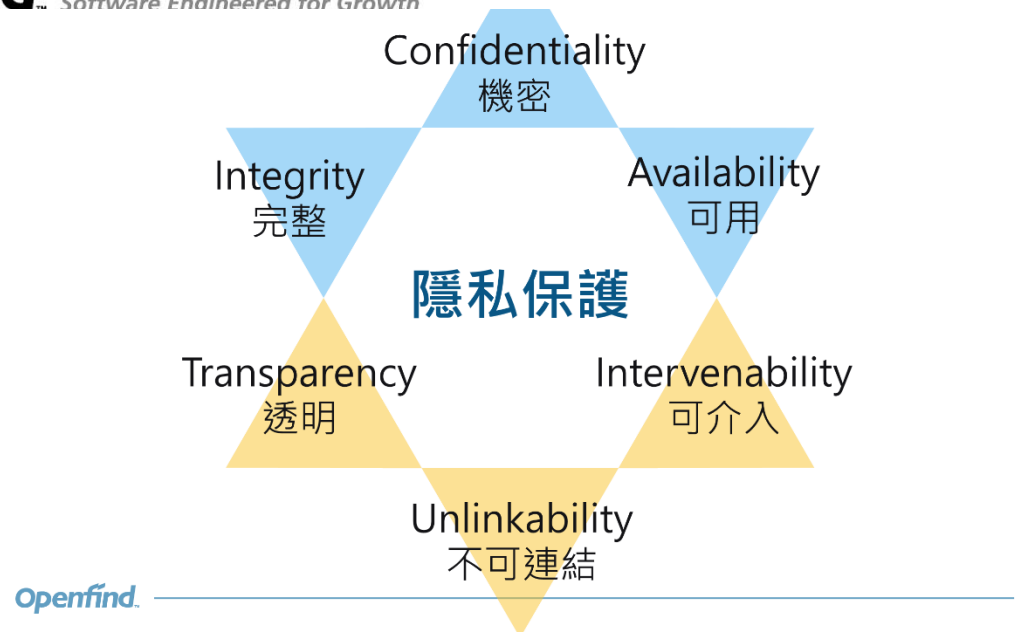
GDPR 精神解析及法規遵循實作

歐盟隱私保護法 GDPR(General Data Protection Regulation) 已在 5 月底上路。迄今或許仍然有許多國內企業一知半解。當然，如果沒有清楚的觀念，就會影響 GDPR 的法規遵循作業。

網擎資訊行銷副總李孟秋很簡單、扼要的方式說明 GDPR 的精神及管理範疇。GDPR 規範的是企業對個人(B2C)的資料蒐集行為，不只是在歐洲有分支機構、營運據點的公司需要注意，其他地區的企業如果有牽涉歐盟公民資料跨境傳輸及處理、分析，例如委外列印帳單業者，也會受到 GDPR 的規範。它也規範資料的控制者(Controller)及處理者(Processor)的義務。

(Openfind 行銷副總 李孟秋)

GDPR 對個資的認定相當寬廣。除了傳統上的姓名、身份證字號外，連網路動態 IP 位址、Cookies、生物特徵（如指紋、指靜脈、長相）或是定位資料（如 GPS、MAC 位址）都被視為保護對象。也就是說，GDPR 不只保護個人資料，也要保障隱私。這使得 GDPR 被視為是反科技、反創新。事實不然；GDPR 是定出企業個資蒐集的框架，使廠商行為不得逾越，並鼓勵其在框架範圍內推出更好的技術、跑出數據分析、提供更好的服務和價值。



此外，GDPR 包含的六大安全原則，除了傳統為人熟知的機密、完整及可用性，還多了不可連結性(Connectivity)、透明性(Transparency)及可介入性(Intervenability)。不可連結性要求確保資料最小化、資料隔離、匿名化／假名化，以及提早刪除資料，企圖從根本阻斷個資外洩的可能。透明度要求不斷紀錄、不厭其煩向個人解釋蒐集的原因、方法及個資用途、以及個資外洩要求通報等，旨在從事前到事後、程序及技術上完全透明化。可介入性，則是反對廠商以技術做不到為由的搪塞態度，要求確保個人可中斷服務、可將資料攜出到別處、可要求刪除資料，一種「重視人高於科技」的價值觀展現。

從臉書爆發劍橋分析(Cambridge Analytica)濫用其 8,700 萬筆個資事件後，許多品牌客戶與之切割來看，不遵循 GDPR 對企業絕對有會商譽乃至於營收上的損害。

也許有些企業擔心，國際上有 GDPR，國內有個資法、營業秘密法、資安保護法的規範，恐怕光是法規遵循就足以造成企業人仰馬翻。尤其 GDPR 更廣泛的認定個資，及它種種規範，像是設置資料保護長、資料外洩的通報期限等，比起國內法規更是嚴格許多。

即使如此，GDPR 和個資法的法規遵循作業其實可以一步到位。因為 GDPR 範疇完全涵蓋個資法，只要先做好個資法的合規，再依據 GDPR 擴大範圍，調整政策、組織流程及工具的設定，即可同時滿足兩種法規，就算未來還有新法規推出，也可以循此因應法規的要求，達到資安的長治久安。

(從組織與技術面雙管齊下，才能達成合規，進而獲致資安長治久安)

實際執行上，法規遵循工作包括組織及技術二層面，前者涉及政策、流程和人事，後者包括服務及軟體工具。組織面的合規有賴企業自己的法務、IT 部門，結合外部顧問及高層支持，以調整出適合的作業流程，這無法假手他人。但是技術層面則可以藉由選擇優良的產品工具滿足大部分要求。

網擎資訊從早期的郵件資安、郵件歸檔，去年買下儲存雲產品、今年再跨入即時通訊(IM)歸檔、AI 為基礎的反詐騙服務。網擎不但力求產品的安全、效能、整合效益、也確保產品符合產業標準，包括 ISO 27001、ISO 27550，具備整體安全性及隱私工程，現在還積極規劃結合現有產品線，實現企業流程的自動化串接，企望能從技術面，協助企業滿足 GDPR 甚至未來法規的遵循。