「GDPR 施行兩周年評估報告之分析及相關議題研析」

委託研究計畫

結案報告

委託單位：國家發展委員會

受託單位：輔仁大學學校財團法人輔仁大學

中華民國 110 年 1 月

「GDPR 施行兩周年評估報告之分析及相關議題研析」

委託研究計畫

結案報告

受委託單位：輔仁大學學校財團法人輔仁大學

研究主持人：張陳弘

研究期程：中華民國 109 年 3 月至 110 年 1 月

研究經費：新臺幣 40 萬元

國家發展委員會委託研究

中華民國 110 年 1 月

摘要

本報告第一章針對歐盟依據 GDPR 第 97 條第 1 項規定所提出的 GDPR 施行兩周年評估報告進行分析，發現整份評估報告具備以下兩項主軸：當事人權利意識的提升與行使的強化，以及創立新的治理模式、樹立新的資料運用文化。歐盟此一全球性資料運用文化的推展趨勢，臺灣勢必無法置身事外，因此，臺灣立法者於個資保護法律制定或修正時，尤應特別注意與全球接軌之需求。

本報告第二章乃說明 GDPR 關於自動剖析決策行為之規範。本報告認為 GDPR 將特別透明性要求僅適用於會對當事人產生法律影響或類似重大影響之全自動剖析決策類型的立法決定，對於個資保護有所不足；於未修法前，本報告主張可透過將演算法資料認定為個資的方式，解決適用範圍不足問題。此外，本報告主張，單純揭露演算法並不等於提供關於運算邏輯之有意義資訊；反之，未揭露演算法原貌亦不等於未提供運算邏輯之有意義資訊。透明化自動剖析決策的關鍵在：使當事人有挑戰該決策之可能。就此透明目的之達成而言，與其讓當事人理解複雜的演算法運算邏輯，不如將不被一般人所親近的程式語言轉化為具體影響因子之說明或解釋（例如供作剖析決策的資料類型、這些類型資料如何地與剖析決策相關、該決策會如何地影響當事人），俾當事人能合理預見剖析決策對其之可能影響，並有透過自己能力改變決策結果之可能。至於是否要就當事人得近用這些資訊內容之權利，給予一個新名詞「請求解釋權」為稱呼，抑或繼續沿用「近用權」一詞，應非重要。

本報告第三章乃說明有關 GDPR 規定非公務機關之正當利益（legitimate interest）權衡條款作為個資運用合法事由之適用範圍，以及相關歐盟法院判決之整理。本報告乃藉由就 WP29 於 2014 年提出的「95 指令第 7 條第 f 款規定之資料控管者之正當利益概念之意見書(Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC)」與歐盟法院(Court of Justice)自 2011 年至 2017 年間作成相關於正當利益權衡條款裁判之整理觀察，說明 GDPR 第

6 條第 1 項第 f 款之正當利益權衡事由適用之要件，以及正當利益權衡時應考量之因素。本報告希冀藉由正當利益權衡條款的論述，能更清晰地突顯個資運用合法事由的設計結構：運用行為的合法基礎建立在運用行為所追求的正當利益凌駕於當事人因此行為所損傷之權益，得對於臺灣個資法就個資運用合法事由設計不足之處，提供未來修法參考。

本報告第四章比較及分析歐盟及美國對於生物特徵資料(biometric data)之規範趨勢及實際案例。關於歐盟 GDPR 部分，主要釐清構成 GDPR 第 9 條第 1 項規定之特種個資的生物特徵資料，必須是將生物特徵資料用以獨特性地識別特定自然人始屬之；並說明 GDPR 針對構成特種資料之生物特徵資料的運用，存在哪些特別保護規範。美國法部分，關於保護生物特徵資料的一般性保護規範，最著名的乃伊利諾州(State of Illinois)於 2008 年制定的生物特徵資料隱私法(Biometric Information Privacy Act, BIPA)。本報告乃說明 BIPA 對於資料控管者運用生物特徵資料之行為的相關要求及 BIPA 適用之實際案例情形。

Abstract

Chapter I of this report provides an analysis on the EU report issued pursuant to Paragraph 1 of Article 97 of GDPR entitled “Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation.” The observation is that the said report hinges on two major aspects, i.e. the enhancement of data subject’s awareness and rights in relation to personal data protection and creation of new governance model and culture of data utilization. The new global phenomenon guided by EU for data utilization certainly will cause an impact on Taiwan. It is advisable that lawmakers shall closely follow up with the global and modern trend of personal data protection in promulgating or modifying Taiwanese personal data protection laws and consider the needs to align Taiwanese regime with relevant global standards.

Under the GDPR, the transparency requirements only apply to a decision based solely on automated processing, including profiling which produces legal effects concerning him or her or similarly significantly affects him or her. Chapter II of this report notes that the limited scope of application of the transparency restrictions is insufficient in protecting personal data. Before the relevant transparency provisions are amended to extend the scope of application, this report proposes that a feasible interim solution could be to include algorithms data as personal data so as to apply the transparency requirements on such data. This report has noted that disclosing algorithms is not equivalent to providing meaningful information about the logic involved; on the other hand, failure in disclosing the original state of algorithms is also not equivalent to not providing of the meaningful information about the logic involve. The notion of making automated processing transparent is that the data subject may have a chance to

challenge and contest the decision making. For the purpose of being transparency in data processing, it is less likely to expect data subjects to comprehend the complex algorithms logics of automated processing even if they are fully disclosed to data subjects. A more practical method to achieve data transparency is to transfer the programming languages to the real categories of data decided by automated processing; how these categories of data are related to automated processing and how such automated processing may has an impact on data subjects; accordingly, data subjects may reasonably anticipate the potential impacts caused by automated processing and to seek possible remedial methods. As to whether such right to be granted to data subjects shall be called “a right to explanation” or “the right of access”, it is not crucial.

Chapter III of this report explains the application of the legitime purpose principle and relevant clauses in the GDPR which governs the scope of utilization of personal data by private entities and introduces relevant EU court decisions. In providing analysis on the circumstances that qualify Item (f), Paragraph I of Article 6 of GDPR and factors that shall be considered in applying the legitimate purpose clause, this report considers and outlines the Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC issued by the Article 29 Data Protection Working Party (WP29) in 2014 and relevant decisions rendered by the EU Court of Justice from year 2011 to 2017. This report proposes that a more in-depth understanding of the legitimate purpose clauses under the GDPR provides useful guidance in re-designing the framework of legitimate grounds for processing personal data in Taiwanese personal data protection laws. The conclusion of the analysis is that, the legitimate grounds for processing personal data can be sought and exist only when the goal pursued in using personal data outweighs damages or losses that may cause to data

subjects. It is hopeful that the introduction and analysis of the legitimate purposes clauses under the GDPR serves as useful guidance in improving the current Taiwanese personal data protection laws, mainly by supplementing the deficiencies of legitimate causes and grounds in using personal data.

Chapter IV of this report studies and analyzes the legal framework governing biometric data and several cases. The GDPR section mainly clarifies that the biometric data that qualifies Paragraph 1 of Article 9 of the GDPR shall be the data that can distinctively identify a specific individual. In addition, this report introduces the relevant clauses in the GDPR that governs the utilization of biometric data. As to the US regulations, this report introduces the well-known general biometric data regulation, i.e. the Biometric Information Privacy Act (BIPA) promulgated in the State of Illinois in 2008. This report outlines the relevant elements in using biometric data by data controllers and the cases applying BIPA.

目錄

第一章 針對歐盟依據 GDPR 第 97 條第 1 項提出之兩周年評估報告進行分析，並提出值得我國借鏡之重點

依據歐盟於 2016 年制定公布、2018 年 8 月 25 日正式施行之「一般資料保護規則 (General Data Protection Regulation, GDPR)[1]第 97 條規定，「歐盟執行委員會(European Commission, 以下簡稱執委會)」於 2020 年 6 月 24 日提出 GDPR 實施兩週年評估報告。[2]以下為重點翻譯與摘要整理：

第一節 兩周年評估報告之翻譯整理

一、資料保護法制作為公民賦權之基石，與歐盟數位轉型之途徑 (DATA PROTECTION RULES AS A PILLAR OF CITIZENS' EMPOWERMENT AND EU'S APPROACH TO DIGITAL TRANSITION)

這是針對 GDPR 所提出的第一份評估與檢視報告。這份報告特別著眼於 GDPR 在兩方面的實施與成效： 第一，將個人資料轉移到第三國以及國際組織；第二，根據 GDPR 第 97 條規定之合作與一致性。

歐洲聯盟基本權利憲章（Charter of Fundamental Rights of the European Union）第 8 條以及歐洲聯盟運作條約（Treaty on the Functioning of the European Union, TFEU）第 16 條均規範了個人資料保護之基本權利。自 2018 年 5 月 25 日開始實施的 GDPR，正是歐盟保障此一基本權利的架構核心。GDPR 強化資料保護，賦予個人更多、更強的權利，提升透明度，確保所有在此架構下的個人資料處理者更

[1] EU, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter "GDPR"], 2016 O.J. L 119/1, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[2] European Commission, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020 COM(2020) 264 final, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN.

為負責可信。同時，讓獨立的資料保護機關擁有更強力的執法權，並建立一套新的治理體系。GDPR 也為所有在歐盟市場營運的公司提供公平的競爭環境，無論該公司在哪裡成立，均確保資料在歐盟內部的自由流通，如此也進一步強化了內部市場。

歐盟的政策制定以綠色轉型以及數位轉型為其兩大特色，強調以人為中心的科技應用，而 GDPR 在這當中扮演極為重要的角色。這在最近的兩份報告中都曾提出：「人工智慧白皮書 (White Paper on Artificial Intelligence)」以及 2020 年 2 月的 「歐洲通訊資料策略 (Communication on a European Strategy for Data) (以下簡稱資料策略)」。

現代經濟日漸依賴各種資料，包括個人資料的運用。GDPR 提供一項重要的工具，確保個人對其個人資料有更佳的掌控，且使這些個資的運用具有正當理由，並以合法、公平、透明的方式進行。同時，GDPR 所採用的以風險為本之方法與原則，例如隱私設計與預設 (privacy by design and by default)，有助於促進可信的創新。執委會提議，為補強資料保護與隱私權的立法架構，將以 e-Privacy Regulation 取代現有的 e-Privacy Directive。這項提議現正由共同立法者們 (co-legislators)評估，並確保其能盡快實施。

個人資料保護乃「歐洲適應數位時代(Europe fit for the digital age)」以及「歐洲綠色協議(European Green Deal)」的優先重點項目。為此，執委會將制定新措施，賦予公民更大力量以在數位轉型中扮演更積極的角色，並將控制數位工具的使用，以利於建立水土中立 (climate-neutral)的社會，促進永續發展。GDPR 替這些新措施建立了基礎架構，確保它的設計能有效賦予個人控制力。

「資料策略」提倡「單一的歐洲資料空間 (a single European data space)」，一個真正的單一資料市場，同時也在綠色轉型與數位轉型的十項相關領域上，創造共同歐洲資料空間 (common European data spaces)。在這些努力當中，最重要的即是建立一個明確可行的架構，一方面讓資料得以安全分享，一方面增加資料的可用性(availability)。

「資料策略」也公布執委會計畫在未來立法中，探討在基於科學研究的需要下，如何以符合 GDPR 規範的方式使用公共資料庫(public database)中的資料。「歐洲雲端聯盟(European cloud federation)」也將支援資料空間(data spaces)，提供符合 GDPR 規範的資料處理以及雲端基礎架構服務。GDPR 確保個人資料受到高度保護(high level of protection)，並賦予個人在各種資料空間中的核心角色；於此同時，也將依情況提供必要的彈性。

很顯然地，不只是歐盟在確保互信及個資保護方面有強烈需求，世界各地的人們都日漸重視個資的隱私與安全。一項最近的全球調查指出，個人在進行消費選擇以及網路活動時，都將資料安全視為重要的考量因素。基於對隱私的日漸重視，已有越來越多公司主動將 GDPR 對個資安全隱私的保護，延伸適用到歐盟以外的顧客。許多企業為提升其對個資的尊重保護，提供創新的產品與服務，乃搭配全新的隱私與資料安全方案，以此作為在全球市場的競爭優勢與賣點。另外，不論在公共部門或私營部門，管理者對大規模資料蒐集與運用的能力均日漸強大，使隱私權在世界上許多不同地方，都逐漸成為重要且複雜的公共辯論焦點。

許多歐盟以外國家都在評估，是否將遵從歐盟所採用的 GDPR，從智利到南韓，巴西到日本，肯亞到印度，美國加州到印尼，這已成為全球性的趨勢。歐盟在資料保護方面居領導地位，可為數位經濟管理設下全球化的標準。國際組織中的一些重要人物，也認可歐盟在此方面的重要性，聯合國秘書長 Antonio Guterres 就曾指出，GDPR 已經「建立一個模範...讓他國能參考並採取相似手段」，他同時也「敦促歐盟及其會員國，繼續帶領數位時代的轉型，扮演科技創新與管理(innovation and regulation)的關鍵角色。」

COVID-19 疫情現今仍未停息，在世界各國陷入危機，急於尋求解決之道的同時，更凸顯出隱私權已成為全球性的重要議題。在歐盟，許多會員國皆採取緊急措施以試圖保護公共衛生。GDPR 明確規範，任何限制措施都必須尊重基本權利和自由的本質(essence)，且必須是

為了民主社會的公共利益，例如，為了保護公共衛生所採取的必要相應措施。隨著控制疫情的各種措施紛紛啟動，決策者需要回應公民的期待，提供他們可信賴的數位解決方案，且這些方案須尊重個人對於隱私及個資保護的權利。

為了追蹤控制病毒的擴散、調整公共政策的應對措施、提供病患協助或實施退場策略，許多國家紛紛推出以資料驅動的解決方案。為確保其可靠性及考量社會接受度，必須將隱私權保護內建(built-in) 在方案當中，例如：使用者自願加入(voluntary signing up by users)、資料最少化(data minimization)和資訊安全，以及排除地理位置資訊(exclusion of geolocation)等方法。歐盟所實施的資料保護與隱私權立法架構 (data protection and privacy legislative framework)已證明為足夠靈活的工具，一方面能讓實用的解決方案(例如接觸史追蹤應用程式)得以發展，一方面又能確保高程度的個資保護。有鑑於此，執委會在 2020 年 4 月 16 日公布接觸追蹤應用程式的指導方針，在對抗全球疫情的戰役中，給予資料保護方面的支持。

個資保護也有助於預防對公民選擇的操控(manipulation)，尤其是經由不合法的個資運用對選民所進行的精準投放(micro-targeting)。同時，保護個資也助於避免民主過程中的干預，保留民主中公開辯論、公平與透明這些不可或缺的要素。因此，在 2018 年 9 月，執委會公布歐盟資料保護法在選舉方面的應用指導方針。

在這次的評估報告中，執委會考量各方所做出的貢獻，包括歐盟理事會(the Council)、歐洲議會(European Parliament)、歐盟個人資料保護委員會(European Data Protection Board，以下簡稱 EDPB[3])、獨立資料保護機構、多方利益相關之專家團體(the Multi-stakeholder expert Group)，以及其他利害關係人，同時也將各方的意見反饋一併納入評估。

[3] EDPB 乃依據 GDPR 第 68 條以下規定所成立之委員會，其成員由歐盟各會員國之個資保護專責機關之首長組成；其任務乃在確保 GDPR 的一致適用性，並就 GDPR 的解釋適用，發布指引、建議及最佳作法。EDPB 之角色相當於 95 指令時期之歐盟資料保護工作小組 (Article 29 Data Protection Working Party, WP29)，https://edpb.europa.eu/about-edpb/about-edpb_en (last visited June 24, 2020)。

在 GDPR 實施兩年後，一般認為已成功達成其目標：強化保護個人對個資保護的權利，以及保障個資能在歐盟自由流通。然而，未來仍然有些方面需要改善。如同大部分利害關係人和資料保護機構所指，執委會也認為，在現階段要對 GDPR 的實施成效給出具體結論還言之過早。會員國及其他利害關係人所提出的大多數問題，在未來幾年，應該都能藉由實施 GDPR 所持續累積的經驗得到改善。惟此份報告仍將指出實施 GDPR 至目前為止所遭遇的挑戰，並試圖提出可能的解決方法。

儘管此份評估報告的重點在 GDPR 第 97 條第 2 項的內容，也就是國際間資料移轉以及合作與適用一致性機制，但也將討論並回應過去兩年當中各方所提出的意見與疑問。

二、 主要發現(MAIN FINDINGS)

- GDPR 的實施以及合作與一致性機制的運作(Enforcement of the GDPR and the functioning of the cooperation and consistency mechanisms)

GDPR 創立新的治理模式，會員國各自擁有獨立的資料保護機關，合作處理跨境案件並共同成立 EDPB。總體評估來說，資料保護機關平衡使用各種強化後的糾正權(corrective powers)，包括警告、譴責、行政罰鍰，以及暫時或永久限制資料運用。執委會指出，資料保護機關視侵權之嚴重性，曾開出幾千歐元到幾百萬歐元不等的行政罰鍰。其他禁令，如禁止資料運用，也產生和罰鍰相當甚至更高程度的嚇阻效果(deterrent effect)。GDPR 的最終目標，是要改變所有相關行動者(actors)的文化與行為以確保個人權利。

雖然現在還無法完整評價新的合作與適用一致性機制，各會員國的資料保護機關藉由建立「一站式機制」(one-stop-shop mechanism)以及大量互助，已逐步發展合作關係。「一站式機制」乃內部市場(internal market)的重要資產，可用來判定許多跨境案件。凡涉及跨境

資料運用的案件，均適用於一站式機制，目前有許多這類重要案件仍在等待判決。這類案件通常涉及大型跨國科技公司，其判決將對很多會員國的個人權利有重大影響。

然而，要在各資料保護機關間形成共同的歐洲資料保護文化，是一項仍在持續進行的過程。資料保護機關尚未完全使用到 GDPR 提供的所有工具，例如，聯合作業(joint operation)，以及可能因此而展開的聯合調查(joint investigation)。

歐盟之間跨境案件的處理應該要能更有效率、更和諧(harmonized)。若以程序上來說，以下幾點都需要進一步改善：救濟提起處理程序(complaint handling procedure)、救濟提起可受理標準(admissibility criteria for complaints)等。EDPB 以及執委會已開始共同思考討論可能的改善方式。

對於 EDPB 及利害關係人之間的持續交流與發展，EDPB 的引導與行動至關重要。至 2019 年年底為止，EDPB 已採用了 67 份文件，包含 10 份新的指引(guidelines)以及 43 份意見(opinions)。利害關係人對於 EDPB 所發布的指引大多表示歡迎，並且針對 GDPR 的主要概念(key concepts)要求額外的指引，但他們也提出國家方針(guidance)和 EDPB 指引間存在某些歧異，並且強調：EDPB 需要給予更多實際的建議，尤其是具體的例子；再者，資料保護機關需要具備更多人力、科技與財務資源，以有效執行其任務。

執委會不斷強調，會員國有義務分配足夠的人力、財務與科技資源給國家資料保護機關。2016 到 2019 年期間，大多數機關都大幅增加了人力及預算。其中，愛爾蘭、荷蘭、冰島、盧森堡以及芬蘭機關的人力在比例上來說增加最多。由於最大的一些跨國科技公司均在愛爾蘭及盧森堡設立，這兩國的資料保護機關在許多重要跨境案件中擔任領頭羊角色，因此對於人力的需求也較他國更高。然而，各會員國資料保護機關的情況仍不盡相同，整體上也不盡理想。資料保護機關的角色極為重要，不只確保 GDPR 在國家層級的實施，也確保 EDPB 內合作與一致性機制能有效運作，尤其是以一站式機制處理跨境案件。

也因此，GDPR 要求各會員國必須提供足夠資源讓專責機關加以運用。

- 使法制和諧，但仍保留一定程度的分殊化之方法(Harmonized rules but still a degree of fragmentation and delivering approaches)

執委會也監督會員國立法(national legislation)上對 GDPR 的實施情況。在這份報告發表之時，除斯洛維尼亞(Slovenia)以外，其他會員國都已採用新的立法，或已修改其國家資料保護法以符合歐盟規範。斯洛維尼亞已被要求向執委會說明此法律調適過程的最後結果。

儘管 GDPR 提供了一套具有一致性、可在全歐盟通用的資料保護法律，仍需要會員國在某些方面的立法，並在其他方面提供進一步具體實施 GDPR 的可能性制度。也因此，GDPR 的實施情況在各國並不一致，尤其是因為條件式規範條款(facultative specification clauses)的廣泛使用。舉例來說，各會員國對於同意兒童使用資訊社會服務的年齡有不同規範，這讓兒童和家長在單一市場(Single Market)中所適用的個資保護權利產生不確定性。這種不一致性也讓跨境商業活動與創新面臨挑戰，尤其是在新科技發展與網路安全解決方案這兩方面。為使內部市場有效運作，並且避免造成公司不必要的負擔，國家法律不應超出 GDPR 所規範之框架(margins)，也不應在沒有 GDPR 框架下制定額外要求。

國家在立法時會面臨一項特殊挑戰，即如何調和(reconciliation)以下兩者並取得平衡：個資保護的權利，以及表現和資訊的自由(freedom of expression and information)。有些國家法律將表現自由視為優先；有些國家則偏重對個資的保護，只在少數特殊情況下豁免個資保護法的運用，比如涉及有公共地位之人時。另外，也有一些會員國藉由立法者達到某種平衡，以及/或是藉由逐案審視(case-by-case assessment)決定是否減縮(derogations)GDPR 的適用範圍。

執委會將持續對國家立法予以評鑑。調和(reconciliation)必須由法律提供、尊重這些基本權利之本質、符合比例且必須的。資料保護法

(以及其解釋與適用)不可影響行使表現與資訊的自由，比如說，以揭露其資料來源對新聞記者施加壓力或製造恐懼感。國家法律於這兩種權利間的權衡取捨，必須符合歐盟法院(Court of Justice)以及歐洲人權法院(European Court of Human Rights)的判例法(case law)。

在廢除處理特殊類別個資的一般禁令時，各會員國法律會遵循不同的實施途徑。為此，執委會的第一步，正是著手調查各會員國的不同實施途徑；接下來，執委會將致力於建立「行為準則(codes of conducts)」，使各會員國間能達成更高的一致性，以使個資的跨境運用更為簡單。另外，EDPB 未來將針對科學研究領域提出個資運用指引，也有助於使會員國間的實施途徑趨於一致。執委會將提供 EDPB 建議，尤其是與健康研究相關時，比如當研究社群遭遇某些特定情況時，執委會將針對此特定情況提出具體說明與分析。

- 賦予個人力量控制其個資(Empowering individuals to control their data)

根據一份基本權利調查(Fundamental Rights Survey)，歐盟 16 歲以上之人口有 69%聽聞過 GDPR，全部人口中 71%的人知道其國家的資料保護機關。

個人對於其權利意識日漸提升，包括：接近使用權、更正權、刪除權、資料可攜權、拒絕權，以及資料運用透明化。GDPR 強化程序權(procedural rights)，使其包含向資料保護機關提出救濟的權利，例如透過代表訴訟(representative actions)，以及司法救濟(judicial redress)。雖然當事人對這些權利日漸熟悉，但仍需進一步使權利行使及執法更加便利。EDPB 一方面正審慎思考，未來將釐清並進一步促進當事人權利的行使，另一方面也計畫提出關於代表訴訟(representative actions)的指令(Directive)。此計畫一旦被採納，將使當事人能在所有會員國發起集體訴訟(collective actions)，降低跨境訴訟(cross-border actions)的成本。

資料可攜權(the right to data portability)尚有許多潛在利益還未被充分利用。它能使當事人自由轉換在不同資料控管者之間、結合不同服務、利用各種創新服務、選擇資料保護最為完善的服務，資料可攜權可說是間接促進了競爭並支持創新。也因此，執委會的優先事項之一，便是開發此權利的諸多潛在利益，尤其隨著物聯網的逐漸普及，越來越多的資料是由消費者產出，也因此增加了消費者面對不公平手段和閉鎖效用('lock-in'effects)的風險。此外，資料可攜權還可在以下方面產生重大效益：身體保健、減少環境足跡、取得公共或私人服務、提高製造業生產力，以及提升產品品質及安全。

「資料策略」十分重視解決眼前資料可攜權面臨的困難，例如目前缺乏一套標準，使資料能以機器可判讀的格式提供；另外，資料可攜權現在只侷限於少數領域(如：銀行、電子通訊)，未來應加以充分開發利用。解決之道，除了可以藉由設計適當的工具，以及將格式與介面標準化，也可以透過強制規範科技界面及機器可讀格式，讓資料可以即時(real-time)傳送攜帶。若能更廣泛使用資料可攜權，則可讓個人能較輕易分享其資料以促進公共利益（例如：參與健康領域的研究），當然，這必須在當事人自願的情況下（資料利他主義，data altruism）。為了替數位服務法(Digital Services Act)相關配套做準備，執委會將更廣泛思考資料與資料相關行為(data-related practices)在平台生態系統(platform ecosystem)中所扮演的角色。

- 組織與中小企業的機會與挑戰(Opportunities and challenges for organisations, in particular small and medium-sized enterprises)

GDPR 結合「非個人資料自由流通規則(Free Flow of Non-Personal Data Regulation)」，能提供企業嶄新機會，促進競爭與創新，確保資料在歐盟內部自由流通，同時，也提供歐盟以外的企業公平競爭的環境。資料可攜權的行使，加上越來越多人試圖尋找更為隱私友善(privacy-friendly)的解決方案，可以幫助企業降低進入市場的門檻，而基於信任與創新，也將提供企業成長的機會。

某些利害關係者認為，GDPR 的適用具有挑戰性，尤其是對中小企業(small and medium-sized enterprises, SMEs)而言。但基於以風險為本之方法 (risk-based approach)，根據經營者規模大小減縮 GDPR 適用範圍並不恰當，因為只考量經營者規模，並不足以評估其運用個資的過程可能對當事人產生的風險。許多資料保護機關已提供實用性工具輔助，以促進中小企業履行 GDPR，採用低風險的個資處理方式。在未來，歐盟應共同積極、廣泛的推行這些努力，避免造成單一市場履行 GDPR 的阻礙。

資料保護機關已發展出許多方式幫助中小企業履行 GDPR 的工具，例如：提供簽約程序範本(templates for processing contracts)、個資運用活動紀錄(records for processing activities)、諮商研討及熱線服務等，且其中有部分措施是由歐盟提供財務支持。未來仍需更多有效方案，以促進中小企業履行 GDPR。

GDPR 為所有類型的公司和組織提供一個工具箱(Toolbox)，以幫助其履行 GDPR，例如：行為準則、認證機制和標準契約條款。這當中的每項工具都應發揮最大效用：行為準則是替中小企業量身訂做，且不包含不成比例的費用，對中小企業來說至為重要且效益最大。至於認證機制，在 GDPR 的框架下，安全(包含網路安全)以及資料保護設計是主要考量關鍵，且最好是可通行全歐盟的共同解決方案。另外，執委會目前也正在研商資料控管者(controllers)與受託運用者(processors)之間的標準契約條款，以配合國際傳輸標準契約條款的持續現代化過程。

- GDPR 應用於新科技(the application of the GDPR to new technologies)

GDPR 對不同科技的運用採取中性立場。此中立設計原則使 GDPR 能適用於各類型新科技的發展。

GDPR 被視為一項重要且靈活的工具，可確保新科技的發展不違背基本權利的保障。在 COVID-19 疫情危機中，GDPR 的資料保護與

隱私權立法架構證明其重要性與靈活性，特別是在設計接觸史追蹤應用程式(tracing apps)和其他科技解決方案，以防堵疫情擴散。未來的挑戰在於闡明如何將已實踐的資料保護原則，應用於需要持續監控的人工智慧、區塊鏈、物聯網或臉部辨識等特定科技。例如，執委會於人工智慧白皮書中開放公共辯論，在哪些特殊情況下，應該允許公共場所使用人工智慧進行遠距生物辨識(如臉部辨識)，以及共同的保障措施。在這方面，資料保護機關應該在新科技設計發展的早期過程，就做好相應準備。

再者，在面對大型數位平台整合公司，包含線上廣告和精準投放(micro-targeting)等領域時，GDPR 的有效、強力執法對於保護個人權利更顯重要。

- 發展現代化的國際資料傳輸工具箱(Developing a modern international data transfer toolbox)

GDPR 提供了一個現代化的工具箱，在促進個人資料從歐盟傳輸到第三國或國際組織的同時，也能確保資料繼續受到高度保護。在過去兩年，執委會積極動用 GDPR 框架下所擁有的工具，促使其發揮最大潛力。

這包括與關鍵合作夥伴積極接觸，以期達成「適足性認定(adequacy decision)」。這種認定的效果能使個人資料得以安全和自由地傳輸至相關的第三國，而無需資料出口國提供進一步的保障措施或獲得任何授權。尤其是 2019 年 2 月生效的「歐盟-日本相互適足性認定(EU-Japan mutual adequacy decisions」創造了全球最大的自由和安全資料流通領域。此外，與韓國的適足性認定正處於發展階段，且正在與亞洲和拉丁美洲的其他重要夥伴進行開放性會談。

歐盟在未來與英國的關係中，適足性認定也扮演重要的角色。適足性認定是貿易(包括數位貿易)的有利因素，也是在執法與安全領域進行密切積極合作的先決條件。此外，要確保兩個如此緊密結合的經濟體之間的公平競爭，資料保護方面的高度一致性是重要因素。根據

關於歐盟與英國未來關係的政治宣言(Political Declaration on the Future Relationship between the EU and the UK)，執委會目前正在根據 GDPR 和資料保護執法指令(the Data Protection Law Enforcement Directive)進行適足性評估。

本報告作為 GDPR 第一次的評估，執委會還需要重新審查根據 95 指令時期通過的適足性認定。執委會與 11 個有關的第三國均進行了對話，以評估其自通過適足性認定以來，該國的資料保護系統如何演變，以及其是否符合現行 GDPR 規定的標準。適足性認定乃貿易及國際合作的關鍵工具，因此，這其中許多國家，為能持續符合適足性認定，均針對其隱私權法予以強化與現代化。同時，額外的保障措施也正列入討論，以處理各國在資料保護方面的差異性。

然而，由於歐盟法院(Court of Justice)將於 2020 年 7 月 16 日公告一項判決，針對部分適足性標準的相關要點加以釐清，執委會將在歐盟法院作成此件判決後，再對適足性認定的現有評估提出個別報告。

除了進行適足性認定以外，執委會也正進行標準化契約條款的全面現代化，依據 GDPR 訂定的規範加以調整，以期更佳反映現代數位經濟的處理操作現況，並考量可能產生的各種需求，以進一步釐清某些保障措施。這些契約條款代表了目前最廣為使用的資料傳輸機制，有數以千計的歐盟公司依此條款提供各式服務給客戶、供應商、經營夥伴以及員工。

在推動 GDPR 的國際發展上，EDPB 扮演重要角色，它提供現有傳輸機制最新指引(guidance)，例如有拘束力的企業守則(binding corporate rules)以及所謂的「例外情形 (derogations)」；同時，EDPB 也幫助建立法律的基礎架構，如行為準則與認證方針，以利於使用 GDPR 所提供的新工具。

為使利害關係人能充分利用 GDPR 資料傳輸工具，EDPB 必須加強其現行於各種傳輸機制的工作，包括進一步簡化有拘束力的企業守則之批准程序，確定做為傳輸工具的行為準則與認證方針，並釐清「國

際資料傳輸規定」(第五章)與 GDPR 領土適用範圍(第 3 條)之間的競合。

另一項 GDPR 的重要國際面向，就是 GDPR 的域外延伸效力(extended territorial scope)，範圍包含歐盟市場上活躍的國外營運者。為確保有效遵守 GDPR 與建立公平的競爭環境，資料保護機關的執法行動必須適切反映域外效力適用範圍。進行資料運用之外國企業，若設立據點在歐盟以外，資料保護機關在需要時必須能要求其在歐盟境內之代表。執法機關需更強力執法，以明確傳達以下立場：即便外國企業在歐盟沒有設立據點，亦不能免除其本應負擔的 GDPR 的責任。

- 在資料保護方面促進融合與國際合作(Promoting convergence and international cooperation in the area of data protection)

GDPR 已經成為國際上資料保護的重要參考依據，且促使許多國家思考建立現代化的隱私權規範。這股促進全球一致性的趨勢帶來許多正向發展，一方面在資料進行國際傳輸時，可加強個人資料安全的保護；另一方面也同時可以促進資料的流通。

在此一趨勢的基礎上，執委會加強一些雙邊、區域和多邊論壇的對話，以促進尊重隱私的全球文化，並推展不同隱私制度之間的融合。在這過程中，歐盟對外事務部(European External Action Service)以及歐盟在第三國家和國際組織代表團的關係網路，都給予執委會積極有力的支持。這些努力使歐盟政策的不同面向間，能有更好的一致性與互補性—從貿易到歐盟與非洲的新夥伴關係皆是如此。G20 和 G7 最近也認可資料保護對數位經濟和資訊流通的貢獻，特別是最先在日本 G20 中提出的「具信任的資料自由流通」概念。「資料策略」中特別強調，執委會嘗試繼續推廣與受信賴夥伴間的資料共享(data sharing)，並同時對抗濫用(abuse)，例如(國外)公務機關不符比例的存取(disproportionate access)個人資料。

為了促進國際上資料保護標準之和諧與一致性，也為了便利資料流通以促進貿易，執委會決心解決「資料策略」中強調的數位保護主義問題。為此，執委會制定了貿易協定中關於資料流通與保護的具體規定，並在雙邊談判（最近一次是與澳洲、紐西蘭及英國）和多邊談判（如當前世界貿易組織的電子商務談判）中列出該條款，排除不合理的限制，例如強制資料在地化之要求。於此同時，也保持各方的監管自主權，以保障資料保護的基本權利。

貿易及資料保護工具(instruments)兩者應共同發展，以確保國際資料流通的自由與安全。這在數位化經濟的發展中，對歐盟企業（包含中小企業）的營運、競爭力與未來成長都極為重要。

