

GDPR 與數位經濟—歐盟的企圖與啟發

理律法律事務所 曾更瑩律師

壹、前言

數位經濟在近年之發展突飛猛進，電腦運算能力之增強、行動裝置之普及、網際網路連線能力與速度之進步，帶動新科技之開發與誕生，商業模式之創新與蓬勃發展。社群網站、通訊軟體被廣泛使用，其型態從早期的部落格、微博、臉書（Facebook）、到近期的Line，將社群網站、即時通訊之功能開發到極致，之後又有其他吸引年輕族群的社交媒體竄起；影音串流技術進步，如今在各大OTT 網站上放映的影片，品質不輸傳統電視甚至青出於藍，各種直播、短視頻平台也在世界各地頭角崢嶸；Uber、Airbnb 等「共享經濟」、「平台經濟」迫使傳統既得利益業者反思與進步，也使大家重新思考與反省傳統管制經濟之方式與內容是否合理；在中國崛起的電子支付、第三方支付等工具，在世界各國包括臺灣，還在摸索與考量是否全盤接受之時，虛擬貨幣、加密貨幣和形形色色的ICO 已經對全球之金融監理機關拋出一道道難解的習題，而其所奠基之區塊鏈技術也在各行各業發展出各種應用；在軟、硬體技術進步，海量資料之蒐集與分析成為可能後，機器學習、人工智慧之急速發展彷彿即將使科幻小說中的場景化為現實，如果此番人工智慧之泡沫在最近持久不消，人工智慧之發展更有可能顛覆目前所有數位經濟之模式與人類未來生活之圖像。

凡此種種，追根究底，「資料」之蒐集、分析、利用，是數位經濟發展背後極為重要的動力，也是上述諸多科技發展與商業模式得以扎根、茁壯的沃土。掌握資料來源、開發創新思維、加上精確分析資料之科學能力，將是未來發展數位經濟的關鍵。然「資料」之蒐集與分析成果之誕生，與「個人資料」和「隱私」密不可分，過往數位經濟發展之模式，大多數奠基於大量「使用者」個人資料與行為模式之分析，進而產生對於隱私以及人權保護不周之疑慮，而有心人士對於個人資料之誤用甚至濫用，亦造成公眾之紛擾與不樂見之後果。是以「個人資料」之保護與數位經濟之發展間應如何調適與平衡，當為現今重要課題。

歐盟的一般資料保護規則（General Data Protection Regulation, GDPR）在今（2018）年5月25日生效，因為涉及域外效力和高額行政罰款，對全世界投下不小之震撼彈。在GDPR 如此重裝備戒護個人資料之下，歐盟將如何調適個人資料之保護與數位經濟之發展？本文茲分享個人觀察心得。

貳、歐盟對於個資保護以及數位經濟發展之企圖與布局

一、美歐個資保護大不同

歐盟各國為世界立法例中，制定完整個人資料保護法典之先驅。在歐盟，個人資料以及隱私之保護，被視為人權之內涵，高規格保護之。而在大西洋對岸的美國，並無全國統一適用之個人資料保護法典，對於個人資料及隱私權保護之法律散見於各州法規中，加上矽谷新創企業強勁旺盛的爆發力，在數位經濟發展之浪潮中不斷拔得頭籌，一路領先全球。歐盟對於美國鬆散之隱私管制方式一直無法認同，過去兩地曾以「安全港」之方式允許歐盟之個人資料被傳輸至美國，在GDPR 生效後，亦持續討論以「隱私盾」方式允許歐盟境內之自然人之個人資料得以傳輸至美國。

歐盟與美國之間對於個人資料以及隱私權保護之歧見，當以歐盟與Internet Corporation for Assigned Names and Numbers（網際網路名稱與數字位址分配機構，簡稱「ICANN」）之間就ICANN 的「WHOIS」資料庫之改良與存廢之大戰為著例之一。ICANN 是在美國商務部主導下，負責全球網域名稱與位址之分配之非營利公司法人，ICANN 的WHOIS 資料庫歷史由來已久，為便利各網站之管理人員彼此連繫，WHOIS 資料庫中存有許多個人資料，方便公眾查詢。多年以來歐盟多次質疑ICANN 的WHOIS 資料庫存放或公開過多不必要之個人資料，對於個人資料以及隱私保護不周；從GDPR立法至生效，特別是在今年GDPR 生效前夕，ICANN 與歐盟雙方數度交火，ICANN 甚至在GDPR 生效當日立即在德國法院提出假處分聲請，企圖得到法律上之支持，取得繼續與歐盟作戰之時間與空間；惟德國法院在很短時間內即駁回ICANN 的聲請，拒絕為ICANN 背書。美歐兩地自由開放與嚴密保護兩股勢力之歧異與角力可見一斑。

