Path dependence and network effects of the GDPR

Melinee Kositwatanarerk* and Klaus Heine†

Abstract

- This article provides an explanation of the global impact of the General Data Protection Regulation (GDPR) by means of a theoretical framework based on path dependence and network effects.
- Path dependence theory gives an in-depth explanation of the antecedents in the past that shape the present and future of the European Union data protection regime. Network effects are the key factor for triggering self-reinforcing processes of path dependence.
- This article explores the main legal mechanisms employed by the GDPR, creating network effects: the adequacy decision, the standard contractual clauses, the binding corporate rules, and the extraterritorial provision.
- The analysis focuses on three phases: (i) the stage preceding the imposition of the Data Protection Directive (DPD) (the preformation phase), (ii) the stage during which the DPD was in force (the formation phase), and (iii) the stage following the introduction of the GDPR (the lock-in phase).
- In order to maintain its network effects, the GDPR may need more simplification to induce existing members to remain within the network, while attracting newcomers to join. Consequently, the GDPR network can expand and maintain its leading position. The recently proposed Digital Omnibus by the European Commission points in that direction.

Background

The global impact of the General Data Protection Regulation (GDPR) is widely recognized. As of 2024, 172 countries have enacted their own data privacy laws.[1] The majority of those laws have a clear influence from the GDPR.[2] Many explanations have been offered to describe this worldwide phenomenon, including the market power of the European Union (EU),[3] regulatory convergence,[4] international policy diffusion,[5] and soft legal globalization.[6] One of the most notable explanations is that provided by Anu Bradford through the so-called Brussels Effect, which elucidates the essence of the EU single market and its regulatory power.[7]

Although most companies are not based in the EU, especially the tech companies,[8] they tend to adhere to the GDPR standards. This is not only because it is explicitly required by the extraterritorial application of the GDPR, but also because of the sizable digital market of the EU. A

* Melinee Kositwatanarerk, Researcher, Erasmus Center of Law and Digitalization, Erasmus School of Law, Erasmus University Rotterdam, Rotterdam, The Netherlands; Office of the President of the Supreme Court of Thailand, Court of Justice of Thailand, Bangkok, Thailand. Tel: +31 10 408 2691; Email: kositwatanarerk@law.eur.nl

† Klaus Heine, Jean Monnet Chair of Economic Analysis of European Integration, Erasmus Center of Law and Digitalization, Erasmus School of Law, Erasmus University Rotterdam, Rotterdam, The Netherlands. Tel: +31 10 408 2691; Email: heine@law.eur.nl

1 Graham Greenleaf, 'Global Data Privacy Laws 2025: 172 Countries, Twelve New in 2023/24' (2 April 2025) SSRN <https://ssrn.com/abstract=5275559> accessed 8 March 2026.

2 Graham Greenleaf, 'Now 157 Countries: 12 Data Privacy Laws in 2021/22' (2022) 176 Privacy Laws & Business International Report <https://www.privacylaws.com/reports-gateway/articles/int176/int176newdplaws/> accessed 5 March 2024.

3 EU data protection rules apply to the EU and European Economic Area (EEA) countries. In this article, the EU refers to all EU Member States and Iceland, Liechtenstein, and Norway, unless explicitly stated otherwise.

4 Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press 1992).

5 Gregory P Corning, 'The Diffusion of Data Privacy Laws in Southeast Asia: Learning and the Extraterritorial Reach of the EU's GDPR' (2024) 30 Contemporary Politics 656.

6 Michael D Birnhack, 'The EU Data Protection Directive: An Engine of a Global Regime' (2008) 24 Computer Law & Security Review 508.

7 Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (OUP 2023).

8 Wayne Duggan, 'The 10 Biggest Tech Companies in the World' *US News & World Report* (14 October 2025) <https://money.usnews.com/investing/articles/most-valuable-tech-companies-in-the-world> accessed 10 November 2025.