同樣地，當活躍於歐洲市場的企業因執法目的而被合法要求分享資料時，必須確保這些企業不須面對法律衝突(conflicts)，且能完全顧及歐盟所保護的基本權利。為了使資料傳輸更順利，執委會決心要與國際夥伴共同建立適宜的法律架構，以避免法律衝突並支持有效之合作形式。其中特別值得注意的是提供必要的資料保護措施(data protection safeguards)，同時以此更有效打擊犯罪。

最後，當發生隱私問題或資料安全事件，可能同時影響多個司法管轄區的多數人時，應進一步加強歐盟和國際監管機構之間的實質合作。特別需要制定適當的法律規範，以便發展更密切的合作與互助，包括允許在調查過程中進行必要的資訊交流。基於同樣精神，執委會正在成立「資料保護學會」(Data Protection Academy)，此平台能讓歐盟和外國資料保護機關分享知識、經驗和最佳做法，以促進並支持隱私執法者之間的合作。

三、 未來前進之路(WAY FORWARD)

為使 GDPR 發揮最大潛力，建立一致性方法(harmonized approach)以及歐盟資料保護的共同文化非常重要，同時也應致力於讓跨境案件的處理更加有效率。這是人民與企業所共同期盼，也是歐盟資料保護

法制改革的重要目標。同樣至關重要的，還有讓個人及企業都能充分利用 GDPR 提供的所有工具，以確保其能有效履行 GDPR。

執委會將繼續針對 GDPR 的實施與會員國進行雙邊交流，也會在必要情況下，運用其所擁有之工具，促進會員國履行 GDPR 的義務。

由於針對各會員國之法律之評估仍在持續進行中(因 GDPR 正式實施之期間尚短)，且許多會員國之特定法律仍在修改中，因此要對現在各國立法間存在歧異(fragmentation)的程度下結論，還言之過早。至於因會員國實施特別限制條款(specification clauses)所造成的法律衝突(conflicts of laws)，則需要更了解其對控管者(controllers)及受託運用者(processors)所帶來的後果。

在持續追蹤這些議題時，會員國法院(national courts)以及歐盟法院的相關判例法(case law)有助於提供對資料保護法規的一致性解釋。會員國法院近期曾作成判決，判定國家法律中某些偏離 GDPR 的條款(provisions)無效。

至於國際方面，執委會將繼續聚焦於促進資料保護法規的一致性，以確保資料流通之安全。這包括例如持續進行改革新的或即時的資料保護法，或是在多邊論壇中推動「具信任的資料流通(Data Free Flow with Trust)」的概念。同時，也包括各種的適足性(adequacy)對話，以及更新標準契約條款和奠定認證機制的基礎架構，以達成傳輸工具箱的現代化與擴充。這其中也包含國際協商(比如在電子化證據的跨境存取方面)，以確保資料進行傳輸時有適當的資料保護措施。最後，執委會也將參與資料保護執法者之間的協商，探討如何促進國際合作與互相協助，並致力於徹底落實一致性之推動。

根據 GDPR 自 2018 年 5 月實施後的評估結果，以下列出後續為支持 GDPR 實施所應採取的行動。在 2024 年提出下一次評估報告前，執委會將持續監督實施成效。

(一)法律架構的實施與補充(Implementing and complementing the legal framework)

會員國應：

- 確認內國法與 GDPR 的一致性；
- 考慮特別限制條款的使用，因特別條款可能造成各國資料保護規範的歧異，危及歐盟內部資料的自由流通；
- 評估實施 GDPR 的國家法律是否在一切情況下都符合 GDPR 設定給會員國的立法框架。

執委會將：

- 就會員國遵守 GDPR 的情況與會員國進行雙邊交流(包括國家資料保護機關的獨立性和資源問題)；善用所有可運用工具，以確保會員國遵守 GDPR；
- 支持會員國間進一步交換意見與做法，討論針對國家層級所需的個別調整，應如何減少其造成個別市場的分歧程度，例如：擁有和健康及研究相關的個資，或是與其他權利如表現自由求取平衡；
- 支持資料保護架構一致性地應用於新技術，以支持創新和科技發展；
- 依據未來經驗和相關的判例法，探討 GDPR 某些條款未來可能的修訂,特別是關於個人資料運用非為其核心業務(低風險)的中小企業的運用記錄，以及資訊服務有關的兒童同意年齡。

(二)使新治理系統發揮全部潛力（Making the new governance system deliver its full potential）

EDPB 和資料保護機關應：

- 各資料保護機關間應更有效率地進行各項籌備工作，借助各會員國的強項並由秘書處積極投入，以強化關於合作與一致性機制的運作，包含程序(procedural)方面；
- 利用所掌握的一切手段，支持 GDPR 的適用與執行，包括進一步釐清 GDPR 的主要概念，以及確保國家指導完全符合 EDPB 通過的指引；
- 鼓勵使用 GDPR 中規定的所有工具，以確保 GDPR 得到一致性的實施；
- 在資料保護機關間建立合作關係，例如發展聯合調查。

執委會將：

- 繼續密切觀察各國資料保護機關的獨立性與執行效率；
- 鼓勵各國資料保護機關間的相互合作(特別是在競爭、電子通訊、網路和資訊安全系統以及消費者政策等領域)；
- 支持 EDPB 針對國家保護機關所採取的程序進行思考，以改進跨境案件的合作。

會員國應：

- 為資料保護機關分配足夠資源，使其能有效執行任務。

(三)對於利害關係人的支持(Supporting stakeholders)

EDPB 和各國資料保護機關應：

- 進一步訂定各項切實可行、易於理解的指引，並對 GDPR 的適用提供明確解釋、避免含糊不清。例如兒童資料之運用與當事人的權利行使，包括行使接近使用權及刪除權，並在過程中諮詢利害關係人；
- 隨著執行上的經驗與進展，當需要進一步釐清時，重新檢視指引，包含歐盟法院的判例法；

- 發展實用的工具，例如資料外洩時的一致性表格(harmonized forms for data breach)以及資料運用活動的簡化記錄，以幫助中小企業履行 GDPR 義務。

執委會將：

- 提供國際傳輸及資料控管者與受託運用者間關係的標準契約條款；
- 提供說明並支持將資料保護規定應用於兒童的工具；
- 根據「資料策略」，尋求確實可行的方法，促進個人利用可攜權，例如讓個人控制其資料的近用權及使用機器產生的資料；
- 通過歐盟網路安全局(ENISA)、資料保護機關和 EDPB 之間的合作，支持資料運用的標準化與認證、尤其是關於網路安全方面；
- 要求 EDPB 就與利害關係人相關的重要具體問題訂定指引；
- 必要時提供指導，同時充分尊重 EDPB 的功能；
- 支持資料保護機關的行動，透過財政支持幫助中小企業履行 GDPR 義務，特別是提供可在其他會員國適用的實用方針與數位工具。

(四)鼓勵創新(Encouraging innovation)

執委會將：

- 密切觀察 GDPR 對創新技術應用的影響，同時考慮在人工智慧領域和「資料策略」下，未來可能採取的行動；
- 鼓勵起草歐盟衛生和研究領域的行為準則(包括提供財政支援)；
- 密切關注 COVID-19 防疫期間之相關應用程式的開發與使用。

EDPB 將：

- 發布 GDPR 在科學研究、人工智慧、區塊鏈和可能的其他科技發展領域的指引；
- 因應科技發展，需要進一步澄清時，應審查該指引。

(五)進一步開發有助於資料傳輸的工具包(Further developing the toolkit for data transfer)

執委會將：

- 根據其 2017 年於「在全球化世界中交換和保護個人資料」中提出的策略，與感興趣的第三國家進行充分對話；這也包括盡快完成與南韓的適足性評估過程(adequacy process)；
- 完成對現有適足性認定的持續評估，並向歐洲議會和理事會報告；
- 完成標準契約條款現代化的工作，以期更新 GDPR 的實施操作，並更好地反映現代商業慣例。

EDPB 將：

- 進一步澄清國際資料傳輸規定(第五章)與 GDPR 領土適用範圍(第 3 條)之間的競合；
- 確保對在第三國設立據點，且落入 GDPR 適用範圍內的經營者進行有效執法，包括需要時任命代表(第 27 條)；
- 簡化具有拘束力的企業守則的批准程序；
- 完成資料傳輸工具的行為準則和認證機制的架構、程序與評鑑標準。

(六)促進融合和發展國際合作(Promoting convergence and developing international cooperation)

執委會將：

- 通過分享經驗和最佳做法，幫助第三國進行新的或現代化的資料保護規則修訂；
- 與非洲夥伴合作，促進資料保護的一致性，並幫助強化其監管機關的能力，以發展歐盟--非洲的新數位夥伴關係；
- 評估如何促進私人企業與執法當局之間的合作，包括：當國外刑法執法機構要存取電子證據時，應協商出資料傳輸的雙邊及多邊架構，以避免法律上的衝突，同時也確保具有完善資料保護措施；
- 與經合組織(OECD)、東協(ASEAN)或 G20 等國際和區域組織合作，促進基於高資料保護標準的可信任的資料流通；
- 設立「資料保護學會」(Data Protection Academy)，增進與幫助歐洲與國際間交流；
- 促進與各國監管機關之間的國際執法合作，包括通過談判合作和互助協定的方式。

第二節 兩周年評估報告之摘要整理

一、報告主旨

（一）GDPR 創立新的治理模式、樹立新的資料運用文化

GDPR 加強資料保護，賦予個人更多的權利，增加透明度，使所有資料控管者更負責及更可被信賴。搭配具有有效執法權力的獨立性國家資料保護機關，讓 GDPR 的實施更具實效性。

GDPR 建立一套新的治理體系，建立一站式機制，並透過會員國與區域組織間的合作及適用一致性的提升，為所有在歐盟市場營運的公司提供公平競爭環境，無論該公司在哪裡成立，均確保資料在歐盟內部的自由流通，促進安全的國際資料傳輸。

（二）GDPR 實施兩年的核心成果

GDPR（資料保護）作為強化公民賦權之支柱與歐盟之數位轉型的重要力量。

二、評估重點

（一）當事人權利行使的強化與權利意識的提升

GDPR 賦予個人得行使例如接近使用權、更正權、刪除權、拒絕權與資料可攜權。

GDPR 使個人於數位轉型之過程中，對其個人資料的利用扮演更積極的角色。以資料可攜權之行使為例，此權利仍存有許多潛在利益，尚未獲得充分開發利用。它能使當事人得更簡易地在不同的服務提供者之間切換，組合不同的服務或使用其他創新服務，並選擇最有利於資料保護的服務。資料可攜權能間接地促進競爭並支持創新，此權利的使用開發，列為執委會的優先事項之一。

（二）GDPR 創立新的治理模式（樹立新的資料運用文化）

1. 獨立專責的資料保護機關搭配強化的執法權力

從警告、譴責、行政罰鍰，到限制資料運用行為，GDPR 規定有效方法（工具）提供獨立專責的資料保護機關用以執行。然而，仍需要搭配必要的人力、技術與財政資源。有鑑於此，許多會員國對於專責機關的預算和人力配置，均有顯著增加。總體來說，於 2016 年至 2019 年間的歐盟會員國資料保護機關共有 42%的新增人力和 49%的新增預算。

2. 一站式機制 (one-stop-shop)的建立

GDPR 建立「一站式機制」，確保 GDPR 可以得到一致且有效率的實踐。亦即，提供一家公司就跨境資料的運用，得以該公司主要機構所在的會員國的資料保護機關作為遵法聯繫窗口，建立公司的個資

保護機制，而無須在資料所跨境的每個國家都為之。當然，此一站式機制的建立，仰賴各會員國間的合作與 GDPR 適用之一致性。

3. 適用一致性的建立

例如透過 EDPB 針對 GDPR 解釋適用與新興資料保護議題所發布之指引，或資料保護機關也能開發一些易於使用的技術工具，讓人民與企業能易於詢問資料保護問題，幫助 GDPR 適用一致性的提升。

4. 合作的建立

過去兩年間，執委會在自由與安全的資料傳輸方面的國際參與，產生重要的影響。歐盟現在與日本共享世界上最大的自由和安全地區資料流通利益。此外，執委會還與 EDPB 合作，考慮將其他資料傳輸機制予以更新，包括訂立標準契約條款，及廣泛使用的資料傳輸工具。EDPB 正在就於歐盟以外傳輸資料的認證和行為準則(certification and codes of conduct)訂定特定方針。

執委會在過去兩年間，加強了雙邊、區域和多邊對話，促進尊重隱私和不同隱私系統之間的融合，有利於公民和企業的隱私保護。執委會致力於更廣泛的外部行動，其中發展如非洲-歐盟夥伴關係(Africa-EU Partnership)及其對國際倡議的支持，比如「具信任的資料自由流通(Data Free Flow with Trust)」。

（三）進一步說明

1. 企業的機會與挑戰

GDPR 結合「非個人資料自由流通規則」，能促進企業競爭和創新，確保資料在歐盟內部的自由流動，以及與歐盟國以外的企業建立公平競爭的環境，為企業提供更多的機會。

雖說 GDPR 的適用具有挑戰性，特別是對於中小型企業而言，但若根據經營者的規模，減縮 GDPR 的適用範圍，並不適當。因為經營者的規模大小，與其所為資料運用行為可能帶給當事人個資保護

的風險，兩者間並無必然關連。惟執委會考量到中小型企業在因應GDPR適用之能力，相較於大型企業的確較為薄弱，因此鼓勵各國之資料保護機關盡量提供實用性工具輔助，以促進中小型企業履行GDPR。

GDPR為所有類型的公司和組織提供一個工具箱(toolbox)，以幫助他們履行GDPR，例如行為準則、認證機制和標準契約條款。行為準則對於中小型企業就GDPR的適用，幫助尤大。

2. GDPR不是科技創新的絆腳石

GDPR所建立的個資保護框架在COVID-19危機期間，證明其重要性和靈活性，特別是在設計接觸史追蹤應用程序(tracing apps)和其他科技解決方案，以防堵疫情擴散。未來的挑戰在於闡明如何將已實踐的資料保護原則，應用於需要持續監控的人工智慧、區塊鏈、物聯網或臉部辨識等特定科技。

3. 發展現代化工具箱(toolbox)促進資料國際傳輸

GDPR提供了一個現代化的工具箱，以促進個人資料從歐盟傳輸到第三國或國際組織，同時確保資料繼續受到保護。這包括與關鍵合作夥伴積極接觸，以期達成「適足性認定」。這種認定的效果能使個人資料能夠安全和自由地傳輸有關的第三國，而無需資料出口國提供進一步的保障措施或獲得任何授權。尤其是2019年2月生效的「歐盟-日本相互適足性認定(EU-Japan mutual adequacy decisions)」創造了全球最大的自由和安全資料流通領域。此外，與韓國的適足性認定正處於發展階段，且正在與亞洲和拉丁美洲的其他重要夥伴進行開放性會談（在兩週年評估報告及新聞稿中關於進行適足性認定之國家，皆未提及臺灣，但在"Two years of the GDPR：Questions and answers"文件中，則有提及臺灣[4]）。

[4] 此份文件中所提及的國家或區域有：Chile, South Korea, Brazil, Japan, Kenya, India, Tunisia, Indonesia, Taiwan and the state of California。*See* European Commission, Two Years of the GDPR: Questions and Answers, June 24, 2020, *available at* https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166.

為了使利害關係人能夠充分利用 GDPR 資料傳輸工具箱，EDPB 必須加強其現行於各種傳輸機制的工作，並澄清國際資料傳輸規定（第五章）與 GDPR 領土適用範圍（第 3 條）之間的競合。由於 GDPR 的域外延伸效力，為確保有效遵守 GDPR 與建立一個公平的競爭環境，資料保護機關的執法行動必須適切反映域外效力適用範圍，即便外國企業在歐盟沒有設立據點，亦不能免除其本應負擔的 GDPR 責任。

4. 促進資料保護領域的融合與國際合作

GDPR 已經成為國際上資料保護的一項重要參考依據。在此一趨勢的基礎上，執委會加強在一些雙邊、區域和多邊論壇上的對話，以促進尊重隱私的全球文化，並發展不同隱私制度之間的融合。這些努力能使歐盟政策與國際間有更好的一致性和互補性。

在促進資料保護標準之和諧與一致性的同時，執委會還決心解決資料策略中強調的數位保護主義問題，制定了關於貿易協定中資料流通與資料保護的具體規定，並在雙邊談判（最近一次是與澳洲、紐西蘭和英國）和多邊談判（如當前的世界貿易組織(WTO)電子商務談判）中列出了該條款，排除了不合理的限制，例如強制資料在地化之要求，同時保持各方的監管自主權，以保護資料保護的基本權利。

最後，當發生隱私問題或資料安全事件可能同時影響多個司法管轄區的多數人時，應進一步加強歐盟和國際監管機構之間的實質合作。特別需要制定適當的法律規範，以便發展更密切的合作與互助，包括允許在調查過程中進行必要的資訊交流，以促進和支持隱私執法者之間的合作。

（四）未來四年內展望

評估報告最末部分整理出執委會對於未來四年內 GDPR 實施的觀察重點（依 GDPR 第 97 條規定，下次評估報告應於四年後之 2024

年作成）。請參閱上述評估報告翻譯整理之「第一章、第一節、三、未來前進之路(WAY FORWARD)」（本報告第 14～20 頁）。

第三節 評估報告值得我國重視及借鏡之重點

一、應值重視之點

整份評估報告具備以下兩項主軸：

1. 當事人權利意識的提升與行使的強化；

2. 創立新的治理模式、樹立新的資料運用文化。

就第 1 主軸而言，相較於 GDPR 對於當事人權利規範完整性：知情權（受告知權）(the right to be informed)、接近使用權(the right of access)、更正權(the right to rectification)、刪除權(the right to erasure)（被遺忘權，the right to be forgotten）、限制使用權(the right to restriction of processing)、資料可攜權(the right to data portability)、拒絕權（反對權）(the right to object)、限制個人自動化決策(automated individual decision-making)權，臺灣個人資料保護法則顯得不完備，目前尚無資料可攜權與拒絕自動剖析決策權之規定；[5]而資料可攜權更是兩週年評估報告中所特別重視的一項當事人權利，認為此權利可以在健康、減少環境足跡、取得公共或私人服務、提高製造業生產力、以及提升產品品質及安全等領域產生重大效益。就此，臺灣立法者應重新盤整增修當事人權利規範，持續推動個資法修正。

第 2 主軸之達成，仰賴各國或各區域間資料保護法制的融合（適用一致性）與合作關係的建立，方能有效促進資料國際傳輸；於執行面上，報告強調「獨立專責的資料保護機關搭配強化的執法權力」的必要性，以及發展現代化工具箱(toolbox)，提供資料利害關係人利用，以符合 GDPR 資料傳輸要求。

[5] 參閱張陳弘、莊植寧，新時代之個人資料保護法制：歐盟 GDPR 與臺灣個人資料保護法的比較說明，新學林，2019 年 6 月，216-229 頁。

歐盟此一全球化個資保護法制（全球性資料運用文化）的推展趨勢，臺灣勢必無法置身事外，因此，臺灣立法者於個資保護法律制定或修訂時，尤應特別注意與全球接軌之需求。此外，藉由報告中強調「獨立專責的資料保護機關搭配強化的執法權力」的重要性，可清楚凸顯臺灣現制欠缺獨立專責的資料保護機關，於個資保護法制推展的重大影響，宜儘速立法解決之。

二、值得借鏡之適例—資料保護影響評估(Data Protection Impact Assessment, DPIA)程序

執委會於此份報告中強調 GDPR 不是科技創新的絆腳石，並以 COVID-19 危機期間，設計接觸史追蹤應用程序和其他科技解決方案，以防堵疫情擴散為例，說明 GDPR 所建立的個資保護框架已能證明其重要性和靈活性。此一觀點，於 EDPB 在 2020 年 4 月發布之「COVID-19 疫情下之利用定位資料與接觸追蹤工具之指引（Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak）」[6]（以下簡稱「接觸追蹤指引）說明得更為清楚：GDPR 的規範架構具有相當彈性，足以兼顧疫情因應（例如創新科技研發）與人權保護；EDPB 堅信為因應 COVID-19 而運用個資時，個資保護乃建立人民信任，創造疫情因應方案能為社會所接受，從而能確保這些方案之有效性，所不可或缺之條件。[7]

本報告始終相信科技始於人性；隱私需求是人性，無法保護隱私的科技，終究無法為人所使用。接觸史追蹤應用程式的研發，是一個

[6] EDPB, Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak [hereinafter Guidelines on Contact Tracing Tools], 21 April 2020, *available at* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf. 中文摘要整理，參閱 國家發展委員會個人資料保護專案辦公室，歐盟 EDPB 發布關於利用定位資料及追蹤接觸工具之指引，https://pipa.ndc.gov.tw/News_Content.aspx?n=D09B8808B663F4AD&sms=AE8BB2204A593B89&s=D60A88A57A734FEE （最後瀏覽日：2020/6/24）。

[7] *Id.* paras. 1-4.

非常好的機會，得以扭轉科技創新總是危害個資保護的社會負面刻板印象。

臺灣也有 COVID-19 的防疫需求，同樣地也研發了類似的接觸史追蹤應用程式—臺灣社交距離 App, Taiwan Social Distancing APP」（以下簡稱「社交距離 App」）。[8]臺灣政府應將社交距離 App 研發視作一次契機，藉以樹立兼顧創新科技研發與個資保護的一個良好典範，讓社會相信資通訊科技的創新與個資保護可以是雙贏局面，而非必然需要相互犧牲；典範樹立的基礎建立在人民對於該 App 的個資保護信任上，而 DPIA 是信任基礎奠實的一項關鍵機制。

上述 EDPB 的「接觸追蹤指引」中，強烈建議接觸史追蹤應用程式之研發，進行 GDPR 第 35 條規範之「資料保護影響評估(data protection impact assessment, DPIA)程序，因接觸史資訊運用對於個資保護具高風險。[9]

臺灣個資法雖未如歐盟 GDPR 般明文設有 DPIA 程序，但臺灣境內的資料控管者仍有可能因 GDPR 的域外效力而須適用 DPIA 程序。此外，DPIA 的施行，有助於提升個資保護，當事人也能因此獲益。職此，GDPR 的 DPIA 程序，值得臺灣個資保護法制借鏡導入。

以下乃整理 GDPR 的 DPIA 制度，供日後臺灣個資法之修法導入參考。

（一）DPIA 之目的與性質

DPIA 之主要目的有：資料控管者遵法責任滿足的確認、提供檢驗之後所進行的資料運用行為是否有按照規劃進行、提供主管機關監管內容的基礎，以及累積資料控管者就個資保護提升的底蘊，最終達到提升當事人自由權利保護的作用。[10]

---

[8] 參閱鍾張涵，防疫也兼顧隱私！一款 App 精準算出「我們與確診者的距離」，天下雜誌，2020/4/21，https://www.cw.com.tw/article/article.action?template=transformers&id=5099958 （最後瀏覽日：2020/10/12）。

[9] EDPB, Guidelines on Contact Tracing Tools, *supra* note 6, para. 39.

[10] *See* PAUL B. LAMBERT, UNDERSTANDING THE NEW EUROPEAN DATA PROTECTION RULES

關於 GDPR 規定之 DPIA 的性質為何，論者有不同見解：

1. 第一種係較窄見解：將 DPIA 理解為只是一種遵法（主要為 GDPR）與否的個資保護確認程序（DPIA 不完全相同於 PIA）；[11]

2. 第二種乃較廣見解：此見解導源於 GDPR 第 35 條第 1 項關於 DPIA 規範目的之理解，認為條文規定係因資料運用行為可能導致自然人之自由權利的高度風險，故須採行 DPIA 程序。條文文字既使用自由權利，而非使用個資保護，即意謂 DPIA 程序不僅評估個資保護的風險，還需評估其他自由權利的風險；[12]在風險評估範圍上，比較類似過去的 PIA 程序。[13]

上述兩種區分見解的形成導源於理論基礎層面之出發點的差異，即 GDPR 第 35 條之 DPIA 程序所預設承擔之功能為何？如果 DPIA 僅是一種個資運用的正當程序要求，其制度目的之重點就可能導向「資料控管者義務」執行面，而將 DPIA 定性為一種遵法評估程序（上述較窄見解）；倘若 DPIA 重視的不僅是一種正當程序的要求，更在乎的是實質、有意義之當事人自由權利的保護，則制度目的重點將轉向為「當事人自由權利」保護面，那麼 DPIA 就不僅只是一種遵法程序之評估，而更是一種實體權利保護之權衡評估（上述較廣見解）。若以實體權利保護評估作為制度基礎之 DPIA，於制度設計與解釋適用上，就應注意不同的實體權利可能導致不同的 DPIA 程序要求，畢竟不同的權利內涵，可能產生不同的保護需求。

321-22 (2018).

11 *See* David Wright, *The State of the Art in Privacy Impact Assessment*, 28 COMPUTER LAW & SECURITY REV 54, 57 (2012); *See* Atanas Yordanov, *Nature and Ideal Steps of the Data Protection Impact Assessment under the General Data Protection Regulation*, 3 EUR. DATA PROT. L. REV. 486, 487 (2017); IT GOVERNANCE PRIVACY TEAM, EU GENERAL DATA PROTECTION REGULATION (GDPR): AN IMPLEMENTATION AND COMPLIANCE GUIDE, 213 (3rd ed. 2019) (Effective risk management is also an important tool for achieving GDPR compliance.).

12 *See* Yordanov, *id.* at 489.

13 *See* Silvia Venier et al., Final Report - A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies, PRESCIENT PROJECT, Mar. 25, 2013, at 50 (Art. 33 of the proposed regulation explicitly provides for privacy impact assessments, except that they are renamed data protection impact assessments (DPIAs), thereby confirming our previous observation on the institutionalisation of PIAs.), *available at* http://publica.fraunhofer.de/documents/N-238503.html.

若觀察 GDPR 第 35 條第 1 項規定，資料控管者之個資運用行為若可能導致自然人自由權利之高度風險時，應採行 DPIA 之要求，似乎導向 DPIA 是實體權利保護評估程序之較廣見解。但一切並非如此單純。如前段所述，即便認為 DPIA 是一種實體權利保護評估程序，其程序要求內容，仍會受到所欲保護之權利類型的影響。假設認為 DPIA 所欲保護之權利類型為個資保護權利，而不及於隱私權，甚或其他自由權利，則個資保護權利與其他自由權利（特別是隱私權）之內涵差異辨清，對於 DPIA 所欲承擔之功能即屬重要。舉例而言，有學者主張隱私是一種「使其不透明的工具(a tool of opacity)」，而個資保護則是一種「使其透明的工具(a tool of transparency)」。[14]隱私的不透明功能在防止干擾私人生活，限制國家權力侵犯私人領域；個資保護的透明功能則在定義得允許運用資料之規則，因此，個資保護的重點在控制資料的運用，加諸資料控管者之義務，並賦予當事人敦促控管者義務履踐之權利。[15]上述理解下之個資保護權利與隱私權利，倆者看似互斥、實則相輔相成：隱私是一種實體權利；個資保護則為程序權利，用以建構實體權利得以實現之制度。[16]職此，即便主張 DPIA 的存立基礎來自於實體權利保護，但若結合的是個資保護權利之程序性概念，則 DPIA 之功能也可能朝向遵法評估程序發展，而往較窄見解偏移。

綜上以言，關於 DPIA 之性質，上述第 2 種之較廣見解，雖說比較符合 GDPR 第 35 條規定之意旨，惟在操作標準上就須區分個資保護、隱私，或其他自由權利之概念差異，而這些概念區分並不簡單。[17]上段所舉之例，僅是一種較為常見之主張，但仍有其他不同見解之討論。[18]因此，本報告傾向階段性主張在 DPIA 甫施行之際，應先讓

[14] *See* Paul de Hert & Serge Gutwirth, Privacy; Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power, in PRIVACY AND THE CRIMINAL LAW, at 3 (2006), *available at* https://works.bepress.com/serge_gutwirth/5/.
[15] *See* Aidan Forde, *The Conceptual Relationship between Privacy and Data Protection*, 1 CAMBRIDGE L. REV. 135, 138 (2016).
[16] *See id*. at 139.
[17] *See* Yordanov, *supra* note 11, at 487-89.
[18] *See generally* Lee A. Bygrave, *The Place of Privacy in Data Protection Law*, 24 U.N.S.W.L.J. 277(2001); Forde, *supra* note 15, at 138-146.

其易於採行，之後再進一步討論不足之處；現階段可暫時先將 DPIA 理解為遵法確認程序。至於此種主張可能產生與 GDPR 第 35 條設定 DPIA 啟動之「可能導致自然人自由權利之高風險」要件不相符之問題，本報告的主張乃：遵法要求評估之最主要法即 GDPR，藉由 GDPR 內關於資料控管者義務與當事人權利之遵法確保，已能相當程度地保護當事人的自由權利。申言之，遵法評估程序之主張，也能達到一定程度之自然人自由權利保護之效果，只是權利類型範圍較為侷限，而非完全與自由權利保護風險評估無關。亦即，大部分評估過後的遵法高風險，得連結至自由權利之高風險。就此觀之，較窄見解之遵法評估程序，尚能符合第 35 條之「可能導致自然人自由權利之高風險」的要件解釋。此外，DPIA 作為遵法評估程序之階段性主張，能暫時性地迴避個資保護權利，與隱私權或其他自由權利間之關係的概念區辨爭議；得留待學術、實務就此議題有較為一致之共識時，再檢討改變之可能性。

本報告上述主張亦可從 GDPR 第 35 條第 7 項規定找到論據；該項規定 DPIA 的風險評估，至少應有下列項目：

- 系統性描述所預定的資料運用行為與目的(第 a 款)；
- 該運用行為與運用目的達成間之必要性與比例性的評估(第 b 款)；
- 對於本條第 1 項規定之對於當事人之自由權利所生風險之評估(第 c 款)；
- 應對運用行為所生風險的方法，包括保護與安全措施、確保個資保護之機制，以及將當事人與其他人相關之權利與正當利益納入考量後，證明運用行為符合 GDPR 要求（第 d 款）。[19]

除了第 a 款是關於資料運用行為與目的之描述外 （風險評估的事實基礎），其他項目之要求內容，究其實際，皆來自於 GDPR 之規範要求：第 b 款來自 GDPR 第 5 條要求、第 c 款來自 GDPR「當事人權

19 GDPR, Art. 35 (7).

利」章節要求（第 12 條～第 22 條）、第 d 款則是其他 GDPR 要求。因此，DPIA 也可簡單理解為：可能違反 GDPR 的風險評估；找到該資料運用行為應特別注意的遵法風險後，再提出控管這些遵法風險的方案。

綜上，DPIA 程序可簡單區分為三層次結構理解：

- 作為風險評估事實基礎的產品概述；
- 遵「法（主要為個資保護法令）」風險的評估；
- 風險控管方案的提出。

最後，本報告呼籲資料控管者不應讓 DPIA 淪為形式遵法工作的敷衍應付程序，[20]應於風險評估後，切實地提出降低或控管這些風險的可行方案，並於運用行為開始後，確實執行。

（二）DPIA 的進行流程概觀

1. 應否進行 DPIA 之判斷

(1) DPIA 的啟動閥—高風險的判斷標準：

GDPR 第 35 條第 1 項規定並未要求任何資料運用行為皆必須進行 DPIA 程序，而僅有在該運用行為可能會對自然人的自由權利造成高風險時，方須進行。[21]故資料控管者應否進行 DPIA 之關鍵在「高風險」與否的判斷，而此判斷應考量該運用行為的性質、範圍、脈絡與目的綜合為之，尤其是在使用新穎資訊運用科技時，應特別注意此高風險的存在可能。[22]GDPR 第 35 條第 3 項例示了三種高風險存在而須進行 DPIA 的情形：

[20] Professor Waldman 即曾撰文質疑目前資料控管者採取的隱私保護措施，只是為了在形式上滿足隱私保護法令的要求，對於隱私保護沒有帶來太多的實質效果。*See* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 773-824 (2020).
[21] GDPR, Art. 35 (1); Raphael Gellert, *The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment*, 3 EUR. DATA PROT. L. REV. 212, 212-14 (2017).
[22] GDPR, Art. 35 (1).

- 基於自動化運用操作，對於自然人的個人特質進行系統性及廣泛性的評估，包括對於自然人的剖析(profiling)[23]，以及基於該評估作成對該自然人產生法律影響或其他相似的重大影響之決定（第 a 款）；
- 大規模地運用第 9 條第 1 項規定的特種個資或第 10 條規定的前科及犯罪個資（第 b 款）；
- 大規模地系統性監督公眾得出入之區域（第 c 款）。[24]

第 35 條第 4 項及第 5 項規定，要求個資保護監管機關應建立並公布須進行與不須進行 DPIA 的資料運用行為類型，以供資料控管者參考。[25]

歐盟個資保護工作小組(Article 29 Data Protection Working Party)（以下簡稱 WP29）[26]，於 2017 年作成之「GDPR 中的 DPIA 與確認運用是否「很可能造成高風險」之指引 (Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation)」（以下簡稱 DPIA 指引）中，[27]以 GDPR 規定為基礎，更具體地提出下述高風險存在可能的判斷因子：

---

[23] GDPR, Art. 4 (4). GDPR 第 4 條第 4 款規定對於「剖析 （或譯為『個人特徵描繪』）(profiling)」行為之定義為：「對個人資料進行任何形式的自動化處理行為，包括使用個資來評量與當事人有關之個人特徵，特別是用來分析或預測有關當事人之工作表現、經濟狀況、健康、個人偏好、興趣、可信度、行為、位置或動向等特徵。」進一步論述，*See generally* Article 29 Data Protection Working Party [hereinafter "WP29"], Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679, 17/EN, WP 251rev.01 (Feb. 6, 2018), *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[24] GDPR, Art. 35 (3).

[25] GDPR, Art. 35 (4), (5).

