
王琍瑩律師專欄同時刊登於 INSIDE 、TechOrange 、天下雜誌網摘精選與數位時代創業新聞：「歐盟高規格 GDPR 數據保護法上路，AI 新創該如何應對？」

如果你是 Apple、Google 或 Yahoo 會員，最近登入帳號，一定會收到新版的隱私條款聲明，要求你按下同意。多數人可能直覺會以為，這是在 Facebook 的「劍橋分析」風暴後，各家業者亡羊補牢的對策。其實並非如此，而是影響層面更深更廣的歐盟個資保護新法 GDPR (General Data Protection Regulation)，即將在 5 月 25 日上路，是它讓大家嚴陣以待。

隱私權是個超過百歲的古典法律概念，但究竟為什麼， GDPR 會引發全球業界草木皆兵？在注重蒐集用戶數據的 AI 時代，這會產生哪些影響？

首先，GDPR 在適用對象、規範內容和處罰等面向，都宣示前所未見的管制力道。其次，GDPR 明文確認「賦權」(Empowerment) 與「當責」(Accountability) 的觀念，徹底顛覆政府與民間「上有政策、下有對策」的表面和諧。再者，GDPR 可算是首部「單挑」應用 AI 與 Big Data 的隱私保護法令，試圖直搗黑盒子核心。

資料來源：https://www.inside.com.tw/2018/05/22/eu-gdpr
https://buzzorange.com/techorange/2018/05/23/gdpr-shock/
https://www.cw.com.tw/article/article.action?id=5090080
https://meet.bnext.com.tw/articles/view/42958

可以想見，GDPR 上路後，數據利用與用戶隱私之間的權衡與折衝，將成為企業無法迴避的挑戰。壞消息是，GDPR 的「最廣、最嚴、最昂貴」讓企業稍有不慎，就可能嚴重受罰；好消息是，在與 AppWorks Accelerator 校友企業進行法務輔導的過程中，針對實務運作，整理出這篇「最小、最大、最透明」的教戰守則，在此公開分享，希望提醒企業看待 GDPR 不只是無奈的法遵成本，更是協助產品與服務最佳化的關鍵。

## GDPR 之最廣、最嚴、最昂貴

GDPR 引發業界焦慮恐慌的紅色警戒，主要原因有以下三點：

1、 適用對象史上最廣

GDPR 適用於任何在歐盟設立據點的企業，無論個資處理是否發生在歐盟境內。相對的，如果企業的產品或服務，有部分用戶是歐盟居民、蒐集或處理到歐盟居民的個資，無論是否為設立在歐盟的企業、不管是 B2C 或 B2B 領域，都在 GDPR 涵蓋的射程內。當然，企業請不要忽略，隱私保護不只影響到用戶黏著度、交易夥伴的合作意願，隨著 GDPR 帶動全球法規風向，法遵稽核勢必也將成為投資與併購案件 Due Diligence 的重要環節。所以，不論企業是否直接適用 GDPR，沒有人是局外人。

2、 規範內容史上最嚴

GDPR 整份文件，光是前言就有 173 點，內文更長達 11 章共 99 條法規，鉅細靡遺規範了什麼才是合法、公平與透明的數據蒐集、處理、利用，包括：使用者權利、系統架構、資安管理、風險評估、通報機制、專責人員、標章制度、跨境傳輸、機關權限、爭議處理、緊急措施等。其中許多定義釐清與執行難度，目前仍存在爭議，有待將來累積個案經驗與實務見解，且戰且走。

3、 天價罰鍰史上最貴

在台灣，現行「個人資料保護法」對違法企業，最高按次處以新臺幣 5 萬元以上、50 萬元以下罰鍰。但一旦違反 GDPR 情節嚴重，最高可能處以 2,000 萬歐元，或全球年營業額 4% 的罰鍰。無論是資料控制者 (Data Controller)、協助進行資料儲存或傳輸的資料處理者 (Data Processor)，都可能受到裁罰。

