長庚人文社會學報
15:2(2022),177-214

數位人權保障研究——以歐盟個人資料保護規則為例

高佩珊*

摘　要

為適應網路科技與大數據 (big data) 時代的來臨，加強對於歐盟民眾個人資料保護與數據傳輸之限制，歐盟於 2018 年 5 月 25 日正式實施《個人資料保護規則》(General Data Protection Regulation，簡稱 GDPR)。相較於歐盟 1995 年提出的《資料保護指令》(Data Protection Directive)，GDPR 對於民眾資料保護提出更加嚴格之規範，且增加高額違規罰款。依據該規範，凡在歐盟營運的所有公司與企業，無論其總部設於何處，皆須遵守此規範；此法規不僅對於跨境資料傳輸與數據蒐集設有嚴格規範，同時具有區域外影響力。儘管被視為史上最嚴格之隱私法規，歐盟亦說明該規範並不包含個人在家中進行處理之有關個人數據與資料，如果該行為與專業或商業活動無關。但若在個人範圍之外，使用民眾個資進行社會文化或金融活動時，則皆需遵守 GDPR。因此，本文將以歐盟數位人權保障研究為題，以做為個案研究，探究歐盟隱私保障法規發展及此個資保護規則重要實施內容，及其實施後所面臨之困難與挑戰，最後綜整結論。

關鍵詞：歐盟、隱私權、數位人權、數據安全、個人資料保護規則

---

* 作者為中央警察大學公共關係室主任，同時為該校國境警察學系暨研究所副教授，Email: pkao@mail.cpu.edu.tw。本文首次發表於中央警察大學「2020 移民事務與國境管理學術研討會」，感謝評論人為本文提出的寶貴意見。

一、前言

2018 年 3 月爆發臉書 (Facebook) 用戶數據遭英國劍橋分析 (Cambridge Analytica) 公司取得和不當使用，[1] 造成大批民眾個人資料與數據外洩。[2] 一時之間，「數位人權」、「資訊安全」(information security) 、「隱私權」(right of privacy)、「資料安全」(data security)、「個資保護」(data protection) 等字眼，成為時下討論最熱門的關鍵字。[3] 關於資料安全，尤其是數位資料的保護，向來注重民眾隱私權 (privacy) 保障的歐盟對於民眾資料之保護與防範早有規範，除不斷強調個人資料保護對於國家安全與社會、經濟發展之重要性，亦不斷呼籲各國必須加速對於民眾個人資料分享的限制，提出嚴格立法規範。面對網路無國界和數據時代的來臨，歐盟從數位人權角度出發，對於跨境資料傳輸與民眾資料蒐集與使用設下嚴格規範，不僅要求「資料在地化」(data localization)，[4] 更以法規限制和禁止跨境傳輸民眾個人資料。[5]

---

1 總部位於英國倫敦的「劍橋分析」公司成立於 2013 年 12 月 31 日，主要營運項目為在全球進行資料 探勘與數據分析。劍橋分析公司因外洩民眾資料遭到政府部門調查，於 2018 年 5 月宣布停止營運和申請破產。關於該公司之介紹可見其官方網頁 Cambridge Analytica (2016), Cambridge Analytica: Data-driven behavior change. Retrieved Jan 11, 2021, from https://cambridgeanalytica.org/

2 此事件造成臉書受到英國及美國國會部門的傳喚與調查，執行長祖克柏 (Mark Zuckerberg) 甚至兩度要求赴美國國會聽證。參見陳正一，〈祖克柏國會作證為個資外洩醜聞道歉〉，《中央社》，2018 年 4 月 11 日。請見 http://www.cna.com.tw/news/firstnews/201804110011-1.aspx。

3 「個資保護」(Data Protection) 意指對於重要資料和資訊的保護、保全過程；隨著高科技的迅速發展與網路時代的來臨，建立和儲存於網路的資料大量快速增加，更加突顯資料保護的重要性。

4 「資料在地化」要求業者將處理資訊所需的伺服器及資料儲存於境內。對於跨境資料傳輸設置限制；例如，俄羅斯全面禁止跨境資料的自由流通，韓國與澳洲等國則於特定範圍內禁止或有條件允許跨境自由流通，美國則未禁止跨境資料的自由流通。參見陳文生 (2016)，〈資料在地化政策與個人資料保護議題〉，《財團法人中華民國國家資訊基本建設產業發展協進會》，2018 年 4 月 11 日。請見 http://www.nii.org.tw/Recents/Detail/74。

然而，對於美國和某些國家而言，數據資料的跨境傳輸某種程度具有重要經濟戰略意涵，倘若要求資料在地化，資料經濟可能會因此受到束縛，亦會使提供網路通訊與電信服務的業者感到相當困擾。對於歐盟而言，正因數位時代的來臨使得政府在跨境數位資料傳輸中的角色遭到稀釋，對於個人資料的保護與要求資料在地化或可適時彰顯政府在民眾隱私保障、國家安全與企業商業利益之間力圖維持平衡。因此，如何在資料經濟盛行與網路無國界時代下，保障民眾隱私與數位人權，同時又能兼顧國家安全與商業經濟利益，成為各國政府亟需思考之重要議題。[6] 因此，本文將以歐盟 GDPR 做為個案研究，輔以文獻探討探究歐盟個人資料保護法規之演變，再分析歐盟據此執行資料保護規範與限制跨境資料傳輸時可能遭遇之困難，冀能提供我國執法機關未來制定科技偵查法等相關政策時參考。

二、重要文獻探討

民眾個人資料之蒐集及使用，不僅涉及個人權利保障與政府執法所需等個人利益與公共利益之間的衡平，同時涉及社會經濟發展利益。迎接大數據與雲端時代的來臨，如何保障民眾數位人權同時兼顧國家安全與商業利益，各國政府各有不同考量與規範。國內外學界對此議題亦分別從民眾隱私權、網路經濟、跨境執法等不同面向，提出許多寶貴看法與觀點。例如，外國學者 Voss (2017) 在他所著的〈歐盟資料

5 具體作法除資料在地化之外，還包括設立法人、多種落地合併的許可、國際條約等，參見鄭美華 (2017)，〈數位經濟時代下的非關稅障礙〉，《NCC News》，10(11)，頁 21-22。

6 曾怡碩 (2014)，〈公私部門的雲端監偵——隱私權 / 營業秘密與國家安全／商業智慧之間的角力〉，《前瞻科技與管理》，4(2)，頁 65-67。

隱私法規改革：個人資料保護規範、隱私盾和刪除權〉(European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting) 文章中，討論近代歷史上歐洲資料隱私法規的發展。[7] Voss 在該篇文章以 2014 年 Google 案件在西班牙判決為例，討論「刪除權」(right to delisting) 的後續發展，以及 2018 年 5 月開始適用的歐盟 GDPR。Voss 指出，歐盟隱私新法規 GDPR 不僅擴大法規適用區域範圍，亦改變個人資料處理原則。該法不只要求企業和公司採取行動以增加資料主體 (data subject)，即消費者，以及資料擁有者的權利，並提出新的規則；包括要求公司進行資料保護衝擊評估和聘僱「資料保護官」(Data Protection Officers)。此外，GDPR 亦詳細規定新的資料紀錄保留義務，以及資料洩露時需進行通知的新要求和裁罰更高的行政罰款。

然而，Voss 認為歐盟 GDPR 中的這些新規定，不只要求公司遵守法規義務，承擔更大的責任保持資料紀錄，某些規定可能還需要調整企業團體的內部組織；例如，設立「資料保護官」(DPO)、建立「資料保護衝擊評估」(Data Protection Impact Assessment) 和允許適當的「資料揭露通知程序」等。該篇文章亦以英國 1998 年的「資料保護法」(Data Protection Act 1998) 為例，說明該法要求企業對於所保存的民眾個人資料紀錄必須提高警覺並審查隱私聲明，以符合歐盟要求。此外，「個人資料保護規則」亦要求企業必須確認營運時，是否涵蓋所有資料主體的權利並對其進行調整，以適應資料主體之請求，同時確定處理資料的法律依據，實施年齡驗證並取得父母或監護人之同意。此外，企業亦須執行有關資料外洩的程序，並在需要時指定資料保護官，確定

[7] Voss, W. Gregory. (2017), "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting," *Business Lawyer*, 72 (1): pp. 221-233.