[26] WP29 係 95 指令時期由歐盟各會員國之個資保護機關、歐盟委員會與歐洲資料保護監督機關所指派之代表所組成。關於 WP29 的組成說明，*see* Article 29 Data Protection Working Party, https://ec.europa.eu/newsroom/article29/news-overview.cfm (last visited June 24, 2020)。在 GDPR 於 2018 年 5 月開始施行後，由 EDPB 取代 WP29 之運作。

[27] WP29, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679 [hereinafter Guidelines on DPIA], 17/EN: WP 248, 4 April 2017, *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

- 為了對自然人剖析所進行的資料運用，尤其是關於自然人的工作表現、經濟狀況、健康、個人偏好、個人行為模式等；
- 資料運用係為了進行會對自然人產生法律或類似重大影響的自動化決定；
- 資料運用係為了進行系統性監控。所謂的「系統性」，乃指運用行為係根據系統發生；是預先安排的，有組織的或有條理的；係作為資料蒐集總體計劃的一部分進行，或是策略的一部分；[28]
- 運用特種個資；
- 大規模地資料運用：何種運用構成「大規模」，應思考涉及當事人之數量、資料量與資料種類範圍、運用行為的持續時間，或運用行為涉及的地域範圍；
- 不同資料庫間的連結使用；
- 有關於「弱勢當事人(vulnerable data subjects)」的資料運用：所謂弱勢當事人，乃指當事人與資料控管者間存在不對稱的權力關係，以致於當事人無法進行有效的同意或反對行為，例如員工與作為資料控管者的雇主間，或兒童、老年人或病患與資料控管者間；
- 屬於創新使用的資料運用行為：由於是創新使用（例如本報告討論之社交距離 App），當事人較難知悉或瞭解該資料運用行為，故應設法給予更多保護；
- 資料的境外傳輸；
- 資料運用行為係為阻止當事人行使權利、使用服務或締結契約：例如銀行運用客戶個資建立信用評等資料庫用以做成核貸決定。[29]

[28] Information Commissioner's Office [hereinafter "ICO"], Accountability and governance: Data Protection Impact Assessments (DPIAs) [hereinafter Data Protection Impact Assessments], 23, May 14, 2018, *available at* https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf.

[29] WP29, Guidelines on DPIA**,** *supra* note 27, at 7-9.

資料運用行為若具備愈多個上述 10 項判斷因子之一，愈可能被認定具備「高風險」而須進行 DPIA。通常而言，同時具備兩種以上判斷因子之資料運用行為，即應進行 DPIA。舉例而言，下列資料運用行為應進行 DPIA：

- 醫院資料系統運用病患健康個資行為，同時涉及「敏感性資料」與「弱勢當事人」因子；
- 道路影像監視系統使用智慧影像分析技術與自動化車牌辨識技術，運用車輛駕駛人個資行為，同時涉及「系統性監控」與「創新使用」因子；
- 公司建置監控系統以監控員工工作情形與網路使用行為所進行的資料運用行為，同時涉及「系統性監控」與「弱勢當事人」因子。[30]

相較而言，網路雜誌使用郵件列表向其訂閱者發送每日摘要，未涉及前述任何因子，即無須進行 DPIA。[31]

然而，上述舉例，僅是就一般情形而言，並不排除在特殊情形下，僅具有一項因子，但卻已對當事人的自由權利產生重大影響，而須進行 DPIA。反之，也有可能在特殊情形下，在具備兩項以上因子的情形下，但卻未對當事人產生重大影響而無須進行 DPIA 之可能。[32]

(2) 進行時間點──資料運用行為進行前：

一旦依上述判斷標準決定資料運用行為應進行 DPIA，依 GDPR 第 35 條第 1 項規定，該程序應於資料運用行為開始前進行。[33]DPIA 愈早進行愈好，縱使在部分運用行為還未確認採用前。蓋儘早進行 DPIA，就能愈早瞭解資料運用行為可能產生之風險，而能評估遵法成本與提升遵法義務之滿足。此外，因為資料運用科技的研發會動態性的調整，故 DPIA 進行與否的判斷，也將是動態性的存在，本就需

30 *Id*. at 9-10.
31 *Id*. at 10.
32 *Id*.
33 GDPR, Art. 35 (1); GDPR, Recital 90.

隨著資料運用情形，隨時進行評估。故儘早進行 DPIA，並不致對資料控管者造成多餘的負擔。[34]

2. 由「誰」進行「何種等級（規模）(level)」的 DPIA

(1) 「誰」負擔執行義務：

依 GDPR 第 35 條第 2 項規定，資料控管者應負責確保 DPIA 程序的進行，並應諮詢個資保護長(Data Protection Officer, DPO)（亦有譯為「資料保護專員」）[35]之意見。[36]實際執行 DPIA 之人或組織，可以是公司內部或外部之他人，但資料控管者仍須對 DPIA 的進行負擔最終責任。[37]如果該資料運用行為，資料控管者有委請其他資料運用者輔助進行時，該資料運用者應協助控管者進行 DPIA。另依第 35 條第 9 項規定，在不實質影響商業或公共利益之保護或運用之進行的前提下，於適當時，控管者應尋求當事人對於其資料運用之意見。[38]

(2) 區分不同等級的 DPIA：

GDPR 雖未具體言及是否得依資料運用狀況，進一步區分適用不同等級（規模）(level)的 DPIA 程序。惟本報告認為，為使 DPIA 更為具體可行，在不過度影響個資保護的基礎上，設法透過不同等級之區分，適度地減輕資料控管者進行 DPIA 程序的負擔，應是一個可努力的方向。

職此，本報告參酌歐盟執委員於 2011 年 1 月針對「無線射頻辨識 (Radio Frequency Identification, RFID)」應用技術所發布的「隱私與資料保護影響評估架構 (Privacy and Data Protection Impact Assessment Framework for RFID Applications, PIA for RFID)」報告，建議循下列標準決定 DPIA 程序需做到何種等級（由簡易至精細）：[39]

---

34 WP29, Guidelines on DPIA, *supra* note 27, at 13.
35 GDPR, Art. 37 (1).
36 GDPR, Art. 35 (2).
37 WP29, Guidelines on DPIA, *supra* note 27, at 13.
38 GDPR, Art. 35 (9).
39 European Commission, Privacy and Data Protection Impact Assessment Framework for

A. 初判標準：

所蒐集資料是否為個資，或雖非蒐集個資，但會將之連結個資使用。亦即，判斷整個資料運用程序是否涉及個資，不論是蒐集階段，或蒐集後的使用階段。

B. 續判標準 1：

若整個資料運用程序，皆未直接涉及個資時，仍應注意該資料運用是否透過個人隨身攜帶裝置所為：

- 1.1：若否，則此資料能與個人連結之風險甚低（非屬條文所稱之「高風險」），無須進行 DPIA；
- 1.2 (level 1)：若是，則可能會使此資料重新產生與個人連結性，而成為個資，例如地理位置資訊，但個資保護風險仍屬偏低（條文所稱高風險中的偏低風險），僅需進行最小規模(level 1)的 DPIA 即可。

C. 續判標準 2：

若整個資料運用程序，直接涉及個資運用時，應再進一步以「資料控管者對這些個資的掌控程度」，區分應進行之 DPIA 等級。以資料控管者透過行動裝置運用個資為例：

- 標準 2.1—掌控程度愈低，DPIA 等級愈低(level 2)：若運用資料的應用程式設計為，資料控管者不直接取得個資，而係暫存於使用者之行動裝置內，需經使用者同意後，資料控管者才能取得個資。由於資料控管者就個資的掌控程度不那麼高，進行中等級(level 2)之 DPIA 即可；
- 標準 2.2—掌控程度愈高、DPIA 等級愈高(level 3)：若運用資料的應用程式設計為，資料控管者直接透過使用者之行動裝置取得個

RFID Applications [hereinafter PIA for RFID], at 7, Jan. 12, 2011, *available at* https://ec.europa.eu/digital-single-market/en/news/privacy-and-data-protection-impact-assessment-framework-rfid-applications.

資，則屬資料控管者掌控個資程度高的情形，應進行最高等級(level 3)之 DPIA。

至於 level 1、2、3 之 DPIA 內容的具體差異，得仰賴未來實際案例之 DPIA 程序操作的累積，再為細部發展。

3. 開始評估：風險評估階段之四步驟進行法

判斷應進行何種等級之 DPIA 後，接續即開始進行風險評估階段(risk assessment phase)。本報告建議循四個步驟進行：

- 步驟 1：涉及資料運用之行為（或產品）的內容描述；
- 步驟 2：指出所評估的產品如何威脅個資保護，並評估這些風險的嚴重程度與發生可能性；
- 步驟 3：對於上述步驟 2 發現的個資保護風險，列出目前與籌劃中已採取或擬採取降低風險的措施。風險控制措施的建議，可分從兩方面著手：技術面與管理面。在技術控制上，可以從例如應用程式的預設(default settings)、授權機制及加密方式上著手。管理控制則可由管控程序之設計著手；[40]
- 步驟 4：列出風險解決方案與剩餘風險(residual risks)。[41]

4. 風險無法合理管控時之向監管機關事前諮商義務（剩餘風險之事前諮商義務）

依 GDPR 第 36 條第 1 項規定，當 DPIA 結果指出該資料運用行為在缺乏保護、安全措施及機制以降低風險時，可能導致對當事人之自由權利傷害的高風險，而控管者認為該風險無法在其能採用之技術及執行成本下，以合理措施降低時，即應於該資料運用活動開始前，向個資保護監管機關諮詢。[42]

---

[40] *Id*. at 12.
[41] *Id*. at 8.
[42] GDPR, Art. 36 (1); GDPR, Recital 94.

5. 做成評估報告書

最後，資料控管者應將經評估可能造成的個資保護風險與建議的風險控制措施，整理列述，做成風險評估報告。當運用了所建議之風險控制措施後，如果還可能存在未被管理的剩餘風險，亦需在此份報告中說明。[43]由於 DPIA 屬於資料控管者進行之內部程序，內容若涉及敏感資訊，例如攸關產品的商業機密，公布之報告可為遮掩處理。

每份 DPIA 報告皆應附列編號。由於 DPIA 是一種動態程序，隨時可能為機動調整，故每份 DPIA 報告於做成後都應編號，以示區分，並標示最新 DPIA 報告的做成日期。[44]

[43] European Commission, PIA for RFID, *supra* note 39, at 10.
[44] *Id*. at 12.

第二章 自動化之個人決策與剖析（automated individual decision-making and profiling）相關規範之目的及內容與歐盟法院判決整理

第一節 概念定義

一、剖析(profiling)

GDPR 第 4 條第 4 款規定對於「剖析（或譯為『個人特徵描繪』）(profiling)」行為之定義為：「對個人資料進行任何形式的自動化處理行為，包括使用個資來評量與當事人有關之個人特徵，特別是用來分析或預測有關當事人之工作表現、經濟狀況、健康、個人偏好、興趣、可信度、行為、位置或動向等特徵。」[45]據此定義，可進一步析分剖析的三項要素：

- 必須存在一個自動化資料運用程序，故 GDPR 規範之剖析，必搭配自動化程序為之；
- 以個資為運用基礎；
- 目的乃在評量（分析、預測）一個自然人的各種個人特徵面向。[46]

欠缺上述任一要素，即非 GDPR 所規範的剖析行為。舉例而言，甲公司基於資料管理便利需求，乃對客戶進行以性別為分類標準的資料整理，但並未依據此分類結果對於客戶行為進行分析預測，縱使此分類行為係透過自動化程序為之，亦非屬 GDPR 規範之剖析行為。[47]

申言之，個人剖析乃藉由個人資料蒐集，經過機器自動化分析以辨識資料間之相關性，再藉由所發現的相關性，找出個人或個人所屬群體的特徵或行為模式，應用於個人，以辨識其目前或未來行為的特

45 GDPR, Art. 4 (4).

46 Article 29 Data Protection Working Party [hereinafter "WP29"], Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679 [hereinafter "Automated Individual Decision-making and Profiling"], 17/EN, WP 251rev.01, at 6-7 (Feb. 6, 2018), *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

47 *Id*. at 7.

徵，可用於例如推測個人之興趣或執行某種類型工作之能力，故可說剖析是關於個人的推論分析。[48]例如，臉書(Facebook)可透過使用者或使用者之臉友的網路行為，藉由剖析技術使用，推論使用者的性傾向或政治傾向。[49]

二、自動化之個人決策(automated individual decision-making)

GDPR 並未如「剖析」般就「自動個人決策（以下簡稱「自動決策」）」於第 4 條為定義性規定，惟就文義而言，乃指資料控管者藉由自動化程序作成與個人相關之決策；概念範圍得包含有人力參與的自動決策，以及無需人力介入即可通過技術方式做出決策能力之完全自動化決策。[50]

自動決策與上述剖析行為之區分乃：自動決策的做成，可能係以剖析為基礎所為，也可能不是；而剖析雖是自動化行為，但可能只是單純的個人特徵描述、分類，並未伴隨決策的產生，又或者伴隨之決策乃人力所為。[51]舉例而言，對於甲的線上貸款申請，若係由銀行行員乙根據對於甲的剖析資料，作成對甲的核貸決定，即未涉及自動決策；但如果銀行設計演算法，使對於甲的核貸決定，基於對甲的剖析資料，完全交由自動化程序完成，則同時包含剖析與自動決策行為，即 GDPR 所稱之自動剖析決策。[52]

---

[48] *Id*.

[49] *See* Carter Jernigan & Behram F.T. Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation,* FIRSTMONDAY.ORG (Oct. 5, 2009), https://firstmonday.org/ojs//index.php/fm/article/view/2611 (last visited Sep. 17, 2020); Jeremy B. Merrill, *Liberal, Moderate or Conservative? See How Facebook Labels You,* N.Y. TIMES (Aug. 23, 2016), https://www.nytimes.com/2016/08/24/us/politics/facebook-ads-politics.html (last visited Sep. 17, 2020).

[50] WP29, Automated Individual Decision-making and Profiling, *supra* note 46, at 8.

[51] *Id*.

[52] *Id*. at 9.

第二節 自動剖析決策技術與個資保護原則之抵觸—以透明化原則為核心

由於自動剖析決策技術建基於多樣且巨量之個資的分析處理，據以評量當事人的各項特徵，並得預測其可能行為，故此技術之運用難以避免地會具備影響當事人自由權利的可能性。[53]例如錯誤的信用評比推論(inferences)，會使得申貸人無法獲得貸款許可或僅能獲得不利條件的貸款許可；被保險人冒險性人格特徵的推論，可能拉高保險費率之計算。

誠然，以商業行銷為例，運用個資，據以評量消費者喜好，預測消費者購買行為，企業過去也做，現在只是採用自動剖析決策技術來做，但目的仍舊相似，有何個資保護需求的特殊性嗎？亦即，強調自動剖析決策行為，考量給予特殊規範的理由為何？過去的商業行銷分析，業者大部分仰賴的是消費者自覺性提出的相關資訊，但自動剖析決策技術所仰賴個資的取得與使用，多半在消費者未察知的狀態下進行。自動剖析決策除了技術運用的不透明特徵外，[54]另一與傳統瞭解消費者行為的差異關鍵在於：現代的推論分析(inferential analytics)技術與所搭配資料的品質與數量之提升，使得推論決策的準確度與推論層面的廣度，皆大幅躍進。[55]此意味著資料控管者藉由自動剖析決策技術影響當事人行為的可能性，大幅提升，致升高人民自由權利保護影響的風險。[56]這也是學者觀察在大數據科技時代，認為對於資料控管者行為的把關，重點常已不在原始資料的正確性，而是藉由這些資料所產生之推論決定的正確性。[57]

以個資為基礎所驅動的自動剖析決策，屬於 GDPR 規範的個資運用行為，須符合 GDPR 規範要求。由於自動剖析決策乃結合運用

---

[53] *Id*. at 5.

[54] *See* Merle Temme, *Algorithms and Transparency in View of the New General Data Protection Regulation*, 3 EUR. DATA PROT. L. REV. 473, 477-78 (2017).

[55] *See generally* CHUCK HEMANN & KEN BURBARY, DIGITAL MARKETING ANALYTICS: MAKING SENSE OF CONSUMER DATA IN A DIGITAL WORLD (2013).

[56] WP29, Automated Individual Decision-making and Profiling, *supra* note 46, at 5-6.

[57] *See* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 270 (2013).

多項技術（例如物聯網、大數據分析、人工智慧及機器學習等）所生的技術運用，因此所結合技術對於個資運用的特徵，大都也顯現於自動剖析決策技術的使用上，而這些特徵常與 GDPR 第 5 條所建立以作為 GDPR 規範基礎的個資運用原則，有所衝突。[58]

申言之，剖析的基礎在龐大、多樣化的個人資料庫，因此極大化運用個資之需求，為剖析技術依存的基礎，且為了能不斷增進剖析的效能，以及更精準的分析預測個人行為、喜好，連續性地累積個人資料，為技術優化所需。故剖析技術具備資料運用極大化與儲存時間極長化的需求特色，但也正與 GDPR 第 5 條第 1 項就個資運用所要求的資料最少化運用(data minimisation)原則（第 c 款）與資料最短化儲存時間原則（第 e 款）相衝突。[59]

此外，剖析涉及對於當事人的特徵分析與行為預測，因涉及「推論」，再加上決策的自動化，可預見錯誤分析、預測發生的可能性，而生決策正確性之質疑。另資料採樣時的偏見存在可能性，以及「個人隸屬群體」的特徵分析預測和「個人特徵分析預測」兩者間可能存在的落差性，使得自動剖析決策技術常被批評有可能深化既定刻板印象與社會隔離，形成社會歧視效應，對個人造成歧視對待；或發生錯誤或偏差預測，而生不公平對待。[60]凡此，皆將對於 GDPR 第 5 條第 1 項第 a 款及第 d 款所規範的公平性(fairness)原則與資料正確性(accuracy)原則，形成威脅。

由於大數據技術的其中一項運作想法來自於藉由已蒐集資料的再使用（目的外使用），推演出原始資料的衍生或隱藏價值。故仰賴大數據技術的自動剖析決策，必然也將伴隨頻繁的目的外使用個資行

---

[58] *See generally* Sandra Wachter, The GDPR and the Internet of Things: A Three-Step Transparency Model, 25 September 2018, at 9-12, *available at* https://www.researchgate.net/publication/323766326_The_GDPR_and_the_Internet_of_Things_A_Three-Step_Transparency_Model; Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1009-11 (2017).

[59] Zarsky, *id*. at 998-1003.

[60] WP29, Automated Individual Decision-making and Profiling, *supra* note 46, at 5-6; *see generally* Tal Z. Zarsky, *An Analytic Challenge: Discrimination Theory in the Age of Predictive Analytics*, 14 ISJLP 11, 22-35 (2017).

為，而升高與 GDPR 第 5 條第 1 項第 b 款目的限定(purpose limitation)原則相抵觸之風險。

自動剖析決策常見新穎技術的使用，可說是嶄新技術的實驗場域，但技術新穎，伴隨的負面效果乃技術的不成熟或運用的不熟悉，將使得資料安全性維護受到挑戰，而升高抵觸 GDPR 第 5 條第 1 項第 f 款資料安全性(data security)原則之風險。[61]

除了上述個資保護原則抵觸風險外，自動剖析決策技術最引人注意或質疑者為「透明化(transparency)原則」的違反。剖析決策的「自動化」個資運用特色，對於仰賴運用程序的透明化以幫助個資保護之原則，形成重大影響。GDPR 第 5 條第 1 項規範的個資運用原則中，第 a 款強調個資運用行為的「透明化」要求，但自動化所伴生的現象就是不透明(opaque)，不易為當事人所察見。故不透明乃自動剖析決策技術運用對於個資保護的最大威脅。甚且，剖析決策要如何運作、要達成何種目標，取決於資料控管者對於演算法(algorithms)的設計選擇，而對於演算法的理解，常超出一般人的得理解能力範疇。此意味即便資料控管者願意公開所採用的演算法，此舉能否滿足 GDPR 所要求的透明化原則，仍存疑義。最後，個資運用過程的不透明，勢必連帶升高對於資料控管者之個資保護違反行為的課責難度，難免對於 GDPR 第 5 條第 2 項規範的課責(accountability)原則有所影響。[62]

透明化原則於個資權利保護扮演舉足輕重的角色，蓋當事人唯有知悉資料控管者的個資運用行為，才有可能行使相關個資保護權利，以及追究控管者之個資侵害責任。而自動剖析決策的「黑箱」樣貌，恰與透明化原則兩相衝突。深入觀察 GDPR 是否已經妥適地處理了此一衝突影響，對於自動剖析決策技術的未來發展與當事人的個資保護，皆深具價值。

---

61 *See generally* Wachter, *supra* note 58, at 11.

62 WP29, Guidelines on Transparency under Regulation 2016/679 [hereinafter "Guidelines on Transparency"], 17/EN: WP260 rev.01, paras. 2-4 (Apr. 11, 2018), *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

第三節 GDPR 對於自動剖析決策的透明化規範

一、GDPR 對於自動剖析決策的規範架構

（一）二分架構

鑑於上述自動剖析決策技術對於個資保護的威脅，在兼顧自動剖析決策技術的開發利益與個資保護利益之權衡下，GDPR 採取的策略是：對於自動剖析決策予以分類，然後挑選出對於上述個資保護原則違反可能性較高、違反結果較為嚴重者，給予特別規範，其他風險較低之類型，則將之與一般個資運用行為等同對待。

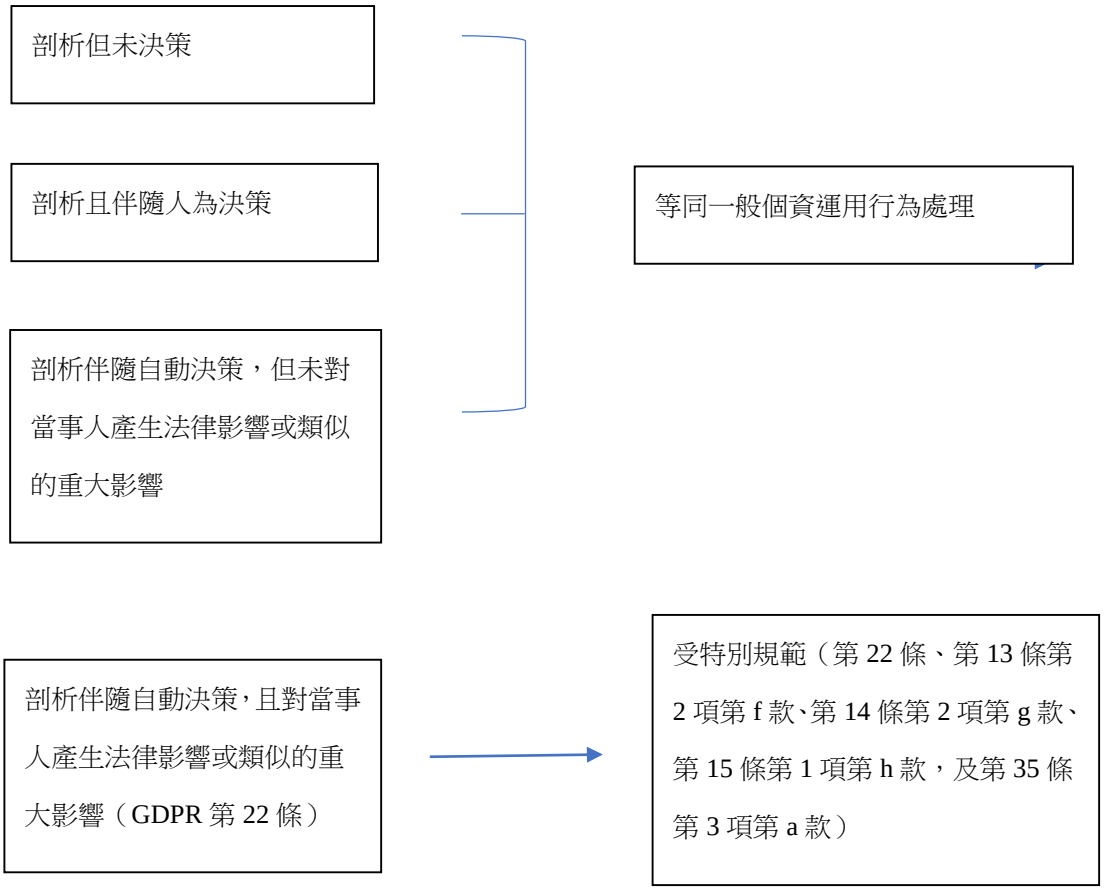
若將「剖析」與「自動化決策」兩種概念為排列組合，可區分為：

- 類型 1：僅進行剖析，未伴隨決策；
- 類型 2：基於剖析行為所為的人為決策（剖析+人為決策）；
- 類型 3：基於剖析行為所為的自動化決策（剖析+自動決策）。此類型又可進一步區分為：
  - 類型 3.1：有人力參與者（僅是參與程序，但對於最終決策無影響力）；
  - 類型 3.2：無人力參與者。[63]

上述類型 3（即 GDPR 第 22 條規範的自動剖析決策）屬於違反 GDPR 第 5 條個資保護原則可能風險較高且後果較嚴重之類型，故 GDPR 針對此類型之自動剖析決策技術的運用，有特別規範設計，主要呈現在第 22 條、第 13 條第 2 項第 f 款、第 14 條第 2 項第 g 款、第 15 條第 1 項第 h 款，及第 35 條第 3 項第 a 款。而為了呼應個資保護風險高且後果嚴重之概念區分，上述對於自動剖析決策的特別規範，明文化「須該自動剖析決策會對當事人產生法律影響或類似的重大影響」的要件要求。

[63] WP29, Automated Individual Decision-making and Profiling, *supra* note 46, at 9.

綜上以言，GDPR 對於自動剖析決策之規範架構，可整列如下：



以下就 GDPR 特別規範的自動剖析決策類型（第 22 條）進行概念闡述。

（二）第 22 條規範之自動剖析決策

1. 定義

(1) 須剖析決策「全然」由自動化程序所為(a decision based “solely on” automated processing, including profiling)：

此一要件乃指無人力介入決策程序。關於人力參與決策程序之理解，應著重在「決策程序」的實質參與（即具有影響或改變決策的權

力），而非僅指形式參與程序運作。[64]亦即，如果人力只是監看自動決策程序，而未介入決策，或不影響自動決策構成之認定，即非屬決策參與。舉例而言，若人力只是用在將自動剖析後的結果套用在該當事人身上，而未對自動剖析結果有任何實質影響力，該程序仍將被認為屬第 22 條規定之自動剖析決策程序。[65]

(2) 對當事人產生法律影響或類似重大影響：

所謂「法律上影響(legal effects)」，乃指影響當事人的法律上權利或地位，例如基於自動剖析程序決定是否給予法律規定之特定社會福利，例如住宅福利；基於自動剖析程序拒絕核發入境簽證或授予公民身分。[66]

所謂「類似重大影響(similarly significant effects)」，乃指該自動決策雖未改變當事人的法律權利或義務，但當事人的權益仍受到重大的影響，其程度與法律影響相差無幾。[67]GDPR 前言的第 71 點所舉之例為：網路貸款之申請被自動剖析決策拒絕。[68]此外，自動剖析決策的結果影響當事人接近使用健康服務，或導致當事人無法獲得工作、教育機會（例如無法獲得大學入學許可）等，亦屬之。[69]

關於自動剖析決策用於「標靶廣告(targeted advertising)」之情形，通常被認為不會對當事人權益產生重大影響，但仍應注意考量下列因素，審慎注意重大影響的形成可能：

- 應注意剖析建構的侵入性，包括追蹤當事人使用不同網站，裝置和服務的足跡；
- 應注意當事人的期待；

---

64 *Id*. at 21; Celine Castets-Renard, *Accountability of Algorithms in the GDPR and beyond: A European Legal Framework on Automated Decision-Making*, 30 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 91, 111-12 (2019).

65 WP29, Automated Individual Decision-making and Profiling**,** *supra* note 46, at 21.

66 *Id.*

67 *Id.* at 21-22.

68 GDPR, Recital 71.

69 WP29, Automated Individual Decision-making and Profiling**,** *supra* note 46, at 22.

- 廣告的傳送方式。[70]

2.「原則禁止、例外允許」的規範模式

承接上述，當自動剖析決策會對當事人產生法律影響或類似的重大影響，且無人力介入決策時，GDPR 第 22 條設下「原則禁止（第 1 項）、例外允許（第 2 項）」的限制：

(1) 原則禁止：

按 GDPR 第 22 條第 1 項規定，當事人有權拒絕接受僅依據自動剖析決策程序就做成對其自由權利造成法律影響或類似重大影響的決定。雖說在體系上，自動決策之規定與當事人的拒絕權同樣置放於“section 4”，而被解釋為當事人得主張的一項權利。但應注意 GDPR 第 22 條的要求（或遵守），並不因當事人有無主張此項權利而有差別，其性質更傾向於是一種個資運用限制原則的要求。[71]意即，倘若資料控管者在非第 22 條第 2 項規定的情形下，作成對當事人產生法律影響或類似重大影響之全自動剖析決策，即便當事人沒有主張此項拒絕權，該自動決策行為仍屬違法。

(2) 例外允許：

依 GDPR 第 22 條第 2 項規定，資料控管者只要是基於下列情形所為之全自動剖析決策，即可不受上述第 1 項禁止規定之限制：

- 該自動決策係為締結或履行當事人與資料控管者間之契約所必要者(第 a 款)；
- 該自動決策係資料控管者基於歐盟法或會員國法的授權，且有採取適當之保護措施以確保當事人之自由、權利及正當利益者。例如為監控及預防詐騙及逃漏稅之目的，依歐盟機構或國家層級監督機構之規範、標準及建議所為之自動決策(第 b 款)；[72]

---

70 *Id.*
71 *Id.* at 20.
72 GDPR, Recital 71.

- 該自動決策係基於當事人之明確同意(explicit consent)者(第 c 款)。[73]

第 a 及 c 款規定之想法，某程度與第 1 項規定是相通的：第 1 項當事人拒絕權之授予，乃基於個資自主權之保護，而於第 2 項第 a、c 兩款規定情形下，雖不允許當事人行使第 1 項的拒絕自動剖析決策權，但契約簽訂與明確同意之行為，已有相當程度保障個資自主權之效果，意即，在個資保護效果上與拒絕權相差無幾。

(3) 小結—與其他個資運用行為之差異：

按 GDPR 第 6 條第 1 項規定，GDPR 對於個資運用行為之規範，其實也是一種「原則禁止/例外允許」的規範模式：原則禁止對於個資之運用，只有在例外具備 6 款(第 a~f 款)運用事由之一的基礎上，才能合法運用個資；只是因為存在第 f 款之「正當利益權衡條款」的概括合法事由，才使得「原則/例外」關係不那麼明顯。

所以，若從「原則禁止/例外允許」的規範模式來看，全自動剖析決策與一般個資運用行為的規範差異在於：

- 一般個資運用行為得有六種運用合法事由：
  - ① 取得當事人之同意；
  - ② 為履行與當事人所簽訂之契約所必要之行為；
  - ③ 遵守法定義務所必要之行為；
  - ④ 為保護當事人或他人之重要利益(vital interests)所必要之行為；
  - ⑤ 履踐公共任務所必要之行為；
  - ⑥ 在與當事人利益保護的權衡下，為追求正當利益(legitimate interests)之目的所必要之行為。[74]
- 全自動剖析決策之個資運用行為僅有三種運用合法事由：

[73] GDPR, Art. 22(2).
[74] GDPR, Art. 6(1).

① 履約之必要；

② 基於法律授權；

③ 取得當事人之明確同意。[75]

3. 當事人的意見表達與抗議(contest)權（依附於基於「契約履行所必要」或「當事人明確同意」所為之自動決策）

雖然 GDPR 第 22 條第 2 項規定僅在第 b 款「履踐法律規定」事由強調資料控管者應就該自動剖析決策行為採取適當之保護措施，以確保當事人之自由權利及正當利益，而第 a 款及第 c 款事由並無類似要求規定。但此適當保護措施要求仍存在於第 a 款、第 c 款事由下之自動剖析決策行為，只是立法者將此要求轉置於同條第 3 項規定，要求基於「履約必要(第 a 款)」或「當事人明確同意(第 c 款)」所進行之自動剖析決策，當事人雖不能行使同條第 1 項的拒絕權，但資料控管者仍有義務執行適當保護措施以確保當事人之自由權利及正當利益，並添加至少應保留當事人有權利要求搭配部分人為參與，以確保得對該自動決策程序表達意見以及爭辯該自動決策之措施。[76]

簡言之，若自動剖析決策係基於法律規定所為，當事人並不存在對該自動決策之意見表達與抗議權，但若係基於契約履行所必要或當事人明確同意所為之自動決策，當事人則享有意見表達與抗議權。

4. 涉及第 9 條特種個資的特別限制

依據 GDPR 第 22 條第 4 項規定，以資料驅動之自動剖析決策若仰賴第 9 條第 1 項規定的特種個資為之，僅能在依據第 9 條第 2 項所規定之當事人明確同意（第 a 款）或基於法律規定（第 g 款）之兩種事由下，並且有採用適當保護措施以確保當事人之自由權利及正當利益時，始得為之。[77]

---

[75] GDPR, Art. 22(2).
[76] GDPR, Art. 22(3).
[77] GDPR, Art. 22(4).

申言之，依第 22 條規定，對當事人產生法律影響或類似重大影響之全自動剖析決策，不論是一般個資或特種個資，原則上都是不行的，當事人皆享有拒絕權，但仰賴一般個資的自動剖析決策有三種例外允許之事由（履約、法定、明確同意），而仰賴特種個資的自動剖析決策則少了一種「履約必要」的例外允許事由。

5. 自動剖析決策禁止適用於兒童？

GDPR 第 22 條規定並沒有區分成人與兒童為不同規定，但前言第 71 點則指出自動決策不得涉及兒童。意即，縱使在第 22 條第 2 項規定例外得允許自動決策的情形，也不得適用於當事人為兒童之情形。[78]

然而，WP29 認為前言第 71 點完全排除第 22 條第 2 項規定例外得允許自動決策的情形適用於兒童，太過絕對，畢竟在某些特定情形下，對於兒童的自動剖析決策，不見得會對兒童不利。鑑於「前言」不具法拘束力，故 WP29 不採上述前言第 71 點見解。[79]但由於兒童的確屬於社會上比較弱勢之群體，資料控管者應盡量避免基於市場行銷目的，對兒童進行剖析決策行為。以線上遊戲為例，自動剖析可找出更可能在遊戲上花錢的玩家，以及提供該被剖析之玩家更符合其興趣的個人化廣告，而兒童的年齡與成熟度，可能會影響他們瞭解此類行銷之動機或後果的能力，而生不利後果。[80]

6. 小結

GDPR 第 22 條規範的自動剖析決策，在規範特殊需求上，分成兩部分思考：

(1) 針對此類型剖析決策會對當事人產生法律影響或類似重大影響，故特別設計「原則禁止、例外允許」制度，且對於涉及特種個資的剖

[78] GDPR, Recital 71; WP29, Automated Individual Decision-making and Profiling, *supra* note 46, at 28.
[79] WP29, *id*.
[80] *Id.* at 29.

