歐盟新規：個人資料保護規則 — 數位防護的新縱深

林思惟/金融聯合徵信中心 研究部經理

由於歐盟會員國在個人資料保護相關法律缺乏一致性的架構，以及近年來雲端計算、行動互聯網、大數據等資訊科技的快速發展，對個人資料保護帶來新的議題與挑戰，歐盟對1995年立法「資料保護綱領 (EU Directive 95/46/EC: the Data Protection Directive)」進行大刀闊斧的改革。歐盟執委會自2012年1月提出資料保護改革草案以來，其嚴苛的規範撼動資訊科技界的巨擘於歐盟經營的根基，紛紛投入龐大的資源向歐盟當局進行遊說，歐洲議會共計收到四千多份相關修正意見，經過4年多的討論，歐洲議會終於在2016年4月27日通過歐盟規則2016/679，亦即「個人資料保護規則（the EU General Data Protection Regulation，以下簡稱GDPR）」，此規則自2016年5月24日起生效，並取代歐盟1995年的 「資料保護綱領」。新法規定2年過渡期，直到歐盟各成員國均實施GDPR，才自2018年5月25日起全面施行新法。

GDPR不僅適用於歐盟地區註冊的企業，非屬歐盟企業組織但在歐盟境內營運，蒐集、處理或利用歐盟人民的個人資料者，須適用本法。此外，GDPR除了提升個資保護強度，且大幅提高了罰款金額上限法規，最高可處罰鍰 2 千萬歐元或年度全球總營業額 4% 的金額。由於GDPR與信用報告機構之營運關係密切，歐盟消費者信用資訊業協會(Association of Consumer Credit Information Suppliers，簡稱ACCIS)[1]亦投入相當人力與資源，針對信用報告產業的特殊議題，積極進行遊說。

一、GDPR修訂重點

1 消費者信用資訊業協會 (ACCIS)，成立於西元1990年，原始註冊地為愛爾蘭首府都柏林，成立宗旨為結合歐盟地區之消費者信用報告機構力量，設定主要共同利益與優先順序，於整體歐盟層次與各國層次，積極影響並遊說有利於會員經營之法制環境，使會員在國內外持續發展業務；並設定重要議題，以信用報告機構之利益與觀點，透過各項跨國合作之專案研究，提供行政部門在制定管制信用報告機構之相關政策時參考。
2006年該協會改制，在比利時登記為國際性非營利組織，總部設於比利時布魯塞爾。目前該組織正式會員有42家位於歐盟地區之信用報告機構(分布於28個國家)，另有6個非正式之非歐盟會員(Associate Member)，分別為：我國(金融聯合徵信中心)、中國大陸(中國人民銀行徵信中心)、墨西哥(Buro de Credito TransUnion de Mexico SA SIC)、泰國(National Credit Bureau Company)、美國(MicroBilt Corporation)、荷屬加勒比海群島(Caribbean Credit Bureau N.V.) 。2016年起，ACCIS增加另一類會員：聯盟會員(Affiliate Member)，目前僅有FICO公司一家。

（一）提升法律位階：由Directive 提升爲Regulation

歐盟在1995 年制定的資料保護綱領（Directive）僅係依歐盟地區廣泛共通的法律框架與指導原則，歐盟各會員國可依各國之情況，制定各國的資料保護之法規與措施，也因而造成了歐盟地區各會員國對資料保護之程度仍存在極大的差異。而GDPR之法律位階屬於Regulation層級，已經過歐洲議會（European Parliament）與歐盟理事會（European Council）的議決，將直接適用於歐盟各會員國，而不再需要透過會員國國內法的轉換，2018年5月直接適用各成員國，這將徹底解決成員國之間的法律制度差異問題，此一改變將降低跨國企業的法規遵循成本，且僅需接受單一的監理機構之監管(One stop shop)。歐盟亦將成立統一之「歐盟資料保護委員會(European Data Protection Board，EDPB)」，藉由發佈意見(opinions)、準則(guidance)、建議等(recommendations)，維持歐盟地區資料保護制度之跨國一致性。

（二）擴大適用範圍Expanded territorial scope

1995年資料保護綱領適用屬地原則，如果企業提供跨境服務，但並未於歐盟地區設立，則可規避歐盟法律。在GDPR的規範，即使資料控制者於歐盟境內沒有設立機構，但其在跨境提供商品或服務的過程中，蒐集處理歐盟居民個人資料，則應當適用GDPR之規範，並需要在歐盟境內指派特定代表負責法令遵循事宜。這一規定將影響大多數資訊科技巨擘(如微軟、Google、Facebook等)。