2023 statistical report shows that the EU has a population of approximately 584 million, with 92 per cent of its total population being internet users.[9] To gain access to the EU single market, companies are required to comply with EU standards.[10] This is due to the EU's considerable market power. In case of non-compliance, the EU imposes sanctions on the infringing companies. Apart from that, companies also have an incentive to adopt the GDPR standards as their uniform global data protection policy, because complying with the GDPR automatically fulfills the lower requirements of other data protection laws that are not as strict.[11]

The Brussels Effect has sought to explain the impact of the GDPR by emphasizing its far-reaching implications worldwide. Distinctively, path dependence and network effects offer additional perspectives on the explanation of the GDPR's dominance. Rather than focusing on its effects, path dependence allows exploration of the antecedents in the past that shape the present and future of the EU data protection regime. In this contribution, it is most productive to concentrate on network effects as triggers of path dependence and to conceive the rules of the GDPR as self-reinforcing in the international arena. Admittedly, path dependence is a broad concept, encompassing, on the micro-level, psychological reinforcement processes such as escalating commitment,[12] on the meso-level, learning effects such as co-evolution in technological components,[13] and, on the macro-level, the historical development of the whole society.[14] A striking implication of path dependence is that the stronger a chosen path is, the more challenging it becomes to deviate from it,[15] which then creates a lock-in stage.[16] In this article, a more tailored analysis is provided on why the GDPR became a global standard for data protection.

The article does not focus on a normative argument. Rather, the article provides a positive explanation of the antecedent conditions at the time of its introduction and the subsequent chain of events leading to its dominance. This does not rule out the possibility that the GDPR is a data protection regime most people may prefer, but this normative point of view is not the focus of the research. In other words, this article makes two contributions: First, it explains why the GDPR has become the dominant global data protection law. Secondly, it argues that alternative legal rules for data protection may emerge over time. However, the GDPR remains predominant and does not deviate from its current path.

In March 2012, the EU Data Protection Supervisor stated in an opinion on the data protection reform package that the reform of EU data protection law 'opens a window of great opportunities to reinforce the legal frameworks in the EU and achieve more global privacy at the same time'.[17] This opinion was reinforced when, in October 2017, the European Parliament set out its vision to 'export EU data privacy standards'.[18] This hinges on the development of EU data protection law from a regional to a global instrument. To this end, the GDPR employs four main legal mechanisms resulting in an expansion of its networks: the adequacy decision[19]; the standard contractual clauses (SCCs)[20]; binding corporate rules (BCRs)[21]; and the extraterritorial provision.[22]

The article commences with an overview of the concept of path dependence, which builds the main theory to describe the GDPR's dominant position. It provides a clear explanation of how European data protection law established a dominant legal path.[23] In the second part, the analysis focuses on three phases: (i) the stage preceding the imposition of the Data Protection Directive

9 Sara Lone, Jesse Weltevreden and Aishwarya Luharuwala, 'European E-Commerce Report 2023' *EuroCommerce Retail & Wholesale* 5 <https://www.eurocommerce.eu/app/uploads/2023/11/2023-european-e-commerce-report-light-version-nov-update-v2.pdf> accessed 20 July 2024.

10 Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2020).

11 ibid 142; See also Michael Dan Birnhack and Guy Mundlak, 'The Brussels Effect(s) and the Rise of a Privacy Profession' (2025) 15 International Data Privacy Law 138.

12 Barry M Staw, 'Knee-deep in the Big Muddy: A Study of Escalating Commitment to a Chosen Course of Action' (1976) 16 Organizational Behavior and Human Performance 27.

13 Giovanni Dosi, 'Technological Paradigms and Technological Trajectories: A Suggested Interpretation of the Determinants and Directions of Technical Change' (1982) 11 Research Policy 147.

14 Douglas C North, *Institutions, Institutional Change and Economic Performance* (CUP 1990).

15 Jörg Sydow, Georg Schreyögg and Jochen Koch, 'On the Theory of Organizational Path Dependence: Clarifications, Replies to Objections, and Extensions' (2020) 45 Academy of Management Review 717, 728.

16 Paul A David, 'Clio and the Economics of QWERTY' (1985) 75 American Economic Review 332; W Brian Arthur, 'Competing Technologies, Increasing Returns, and Lock-In by Historical Events' (1989) 99 Economic Journal 116; North (n 14); For a legal application see Klaus Heine and Wolfgang Kerber, 'European Corporate Laws, Regulatory Competition and Path Dependence' (2002) 13 European Journal of Law and Economics 47.

17 European Data Protection Supervisor, 'Opinion on the "Data Protection Reform Package"' (2012) 3.

18 'Future of Europe: European Parliament Sets Out Its Vision' (European Parliament, October 2017) <https://www.europarl.europa.eu/resources/library/media/20171023RES86651/20171023RES86651.pdf> accessed 30 May 2024; see Bradford (n 10) 18.

19 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), OJ 2016 L 119/1, art 45.

20 General Data Protection Regulation, art 46(2)(c)(d); Standard Contractual Clauses (SCC), European Commission, <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en> accessed 9 May 2024.