析決策例外允許的情形更為嚴格；GDPR 前言第 71 點更是完全禁止自動剖析決策適用於兒童。

(2) 由於是「全自動（剖析及決策皆自動進行）」，屬於最不透明的剖析決策類型，因此有使之更為透明的特別規範需求，至少也要與其他類型的剖析決策之透明度拉近。但此特別透明化需求，並未規定於第 22 條，而係於第 13～15 條及第 35 條、第 37 條為特別規範。具體條文設計，請續參下述。

二、GDPR 對於自動剖析決策的透明化規範

（一）自動剖析決策是否落入 GDPR 第 89 條特權規範範疇，而得減輕透明化規範要求？

GDPR 第 89 條針對基於公益之檔案儲存(archiving)目的、基於科學或歷史研究(scientific or historical research)目的，以及基於統計(statistical)目的，而進行的個資運用行為，賦予若干運用特權（即放寬運用管制），俾使這些個資運用行為，相較於其他個資運用行為，能更容易進行。例如同條第 2 項規定，為科學、歷史、統計目的之個資運用行為，歐盟法或會員國法得就 GDPR 賦予當事人之第 15 條（近用權）、第 16 條（更正權）、第 18 條（限制處理權）及第 21 條（拒絕權），制定例外規定。

論者嘗討論剖析（推論分析）目的之個資運用行為，是否屬於統計目的，而得享有 GDPR 第 89 條的特權保護，肯[81]、否[82]兩說皆有論者主張。一旦肯認推論分析得屬於統計目的，對於本報告所討論「透明化原則」適用之影響，除了上述第 15 條規定之近用權，歐盟或會員國得另以法律為特別限制外，關於資料控管者運用之個資非取自當事人時，依 GDPR 第 14 條第 5 項第 b 款規定，控管者對於當事人之告知義務，亦將有條件地獲得免除。

---

[81] *See* Viktor Mayer-Schonberger & Yann Padova, *Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation,* 17 COLUM. SCI. & TECH. L. REV. 315, 330 (2016).

[82] *See* Zarsky, *supra* note 58, at 1007-08.

GDPR 前言第 162 點應可認為已釐清上述問題：第 89 條規定之「統計目的」意指基於統計目的所為之個資運用的呈現結果非為個資形式，而係總體資料(aggregate data)形式，且該統計結果或個資不能用於支持作成關於任何特定當事人之措施或決定。[83]意即，推論分析如屬個資，或推論分析雖為總體資料但用於對關於當事人之相關決策，皆非屬第 89 條規定所稱之「基於統計目的之運用行為」。由於自動剖析決策之推論分析乃用以支持關於當事人之決策作成，故剖析決策即便使用統計技術，亦非第 89 條賦予特權之統計行為。

（二）知悉制度

1. 資料控管者的告知義務(GDPR 第 13、14 條)

在 GDPR 第 5 條第 1 項第 a 款的「公平性與透明化原則」要求下，資料控管者負擔主動告知義務，使當事人知悉其何種個資、被誰、以何種方式進行運用，以及對其權利保護會產生何種風險、有何安全機制避免這些風險的發生。[84]GDPR 第 12～14 條即在此公平性與透明化原則的要求下為具體告知規範之設計。

在告知方式上，依 GDPR 第 12 條第 1 項規定，資料控管者應採取適當措施，使用清楚、簡易之語言，告知第 13 條及第 14 條規定直接蒐集或間接蒐集時，應提供與當事人的個資運用資訊、告知第 15～22 條規定當事人得主張之權利，以及第 34 條規定之個資侵害事件通知。

上述 GDPR 的告知制度設計，適用於自動剖析決策此個資運用行為，可能會產生水土不服的規範落差，主要原因發生在「推論」此一運用特徵上。進行自動剖析決策所仰賴的原始資料，可能直接取自於當事人，也可能來自於當事人以外之第三人，但決策本身與決策所仰賴的剖析，即便被認定屬於個資，資料控管者也無須負擔主動向當

83 GDPR, Recital 162.

84 EU. AGENCY FOR FUNDAMENTAL RIGHTS ET AL., HANDBOOK ON EUROPEAN DATA PROTECTION LAW 207 (2018).

事人告知之義務，蓋這些推論資料既非取自當事人，亦非來自第三人，而係由控管者自己所產出。[85]

為了解決上述規範落差，GDPR 特別針對第 22 條規範之自動剖析決策，於直接蒐集時之第 13 條第 2 項第 f 款及間接蒐集時之第 14 條第 2 項第 g 款規定應告知事項：「存在第 22 條第 1 項及第 4 項所定自動決策者，至少在該等情況，對當事人個資運用所涉邏輯的有意義資訊(meaningful information about the logic involved)，以及對當事人重要性與預期結果(the significance and the envisaged consequences of such processing for the data subject)。」[86]由於此告知事項乃屬為維護公平、透明之運用所需之第二層次告知資訊（非第一層次告知應提供的基本資訊），故於告知方式上，得以網址連結或 QR code 掃描為之。[87]

申言之，若資料控管者欲對當事人進行第 22 條第 1 項規定之自動剖析決策，他必須特別負擔下列告知義務：

- 告知當事人即將對其進行自動剖析決策行為；
- 提供此自動剖析決策所涉運算邏輯的有意義資訊；
- 解釋此自動剖析決策對當事人的重要性與預期之結果。[88]

然而，在實務操作上，上述告知義務要求，對資料控管者形成不小挑戰。由於自動剖析決策的運算邏輯日趨複雜，控管者如何提出讓當事人能夠理解的說明，是道難題。此外，演算法的說明，也常涉及營業秘密或智慧財產權保護爭議，願否或能否提供，也常陷糾結。因此，WP29 於指引(Guidelines)提供的意見乃：上述所要求之「告知所涉運算邏輯的有意義資訊」，並不必然需要是關於所用演算法的複雜

---

85 *See* Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494, 545 (2019).

86 GDPR, Art. 13 (2)(f); GDPR, Art. 14 (2)(g).

87 分層隱私方法之說明，WP29, Guidelines on Transparency, *supra* note 62, paras. 35-39；張陳弘，新興科技下的資訊隱私保護：「告知後同意原則」的侷限性與修正方法之提出，臺大法學論叢，第 47 卷第 1 期，2018 年 3 月，223-225 頁。

88 GDPR, Recital 60; WP29, Automated Individual Decision-making and Profiling, *supra* note 46, at 25.

解釋，或者是揭露完整的演算法；只要所告知的資訊足以使當事人能夠理解作成該自動決策的理由，即為已足。[89]

舉例而言，銀行以自動剖析進行信用評分以決定核貸與否，銀行應提供解釋內容有：

- 該自動剖析決策程序有助於銀行作成更公平及負責任的核貸決定；
- 提供自動決策的資訊來源，包括當事人所提供的申貸資訊、有關當事人之先前帳戶行為的資訊（包括任何欠款），以及相關政府公開資訊（例如當事人的詐欺或破產記錄）等；
- 所使用的信用評分方法會定期進行測試，以確保它們保持公平、有效；
- 提供聯繫資訊，使當事人得以行使第 22 條第 3 項規定之意見表達與抗議權。[90]

此外，資料控管者亦應設法提供簡單易懂之說明，讓當事人瞭解影響信用評分的重要因素，俾當事人能對評分結果有所預期，亦能藉由改善己身行為，得到對其有利的評分決定。[91]

然而，運用個資所生的推論行為，其樣態不僅只有 GDPR 第 22 條規定之全自動剖析決策，還包括「剖析但未決策」、「基於剖析的人為決策」，及「未對當事人產生法律影響或類似重大影響的自動剖析決策」，關於這些部分之推論資料，資料控管者尚不負擔主動告知義務。

2. 當事人的接近使用權（GDPR 第 15 條）

GDPR 第 15 條規定當事人的「接近使用權(the right of access)（以下簡稱「近用權」），乃為賦予當事人有權請求取得資料控管者就相

[89] WP29, *id*.
[90] *Id.* at 25-26.
[91] *See* Sandra Wachter, Brent Mittelstadt & Chris Russell, *Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR*, 31 HARV. J. L. & TECH. 841, 844-45 (2018).

關於他的個資運用資訊。此一權利乃當事人行使其他權利的必要性權利，蓋若無從接近使用控管者就個資運用之資訊，當事人就無法確實行使諸如發現個資錯誤的資料更正權，或不欲控管者使用個資的刪除權或拒絕權。[92]另資料控管者應注意確認其提供的資訊是否為當事人容易理解之內容，例如技術語彙的縮寫或編碼術語之內容，通常會被認定屬於不易理解之內容，而需進一步解釋。[93]

關於前述資料控管者對於推論資料無須負擔主動告知義務所形成的不透明問題，或許可以藉由當事人主動行使近用權得到解決。但第 15 條第 1 項第 h 款僅特別針對第 22 條規範之全自動剖析決策，規定當事人有權向資料控管者請求確認其個資是否被用作自動剖析決策，以及請求獲得與該自動剖析決策之運算邏輯相關的資訊，以及重要性與預期結果;[94]針對其他類型之推論資料，當事人能否主張近用，解釋上存有爭議，其關鍵在於是否認定推論資料亦屬個資（詳參後述）。

綜上，推論資料的知悉，也無法完全仰賴當事人近用權的行使，獲得解決。

（三）資料保護影響評估與個資保護長

GDPR 第 35 條規範「資料保護影響評估(data protection impact assessment) （以下簡稱 DPIA）」程序，[95]其主要目的乃：資料控管者遵法責任滿足的確認、提供檢驗之後所進行的資料運用行為是否有按照規劃進行、提供主管機關監管內容的基礎，以及累積資料控管者就個資保護提升的底蘊，最終達到提升當事人自由權利保護的作用。[96]

92 EU. AGENCY FOR FUNDAMENTAL RIGHTS ET AL., *SUPRA* NOTE 84, at 219.
93 *Id*. at 218.
94 GDPR, Art. 15(1)(h); GDPR, Recital 63.
95 GDPR, Art. 35.
96 *See* PAUL B. LAMBERT, UNDERSTANDING THE NEW EUROPEAN DATA PROTECTION RULES 321-22 (2018).

GDPR 第 35 條第 1 項規定並未要求任何資料運用行為皆必須進行 DPIA 程序，而僅有在該運用行為可能會對自然人的自由權利造成高風險時，方須進行。[97]故資料控管者應否進行 DPIA 之關鍵在「高風險」與否的判斷，而此判斷應考量該運用行為的性質、範圍、脈絡與目的綜合為之，尤其是在使用新穎資訊運用科技時，應特別注意此高風險的存在可能。[98]GDPR 第 35 條第 3 項例示了三種高風險存在而須進行 DPIA 的情形：

- 基於自動化運用操作，對於自然人的個人特質進行系統性及廣泛性的剖析評估，以及基於該剖析作成對該自然人產生法律影響或其他相似的重大影響之決定（第 a 款）；
- 大規模地運用第 9 條第 1 項規定的特種個資或第 10 條規定的前科及犯罪個資（第 b 款）；
- 大規模地系統性監督公眾得出入之區域（第 c 款）。[99]

由於上述第 a 款規定的文字使用是一旦使用會對當事人產生法律影響或其他相似重大影響的自動剖析決策程序，就應進行 DPIA，而不需要是該決策完全自動化完成，因此其適用範圍會大於 GDPR 第 22 條規範之全自動剖析決策。[100]但反言之，只要是 GDPR 第 22 條規範之自動剖析決策，就必然落入第 35 條第 3 項第 a 款所規定應進行 DPIA 程序之情形。

此外，因資料控管者採用自動剖析決策時，常可能涉及對於當事人為定期且系統性的大規模監控。一旦此類監控行為屬於控管者的核心活動時，依 GDPR 第 37 條第 1 項第 b 款規定，資料控管者應設置「個資保護長(Data Protection Officer, DPO」專責監管自動剖析決策的進行。

---

97 GDPR, Art. 35(2); Raphael Gellert, *The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment*, 3 EUR. DATA PROT. L. REV. 212, 212-14 (2017).
98 GDPR, Art. 35(1).
99 GDPR, Art. 35 (2).
100 WP29, Automated Individual Decision-making and Profiling, *supra* note 46, at 29.

依據 GDPR 第 37 條第 1 項規定，資料控管者於下列三種任一情形下，應設置 DPO：

- 公務機關或機構(a public authority or body)[101]所為的資料運用行為，但不包括法院行使司法權而運用之情形（第 a 款）；
- 資料控管者或受託運用者的核心活動(core activities)[102]，依其行為性質、範圍及目的，需求定期且系統性地[103]大規模(large scale)[104]監控當事人（第 b 款）；
- 資料控管者或受託運用者的核心活動含有大規模運用第 9 條所規定的特種個資與第 10 條規定的前科與犯罪相關個資（第 c 款）。[105]

另依同條第 4 項規定，雖非上述第 1 項規定之情形，但依歐盟法或會員國法之要求應設置 DPO 時，資料控管者或受託運用者亦負擔義務設置 DPO。[106]DPIA 程序的進行與 DPO 的設置，皆將有助於自動剖析決策的透明化。

---

[101] GDPR 並未進一步就公務機關或機構為定義，其理由乃將之交由各會員國之內國法決定；但基本概念為：除了所熟知的中央公法人與地方自治團體外，尚包括其他受公法所規範之組織。*See* WP29, Guidelines on Data Protection Officers (‘DPOs’), 16/EN: WP 243rev.01, at 6 (Apr. 5, 2017), *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

[102] GDPR 前言第 97 點對於「核心活動」之意義，補充一項重點說明：資料運用活動乃資料管控者的主要活動(primary activities)，而非只是輔助活動(ancillary activities)。故核心活動之要求應理解為：該私法組織為達營運目標所需要的主要行為。GDPR, Recital 97.

[103] GDPR 前言第 24 點內容中有說明如何認定該資料運用行為構成對於當事人之「監控」行為：應確認當事人是否於網路中被追蹤，包括潛在的後續個資運用技術之使用，包括描繪自然人特徵之建檔行為，特別是為了做出關於當事人的決定，或分析或預測當事人的個人偏好，行為和態度。GDPR, Recital 24.另 WP29 對於「系統性」意涵的解釋為：根據系統設定而發生；預先安排地、有組織地、有方法地發生；作為籌略規劃的一部分而發生。*See* WP29, *supra* note 101, at 8.

[104] GDPR 第 37 條第 1 項規定並未定義多大範圍的資料運用構成「大規模」，不過，GDPR 前言第 91 點提供一些判斷因子，例如地域廣狹、影響當事人數量、權利傷害風險等。GDPR, Recital 91.

[105] GDPR, Art. 37 (1).

[106] GDPR, Art. 37 (4).

第四節 GDPR 對於自動剖析決策透明化規範之不足與解決方法的提出—歐盟法院見解之發展

自動剖析決策技術的使用為人們的生活帶來便利性，也增進政府與企業就所掌事務處理之效率，但同時因此類技術使用的不透明，升高人們對於個資保護侵害的擔憂。如何適度地讓自動剖析決策更透明到足以讓人們信任此技術的使用，又不讓「更透明」的義務負擔令資料控管者無力負荷，而阻礙自動剖析決策技術的使用與發展，乃為規範制度設計之中心思維。[107]

申言之，個資保護利益與自動剖析決策技術利益的衝突發生時，兩項利益都應被納入考量，不宜偏廢。極高的透明化要求固有益於當事人的自由權利保護，但同時也會對資料控管者造成沈重的義務負荷，一來一回間的利益權衡，於制度設計與個案適用間，應完整思考。

以下乃先提出本報告就 GDPR 對於自動剖析決策之特別透明規範不足的觀察，接續再提出本報告就不足之處所提出解決方法之設想。

一、GDPR 僅特別規範「第 22 條之自動剖析決策」類型，透明化保護不足

（一）不足之處

GDPR 對於自動剖析決策技術的特別透明化要求，僅適用於第 22 條之全自動剖析決策，而未特別規範其他類型，此立法決定應值得被思考是否對當事人的透明化保障不足。[108]

承前述整理，會對當事人產生法律影響或類似重大影響的全自動剖析決策技術，因具備剖析與決策皆機器決定之特徵，GDPR 特別規範的特色呈現在兩方面：

---

[107] 嘗有學者主張 GDPR 第 22 條規定或許是 GDPR 抗拒大數據革命的一個最明顯例子。*See* Zarsky, *supra* note 58, at 1017.

[108] *See id*. at 1015-18.

- 因會對當事人產生法律影響或類似重大影響，故對於能進行此類個資運用行為的限制較為嚴格（從 6 種運用合法事由限縮為 3 種）；
- 由於剖析與決策皆機器決定，屬於最不透明的剖析決策類型，故有特別規範使之「更為透明」的需求。

其中關於透明化的特別規範部分，由於全自動剖析決策乃仰賴機器運算演算法，作成與當事人相關之決定，相較於一般個資運用行為，當事人「看見」，就能大致瞭解該運用行為之作用，對於全自動剖析決策之個資運用行為，當事人能看見的行為外觀是「機器」，但機器外觀不是此類個資運用行為的重點，驅使機器運作的演算法才是個資如何被運用而致影響當事人自由權利的靈魂。因此，GDPR 對於全自動剖析決策特別透明化規範之重點在「演算法的說明（包括演算法的運算邏輯與預期所得之結果）」。

若上述理解無誤，那麼照理說，所有涉及演算法使用的自動剖析決策，都有上述特別透明化規範需求。至於是否會對於當事人產生法律影響或類似重大影響之因素，所影響的特別規範需求，乃關於運用合法事由範圍的限縮，不應影響透明化規範需求。蓋即便該技術的個資使用，對於當事人權利影響輕微，當事人仍應有權行使相關之個資保護權利，而透明化乃這些權利行使的前提性要求。

另基於剖析所為之決策，若非機器自動所為，而係由人力決策取代，亦不屬 GDPR 的特別透明化要求之規範對象。然而，只要涉及剖析，就可能有演算法說明的需求，即便以人力決策取代機器自動決策，仍然無法阻免人力決策受到剖析結果的影響。職此，排除基於剖析之人力決策的特別透明規範適用，對於特別透明化要求所要達到當事人之個資保護目的，將有所減損。

（二）解決之道

對於 GDPR 就特別透明化規範僅侷限適用於全自動剖析決策之不足問題，期待之後 GDPR 修法時，能將「全」之要求移除，使第

13～15 條的特別告知要求，得適用於所有自動剖析決策類型。惟於 GDPR 未修法前，本報告主張或能透過將「剖析決策（推論）資料」解釋為個資之路徑，獲得解決。

GDPR 之所以要在第 13～15 條特別規範演算法的說明要求，相信其中一項因素乃在避免解釋上的爭議：

自動剖析決策技術的使用，既然涉及個資運用，依據 GDPR 第 13～15 條規定，資料控管者本就負擔個資運用說明義務，相對地，當事人本就享有個資的近用權。那又為何要特別在第 13 條第 2 項第 f 款、第 14 條第 2 項第 g 款，及第 15 條第 1 項第 h 款特別規定「演算法之說明」屬於應告知或得近用之內容？立法思考或在於：控管者可能得主張演算法內容與演算法可能得出之結果，非取自於當事人或第三方之個資，而係由控管者自行產出之資料，不在應告知內容之範疇；另由於與演算法相關之資料，非屬個資，因此亦不屬當事人得行使近用權之對象。為了使演算法之說明得納入告知範圍（控管者的主動告知或當事人的近用權行使），GDPR 乃明定演算法說明之告知要求，惟僅適用於第 22 條之全自動剖析決策。

上述思考邏輯的其中一項重點在於：演算法相關資料不是個資，故須另外特別規定此屬於當事人近用權得行使範疇。然而，演算法資料是不是個資，容有爭論空間。如果演算法資料屬於個資，即便 GDPR 第 15 條沒有特別規定演算法資料屬於近用權範疇，亦無礙演算法資料得成為當事人近用權行使對象。那麼現未納入第 15 條第 1 項第 h 款特別規範範疇之非第 22 條之自動剖析決策類型，當事人仍得透過第 15 條的近用權行使，請求資料控管者揭露演算法資料。

以下茲就演算法相關資料（即推論資料）得否作為個資的可能性與影響，為進一步闡述。

自動剖析決策乃以巨量且多元的個資作為基礎，對個人所為的分析推論決定，已如前述，但該推論本身是否亦屬個資，歐盟法院曾有不同見解的發展過程。此一問題的釐清實益，例如若推論亦屬個資，

則 GDPR 第三章規範的當事人權利，原則上都可針對推論為之，但一旦認為推論本身非屬個資，則當事人將無從對之行使權利；又或者當判斷自動剖析決策是否涉及特種個資運用時，倘所運用之個資皆非特種個資，但推論之結果涉及性傾向或政治傾向等特種個資時，判斷結果就將有所不同：若推論屬個資，則該自動剖析決策涉及特種個資運用；反之，則否。

1. 歐盟法院見解的發展

(1) *YS and M and S* 案件：

歐盟法院就基於個資所為的推論，是否屬個資，有不同見解的發展。於 2014 年的 *YS and M and S* 案件（涉及合法居留權決定之爭議）中，法院認為依據個資所為的與法律相關的分析(legal analysis)並非個資。[109]本案之歐盟法院「佐審官(advocates general)」進一步說明，應將推論區分為推論理由與推論決定，推論的結果是個資，但屬於推論過程的分析理由，不是個資。[110]既然推論理由不是個資，當事人自然無從針對推論理由行使各項權利，例如近用權或更正權。故本案法院即出現以下論述：

近用權不是用來提供當事人用以判斷資料控管者以個資為據所作成的決策是否正確的程序權利，[111]意即，近用權不是設計來使依據個資所為之決策程序需完全透明（得近用）的權利；近用權的作用在於提供有關於個資被使用狀況的資訊，以確保運用程序合法，而得以提出異議。[112]本案之歐盟法院佐審官亦認為，當事人的個資近用權來自於其基礎性自由權利的保障，特別是隱私權。然而，具法律效果的分析資訊並不在隱私權保護範疇，因此無從對之行使近用權。[113]意即，

[109] Joined Cases C-141 & 372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I- 2081, para. 39.

[110] Cases C-141/12 & 372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel, 2013 E.C.R. 1-838, at 49, n.40.

[111] YS and M and S, 2014 E.C.R. I- 2081, paras.45-46.

[112] *Id*. para. 44.

[113] YS and M and S, 2013 E.C.R. 1-838, para. 60 (“Moreover, a person is entitled to access his personal data because he has an interest in the protection of his fundamental rights and freedoms, in particular his right to privacy, when Member States process information that concerns him. Denying access to the data processed or to information about that process

當事人並無權利得以知悉資料控管者作成與之相關決策之推論理由。

(2) *Nowak* 案件：

歐盟法院於 2017 年的 *Nowak* 案件中，[114]修正了上述見解，雖然最終結論仍然相近。

本案涉及當事人針對閱卷評分決定行使近用權與更正權之爭議。法院認為試卷作答(exam script)與審閱者之評閱(comments of the assessor)皆屬應試者之個資。[115]若將審閱者之評閱當作應試者最終獲得分數之推論理由，那麼本案法院乃放寬了個資認定範圍，將 *YS and M and S* 案中認為不屬個資的推論理由，改變見解認定亦屬個資。

然而，在應試者得否針對「推論理由」部分，行使相關之當事人權利時，最終結論卻與 *YS and M and S* 案，相去無幾，法院仍然拒絕近用、更正權的行使。主要原因在於：*Nowak* 法院雖然認為推論理由屬個資，但當事人針對推論理由行使個資保護權利的範圍，尚須取決於該個資被運用時所處之脈絡(context)為決定。[116]以本案為例，當事人不能針對評閱理由行使更正權，否則將破壞考試制度之目的。[117]因此，在判決結果上，即便評閱理由被認定屬個資，該應試者仍無法針對評閱理由行使更正權。

2. WP29 見解

WP29 曾於 2018 年作成之關於自動剖析決策的指引中，在論述自動決策概念時，說明自動決策所仰賴的個資形式有：

---

would render ineffective other parts of Directive 95/46. It might not be possible to verify, for example, whether personal data are processed only if necessary to perform a task in the exercise of official authority vested in the controller, or to obtain the rectification or erasure of that data. By contrast, legal analysis as such does not fall within the sphere of an individual's right to privacy. There is therefore no reason to assume that that individual is himself uniquely qualified to verify and rectify it and ask that it be erased or blocked. Rather, it is for an independent judicial authority to review the decision for which that legal analysis was prepared.") (citations omitted).

114 Case C-434/16, Peter Nowak v. Data Prot. Comm'r, 2017 E.C.R. I-994.

115 *Id.* para. 34

116 *Id.* para. 53.

117 *Id.* para. 56.

- 直接由當事人所提供者(provided data)，例如當事人姓名或電子信箱；
- 觀察而得之資料(observed data)：此觀察資料仍然是由當事人所提供，但是為非直接或被動地提供，例如自應用程式所取得之地理位置資訊、網頁點閱行為資訊，或鍵盤鍵入行為資訊等；
- 衍生資料(derived data)：例如從當事人留下的郵遞區號，得知其居住的地理區域；
- 推論資料 (inferred data) ：例如從當事人的金融記錄推論（信用評分）其信用等級。[118]

由以上分類之論述可知，WP29 認為推論資料亦屬個資，並不進一步區分推論的理由與結果，且對於當事人就推論資料行使個資保護權利上，亦未出現上述歐盟法院之「脈絡」標準限制見解。同以更正權行使為例，指引即說明更正權得行使於自動剖析決策過程中所輸入之個資(input personal data)及所輸出之個資(output personal data)。[119]

職此以言，WP29 的立場比較是認為個資保護法律所賦予當事人的個資保護權利，乃在用以確保正確決定的作成，而推論的理由攸關推論決定的正確性，故理由部分自然也是個資保護權利行使的對象。[120]

3. 小結

上述歐盟法院的兩項判決見解所依據的個資保護法律為歐盟於 1995 年頒布的個資保護指令(Directive 95/46/EC)，[121]而非 2018 年開始施行的 GDPR；而上述 WP29 的指引見解，則是針對 GDPR 規定所

---

[118] WP29, Automated Individual Decision-making and Profiling, *supra* note 46, at 6.

[119] *Id*. at 18 ("The rights to rectification and erasure apply to both the 'input personal data' (the personal data used to create the profile) and the 'output data' (the profile itself or 'score' assigned to the person).") (citation omitted).

[120] *See* Wachter & Mittelstadt, *supra* note 85, at 539.

[121] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. L 281/ 31, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en.

為之闡釋。以時間序與 GDPR 作為現行解釋適用法律而言，毋寧應以 WP29 之見解較為可採。畢竟推論正確性的判斷，常仰賴理由構成部分的觀察，一旦當事人無法近用推論理由，將對於當事人確認運用程序的合法性與正確性，造成影響。[122]

此外，不區分推論理由與結果，而將兩者同視為屬個資之「推論資料」的處理方式，還能維持「政府/私人」作為資料控管者的規範一致性。因為倘若資料控管者為政府機關時，基於民主原則作用所生之政府資訊公開要求，當事人原則有權近用政府基於其個資對其作成決策之相關資訊，包括理由部分。相較而言，當資料控管者為非政府機關時，當事人即無從依據政府資訊公開法令向控管者請求近用推論資料。申言之，若堅持依 GDPR 規定，當事人無法近用「推論理由」，則當資料控管者為政府機關時，當事人尚得依政府資訊公開法令尋得近用推論理由資料的可能；而此一近用可能性，並不存在於控管者為私人時。[123]

最後，認定推論資料（不分理由與結果）屬於個資，對於當事人之近用權保障，更為完整。承前述，GDPR 第 15 條第 1 項第 h 款之近用推論資料權，僅針對第 22 條之全自動剖析決策類型，但推論資料的產生，不僅限於全自動剖析決策，已如前述。一旦認定推論資料非屬個資，則當事人將無權近用非全自動剖析決策類型之推論資料，此結果恐有違透明化原則要求。反言之，只要認定推論資料屬於個資，即便是不屬於第 22 條之推論資料，由於仍然屬於與當事人相關之個資，當事人自得對之行使近用權。

惟應注意當事人之近用權並非絕對性權利，依 GDPR 第 15 條第 4 項規定，當近用權的行使會影響他人自由權利時，此權利行使即受限制。由於推論資料的近用，常可能涉及資料控管者之營業秘密或智慧財產權（特別是著作權），故控管者得據以拒絕當事人近用權的行使（即拒絕揭露推論資料）。[124]此外，推論資料的揭露也常可能因涉

[122] *See* Wachter & Mittelstadt, *supra* note 85, at 530-31.
[123] *Id*. at 531.
[124] GDPR, Recital 63; *Id*. at 546.

及第三人之隱私權，而得被拒絕揭露。[125]例如剖析產出的資料，除了個人特徵描繪外，也常見個人所屬群體之特徵描繪，一旦揭露，就可能產生對該群體之第三人隱私權的影響。但此近用權無法行使之結果，即本報告所欲強調之「透明與否」的結果，取決於利益權衡後的解釋決定。

二、GDPR 對於自動剖析決策的特別規範能否滿足足夠的透明化要求？

（一）不足之處

即便透過上述解釋，使得所有類型之自動剖析決策所採用之演算法說明得納入 GDPR 規範應予告知之範疇，但隨即衍生需處理之另一爭議：應告知的範圍與程度？蓋若與一般個資運用行為一樣，僅是揭露自動剖析決策技術所採用的演算法，非專家之當事人甚難理解其運算邏輯。[126]資料控管者是否應負擔使當事人完全理解之義務？抑或控管者只要單純揭露所採用之演算法即可，當事人能否理解，不在義務負擔範疇？

就上述爭議，如果採單純揭露說立場，那麼 GDPR 現行之告知制度，於解釋適用上就不生問題。惟若主張資料控管者所負擔之告知義務，不僅只是演算法的揭露，而應負責解釋至當事人能夠徹底瞭解演算法的運算邏輯，方為已足。那麼 GDPR 現行規定能否支持當事人享有請求控管者「解釋」演算邏輯的權利（請求解釋權），即非清楚。

對於非專家之當事人而言，演算法的運算邏輯即便揭露，亦不易理解；當事人在不懂的狀態下，只能任由控管者宰割。為了揭開黑箱，讓當事人瞭解關於其之自動剖析決策如何形成，當事人應該享有請求資料控管者將自動剖析決策解釋至其能懂程度之權利，否則光是攤開

[125] *See* Wachter & Mittelstadt, *supra* note 85, at 547.
[126] *See* Temme, *supra* note 54, at 476.

演算法，在看不懂的情況下，效果等同未攤開，意即，貌似透明，實仍處暗黑霧境中。

單純揭露說應不符合 GDPR 現行規定之立場，畢竟依 GDPR 第 13～15 條關於自動剖析決策之特別透明化要求，資料控管者至少要告知所涉運算邏輯的有意義資訊，故僅是單純揭露，恐無法符合「有意義」資訊之要求。因此，爭論重點應轉移至「解釋至何種程度」的討論，但從「單純揭露」過渡至「解釋義務」，應先處理 GDPR 之法律依據問題，蓋「解釋」一字並未出現於 GDPR 法條規定文字中。

綜上，就上述揭露不足問題的解決之道的提出，有兩順序性問題應予處理：先解決法律依據，再討論解釋程度。茲進一步論述如下。

（二）解決之道—請求解釋權(a right to explanation)？

承上述，近年來由於自動剖析決策技術的發展，論者企圖在 GDPR 規定中，透過解釋建立一種新型態的當事人權利—請求解釋權(a right to explanation)，[127]目的在於有效揭開剖析決策過程（例如演算法的使用）之「黑箱(black box)」，[128]以落實透明化原則要求。

然而，此請求解釋權建構的主張，被質疑並無 GDPR 之法據。[129]此外，得請求資料控管者解釋，與即使控管者解釋了，當事人能否理解，在現實上難免出現落差，而有執行困難。最後，徹底揭露剖析決策資訊，雖然可能有助於當事人自由權利保護，但同時也可能影響資料控管者的營業秘密或智慧財產權，以及第三人的權利保護。[130]因此，遂生反對請求解釋權之主張。[131]

---

[127] *See generally* Bryce Goodman & Seth Flaxman, European Union Regulations on Algorithmic Eecision-making and a "Right to Explanation"(2016), *available at* http://metromemetics.net/wp-content/uploads/2016/07/1606.08813v1.pdf.

[128] 關於演算法黑箱概念之說明，*see generally* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2016).

[129] *See* Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7(2) INT'L DATA PRIVACY L. 76, 80-90 (2017).

[130] *See* Temme, *supra* note 54, at 483-84.