二、GDPR對於數位經濟之宣示

歐盟GDPR 如此高規格保護個人資料，難道不擔心扼殺其本土境內原本已經落後美國的數位經濟？在GDPR 生效之後，歐盟本土網站亦有被迫關閉停止營業者，例如英國的工具共享平台StreetLend，原先係一以倫敦為主要服務區域，為便利鄰居、朋友分享借用家中閒置不用的工具之平台，例如家中如有平常使用機率不高的梯子、螺絲起子或電鑽等，均可加入分享之行列。在2018年4月，GDPR 正式生效以前，StreetLend 即在其官網上宣布因為GDPR 造成之不確定性與風險，加上違法之高額罰款，使其不得不宣布停止營業。GDPR 之威力可見一般，尤其係對於新創與中小企業之影響甚為顯著。

然GDPR 果真忽視數位經濟發展，棄新創與中小企業於不顧？實則GDPR 前言揭示諸多上位原則與精神，顯示GDPR 之目標包含促進個人資料自由流通以及建立消費者信任等，亦透露促進數位經濟之發展實為歐盟未來之目標之一，而GDPR 之實施與生效乃為其一手段。

GDPR 前言第5點，表示歐盟內部市場之功能，所帶來的經濟與社會之整合，造成個人資料跨境流通之實質增加；公部門與私部門間對於個人資料之交換，包含歐盟境內之自然人、協會、組織之間之資料交換，業已增加。歐盟呼籲成員國之中央主管機關間應相互合作，以便協助彼此履行有關任務。GDPR 前言第6點，表示科技之快速發展與全球化之進程對於個人資料保護帶來新的挑戰，個人資料蒐集與分享之規模與幅度大為增加，科技使得公、私部門均得以史無前例之幅度使用個人資料以從事相關活動。自然人不斷允許其個人資料為公部門以及私部門所蒐集、利用，科技已使經濟與社交生活轉型，是以應進一步「促進」(facilitate)個人資料於歐盟境內之自由流動，以及向第三國以及國際組織之自由流動，並同時確保對於個人資料高規格之保護。以上種種，表示歐盟亦了解在現今科技發展與經濟環境下，個人資料大量被蒐集與利用之現實，也肯認在此發展趨勢與環境之下，個人資料自由流動有其必要，惟歐盟同時亦強調對於個人資料需要高規格之保護。

GDPR 前言第7點，表示為建立數位經濟在歐盟內部市場之發展，建立「信任」十分重要，基此，有關發展需要歐盟建立堅強且更為一致之個資保護架構，該架構必須奠基於強力執法。自然人應被賦予對其自身之個人資料之掌控權，法規面以及實務面對於自然人、業者以及主管機關之確定性應被加強。GDPR 前言第9點則指出雖然過去歐盟個人資料保護指令之立意甚佳，惟未能避免歐盟成員國在執行個人資料保護法規之分歧，造成法律之不確定性，也造成公眾認知在個人從事網路活動時，對於自然人之保護存有相當大之風險，是以，歐盟認為在歐盟境內之成員國若對於個人資料之保護彼此之間存有歧異，將大為阻礙個人資料在歐盟境內之自由流通，造成歐盟經濟活動發展之障礙，扭曲競爭，也妨礙各國主管機關履行其職務。GDPR 前言第10點則繼續強調，為達成一致且高標準之個人資料保護，移除個人資料在歐盟境內自由流動之障礙，歐盟成員國應對於個人資料之保護採取統一且一致性之規則制定與解釋；GDPR 前言第11點更強調，在歐盟境內對於個人資料有效之保護，端視各國對於違反個人資料法規之制裁與執行採取一致性之強度與密度；GDPR 前言第13點亦闡述，為確保在歐盟境內對於自然人之保護程度之一致，避免彼此之間之歧異造成個人資料之自由流動之阻礙，GDPR之規範對於不論大小之業者，含微型企業、中小企業等，均應具有法律上之確定性且應透明，對於歐盟境內之自然人提供相同程度且法律上具有執行力之權利，同時各成員國之主管機關應採取一致性之執法力度並彼此合作。為此，GDPR 對於員工人數少於250人之企業採取法規部分鬆綁，也鼓勵成員國在適用GDPR 時對於微型企業以及中小企業作不同考量。