21 General Data Protection Regulation, art 47.

22 ibid art 3.

23 Jörg Sydow, Georg Schreyögg and Jochen Koch, 'Organizational Path Dependence: Opening the Black Box' (2009) 34 Academy of Management Review 689, 699.

(DPD) (preformation phase), (ii) the stage during which the DPD was in force (formation phase), and (iii) the stage following the introduction of the GDPR (lock-in phase). This is a stylized model, and in reality, the three phases may overlap. However, this distinction is useful for gaining a theoretical understanding of the GDPR's legal development and for qualifying the finding that most countries in the world follow the GDPR's data protection regime. Finally, four main legal mechanisms of the GDPR are discussed with an explanation of how these mechanisms create the network effects of the GDPR.

Path dependence and network effects

The concept of path dependence is used to explain practices of today that are the result of yesterday's historical choices.[24] The conditions of the past may have changed, but the initial choices still affect current actions. Once a decision has been made for a particular solution, it triggers repercussions and initiates self-reinforcement. The path is then created. However, the historical choice made in the initial can be either intentional or random, and either strategic or the result of a minor event. The key point to emphasize is that the historical choice becomes 'decisive in determining the final outcome'.[25]

This observation of path dependence is applicable to all contexts, decisions, and practices. Law is not an exception, and there are several reasons and factors why a legal path remains unchanged over time. These factors have been comprehensively discussed in the legal literature, including the literature addressing the emergence and evolution of common law,[26] the preeminence of Delaware corporate law,[27] and copyright law.[28] When legal path dependence is significant, states lack an incentive to contribute to the development of the law or to offer an alternative. The switching costs are so constraining that the legal lock-in remains over time. Delaware corporate law serves as an example.[29] Network effects play a dominant role in the establishment and endurance of Delaware corporate law through the training of lawyers in Delaware corporate law, specialized corporate law courts in Delaware, and incorporation in Delaware without a production site there. Although many argue that it does not provide welfare-maximizing rules, network effects have created a lock-in to Delaware law, making switching costs to another corporate law relatively high.[30]

However, it is not always necessary that the initially chosen path becomes inefficient or inferior through the lock-in compared to other options. Liebowitz and Margolis identify, for example, a sort of path dependence with no effect on efficiency.[31] An optimal path may simply persist because switching between paths would be prohibitively costly. An example of this is the driving side in a country, which may be on the left or right. This purely solves a coordination problem without any effect on efficiency. Therefore, lock-in does not necessarily mean it is inferior to other alternatives.

The phenomenon of path dependence can be explained by several self-reinforcing mechanisms that trigger individually or collectively a legal path. With regard to the GDPR, network effects play a key role in explaining the self-reinforcement of the GDPR. A well-known example of path dependence through network effects can be found in the establishment of the QWERTY keyboard. The example illustrates how the decision-making of different actors in a network lets a path emerge.

The typewriter was invented in the nineteenth century, and initially, there were various layouts available. To avoid the jamming of typewriter keys when typing speed reaches a certain level, the Remington typewriter company designed the QWERTY keyboard to limit the maximum typing speed.[32] The QWERTY keyboard became very popular among secretaries and writing bureaus, despite the existence of other keyboard options. Subsequently, as typewriter mechanics advanced and key jamming became less of an issue, the QWERTY keyboard remained dominant. This was despite the existence of alternative keyboards, such as the DVORAK keyboard, which led to a lock-in stage of the network.[33] Everyone was trained and got used to the order of the QWERTY, which made it difficult to switch to any other type of keyboard. There were several attempts to introduce a new order of the keyboard in order to increase typing speed and ergonomics. But these attempts were unsuccessful, since neither professional typist was willing to do an extensive training on a new keyboard, nor were writing

24 See David (n 16).

25 Sydow, Schreyögg and Koch (n 23) 693.

26 Oona A Hathaway, 'Path Dependence in the Law: The Course and Pattern of Legal Change in a Common Law System' (2001) 86 Iowa Law Review 601; see also Clayton P Gillette, 'Lock-In Effects in Law and Norms' (1998) 78 Boston University Law Review 813.

27 Heine and Kerber (n 16).

28 Stefan Larsson, 'The Path Dependence of European Copyright' (2011) 8 SCRIPTed 8.

29 See Michael Klausner and Marcel Kahan, 'Path Dependence in Corporate Contracting: Increasing Returns, Herd Behavior and Cognitive Biases' (1996) 74 Washington University Law Quarterly 347.