任何適用的監管機構。如果進行跨境傳輸民眾個人資料時，企業需依據美歐「隱私盾」協議進行自我認證，並關注有關民眾資料「刪除權」的後續發展，以免影響網路訊息的進入和訪問。

Voss 與另一位學者 Houser (2018) 在他們共同發表的〈GDPR: Google 和 Facebook 的終結或資料隱私新模式？〉(GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?) 一文當中指出，歐盟資料保護機構近年來雖然針對美國科技公司違反區域和國家資料保護法規而進行加強執法；然而，卻依然很難改變一直以來美國公司將個人資料作為免費交換的商業模式。兩位學者認為劍橋分析公司因為外流臉書用戶數據而宣告破產一事，顯示美國隱私保障法規的不足。因此，兩位學者在該篇文章中，試圖解釋美國與歐盟兩地對於隱私和資料保護法規之差異，以及雙方因為意識形態差異所導致的執法行動分歧。兩位學者建議美國公司應做出改善，以便能更加合法的處理和使用歐盟境內民眾的資料。因為美國企業如果無法符合歐盟自 2018 年 5 月 25 日開始實施的 GDPR 規範內容，由於該法規具有域外適用性，可能導致企業遭受高達 40 億美元的罰款。

因此，Voss 與 Houser 認為歐盟 GDPR 的實施，會改變一直以來在美國相對寬鬆的隱私法規下經營的美國企業的商業模式。兩位學者欲瞭解這種新的商業模式是否會導致 Google 與 Facebook 的終結，亦或是因此能為美國企業的經營建立黃金標準，帶來新契機？對此，Voss 與 Houser 的研究發現，美國和歐盟的法律及執法行動最主要的不同在於，歐盟認為保障民眾資料隱私乃不可剝奪之權利；但在美國，甚至連美國憲法都未提及隱私權。Google 西班牙一案證實，美國和歐盟在隱私權保障與言論自由上，存在基本的意識形態衝突。Voss 與 Houser 指出，歐洲向來重視「隱私權」和「被遺忘權」(right to be forgotten)，因此「公眾知情權」和「隱私權」之間的衝突很容易解決，但在美國卻未必是

那麼容易。雖然 GDPR 的實施，可能會為歐洲公司帶來一些適應上的新課題；但歐洲自 1995 年以來便已經根據嚴格的隱私法規制定操作指令，因此企業很快便能適應新法規。雖然如兩位學者所言，歐盟 GDPR 的實施將為企業提供新的商業模式，但與此同時必然也會衝擊企業如何使用消費者的資料而獲利。例如，臉書執行長祖克柏 (Mark Zuckerberg) 曾表示，歐盟法規的修正能為臉書全球用戶提供更多的保護；然而，臉書卻在歐盟實施 GDPR 後，將用戶資料儲存地從歐盟轉移回美國。此舉顯示，臉書未來仍可能挑戰歐盟隱私法規對其業務經營的適用性。從歐洲角度來看，長期以來正是因為美國隱私法規過於寬鬆，導致歐洲企業與美國科技公司之間的競爭存在不公平。Voss 與 Houser 對此提出建議，即使 GDPR 的實施不會造成 Facebook 和 Google 的終結，但它們卻必須修正過去的做法，以符合歐盟新的法規。

McDermott (2017) 在其文章〈大數據時代下資料保護權的概念化〉(Conceptualising the Right to Data Protection in an Era of Big Data) 中指出，歐盟透過 2007 年簽署、2009 年生效的《里斯本條約》(Treaty of Lisbon) 賦予《歐洲聯盟基本權利憲章》(Charter of Fundamental Rights of the European Union) 效力。McDermott 認為歐盟於該憲章第 2 章第 8 條「個人資料保護」(Protection of Personal Data) 中，宣布獨立的資料保護基本權利，[8] 此項權利的創建意義十分重大。因為它不只不同於隱私權，亦突顯出歐洲法律秩序的獨特性。因此 McDermott 在該篇文章

8 歐盟於該憲章第 2 章第 8 條個人資料保護中宣布：1. 每個人皆有權利保護與他或她有關的個人資料數據；2. 此類數據必須出於特定目的並在相關人員同意或法律規定的其他合法依據基礎上進行公平處理，且每個人皆有權利訪問已被收集的有關他或她的數據資料，並有權對此進行糾正；3. 遵守這些規則應受獨立機關控制。關於「歐洲聯盟基本權利憲章」內容，可參見 EUR-Lex (2012), "CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION," *Office Journal of the EuropeanUnion*. Retrieved June 17, 2021, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT

試圖檢視這項新的資料保護權利，並探究支撐此項權利的原則。他認為歐盟資料保護的權利反映出歐洲法律秩序中固有的一些關鍵價值，意即隱私 (privacy)、透明 (transparency)、自治 (autonomy) 和不歧視 (nondiscrimination) 原則。他還分析在大數據時代下，實踐保障隱私的權利可能會遭遇的一些挑戰。[9] McDermott 認為，歐盟於 1995 年提出的「資料保護指令」(DPD) 中，並未提及維護民眾數據資料保障的人權，反而較側重於「資料控制者」(data controller) 應遵守的程序性義務。相比之下， GDPR 在權利方面就有明確的架構；例如，該規範第 1 章第 1 條便指出，「保護自然人的基本權利和自由，尤其是保護個人資料的權利」。

McDermott 指出，在起草《歐盟基本權利憲章》之前，隱私權的概念早已在歐洲法律秩序中確立，民眾可能會想了解獨立的資料保護權會帶來什麼樣的附加價值或需求？特別是考慮到「歐洲人權法院」(European Court of Human Rights) 在許多案件裁決中，皆已包含資料保護權的概念。例如，《歐洲人權公約》(European Convention on Human Rights) 第 8 條即明定，應將個人資料和數據僅用於收集的有限目的。然而，資料保護又與隱私權和思想自由、良心和宗教、言論自由等密切相關。特別是言論和思想表達的自由具有一些獨特的元素，應將其框架轉化為獨立權利。這些要素指的是應當為特定目的，公平地處理數據，並且僅在有關人員的同意或法律規定的其他合法基礎上，才能進行資料的處理；且民眾有權訪問和更正資料處理者所收集的資料，資料處理者亦須受到獨立機構的監管。McDermott 認為在資訊流通的大數據時代下，使用民眾數據和資料的用途、資料的全球化與國際合作，以及

9 詳見 McDermott, Yvonne (2017), “Conceptualising the Right to Data Protection in an Era of Big Data,” *Big Data & Society*, January-June, pp. 1-7. Retrieved March 15, 2021, from https://journals.sagepub.com/doi/10.1177/2053951716686994

對於未來風險的預測等，皆會對實現數位人權的保障提出挑戰。因此，McDermott 呼籲在不斷變化的全球秩序中，吾人極需反思支撐資料保護的這些原則，並加強實現資料保護權，以使其成為所有人應擁有的基本人權。

劉靜怡 (2019) 在其文章〈淺談 GDPR 的國際衝擊及其可能因應之道〉中，[10] 對於 GDPR 主要規定內容進行分析，並且以日本作為個案研究，藉此說明各國和歐盟之間如何協商遵守 GDPR 規範之程序和相關事務，期望長期忽視此一國際規範發展的我國，能在歐盟個人資料保護規則正式生效時，取得適足性認定。如此我國才能有效處理歐盟嚴格實施個資保護後，對各國政府和企業所帶來的影響與衝擊。她認為 GDPR 當中，最為棘手最難處理的是該法規如何處理資料的刪除權，以及資料續轉至第三國的部分。即使相關國家取得歐盟「適足性認定」的標準，第三國有時並未獲得歐盟認證，如此一來資料可能無法續轉至第三國進而形成國際衝擊。另一個重要議題則是有關於救濟和賠償的部分，劉靜怡指出過去歐盟指令遭受質疑的部分，就是因為救濟和賠償的效果不高，因此 GDPR 對此便提高標準，但這一切最後仍須仰賴法院的判斷。劉靜怡建議，我國如想取得歐盟對於個資保護「適足性認定」的目標，除了對於 GDPR 相關規定的重點和特色必須加以掌握外，還應觀察和瞭解各國是如何應對歐盟實施 GDPR 所造成的衝擊，亦須觀察此規範對於國際發展趨勢可能形成的影響，對於我國完善既有的個人資料保護法制與實務才能有所助益。

翁逸帆 (2019) 在〈資訊委員的時代角色—以 GDPR 及英國 2018 年資料保護法為中心〉文章當中，試圖了解英國資訊委員在個人資料加值應用的數位經濟時代下，所面對的實際挑戰以及相對應的法規工

10 詳見劉靜怡 (2019)，〈淺談 GDPR 的國際衝擊及其可能因應之道〉，《月旦法學》，286，頁 5-31。

具和職權之實踐。[11]翁逸帆指出，英國 2018 年的「資料保護法」(Data Protection Act 2018) 對於個資的處理與保護方式，主要規範來源為歐盟的 GDPR。資訊委員的設置和他的任務及職權，依照 GDPR 的規範；至於資訊委員的一般職權與保障機關功能等，則是依照資料保護代表人 (Data Protection Representative)。英國的資料保護法規要求資訊委員對於不同領域的特殊個資處理，負有提供行為準則 (codes of practice) 的義務，同時新增資訊與通訊技術應用時代法規業務，包含公部門資訊的再利用規則、資料留存的規則、電子交易驗證與信任服務規則、網路架構與資訊系統規則等。透過對於以上規則的業管，資訊委員得以更加有效整合資源，平衡各項個人權利的保護義務。翁逸帆以劍橋分析公司外洩民眾個資一案，分析資訊委員就線上平台服務條款關於第三人利用個資的設計問題、人格特徵剖析與精準投放假新聞的面向，以及產學合作與特定目的外利用個資等問題，觀察與分析資訊委員所實踐的職權。由於英國幾乎將所有與個人資料以及各類政府資訊、線上資訊有關的問題交給個資委員處理；對於網路無國界的特性，英國政府應投入更多資源，加強個資委員的職權效果與執行能力。至於我國，翁逸帆認為因我國尚未建立獨立專責的個資保護機關，未來在因應類似情況時，恐需付出更大代價與成本。