以上載於GDPR 前言之宣言，顯示歐盟亦有發展數位經濟之共識與決心，但是歐盟認為數位經濟之發展必須以完善之個人資料保護為前提，於此前提，取得消費者之「信任」十分重要，惟有維持歐盟對於個人資料保護之高標準始有可能建立「信任」；而歐盟成員國彼此之間若對於個人資料之保護採取之標準不一，執法程度嚴峻、寬鬆不同，將不利個人資料在成員國間之自由流動，連帶阻礙歐盟整體數位經濟之發展與市場競爭。是以，歐盟利用GDPR 統一（或強迫）其成員國對於個人資料保護之程度與執法力度，乃著眼於促進其境內個人資料之自由流動，同時希望個人資料之自由流動能進一步帶動歐盟整體數位經濟之發展，不可不謂用心良苦。在今年臉書（Facebook）與劍橋分析（Cambridge Analytica）爆出個人資料遭濫用之事件後，世人對於個人資料之保護更為重視，也開始對於過去以「隱私」換「便利」之網路使用型態以及「免付費」數位經濟之發展模式加以反思，GDPR 所要求之諸多法規遵循措施正好可用以重建「信任」，而GDPR 之域外效力也使GDPR 不但成為全球各地有識之士共同閱讀與理解之法律文件，其中諸多原則也成為評斷個人資料保護是否周全之標準。是以雖然GDPR 陳義甚高，法律遵循義務十分繁重，連歐盟境內之企業也大嘆吃不消，其中所揭示之基本原則儼然已成為檢視對於人權保護之程度與方式某種意義上之普世基準。

三、歐盟擬促進「非屬個人資料之資訊」之自由流通

在制定GDPR 之同時，歐盟內部也在討論另外一套法案，亦即對於「非屬個人資料之資訊在歐盟境內自由流動之架構」（Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union），此草案於2017 年9 月間提出討論。該草案之提案說明開宗明義即提到新型數位科技、例如雲端運算、大數據、人工智慧、物聯網等等，都是為了能夠增進使用者靈活度、生產力、速度與自治能力之工具；歐盟之數據市場預估在2016 年至少有六千億歐元的產值，與2015 年相比成長9.5%，而根據歐盟之研究，歐盟之數據市場到2020 年時有成長到超過一兆零六十億歐元之潛力；而為了將此潛力化為可能，歐盟提案意在處理下列問題：

- (一) 改進歐盟單一市場境內因各成員國資料在地化（data localization）要求所形成之非屬個人資料之資訊之流通障礙；
- (二) 確保主管機關於執法時取得資料之權力不受阻礙；
- (三) 確保資料之專業使用者能在不同之資料儲存處理服務提供者之間自由轉換，同時不對服務提供者造成多餘之負擔或因而扭曲市場。

歐盟之目標係達成更具競爭力、統整之資料儲存、處理之內部市場。為達非屬個人資料之資訊得以在歐盟境內自由流通之目標，歐盟在提出上述法規草案之時，不僅進行相關研究，亦徵詢公共意見（public consultation）、進行影響評估（impact assessment）等等。

該草案文字在一開始提到，隨著經濟數位化之加速，資通訊科技（Information and Communications Technology, ICT）已不再係單獨之領域，而係所有現代創新經濟與社會體系之基礎。電子資訊是該體系之中心，當分析電子資訊或將電子資訊與服務以及產品結合之時，將產生更大之效益。資料之價值鏈建立在不同之資料相關活動上，包括資料之生成、蒐集、彙總、組織、儲存、處理、分析、行銷、分銷、利用與再利用等活動。資料價值鏈之建立奠基於有效果並有效率之資料儲存與處理功能；然而，在歐盟單一市場境內，有效果與有效率之資料儲存與處理功能、以及資料經濟之發展為兩種對於資料流通性以及單一市場之障礙所阻撓。其一為歐盟成員國內國法下之「資料在地化」之法令要求；其二則為私人之間在法律上、合約上以及技術上對於更換資料儲存或處理服務提供者所形成之障礙。因此，為求法規明確化以及提供公平競爭之環境，為歐盟內部市場所有相關參與者訂定統一之規範乃為關鍵。