30 Michael Klausner, 'Corporations, Corporate Law, and Networks of Contracts' (1995) 81 Virginia Law Review 757.

31 Stan J Liebowitz and Stephen E Margolis, 'Path Dependence, Lock-In, and History' (1995) 11 Journal of Law, Economics, and Organization 205, 207.

32 See David (n 16).

33 Liebowitz and Margolis (n 31) 213.

bureaus and companies willing to invest in new typewriter equipment. Even today, the virtual keyboards on smartphones and tablets still use the QWERTY keyboard, thereby reinforcing a 150-year-old standard.

A network can be either physical, like an electricity grid, or virtual, like, for example, professional typists using the QWERTY keyboard. Network effects occur when participation in a network influences the behavior of others.[34] As the number of participants in a network increases, it attracts a greater number of newcomers to join and benefit the members of the network using the same technology or standard.[35] Being a member of the network becomes cheaper when its size grows, as network effects create mutual advantages from which all users benefit alike.[36] The network effects can be either direct or indirect.

Examples of digital technologies with a direct network effect include mobile phone networks, social media networks, and messaging applications. The presence of a greater number of users within the same social media network, or messaging application, influences the decision of existing users to remain within the network, as well as attracting other users to join. As the number of users grows, the network becomes increasingly robust. For instance, if the majority of people use WhatsApp, it influences the remaining people to also join the platform. Those relocating to Europe are quasi-forced to join WhatsApp to communicate with colleagues and friends. When returning to their home countries, such as China, the Republic of Korea, or Japan, they would use the dominant network in those regions, including WeChat, KakaoTalk, or LINE. It is always challenging for a new network to compete with an established one. It is unlikely that any individual user would switch to the new network, unless there was a collective and simultaneous move by their acquaintances.[37] The direct network effect implies coordination, where the shift of only a minority of users to an alternative network excludes the benefits of the existing network.[38]

The second category of network effects is that of indirect externality. In this scenario, the network benefit is not directly correlated with the number of participants in one group of users. Instead, the number of users on one side yields greater value to another group of users. The indirect network effects may take the form of a service, a side product, or an after-sales service, which becomes more accessible and affordable due to network expansion.[39] For example, customers opt for Apple or Android smartphones because the associated application platforms offer a wide variety of regularly updated applications. The Microsoft smartphone ultimately failed because it could not attract enough application developers, making it an unattractive alternative for customers, although its operating system was at least as good as those of Apple or Google.

In the case of the GDPR, the direct network effect grows with the number of third countries, controllers, and processors that adhere to the GDPR standards. Meanwhile, the indirect network effect emerges when data protection lawyers and other legal professionals become more skilled and specialized in the GDPR. Therefore, GDPR legal services are widely available and easily accessible to members of GDPR networks. Controllers and processors can easily seek advice on the GDPR rather than on the more niche local data protection law of a third jurisdiction. These direct and indirect network effects create path dependence for the GDPR.

The EU data protection path

It is useful to distinguish between three phases of a path-dependent process: The preformation phase, the formation phase, and the lock-in phase.[40] The distinction among the three phases helps elucidate the legal evolution of the GDPR in general and the decision-making of the lawmaker at each stage in particular.

In the preformation stage, actions are still scattered, and there is independence and flexibility to choose between various options. However, once a decision has been made for a particular solution, it triggers repercussions and initiates self-reinforcement. The path is initially created, leading to the formation phase. During this formation phase, past events influence the selection, and a specific regime becomes dominant over others. The reinforcement of the leading regime turns into a repetitive pattern. The historical choice becomes 'decisive in determining the final outcome'.[41] However, minor deviations from the main route remain common. It is a transition period when some configurations become more influential than others, but they have not yet achieved monopolistic dominance. Consequently, the formation phase leads to a lock-in, where one pattern becomes dominant and deviating from the established path becomes nearly impossible. Thus, the third phase shuts down the possibility of choosing among multiple options available.

34 Stan J Liebowitz and Stephen E Margolis, 'Network Externality: An Uncommon Tragedy' (1994) 8 Journal of Economic Perspectives 133.
35 Gillette (n 26) 818.
36 Klausner and Kahan (n 29) 352.
37 ibid
38 ibid
39 Liebowitz and Margolis (n 34) 135.
40 See Sydow, Schreyögg and Koch (n 15) 718–719.
41 Sydow, Schreyögg and Koch (n 23) 693.