（三）企業必須設置「資料保護長Data protection officer，DPO」

為確保企業(條文所稱「資料控制者 data controller」或「資料處理者data processor」)之有效遵循法規，GDPR歐盟要求如果企業員工超過250人，且核心業務涉及到對歐盟居民的資料處理，大型企業必須設立資料保護長(DPO)。此一職位並必須有效依法履行職責，若企業違反GDPR之規範，DPO將被追究法律責任。

（四）資料蒐集與處理須取得明確有效同意

1995年資料保護綱領並沒有規定同意應當是「明示同意」還是「默認同意」。 GDPR規範企業負有保護資訊蒐集更加透明化的責任，所以企業必須獲得用戶之同意，該同意必須由資料當事人自主的授予(freely given)、具體(specific)、知情(informed)以及明確(unambiguous)，方能取得並處理個人資料，尤其針對敏感性資料(sensitive data)更必須明確清楚(explicit)，企業必須能夠證明已取得資料當事人之同意，當事人保持沉默、未表示意見或無作為情形，皆不構成前述「同意」，兒童或青少年個資之取得及處理，須事先獲得父

母或監護人同意。既有同意若符合GDPR的要求，則仍然有效。且企業必須提供資料當事人以簡單的方式，撤回授權企業取得與處理個人資料的同意，用戶個人資料被取得後將被用在什麼用途，也必須清楚直白地說明陳述。

（五）個人資料可攜權Data portability

GDPR除了規範企業，也使歐盟公民能對自己的個資擁有更大的操控權，包括「資料可攜權」，也就是在不同服務間移動個資的權利，用戶可以將其個人資料以及其他相關資料從一個網路服務供應商（ISP）轉移至另外一個ISP(例如將所有連絡人資料和郵件從Google移動到Yahoo)。

（六）個人資料外洩通報Data breach notification

GDPR規定，企業(含資料控制者或資料處理者)若發生個人資料外洩事件(data breaches)，必須於知悉後72小內通報其資料保護主管機關(Data Protection Authority)，且若對資料當事人之權益有重大危害之虞，雖未明確規範期限，惟亦應及時(without undue delay)通知資料當事人。

（七）IT系統之資料保護設計Data protection by design and by default

企業為了提供產品和服務，必須蒐集與處理個人資料，除須符合明確同意等規範外，亦必須遵循個人資料蒐集最小原則(data minimization)，GDPR亦將「個人資料」擴大解釋為涵蓋可直接或間接過濾出特定對象資訊之資料類型，例如網路瀏覽器Cookies、網路IP位址或足以辨識特定個人身分或性別之基因、生物特徵或醫療資料等。且GDPR引入「資料保護設計(Data protection by design and by default)」制度，亦即企業於新資訊系統建置與設計時，即應將資料保護之設計納入考量，亦即各類產品或和業務線，在業務設計的最初階段，就需要與IT廠商充分協商，並通過技術、合約、管理等措施落實遵循GDPR之要求。

（八）被遺忘權Right to be forgotten

被遺忘權（Right to be forgotten）是新的保護規則的另一大重點。增加被遺忘權利的目的，旨在賦予個人可更有效的控制其個人資料。在1995年資料保護綱領即規範了資料當事人除可要求查閱、複製資料控制者所擁有的個人資料，若該資料有不正確、不完整時，可要求更正、刪除或封鎖（rectification, erasure or blocking），GDPR更進一步提出被遺忘權的規範，亦即認為除了資料不正確或不完整外，有其他理由時(例如：非法處理個人資料、資料當事人同意已經撤回等六種情況)，個人均可要求刪除控制者所掌控之個人資訊。在此之前，歐洲法院已有判例裁定個人可以要求搜尋引擎(Google)從包括「不相關」或「過期」的個人資訊結果中移除連結。

（九）反對權（Right to object）

在GDPR，個人反對權（Right to object）與「被遺忘權」，乃是不同之權利。個人反對權係資料當事人有權，在特定情況下，反對資料之處理，除非資料控制者證明處理該資料有重大正當理由，勝過資料當事人之基本權利與自由。當資料當事人提出反對時，資料控制者應立即停止處理該個人資料。反對權亦適用於以大量個人資料所自動化產生之「描繪（profiling）」活動，亦即，資料當事人有權瞭解一項特定服務是如何做出特定決策的，此一規範將對以大數據為基礎，運用機器學習、人工智慧技術進行資料分析與研判的服務(例如，Facebook 透過演算法提供客製化資訊內容)，將形成重大挑戰，畢竟類似「黑盒子」的機器學習技術很難適用「反對權」。