草案第4 條要求成員國不得限制資料之儲存或處理必須限定位於某一成員國境內；除非為了公共安全之考量，資料之儲存與處理在任一成員國都不得被禁止或限制；成員國若有「資料在地化」之立法，應於草案生效後十二個月內廢除之。草案第5 條規定，各主管機關依照歐盟法或各成員國法下之規定行使職權要求資訊提供之權力，不可因此受到影響；主管機關查詢資料之要求或命令，不可以資料儲存在其他會員國為由而加以拒絕；如果某一成員國之主管機關業已窮盡各種可得之方法索取資料，但仍無法取得時，該成員國之主管機關得請求其他成員國之主管機關協助以取得資訊。草案第6 條則要求歐盟鼓勵業者自律，訂定準則或最佳行為規範以方便使用者更換服務商，以便專業之資訊使用者能在獲取更充分、詳細、透明之資訊之前提下，與資料儲存與處理之業者簽訂服務契約。草案第7 條則要求各成員國就草案所規範之事項設置單一連繫窗口以促進未來成員國之間以及與歐盟之間就相關事宜之溝通。

觀察上述草案，雖然該草案著眼於歐盟單一市場之整合，希望透過去除成員國間之法規壁壘等方式，加大歐盟內部單一市場規模，強化歐盟在數位經濟之角色，增加歐盟在資訊市場之產值；惟該草案涉及「資料在地化」立法廢除、擴大主管機關向民營業者索取資料之權力、迫使民營業者便利其等之客戶互相轉換服務提供商，在歐盟境內整合之阻力勢必不小，未來該草案是否能順利在短時間內完成立法亦值得觀察。

然若將該草案與甫生效之GDPR 綜合觀之，可知歐盟之企圖心不只在於建立「信任」、保護基本人權、提升歐盟境內之個人資料與人權保護，更在鞏固歐盟單一市場之地位，希望歐盟境內之自然人之個人資料能在高規格之保護下在歐盟境內自由流通，發展歐盟境內之數位經濟，同時也倡議「非屬個人資料之資訊」在歐盟境內自由流通，促進歐盟各成員國對於數位、資訊經濟之競爭，激發資訊與產品、服務間之加值效應，最終不僅係將歐盟建置為相較於世界其他各地而言，個人資料保護與人權保護較為完整、周全之數位經濟發展環境，亦希望資訊經濟、資料分析、處理、儲存等業者能在單一市場自由流通之環境下，發揮相輔相成之綜效。

叁、GDPR 給予數位經濟發展之空間

GDPR 加諸業者繁複之法遵義務，但亦有若干措施給予數位經濟某種程度之發展空間，茲試舉數例說明

之：

一、匿名化 (Anonymisation) 與去連結化 (Pseudonymisation)

(一) 匿名化 (Anonymisation)

承襲GDPR 之前身，歐盟個人資料保護指令，對於「匿名化」資料之看法與見解，GDPR 在前言第26 點明白宣示，個人資料保護之各項原則對於「匿名化」資料並不適用，而所謂「匿名化」資料意指與「已識別」或「可得識別」之個人無關之資料，或是經過匿名化處理而無法再藉以識別任何個資當事人 (data subject) 之資料，是以GDPR 並不適用於匿名化資料之處理，包含為統計或為研究目的所為之處理。匿名化資料一方面並不適用GDPR 之相關規範，得以自由處理與利用，另一方面，依照歐盟正在草擬之「非屬個人資料之資訊在歐盟境內自由流動之架構」，匿名化資料非屬個人資料，歐盟未來亦會致力於促進該等資料在歐盟單一市場內之流通。是以，如數位經濟業者能從「匿名化」之角度開發其業務，或許能降低其被控侵害他人個人資料或隱私之風險，亦能減少其在GDPR 下之法遵義務。

然而，個人資料如何進行「匿名化」？資料科學家以及資訊工程師等均表示個人資料要完全「匿名化」在現實上幾乎不可能。「匿名化」之概念在GDPR 誕生之前即幾經討論，歐盟 Article 29 Data Protection Working Party 在2014 年4 月10 日提出關於「匿名技術之意見」(Opinion 05/2014)。此份「匿名技術之意見」對於個人資料之「匿名化」提示若干重點如下：