三、歐盟數位人權保障重要政策與法規

相較於世界各國，歐盟「數位人權」(digital rights) 的概念發展得相當早，數位人權有時亦被稱為「數位權利」、「數位公民權」，如

11 詳見翁逸帆 (2019)，〈資訊委員的時代角色——以 GDPR 及英國 2018 年資料保護法為中心〉，《月旦法學》，286，頁 32-50。

同離線世界 (offline world) 中的基本人權，只是存在於線上世界 (online world)。「聯合國人權理事會」(UN Human Rights Council) 在 2012 年達成一項決議，明言「人們在離線狀態下的相同權利也必須在網路上得到保護」，因此聯合國建議將現有的人權擴展到網絡空間中 (Nitsche and Hairsine, 2016)。數位人權意指網路時代的人權；例如，「線上隱私」(online privacy) 權和「言論自由」(freedom of expression) 權，此皆為聯合國 1948 年通過的《世界人權宣言》(The Universal Declaration of Human Rights) 內所規定的平等和不可剝奪權利之延伸 (United Nations, 1948)。因此，斷開人們與網路的連接等同於侵犯這些權利違反國際法。隨著民眾越來越習慣在網路和社交平台上使用和共享訊息，民眾的數位權利，尤其是隱私權和言論自由權更加重要。民眾不只需要瞭解政府和企業、電訊和網路業者等，是如何使用他們的個人資料？是否經過民眾的同意使用？還包括這些機關團體和業者是否能公正、謹慎地處理、出售或共享這些訊息？因此，隱私權的規範便顯得相當重要。

但在保障民眾隱私之際，與此同時，民眾又有言論表達的自由，包含在網路世界中進行個人言論的發表和意見的撰寫，有時這些訊息又有可能無國界的迅速、廣泛流傳。依照世界人權宣言第 19 條：「人人有權享受主張和發表意見的自由；此項權利包括持有主張而不受干涉的自由，和通過任何媒介和不論國界尋求、接受和傳遞消息和思想的自由」(United Nations, 1948) 。在民眾亦擁有知的權利之下，限制新聞的發布與資訊的流通，似乎又違背民主國家的價值。因此，個人隱私權、言論表達自由與獲得資訊的權利之間是否互相抵觸？又該如何平衡，值得吾人深思。本文將以歐盟數位人權保障做為研究，分析歐盟對於民眾個人資訊和隱私權之相關重要保障；以下將就歐盟重要資料保護規範之法規發展與演變做一說明。

歐盟在數位人權保障上的重要法規最早可以雖溯至 1995 年的《資

料保護指令》(Data Protection Directive，簡稱 DPD)。然而，當時僅為一「指令」(Directive)，沒有直接拘束力，且所謂的個資保護是由各會員國依據該指令規範，各自制訂合適的國內法律並據以執行。在民眾資料跨境傳輸上，根據該指令第 25 條，跨境傳輸民眾資料採「互惠原則」(EUR-Lex, 1995)，倘若第三國無法符合適當標準 (adequacy standard)，則為保護歐盟民眾個人資料隱私，歐盟將採取必要措施防止將民眾資料轉移至該國。此項規定對於一向對隱私採取寬鬆政策、標榜資料經濟的美國而言，可能無法適應歐盟指令。為免會造成資料保護法規的差異，美國遂於 2000 年公布「安全港原則」(safe harbor principles) 文件，以作為美國企業接收歐盟傳輸過來的資料，需遵循之準則 (丁俊和，2019)。隨著歐盟單一市場發展的逐漸完整與完善，以及網路服務的普及，歐盟執委會 (European Commission) 遂於 2009 年開始進行討論，期盼能推動、協調適用歐盟全境對於資料保護的法規，以降低歐盟會員國在個資保護法規上的差異性。歐盟執委會隨後於 2012 年 1 月提出新版的《個人資料保護規則》(General Data Protection Regulation，簡稱 GDPR) 草案，同時藉此亦能促進打擊犯罪和恐怖主義的跨境合作。2015 年 12 月 15 日，歐洲議會、理事會和執委會就新的資料保護規則達成協議，並於 2016 年 4 月 8 日定稿法規內容，同年 4 月 14 日獲得歐洲議會批准，[12] 並設定兩年的緩衝期。GDPR 最後於 2018 年 5 月 25 日正式生效，成為一部相當完整且嚴格的歐盟隱私法規。

2018 年以來開始實施的歐盟 GDPR 共有 11 章，它與 1995 年建立的 DPD 最大不同在於，個人資料保護規則直接適用於歐盟全境，無

12 關於歐盟「個人資料保護規則」詳細英文法規內容，可見 Union Law (2016), "Regulation (EU) 2016/679 of the European Parliament and of the Council," *Official Journal of the European Union*. Retrieved August 8, 2021, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

須再轉換為歐盟各會員國的國內法；意即往後凡是與歐洲民眾有關之資料保護都必須受到此部法規的嚴格規範，以符合歐盟的隱私保護規範。歐盟還成立獨立委員會 -「歐盟資料保護委員會」（European Data Protection Board）(蔡柏毅，2017)，經由發表意見（opinions）、準則（guidance）、公眾協商（public consultations）等 (EDPB, 2018)，保持歐盟資料保護制度的跨國一致性。歐盟從規範企業團體 (Business) 與公民 (Citizens) 兩大部分著手，認為更嚴格的資料保護規範意味著，民眾可以更好地控制自己的個人資料保護隱私，企業亦能從公平的競爭環境中受益。

儘管 GDPR 被視為史上最嚴格的隱私法規，歐盟亦說明一些例外情形。例如，該規範則並不適用於個人因為個人因素或在家中進行的活動而處理的資料（purely personal or household activity），如果該行為與專業或商業活動無關。但如果在個人範圍之外，使用個人資料進行社會文化或金融活動時，就必須遵守此資料保護法。個人資料 (personal data) 指的是與已識別 (identified) 或可識別 (identifiable) 的生活個體有關的任何資訊，包含不同訊息的集合以識別出特定人員身份的資料，或是經由未識別、加密或使用假名仍可以用於重新標識個人的資料，則仍然屬於個人資料；皆在 GDPR 保護的範圍內。該規則亦說明此法規不適用於歐盟法以外治權領域之活動（outside the scope of Union Law），或者主管機關為維護及預防對於公共安全造成威脅所作之預防、調查、偵查或追訴刑事犯罪或執行刑罰之目的所為的個人資料處理 (Union Law, 2016)。

在 GDPR 當中，最值得注意的是該法第 17 條所明列的「刪除權」(right to erasure)，或稱「被遺忘權」(right to be forgotten) (Union Law, 2016)，即希望加強個人對於個人資料保護的主動性。歐盟委員會認為透過行使被遺忘權，每個人便能自主控制個人資料保護隱私，阻止有關

個人身份與資訊 (personally identifiable information) 的外洩或曝光。此次納入「被遺忘權」起源於 2010 年的西班牙 Google 案，當時一位西班牙公民以歐盟 1995 年 DPD 為依據，向當地保護個人資料的監管機構投訴，抱怨過去他曾因欠債而被政府下令拍賣資產的消息，即使在他後來已經還清債務，仍然能於網路上搜尋得到。他因此要求報社與 Google 移除關於他個人資料的搜索結果，卻未能成功 (甄美玲，2016)。當地個資監管機構認為報社是受到政府部門的委託，才會合法刊登公告，因此報社無需移除相關資訊。但 Google 的搜索引擎業務屬於處理個人資料之活動，仍須受到 DPD 的規範。

Google 因此不服裁定提出上訴，西班牙法庭認為此事件需向歐盟法院 (Court of Justice of the European Union) 尋求指示，才能正式審理該案件。歐盟法院遂於 2014 年 5 月做出裁決表示，Google 為「資料控制者」，因此其搜索引擎業務為處理個人資料之活動，仍需受歐盟指令規範；即使這些資料為合法發佈，當事人仍有權利要求 Google 移除第三者發佈之個人資料。[13] 歐盟法院認為，依照《歐盟基本權利憲章》(EU Charter of Fundamental Rights)，[14]「資料當事人」擁有隱私權 (privacy rights) 和保護個人資料之權利 (European Commission, 2012)，這兩項權利高於 Google 營運的商業經濟利益和民眾獲取資料當事人個資之公共利益。因此，這位西班牙公民有權利要求網路搜尋業者移除或遮蓋事關個人的敏感資料。紀珮宜 (2017) 在其文章〈由歐盟資料保護規則論