（十）對自動化決策之限制

GDPR對於以大量個人資料所自動化產生之「描繪（profiling）」進而進行決策有諸多規範。自動化決策之概念係指：以自動化方式處理個人資料的分析與預測活動，而產生對資料當事人包括工作表現、經濟狀況、位置、健康狀況、個人偏好，可信賴度或者行為表現等之判定。GDPR規定：「描繪（profiling）」必須具有法定依據或者獲得用戶明確同意；用戶必須是在充分知情下做出同意授權；不得針對敏感議題(例如：種族、政治立場、宗教信仰、性取向等)進行。

（十二）資料保護影響評估(Data Protection Impact Assessments，DPIA)

GDPR 要求企業必須進行「資料保護影響評估(Data Protection Impact Assessments，DPIA)」，用以辨識業務活動中涉及個人隱私權利的風險，並加以衡量、管理與因應，並於蒐集與處理個人資料前，評估該等風險與業務活動必要性與對稱性。DPIA與許多企業已實施之「隱私影響評估(Privacy Impact Assessments，PIAs」類似，惟PIAs並無明確的規範與定義，DPIA則強化了其內涵與一致性。

（十二）大幅提高罰則金額

GDPR大幅提高違規罰款的金額，依違反情節給予不同程度的罰款，例如：沒有合法理由，拒絕用戶刪除個人數據請求，沒有建立企業對用戶數據保護的文件化管理，最高將被處以1000萬歐元或全球營業總額的2%的罰款；第三類違規行為：非法處理個人數據；沒有合法理由，拒絕用戶關於停止處理個人數據的請求；在數據洩露事故發生之後，沒有及時通知監管機構；沒有執行隱私風險評估；沒有任命數據保護官，違法向第三國傳輸個人數據；最高將被處以2000萬歐元或全球營業總額4%的罰款。

二、ACCIS對GDPR之關注焦點及GDPR立法結果

GDPR與信用報告機構之營運關係密切，自GDPR於2012年啓動修法工程起，ACCIS即投入相當人力與資源，針對信用報告產業的特殊議題，積極進行遊說。並對業界重大議題，以ACCIS名義，提出說帖(Response to the proposal for a General Data Protection Regulation–Perspective of Credit Reporting Agencies)，並積極進行遊說，長達四年的努力，成果大致符合ACCIS的預期。其重點如下：

（一）企業之「合法利益」仍列爲得以處理個人資料之要件之一

1995年制定的資料保護綱領（Directive）第7條(Article 7)規範了企業得以處理個人資料的6項要件，其中(f)項允許在企業追求其「合法利益(legitimate interests)」之範圍內，可以作為處理個人資料之依據。在GDPR的立法過程中，此一規定引發相當程度的討論，許多消費者保護團體主張企業「合法利益(legitimate interests)」定義與界線並不容易認定，企業可能過分主張其「合法利益」而犧牲了資料當事人的權利。ACCIS針對此一議題，積極主張應予保留。GDPR最終結果：未將「合法利益」刪除。

（二）對「合法利益」之反對權(Right to Object)之限縮

GDPR立法階段曾將「合法利益」列為資料當事人行使「反對權」的重點，並設計極為嚴苛，對信用報告機構業者極為不利的規範(例如：一經資料當事人反對，信用報告機構即刪除，或應停止對其個人資料的處理與利用)。GDPR最終結果：未將嚴苛之「反對權」行使規範納入。

（三）對自動化決策之「描繪（profiling）」活動不強制人工介入

GDPR對於以大量個人資料所自動化產生之「描繪（profiling）」有相當程度的疑慮，而信用報告機構所提供之「信用評分」服務類似於profiling之概念，若所有信用評分結果都必須經人工審視，在實務上，對十分重視即時回應的信用交易十分不利。GDPR最終結果：未將人工介入之強制性要求納入。

（四）移除對敏感性資料的限制使用

GDPR原有意定義特殊類別的個人資料(special categories of personal data)，諸如：性別、法院或行政判決等，並限制不得處理使用。由於法院判決與行政裁罰資料長久以來為信用報告機構所蒐集與提供，且該項資訊對於金融機構避免消費者過度負債(over-indebtedness)有極大之助益。GDPR最終結果：未限制法院判決與行政裁罰資料之使用。