[131] *See generally* Bryan Casey, Ashkon Farhangi & Roland Vogl, *Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise*, 34 BERKELEY TECH. L.J. 143, 153-163 (2019); Wachter & Mittelstadt, *supra*

按 GDPR 第 13 條、第 14 條就自動剖析決策課予資料控管者的告知義務乃：告知對當事人所為之個資處理所涉邏輯的有意義資訊，以及對當事人的重要性與預期結果。第 15 條之當事人近用權，得請求控管者告知之自動剖析決策內容，亦大致如上。申言之，不論是控管者的主動告知或當事人的請求告知，告知內容大致為：告知當事人即將對其進行自動化剖析決策行為、提供此自動化剖析決策所涉運算邏輯的有意義資訊，以及告知此自動化剖析決策對當事人的重要性與預期之結果。

上述法條規定文字中沒有出現「解釋」一字用語。因此形成爭議討論：條文僅要求資料控管者提供與剖析決策有關運算邏輯的有意義資訊，如果當事人自己看不懂，控管者並無法定義務負責解釋到讓當事人懂。[132]然而，持不同意見者認為，雖 GDPR 的法條規定文字沒有出現「解釋」一字，但前言第 71 點中，確有說明為提供當事人適當保護，當事人有就該自動剖析決策獲得解釋(explanation)的權利，以挑戰該決定。[133]惟前言並無法拘束力。

雖說 GDPR 第 13～15 條針對自動剖析決策的告知制度，並未明白使用「解釋」一字，但透過強調控管者應提供剖析決策所涉演算法之「有意義資訊」，而非只是「資訊」，再結合前言第 71 點之說明，應可有效提供請求解釋權之法據。[134]不過，重點將從「解釋權」用語選擇，轉換至「得請求解釋到何種程度」之爭論，即告知（或解釋）到何種程度算是滿足「有意義」資訊之要求。

依據前言第 71 點提供的一點薄弱線索：有意義資訊的滿足，要能使當事人有挑戰自動剖析決策之可能；再輔以 GDPR 第 22 條規定，資料控管者就自動剖析決策應採行適當保護措施以確保當事人自由權利，其中至少要能保障當事人有就該剖析決策表達意見與挑戰

note 85, at 503-04.

132 WP29, Automated Individual Decision-making and Profiling, *supra* note 46, at 25.

133 GDPR, Recital 71 ("In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an **explanation** of the decision reached after such assessment and to challenge the decision.").

134 *See* Casey, Farhangi & Vogl, *supra* note 125, at 160.

(contest)該決策之能力。於此目的達成上，當事人並不一定需要瞭解驅使該自動剖析決策的演算法邏輯，或許只要瞭解剖析決策可能影響的自由權利（例如什麼類型的個資會被運用或資料來源），以及當事人哪些行為或條件會影響決策的決定，即為已足；反之，若僅解釋演算法邏輯，反而可能無助於理解剖析決策之範圍與理由。[135]舉例而言，關於當事人的汽車保險費率計算，保險公司仰賴自動剖析決策為之，公司應說明該剖析決策僅針對汽車保險費率計算進行，以及當事人的哪些條件（例如性格衝動）或行為（例如常開快車）會影響保險費率的決定，至於就演算法本身的運算邏輯理解，對當事人而言，反非關鍵。[136]

具體而言，與其提出複雜的演算法邏輯解釋，控管者不如說明：

- 所擬運用的資料類型；
- 為何這些類型資料與此剖析決策相關；
- 該剖析是如何在此自動決策程序被建立；
- 為何該剖析會被用於此自動決策；
- 該決策將如何被使用於當事人身上。[137]

總言之，依據 WP29 指引的說法，GDPR 就自動剖析決策之告知制度設計的目的，乃用以顯示該自動化程序如何幫助資料控管者能作成更準確，公正和負責任的決策，並說明該程序所使用的資料，特徵和方法如何適切於該目標的實現。[138]因此，演算法的複雜邏輯並非實現上述目的所必須之資訊，而簡單的演算法邏輯描述，已能於上述所舉具體說明內容中完成。

綜上以言，本報告認為 GDPR 規定足以支持當事人之請求解釋權的行使，惟請求解釋之內容（或程度），重點不應在複雜的演算法

---

135 WP29, Automated Individual Decision-making and Profiling, *supra* note 46, at 25-26; Wachter, Mittelstadt & Russell, *supra* note 91, at 863.
136 *See* Wachter, Mittelstadt & Russell, *id*. at 863- 67.
137 *Id*. at 844.
138 WP29, Automated Individual Decision-making and Profiling, *supra* note 46, at 26.

邏輯之解釋。此立場的最核心理由乃：解釋到懂，對於當事人權利行使無加成效果，但卻可能會對控管者造成過苛成本負擔。申言之，當事人請求解釋的目的在於瞭解其如何被推論、其權利可能如何受到此剖析決策的何種影響，與其要求資料控管者說明複雜的運算邏輯理論，不如要求控管者具體說明在該剖析決策程序中可能影響剖析決策判斷的因子，當事人更易於理解，也更有可能得藉由行為或條件的改變，以獲得對其有利的決策結果。[139]此外，資料控管者不用耗費資源在設法讓當事人理解所採演算法的運算邏輯；也因為無須完整交待演算法的運算邏輯，因此於控管者的營業秘密與智慧財產權的影響上，也得減輕。

[139] 職此，有學者主張應以「請求合理推論權(a right to reasonable inferences)」取代「請求解釋權」。*See* Wachter & Mittelstadt, *supra* note 85, at 543-48.

第三章 有關 GDPR 非公務機關之正當利益（legitimate interest）之適用範圍及相關歐盟法院判決整理

第一節 作為個資運用合法事由之一的正當利益權衡條款—95 指令至 GDPR 的發展

正當利益權衡條款作為資料控管者啟動合法運用個資的事由之一，早已規範在歐盟於 1995 年通過的個資保護指令（以下簡稱「95 指令」）[140]的第 7 條的第 f 款，[141]只是 95 指令時期，論者對於個資運用合法事由之討論，大多聚焦於第 7 條第 a 款的當事人同意，[142]而鮮少論及第 7 條第 f 款之正當利益權衡事由。[143]

95 指令第 7 條第 f 款規定，若資料控管者的個資運用行為係以追求資料控管者或第三者或資料揭露之對象之正當利益為目的所必須者，得合法啟動運用行為，但如果當事人受第 1 條第 1 項保護之利益或基本自由權利凌駕於這些正當利益時，則這些正當利益追求例外不得作為運用合法事由。[144]此正當利益權衡條款在當初立法時，歷經多次修正，不過於實質內容上沒有太大差異，主軸都是在資料控管者所追求的正當利益須凌駕於當事人的利益或自由權利，也因此第 f 款事由被習稱為「正當利益權衡條款」。[145]然而，95 指令第 7 條第 f 款規定並未進一步提供如何進行利益權衡之標準，而係將此任務交付予各會員國發展，但實際執行情況未盡如人意，甚至有論者指出正當利益

---

[140] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. L 281/31, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri=CELEX:31995L0046&from=EN.

[141] EU, 95 Directive, Art. 7(f).

[142] EU, 95 Directive, Art. 7(a) (“the data subject has unambiguously given his consent”).

[143] Irene Kamara & Paul De Hert, Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach, Brussels Privacy Hub Working Paper Vol. 4, Aug. 2018, *available at* https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf. At 4

[144] EU, 95 Directive, Art. 7(f) (“processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed , except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (d)”).

[145] Irene Kamara & Paul De Hert, Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach, Brussels Privacy Hub Working Paper Vol. 4, 9, Aug. 2018, *available at* https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf.

權衡條款的寬鬆運用可能會導致不確定性，並有可能架空個資運用合法事由作為個資保護的作用；且各國適用的不一致性，也導致向歐盟法院的興訟案件。[146]也因此 WP29 乃於 2014 年作成關於「95 指令第 7 條第 f 款規定之資料控管者之正當利益概念之意見書(Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC)」（以下簡稱「正當利益概念意見書」），[147]欲使此正當利益權衡條款的操作能更為明確，能具有一致性。

GDPR 第 6 條第 1 項第 f 款規定正當利益權衡條款，規範核心大致延續 95 指令第 7 條第 f 款規定，仍在「資料控管者或第三者或資料揭露之對象之正當利益」與「當事人之利益或自由權利」倆者間進行權衡，惟仍具有下列差異：

1. GDPR 第 6 條第 1 項第 f 款對於 95 指令第 7 條第 f 款之「資料控管者或第三者或資料揭露之對象」文字做了修正，將「資料揭露之對象」併入「第三者」範圍；

2. 95 指令第 7 條第 f 款將當事人受保護之權益連結至 95 指令之第 1 條第 1 項之對於當事人權利保護的立法目的，而 GDPR 則移除與當事人權益保護之立法目的之連結（95 指令第 1 條第 1 項相當於 GDPR 第 1 條第 2 項[148]）。雖說此文字調整看似將使應受權衡之當事人的利益與自由權利範圍變大，而不僅限於 GDPR 第 1 條第 2 項所指之權益，但實質規範內涵應無差異。蓋按 GDPR 第 6 條第 1 項第 f 款規定，應受權衡之當事人的權益文字：the interests or fundamental rights and freedoms of the data subject which require

[146] Federico Ferretti, Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights?, 51 Common Law Market Review 1, 16 (2014), *available at* https://bura.brunel.ac.uk/bitstream/2438/9724/1/Fulltext.pdf.

[147] WP29, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC [hereinafter Opinion on the Notion of Legitimate Interests], 844/14/EN: WP 217, April 9, 2014, *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[148] GDPR, Art. 1(2): "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."

protection of personal data，與 GDPR 第 1 條第 2 項所指之權益的規定文字：fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data，相差無幾；

3. 就「當事人」利益或自由權利之權衡部分，特別強調當當事人為「兒童」時，尤應注意其權益保護；

4. GDPR 於第 6 條第 1 項末段規定，以正當利益追求作為個資運用合法事由，並不適用於「公務機關」執行其任務之情形。[149]

上述第 1、2 兩點差異僅是文字上的修正，並無實質規範內涵之區別；第 3、4 點才是 GDPR 第 6 條第 1 項第 f 款之正當利益權衡條款，相較於 95 指令時期之第 7 條第 f 款規定的主要差異。

此外，95 指令第 7 條第 f 款規定嘗面臨欠缺有效的利益權衡標準可資操作的批評，歐盟於制定 GDPR 時企圖改善之。GDPR 於前言第 47 點提出正當利益之權衡應考量當事人與資料控管者間之關係所生的合理期待：對於當事人愈無法合理預見之個資運用行為，於利益權衡時，愈應偏向保護當事人的權益。[150]另於前言第 48 點與第 49 點分別提出具體案例說明：例如企業基於內部管理目的，就企業內部間之員工或客戶的個資使用或傳輸，得具有正當利益；[151]又例如，甲律師事務所為了確保所內網路使用安全，以維護事務所之正當利益（例如客戶機密資訊安全的維護），乃監控所內人員所使用的相關電腦設備，以限制所內人員瀏覽特定具危險性之網站。[152]

整體而言，GDPR 與 95 指令的正當利益權衡條款規定之主要規範結構，並無太大差異，因此，WP29 於 2014 年提出的正當利益概念意見書，就正當利益權衡條款之概念與如何操作之論述，於 GDPR 時期仍亟具參考價值。以下乃以此份意見書為主軸，輔以相關學說論述，開展正當利益權衡條款之論述。

149 GDPR, Art. 6(1).
150 *See* GDPR, Recital 47.
151 *See* GDPR, Recital 48.
152 *See* GDPR, Recital 49.

第二節 正當利益權衡條款之概念與操作

一、概念—以正當利益權衡條款回看運用合法事由的立法原理

按 GDPR 第 6 條第 1 項規定，個資控管者的個資運用行為，必須具備所列六款合法性事由之一：

- 取得當事人之同意（第 a 款）；
- 為履行與當事人所簽訂之契約所必要之行為（第 b 款）；
- 遵守所負擔的法定義務所必要之行為（第 c 款）；
- 為保護當事人或他人之重要利益(vital interests)所必要之行為（第 d 款）；
- 履踐公共任務所必要之行為（第 e 款）；
- 在與當事人利益保護的權衡下，為追求正當利益(legitimate interests)之目的所必要之行為（第 f 款）。[153]

此項立法規定顯示個資運用合法事由的雙階結構設計：一階是以「當事人之同意」作為個資運用的合法性事由，無須搭配「必要性」要件要求；另一階則是「其他事由」搭配「必要性」要件的設計。亦即，除當事人同意外的其他五款合法事由的使用，都必須進一步在個案脈絡下判斷該個資運用是否屬於達成該事由的必要行為。

此種雙階結構設計的主要思考在於，「當事人同意」乃係以當事人的自主決定權作為個資運用的正當性基礎，只要當事人同意，就可以滿足個資保護需求，而無須再去考量不同個案脈絡下的必要性思考。然而，「其他合法事由」則會隨著個案情形的不同，而有運用行為必要與否考量的需求。[154]簡言之，相較於「當事人之同意」得產生保護當事人自主決定權的效果，「其他事由」的使用卻是產生壓縮當事人自主決定權之效果，故必須再加上「必要性」要件，來補充資訊自主決定權保護之不足。

---

153 GDPR, Art. 6(1).

154 WP29, Opinion on the Notion of Legitimate Interests, *supra* note 147, at 13.

第 f 款之正當利益權衡條款事由，其實就表彰著 GDPR 第 6 條對於個資運用合法事由設計的理論基礎：除非當事人同意，否則資料控管者的個資運用行為必須具備正當利益，且此正當利益必須凌駕於當事人因個資被使用而損傷之利益。

申言之，GDPR 第 6 條第 1 項規定的個資合法運用事由中，「取得當事人之同意（第 a 款）」係立法者以當事人的個資自主決定權此一正當利益作為規範基礎。另外第 b 款至第 e 款規定的四款事由，是立法者特定四種脈絡—履約必要行為、遵守法定義務必要行為、保護當事人或他人之重要利益必要行為、履踐公共任務必要行為—下，所預設具有正當利益的規範基礎（即已經過立法者進行初步的利益權衡決定）。第 f 款事由，則是立法者未預設特定脈絡的正當利益條款，也因為未預設特定脈絡（即未預先經過立法者的利益權衡），故尚須經過事後具體個案適用的利益權衡後，才能判定是否為具備正當利益之合法運用事由。[155]

職此，此六款事由的立法設計可以這麼思考：1.要具備凌駕當事人利益的正當利益才可以合法運用個資；2.立法者設定當事人的同意可以抵銷當事人利益的傷害，故不須另行尋求運用的正當利益；3.立法者預設第 b 款至第 e 款之正當利益可以是凌駕當事人利益的正當利益；4.第 f 款是未預設凌駕當事人利益的正當利益。

就同為滿足凌駕當事人利益的正當利益要求而言，這六款事由彼此間並不存在適用上的法定優先順序關係。故有論者主張將第 f 款事由當作「最後合法事由」的選擇，只有在無法使用前五款事由時，才會使用第 f 款事由。[156]此一見解應不足採。充其量頂多說在沒有把握找到凌駕當事人利益的正當利益之情形下，取得當事人的同意是比較好的選擇，但這仍然不是適用優先順序的關係。

有論者主張，在現代資訊時代，正當利益權衡條款是不可或缺的一項個資運用合法事由。正當利益權衡條款乍視賦予資料控管者更寬

[155] *Id*. at 9.
[156] *Id*. at 10.

廣的個資運用空間，而不利於當事人自由權利之保護，但相較於其他個資運用合法事由，它實則能更確保控管者的運用行為責任與更有效地保護當事人權益。蓋正當利益權衡條款的使用，相較於其他運用事由，更進一步地要求控管者針對具體個案進行更詳細的利益權衡（詳參下述）。[157]

二、操作

（一）確認為追求資料控管者或第三者的正當利益所必須之運用行為

1. 正當利益

(1)「利益」與「目的」的概念區分：

資料控管者運用個資之行為所追求己身或第三人之利益(interest)的概念，與控管者運用行為之「目的(purpose)」的概念相近，但仍應區別：「目的」是資料為何被運用的理由，即資料運用行為的意圖；「利益」則是控管者在資料運用過程中可能獲得的更廣泛利益，或是對控管者或社會而言，從運用過程所可能衍生的好處(benefit)。[158]舉例而言，核電廠工作員工的健康與安全之保障，對於核電廠而言具有「利益」。因此，核電廠即可能產生運用特定類型之個資，以幫助確保員工的健康和安全之「意圖（目的）」。[159]

(2)「正當」利益概念：

可被資料控管者用作衡量之追求己身或第三人的利益，必須是現存(present)、真實(real)的利益，且該利益亦須足夠明確、具體，以資進行利益權衡。[160]尤應注意該利益必須「正當」。正當利益的概念，可以包括廣泛的利益，無論是微不足道的、或是非常重要的，抑或直

---

[157] Centre for Information Policy Leadership (CIPL), Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR, at 15-16, May 19, 2017, *available at* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.

[158] WP29, Opinion on the Notion of Legitimate Interests, *supra* note 147, at 24.

[159] *Id*.

[160] *Id*. at 25.

觀式的存在、或具爭議性的存在。亦即，在正當性判斷上，會盡量放寬範圍，至於正當性程度的考量，則留待後續雙方之利益權衡階段時，再行為之。[161]以下乃構成正當利益之例示參考：

- 行使媒體的言論自由權；
- 習用之市場營銷或廣告行為；
- 執行法律要求；
- 防止詐欺、濫用服務或洗錢；
- 出於安全或管理目的員工監控行為；
- 舉報(whistle-blowing)行為；
- 維護資訊科技與網路安全；
- 用於歷史、科學或統計目的之運用；
- 用於研究目的之運用。[162]

(3) 小結：

綜上，GDPR 第 6 條第 1 項第 f 款之「正當利益」必須是：

- 合法的(lawful)利益（即符合歐盟法律或歐盟會員國法律之利益）；
- 足夠具體明確，以資與當事人之權益進行利益權衡；
- 現存(present)、真實(real)的利益。[163]

2. 資料控管者或第三者(third parties)

依 GDPR 第 6 條第 1 項第 f 款之規定，正當利益之追求不僅只限於資料控管者之利益，也包括控管者以外之第三者的利益。舉例而言，公司將高階管理層之經理人員的薪水公開，此種薪水披露的個資使用行為，其利益主要不是為了管控此個資的該公司（資料控管者），而

[161] *Id*. at 24.
[162] *Id*. 25.
[163] *Id*.

是為了其他利益相關者（第三者）的利益，例如其他僱員或新聞工作者或公眾。[164]不過，此例的個資運用情形，也常見得適用第 6 條第 1 項第 c 款：遵守法律義務所必須行為之運用事由。

3. 必須性

「必須性」要件存在於第 6 條第 1 項之第 b 款至第 f 款等五項運用合法事由，非為第 f 款所獨有之要件，只是於適用第 f 款時更應特別留意「必須性」要件之要求，亦即，應特別注意是否有其他侵害更小的方式得以對於運用目的的達成具有相同效果。[165]

4. 不適用於公務機關（資料控管者）執行其任務（正當利益）之情形

95 指令第 7 條第 f 款的使用並未特別排除資料控管者是公務機關執行其公務的情形。[166]不過，GDPR 於第 6 條第 1 項末段規定，則明確指出以正當利益追求作為個資運用合法事由，並不適用於公務機關執行其任務之情形。[167]

（二）確認當事人的「利益(interests)」及「基本權利與自由(fundamental rights and freedoms)」

若按 95 指令第 7 條第 f 款規定之文字使用，當事人之利益乃指「當事人受 95 指令第 1 條第 1 項所保護之基本權利與自由的利益(the interests ‘for’ fundamental rights and freedoms of the data subject which require protection under Article 1 (1))，但指令第 1 條第 1 項規定的文字僅有「自然人的基本權利與自由(the fundamental rights and freedoms of natural persons)」，並沒有強調基本權利與自由「的利益(the interest for……)。因此，WP29 於「正當利益概念意見書」中指出， “for”一字應是 “or”一字的誤繕，第 7 條第 f 款的正確的文義應是當事人受保

164 *Id*. at 27.
165 *Id*. at 29.
166 *Id*. at 26.
167 GDPR, Art. 6(1).

護之「利益(interests)」或(or)基本權利與自由(fundamental rights and freedoms)。[168]

關於當事人之利益或基本權利與自由的解釋應盡量從寬為之。這也是立法者為何在 95 指令第 1 條第 1 項規定「基本權利與自由」，另外放入「利益」之意旨。此從寬解釋立場主要導因於資料控管者與當事人之資訊權力不對等關係日益增加，藉此強化當事人之隱私權與自主權之保護。[169]且若相較於前述資料控管者或第三者之利益被要求必須是「正當」利益，當事人之利益只要是「利益」即可，並無「正當性」要求，亦可知當事人之利益保護，相較於資料控管者或第三者之利益要來得廣得許多。也因此，關於當事人的利益保護，不應限縮解釋為與合法活動相關之「正當」利益（與資料控管者之合法性的正當利益要求有別）。舉例而言，某甲雖在乙超市犯下竊盜行為，但不代表甲對於超市內監視器所攝錄關於甲的影像，不享有應受保護之利益，亦即，乙並不享有毫無限制散布甲偷竊影像的權利（仍須經過利益權衡的判斷。續參下述）。[170]

（三）雙方的利益權衡

此款正當利益運用事由使用的一項重點在於資料控管者（或第三者）所追求的正當利益必須凌駕於當事人的利益或自由權利。[171]兩種利益權衡標準之操作，主要有四個步驟：[172]

1. 步驟一：評估資料控管者（或第三者）的正當利益

評量正當利益時，應注意個資運用行為的必要性與比例性。[173]正當利益的類型常見有：

- 資料控管者的基本權利行使（個人利益）：例如新聞媒體運用個資行使新聞自由權。假設甲新聞媒體為報導乙政務官的貪污醜聞，

[168] *Id*. at 29.
[169] *Id*.
[170] *Id*. at 30.
[171] *See* Bart Van der Sloot, *Editorial*, 3 EUR. DATA PROT. L. REV. 1, 8-9 (2017).
[172] WP29, Opinion on the Notion of Legitimate Interests, *supra* note 147, at 33.
[173] *Id*. at 34.

乃調查、蒐集關於乙消費習慣的資料。此運用行為應可認為合乎新聞自由權行使之必要性與比例性要求。但若甲去蒐集並揭露乙之不相關於貪污醜聞的私生活細節，例如乙在大學時期與女朋友間的恩怨情仇，則無法符合必要性與比例性之要求；

- 資料控管者就公共利益之追求（公共利益）：例如某慈善團體基於醫療研究目的而運用個資，或某非營利組織為喚起公民注意政府的貪腐行為而運用個資。[174]

資料控管者所追求之正當利益，於追求個人利益的同時，也可能兼具公共利益促進效果。例如提供金融服務之資料控管者為追求提供服務系統之安全性而運用服務使用者之個資，此運用行為不僅為追求控管者之營運利益，亦具有打擊金融舞弊此公共利益之效果。[175]一般而言，該正當利益之追求，除了控管者自己之正當利益的追求外，若同時兼具公益追求效果者，能帶給該正當利益於權衡時之加值效果。[176]

2. 步驟二：對當事人之權益所造成的影響(impact)

於評量當事人之利益或基本權利與自由受影響之程度時，應注意下列因素：

- 「影響」之認定：「影響」概念的範圍大過「傷害(harm)」或「損害(damage)」，其尚包括了運用個資可能造成的潛在後果；情緒性影響(emotional impacts)也在考量範圍。[177]在影響評估上，應特別注意兩項要素：風險實現的可能性與造成後果的嚴峻性。[178]舉例而言，透過網路與歐盟境外的據點進行資料交換，系統間的不一致性愈高，駭客可利用系統漏洞展開攻擊的風險性就愈高。[179]

---

174 *Id*. at 34-35.
175 *Id*. at 35.
176 *Id*.
177 *Id*. at 37; *see also* Diana Dimitrova, *Rigas Satiksme: The Scope and Limits of Data Protection*, 3 EUR. DATA PROT. L. REV. 418, 421 (2017).
178 WP29, Opinion on the Notion of Legitimate Interests, *supra* note 147, at 38.
179 *Id*.

- 資料的性質：例如運用的個資是否屬敏感性資料，又或者所運用之個資是否屬公開可得的資料。凡此都會影響評估的結果。[180]
- 個資運用的方式：例如所蒐集到的個資是否會向大眾揭露；所運用的個資是否會與其他個資結合運用。[181]
- 當事人的合理期待：通常當事人對於資料控管者就個資運用的合理期待性愈低，對於當事人所造成的影響愈高。[182]
- 資料控管者與當事人的地位：資料控管者是個人、小公司、跨國公司或政府機關，在具體情況下，可能會造成評估的影響。例如跨國公司可能有比較多的資料來源與比較大的取得個資能力，故具備較佳地位得以壓迫當事人利益。相對而言，當事人是兒童或員工，亦可能對評估形成影響。[183]

3. 步驟三：暫定的權衡結果

第三步驟就是對於上述兩項利益進行權衡，產出一個暫定的結果。而之所以稱作「暫定」，係因為部分情形有可能需進行第四步驟的權衡：資料控管者可以考慮是否有可能採取額外的方式去降低運用個資對於當事人所生的不當影響（續參下述）。[184]

申言之，當步驟三的權衡結果處於「兩可」的狀態（即雙方利益經權衡後，沒有明顯的哪方佔贏）時，可得允許資料控管者提供「額外」的資料保護措施，以防免或降低對於當事人所造成的不當影響，藉此取得凌駕於當事人權益的權衡結果（下述步驟四）。換言之，若步驟三的權衡結果若已明確得出某方佔贏的結果，則無須進行下列步驟四。

---

180 *Id*. at 38-39.
181 *Id*. at 39-40.
182 *Id*. at 40.
183 *Id*. at 40-41.
184 *Id*. at 41.

4. 步驟四（不一定會進行）：是否有額外的保護措施以防免對於當事人所造成的不當影響

第四步驟則是考量資料控管者是否有採取額外的（非 GDPR 所要求的）保護措施，以防免對於當事人所造成的不當影響。例如去識別化或加密技術的使用、強化運用過程的透明化、當事人無限制退出權(opt-out)的授予等。資料控管者的保護措施愈完善、愈可符合「正當利益權衡條款」合法事由的要求。[185]

（四） 小結

1. 正當利益權衡條款操作之思考順序

正當利益權衡條款作為個資運用合法事由之個案操作，思考順序如下：[186]

- 先行步驟—評估選擇何款合法事由作為運用基礎：「正當利益權衡條款」事由，在使用上常與「當事人同意」、「契約」及「法律義務」等合法事由產生擇用關係之可能。此際，即有挑選與個案最適切之合法事由的需求。一旦挑選「正當利益權衡條款」作為合法事由，即續行下列步驟；
- 步驟 1—判斷資料控管者的個資運用行為所追求之利益是否構成「正當利益」；
- 步驟 2—決定該運用行為是否屬於追求該正當利益所「必要」之運用行為；
- 步驟 3—確認當事人受該運用行為所影響之利益或基本自由權利；
- 步驟 4—（暫定）雙方利益權衡：權衡該運用行為所追求的正當利益是否凌駕於當事人的利益或自由權利；

185 *Id*. at 42-43.
186 *Id*. at 55-56.

- 步驟 5—權衡後，是否「凌駕」不明時，則進行控管者額外保護措施之權衡，以建立最終權衡決定。

2. 假設案例說明

(1) 新聞自由 v. 隱私權：

記者甲在台北市議員選舉期間，於網路新聞報中，報導一則經過詳細調查、事實正確的報導，乃有關現任台北市議員乙在這屆任期中，出席率不到 10%，且最近被爆出指派自己 17 歲的女兒擔任議員助理之新聞。在此假設案例中，資料控管者甲的正當利益乃新聞自由，而關於乙與其女兒個資的運用乃報導此新聞必要的方式。該則網路報導影響乙的隱私利益，但因乙為公眾人物，且開會出席率及助理之任命與公共事務相關，故隱私保護利益偏低。甲之新聞自由與乙之隱私利益相權衡後，應認為新聞自由利益得凌駕於隱私利益之上，而得以正當利益權衡條款作為個資運用的合法事由。[187]

(2) 債權執行 v. 隱私權：

甲向車商乙購買名貴跑車，300 萬頭期款以開立支票方式支付。甲取車後，即消失無蹤，其所開立的支票亦跳票未兌。乙乃與債務清償公司丙簽訂契約，委託丙向甲追討債務。丙找到甲後，對甲進行全天候跟監，並竊聽甲的電話通訊，企圖找出甲的藏錢所在。資料控管者乙（丙為受託運用者）的正當利益為對甲之債權，但其所雇用之丙所採的個資運用手段，是否為實現債權的必要方式，有待斟酌。退步言，縱使符合必要性要求，但在與甲的隱私利益相權衡時，由於竊聽屬違法手段，故乙的正當利益應無法凌駕於甲的隱私利益之上，從而，正當利益權衡條款無法作為運用個資的合法事由。[188]

(3) 管理目的之網路監控 v. 隱私權：

甲公司監控員工在上班時間使用公司網路的狀況，所運用的資料可以顯示員工瀏覽過哪些網站及下載過哪些資料。甲的監控行為並沒

[187] *Id*. at 58.
[188] *Id*. at 61.

有事先告知員工與工會代表，亦沒有足夠的資訊可以讓員工能預見公司此一監控行為的存在。甲具有公司網路安全維護的正當利益，監控手段對於此正當利益的維護或許具有必要性，但此監控行為並不符合比例性與透明化要求，亦違背了當事人的合理期待。故利益權衡之結果不應認為甲此一監控行為得以正當利益權衡條款作為合法事由。[189]

(4) 網路個資運用 v. 隱私權：

甲網路公司提供搜尋引擎、影片分享與社群網站等服務。甲於網站有說明會蒐集這些服務使用者的個資，並作結合使用。甲公司雖然有提供部分工具供當事人拒絕個人化廣告或網路小餅乾(cookies)的植入，但這些工具並不易為當事人所使用。另當事人無權拒絕甲就不同來源所蒐集到的個資為組合使用。雖說甲就使用者個資的組合使用，有助於優化其服務之提供，對甲而言具有正當利益，但由於甲與當事人間明顯存在權力不對等狀態，故正當利益權衡條款不宜作為甲運用個資的合法事由。就本案言，取得當事人之同意應該是一個比較適切的運用合法事由。[190]

三、正當利益權衡條款與當事人之拒絕權(the right to object)行使之關係

依 95 指令第 14 條第 1 項第 a 款規定，當事人至少在資料控管者使用指令第 7 條第 e 款和第 f 款的情況下，於該事件情況下具有迫切的正當事由(compelling legitimate grounds)時，得享有隨時對該運用行為表達拒絕（或反對）之權利；若該拒絕權確實合理，則控管者不得再對這些個資進行運用。

上述條款規定，大致為 GDPR 所繼受而規定於第 21 條。第 21 條第 1 項規定，當資料控管者的個資運用行為係基於「履踐公共任務之必要（第 6 條第 1 項第 e 款）」或「正當利益權衡條款（第 6 條第 1 項第 f 款）」時，當事人有權隨時依據特定狀況之需求，拒絕控管者繼續使用其個資，包括用於個人特徵描繪（剖析）(profiling)所需。

189 *Id*. at 63.
190 *Id*., at 68.

但若該控管者能證明該運用行為具有優先於當事人利益、基本權利及自由的迫切正當事由(compelling legitimate grounds)時，或該運用行為係為建立、行使或辯護法律上主張所需時，則當事人不得行使拒絕權。[191]申言之，當事人對於控管者的個資運用行為並不具備一般性的拒絕權，而僅能在特定情形下為之。另依據第 21 條第 2 項規定，若個資係被直接用作行銷目的時，該當事人有權隨時拒絕為行銷目的所涉及其個資之運用，包括與該直接行銷有關範圍內之剖析行為。[192]於當事人行使此項拒絕權時，該個資即不得再用於市場行銷目的(第 3 項)。[193]

上述 95 指令與 GDPR 規定的關鍵差異在於:「迫切的正當事由」之要件的設計思考。於 95 指令，此迫切正當事由乃當事人得行使拒絕權的一項要件，故當事人負擔舉證責任證明於該具體事件中，其具有迫切的正當事由以停止資料控管者的個資運用行為。[194]然而，於 GDPR 規定中，「迫切的正當事由」的角色從當事人之拒絕權行使要件，轉而成為資料控管者得拒絕當事人行使拒絕權之要件。意即，當事人就拒絕權的行使不再需要舉證具備迫切正當事由，而是待當事人拒絕權行使後，資料控管者若欲拒絕此拒絕權之行使，得主張個資的繼續運用具有凌駕於當事人權益之迫切正當事由。此一拒絕權之法制轉變，明顯對當事人較為有利。

綜上以言，當資料控管者使用「正當利益權衡條款」（95 指令第 7 條 f 款或 GDPR 第 6 條第 1 項第 f 款）作為個資運用行為之合法事由時，即應注意當事人得行使拒絕權之可能，並具有明確提醒當事人得行使拒絕權之義務。[195]

191 GDPR, Art. 21 (1); GDPR, Recital 69.
192 GDPR, Art. 21 (2).
193 GDPR, Art. 21 (3).
194 WP29, Opinion on the Notion of Legitimate Interests, *supra* note 147, at 45.
195 GDPR, Art. 21 (4).

第三節 歐盟法院裁判

一、*Riga Satiksmes* Case[196]

（一）背景事實

2012 年 12 月於里加(Riga)發生一起交通意外：一輛計程車在路邊停下，一台屬於里加電車公司(Riga Satiksme)的無軌電車(trolleybus)此時駛經計程車旁邊，計程車後座乘客打開車門，刮到無軌電車並造成損壞。[197]由於計程車司機一開始被認為該為這起意外負責，Riga Satiksmes 乃向計程車司機的保險公司要求民事賠償。然而，保險公司拒絕此要求，認為意外的發生是由於乘客的行為所造成，而非計程車司機。保險公司並表示，Riga Satiskme 可對乘客提起民事訴訟。[198]

Riga Satiksme 向國家警局(national police)申請提供意外後被行政裁罰之人的資料：計程車司機與乘客聲明的副本，以及計程車司機與乘客之姓、名、身分證件號碼與住址。Riga Satiksme 向警局表示，這些資料只會被其用於向乘客提起民事訴訟求償。[199]

警局僅批准了 Riga Satiksme 就「提供司機及乘客的姓名」的申請，但拒絕提供倆人的身分證件號碼、住址與聲明副本；[200]警局的說明理由乃：這些行政程序檔案，依法只能提供給與此行政程序有相關之人，而 Riga Satiksme 並非此程序之相關人，故依法 Riga Satiksme 並無權利取得這些資料。[201]

（二）拉脫維亞法院裁判

針對警局拒絕提供乘客之身分證件號碼與住址，Riga Satiksme 向拉脫維亞地區行政法院(District Administrative Court, Latvia)提起行

196 Case C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiks, May 4, 2017, *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=190322&doclang=EN.
197 *Id*. para. 12.
198 *Id*. para. 13.
199 *Id*. para. 14.
200 *Id*. para. 15.
201 *Id*. para. 16.