[13] 此次事件發生後，台灣也曾有類似案件，惟 Google 台灣分公司當時表示「被遺忘權」在台灣並未被確立，其適用應僅限於歐洲區域，至於是否擴張至其他地區仍持保留，聲稱當事人的主張無所依據。關於發生於台灣的 Google 類似案件可見〈被遺忘權在台灣是否能主張，待定！〉，《科技新報》，2016 年 7 月 24 日。請見 https://technews.tw/2016/07/24/right-to-be-forgotten-google-taiwan/。

[14] 關於歐盟基本權利憲章內容可見 European Commission (2012), “EU Charter of Fundamental Rights”. Retrieved November 23, 2019 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

被遺忘權之爭議〉中，就曾經解釋歐盟「被遺忘權」之概念。[15]她指出，「被遺忘權」事實上一直存在於歐盟體系內，但長期以來各界對於此一權利之行使與落實產生許多爭議。例如，所謂「資料控制者」(data controller) 的定義與範圍過於廣泛，使得許多網路使用者皆可能落入此定義當中。此外，過去對於「被遺忘權的權利內涵與例外」的解釋始終存在爭議；若由資料控制者決定個案是否符合該條件或例外，將使資料控制者承擔過多負擔。另外，行使被遺忘權還可能導致個人言論表達自由受到侵害。

對於歐盟法院於 2014 年對 Google 案件的判決，紀珮宜認為該判決說明「被遺忘權」雖然被確定為歐盟公民擁有的權利；然而，當時在歐盟執委會公布之草案、法院之判決、歐盟 GDPR 最終版本等，皆未能有效解決被遺忘權相關問題與爭議，致使能否真正落實被遺忘權以保障個人隱私，仍然備受質疑。針對歐盟 GDPR 中，對於被遺忘權之規定是否能解決相關爭議。紀珮宜悲觀地認為，即使是個人資料保護規則，仍然無法清楚定義資料控制者；至於被遺忘權的權利內涵與例外，雖然被直接列入條文當中，但應由誰來判斷個案情況是否符合條文規範並未明確指定。因此；被遺忘權與個人言論自由之間的衝突仍舊無法解決。該篇文章似乎點出為何歐盟執委會會在「個人資保護規則」正式實施兩年後，於 2020 年 6 月發布關於 GDPR 的評估報告當中，坦承法案難以全面實施，且可能造成企業負擔。[16]

如同 McDermott (2017) 所言，歐盟對於資料保護的權利反映歐洲法律秩序中固有的一些重要價值，即隱私 (privacy)、透明 (transparency)、

15 紀珮宜，〈由歐盟資料保護規則論被遺忘權之爭議〉，《經貿法訊》，214，頁 8-24，2017 年 5 月 25 日。

16 楊又肇 (2020)，〈GDPR 上路兩年後歐盟坦承難以全面實施〉，《聯合新聞網》，2021 年 1 月 19 日。請見 https://udn.com/news/story/7086/4658955。

自治 (autonomy) 與不歧視 (nondiscrimination) 原則。McDermott (2017) 解釋，「隱私」本身就是一項基本權利，尋求資料保護的一種價值。關於隱私權的涵義有不同的表述，從只涉及合理的隱私期望此種相對有限的隱私概念到廣義的獨處的概念，甚至到更廣泛的觀點，認為隱私權與個人身份的保護息息相關。他認為資料保護 (data protection) 顯然與個人身分保護有關；即使某些資料，例如民眾的醫療訊息，可能屬於對隱私的合理期望，但其他資料，如個人地址和電話號碼則不屬於此種範圍。「透明」的原則可見於 GDPR 第 58 條要求，[17]任何傳達予公眾或資料主體之資訊皆須簡潔、容易獲得且易於理解，以清楚簡單語言表示。資料保護的另一個重要價值則是個人的自治權，個人資料保護規則第 7 條指出，當事人應有其個人資料之控制權；且關於當事人、業者及公務機關之法及實務之安定性均應該提昇。「不歧視」原則體現在 GDPR 第 71 條，為確保對於資料主體之公平與透明的資料處理，於考慮個人資料處理之特定情況與脈絡時，資料控管者應於建檔時使用適當之程序、實施科技化、有組織的措施，以確保個人資料之得以更正及將錯誤風險降至最低，並應在考慮資料主體之利益與權利所受風險。同時亦須預防包含，但不限於種族、人種、政治態度、宗教信仰、貿易聯盟會員、基因或健康狀態、性傾向等理由對當事人之歧視下，保護個人資料 (Union Law, 2016)。

根據 GDPR，民眾個人資料的定義為能夠辨識出關於個人的任何資訊與個人在網路上的相關資料，包含個人資料、Cookie、IP 位置、行動裝置 ID、社群網站的活動紀錄等。該法規詳細明定資料當事人的權利，並賦與資料當事人更正及刪除 (rectification and erasure) 資料的權利 (第 16 條至第 17 條)，亦規範個資的可攜權 (right to data portability)

[17] 透明原則為資料主體（當事人）之權利之一，亦可參見個人資料保護規則 (GDPR) 第 12 條至第 14 條。

(第 20 條) 與拒絕權 (right to object) (第 21 條) 等，清楚規定資料控制者與處理者的義務。在規範個人資料的跨境傳輸、政府監理體制、救濟措施等方面，無論是在歐盟營運的企業或跨國公司在歐盟的分支機構，凡是以歐盟市場為目標者都必須嚴格遵守此個人資料保護規則。企業亦需遵守歐盟個資保護規則中所規定的各項義務，強化對個資處理的安全水準，遵守跨境傳輸個資至歐盟境外第三國的規範。企業也須紀錄完善，確實執行個資管理計畫與執行個資保護之風險評估，設立「資料保護官」，若獲知個資受到侵害，資料保護官必須在 72 小時內做到通報與通知。

歐盟《個人資料保護規則》一共有 11 章 99 個條文，其主要規定內容包含以下要點 :[18]

1. 第 1 章總則 (General Provisions) 與第 2 章原則 (Principles)：

個資之蒐集應基於特定、明確且正當的目的；且應適當且僅限於與目的相關的有關者。蒐集之個資應準確，錯誤資料應予以刪除或修正，個資儲存時間不能多於處理目的所須使用之時間，且資料處理須確保個資受到完善之安全保護。

2. 第 3 章資料主體之權利 (Rights of the data subject)：

個資之蒐集、處理、利用須經資料當事人之明確同意，可以書面請求同意。當事人可隨時撤銷同意，且有權利向資料控制者查詢、閱覽及複製其個人資料，亦有權要求更正、刪除、限制資料控制者對其個資之處理。資料控制者負有義務通知資料接收者，有關資料當事人相關資訊之更動，資料當事人有權將其資料轉移至另

[18] 關於 GDPR 詳細英文規範，可參見 Union Law (2016), "Regulation (EU) 2016/679 of the European Parliament and of the Council," *Official Journal of the European Union*. Retrieved August 8, 2021, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

一資料控制者，無需受到限制。當事人亦有權利對其個人資料因為公益、公權力或資料控制者合法權益目的之處理提出異議。

3. 資料控制者與處理者之義務 (第 4 章)：

資料控制者應就資料蒐集者的資訊、資料蒐集原因、當事人權益等資訊告訴當事人，且須採取相關技術與內部措施確保個資處理程序與方式合乎相關規範。歐盟境外資料控制者與處理者於處理歐盟居民個資時，應在歐盟境內指定代表人。資料控制者僅能委託合乎歐盟資料保護相關規範之資料處理者，且資料處理者處理資料時應受合約之規範。資料控制者應保留資料處理活動之記錄，並與資料處理者、資料監管機關合作。資料控制者與資料處理者應採行適當技術（如去連結化或加密）以確保民眾個資安全。如果民眾個資遭到外洩，企業與機關必須於 72 小時內通報主管機關，情節嚴重者亦需通知當事人。資料控制者應進行資料保護風險之影響評估，資料控制者與資料處理者之企業核心業務如涉及需定期、系統性、大規模監測當事人之資料處理時，需設立「資料保護官」。主管機關應鼓勵企業建立「行為準則」(Code of Conduct)，各產業協會亦可設立行為準則供資料控制者與資料處理者採行，以符合歐盟個人資料保護規則。主管機關亦應鼓勵機關與企業創設資料保護認證機制 (certification mechanism)，以利資料控制者與處理者申請認證，以顯示符合歐盟資料保護規範。

4. 跨境資料傳輸之規範 (第 5 章)：

對於歐盟居民個人資料傳輸至第三國，歐盟採有條件允許以下情況 : (1) 對個資保護程度跟歐盟水準相當，且得到歐盟適足性認定 (adequacy decision) 之第三國；(2) 資料控制者與資料處理者彼此已簽訂歐盟執委會公布之「標準資料保護條款」(standard data protection clauses) 或稱「標準契約條款」(standard contractual clauses）；(3) 適用同一企業集團或進行經濟合作活動的不同集團內企業，且經主管機關核准的企業拘束規則 (binding corporate

rules)；(4) 歐盟資料控制者或資料處理者採行之行為準則，搭配第三國之資料控制者或資料處理者具法律效力且可執行之承諾；(5) 歐盟資料控制者或資料處理者經過認證，搭配第三國之資料控制者或資料處理者具法律效力且可執行之承諾；(6) 部分排除適用 (derogation)，意指在某些情況下，雖然無法確保個資被傳輸到第三國得以繼續受到完善保護，但如獲得當事人明確同意且已告知相關風險下，可以將其個資傳輸至第三國。