第一、個人資料是否已經完全匿名化，歐盟個人資料保護指令並未採取科學上絕對無法識別個人之標準，而係以經匿名化處理之個人資料，在日後是否於「合理」之情況下無法再被識別為準，同時亦需考量在「資料開放」政策風行之下，個人可能在低成本之情況下再為識別之可能性。此一概念試圖在進行「匿名化」之努力以及「再為識別」所可能花費之時間以及資源之間取得平衡。

第二、有效個人資料「匿名化」之標準包括三要素：(1) 並未挑出單一之個人 (no singling out of an individual)、(2) 經過「匿名化」處理之資料與個人有關之記錄不再有所連結 (no linkability between records relating to an individual)、(3) 無法自資料再推論出與某位個人相關 (no inference concerning an individual)。

第三、所謂「匿名化」係指對於資料控管者 (Data Controller) 以及對於其他任何人而言，均無從識別。若資料控管者以單一事件 (Event) 為單位分類資訊，以僅僅抹去個人之姓名或識別碼之方式進行匿名化，效果仍然有限，控管者必須先將資料彙整，僅提供經過彙整之後之資訊，始該當匿名化資訊。

第四、當第三方接收到經適當匿名化處理之資料之後，由於該等資料已經無法識別個人，第三方於利用與處理該等資料之時，無需再遵守個資保護相關原則。

第五、將所蒐集來之個人資料進行「匿名化」時，仍然屬於個人資料之「處理」之一種，資料控管者在進行「匿名化」時仍應考量「目的限制」，亦即個資當事人對於個人資料處理之合法期待，是以「匿名化」仍然必須在蒐集之原始目的範圍內為之。

此份「匿名技術之意見」同時對於目前已知之資料匿名化處理技術加以討論與著墨，對於某些技術之使用與弱點加以提點與建議。未來此份文件仍將是在GDPR 架構下解釋「匿名化」資訊以及鑑別某項資料是否應被視為個人資料之重要參考依據。數位經濟發展如欲「擺脫」GDPR 沉重的法遵義務，應考量盡量蒐集與利用「匿名化」資訊。

(二) 去連結化 (Pseudonymisation)

GDPR 對於「去連結化」此一概念討論甚多，一般認為若資料控管者對於個人資料進行「去連結化」，將有助於其對GDPR 各種要求之遵循。GDPR 第四條第五款將「去連結化」定義為將個人資料處理之後，使得該等個人資料在無其他額外資訊之協助比對之下，無法再歸屬至任何特定之個資當事人，而該等「額外資訊」必須與經「去連結化」處理後之資料分別保存，同時應有組織上與技術上之措施以確保該等資料無法再指向任何「已識別」或「可得識別」之個人。所謂「額外資訊」之保存可以加密方式為之，亦應考量限制可以閱覽、使用該等「額外資訊」之人員之人數。應注意的是，「去連結化」之資訊對於資料控管者來說仍然係個人資料，GDPR 各條款仍然對其適用。然若採行「去連結化」，對於GDPR 之遵循，至少有下列益處，對於歐盟推動數位經濟亦有幫助：

第一、GDPR 第6 條第1 項 (f) 款，對於個人資料之合法處理事由，訂有將資料控管者以及個資當事人之利益加以權衡考量之所謂「正當權益」(legitimate interests) 之事由，亦即資料控管者可為其自身或

第三人之「正當權益」處理個人資料，但需權衡個資當事人之利益、基本權利與自由，而僅得於資料控管者或第三人之「正當權益」不為個資當事人之利益、基本權利與自由所凌駕時，始得為之；特別係在個資當事人係孩童之情況下。GDPR 第6 條第4 項對於非基於個資當事人同意而處理個人資料時，訂有利益權衡之考量因素，其中（e）項即為適當安全措施之採行，該等安全措施包含「加密」以及「去連結化」。

第二、GDPR 第25 條宣示從設計面保護個資以及個資保護應為原始設定之原則（Data Protection by design and by default），要求資料控管者在考量當時科技水平、實施之成本、個資處理之性質、範圍、情境、目的，以及對於個資處理對於自然人權利與自由可能造成之風險之下，在技術上與組織上採行適當之措施，以有效之方式將個人資料保護內建於處理程序之中。所謂之技術上與組織上適當之措施，其中之一即為對於所持有之個人資料「去連結化」。