## 教戰守則之最小、最大、最透明

資料來源：https://www.inside.com.tw/2018/05/22/eu-gdpr
https://buzzorange.com/techorange/2018/05/23/gdpr-shock/
https://www.cw.com.tw/article/article.action?id=5090080
https://meet.bnext.com.tw/articles/view/42958

GDPR 引進「賦權」與「當責」的觀念，將一直以來被誤認為配角的用戶與企業，重新拉回鎂光燈下，企業不再只是配合主管機關規定，或是請律師擬定隱私權政策文件的被動角色，這主要包括三個面向：

1、 最小限度利用個資

隨著科技演進，個資的定義愈來愈廣，泛指一切可識別化的個人資料。GDPR 明文指出，以不可逆的方式得出完全無法辨識出用戶個人的「去識別化資料」(Anonymous Data)，雖不屬於隱私保護範疇，但可透過交互比對、勾稽辨識出用戶個人身分的「去連結化資料」(Pseudonymised Data)，仍可能構成個資。相對的，GDPR 也確立個資的蒐集、處理、利用都必須遵循「最小限度原則」，也就是不得逾越預先設定的「特定目的」。

從數據分析的效率而言，蒐集資料本來就不是愈多愈好，過多的雜訊、不知所以的運算，結果也只是 “Garbage in, garbage out.” 而已。話雖如此，卻是知易行難，舉例來說，當用戶使用 Google 的搜尋服務，Google 除了依賴輸入的關鍵字外，可能也參照用戶的 Gmail 使用行為、結合即時的位置資訊，從而得出最佳化的搜尋結果。類似這樣的數據再利用 (Data Recycling)，便可能與「最小限度原則」相扞格。GDPR 為此提供了「特定目的相容性」的判斷基準，包括新舊目的關聯性、資料蒐集的背景脈絡、用戶與企業的關係、用戶的合理期待、允許使用的結果、資料的本質等等，可供企業斟酌參考。

2、 最大程度賦權用戶

個資永遠屬於當事人，不是任何企業可以據為己有。GDPR 強調「賦權」用戶，包括接取資料權 (Right to Access)、遷移資料權 (Right to Data Portability)、更正權 (Right to Rectification) 與刪除權 (Right to Erasure / Right to Be Forgotten)。事實上，由於用戶本人對個資的正確性最為熟悉，企業如果能夠藉由「賦權」機制，鼓勵用戶隨時主動更新個資，像玩樂高積木一樣，拼湊出自己認為的長相，不但能夠落實 GDPR 的法遵要求，更有助於優化數據分析。典型的例子，就是過濾垃圾郵件和 Facebook 廣告偏好 (Ad Preferences) 的設定機制，由用戶主動參與特徵標示，使企業得以進行更精準、更值錢的數據分析。

以實現「賦權用戶」為前提，GDPR 特別要求企業「講人話」來取代晦澀難懂的隱私政策。企業必須用最直接、最淺顯易懂的方式，揭露隱私政策，並且遵循「確認後同

資料來源：https://www.inside.com.tw/2018/05/22/eu-gdpr
https://buzzorange.com/techorange/2018/05/23/gdpr-shock/
https://www.cw.com.tw/article/article.action?id=5090080
https://meet.bnext.com.tw/articles/view/42958

意」(Affirmative Consent) 的流程，前者例如「Multilayered Privacy Notice」，後者例如「Opt-in」機制。Facebook 在「劍橋分析」事件爆發後，陸續提出「Privacy Shortcut」、「Clear History」這些隱私保護優化措施，便是著眼於此。