5. 獨立監理機構及政府組織之合作與一致性 (第 6、7 章)：

包括歐盟各會員國資料保護監理主管機關之職權與獨立性；各主管機關應互相合作以確保法規施行之一致性；設立資料保護委員會等。

6. 救濟措施、責任與制裁 (第 8 章)：

當事人若認為其個人資料遭受到侵害，可向主管機關提出控訴；若不滿意主管機關處理結果，可對主管機關做出之決議提出司法訴訟；當事人亦可對資料控制者與資料處理者提出司法訴訟。當事人應就其受到之損害，向資料控制者與資料處理者申請補償；主管機關對於違反 GDPR 者除進行稽核要求修正外，亦可以處以罰鍰。對於部分違法情事，如資料控制者違反其認證義務或認證機構違反其義務時，最高罰鍰可達 1,000 萬歐元或其全球營業額之 2%。另對於部分違法情事，如違反個資處理基本原則、傳輸個資至第三國等，最高罰鍰可達 2,000 萬歐元或其全球營業額之 4%。[19]

7. 有關具體資料處理情況之規定 (第 9 章)。

8. 委員會之指派和執行 (第 10、11 章)。

[19] 關於歐盟一般資料保護規章 11 個章節的中文詳細內容說明，可參閱《駐歐盟兼駐比利時代表處》，〈歐盟一般資料保護規章 GDPR 簡介〉， 2018 年 5 月 23 日。請見 https://www.taiwanembassy.org/be/post/6571.html。

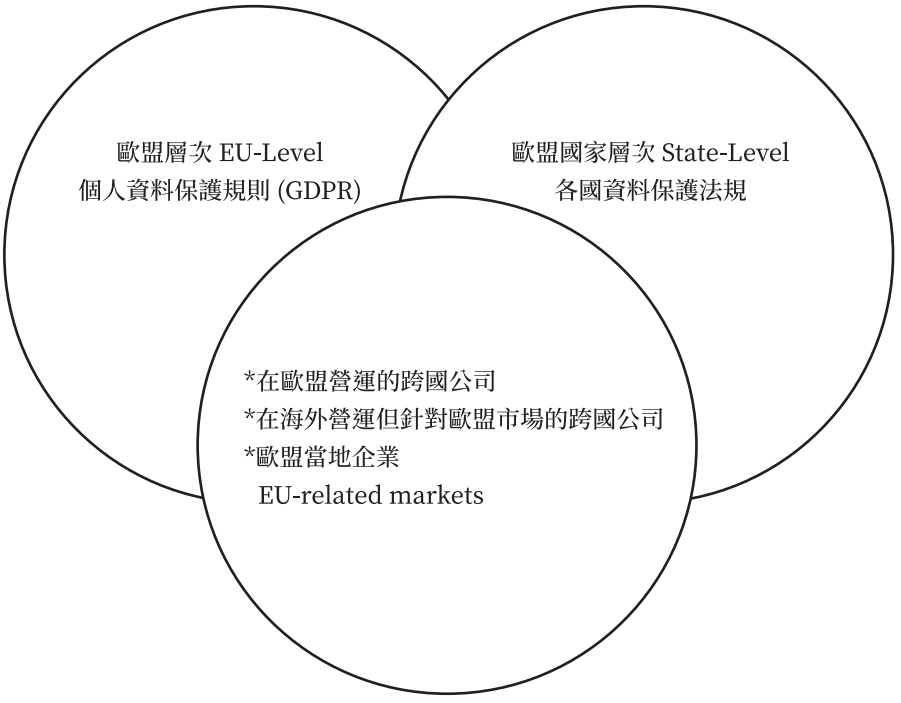

圖 1：歐盟個人資料保護規範實施範圍（本圖由作者自製）

歐盟執委會認為 GDPR 法案之通過對於政府、企業與民眾的權益皆能提供保障。對於企業而言，可由國家取得歐盟適足性認定的認證資格，企業便無需再個別取得歐盟的認證，此舉有益於鼓勵企業以創新想法、方法與技術處理隱私權議題和資料安全問題。企業經由設計 (design)、預設 (default) 機制對資料進行保護與處理，亦能激勵提供新服務的公司尋找創新的解決方案。此外，GDPR 法規中的「風險基礎管理方法」(risk-based approach) 亦能協助公司降低資料處理的風險，免於受到過多的責任約束。歐盟個資保護規則不僅提供一套共同的管理工具，亦建立行為準則與認證機制，協助各企業公司管理、處理資料以符合歐盟法規。有關歐盟個資保護規則範圍整理如圖 1 所示。

GDPR 亦擴增使用者權利和保護措施；例如，個人資料的分享、可攜性或在民眾個資遭到洩露時提出警訊，協助資料使用者能夠更好的管理其個資。相較於過去的法令，GDPR 提高「資料主體」(data subject)，即資料當事人對於個資的主控性。依照該法規第 17 條第 1 款的規定，資料當事人有權要求「資料控制者」(data controller) 刪除與他或她個人有關的資料，且不得有無故拖延的情況 (Union Law，2016)。資料控制者有義務在不得拖延的情況下刪除資料當事人的個人資料 (“The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies”)[20] 例如，民眾可以要求 Google 刪除其個人資料，或不同意資料控制者繼續處理其個資。資料控制者若無其他合法理由，必須刪除與資料當事人有關之個人資料。該法規第 2 款同時規定資料控制者將個人數據、資料公開時，負有該法第 17 條第 1 款之義務，刪除個人數據。另資料控制者應考慮使用可用的科技和合理的步驟與成本，包括可行之技術方式通知資料處理者，資料當事人已要求刪除與個人數據、資料有關的任何連結、複製或再製 (“Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those

[20] Financial Supervisory Commission, R.O.C. Taiwan (2016), “Regulations (EU) 2016/679 of the European Parliament and of the Council”, *Office Journal of the European Union.* Retrieved January 10, 2022, from https://www.fsc.gov.tw/fckdowndoc?file=/4-20%20EU%20GDPR%20FINAL.pdf&flag=doc。

personal data")。[21]但第 17 條第 3 款卻也說明，以上第 1 款和第 2 款不適用於以下情況：

(a) 當行使言論和資訊自由權時。

(b) 歐盟或歐盟會員國要求資料控制者基於公共利益或行使官方要求遵守之法律義務時。

(c) 為公共利益理由且符合此法規相關規定。

(d) 為公共利益建檔所需或為科學、歷史研究或統計目的且符合此法第 89 條第 1 款中所提之權利可能無法實現，或處理資訊過程可能嚴重損害該權利之實現。

(e) 建立、行使或為法律主張辯護。

以上條文顯示該法仍保有空間，說明若為行使言論自由和資訊自由的權利，或基於公眾利益理由所需而存檔，或為科學或歷史研究、進行統計等情況，處理該筆個人資料不受第 17 條第 1 款和第 2 款約束。

除了在歐盟層次提出共同的資料保護規範外，歐洲各國亦在國家層次上制訂各自的資料和隱私保障專屬法規，以符合歐盟 GDPR 之實施。例如，英國 2018 年制定的資料保護法及「資訊專員辦公室」(Information Commissioner's Office) 之設立。[22] 英國 2018 年資料保護法規範管理組織、企業或政府應該如何合法的使用民眾個人資訊。[23] 該法規定任何機關團體使用個人資料時，都必須遵循嚴格的「資料保護原則」(data protection principles)，確保資訊能受到公平、合法和透明

[21] 同前註。

[22] 關於英國資訊專員辦公室的成立背景及工作任務，參見 ICO (2018), "History of ICO". Retrieved August 8, 2020, from https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/。

[23] 關於英國「2018 年資料保護法」(The Data Protection Act 2018) 內容，可見 The National Archives (2018), "The Data Protection Act 2018", Retrieved November 23, 2019, from https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted。

的使用。此外，民眾資料只能用於特定、具體的目的，並以最適當安全的方式進行資料的處理，包括防止非法或未經授權的處理、訪問、丟失、銷毀或損壞資料，以妥善維護民眾隱私權。對於敏感的資訊；例如，比賽、民族背景、政治觀點、宗教信仰、工會會員資格、遺傳學、生物特徵識別 (用於標識)、健康、性生活或性取向等資料，都必須給予更強的法律保護。對於有關刑事定罪和罪行的個人資料亦必須有單獨的資料保護措施。

另一方面，根據此資料保護法，民眾有權瞭解政府和其他組織為其所儲存的資訊，包含瞭解如何使用、訪問其個資，更新錯誤或已刪除的資料，停止或限制資料的處理、資料的可攜性，以及在某些情況下應如何處理民眾個人資料。當某個組織欲使用民眾的個人資料，進行某些自動化決策過程的分析；例如，預測個人的行為或興趣的操作時，民眾亦具有許可權 (The National Archives, 2018)。