第三、GDPR 第32 條揭示保護個人資料安全之基本原則，要求資料控管者以及處理者在考量當時科技水平、實施之成本、個資處理之性質、範圍、情境、目的，以及對於個資處理對於自然人權利與自由可能造成之風險之下，在技術上與組織上採行適當之措施，以針對可能之風險保護個人資料之安全，其中，個人資料「去連結化」即為GDPR 所舉出之技術上與組織上適當之措施之範例之一。

第四、GDPR 第33 條要求資料控管者於知悉個人資料侵害事故時，最遲於72 小時內通知歐盟之監管機關，除非資料控管者依照GDPR 所訂定之相關原則能證明該個人資料侵害事故對於自然人之權益與自由並無風險。GDPR 第34 條亦規定如該個人資料侵害事故對於自然人之權益與自由有可能造成風險時，資料控管者應立即通知個資當事人，而如資料控管者原已採行適當措施使所外洩之資料無從識別個資當事人時，該等通知義務得以豁免。若資料控管者於個資處理流程中採行「去連結化」措施，而所外洩之資料限於已「去連結化」之部分而不含得以重新識別當事人之資料時，資料控管者比較可能證明與主張個人資料侵害事故對於個資當事人之權益無影響或所外洩之資料無從識別個資當事人，而免除對於監管機關或個資當事人之通知義務。

二、取得當事人同意之方式

GDPR 第13 條以及第14 條要求資料控管者對於個資當事人所應履行之資訊揭露義務非常繁重，需告知個資當事人之資訊不但項目眾多，又要求告知個資當事人其等在GDPR 規範下所享有之諸多權利，加上歐盟以及成員國各自之法律規定，合乎歐盟規定之個人資料告知事項/ 隱私權政策不僅無法將其要義「一言以蔽之」，也相信沒有任何一位非專業人士之個資當事人有耐性與能力一一讀完。

幸好，GDPR 在取得當事人同意之「形式」方面之要求，並未如對於資訊揭露之要求一般複雜；一來並未要求以書面為之，也不要求以電子簽章或電子文件為之，如此數位經濟之業者可以利用在網頁上點選「同意鍵」方式取得當事人同意；二來在同意之實質內容上，並未要求資料控管者在取得當事人同意之前先對當事人諄諄教誨（要求個資當事人將冗長之個資資訊揭露事項讀完或對個資當事人口頭念一遍），只要將個資處理之目的講清楚、說明白，並告訴個資當事人其等有隨時撤回/ 撤銷個資同意之權利，即可取得有效之個資同意，至於冗長的個人資料告知事項/ 隱私權政策，只要提供網頁連結給個資當事人參考即可。此種取得同意之方式較為簡便，對於數位經濟業者來說較為容易遵循，也方便個資當事人對於個資蒐集之目的得以一目了然。

三、行使當事人權利之例外

GDPR 第15 條至第23 條，賦予個資當事人諸多基本權利，乃係本次GDPR 傲視全球之亮點之一。該等當事人權利包括：個資當事人近閱權（Right of access by the data subject）、更正權（Right to rectification）、刪除權/ 被遺忘權（Right to erasure/ right to be forgotten）、限制處理權（Right to restriction of processing）、資料可攜權（Right to data portability）、拒絕權（Right to object）、對於個人之自動化決策與側寫（Automated individual decision-making, including profiling），對於個資當事人之保護十分周全綿密。

同時，GDPR 也鼓勵採取去連結化、加密或其他技術上或組織上之措施，以保護個人資料之安全，因此，企業在處理利用個資之過程中，很有可能已經將部分個人資料匿名化，而有再識別之困難。若此時個資當事人回過頭來要求行使上述個資當事人之權利，例如目前最著名之「被遺忘權」，難道資料控管者此時應該將已經除去識別資訊或匿名化之資訊再度識別，以方便個資當事人行使「被遺忘權」？若答案為肯定者，則不啻減低企業以匿名化方式處理個人資料之動力，亦提高數位經濟業者進行資料分析之成本與風險。