3、 最透明的決策機制

我們知道機器學習，尤其深度學習，有如在黑盒子內進行的過程，就像人類的神經網路，究竟如何決定數據的關聯性與權重以形成決策，向來是個難解的謎團。但是，我們也知道，過去人們以為電腦一定比人腦準確、不受外在因素影響，在人工智慧的領域已經不再適用，「演算法公平性」的議題因此興起。GDPR 強調「透明處理原則」，針對「個人化自動決策」(Automated Individual Decision-Making) 賦予用戶請求解釋、拒絕適用的權利 (Right to Explanation / Right Not to Be Subject)，其實就是將近年來學術討論逐漸熱絡的「可信任 / 解釋的人工智慧」(Trustable/Explainable AI) 直接納入法律，試圖引起全面性的重視。

「可信任 / 解釋的人工智慧」主要探討如何盡可能減少黑盒的節點、避免演算法偏見與歧視。當「個人化自動決策」，對用戶形成法律效果或其他重大影響，包括個人資料的「剖析建檔」(Profiling)，企業必須確保模型本身是由正確的數據訓練出來，不得標示種族膚色、宗教信仰、政治立場、性傾向等可能導致歧視的特徵，並應事先向用戶說明自動決策的存在、取得用戶同意。

此外，企業至少要有能力在足以保護用戶權益的範圍內，簡要說明怎樣的數據會導致怎樣的決策、數據的變動如何影響決策的變動，並賦予用戶可以拒絕適用、表達意見、要求「工人」智慧介入判斷的權利。

舉例來說，如果線上汽車保險業務完全透過演算法，自動決定用戶的保費金額，企業必須能夠說明如何計算保費高低？是由哪些因素所決定？例如，是受到用戶年齡、健康狀況、駕駛習慣、肇事紀錄等因素影響。而如果用戶認為權益受損，則可以表示異議。

GDPR 的「透明處理原則」，除了挑戰人工智慧的黑盒子以外，在技術層面也不斷對工程師喊話，主張從設計端開始的隱私保護 (Privacy by Design)。當企業判斷某項個資處理環節，可能侵害用戶權益時，就必須進行「資料保護影響評估」(Data Protection Impact Assessment)，提出解決方案，必要時並應向主管機關彙報。此外，

資料來源：https://www.inside.com.tw/2018/05/22/eu-gdpr
https://buzzorange.com/techorange/2018/05/23/gdpr-shock/
https://www.cw.com.tw/article/article.action?id=5090080
https://meet.bnext.com.tw/articles/view/42958

GDPR 也鼓勵企業常設資料保護專責人員 (Data Protection Officer) 協助建立常規，並建議主管機關與業界，協力建立行為準則與認證機制，共同促成法的實踐。

## 結語：企業要當太陽，不當北風

對台灣企業來說，即便完全遵守「個人資料保護法」，是否仍有違反 GDPR 的疑慮，恐怕是現階段最擔心的事情。有鑑於此，國發會已陸續邀集各部會研擬因應策略，除了進一步了解有無參照修法的必要之外，並針對各式各樣實務疑慮，循官方途徑展開協商。在這個過渡時期，我們建議企業兼顧天平的兩端，在策略方向上，必須掌握數據作為商業競爭的致勝關鍵，而在執行層面，仍應落實個人資料歸個人控制的原則，不能偏廢。

其實，當我們用資料科學的角度來解讀，就會清楚發現企業和用戶並非對立，而是站在同一陣線。看待 GDPR 未必要從法遵成本的角度來思考，當企業提供體貼用戶的隱私保護，確保用戶心甘情願提供個資、樂於即時更新資料，便能降低數據分析錯誤的風險，並優化產品與服務的效能與價值。

有了以上的認識，在 GDPR 上路後的數據利用，反而更像是「北風與太陽」的故事。一旦隱私保護內化成為企業 DNA，企業與用戶都將因此受益，到時候，如何處理數據不觸法，便不再是一個恐怖的話題。

資料來源：https://www.inside.com.tw/2018/05/22/eu-gdpr
https://buzzorange.com/techorange/2018/05/23/gdpr-shock/
https://www.cw.com.tw/article/article.action?id=5090080
https://meet.bnext.com.tw/articles/view/42958