四、GDPR 實施後遭遇之困難與挑戰

GDPR 實施後所遭遇的最大問題在於資料的跨境傳輸限制上。在大數據時代和資料經濟盛行的年代，網路資訊的快速傳遞和網路無國界的特性，都讓民眾的數位人權遭受到威脅與風險，隨時有個資外洩的可能。無論是以美國與歐盟早先簽署的「安全港」(Safe Harbor) 協議，或者隨後取代安全港的「隱私盾」(Privacy Shield) 協議等，仍無法完美遵守跨境傳輸資料的原則。過去美國一向主張資訊自由流通，並未嚴格限制和禁止跨境資料的傳輸，僅要求業者自律並由「聯邦貿易委員會」(Federal Trade Commission) 在行業規範、第三方程序等，促使業者進行自我監督。業者如未遵守規範，便會由聯邦貿易委員會進行罰鍰或提起

行政訴訟。過去美國並無全國聯邦層級的個資保護或跨境資料流通的限制規範，即使在 1996 年的《電信法》(Telecommunications Act of 1996) 都僅有非常少數的保護資料隱私條款。[24]當時的電信法僅在第 7 篇第 702 項條款，規範消費者資訊隱私 (Privacy of Customer Information)。[25]

根據第 702 條款，每個電信運營商，包含與其他電信運營商、設備製造商和客戶，以及由電信營運商轉售給某公司的電信服務商，都有責任保護民眾資訊的隱私。電信運營商從其他業者處所接收，或獲取的私人訊息僅能作為提供電信目的之使用，不得將此類信息用於營利所為。該條款同時要求電信營運商依照法律要求，或在取得客戶同意之下，將其提供的電信服務僅能使用、披露或許可於，可單獨識別的客戶專有之網絡資訊上。然而，科技的日新月異同時也大大地影響政府部門取得 (access) 和存取 (store) 通訊裝置內，所儲存的內容和靜態資料，即儲存中的資料 (data at rest, DAR) 的執法能力。智慧型手機的發展更造成在這些通訊設備上，產生和保存資料內容的方式；除語音

24 美國 1996 年的電信法是為修正 1934 年的通訊法 (The Communication Act of 1934)。1934 年的通訊法乃羅斯福總統於同年 6 月 19 日所簽署，該法共有 7 篇 714 項條款。法規於第 1 款言明為規範州際和外國有線和無線電通信，以便盡可能地向美國全國民眾提供快速、有效、覆蓋全國，乃至世界範圍的有線和無線電通信，並以國防為宗旨，促進生命和財產安全為目的集中力量，確保更有效地執行該政策，並以合理的費用提供適當設施的服務。法律將權力授予幾個機構相關權限，並創建聯邦通訊委員會。關於該法規內容，可見 Bureau of Justice Assistance (1934), “Communication Act of 1934”. Retrieved June 20,2020, from https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1288#vf4tzl。

25 1996 年 1 月 3 日，美國國會以 1996 年電信法對 1934 年通訊法部分內容做一修訂與刪除，為美國 62 年來對電信政策進行第一次重大改革。1996 年的電信法共有 7 篇 710 項條款；相較於 1934 年的通訊法，電信法消除一些技術偏見並刪除一些法規，以能提供有利於競爭的國家政策架構。通過開放所有電信市場競爭，以加速民營部門能向民眾迅速提供先進的訊息技術和服務，當中也包含一些網路規範。關於 1996 年電信法規內容參見 Federal Communications Commission (2013), “Telecommunications Act of 1996”. Retrieved June 20, 2020, from https://www.fcc.gov/general/telecommunications-act-1996。

通訊之外，還包含通訊記錄、全球定位系統的定位點、手機或電腦內儲存的資料、電子郵件和照片，以及儲存在雲端 (cloud) 的資料等。其中有些資料需要從電信供應商或個人方面獲得，有些則得以直接取得 (CRSR, 2017)。對於電信服務業者而言，必須思考如何能同時保護客戶個人隱私和維護公司商譽，特別是全球消費者的信賴，亦須避免歐盟質疑美國政府與資通訊業者聯手侵犯消費者個人隱私，違反歐盟規定。

此次歐盟 GDPR 的嚴格立法，代表歐盟在推動個人隱私權的保護上不遺餘力；然而，對於一向主張網路自由、資訊自由流通的美國，可能不樂見歐盟推動被遺忘權的立法，認為此舉將增加美國網路營運業者的成本。

為免歐美雙方對於個人資料流通持有不同態度與措施，限制雙方貿易往來及產業發展，進而影響貿易及投資關係，在經歷多次談判後，雙方同意建立機制以允許美國企業能符合歐盟 1995 年個人資料保護指令中，所規範的「適當層次的保護」(adequate level of protection) (Weiss and Archick, 2016)。美國商務部與歐盟委員會最後於 2000 年 7 月 26 日簽定《安全港隱私原則》(Safe Harbor Privacy Principles)，即所謂的「安全港架構」(U.S.-EU Safe Harbor Framework)。安全港架構要求美國公司如果需要將歐盟民眾的資料跨境傳輸至美國時，必須盡到保護資料的責任。此外，歐盟得以將安全港原則限制在國家安全、公共利益或執法要求所必需的範圍內。根據安全港架構，美國企業和公司可以每年向商務部進行自我認證，證明其已遵守歐盟資料隱私保護標準的七項基本原則和相關要求。

七項基本原則包含通知 (notice)、選擇 (choice)、下轉 (onward transfer) 、安全 (security) 、資料完整性 (data integrity) 、進入 (access) 、執行 (enforcement)。所謂「通知」意指企業、團體組織必須告知民眾收集其個人資訊時，民眾如何聯繫組織詢問或投訴向其披露訊息的第

三方方式。「選擇」則指組織必須為民眾提供機會選擇是否退出其個人訊息，如遇 (a) 向第三方披露或用於與其目的不符之最初收集或隨後由個人授權之訊息。對於敏感資料，必須提供民眾明確選擇加入將轉讓給第三方或用於除此以外的其他目的最初收集或隨後授權。所謂敏感的資料包括醫療或健康狀況、種族或種族血統、政治觀點、宗教或哲學信仰、工會會員資格，或有關個人性生活等資訊。「下轉」是指向第三方傳輸民眾訊息時，組織必須做到符合通知和選擇原則，作為代理人的第三方必須通過簽訂安全港協議，提供相同級別的隱私保護，遵守指令或其他充分性調查結果，或簽訂指定等效的隱私保護合約。企業機關團體如欲繼續轉移訊息至第三方時，必須做到通知和選擇原則，要求第三方提供相同級別之隱私保護。「安全」性原則指創建、維護、使用或傳播個人資訊的組織訊息，必須採取合理的預防措施來保護它免受丟失、誤用和未經授權的訪問、披露、更改和破壞。[26]「資料完整性」原則則指個人訊息必須與使用目的相關，使用資料之組織應採取合理步驟，確保資料在預期用途、準確性、完整性皆是可靠的。且個人有權「進入」機關團體和企業持有的有關他們的個人訊息，且有權更正或刪除錯誤之處。企業或團體機關需達到告知民眾收集和使用其訊息的目的，讓民眾選擇是否願意將其資料或訊息向第三方揭露或用於與最初收集或個人授權目的不符之處。機關團體和企業必須「執行」有效的隱私保護，包括可驗證之機制；倘若企業或機關團體組織未遵守規範時，須提供隨時可用且能夠負擔的補救措施和嚴格的制裁機制，以確保合乎規範中的七項基本原則。

然而，《安全港協議》在 2015 年 10 月 6 日，卻因保障措施提供

26 關於此七項原則內容，詳見 Weiss, Martin A. and Kristin Archick (2016), "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield," *Congressional Research Service*. Retrieved August 8, 2021, from https://fas.org/sgp/crs/misc/R44257.pdf.