政訴訟。於 2014 年 5 月 16 日的判決中，法院站在 Riga Satiksme 一方，判決警局應提供乘客之身分證件號碼與住址。[202]

國家警局向法院提起上訴請求撤銷原判決。上訴法院向拉脫維亞國家資料保護局(National Data Protection Agency, Latvia)尋求法律意見。國家資料保護局於 2015 年 10 月 13 日的回覆中認為，具備 95 指令第 7 條第 f 款之事由，只是允許國家警局得合法提供 Riga Satiksme 申請之個人資料，但並未產生強制國家警局必須提供個資的法律效果。[203]不過，國家資料保護局同時指出 Riga Satiksme 有兩種其他方式可以得到其所要求之資料： (1) 向國民登記機關(Civil Registry)提出申請；(2) 根據 Articles 98 to 100 of Latvian Law on Civil Procedure 向法院申請提供證據(evidence)，讓法院命國家警局提供個人資料。[204]

然而，法院對國家資料保護局提供的上述兩種獲得乘客之身分證件號碼與住址之方式表示懷疑。法院表示，首先，如果向 Civil Registry 提出的申請中，只提到計程車乘客的名字而無身分證件號碼，可能會有許多同名同姓之人，而無法確認是誰；其次，根據國家法律，要能向法院申請提供證據，申請者必須至少知道被告的地址。[205]

此外，法院對於 95 指令第 7 條第 f 款規定之「必要性(necessity)」要件應如何解釋，亦存有疑慮。[206]

拉脫維亞最高法院的行政部門(Supreme Court, Administrative Division, Latvia) 決定暫停審理程序，並將下列問題向歐盟法院(Court of Justice)提出先決裁決(preliminary ruling)之請求：

1. 95 指令第 7 條第 f 款中這句「當個資運用目的是為了...第三方或資料揭露之對象之正當利益所必要」的含意，是否得解釋為國家警局必須向 Riga Satiksme 揭露其所蒐集之個人資料，因為這些資料是 Riga Satiksme 展開民事程序所必須；

[202] *Id*. para. 17.
[203] *Id*. para. 18.
[204] *Id*. para. 19.
[205] *Id*. para. 20.
[206] *Id*. para. 21.

2. 照檔案文件看來，Riga Satiksme 欲索取個資的計程車乘客在意外發生時尚未成年，此事實對上述問題之答案是否有所影響。[207]

（三）歐盟法院裁判

歐盟法院認為拉脫維亞法院所提出的兩個問題應當一併考量；主要重點在於：95 指令第 7 條第 f 款是否必須解釋為強制揭露個人資料予第三方之法律效果，以使第三方能針對當事人所造成的損壞向民事法院提起訴訟？而此當事人尚未成年之事實是否對此條文解釋有所影響？[208]

於本案中有兩點共識基礎：第一，Riga Satiksme 欲索取之資料(身分證件號碼、地址)屬於 95 指令第 2 條第 a 款所定義之「個人資料」；第二，被索取資料之國家警局該當於 95 指令第 2 條第 d 款之資料控管者(controller)。[209]

歐盟法院認為 95 指令第 7 條第 f 款並未有強制效果，而只是給予資料控管者對個資進行運用的可能性。[210]

歐盟法院闡述 95 指令第 7 條第 f 款的適用，必須滿足三項要件：

1. 乃為追求資料控管者或第三者或資料揭露之對象之正當利益為目的所必須者；
2. 為了上述正當利益追求，而有必要運用個人資料；
3. 受 95 指令第 1 條第 1 項保護之當事人的利益或基本自由權利未凌駕於上述正當利益。[211]

針對要件 1 的正當利益追求要求，法院認為如同本案佐審官(Advocate General)在他提出的意見書(Opinion)的第 65、79、80 點中指出，第三方想獲得損壞其財產之人的個人資料以對該人提出法律訴訟，這毫無疑問可算是正當利益；且 95 指令第 8 條第 2 項第 e 款規

[207] *Id*. para. 22.
[208] *Id*. para. 23.
[209] *Id*. para. 24.
[210] *Id*. para. 26.
[211] *Id*. para. 28.

定也同樣指出，禁止特種個資（敏感性個資）之運用規定不適用於為了成立、行使或捍衛法律主張而需要運用個資之情形。[212]

關於要件 2 之「必要性(necessity)」要件，法院提醒應謹記只有在絕對需要的情形下，對個資的保護才能受到限縮或限制。就此而言，根據拉脫維亞法院提供的資料，只包含造成電車損壞的當事人之姓名，並沒有足夠的精確性足以識別當事人，Riga Satiksme 也就無法對該人採取法律行動。也因此，為達對造成電車損壞之人提起訴訟求償之目的，必須取得該人之地址或身分證件號碼。[213]

最後，關於第 3 個要件就相衝突之權利與利益間的權衡，必須取決於個別案件中的具體情況。[214]法院主張應將下點列入權衡考量：因為資料運用而造成當事人之基礎性權利遭到侵犯，其嚴重程度可能會因資料能否由公共資源(public sources)中被取得而有所差異。[215]

至於拉脫維亞法院提請先決裁決的第 2 個問題，歐盟法院認為權衡相衝突之利益時，當事人的年紀是應該列入考量的因素之一。然而，如同佐審官在意見書第 82 點及第 84 點中所指，在此案例中，造成損壞之當事人未成年的事實，並不足以作為正當理由拒絕向承受損壞之第三方揭露當事人（或當事人之監護人）之個資。[216]

歐盟法院總結上述，認為 95 指令第 7 條第 f 款須理解為：並不強制揭露個資給第三方，以使第三方能針對有個資保護疑慮之當事人所造成的損毀，提起民事訴訟。然而，95 指令第 7 條第 f 款也不排除得依據國家法律揭露個資之可能性。[217]

---

[212] *Id*. para. 29.
[213] *Id*. para. 30.
[214] *Id*. para. 31.
[215] *Id*. para. 32.
[216] *Id*. para. 33.
[217] *Id*. para. 34.

二、*Ryneš* Case[218]

（一）背景事實

在 2007 年 10 月 5 日至 2008 年 4 月 11 日期間，Frantisek Ryneš（以下簡稱 Ryneš）在他住所的屋簷下安裝並使用固定式錄影監視系統(無法移動鏡頭位置)；監視系統錄影的範圍包括其住所入口、公共走道，以及對面住家的入口。該系統採連續錄影，內容只有影像、無聲音，所錄畫面的檔案存放在硬碟中，當硬碟容量已滿，新錄製的檔案會覆蓋舊的檔案並將舊檔案刪除。由於未安裝顯示銀幕，監視畫面無法即時觀看。Ryneš 是唯一能存取系統檔案資料的人。[219]

捷克最高行政法院(Supreme Administrative Court)認為，Ryneš 安裝錄影監視系統的唯一理由是為保護其個人及家人之財產、健康與性命安全。而過去幾年來，Ryneš 與其家人確實曾遭遇多次不明人士的攻擊。而且，在 2005 至 2007 年間，其住所之窗戶也曾多次被破壞。[220]2007 年 10 月 6 至 7 日的晚間，攻擊事件又再次發生。Ryneš 家的一扇窗戶被擊中破裂。錄影監視系統所攝錄的兩名嫌疑犯的畫面被交給警察，並在後續的刑事訴訟中被使用。[221]

其中一名嫌犯要求確認 Ryneš 的錄影監視系統是否合法。主管機關於 2008 年 8 月 4 日的決定，認為 Ryneš 已違反 Law No 101/2000，理由如下：

- 作為資料控管者，Ryneš 在沒有得到同意的情況下，使用錄影監視系統蒐集路上行人及進入對面住所之人的個資；
- Ryneš 並未告知上述人等其個資會被運用、運用的範圍及目的、被誰及用甚麼方法運用、或是誰能夠存取這些個資；

---

[218] Case C-212/13, Frantisek Ryneš v. Urad pro ochranu osobnich udaju, Dec. 11, 2014, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62013CJ0212&from=EN.
[219] *Id*. para. 13.
[220] *Id*. para. 14.
[221] *Id*. para. 15.

- 作為資料控管者，Ryneš 未履行其義務，向主管機關報告個資之運用。[222]

Ryneš 針對上述決定提起訴訟。Prague City Court 於 2012 年 4 月 25 日判決駁回。Ryneš 再度向捷克最高行政法院上訴。[223]

捷克最高行政法院決定暫停審理程序，並將下列問題提請歐盟法院(Court of Justice)給予先決裁決(preliminary ruling)：

若一錄影監視系統是安裝在住宅、以保護屋主財產、健康與生命為目的，此狀況下的個人資料運用，是否可以被認定為屬於 95 指令第 3 條第 2 項所指之「由自然人在純粹的個人或家庭活動中所為 (by a natural person in the course of a purely personal or household activity)」之個資運用，而不適用 95 指令規範，即使該系統也同時監看公共空間?[224]

（二）歐盟法院裁判

依 95 指令第 2 條第 a 款的個人資料定義，監視器所錄下之個人影像屬個人資料，因為此影像使被錄影之人的身分得以被辨識。[225]且錄影形式的監視系統，將錄製資料存放於持續錄影的機器硬碟中，構成 95 指令第 3 條第 1 項規定所指之自動運用個人資料。[226]

依據 95 指令第 1 條規定及前言第 10 點說明，95 指令之目的乃為確保對自然人之基本權利與自由的高度保護，特別是對隱私的權利與關於個資的處理。[227]另依歐盟基本權利憲章(the Charter of Fundamental Rights of the European Union)第 7 條就「對私人生活的基本權利之保護」規定，要求只有在嚴格必要(strictly necessary)的情形下，對個資的保護才能受到限縮或限制。[228]

---

222 *Id*. para. 16.
223 *Id*. para. 17.
224 *Id*. para. 18.
225 *Id*. para. 22.
226 *Id*. para. 25.
227 *Id*. para. 27.
228 *Id*. para. 28.

既然對 95 指令規定的解釋，必須符合歐盟基本權利憲章所保障之基本權利，那麼 95 指令第 3 條第 2 項規定所指出的例外不適用 95 指令之情形，也必須從嚴解釋為：僅限於個人資料運用發生於「純粹(purely)」的個人或家庭活動，而非「只是(simply)」個人或家庭行動。[229]依照 95 指令前言第 12 點之說明，就自然人而言，信件、通訊錄構成「純粹的個人或家庭活動」，即使其內容可能在無意間涉及他人的私人生活。[230]

歐盟法院認為，本案之錄影監視系統從資料控管者的私人場所向外監看公共空間，即使所攝錄內容只有部分是公共空間，也將使影像攝錄行為不符合 95 指令第 3 條第 2 項所規定之「純粹的」個人或家庭活動。[231]

由於 Ryneš 的影像攝錄行為不屬於 95 指令第 3 條第 2 項之排除使用 95 指令之情形，法院同時指出在 95 指令的適用情形下，Ryneš 得考慮 95 指令第 7 條第 f 款正當利益權衡條款規定，主張影像攝錄行為乃保護其個人及家人的財產、健康與生命等之正當利益；且屬於 95 指令第 11 條第 2 項得免除告知義務之情形。[232]

三、*ASNEF* Case[233]

（一）背景事實

西班牙最高法院認為，資料控管者為了資料控管者或第三者之正當利益，而需要在未取得當事人同意的情況下對個人資料進行運用，西班牙國內法律要求不僅必須尊重當事人之基本權利與自由，同時這些個資也必須出現在 Article 3(j) of Organic Law 15/1999 所列之檔案(files)中。此一見解形同以西班牙國內法律(Organic Law 15/1999 和

[229] *Id*. paras. 29-31.
[230] *Id*. para. 32.
[231] *Id*. para. 33.
[232] *Id*. para. 34.
[233] Joined Cases C-468/10 and C-469/10, ASNEF and FECEMD v. Administraction de Estado, Nov. 24, 2011, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62010CJ0468&from=EN.

Royal Decree 1720/2007)限縮了 95 指令的適用範圍。[234]西班牙最高法院認為此種限制會對 95 指令保護資訊自由流通利益構成阻礙，而避免 95 指令和西班牙國內法律之間矛盾的唯一方法，就是主張：只要運用的是 Article 3(j) of Organic Law 15/1999 所列檔案(files)以外的個人資料，皆算是侵害當事人的利益或基本權利及自由，而無法使用 95 指令第 7 條第 f 款之正當利益權衡條款。[235]然而，西班牙最高法院不確定此種解釋是否與 95 指令之立法原意相符合，因此決定暫停審理程序，並將下列問題提請歐盟法院給予先決裁決：

當國家法律規定，為了資料控管者或第三者之正當利益，而需要在未取得當事人同意的情況下對個人資料進行運用時，不但當事人之基本權利與自由不得受到過度侵害，同時這些資料也必須出現在公共資料來源中，那 95 指令第 7 條第 f 款是否必須解釋為排除此種國家法律的適用？[236]

（二）歐盟法院裁判

95 指令第 1 條要求會員國確保自然人之基本權利與自由，特別是在處理個人資料時所涉及之隱私。[237]95 指令第二章(個人資料運用合法性的一般性規則)規定，除了第 13 條所允許的例外情形，所有個資的運用都必須符合兩項原則：1.符合第 6 條規定之關於資料品質的運用一般性合法原則要求；2.具備第 7 條規定得使資料運用具合法性基礎的六項事由之一。[238]

根據 95 指令前言第 7 點說明，不同國家對個資運用的法律規定各不相同，其間差異對歐洲內部市場的建立與運作有重大影響。[239]而 95 指令之目的(如同前言第 8 點所示)是要確保各會員國在個資保護上，對個人基本權利與自由具有相同程度之保護。前言第 10 點補充：會員國內國的類似性法律（個資保護法律）規定不得導致其提供的個資

[234] *Id*. para. 19.
[235] *Id*. para. 20.
[236] *Id*. paras. 21-22.
[237] *Id*. para. 25.
[238] *Id*. para. 26.
[239] *Id*. para. 27.

保護因而有任何削弱，反而必須設法確保在歐盟中的高規格保護。[240]相應來說，各會員國的國家法律應追求盡可能達到一致性，而非僅限於有限度的一致。這也是為何 95 指令在確保資訊自由流通的同時，也要保證對當事人權益的高度保護。[241]

為了要確保所有會員國都能提供相同程度的保護，95 指令第 7 條列出所有完整的條件要求，限制在何種情況下個人資料的運用才具有合法性。[242]因此，第 7 條的條文文字乃使用「只有在以下情況，可以運用(may be processed only if)」的用詞，以及在每一項事由間選用「或者」一字。[243]職此，針對第 7 條規定個資運用的合法條件，會員國並不能在條文規定以外再增加新的事由，也不能在第 7 條規定之事由上，強加額外的條件要求，而使第 7 條的六項運用事由的適用範圍受到影響。[244]

會員國根據 95 指令第 5 條所擁有的裁量權範圍，必須符合 95 指令的立法目標，在資訊自由流通與保護私人生活之間取得良好平衡。[245]即，95 指令保留了相當程度的彈性，讓會員國自行決定細節。因此，需要區分清楚以下兩類國家立法方式的不同：

- 第一類是增加額外要求，改變了 95 指令第 7 條所定原則之範圍；
- 第二類則僅僅是針對原則提供具體說明。

第一類方式應該被排除；只有第二類國家措施，會員國才有根據 95 指令第 5 條規定享有裁量權。[246]

職此，於 95 指令第 5 條規範下，會員國不能就 95 指令第 7 條規定增加額外的關於個資運用合法條件的新條款，也不能藉由增加額外規定使第 7 條的六項原則（運用事由）的適用範圍受到影響。[247]

---

240 *Id*. para. 28.
241 *Id*. para. 29.
242 *Id*. para. 30.
243 *Id*. para. 31.
244 *Id*. para. 32.
245 *Id*. para. 34.
246 *Id*. para. 35.
247 *Id*. para. 36.

95 指令第 7 條第 f 款所列之個資合法運用事由，必須符合兩項要件：

- 第一，當目的是為了控管者或第三者的正當利益，而有必要對個人資料進行運用；
- 第二，這些正當利益須不能為當事人之利益或基本權利及自由所凌駕。

而第 7 條第 f 款規定排除了任何國家法律(national rules) 額外添加上述兩要件以外的條件規定，以加強限制資料控管者的個資運用行為。[248]

綜上以言，西班牙國內法律就 95 指令第 7 條第 f 款的適用，添加了該被運用的個資必須取自於「公共資料來源」的條件限制，違背了 95 指令第 5 條及第 7 條第 f 款之意旨，應被排除適用。[249]

當然，侵害當事人之權利的嚴重程度，會因為該被運用之資料是否已在公共來源(Public sources)公開而有所差別。但一旦如同西班牙國內法律般將「取自公共來源」之要求，明定為 95 指令第 7 條第 f 款的適用要件時，就等於排除了因個案之特殊情況而有所不同權衡需求的可能性，因而有違 95 指令第 7 條第 f 款之立法意旨。[250]

四、*AEPD v. Google* Case[251]

（一）背景事實

AEPD v. Google 的案例事實乃關於一位西班牙公民 Mario Costeja González 因於 1998 年積欠社會保險債務(social security debts)，導致不動產被強制拍賣，此事件被西班牙一家高發行量的日報 La Vanguardia 報導，並被上傳至日報網頁上。因此，只要利用西班牙的

[248] *Id*. para. 39.
[249] *Id*. para. 49.
[250] *Id*. paras. 44-47.
[251] Case C-131/12, Google Spain SL, Google Inc. v Agencia Espa?ola de Protecci?n de Datos (AEPD), Mario Costeja Gonzalez, May 13, 2014 (Google Spain v. AEPD), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN.

Google 搜尋引擎輸入他的名字，就會出現他的財產被強制拍賣的兩則新聞報導連結。[252]

González 於 2009 年主張該強制拍賣事件已結案多年，乃向該報社要求移除或修改該網頁新聞報導。報社拒絕其請求。González 亦於 2010 年請求 Google 西班牙分部(Google Spain)或 Google 美國總部(Google Inc.)請求移除該新聞搜尋之連結，仍未獲實現。[253]

González 乃於 2010 年向西班牙資料保護局（Agencia Española de Protección de Datos, AEPD)請求命 La Vanguardia，與 Google Spain 或 Google Inc.，將該則新聞連結移除。AEPD 於同年 7 月駁回 González 對 La Vanguardia 的請求，理由乃因該新聞存在具有正當理由（讓拍賣得為大眾所知，以順利進行）;[254]但核准了 González 對 Google Spain 及 Google Inc.的請求。[255]

Google Spain 及 Google Inc.乃向西班牙國家高等法院(Audiencia Nacional)提起訴訟要求駁回 González 的請求。[256]由於本案涉及 95 指令的解釋適用，西班牙法院乃將本案提交歐盟法院，請求就下列問題作成先決裁決：

- 95 指令與西班牙國內法是否適用於總部非設於歐盟境內的 Google 公司；
- Google 所經營的搜尋引擎行為，是否屬 95 指令第 2 條第 b 款及第 d 款所規範之資料控管者所為之資料運用行為；
- 95指令規定的刪除權與（或）拒絕權(the right of erasure and/or the right to object)是否能導出被遺忘權(the right to be forgotten)。[257]

[252] *Id*. para. 14.
[253] *Id*. para. 15.
[254] *Id*. para. 16.
[255] *Id*. para. 17.
[256] *Id*. para. 18.
[257] *Id*. para. 20.

（二）歐盟法院裁判

1. 資料運用活動內容發生在歐盟境內，屬 95 指令的規範地域範圍

Google 抗辯實際的資料運用乃完全由 Google Inc.操作，而此公司設址於美國，Google Spain 只是 Google Inc.的子公司(subsidiary)，乃負責增進線上廣告商品及服務的銷售，而與搜尋引擎的資料運用行為無關。[258]然而，法院認為 95 指令第 4 條第 1 項第 a 款的適用應解釋為，係要求資料運用活動內容是由資料控管者所設立的組織在歐盟會員國的領域範圍內所進行；重點是在要求資料運用活動內容在歐盟境內，而不是要求該控管者要在歐盟境內；[259]而本案中 Google Spain 為 Google Inc.設立在歐盟會員國境內的子公司，在會員國境內利用搜尋引擎功能促銷線上廣告服務，進行商業及廣告活動以營利，應受 95 指令之規範。[260]

2. Google 所經營的搜尋引擎行為，屬 95 指令第 2 條第 b 款及第 d 款所規範之資料控管者所為之資料運用行為

法院認為搜尋引擎乃自動地、經常性地、系統性地於網路上搜尋資料，搜尋引擎經營者乃藉此技術，在索引程式架構內，持續性地蒐集、擷取、紀錄，組織這些資料，並儲存於經營者的伺服器內，當接獲搜尋指令時，即可將搜尋結果提供給使用者。這些行為無疑地應被歸類為 95 指令第 2 條第 b 款所定義之資料運用行為。[261]由於搜尋引擎經營者乃決定搜尋引擎的運作方式及目的者，故其亦該當於 95 指令第 2 條第 d 款定義之資料控管者。[262]職此，搜尋引擎的經營者必須受到 95 指令的規範。

在本案，搜尋引擎的作用乃令網路使用者，得以個人姓名進行搜尋，經由搜尋結果獲取有關個人在網路上的資料，而該等資料可能大幅含括個人的私生活細節。如果欠缺搜尋引擎技術，這些個人資料即

[258] *Id*. para. 43.
[259] *Id*. para. 52.
[260] *Id*. paras.56-58.
[261] *Id*. para. 28.
[262] *Id*. paras. 32-33.

甚難產生相互連結關係。[263]由於搜尋引擎經營者掌控搜尋引擎的運作方向，故其有責任確保此搜索引擎的運作模式與隱私保護間，不至於陷入責任歸屬與權力作用的失衡。[264]

總結而言，搜尋引擎所進行的資料使用行為，屬於 95 指令第 2 條第 b 款定義之「運用」行為，而其經營者也必須被認定為第 2 條第 d 款規範之資料運用之控管者。[265]

3. 搜尋引擎經營者的責任程度：是否有義務移除以「姓名」作為關鍵字所得的搜索結果

本案的核心爭議問題乃：95 指令第 12 條第 b 款、第 14 條第 1 項第 a 款是否應該被解釋為：搜尋引擎經營者有義務移除以「姓名」作為搜尋基礎所連結至由第三人製作的網內含有關於該個人的相關資訊，當該資訊對其個人可能造成偏見的形成，或他希望在一段期間後被遺忘，即便該網頁的內容是合法的。[266]即刪除權（被遺忘權）的討論。

95 指令第 12 條第 b 款規定提供當事人有權利自資料控管者處獲得適當的更正、刪除或阻止不符合 95 指令規定的資料運用，尤其是因為資料性質的不完整或不正確。符合 95 指令要求的範圍很廣，例如第 6 條規定對資料品質的要求、第 7 條對合法處理個人資料之要求。以第 6 條第 1 項第 c 款至第 e 款為例，即便一開始是合法地對正確資料的運用，也可能隨著時間的經過，使得該資料運用不再是當初資料蒐集或處理之目的所需，故若繼續運用該資料，將顯得不適當、不相關或不再有關，或超過當初目的範圍。[267]若符合此情形，當事人即得依第 12 條第 b 款規定阻止搜尋引擎經營者進行該資料的運用行為。第 14 條第 1 項第 a 款規定當事人，至少在關涉第 7 條第 e 款及第 f

[263] *Id*. paras. 36-37.
[264] *Id*. para. 38.
[265] *Id*. para. 41.
[266] *Id*. para. 89; Herke Kranenborg, *Google and the Right to Be Forgotten*, 1 EUR. DATA PROT. REV. 70, 72 (2015).
[267] *Id*. para. 93.

款的案件情形下，得在任何時間，於基於有關特殊情況下的急切的正當理由，反對運用有關其個人的資訊。[268]

歐盟法院認為 Google 的資料運用行為屬於第 7 條第 f 款的涵蓋範圍。資料控管者得在追求控管者或第三者之正當利益的必要範圍內，運用個人資料，但若當事人具有更高的利益或基本權利與自由應受保障時，則應禁止。職此以言，當事人可得依據上述規定，主張歐盟人權憲章第 7 條（尊重私人及家庭生活的權利）及第 8 條（保護個人資料的權利）等基礎性權利的保護，請求其個人資料不再為一般大眾搜尋可得，當這些基礎性權利的保護利益，不僅大於搜尋引擎經營者的經濟利益，也大於一般大眾知悉以當事人的姓名所搜尋而得資料的利益的情況時。[269]

就本案言，對於利用 Google 搜尋引擎，以 González 姓名作為搜尋基礎所連結而得之 La Vanguardia 日報的網頁關於 González 的不動產拍賣新聞，考量該資訊對於當事人私人生活的敏感性，以及該資料內容乃關涉 16 年前的新聞，並衡量並無特殊理由須保持公眾知悉此則新聞的利益，故 González 應有權依據第 12 條第 b 款及第 14 條第 a 款之規定，請求 Google 移除這些搜尋連結結果。[270]

歐盟法院於本案中認為，在歐洲，當事人有權利要求 Google 刪除以其姓名搜索可得之網頁連結，除非有更高的正當利益得凌駕於當事人的個資保護利益，以支持拒絕移除。然而，移除的方式並非徹底在網路上刪除其姓名搜索可得連結之網頁內容，以本案為例，González 並無權要求 La Vanguardia 日報刪除有關其不動產拍賣資訊的網頁內容，而只是得要求搜尋引擎經營者刪除網頁連結，讓該有關個人資料的網頁內容較難搜尋而得。[271]

---

[268] *Id*. paras. 76, 95.
[269] *Id*. paras. 86, 97.
[270] *Id*. paras. 98-99.
[271] Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J. LAW TEC. 349, 365 (2015).

4. WP29 所提供的利益權衡標準

在 *Google Spain v. AEPD* 判決後，當事人有權利要求網路搜尋引擎業者刪除以其姓名搜索可得之網頁連結，除非有更高的合法利益得凌駕於當事人的隱私利益上以支持拒絕移除。然而，就如何判斷資料控管者是否存在凌駕於當事人利益之正當利益而得拒絕當事人之被遺忘權的行使，判決雖有概述，但缺乏更具體明確的利益權衡操作標準。有鑑於此，WP29 於 2014 年 11 月做成「Guidelines on "Google Spain"」意見書，[272]提出下列 13 點判斷因素，供作利益權衡判斷操作參考：

(1) 是否以自然人姓名為基礎，產生與自然人相關的搜尋結果。所謂的「姓名」，包括假名(pseudonyms)與綽號(nicknames)，如果假名與綽號的搜尋結果亦得連結該自然人的真實身分；

(2) 當事人是否為公眾人物或在公共事務場域扮演一定角色。此一因素存在「程度性」判斷，「公眾／公共」成分愈濃厚之當事人，就其個資愈不容易行使被遺忘權；

(3) 當事人是否為未成年人。例如未滿 18 歲的未成年人行使被遺忘權的成功可能性較高。因相較於成年人，未成年人多出了未成年人最佳利益保障之需求；

(4) 資料內容是否正確。通常愈不正確或愈易誤導的資料內容，當事人被遺忘權的行使愈易成功；

(5) 就個資使用的正當利益維護而言，該資料是否相關或是否多餘。就此因素之判斷，可進一步為下列思考：

① 該資訊是否與當事人的職場生涯(working life)相關。此思考乃係運用「職場生涯／私人生活」之二分標準。由於並非所有個資

[272] WP29, Guidelines on the Implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/121 [hereinafter Guidelines on "Google Spain"], 14/EN: WP 225, Nov. 26, 2014, *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

皆與自然人私密生活相關，故搜尋引擎的搜尋結果，若與當事人的私密生活愈不相關，該搜尋結果的存在就愈易為大眾所接受；

② 該搜尋結果之內容是否屬仇恨、侮辱或誹謗言論，而需負擔民、刑事責任。愈屬於此類搜尋結果，其言論價值愈低，取向於保障資訊隱私的被遺忘權就愈易獲得保障；

③ 搜尋結果是否清楚地顯示僅是個人意見，抑或為事實確認之陳述。若搜尋結果顯示的是事實確認的陳述，被遺忘權行使較可能被允許，蓋事實有正確與否之區分；若搜尋結果僅關乎個人意見陳述，例如某人對作為政治人物之當事人之公務決策之評論意見，縱使該意見會令該當事人受傷害或不愉快，該當事人之被遺忘權的行使也不易成功；

(6) 搜尋所得資料性質是否敏感。搜尋所得之資料內容愈關乎當事人之私密敏感事務，被遺忘權的行使愈易成功；

(7) 資料是否久未更新。就運用目的而言，資料是否超過所需存在時間；若是，被遺忘權行使可能性愈高；

(8) 搜尋結果是否會對當事人造成偏見（或歧視）效果或造成不合比例的隱私之負面影響。愈可能造成上述效果之情形，被遺忘權行使的可能性愈高；

(9) 搜尋結果顯示的個資內容是否會將當事人置於險境，例如提供當事人被他人跟蹤騷擾的風險。該風險愈高，被遺忘權行使的可能性愈高；

(10) 原始資料是在何種脈絡下被蒐集，以致得為搜尋結果所顯示。例如若該個資運用是基於當事人同意所為，但嗣後當事人撤回其同意；於此情形下，被遺忘權行使的可能性愈高；

(11) 原始資料的公開是否因新聞報導之目的所為。與新聞自由利益愈相關，被遺忘權行使的可能性愈低；

(12)將資料公開之人是否具有法定職權或負擔法律義務而將該個資公開（例如公職參選人之個資公開）。愈屬於此種類型的個資公開，當事人之被遺忘權行使的可能性愈低；

(13)資料是否有關刑事犯罪。此種個資公開情形，多半存有特別法規定;而處理原則通常是:對於已發生經過多年的青少年犯罪資料，愈可能准許被遺忘權的行使，而愈嚴重且愈近期的犯罪事件，准許行使被遺忘權的機會愈低。[273]

五、*Lecce* Case[274]

（一）背景事實

義大利公民 Mr.Manni 是建築公司 Italiana Construction Srl 的唯一負責人。Italiana 取得一項遊客中心(tourist complex)的工程合約。[275]Mr. Manni 對萊可斯商會 (Lecce Chamber of Commerce)提起訴訟，主張遊客中心的單位賣不出去，是因為在公司註冊登記(company register)中，可明顯看出他是已被宣告破產 Immobiliare e Finanziaria Salentina Srl (Immobiliare Salentina)公司的唯一負責人與清算人(liquidator)。[276] Mr. Manni 主張,公司登記中所出現與他相關的個資，係透過一家專門在公共註冊系統「挖」資料之私人公司對其進行背景調查之後所產出。他乃向 Lecce 商會要求將其個資從公司登記中移除，但 Lecce 拒絕了他的請求。他就商會該決定向法院提起訴訟，要求 Lecce 商會刪除、匿名、或遮蓋其與 Immobiliar Salentina 清算有關的資料；同時，也要求商會補償他的名譽損失。[277]

在 2011 年 8 月的判決中，法院(Court of Lecce, Italy)贊同 Mr. Manni 之主張，判命 Lecce 商會將 Mr. Manni 與 Immobiliar Salentina

---

[273] *Id*. at 13-20.
[274] Case C-398/15, Camera di Commercio, Industria, Aritigianato e Agricoltura di Lecce v. Salvatore Manni, Mar. 9, 2017, *available at* http://curia.europa.eu/juris/document/document_print.jsf?docid=188750&text=&dir=&doclang=EN&part=1&occ=first&mode=lst&pageIndex=0&cid=17194895.
[275] *Id*. para. 23.
[276] *Id*. para. 24.
[277] *Id*. paras. 25-26.

清算有關的資料加以匿名，並支付 Mr. Manni 補償金以及利息與其他費用，理由乃：公司登記中所列資料，若將個人姓名與公司之某階段(如清算)相連結，則不允許將此筆資料永久保存，除非保存或公開這筆資料符合特殊的一般利益(general interest)。由於民法並未明確指出公司註冊登記的最長時間為何，法院認為，在清算結束「一段適當時間後」，且公司的註冊紀錄已從公司登記(register)中移除，此時已無需要繼續聲明該公司清算當時之負責人姓名。如果是為符合 Legislative Decree No 196，以及公眾對於某公司曾經存在、興衰的歷史記憶情感，匿名之公司資料也能達到同樣目的。[278]

Lecce 商會針對此判決向義大利最高法院(Court of Cassation, Italy)提起上訴。最高法院決定停止審理程序，並將下列問題提請歐盟法院給予先決裁決：

1. 95 指令第 6 條第 1 項第 e 款規定，個資保留的格式允許識別當事人的時間，不應超過為蒐集資料或對其進行進一步處理的目的所需時間。這項原則，是否一定優先於公司註冊登記所遵循的公開原則，即任何人在任何時間都可以取得登記中與個人相關的資料？
2. 在 Article 3 of Directive 68/151 規範下，當該資料已不能再公開，而是只能經由資料管理人在個案評估的基礎上，讓某些人在某段限定期間可以取得的情形下，是否可准許取消時間限制、且讓任何人都可以參考公司登記中的資料？[279]

（二）歐盟法院裁判

歐盟法院認為，義大利最高法院的提問之重點在於：Article 3 of Directive 68/151 與第 6 條第 1 項第 e 款是否必須用以下方式解釋：會員國可以(甚或必須)准許個人向負責公司註冊登記之機關提出要求，

[278] *Id*. paras. 27-28.
[279] *Id*. para. 29.