三、GDPR對信用報告機構之影響

GDPR除加強個人資料保護的強度之外，亦使歐盟28成員國資料保護規定獲得統一，可望減少跨國企業在遵守各成員國資料保護規定上之不便情形，由於其適用範圍對象涵蓋非歐盟國家之企業，在立法階段，即引發全球性資訊巨擘與跨國大企業的高度關注，藉由商業全球化、網路化的發展，個人資料的跨國蒐集、處理與傳遞在所難免，而GDPR的實施，首波衝擊將影響與歐盟市場往來密切的商業活動（主要為美國企業）帶來巨大的衝擊，進而擴及至全球其他與歐盟有經貿往來之區域。

以信用報告機構經營的角度而言，雖然ACCIS在GDPR立法上的遊說成果，大致保住了既有的經營基礎，但GDPR於2018年的正式實施，仍對信用報告業者帶來許多不確定性的因素。

（一）各會員國資料保護程度的差異有待解決

GDPR跨國一致性的規範，將凸顯各國現有資料保護程度的差異，而歐盟層級的「歐盟資料保護委員會(European Data Protection Board，EDPB)」，亦將徵詢各國的實務，藉由發佈意見與準則(opinions and guidance)，補充GDPR未明確規範的空間，以利GDPR跨國一致性的執行。

（二）信用報告機構之可歸責性(Accountability)增加

在GDPR的規範下，信用報告機構不論擔任資料「控制者(controller)」或是資料「處理者(processor)」的角色，其「可歸責性」將更為清楚，違反規定所付出的代價將更高，因此信用報告機構應建立遵循GDPR要求之內部健全的管理與控制機制，並證明該機制可有效運作。

（三）資料當事人權利(Data Subject Rights)之行使

GDPR新增了許多保護資料當事人權益的規範，例如：個人資料之刪除與更正；資料可攜權Data portability(企業必須免費提供完整的電子檔案資料)；個人資料處理的通知等，在信用報告機構的現行運作中，皆已有一定遵循機制，例如：接受資料當事人對信用資料的爭議及後續處理；資料揭露期限的訂定；(免費)信用報告的提供等，惟是否符合GDPR之要求，信用報告機構業者應進行盤點與比對，若有不足之處，擬訂改善計畫並與監理機關密切溝通。

（四）只是開始，不是結束

在「合法利益」、「被遺忘權」、「反對權」、「特殊類別的個人資料」等議題，雖然信用報告機構業者在GDPR的立法中占了

上風，但該等議題已引發各界的關注，後續可預期將有更多消費者保護團體針對此等權利提出「是否濫用」的質疑，「歐盟資料保護委員會」亦將密切注意其發展，任何一個會員國資料保護主管機關(Data Protection Authority)所作的決定，都可能影響整體歐盟，信用報告機構宜小心應對。

四、GDPR對我國信用報告機構發展之啓發

個人資料保護的立法概念，一般偏重於保護社會大眾與相對具有權力與經濟優勢之公務機關或私人企業往來時，其個人資料之合理運用與隱私權利的適度保障。若將此種消費者保護概念，應用於民眾與金融機構往來希望能以合理的條件取得所需信用的情境中，則產生諸多值得特別深入探討的面向。

在信用交易市場中，「信用需求者」與「信用供給者」之間存在之資訊不對稱，是阻礙信用交易效率進行的最大障礙，「信用需求者」必須提供足以供「信用供給者」評估信用風險所需之資料，以換取從「信用供給者」取得信用的機會。

當「信用供給者」為金融機構時，由於金融機構授予「信用需求者」之資金係來自於社會大眾的存款，金融監理機關基於金融穩定的考量，對金融機構的信用風險管理會訂定較高的標準，並以監理手段要求銀行確實遵循。除此之外，監理機關亦可能透過法制的設計與安排，設立專責跨機構蒐集與提供信用資料的「信用報告機構」，以提升銀行對「信用需求者」信用資訊可蒐集的廣度與深度；於此情境下，有信用需求之個人必須犧牲較多的個人資料保護程度，甚至必須放棄某種程度之「被遺忘權」，以換取使用社會大眾存款的機會，以及整體金融信用體系的健全發展，進而建立公平合理的信用市場紀律。