不足而被歐洲法院判定為無效 (The Guardian, 2015)，[27] 改由歐盟 28 個會員國自行訂立美國企業使用其國民隱私資料之相關規定，或拒絕讓資料傳輸送至美國。隨著《安全港協議》失效後，向來將資料隱私視為消費者權益一部分的美國，迅速與歐盟於 2016 年 7 月再度協商簽訂《隱私盾協議》(EU-US Privacy Shield)(紀珮宜 , 2016)，允許歐盟民眾個資可以存放在美國境內的數據中心 (data centers)。[28] 由歐盟執委會與美國商務部 (Department of Commerce) 所簽訂的「隱私盾協議」(EU-US Privacy Shield Agreement) ，旨在為大西洋兩岸的公司提供一種機制，在將民眾個人資料從歐盟轉移到美國，進行跨大西洋商業活動時能符合歐盟資料保護要求。意即企業或機關只有在達到 GDPR 所規範的具有「充分保護」的情況下，方能將歐盟民眾的資料提供給歐盟以外的國家。美國亦首度承諾歐盟，美國為執法和國家安全行動需要所收集的個人資料將會受到非常清楚的監管與限制約束，同時承諾不會對歐洲民眾進行無差別的大規模監控，且收集到的民眾資料亦僅限於用於防擴散、反恐與網路安全等目的。

根據隱私盾協議，歐盟民眾若覺得個人資料受到侵害時，可以以下列方式進行求助 : (1) 向企業進行投訴，企業需在 45 日內給予回覆；(2) 向本國資料保護機構投訴，該機構可與美國商務部、聯邦貿易委員會共同合作進行調查；(3) 向名單內的企業所加入的免費替代性糾紛解決機制求助；(4) 向隱私保護專家組尋求仲裁，其做出的裁決具約束性。

---

[27] 關於歐盟法院對於安全港協議之判決可見 The Guardian (2015), “What is ‘safe harbour’ and why did the EUCJ just declare it invalid?”. Retrieved October 6, 2020, from https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection。

[28] 美歐「隱私盾協議」內容可見，European Commission (2017), “ EU-US Privacy Shield”. Retrieved March 31, 2021, from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en。

美國也會建立獨立的監察專員機制，負責處理民眾提出的申訴和諮詢，意謂著民眾在資料隱私權上能夠獲得申訴與強制仲裁的機會 (劉耀華 , 2016)。此外，此項「隱私盾協議」亦需經由歐盟各會員國個資管理機關核准，並訂定執行細則；許多企業包含微軟等公司皆加入隱私盾協議 (科技新報 , 2020)。歐盟始終將民眾資料隱私權視為人權保護的一種方式，且以法令禁止跨境傳輸歐盟民眾資料至歐盟以外的區域，除非獲得歐盟認證具備足夠保護民眾隱私權的區域。然而，在川普執政時期卻曾經簽署多項法案放寬政府收集民眾資料、網路數據，並加強監控執法。對於歐盟而言，美國對於民眾的數位人權與資安保障並不充足，甚至挑戰歐洲法律重視人民隱私權與數據保護的底線。結果，隱私盾協議在實施四年後，於 2020 年 7 月 16 日遭到歐洲法院裁定失效，法院認為該協議無法符合歐盟相關保障隱私法規，無法確實保障民眾資訊安全 (自由時報 2020)。所幸除民眾個人資料做為的商業用途的國際傳輸外，歐盟未限制傳輸與國家安全、公共利益有關的數據訊息。

有鑑於未來幾年數位資料的急劇增加，資料的再使用或共享可能與資料安全保障互相衝突，或遭遇技術障礙；歐盟執委會為建立一個單一的歐洲資料空間，充分體現歐洲的規則和價值觀，發揮數位經濟的潛力，於 2020 年 2 月 19 日發布〈歐洲資料戰略〉(A European strategy for data)，藉此宣示歐盟未來數位政策轉型之藍圖 (European Commission, 2020)。「歐洲資料戰略」建立於四大支柱上：(1) 建立一個跨部門的資料訪問和使用的治理框架，尤其是對於資料共享的規範；(2) 加強歐洲的資料空間和雲端基礎設施；(3) 賦權個人控制他們的個人資料以及投資相關技能和能力；(4) 促進在戰略部門和公共領域開發共同的歐洲資料空間利益，例如製造業、綠色交易、健康和金融等。歐洲資料戰略旨在使歐盟成為資料驅動型社會的領導者，創建單一資料市場以允許資料在歐盟內部和跨部門之間自由流動，造福企業、研究人員和公共

管理部門，對資料做出更好的決策供所有人使用。

歐盟針對數位時代的資料治理與規範，除提出「歐洲資料戰略」外，同時公布《人工智慧白皮書》(White Paper: On Artificial Intelligence—A European approach to excellence and trust)。歐盟期望以建立數位資料治理架構，結合開發人工智慧，確保歐洲在遭遇數位浪潮變遷下能保足夠之競爭力、資料主權與技術領先。該份白皮書要求訓練 AI 的資料須涵蓋廣泛人口，避免產生偏見並詳細記錄 AI 訓練過程；使用者與 AI 互動時，須告知使用者正在與自動化系統互動，而非真人；歐盟以外開發的 AI 可能要重新訓練才，方能進入歐洲市場，以確保符合歐盟規範 (郭家宏 , 2020)。除《歐洲資料戰略》與《人工智慧白皮書》的公布，為促進歐盟各國之間的資料和數據共享，加強歐盟民眾和企業對資料數據的掌控力和信任，亦為歐盟的經濟發展和社會治理提供足夠的支撐力，歐盟執委會於 2020 年 11 月 25 日提出《數據治理法案》(Data Governance Act)。執委會為促進數位資料和數據的共享和使用，將在戰略部門和公共利益領域建立共同歐洲資料空間，包含共同的歐洲工業 (製造業)、綠色協議、移動、衛生、金融、能源、農業、公共行政、技能等資料數據空間 (劉耀華 , 2020)。法案就是在《數據戰略》規劃下公佈的第一個成果，旨在尊重歐盟數據保護等基本規則和價值觀的前提下，促進九個共同數據空間的建立和發展，為歐盟社會治理和經濟發展提供更多具有使用價值的數據。這些數據空間的建立旨在獲得民眾的信任，亦符合 GDPR 對於個人資料保護之規範。

五、結論

本文綜合以上研究，將歐盟對於隱私權規範之法案內容整理如下：雖然歐盟原則上禁止將民眾個人資料從歐盟境內流至其他區域，但如果相關資料流入的國家或區域對於個資保護具備足夠安全的措施，且獲得歐盟的認證與核可，便可允許跨境資料的傳輸。也就是說，歐盟採取的是「原則禁止、例外允許」的模式。例如，企業自主採行符合規範的適當保護措施，自行擬定具約束性企業規則，並報請歐盟個資主管機關許可，取得特定認證後，或者在取得個資當事人的明確同意之下，歐盟民眾個資便能被允許跨境傳輸。第三國對於個資的保護水準若能達到歐盟 GDPR 標準的適足性認定，取得認定資格便可自由與歐盟間進行個資跨境傳輸。可見歐盟在維護基本人權之際，仍努力降低 GDPR 為政府執法、數位經濟帶來之衝擊，試圖在個人隱私保障、國家安全與商業情報利益之間取得平衡。惟可惜，在歐盟 GDPR 實施兩年後，2020 年 6 月歐盟執委會發布關於 GDPR 的評估報告，最終認為 GDPR 雖然已實現大部分目標，但仍有改善空間。執委會亦坦承法案難以全面實施，甚至可能造成企業負擔，一些新技術也難以推行。無獨有偶，歐盟與美國於 2016 年所簽的隱私盾協議，亦在 2020 年遭歐洲法院裁定失效。歐洲法院認為該協議無法確實保障歐洲公民的資訊安全，僅允許有關國家安全、公共利益等數據訊息的國際傳輸。

歐洲議會在 2021 年 3 月 16 日發表的《歐洲資料戰略一覽》 (At a Glance—A European strategy for data) 中說明，資料代表歐洲數位轉型的驅動力。[29] 議會因此在 3 月初的全體會議期間，趁議會表決自身所提的

[29] *European Parliament* (2021), “A European Strategy for Data”. Retrieved August 5, 2021, from https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690527/EPRS_ATA(2021)690527_EN.pdf

歐洲資料戰略倡議報告和對於歐盟執委會就個人資料保護規則所做的評估做出決議之前，就資料議題進行辯論。最後，議會「公民自由、司法和內政委員會」(Committee on Civil Liberties, Justice and Home Affairs)就委員會所做的 GDPR 評估報告，[30]同樣表達對該規範實施漏洞的各種擔憂。由於各國對於隱私概念與規範的不同，加上對於數據傳輸限制標準亦不相同，未來各國仍須思考如何在維護民眾個人資料保護之際，亦能維護國家安全，維持社會、區域及經濟安全，有效保持區域社會與數字經濟之穩定及繁榮發展，進而達到互利、共榮。歐盟除藉由嚴格立法建立個人資料保護制度，設立資料保護專案辦公室用以協調、監督、整合各機關個資保護事宜，並設立專責窗口協調各地執行個資法外，亦與各國簽亦與各國簽定協議進行合作，規定重要數據資料儲存本地之義務，大力提升民眾在個資保護上之主動權，期能最終達到落實跨境資料傳輸之隱私權合法保障。

由此可知，在大數據時代下，歐盟雖對於數位經濟的發展展現強烈企圖心，仍然用心保障民眾隱私，以嚴格立法保護個人資料與數據傳輸，限制民眾資料與數據之傳輸作為商業用途。但在政府執法所需上，如能符合歐盟規範的隱私權保障，與他國之間跨境資料的傳輸仍能進行。儘管在雲端來臨、數位經濟盛行之際，無法嚴密規範數位資料之傳輸與使用，且在實施上仍會遭遇許多困境，但歐盟以立法表達對於數位人權保障之重視，仍值得各國借鏡。至於台灣企業，在全球化時代下如欲佈局全球並與歐盟進行商業往來，無論企業做為資料控管者或處理者，在蒐集和使用歐盟民眾相關個資時，務必遵守 GDPR 規範，以免遭受巨額罰款。我國政府部門則應努力與歐盟法規連結，行政部門亦應持續與歐盟溝通，以確保台灣企業在歐盟的營運業務不會受到歐盟對於 GDPR 之衝擊與影響，避免企業或機關遭受罰則。