限制他人存取與該個人相關、且記錄在公司登記中之個資(在該公司已解散一段時間後，以及以個案評估的模式下)。[280]

在本案例中，一開始的關注點在於第三方是否可以存取公司登記中的這種個人資料，並未特別關心這些資料後續是否被其他公司進行運用。[281]依照 Article 2(1)(d) of Directive 68/151，會員國須採取必要措施，以確保公司履行其義務，針對被授權在法律上或與第三方交涉時代表公司之人、參與經營管理或控管該公司之人，公開其任命、離職或其他個人細節(particulars)。另外，根據 Article 2(1)(j)，清算人之任命、其他相關個人細節(particulars)與其權力範圍(respective powers)也必須公開。[282]依照 Article 3(1) to (3) of Directive 68/151，這些個人細節(particulars)必須在每一個會員國的中央註冊登記(central register)、商業註冊登記(commercial register)或公司註冊登記(company register)(統稱「註冊登記」) 中轉錄下來，而需要時必須能取得部分或全部這些個人細節的影本。[283]可確定的是，個人細節包含 95 指令第 2 條第 a 款定義之「個人資料」。法院的判例法明確表明，即使個人訊息是作為專業活動的一部分資料而遭到揭露，並不代表該訊息不能被歸類為個人資料。[284]此外，主管機關負責轉錄與保存公司登記中之資訊，且在適當情況下交予提出要求之第三方，在 95 指令第 2 條第 a 款及第 d 款的定義下，主管機關已構成「運用」個人資料，也就成為資料之「控管者」。[285]

根據 95 指令前言第 25 點說明，指令目的乃在確保自然人之基本權利與自由能得到高度保護，尤其是對隱私之權利，而高度保護主要呈現在兩方面：首先，對於負責運用資料之控管者所規範之義務，特別是資料品質、技術安全、告知主管機關、以及可以對資料進行處理之情況為何等方面；其次，賦予當事人之權利，能被告知個資被進行

[280] *Id*. para. 30.
[281] *Id*. para. 31.
[282] *Id*. para. 32.
[283] *Id*. para. 33.
[284] *Id*. para. 34.
[285] *Id*. para. 35.

運用、可查閱該資料、可要求更正、甚至在某些情況下可拒絕其個資之運用。[286]

負責公司註冊之機關對個資的運用須具備 95 指令第 7 條所規定之合法事由：第 c 款之遵守法律義務所必要、第 e 款之使其官方權力或執行公共任務所必要，或第 f 款為追求資料控管者或是接受資料揭露之第三方之正當利益（即查閱該個資的正當利益）所必要。[287]

在本案例中，進入主程序之雙方的爭議分歧點乃：在某間公司停止營業一段時間後、且在當事人的要求下，負責公司登記之機關是否應該刪除或匿名其相關個人資料，或是限制其公開？若是，此項義務是否源於 95 指令第 6 條第 1 項第 e 款規定？[288]

根據 95 指令第 6 條第 1 項第 e 款規定，會員國必須確認，儲存個人資料的期限應視當初運用該資料之目的而定，而允許識別當事人的部分，則儲存時間不應超過為達當初目的所需的時間。若因為歷史、統計或科學因素需要，資料須儲存超過所需時間，會員國必須提出適當的保護措施(safeguards)。[289]若有未能遵守此規定之情況，會員國為保證當事人之權利，能自資料控管者處刪除或隱匿其相關資料。[290]

根據 95 指令第 14 條第 1 項第 a 款，會員國應賦予當事人權利，在針對其特殊情況之合法基礎下，可反對與其相關之資料運用；若反對具有正當性，資料控管者所進行的資料運用就不能再牽涉到相關資料。[291]

要決定會員國是否必須賦予自然人權利，可要求負責公司登記之機關刪除或遮擋其在公司登記中之個資，或是限制個資的存取，首先必須確定該註冊登記的目的。從這方面來看，Directive 68/151 所提出資料公開的目的是很明確的：要保護與股份公司(joint stock companies)和有限責任公司(limited liability companies)相關的第三方利益，因為

[286] *Id*. paras. 37-38.
[287] *Id*. para. 42.
[288] *Id*. para. 44.
[289] *Id*. para. 45.
[290] *Id*. para. 46.
[291] *Id*. para. 47.

第三方擁有的唯一保障只有其資產。為了這個目的，相關公司的基本文件應該公開，如此第三方才能確認其內容及公司的相關資訊，尤其是公司主要負責人的個人細節。[292]此外，有鑑於會員國之間貿易日益頻繁，Directive 68/151 的主要目的是要保障公司與第三方之間往來的法律確定性(legal certainty) ；且任何人想與位在其他會員國之公司發展貿易關係，都必須能輕易取得該公司組成或負責人之重要資訊。這就需要所有相關資訊都明確地記錄在公司註冊中。[293]從法院的判例法中可以明確得知，Article 3 of Directive 68/151 所提出之資料公開，目的是為了讓任何有興趣之第三方都能獲得充分訊息，而不必另外提出需受保護之權利或利益。法院也指出，Article 54(3)(g) of the EEC Treaty 中的用字，就是指一般性地(generally)對第三方利益的保護，並未區分或排除任何類型的第三方，也因此，不能將 Article 54(3)(g) 中所指之第三方限縮為只包含公司之債權人(creditors)。[294]至於為了達成 Article 3 of Directive 68/151 之目的，是否需要在公司已經結束後，仍然將 「自然人」之個資保留在公司登記上，且/或讓任何第三方都得以存取，關於這一點，並無任何明確法條規定。[295]

然而，就像佐審官所指出(意見書的第 73-74 點)，即使在公司已經解散後，與其相關之權利與法律關係仍持續存在。因此，若產生糾紛時，可能還是需要藉由 Article 2(1)(d)(j) of Directive 68/151 所定義之資料以判定該公司行為之合法性，第三方也才能藉以對公司成員或清算者提起訴訟。[296]再者，依照各會員國所規定之限制期(limitation period)不同，會需要用到這些個資的糾紛，有可能在公司解散後多年才出現。[297]由於各種可能情況的範圍極廣，其中可能牽涉不同會員國的成員、以及在各國、各領域都分歧極大的限制期，對於從公司解散到公司登記應該何時停止紀錄及公開資料，目前看來似乎不可能訂出

[292] *Id*. paras. 48-49.
[293] *Id*. para. 50.
[294] *Id*. para. 51.
[295] *Id*. para. 52.
[296] *Id*. para. 53.
[297] *Id*. para. 54.

一個單一的時間限制。[298]在此情況下，會員國無法保障自然人(在公司解散一段時間後)有權利刪除或隱匿其個資，使公眾無法取得。[299]

上述就 95 指令第 6 條第 1 項第 e 款及第 12 條第 b 款的解釋，並未造成對當事人基本權利之不合比例的干預(disproportionate interference)，特別是當事人對尊重個人生活的權利。[300]

首先，Article 2(1)(d) and (j) and Article 3 of Directive 68/151 僅要求公開部份的個人資料，即有權代表公司或參與行政運作者、監管公司者、曾被指派為公司清算人者之身分與職務內容；其次，如同上述所指出之 Directive 68/151 所提出資料公開的目的是因為股份公司和有限責任公司提供給第三方利益的唯一保障只有其資產，因此增加了第三方的經濟風險。既然如此，則有正當基礎(justified)要求選擇透過這類公司進行貿易之自然人，公開其身分與公司職務之相關資訊。最後，雖然需要優先考慮保護第三方利益以及確保法律確定性、公平貿易以及內部市場適當運作，也不能排除可能在特殊狀況下，個別案件有合法理由，足以正當限制第三方(在公司結束足夠長的時間後)對公司登記中個資進行存取。[301]然而，在個案評估的基礎上，當事人是否可以要求負責公司登記之機關限制對其個資的存取，最終的決定權還是屬於國家法律決定。[302]

個案評估須考量所有相關因素，判斷是否有合法且極重要(overriding)的原因，足以正當限制第三方存取 Mr. Manni 在公司登記中的資料。Mr. Manni 宣稱，他現擔任唯一負責人之公司 Italiana Costruzioni，所建造的遊客中心出售遇到困難，是因為潛在買家能夠獲得公司登記中關於 Mr. Manni 的資料，但單憑此項宣稱，並不足以構成上述之「合法且重要的」原因，特別是考量到存取該資訊也符合潛在買家的合法利益。[303]

---

[298] *Id*. para. 55.
[299] *Id*. para. 56.
[300] *Id*. para. 57.
[301] *Id*. paras. 58-60.
[302] *Id*. para. 61.
[303] *Id*. para. 63.

六、小結

歐盟法院於 *Riga Satiksmes* 案闡述了 95 指令第 7 條第 f 款的適用，必須滿足三項要件：

1. 為追求資料控管者或第三者之正當利益為目的所必須者；
2. 為了上述正當利益追求，而有必要運用個人資料；
3. 受 95 指令第 1 條第 1 項保護之當事人的利益或基本自由權利未凌駕於上述正當利益。

並針對此三要件要求，進行本案論述。在第 3 項要件檢驗中，就當事人之基礎性權利受侵害的嚴重程度判斷，強調應注意該資料能否由公共資源(public sources)中被取得，會影響判斷結果；此外，當事人的年紀，也是應該列入考量的因素之一。更重要的是，歐盟法院於本案中認為符合 95 指令第 7 條第 f 款之法律效果，僅是賦予警局提供乘客個資予 Riga Satiksme 的合法事由，並不能理解為警局就因此有提供給 Riga Satiksme 乘客個資的法律強制義務。

歐盟法院於 *Ryneš* 案認為，本案之錄影監視系統從資料控管者的私人場所向外監看公共空間，即使所攝錄內容只有部分是公共空間，也將使影像攝錄行為不符合 95 指令第 3 條第 2 項所規定之「純粹的」個人或家庭活動。本案於適用 95 指令的情形下，法院認為 Ryneš 得考慮 95 指令第 7 條第 f 款規定，主張影像攝錄行為乃保護 Ryneš（資料控管者）個人及其家人的財產、健康與生命等之正當利益。

歐盟法院於 *ASNEF* 案揭示：會員國之國內法律不得額外添加 95 指令第 7 條第 f 款所無之要件限制，用以加強限制資料控管者的個資運用行為。於本案，西班牙國內法律就 95 指令第 7 條第 f 款的適用，添加了該被運用的個資必須取自於「公共資料來源」的條件限制，違背了 95 指令第 7 條第 f 款之意旨，應被排除適用。

歐盟法院於 *AEPD v. Google* 案先確認本案適用 95 指令後，接續討論 Google 的資料運用行為是否屬於指令第 7 條第 f 款的涵蓋範圍。法院認為，González 得主張歐盟人權憲章第 7 條（尊重私人及家庭生

活的權利）及第 8 條（保護個人資料的權利）等基礎性權利的保護利益，已凌駕於搜尋引擎經營者（資料控管者）的經濟利益，以及一般大眾(第三者)知悉以當事人的姓名所搜尋而得資料之利益，使 Google 的個資運用行為不再符合第 7 條第 f 款規定。然後，González 得依據 95 指令第 12 條第 b 款及第 14 條第 a 款之規定，請求 Google 移除以 González 姓名作為搜尋基礎，所連結而得之 La Vanguardia 日報的網頁之搜尋結果。

歐盟法院於 *Lecce* 案雖主要討論「在 95 指令第 6 條第 1 項第 e 款規定下，某間公司停止營業一段時間後，於當事人的要求下，負責公司登記之機關是否應該刪除或隱匿公司登記中與該當事人相關之個資，或是限制個資公開」，但歐盟法院得出會員國無法保障自然人(在公司解散一段時間後)有權利刪除或隱匿其個資，使公眾無法取得之結論，乃取決於註冊登記之目的「保障第三方得知該公司組成或負責人之重要資訊的商業利益」，與當事人自由權利保障之權衡，而得出判斷標準：當事人須具備合法且極重要(overriding)的原因，足以正當限制第三方存取在公司登記中的資料，始得正當限制第三方(在公司結束足夠長的時間後)對公司登記中的個資進行存取。也涉及 95 指令第 7 條第 f 款之正當利益權衡。

第四節 歐盟會員國案例簡介

由於歐盟各會員國之國內判決，不易搜尋到英文版本，囿於語言能力限制，下列案例之整理，乃轉引自 Future of Privacy Forum & NYMITY 所撰寫之「以 GDPR 規範之正當利益為基礎之個資運用行為 (Processing Personal Data on the Basis of Legitimate Interests under the GDPR)」英文報告內容，[304]合先敘明。

[304] Future of Privacy Forum & NYMITY, Processing Personal Data on the Basis of Legitimate Interests under the GDPR, *available at* https://info.nymity.com/hubfs/Landing%20Pages/Nymity%20FPF%20-%20Legitimate%20Interests%20Report/Deciphering_Legitimate_Interests_Under_the_GDPR.pdf?hsCtaTracking=9cf491f2-3ced-4f9c-9ffa-5d73a77a773e%7C7469b2ec-e91c-4887-b5db-68d407654e23.

一、Federal Labour Court, Germany (July 27, 2017)

一家公司在員工的電腦安裝監視軟體，可以記錄所有的鍵盤輸入與定期生成的螢幕截圖。該員工被解雇後，向法院提告公司此監控行為。法院最終判決認為公司此一監控方式太具侵略性，無法主張此屬公司之正當利益而合法。蓋公司運用員工所有的鍵盤輸入資料，可以讓公司建立一份關於該員工全面、完整的個人檔案，除了與公司事務有關的資料外，還包括其私人生活資料。此外，可能還會包括運用到特種資料（敏感性資料）。[305]

二、Federal Court of Justice, Germany (June 4, 2013)

一家徵信社基於業務需求，為其客戶們在其徵信對象之車輛安裝隱藏式車載 GPS 接收器，以便監視徵信對象的活動。客戶委託徵信的動機主要是關於經濟和私人利益，其中一些涉及婚姻糾紛。法院在判斷對於徵信對象的個資運用行為是否滿足正當利益權衡條款要求時，認為運用 GPS 資訊之行為，必須具備強有力(strong)的正當利益，始得為之，例如用於自我防衛(self-defense)。然而，本案之經濟和私人利益不符合強有力的正當利益之要求。[306]

三、Data Protection Authority, Supreme Administrative Court of Sweden (April 28, 2016)

一家保全公司和一家石油公司協會向瑞典資料保護機關（Data Protection Authority, DPA）提交了一項免除資料保護法適用的申請，以解決普遍存在於這個行業間的「加油後卻逃離未付費」的問題：每年約有 10 萬起此類偷油行為，造成擁有 1400 個加油站據點的公司，每年約 540 萬美元的損失。申請人想要在加油站入口處裝設一個專用攝錄器以自動讀取車輛牌照號碼，並將這些資料與保全公司資料庫（包含車輛清單和相關資料）中註冊的資料進行比對使用。此一申請被 DPA 駁回，理由是此監視系統也涉及犯罪資料（即保全公司資料庫的「黑名單(blacklists)」資料）的運用，且全面性地運用加油車輛

[305] *Id.* at 21-22.
[306] *Id.* at 22.

的車牌號碼屬於大規模資料運用行為。申請人就 DPA 之駁回決定，向法院提起訴訟。一審法院維持 DPA 決定；申請人上訴。上訴法院廢棄 DPA 決定。DPA 上訴至最高行政法院，最高行政法院廢棄上訴法院判決，維持 DPA 的原初決定。理由主要乃犯罪資料的運用適用特別法規定，且申請提案亦未交待資料不正確性與全面性運用的風險、多少公司將參與，以及所形成的隱私風險。DPA 與法院在運用正當利益權衡條款進行利益權衡時，於本案，著重在「必要性(necessity)」的論述，認為申請人的申請提案未滿足此要件要求：因此資料運用行為乃不區分對象的全面性運用，與目的達成間不成比例。[307]

四、Data Protection Authority, The Netherlands (Investigation into the combining of personal data by Google, Report of Definitive Findings. November 2013)

一家公司將自使用者使用其公司所提供的數項服務與產品（網路搜尋引擎、視訊串流網頁、網頁瀏覽器、網路地圖、電子郵件）所獲得的個人資料，進行連結使用，引起荷蘭資料保護機關（Data Protection Authority, DPA）進行調查。此公司在隱私權政策內說明其連結使用上述個資的四項目的：對於使用者的需求提供量身定做的服務、產品開發，量身定做廣告的顯示，以及網站分析。DPA 認為該公司的資料運用行為並非立基於當事人的有效同意上，蓋同意並不明確，且告知亦不充分。至於在正當利益權衡條款使用上，DPA 雖認為該公司運用資料目的乃為發展新型態的網路服務，屬於公司的正當利益，但仍須考量此舉可能會對當事人之隱私保護的影響。為了符合正當利益權衡條款要求，公司必須建立安全機制以防免對於當事人形成任何不成比例的不利益。於本案，DPA 認為公司的正當利益並未凌駕於當事人個資保護利益，主要乃不符合「必要性」要求，理由有：

- 所運用資料之性質，即公司蒐集而得之資料，有些甚具敏感性，例如付款資料、位置資料等；

[307] *Id.* at 23.

- 公司運用資料所提供之服務，從使用者觀點來看，乃基於完全不同之目的；
- 缺乏足夠且具體的資訊；
- 欠缺有效的選擇退出機制；
- 荷蘭的網路使用者幾乎沒有不使用該公司所提供服務之可能，即便不註冊使用者帳戶。例如使用搜尋引擎或網路地圖。[308]

五、Data Protection Authority, France Deliberation No. 2012-214 (July 19, 2012)

法國資料保護機關（Data Protection Authority, DPA）調查一家線上零售業者保存顧客的銀行資料超過所發生的交易行為所需求的時間。DPA 調查發現，該業者將系統預設保留顧客每一筆交易之相關銀行資料（例如持卡人姓名，卡號，有效期，以及 CVV 代碼）。業者主張兩項運用合法事由：履約所必須及追求正當利益所必要。DPA 認為，業者保留銀行資料行為，已超過履約（線上交易）所必須之範圍。正當利益權衡條款主張部分，DPA 雖肯認該業者保存這些個資，有助於使下次付款更為簡便，並可優化交易業務，而具有正當的商業利益，但鑑於銀行資料的敏感性，業者應有限期保存之要求，期限屆至，即應刪除。此保存期間，DPA 認為依法最長只能保存 13 個月。此外，該業者亦未提供適當的資料安全維護措施，升高當事人之個資保護風險。[309]

六、Spanish National Court of Appeals, June 6, 2012

一家公司運用了近 3700 萬西班牙人的個人資料，創建了一個自動資料檔案庫，資料內容包括身分證字號、現在和以前的地址以及出生日期。這些資料是從選舉和市政登記冊（不是公開可得之來源）和信用報告系統蒐集而得。該公司建立此資料庫之目的，乃透過將資料販售給第三方（例如收債員、詐欺調查員），以獲取商業利益；而其

[308] *Id.* at 24-25.
[309] *Id.* at 25-26.

他人也可以透過蒐尋該網站，掌握當事人居住地點。西班牙資料保護機關（Data Protection Authority, DPA）認為該公司所為之個資蒐集與傳輸行為，皆未經當事人同意，係屬違法，遂對該公司進行裁罰。該公司主張指令第 7 條第 f 款之正當利益權衡條款為抗辯。法院認為公司此一主張並無理由，判決理由為：

- 該公司所運用資料非取自公開可得之來源；
- 該公司運用行為僅為牟取己身商業利益，此利益並未凌駕於當事人被傷害之隱私權利。[310]

[310] *Id.* at 26-27.

第四章 比較及分析歐盟及美國對於生物特徵資料之規範趨勢及實際案例

第一節 歐盟 GDPR 規定

一、生物特徵資料(biometric data)之定義與概念釐清

（一）生物特徵資料之定義

GDPR 第 4 條第 14 款將「生物特徵資料(biometric data)」定義為：「透過特定技術處理(specific technical processing)所得關於自然人之身體的(physical)、生理的(physiological)或行為的(behavioural)特徵而允許(allow)或確認(confirm)該人之獨特辨識性(unique identification)之個人資料，例如臉部圖像(facial images)或指紋資料(dactyloscopic data, i.e. fingerprint data)。[311]據此定義，生物特徵資料得區分為兩大類：

- 身體或生理特徵資料：身體特徵與生理特徵倆者概念區分並不清楚，大多論述亦未區分使用。[312]例如指紋、臉部、虹膜(iris) 、視網膜(retina)、耳形(ear shape)等。
- 行為特徵資料：例如鍵盤敲擊(keystroke)、步態(gait)、簽名(handwritten signature)、眼動追蹤(eye tracking)等。

（二）構成 GDPR 第 9 條第 1 項規定之特種個資的生物特徵資料

依 GDPR 第 9 條第 1 項規定，得被當作特種個資而受 GDPR 特別保護的生物特徵資料，必須是將生物特徵資料用以獨特性地識別(uniquely identify)特定自然人。申言之，GDPR 關於生物特徵資料之特別保護的適用，不僅仰賴資料本身的生物特徵屬性，尚須加上資料被使用的目的。若以基因資料(genetic data)作為第 9 條第 1 項規定之特種個資而受特別保護的比較以觀，基因資料本身的屬性即足以支撐其之敏感特性而受特別保護，而無須再考量基因資料被運用的目的。

311 GDPR, Art. 4(14).
312 *See* Catherine Jasserand, *Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data*, 2 EUR. DATA PROT. L. REV. 297, 304 (2016).

整言之，GDPR 第 4 條第 14 款定義的「生物特徵資料」，並非特種個資；第 9 條第 1 項規定的「用以獨特性地識別特定自然人的生物特徵資料」，才是得受 GDPR 特別保護的特種個資。

（三）概念釐清

1.「特定技術處理(specific technical processing)」之要素：從生物特徵變為生物特徵辨識資料

生物特徵資料的形成，須經特定技術處理，[313]通常為下列步驟：

- 註冊(enrollment)程序：首先，取得該生物特徵的「影像(image)」，此影像習稱之為生物特徵「樣本(sample)」；
- 特徵提取(feature extraction)程序：接著，將樣本內的資訊特徵透過軟體程式「提取(extract)」；
- 模組(template)與比較(comparison)程序：最後，將提取之特徵建立「生物特徵『模組(template)』」並儲存，作為日後比較以辨識特定自然人之用。[314]

以智慧型手機的生物特徵辨識技術之運用為例，具備此項功能之手機需配備有：(1)掃描裝置，用以取得生物特徵影像（例如指紋或臉部圖像）、(2)相關軟體，用以提取生物特徵；(3)資料儲存空間，用以儲存生物特徵模組，以供日後比較辨識之用。[315]

上述技術運用會產生兩種資料形式：生物特徵樣本與生物特徵模組，相對於此兩種技術資料，未經過技術轉化前之生物特徵資料（例如指紋），可稱之為原始資料(raw data)。若按 GDPR 第 4 條第 14 款

[313] GDPR, Recital 51 (“The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.).
[314] *See* Jasserand, *supra* note 312, at 302-03.
[315] J. P. Raynal, *With Great Technology Comes Great Responsibility: Why Smartphone Users' Biometric Data Needs to Be Protected*, 48 HOFSTRA L. REV. 179, 191 (2019).

之「生物特徵資料」定義，則不包括未經特定技術處理的原始資料。[316]

2. 「獨特性地識別(uniquely identify)」之要素：「識別」與「確認」之區分

WP29 於 2012 年發布的「生物特徵技術發展之意見書(Opinion 3/2012 on developments in biometric technologies)」中，[317]區分「生物特徵識別(biometric identification)」與「生物特徵確認/驗證(biometric verification/authentication)」之不同：

- 「識別(identify)」是從多數人中辨識出特定人，是一種「一對多的配對程序(one-to-many matching process) 」。例如政府就護照制度設計指紋辨識功能，人民使用護照通關時，護照內的指紋模組，不僅用於「確認」是否為使用者本人，尚用於與指紋模組資料庫比對，「識別」使用者是否為政府列管之人員；
- 「確認(verify)」乃辨識該人是本人，是一種「一對一的配對程序(one-to-one matching process) 」。例如，上述護照內的指紋模組用於確認是否為使用者本人。[318]

據上，「識別」與「確認」兩種用語雖都含有辨識作用，但作用目的仍有區別。

GDPR 第 4 條第 14 款之生物特徵資料的定義規定與第 9 條第 1 項生物特徵資料構成特種個資之規定，使用 identification, identify，未使用 “verification”一字；但 GDPR 前言第 51 點則同時使用 identification 與 authentication（「允許獨特識別或驗證自然人之特性(allowing the unique identification or authentication of a natural person)」，

316 *See* Jasserand, *supra* note 312, at 303.
317 WP29, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN: WP193, April 27, 2012, *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.
318 *Id*. at 5-6.

而 WP29 的上述意見書乃將 verification 與 authentication 當作同義字使用。

GDPR 用字的不一致，使得生物特徵資料是否構成第 9 條第 1 項特種個資的判斷產生困擾。舉例而言，A 公司生產具指紋辨識功能之智慧型手機，該辨識功能僅用作開機之本人確認使用。亦即，手機內經由前述技術步驟所形成的手機使用者之指紋模組，僅供該使用者配對其指紋以供開機使用。故 A 公司的指紋運用行為，乃一對一的配對運用，屬「確認」作用，而非「識別」作用。倘若主張 GDPR 第 4 條第 14 款結合第 9 條第 1 項規定，生物特徵資料構成特種個資之要件，乃將生物特徵資料用以「識別」特定自然人的話，則 A 公司的指紋運用行為，不構成特種個資的運用。反之，若認為依 GDPR 前言第 51 點之說明，構成特種個資的運用行為，包括將生物特徵資料用以「確認」特定自然人的話，則 A 公司的指紋運用行為，構成特種個資運用。

本報告認為，GDPR 第 4 條第 14 款就生物特徵資料之定義的文字使用乃「允許或確認自然人之獨特辨識性(allowing or confirming the unique identification of that natural person)之個人資料」，於動詞使用了「允許(allow)」及「確認(confirm)」，前者或可對應「識別(identify)」、後者可對應「確認(verify)」，但此款規定畢竟為名詞定義，重點應在「獨特辨識性(unique identification)」，亦即生物特徵資料乃指具獨特辨識性之個資，得以識別或確認特定自然人；但就「辨識」作用而言，「識別」可以包含「確認」，但「確認」無法包含「識別」。

申言之，GDPR 第 4 條第 14 款的定義在設定資料須具「獨特辨識性」，方得為生物特徵資料，而具獨特辨識性的生物特徵資料，具有允許找出或確認特定自然人之作用。因此 GDPR 第 9 條第 1 項進一步設定生物特徵資料要能構成特種個資，尚須加上一動作（動詞）要件：「用以獨特性地識別特定自然人(for the purpose of uniquely identifying a natural person)」；此部分的動詞使用，既未與 GDPR 第 4 條第 14 款規定般併同使用「確認(confirm)」，則應認為立法者有意

將使用具獨特性辨識作用之生物特徵資料，用於「確認」特定自然人之資料運用行為，排除在特種個資特別規範之外。至於 GDPR 前言第 51 點之說明，應理解為對 GDPR 第 4 條第 14 款之定義規定的說明，而非第 9 條第 1 項的特種個資規定之說明。

二、GDPR 對於構成特種個資之生物特徵資料的特別保護規範

（一）GDPR 第 9 條規定之適用

依 GDPR 第 9 條第 1 項規定，對於構成特種個資之生物特徵資料的運用行為，原則應予禁止，只有在具備同條第 2 項所規定的合法事由下，才能例外為之。

依 GDPR 第 9 條第 2 項規定，資料控管者得基於下列事由就特種個資進行運用：

1. 基於當事人的明確(explicit)同意之運用

除非另有歐盟法或會員國法律（即特別法）規定不得運用特種個資外，資料控管者得基於取得當事人的明確(explicit)同意進行個資運用。[319]相較於以當事人的「清楚(unambiguous)同意」作為一般（非特種）個資之合法運用事由，[320]明確同意存在更高程度之要求。「明確性」要求可呈現為，例如「書面」同意；而此一「書面同意」所呈現得符合明確性之要求，在網路世界表達同意時，得改以電子形式呈現，例如寄送電子郵件(email)，傳送經掃描(scanned)附有當事人簽名之電子文件，或使用電子簽章。[321]雖說同意並非一定要使用「書面」形式，才能符合「明確性」要求，口頭說明亦可能可以說明得非常清楚而符合明確性要求，但會有事後舉證確認的麻煩。

319 GDPR, Art. 9(2)(a).
320 GDPR, Art. 6(1)(a); GDPR, Art. 4(11).
321 *See* WP29, Guidelines on Consent under Regulation 2016/679, 17/EN: WP259rev.01, 18, April 10, 2018, *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

2. 基於履踐「勞工法」與「社會安全和社會保護法」對於當事人權利義務保護所必要之運用

公司／組織（即資料控管者）基於歐盟或會員國法律或集體協議之要求，為履行資料控管者所負擔在「勞工法」與「社會安全和社會保護法」領域對於當事人的權利和義務之保護，所必要的個資運用行為。[322]

3. 基於保護當事人或他人之重大利益(vital interests)所必要之運用

當當事人在身體上或法律上無法給予同意情形下，基於保護當事人或他人之重大利益，得對當事人之特種個資進行必要之運用。[323]另依 GDPR 前言第 46 點說明，此款運用事由原則上僅有當該運用行為明顯無法基於其他合法事由為之者始得為之。[324]

4. 慈善團體或非營利組織所為之正當、具適當保護措施之運用

基金會、協會或任何其他非營利組織，基於政治、哲學、宗教或工會之目的，就其正當活動過程中所為之已為適當保護措施之運用，且該運用僅涉及該組織之成員或其過去成員，或與該組織目的有關而定期接觸該組織之人，且這些個資在未經當事人同意下，不會對外揭露者。[325]

5. 當事人明顯(manifestly)已自行公開之特種個資的運用

由於係針對特種個資運用合法事由的規定，條文雖僅規定當事人明顯已自行公開之要求，[326]但應嚴格解釋為當事人「刻意地(deliberately)」使個資公開的情形。[327]舉例而言，甲患有隱疾，經朋友告知乙醫生就此疾病治療是專家，甲乃加入乙設定為公開狀態的臉書社團，並在乙的臉書上留言詢問關於此疾病之治療事宜。雖然甲患有隱疾之健康個資，明顯係甲自行公開於乙的臉書上，但甲留言的目

322 GDPR, Art. 9(2)(b).
323 GDPR, Art. 9(2)(c).
324 *See* GDPR, Recital 46.
325 GDPR, Art. 9(2)(d).
326 GDPR, Art. 9(2)(e).
327 *See* EU. AGENCY FOR FUNDAMENTAL RIGHTS ET AL., *SUPRA* NOTE 84, at 162.

的是為尋求乙的醫療建言，而非刻意欲向大眾公開其患有隱疾之資訊，故不宜認為屬「明顯已自行公開」而得作為特種個資運用事由。

6. 為進行法律訴訟主張所必要之運用

資料控管者為建立、行使或防禦法律上之請求或法院執行其司法權所必要之運用。[328]例如法院在審理親子關係訴訟，如有確認親子關係確實存在的必要，即可依此款規定運用基因個資。

7. 為維護重要公益之必要運用

此款運用事由之使用須符合（齊備）下列要件：

- 基於維護重要公共利益(substantial public interest)所需；
- 依據歐盟法或會員國法；
- 符合比例原則、尊重當事人權利、採取具體保護措施。[329]

8. 其他運用事由

- 依據歐盟法或會員國法律或基於與健康專業人員所定且受 GDPR 第 9 條第 3 項要件及保護措施所拘束之契約，基於預防或職業醫學之目的，為評估員工之工作能力、醫療診斷、為提供健康或社會照護或治療，或為健康管理或社會照護系統及服務，而有必要之運用；[330]
- 依據歐盟法或會員國法規定，在採取適當及具體安全措施保護當事人之權利與自由（尤其是職業秘密）下，基於公共衛生領域之公共利益所為之運用（例如為防止對於健康之嚴重的跨境威脅，或為確保健康照護、醫療產品或醫療設備之品質與安全的高標準）；[331]

328 GDPR, Art. 9(2)(f).
329 GDPR, Art. 9(2)(g).
330 GDPR, Art. 9(2)(h).
331 GDPR, Art. 9(2)(i).

- 為了公共利益的存檔目的，科學或歷史研究目的，或符合第 89 條第 1 項規定之統計目的，基於歐盟法或會員國之對目的達成合比例性之法律，在尊重資料保護權利的本質，以及提供當事人之基本權利與自由適當及具體的保護措施下，所必要之運用行為。[332]

（二）GDPR 第 22 條第 4 項的全自動剖析決策特別保護之適用

依據 GDPR 第 22 條第 4 項規定，以資料驅動之自動剖析決策，若仰賴第 9 條第 1 項規定的特種個資為之，僅能在依據第 9 條第 2 項所規定之當事人明確同意（第 a 款）或基於法律規定（第 g 款）之兩種事由下，並且有採用適當保護措施以確保當事人之自由權利及正當利益時，始得為之。[333]

申言之，依 GDPR 第 22 條規定，對當事人產生法律影響或類似重大影響之全自動剖析決策，不論是一般個資或特種個資，原則上都是不行的，當事人皆享有拒絕權，但仰賴一般個資的自動剖析決策有三種例外允許之事由（履約、法定、明確同意），而仰賴特種個資的自動剖析決策則少了一種「履約必要」的例外允許事由。

（三）GDPR 第 27 條第 2 項之歐盟境外資料控管者或受託運用者委派歐盟境內代表人之特別義務

依據 GDPR 第 3 條第 2 項規定，GDPR 除了規範設立在歐盟境內進行個資運用活動的資料控管者或受託運用者外，亦可能在下列兩種情形下，擴及規範設立於歐盟境外的控管者或受託運用者：

- 基於提供商品或服務所需，針對歐盟境內之當事人進行個資運用行為；
- 基於「監控 (monitoring)」歐盟境內自然人行為所需，對當事人進行個資運用行為；

而上述設立於歐盟境外的控管者或受託運用者，依據 GDPR 第 27 條第 1 項規定，應以書面委派歐盟境內之代表。惟此一要求，依

[332] GDPR, Art. 9(2)(j).
[333] GDPR, Art. 22(4).