財團法人金融聯合徵信中心(以下簡稱聯徵中心)即循上述概念，在「銀行法」、「銀行間徵信資料處理交換服務事業許可及管理辦法」的法規安排下所設立之非營利性財團法人機構。聯徵中心採「會員制」管理，透過「會員規約」(目前會員僅限經許可設立之金融機構，包括：銀行、信用合作社、票券金融公司、證券金融公司、農會信用部、漁會信用部、信用卡公司、經營授信業務之保險公司等)，經營會員機構信用資訊之蒐集、處理與交換之特許業務，以解決「信用需求者」與「信用供給者」之間存在之資訊不對稱的癥結，經逾四十年的運作，個人資料保護與授信管理目的個人資料分享，大致維持均衡與穩健。

如今，隨著數位科技的發展，「普惠金融（financial inclusion）」得以快速發展並有效實現，模糊與動搖了原本牢固封閉的金融領

域。「普惠金融」的目標為讓經濟地位弱勢者(即：無法獲得金融服務者unbanked，以及金融服務不足者underbanked)，藉由取得與享用完整的金融服務(存款、匯款、貸款、保險、理財等現代經濟活動所必須之服務)，達成脫離貧窮的實質目的，其方式為透過金融科技大幅降低提供金融服務成本與門檻，提升對經濟活動的相對弱勢者金融服務的深度與廣度，而不論該種金融服務之提供係來自於傳統金融機構，或來自於非金融機構的科技業者，數位化個人資料廣泛的蒐集處理與利用皆為必要的途徑，而在現今的資訊科技環境下，個人資料之保護運用，亦變得十分複雜與棘手，此即歐盟訂定GDPR的主要背景。

傳統信用報告機構所蒐集、使用之信用資料，係以資料來源清楚可信、資料定義明確的結構化資料為主；而新型態信用報告服務提供者所使用之數位資料，其資料範圍廣泛、資料面向多元、資料即時且動態，加以處理大量資料之分析方法之日益成熟，藉由多維度資訊彼此的關聯性來描繪資料主體之信用狀況，已實質改變傳統信用分析之既有框架。

但新型態信用報告服務提供者所大量使用之數位資料，除了須面臨資料缺乏一致性客觀定義、資料的變動並未經嚴謹的更新與更正程序、資料操弄與作假疑慮及資料與信用良好與否的相關性難以驗證等先天性課題外；在應用大數據資料之情形下，若資料當事人引用前述歐盟GDPR行使「被遺忘權」或「反對權」，或質疑大數據可能帶來的「資料獨裁問題」（意指：在大數據的環境下，透過人工智慧技術，根據數據分析將人群進行分類與標籤化)，亦會產生GDPR所至為關切的以資料進行被分析對象的「描繪」與資料當事人之「反對權」議題。

在數位資訊科技一日千里的高度動態環境中，「資料保護」與「普惠金融」兩種概念的相互碰撞，激起了跨領域之監管議題，政府不同部門間對於數位科技所帶來全新的便利與威脅，雖必然存在不同立場的觀點，但監管者都必須強化對數位科技的認識，在一定程度的專業理解下，進行跨部門的溝通與論證，甚至應用數位科技強化監管的效率與效能，亦即「法遵科技(RegTech）」的新概念。除此之外，任何監管措施實施之前，亦應充分與被監管者進行有效的溝通，在可控制的範圍內進行試作，透過實際操作，確實瞭解科技運用的潛在風險與威脅，並以風險為基礎（risk-based），設計有效且精準法規遵循與金融監理措施，實質降低被監理者法規遵循之負擔，此即為「監理沙盒(Regulatory Sandbox)」的概念。

雖然GDPR的實施及歐盟地區信用報告機構的發展對於聯徵中心無明顯或立即的影響，惟從GDPR的修訂或觀察目前影響全球或歐盟

信用報告業發展的重大趨勢，皆可發現資訊科技發展所帶動的數位化、網路化、行動化、雲端化所產生之個人資料保護與使用議題、資訊跨國傳遞與金融跨國監理議題等，早已成為信用報告業者之關注焦點；聯徵中心仍應未雨綢繆，瞭解國際趨勢，針對個人資料保護等相關議題預作研議，俾於未來議題形成與討論階段，以公益性信用報告機構之立場，向政策制定部門提出妥適之建議，以當事人權益為優先考量之前提下，兼顧我國信用報告機構之健全發展。