30 同前註。

參考文獻

中文部分

丁俊和 (2019)，〈個人資訊新時代〉，《全國律師月刊》，10 月號，頁 2-4。

陳正一 (2018)，〈祖克柏國會作證為個資外洩醜聞道歉〉，《中央社》，2018 年 4 月 11 日。請見 http://www.cna.com.tw/news/firstnews/201804110011-1.aspx。

陳文生 (2016)，〈資料在地化政策與個人資料保護議題〉，《財團法人中華民國家資訊基本建設產業發展協進會》，2018 年 4 月 11 日。請見 http://www.nii.org.tw/Recents/Detail/74。

曾怡碩 (2014)，〈公私部門的雲端監偵——隱私權 / 營業秘密與國家安全 / 商業智慧之間的角力〉，《前瞻科技與管理》，4(2)，頁 65-67。

翁逸帆 (2019)，〈資訊委員的時代角色——以 GDPR 及英國 2018 年資料保護法為中心〉，《月旦法學》，286，頁 32-50。

紀珮宜 (2017)，〈由歐盟資料保護規則論被遺忘權之爭議〉，《經貿法訊》，214，頁 8-24，2017 年 5 月 25 日。

蔡柏毅 (2017)，〈歐盟個人資料保護規則導讀〉，《金融聯合徵信》，30，頁 9-18。

楊又肇 (2020)，〈GDPR 上路兩年後歐盟坦承難以全面實施〉，《聯合新聞網》，2021 年 1 月 19 日。請見 https://udn.com/news story/7086/4658955。

劉靜怡 (2019)，〈淺談 GDPR 的國際衝擊及其可能因應之道〉，《月旦法學》，286，頁 5-31。

劉耀華 (2016)，〈借歐美「隱私盾」協議，敲響我國網路數據保護的警鐘〉，《通信世界》，2016 年 8 月 8 日。請見 http://www.google.com.tw/amp/s/kknews.cc/world/lrzybe.amp。

甄美玲 (2016)，〈在一片爭議聲中「被遺忘權」在歐盟確立和實施〉，《傳媒透視》，2016 年 6 月 16 日。請見 http://gbcode.rthk.org.hk/TuniS/app3.rthk.hk/mediadigest/content.php?aid=2071。

鄭美華 (2017)，〈數位經濟時代下的非關稅障礙〉，《NCC News》，10(11)，頁 21-22。

郭家宏 (2020)，〈歐盟發布 AI 白皮書！訓練數據、過程皆有規範，將如何衝擊科技產業？〉，《科技報橘》，2020 年 2 月 20 日。請見 https://buzzorange.com/techorange/2020/02/20/european.commission-ai-white-paper/。

劉耀華 (2020)，〈歐盟公布數據治理法案，大力推動單一數字市場建立〉，《騰訊新聞》，2020 年 12 月 8 日。請見 https://xw.qq.com/cmsid/20201208A0F25C00。

〈被遺忘權在台灣是否能主張，待定！〉，《科技新報》，2016 年 7 月 24 日。請見。https://technews.tw/2016/07/24/right-to-be-forgotten-google-taiwan/。

《駐歐盟兼駐比利時代表處》，〈歐洲法院裁定隱私護盾協議失效恐波及美網路巨頭〉，《自由時報》，2020 年 7 月 16 日。請見 https://news.ltn.com.tw/ news/world/breakingnews/3231076。

〈歐盟一般資料保護規章 GDPR 簡介〉，2018 年 5 月 23 日。請見 https://www.taiwanembassy.org/be/post/6571.html。

〈嚴厲打擊美國監聽，歐洲最高法院否決歐美資料傳輸機制〉，《科技新報》，2020 年 7 月 17 日。請見 https://technews.tw/2020

/07/17/ europes-top-court-strikes-down-flagship-eu-us-data-transfer-mechanism/。

外文部分

Bureau of Justice Assistance (1934), “Communication Act of 1934”. RetrievedJune 20, 2020, from https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1288#vf4tzl

Cambridge Analytica (2016), Cambridge Analytica: Data-driven Behavior Change. Retrieved Jan 11, 2021, from https://cambridgeanalytica.org/.

Congressional Research Service Reports R44481 (2017), “ Encryption and the “Going Dark” Debate”. Retrieved August 8, 2021, from https://www.everycrsreport.com/reports/R44481.html.

European Data Protection Board (2018), “Who We Are”. Retrieved November 23, 2019, from https://edpb.europa.eu/edpb_en.

EUR-Lex (2012), “Charter of Fundamental Rights of the Eupropean Union,” *Office Journal of the European Union*. Retrieved June 17, 2021, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT.

EUR-Lex (1995), “ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,” *Office Journal of the European Union.*Retrieved June 17,2021, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

European Parliament (2021), “ A European Strategy for Data”. Retrieved August 5, 2021, from https://www.europarl.europa.eu/RegData/etudes/

ATAG/2021/690527/EPRS_ATA(2021)690527_EN.pdf.

European Commission (2017), " EU-US Privacy Shield". Retrieved August 13, 2021,from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shielden.

European Commission (2012), "EU Charter of Fundamental Rights". Retrieved August 13, 2021, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TEuropen.

European Commission (2020), "European Data Strategy". Retrieved August 13, 2021, from https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

Federal Communications Commission (2013), "Telecommunications Act of 1996". Retrieved August 8, 2021, from https://www.everycrsreport.com/reports/R44481.html.

Federal Communications Commission (2016), "U.S.-EU Safe Harbor Framework".Retrieved August 13, 2021, from https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-saf-harbor-framework.

Financial Supervisory Commission, R.O.C. Taiwan (2016), "Regulations (EU)2016/679 of the European Parliament and of the Council", *Office Journal of the European Union.* Retrieved January 10, 2022, from https://www.fsc.gov.tw/fckdowndoc?file=/4-20%20EU%20GDPR%20FINAL.pdf&flag=doc。

Information Commissioner's Office (2018), "History of the ICO." Retrieved August 5, 2021, from https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/.

McDermott, Y. (2017), "Conceptualising the Right to Data Protection

in an Era of Big Data". Big Data & Society, January-June, 1-7. Retrieved March 15, 2021, from https://journals.sagepub.com/doi/10.1177/2053951716686994.

Nitsche, L. and K. Hairsine. (2016), "What are digital rights?" DW. Retrieved March 17, 2021, from https://www.dw.com/en/what-are-digital-rights/a-36703292.

The Guardian (2015), "What is 'safe harbour' and Why Did the EUCJ just Declare It Invalid?". Retrieved August 13, 2021, from https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection.

The National Archives (2018),"The Data Protection Act 2018". Retrieved November 23, 2019, from https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The National Archives (2018), "The Data Protection Act 2018." Retrieved August 5, 2021, from https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

United Nations (1948), "Universal Declaration of Human Rights". Retrieved August 20, 2021, from https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Union Law (2016), "Regulation (EU) 2016/679 of the European Parliament and of the Council," *Official Journal of the European Union*. Retrieved August 8, 2021, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Voss, W. G. (2017), "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting," *Business Lawyer*, 72 (1): 221-233.

Weiss, M. A. and K. Archick (2016), “ U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield,” Congressional Research Service. Retrieved August 8, 2021, from https://fas.org/sgp/crs/misc/R44257.pdf.

A Study on EU Digital Human Rights Protection — A Case Study of GDPR

Pei-Shan Kao *

Abstract

In order to adapt to the advent of cloud world, internet technology and big data era, and to strengthen restrictions on personal data transmission of European Union (EU) citizens, the EU has formally implemented the "General Data Protection Regulation" (GDPR) on May 25, 2018. Compared with the "Data Protection Directive" realised by the EU in 1995, the GDPR designed and enhanced more stringent regulations for the protection of people's personal data. In addition, it also increased high fines for violations of the regulations. According to the GDPR, all companies and enterprises operating in the EU, no matter where their headquarters are located, must follow this regulation. The regulation not only sets strict regulations on cross-border data transmission and collection, but also has influence outside the region. Although it is regarded as the most stringent privacy regulation in history, the EU also explained and stated that the regulation does not include data and information processed at home by individuals for personal factors if the behavior is not related to professional or commercial activities. However, if one uses other people's data for social, cultural or financial activities outside the scope of the individual, he must be abided by this personal data protection law. Therefore, this article will take the EU's digital human rights protection as the research topic, and use the GDPR as a case study to explore the development of EU privacy protection regulations and the important implementation of this data protection

rule. It will also discuss and examine the difficulties and challenges the regulation faced after the implementation, hence making the conclusion.

Keywords: EU, Privacy, Digital Data, Data Security, GDPR

* Director of Public Relations Office & Associate Professor of Department of Border Police, Central Police University, Email: pkao@mail.cpu.edu.tw.