同條第 2 項第 a 款規定，不適用於非經常性（偶發性）且不太可能會對當事人的自由權利造成風險的資料運用行為。不過，此一排除委派代表義務之規定，不適用於大規模的運用第 9 條第 1 項之特種個資與第 10 條之前科及犯罪個資的情形。亦即，只要是大規模的運用構成特種個資之生物特徵資料行為，即便是偶發性的運用，設立於歐盟境外的資料控管者或受託運用者，仍負擔有於歐盟境內委派代表人之義務。

（四）GDPR 第 30 條第 5 項之個資運用紀錄保存義務

依 GDPR 第 30 條第 1、2 項規定，資料控管者與受託運用者皆負擔其負責之資料運用紀錄的保存義務。但依同條第 5 項規定，此資料運用紀錄保存義務不適用於員工人數低於 250 人以下之企業或組織，除非其所為之資料運用會對當事人的自由權利造成風險，或非偶然性之運用，或其運用包括第 9 條第 1 項所定之特種個資或第 10 條所定涉及前科及犯罪之個資。亦即，即便是員工人數低於 250 人以下之企業或組織，運用構成特種個資之生物特徵資料，仍須負擔個資運用紀錄保存義務。

（五）GDPR 第 35 條第 3 項之資料保護影響評估(DPIA)程序進行義務

依 GDPR 第 35 條第 1 項規定，一旦資料控管者的個資運用行為可能導致自然人的自由權利保護之高風險時，控管者應於個資運用前，進行資料保護影響評估程序。而依同條第 3 項的「高風險」例示規定，其中第 b 款規定運用大規模之第 9 條第 1 項的特種個資，或第 10 條之前科及犯罪個資，構成「高風險」，應進行資料保護影響評估程序。故資料控管者於大規模運用構成特種個資之生物特徵資料之前，應進行資料保護影響評估程序。

（六）GDPR 第 37 條第 1 項規定之個資保護長(DPO)設置義務

依 GDPR 第 37 條第 1 項第 c 款規定，資料控管者或受託運用者之核心活動，涉及大規模地運用第 9 條第 1 項規定之特種個資或第 10 條規定之前科與犯罪相關個資時，應指定 DPO。

第二節 美國法

就生物特徵資料的保護，美國法欠缺一部類如歐盟 GDPR 般之一般性的聯邦法保護規定，而僅具有個別領域（或事務）的部門式規範，例如美國國土安全部於 2017 年針對旅客所進行的「旅客確認服務(Travelers Verification Service)計畫」，使用臉部辨識技術以確認旅客身分。[334]

於美國州法層次，則存在有保護生物特徵資料的一般性保護規範，最著名的乃伊利諾州(State of Illinois)於 2008 年制定的生物特徵資料隱私法(Biometric Information Privacy Act, BIPA)。[335]此外，德州(State of Texas)2009 年於商業法典(Texas Business and Commerce Code)中制定「蒐集或使用生物識別碼(Capture or Use of Biometric Identifier, CUBI)」條文保護生物特徵資料。[336]華盛頓州(State of Washington)於 2017 年制定與德州類似的法律規定。[337]加州(State of California)於 2018 年制定加州消費者隱私權法(California Consumer Privacy Act of 2018, CCPA)，於 2020 年 1 月 1 日生效，[338]一般性地保護消費者隱私權，故若涉及消費者生物特徵資料的運用行為，即受 CCPA 規範。

相較於 BIPA 與 CCPA 有提供隱私受侵害之當事人的民事訴權規定，德州與華盛頓州之法律則欠缺民事訴權規定，而僅有司法部(attorney general)的民事懲罰權(civil penalty)。[339]

---

334 *See* Raynal, *supra* note 315, at 197-98.
335 ILL. COMP. STAT. § 14/15(b) (2008).
336 TEX. BUS. & COM. CODE ANN. § 503.001(a) (2009).
337 WASH. REV. CODE ANN. § 19.375.010 (2017).
338 CAL. CIV. CODE § 1798.100 (2018).
339 *See* Ian Taylor Logan, *For Sale: Window to the Soul Eye Tracking as the Impetus for Federal Biometric Data Protection*, 123 PENN. ST. L. REV. 779, 799-80 (2019).

以 BIPA 為例，此法對於資料控管者的生物特徵資料運用行為，有六項核心要求：

一、 制定可供公眾閱覽的書面政策、建立資料保留時間表及銷毀指南；

二、 當資料原始運用目的已達成時，或在控管者與當事人的最後一次互動的時間起三年內，應銷毀資料，二者以時間先到者為準；

三、 當事人書面同意之要求；

四、 不得販售生物特徵資料；

五、 不得揭露生物特徵資料，除非經當事人同意，或必須揭露該資料才能完成當事人要求或授權的金融交易，或揭露是根據法律或令狀(subpoena)要求；

六、 生物特徵資料的儲存必須使用業界接受的合理標準，且應高於其他機密資料(confidential information)的保護標準。[340]

第三節 近期案例

一、歐盟法院裁判

（一）*Staatssecretaris* Case[341]

2013 年 11 月 15 日，一家依據荷蘭法律註冊成立的公司，代表土耳其國民 A 提交了一份臨時居留許可申請，以便 A 可以在荷蘭就業。荷蘭的國家安全與司法大臣(the Staatssecretaris van Justitie en Veiligheid)(State Secretary for Justice and Security, Netherlands) (以下稱 Staatssecretaris)於 2014 年 3 月 28 日核准了 A 的申請案，但附帶條

[340] 740 ILL. COMP. STAT. § 14/15 (2010); Raynal, *supra* note 309, at 204-05.

[341] Case C-70/18, Staatssecretaris van Justitie en Veiligheid v A, B, P, Oct. 3, 2019, *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=218617&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6956033.

件要求 A 必須提供臉部影像(a facial image)與 10 隻手指指紋(10 fingerprints)的生物特徵資料(biometric data)。[342]

B 是土耳其國民，其配偶 P 是荷蘭居民，具有土耳其和荷蘭雙重國籍。2014 年 2 月 17 日，P 為家庭團聚而為 B 向主管機關提出臨時居留許可申請。[343]Staatssecretaris 最終於 2014 年 4 月 4 日批准了該臨時居留許可的申請，但附帶條件要求 B 必須提供臉部影像與 10 隻手指指紋。[344]

上述兩申請案中，A 與 B 皆提交了臉部影像與指紋，以獲取臨時居留證，但 A 與 B&P 皆就 Staatssecretaris 要求 A 與 B 提交生物特徵資料部分，分別於 2014 年的 3 月 28 日與 4 月 4 日，向 Staatssecretaris 提起行政訴願(an administrative appeal)。[345]Staatssecretaris 於 2014 年 12 月 23 日及 2015 年 1 月 6 日分別駁回了 B&P 及 A 的訴願；B&P 及 A 分別就該駁回決定向荷蘭的 Hague 地方法院(District Court, The Hague, sitting in Rotterdam, Netherlands)提起訴訟。[346]

Hague 地方法院於 2016 年 2 月 3 日判決 Staatssecretaris 敗訴；Staatssecretaris 向荷蘭的國務委員會(Council of State, Netherlands)提起上訴；國務委員會決定向歐盟法院就爭議問題提請先決裁決。[347]

歐盟法院指出，Article 13 of Decision No 1/80 原則上禁止採用任何新的國家措施，其目的或效果是使土耳其國民行使在會員國領土間為了工作所為的移動自由，受到與 Article 13 of Decision No 1/80 生效時相比更為嚴格的條件限制。[348]歐盟法院認定，荷蘭政府對於會員國之國民欲申請停留於荷蘭超過 90 天的暫時居留申請，要求提供臉部影像與指紋等生物特徵資料之規定，已構成 Article 13 of Decision No 1/80 所為之更為嚴格的新限制。[349]依據歐盟法院的判決先例，此更為

[342] *Id.* para. 21.
[343] *Id.* para. 22.
[344] *Id.* para. 23.
[345] *Id.* para. 24.
[346] *Id.* para. 25-26.
[347] *Id.* para. 28-31.
[348] *Id.* para. 37.
[349] *Id.* para. 41-43.

嚴格的新限制，原則應予禁止，除非該限制是在 Article 14 of Decision No 1/80 所指的限制範圍內，或具有出於公益的優勢理由(an overriding reason in the public interest)，而該限制適切於達成所欲追求的正當目的，且未逾越必要性要求。[350]

歐盟法院依據上述標準，分別檢驗論述如下：

1. 優勢公益性判斷

歐盟法院認為本案所適用法令具備優勢公益之立法目的，理由如下：

首先，要求提供臉部影像與指紋等生物特徵資料之規定的立法目的乃為防止非法入境與居留，就此立法目的，歐盟法院過去即有認定構成出於公益的優勢理由之判例；[351]

其次，法院認為簽發護照時蒐集和保留指紋，以防止偽造及偽用護照之目的，屬於歐盟認可的公共利益目標，即防止非法入境行為的發生；[352]

最後，打擊身分詐欺的重要性是歐盟立法機構所強調的。[353]

2. 手段與目的達成之適切性(appropriateness)判斷

申請人之臉部影像與指紋的蒐集、紀錄，與保存，可以準確地識別申請人之身分，有助於上述優勢公益目的之達成。[354]

3. 手段與目的達成之必要性(necessity)判斷

自然人的臉部影像與指紋受歐盟基本權利憲章(the Charter of Fundamental Rights of the European Union)第 7 條及第 8 條之保護。根據歐盟法院判決先例，對此兩項基本權利之限制，須受嚴格必要性(strictly necessary)之檢驗。[355]

---

[350] *Id.* para. 44.
[351] *Id.* para. 46.
[352] *Id.* para. 47.
[353] *Id.* para. 48.
[354] *Id.* para. 50.
[355] *Id.* para. 56.

臉部影像與指紋的蒐集，提供了一種可靠的識別特定人的方法。另這些個資不具親密性(intimate nature)，不會給相關人士造成任何特別的身體或精神上的不舒服。[356]歐盟立法機構在 Regulation No 767/2008 中本就規定有簽證申請人負擔提供其指紋和臉部影像的義務。[357]此外，依呈交至法院的資料中顯示，申請人的臉部影像與指紋資料，僅限於具合法使用權限之公務員得以接近使用。[358]

關於在個資的保存期間所必須滿足的客觀標準要求：確立所保留之個資與所追求目的間的連結性。[359]在本案中，依荷蘭的相關規定要求，生物特徵資料應在拒絕臨時居留許可的申請、該人離開荷蘭，或合法居留期限屆至之後，在中央檔案系統中保留 5 年；如果第三國國民在荷蘭居留期間歸化荷蘭籍，則將立即銷毀生物特徵資料。[360]在這 5 年的個資保存期間，需隨時確立資料保留與防止和打擊身分和文件詐欺之目的間的連結關係。[361]法院認為保留申請人之生物特徵資料，用以確認其居留於荷蘭期間的合法性，有其必要，特別是在考量延長居留許可時。[362]至於拒絕申請及合法居留期結束後或該居留證有效期屆滿之後，仍保留個資 5 年期間，主要乃用於阻止這些人使用不同之身分，再次提出新的申請。[363]因此本案所適用之 5 年的個資保存期間規定，就防止和打擊身分和文件詐欺之目的而言，並未過長。[364]

綜上以言，本案所適用之荷蘭法令規定，即便已構成 Article 13 of Decision No 1/80 所為之更為嚴格的新限制，但因符合上述三項標準要求，仍屬合法。[365]

---

356 *Id.* para. 58.
357 *Id.* para. 59.
358 *Id.* para. 62.
359 *Id.* para. 63.
360 *Id.* para. 64.
361 *Id.* para. 65.
362 *Id.* para. 66.
363 *Id.* para. 67.
364 *Id.* para. 68.
365 *Id.* para. 69-70.

（二）*Willems* Case[366]

歐盟法律規定：

- Article 1(2)(3) of Regulation No 2252/2004：

1. 護照和旅行證件應有一儲存介面，內含臉部影像；若是歐盟會員國，介面內還需含指紋。資料應被安全保護，儲存媒介應具有足夠的容量，以保護資料的完整性、真實性和保密性；
2. 本規則適用於會員國簽發的護照和旅行證件。它不適用於會員國發給其國民的身分證，或有效期不超過 12 個月的臨時護照和旅行證件。[367]

- Article 4(3) of Regulation No 2252/2004：

生物識別資料應蒐集並儲存在護照和旅行證件的儲存媒介中，以便核發此類證件。就本規則言，護照和旅行證件中的生物特徵資料僅可用於驗證：

(a)護照或旅行證件的真實性；

(b)當法律要求出示護照或旅行證件時，得透過可比較之特徵證明持有人的身分。[368]

荷蘭護照法(Stb. 1991, No 498, the Passport Law)規定：

- 國家護照(national passport)是荷蘭簽發的旅行證件之一(Article 2(1))；
- 荷蘭身分證(identity card)作為在歐洲的旅行證件，對於 1957 年 12 月 13 日在巴黎通過的「歐盟理事會成員國之間關於人員流動管理規則之歐盟協定(the European Agreement on Regulations

366 Joined Cases C-446/12 to C-449/12, W.P. Willems (C-446/12) v Burgemeester van Nuth, H.J. Kooistra (C-447/12) v Burgemeester van Skarsterlân, M. Roest (C-448/12) v Burgemeester van Amsterdam, and L.J.A. van Luijk (C-449/12) v Burgemeester van Den Haag, April 16, 2015, *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=163716&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1946450.

367 *Id.* para. 7.

368 *Id.* para. 8.

governing the Movement of Persons between Member States of the Council of Europe)」之締約國有效(Article 2(1))；

- 旅行證件必須含有一張臉部影像、兩個指紋和持有人的簽名(Article 3(3))。[369]

Mr Willems 和 Ms Roest 和 Ms van Luijk 分別提出護照申請，但皆因拒絕提供臉部影像或數位指紋(digital fingerprints)，而遭主管機關 Burgemeester 駁回申請。Mr Kooistra 提出身分證申請，因拒絕提供數位指紋與臉部影像，被 Burgemeester 駁回申請。[370]這些申請人拒絕提供生物特徵資料的主要理由乃：政府建立和儲存申請人之生物特徵資料，嚴重侵犯其身體完整性和隱私權；且政府之後也可能會將生物特徵資料用於目的以外的用途，特別是將這些資料用於司法目的或為情報和安全部門所使用。[371]

申請人向法院提起訴訟，法院就下列問題提請歐盟法院給予先決裁決：

- 在 C-447/12 案中，荷蘭身分證是否屬於 Article 1(3) of Regulation No 2252/2004 的範圍。蓋歐盟理事會成員國之間關於人員流動管理規則之歐盟協定清楚表明，荷蘭身分證也可作為歐盟內的旅行證件。Article 1(3) of Regulation No 2252/2004 就身分證之規定，是否應與後段之「有效期不超過 12 個月的臨時護照和旅行證件」同樣理解，將不得作為旅行證件之身分證解釋為「有效期為 12 個月或更短」之身分證，而荷蘭身分證的有效期為 5 年，故不在排除之列；
- Regulation No 2252/2004 是否限制辦理護照及身分證所蒐集而得之生物特徵資料，未來轉做其他目的使用。[372]

[369] *Id.* paras. 10-12.
[370] *Id.* para. 16.
[371] *Id.* paras. 17-18.
[372] *Id.* paras. 22-24.

關於第一個問題：是否應將 Article 1(3) of Regulation No 2252/2004 解釋為不適用於會員國發給其國民的身分證，例如荷蘭身分證，不論身分證的有效期間長短，也不論是否有可能將身分證用於該國境外旅行。[373]首先，必須確定 Regulation No 2252/2004 規定是否因身分證的有效期間而異。Article 1(3)的第二句可以清楚地看出，該規定限制了該規則的適用範圍，條文將兩類文件排除在外：「會員國發給其國民的身分證」、「有效期不超過 12 個月的臨時護照和旅行證件」。鑑於條文文字使用「或(or)」連接兩類排除文件，故此兩份文件應被解釋為彼此獨立。[374]因此，根據 Article 1(3) of Regulation No 2252/2004 的法條文字，Regulation No 2252/2004 不適用於會員國發給其國民的身分證，不論其是否為臨時身分證，也不論其有效期間長短。[375]

關於第 2 個問題：Article 4(3) of Regulation No 2252/2004 是否必須解釋為要求會員國保證依據此規則所蒐集和儲存的生物特徵資料，不得用於核發護照或其他旅行證件以外之其他目的使用。歐盟法院認為，參照 Regulation No 444/2009 前言的 recital 5 就 Article 4(3) of Regulation No 2252/2004 之說明，Article 4(3)並不限制會員國制定國內法律對這些資料進行其他目的之使用。此屬會員國之內國立法權限範疇。[376]

二、美國法院裁判

（一）*In re Facebook Biometric Info. Privacy Litig.*

在 2015 年的 *In re Facebook Biometric Info. Privacy Litig.*案件中，數名伊利諾州州民主張臉書(Facebook)未經當事人同意，使用臉部掃描程式蒐集並儲存數千位使用者之臉部資料的生物特徵資料運用行為，違反 BIPA 規定，乃向法院提起民事訴訟請求損害賠償。[377]臉書

[373] *Id.* para. 30.
[374] *Id.* para. 33.
[375] *Id.* para. 36.
[376] *Id.* paras. 47-48.
[377] In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1159 (N.D. Cal.

主張本案不適用 BIPA 規定，因為原告作為臉書使用者，已同意臉書使用政策中規範紛爭解決之準據法為加州法，而非伊利諾州法。[378]但法院於 2016 年最終認為本案關於 BIPA 的爭議處理結果，對於伊利諾州具有重要利益，而決定受理該訴訟。[379]臉書遂轉而主張依 BIPA 關於生物特徵資料之定義，應排除照片(photographs)或取自於照片之資料(any information derived from those photographs)，而臉書的臉部掃描圖像完全取自於用戶上傳臉書之照片，故不屬 BIPA 規定之生物特徵資料。[380]但法院拒絕臉書的此項主張，蓋生物特徵識別符碼(biometric identifier)的掃描通常基於圖像或照片而得，一旦將此類型排除 BIPA 適用，將大幅削弱 BIPA 的適用性。[381]聯邦第 9 巡迴上訴法院於 2019 年拒絕臉書的上訴。因此，臉書乃與進行消費者集體訴訟的伊利諾州臉書用戶成立 6.5 億美元的現金和解。[382]美國聯邦法院法官於 2021 年 2 月 26 日最終批准臉書以 6.5 億美元達成此集體訴訟案的和解，並諭令應盡速支付賠償金給伊利諾州參與提告索賠的約 160 萬用戶。[383]

2016).

[378] *Id.* at 1159.

[379] *Id.* at 1169.

[380] *Id.* at 1170("Facebook has also moved to dismiss on the ground that the statute excludes from the definitions of 'biometric identifier' and 'biometric information' (1) photographs and (2) any information derived from those photographs. Dkt. No. 69 at 10–11. Facebook says that its biometric data is derived exclusively from uploaded photographs and therefore it cannot be subject to BIPA.").

[381] *Id.* at 1171 ("The statute's focus is on newer technology like scans of face geometry, whose 'full ramifications' are not known. *Id.* at 14/5(f). Read together, these provisions indicate that the Illinois legislature enacted BIPA to address emerging biometric technology, such as Facebook's face recognition software as alleged by plaintiffs, without including physical identifiers that are more qualitative and non-digital in nature. 'Photographs' is better understood to mean paper prints of photographs, not digitized images stored as a computer file and uploaded to the Internet. Consequently, the Court will not read the statute to categorically exclude from its scope all data collection processes that use images. And to read that categorical exclusion into the statute would substantially undercut it because the scanning of biometric identifiers is often based on an image or photograph.").

[382] In re Facebook Biometric Information Privacy Litigation, LABATON SUCHAROW, Updated: October 28, 2020, https://www.labaton.com/cases/in-re-facebook-biometric-information-privacy-litigation (last visited Dec. 22, 2020).

[383] 參閱中央通訊社，臉部辨識標註照片被控侵犯隱私臉書花 181 億和解，2021/02/27，https://www.cna.com.tw/news/firstnews/202102280175.aspx（最後瀏覽日：2021/03/02）。

（二）*Norberg v. Shutterfly, Inc.*

於 2015 年的 *Norberg v. Shutterfly, Inc.* 案件中，[384]原告主張 Shutterfly 公司使用臉部辨識技術蒐集其生物特徵資料，違反 BIPA 規定，蓋他們並非 Shutterfly 所提供服務的「活躍用戶(active users)」。[385]Shutterfly 提出與上述案例中臉書主張的同樣主張：BIPA 關於生物特徵資料之定義，排除「照片資料」或「取自於照片之資料」。法院拒絕 Shutterfly 的此一主張，並認為原告所提出之主張合理，蓋原告並非 Shutterfly 網站之顧客，因此原告無法閱讀該網站關於生物特徵資料的書面政策，也無機會提供其同意使用。[386]

[384] Norberg v. Shutterfly, 152 F. Supp. 3d 1103 (N.D. 111. 2015).
[385] *Id.* at 1106.
[386] *Id.* at 1105.

第五章 結論與建議

本報告第一章針對歐盟依據 GDPR 第 97 條第 1 項規定所提出的 GDPR 施行兩周年評估報告進行分析，發現整份評估報告具備以下兩項主軸：當事人權利意識的提升與行使的強化，以及創立新的治理模式、樹立新的資料運用文化。就第 1 主軸而言，相較於 GDPR 對於當事人權利規範完整性，臺灣個資法則較為不完備。就第 2 主軸目標之達成，評估報告強調需仰賴各國或各區域間資料保護法制的融合與合作關係的建立。於執行面上，報告強調「獨立專責的資料保護機關搭配強化的執法權力」的必要性。歐盟此一全球化個資保護法制（全球性資料運用文化）的推展趨勢，臺灣勢必無法置身事外，因此，臺灣立法者於個資保護法律制定或修正時，尤應特別注意與全球接軌之需求。

本報告第二章乃說明 GDPR 關於自動剖析決策行為之規範。以資料驅動的自動剖析決策技術刻正急速發展中，且應用層面廣泛，具有可全面性地影響人們生活的可能。在不遠的未來，若說人們將過著機器決定的人生，或許過於危言聳聽，但說人們正在這條道路上被推動著，應非無稽，只是或緩或急之別。倘若無法或不應完全阻止自動剖析決策技術的發展應用，那麼就應設想如何不讓人生在不自覺中由機器掌控，而斲傷為人之尊嚴。就此，GDPR 為使當事人能知悉關於其之自動剖析決策被應用著，規範有特別透明化要求：使該技術所涉運算邏輯的有意義資訊，以及對當事人的重要性與所預期結果，成為資料控管者負擔之告知義務與當事人得近用資訊範疇。

然而，GDPR 將特別透明規範僅適用於會對當事人產生法律影響或類似重大影響之全自動剖析決策類型的立法決定，對於個資保護的透明化要求，應有不足；於未修法前，本報告主張可透過將演算法資料認定為個資的方式，解決適用範圍不足問題。至於應否建構一種新型態權利—請求解釋權，讓當事人有權請求資料控管者負擔解釋至其能瞭解演算法之運算邏輯的義務？本報告主張，單純揭露演算法並不等於提供關於運算邏輯之有意義資訊；反之，未揭露演算法原貌亦不

等於未提供運算邏輯之有意義資訊。透明化自動剖析決策的關鍵在：使當事人有挑戰（抗議）該決策之可能。就此透明目的之達成而言，與其讓當事人理解複雜的演算法運算邏輯，不如將不被一般人所親近的程式語言轉化為具體影響因子之說明或解釋（例如供作剖析決策的資料類型、這些類型資料如何地與剖析決策相關、該決策會如何影響當事人），俾當事人能合理預見剖析決策對其之可能影響，並有透過自己能力改變決策結果之可能。至於是否要就當事人得近用這些資訊內容之權利，給予一個新名詞「請求解釋權」為稱呼，抑或繼續沿用「近用權」一詞，應非重要。

臺灣個資法欠缺對於自動剖析決策技術的特別透明化規範，勢將升高當事人自由權利遭受損害之風險，應儘速修法填補；GDPR 相關規範的比較法觀察，能提供修法方向之參考。

最後，本報告仍欲再次強調：個資保護利益與自動剖析決策利益的衝突發生時，兩項利益都應不被偏廢地納入考量；極高的透明化要求固有益於當事人的自由權利保護，但同時也會對資料控管者造成沈重的義務負荷，一來一回間的利益權衡，於制度設計與個案適用間，應完整思考。

本報告第三章乃說明有關 GDPR 規定非公務機關之正當利益權衡條款作為個資運用合法事由之適用範圍，以及相關歐盟法院判決之整理。本報告乃藉由就 WP29 於 2014 年提出的「正當利益概念意見書」與歐盟法院自 2011 年至 2017 年間作成相關於正當利益權衡條款裁判之整理觀察，說明 GDPR 第 6 條第 1 項第 f 款之正當利益權衡事由適用之要件，以及正當利益權衡時應考量之因素。本報告希冀藉由正當利益權衡條款的論述，能更清晰地突顯個資運用合法事由的設計結構：運用行為的合法基礎建立在運用行為所追求的正當利益凌駕於當事人因此行為所損傷之權益，得對於臺灣個資法就個資運用合法事由設計不足之處，提供未來修法參考。

本報告第四章係比較及分析歐盟及美國對於生物特徵資料之規範趨勢及實際案例。關於歐盟 GDPR 部分，主要釐清構成 GDPR 第 9

條第 1 項規定之特種個資的生物特徵資料，必須是將生物特徵資料用以獨特性地識別特定自然人始屬之；並說明 GDPR 針對構成特種資料之生物特徵資料的運用，存在哪些特別保護規範；最後，整理兩件歐盟法院裁判，提供實務見解參酌。美國法部分，欠缺一部類如歐盟 GDPR 般之一般性的聯邦法保護規定。至於州法層次，則存在有保護生物特徵資料的一般性保護規範，最著名的乃伊利諾州於 2008 年制定的 BIPA。本報告乃簡述 BIPA 對於資料控管者運用生物特徵資料之行為的相關要求，並提供兩則美國法院判決，說明 BIPA 適用之實際案例情形。

參考文獻

一、中文文獻

張陳弘、莊植寧（2019），新時代之個人資料保護法制：歐盟 GDPR 與臺灣個人資料保護法的比較說明，新學林。

張陳弘（2018），新興科技下的資訊隱私保護：「告知後同意原則」的侷限性與修正方法之提出，臺大法學論叢，第 47 卷第 1 期，201-297 頁。

二、英文文獻

Article 29 Data Protection Working Party. (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679* (17/EN WP248). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Article 29 Data Protection Working Party. (2018). *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679* (17/EN WP251 rev.01). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Article 29 Data Protection Working Party. (2018). *Guidelines on Consent Under Regulation 2016/679* (17/EN WP259 rev.01). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Article 29 Data Protection Working Party. (2018). *Guidelines on Transparency under Regulation 2016/679* (17/EN: WP260 rev.01). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

Article 29 Data Protection Working Party. (2017). *Guidelines on Data Protection Officers ('DPOs')* (16/EN: WP 243rev.01). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

Article 29 Data Protection Working Party. (2014). *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC* (844/14/EN: WP 217). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

Article 29 Data Protection Working Party. (2014). *Guidelines on the Implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/121* **(**14/EN: WP 225). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

Article 29 Data Protection Working Party. (2012). *Opinion 3/2012 on developments in biometric technologies* (00720/12/EN: WP193). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

Bygrave, L. A. (2001). The Place of Privacy in Data Protection Law. *University of New South Wales Law Journal*, *24*(1), 277-283.

Casey, B., Farhangi, A., & Vogl, R. (2019). Rethinking explainable machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise. *Berkeley Technology Law Journal*, 34(1), 143-188.

Castets-Renard, C. (2019). Accountability of Algorithms in the GDPR and beyond: European Legal Framework on Automated Eecision-making. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 30(1), 91-138.

Centre for Information Policy Leadership (CIPL). (2017). *Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR*. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.

De Hert, P., & Gutwirth, S. (2006). Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. In E. Claes, A. Duff, & S. Gutwirth (Eds.), *Privacy and the Criminal Law* (pp. 61-104). Intersentia. https://works.bepress.com/serge_gutwirth/5/.

Dimitrova, D. (2017). Rigas Satiksme: The Scope and Limits of Data Protection, *European Data Protection Law Review*, 3(3), 418-422.

European Commission. (2020). *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN.

European Commission. (2020). *Two Years of the GDPR: Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166.

European Commission. (2011). *Privacy and Data Protection Impact Assessment Framework for RFID Applications*. https://ec.europa.eu/digital-single-market/en/news/privacy-and-data-protection-impact-assessment-framework-rfid-applications.

European Data Protection Board. (2020). *Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak*. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

European Data Protection Board. (2020). *Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak*. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200320_healthdatascientificresearchcovid19_en.pdf.

EU. AGENCY FOR FUNDAMENTAL RIGHTS ET AL. (2018). HANDBOOK ON EUROPEAN DATA PROTECTION LAW.

Ferretti, F. (2014). Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights?. *Common Law Market Review*, 51(1). https://bura.brunel.ac.uk/bitstream/2438/9724/1/Fulltext.pdf.

Gellert, R. (2017). The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment. *European Data Protection Law Review (EDPL)*, 3(2), 212-217.

Goodman, B.& Flaxman, S. (2016). European Union Regulations on Algorithmic Eecision-making and a "Right to Explanation". http://metromemetics.net/wp-content/uploads/2016/07/1606.08813v1.pdf.

Forde, A. (2016). The Conceptual Relationship Between Privacy and Data Protection. *Cambridge Law Review, 1*, 135-149.

Future of Privacy Forum & NYMITY. Processing Personal Data on the Basis of Legitimate Interests under the GDPR. https://info.nymity.com/hubfs/Landing%20Pages/Nymity%20FPF%20-%20Legitimate%20Interests%20Report/Deciphering_Legitimate_Interests_Under_the_GDPR.pdf?hsCtaTracking=9cf491f2-3ced-4f9c-9ffa-5d73a77a773e%7C7469b2ec-e91c-4887-b5db-68d407654e23.

Hemann, C. & Burbary, K. (2013), Digital Marketing Analytics: Making Sense of Consumer Data in a Digital World.

Information Commissioner's Office (2018). *Accountability and governance: Data Protection Impact Assessments (DPIAs)*. https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf.

IT Governance Privacy Team (2019). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide* (3rd ed.). IT Governance Publishing. https://doi.org/10.2307/j.ctvr7fcwb

Jasserand, C. (2016). Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data. *European Data Protection Law Review*, 2(3), 297-311.

Kamara, I. & De Hert, P. (2018). Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach. *Brussels Privacy Hub Working Paper*, Vol. 4. https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf.

Kranenborg, H. (2015). Google and the Right to Be Forgotten, *European Data Protection Law Review*, 1(1) 70-79.

LAMBERT, P. B. (2018). UNDERSTANDING THE NEW EUROPEAN DATA PROTECTION RULES. AUERBACH PUBLICATIONS.

Logan, I. T. (2019). For Sale: Window to the Soul Eye Tracking as the Impetus for Federal Biometric Data Protection. *Penn State Law Review*,123(3)779-811 (2019).

Mayer-Schonberger, V., & Padova, Y. (2016). Regime Change: Enabling Big Data Through Europe's New Data Protection Regulation. *Columbia Science and Technology Law Review*, 17(2), 315-335.

PASQUALE, F. (2016). THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION.

Rustad, M. L. & Kulevska, S. (2015). Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow. *Harvard Journal of Law & Technology*, 28(2), 349-417.

Raynal, J. P. (2019). With Great Technology Comes Great Responsibility: Why Smartphone Users' Biometric Data Needs to Be Protected. *Hofstra Law Review*, 48, 179-214 (2019).

Sloot, B. V. (2017). Editorial. *European Data Protection Law Review*, 3(1), 1-12.

Temme, M. (2017). Algorithms and Transparency in View of the New General Data Protection Regulation. *European Data Protection Law Review (EDPL)*, 3(4), 473-485.

Tene, O., & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, 11(5), [xxvii]-274.

Venier, S., Mordini, E., Friedewald, M., Schütz, P., Hallinan, D., Wright, D., Finn, R. L., Gutwirth, S., Gellert, R., & Turnheim, B. (2013). *Final Report - A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies*. Prescient Project. http://publica.fraunhofer.de/documents/N-238503.html.

Wachter, S., & Mittelstadt, B. (2019). Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, 2019(2), 494-620.

Waldman, A. E. (2020). Privacy Law's False Promise. *Washington University Law Revie, 97*(3), 773-834. https://doi.org/10.2139/ssrn.3339372.

Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology (Harvard JOLT)*, 31(2), 841-888.

Wachter, S., Mittelstadt, B. & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, 7(2), 76-99.

Wachter, S. (2018). The GDPR and the Internet of Things: A Three-Step Transparency Model. https://www.researchgate.net/publication/323766326_The_GDPR_and_the_Internet_of_Things_A_Three-Step_Transparency_Model.

Wright, D. (2012). The State of the Art in Privacy Impact Assessment. *Computer Law & Security Review, 28*(1), 54-61. https://doi.org/10.1016/j.clsr.2011.11.007.

Yordanov, A. (2017). Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation. *European Data Protection Law Review, 3*(4), 486-495.

Zarsky, T. Z. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, 47(4), 995-1020.

Zarsky, T. Z. (2017). An Analytic Challenge: Discrimination Theory in the Age of Predictive Analytics. *I/S: Journal of Law and Policy for the Information Society*, 14(1), 11-36.

GDPR 施行兩周年評估報告之分析及相關議題研析/張陳弘
計畫主持 -- 初版. -- 臺北市 : 國發會, 民 110.01
面: 表，公分
編號: (110)002.0901
委託單位：國家發展委員會
受託單位：輔仁大學學校財團法人輔仁大學
資訊法規
312.07

GDPR 施行兩周年評估報告之分析及相關議題研析
委託單位：國家發展委員會
受託單位：輔仁大學學校財團法人輔仁大學
計畫主持人：張陳弘
出版機關：國家發展委員會
電話：02-23165300
地址：臺北市寶慶路 3 號
網址：http://www.ndc.gov.tw/
出版年月：中華民國 110 年 1 月
版次：初版
刷次：第 1 刷
編號：(110)002.0901 (平裝)