟居民個資的使用權及隱私權，能自主掌控個資，並在整個歐洲創建一致的資料隱私法，與世界上任何儲存或處理歐盟居民資料的公司均息息相關，不符合規定的公司將面臨巨額罰款，最高 2,000 萬歐元或年度全球營業額之 4%，以較高者為準。以下為 GDPR 重要內容：

1. 個資之定義為有關識別或可得識別自然人之任何資訊，並明文涵蓋網路識別碼，如 IP 位址、cookie 碼、GPS 等。
2. GDPR 中亦規定禁止處理之資訊，包括民族或種族來源、政治見解、宗教信仰、工會會員、基因資料、生物特徵（例如人臉辨識、視網膜、指紋），以及個人健康資料或性生活或性傾向資料等，原則上不得蒐集、處理或利用，但基於個人同意、公共利益等情形除外。
3. 無論公司所在位置及處理資料的地點為何，只要有蒐集、處理或利用歐盟居民之個資，即有適用本法。
4. 當事人之權利包括接近使用權、更正權、刪除權（被遺忘權）、反對權及資料可攜權。
5. 各會員國除法院及司法權外之公務應設立至少一個獨立機關，監督 GDPR 之適用。
6. 跨境傳輸：禁止傳輸至歐盟以外之地區或國家，但有下列情形之一，可享例外許可：(1)接受國具備「適當保護水平」，(2)資料管理者已提供適當保護措施，(3)當事人明確同意，(4)基於重要公共利益之維護，(5)基於保護當事人之重要利益所必要。
7. 違規處罰適用於資料控制者和資料處理者，但適用對象限於企業，未針對自然人或公務機關之違反行為制定處罰規範，而係委由各會員國自行訂定有效、適當且具懲戒性的罰則。
8. 取得“同意使用資料”新增嚴格的參數，要求使用易懂、易於取得的表單，並使用清晰且易於理解的語言，撤回同意必須一樣容易。
9. 個資外洩知悉後 72 小時內通報監管機關。
10. 主張「刪除權」的人可要求刪除個人資料、停止傳播該資料並阻止第三方處理該資料。
11. 個人可要求並接收其個人資料並傳送給另一個資料控制者。
12. 儘管設計隱私的規定已存在多年，然 GDPR 使其成為法律必要條件，規定資料保護必須在設計系統時即納入考慮，而非事後考慮或附加。
13. 公司將被要求指派一名資料保護長 (Data Protection Officer, DPO)。

資料來源：“Here Are 8 Things Every Business Needs To Do Now To Get GDPR Ready,” Forbes, 2018 年 5 月 7 日。

<<https://www.forbes.com/sites/bernardmarr/2018/05/07/here-are-8-things-every-business-needs-to-do-now-to-get-gdpr-ready/#3752c7e77cf6>>