關於此，GDPR 第11 條規定，於資料控管者處理個資之目的不再需要識別個資當事人之時，資料控管者並無義務僅僅為了遵循GDPR 各種規範之目的，繼續保存、取得或處理額外得以用來識別該等個資當事人之資訊。此時，如有可能，資料控管者應將上情通知個資當事人。在此情形下，GDPR第15 條至第20 條個資當事人之種種權利即不再適用，除非個資當事人自行提出額外資料以便得以再識別該名個資當事人。GDPR 前言第57 點表示，若資料控管者所處理之個人資料並不允許資料控管者識別某一自然人，該資料控管者無庸為了遵循GDPR 下之義務，另行取得額外資訊以資識別某一自然人；然而，若個資當事人主動提供相關之額外資訊，資料控管者亦不應拒絕協助個資當事人進行再識別。有關之識別資訊包含數位識別，例如以過去個資當事人登入資料控管者所提供之線上服務所需之資訊等，作為識別之方式。

上述規定應係在「當事人權利之行使」，「資料控管者進行匿名化、去識別化所為之努力」，與「再識別所需耗費之成本與資源」等之間，所為之利益權衡，正好可以在數位經濟之發展，以及GDPR 繁重之法律遵循義務之間，有所平衡與調適。

四、對於微型、中小企業之放寬措施

數位經濟之誕生與崛起，都會經過微型企業、中小企業這段過渡期，歐盟制定 GDPR，意圖對於微型企業、中小企業，提供較為寬鬆之法律管制。GDPR 前言第167 點要求歐盟執委會在行使GDPR 所賦予之權力時，應考量針對微型企業以及中小企業採取特定之措施。GDPR 第40 條要求成員國、監管機關、歐盟執委會等應鼓勵建立為適用GDPR 之行為規範（Code of Conduct），並要求其等考量微型企業以及中小企業之特殊需求。GDPR 第42條要求成員國、監管機關、歐盟執委會等應鼓勵個人資料保護認證措施之建立，特別是在整個歐盟之層次上，考慮建立該等認證措施，包含個人資料保護標準等等，而在建立相關認證措施時，GDPR 亦要求對於微型企業以及中小企業之特殊需求加以考量。

除了在執法層面以及在行為規範、認證措施等面向考量微型企業以及中小企業之特殊需求以外，GDPR 具體豁免微型企業以及中小企業之法律遵循義務，在於以員工人數是否達到250 人為標準，決定一企業是否應該依照GDPR 第30 條規定，對於企業之個人資料處理活動保留紀錄。GDPR 第30條對於企業處理個人資料所應保留之活動紀錄訂有詳細的規定與要求，為符合該條規定，企業必須為其處理個人資料之活動保留下列資訊：

- (一) 資料控管者之姓名以及連絡方式；
- (二) 處理資料之目的；
- (三) 個資當事人之類別以及個人資料之類別；
- (四) 個資被揭露之對象之類別，含位於第三國者或國際組織；
- (五) 個資傳輸至第三國或國際組織者，第三國或國際組織之名稱，依GDPR所要求採取的適當保護措施相關之文件；
- (六) 各種不同類別之資料預計可能之刪除時限；
- (七) 依GDPR 所要求採取的技術上與組織上之措施之簡述。新創企業之員工人數應遠低於250 人，得以豁免上述繁複之記錄義務，可節省不少資源，集中力量發展數位經濟。

肆、結語

綜上所述，GDPR 闡述與擘劃對於個人資料、隱私、人權保護之崇高藍圖，畢竟「科技始終來自人性」，來自於個人者終將回歸至個人，能取得個人之信任與信賴，數位經濟才有沃土繼續茁壯成長，若任由個人資料或隱私遭到濫用，可能造成意想不到之後果，不可不慎。歐盟在利用GDPR 提高個人資料保護水準並統一成員國間對於個人資料保護制度與法規之歧異之同時，亦著眼於個人資料在歐盟單一市場內之自由流動，以及歐盟整體數位經濟之發展，兼以計畫更進一步推動與促進歐盟境內「非屬個人資料」之流通、分析與發展之相關措施，企圖心可見一般。

GDPR 繁重之法律遵循義務造成業者不小之負擔與壓力，在推行之初，法規解釋之不明確確實對於企業經營造成風險，目前全世界仍在觀察中，而在GDPR 之條文中存有若干可能對於數位經濟發展有利之措施，或許並沒有想像中便利與廣泛全面，但仍某程度展現GDPR 之規範方向，數位經濟業者可考量並利用。歐盟以上作法未必係個人資料保護與數位經濟發展最佳之調適方式，但仍值得參考借鏡，讓我們拭

目以待。

（以上為作者個人意見，未必代表理律法律事務所之立場或主張）