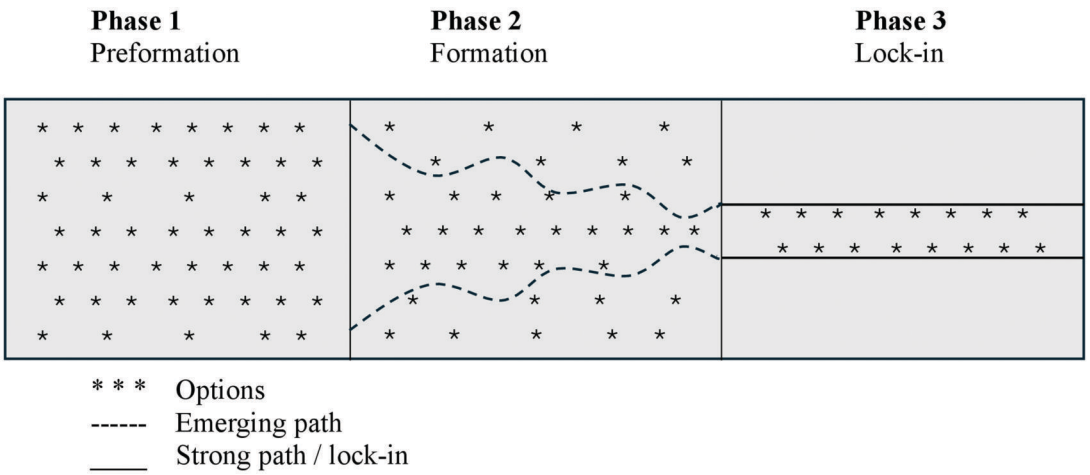

Figure 1. The emergence of a path-dependent pattern. This diagram is adapted from Sydow and others, Organizational Path Dependence: Opening the Black Box (2009) 34 Academy of Management Review 689.

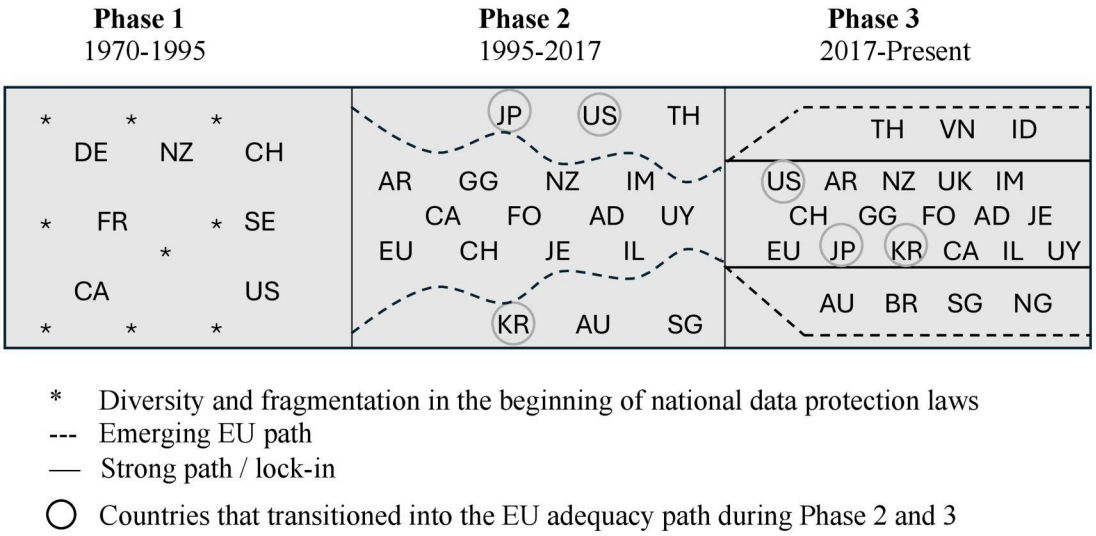

Figure 2. Timeline of data protection path integrated into the EU baseline.

Figure 1 illustrates the three phases. The dotted line in Phase 2 demonstrates some fluctuation of the primary trend, which undergoes a process of formation. Upon transition to Phase 3, the trajectory becomes more eminent and finally petrifies into a clear straight line. This model can be transferred to law and to the emergence of the GDPR as the dominant data protection standard.

Figure 2 depicts the network growth of the EU data protection law path in relation to third countries joining the adequacy decision network, and third countries having their data protection law influenced by the GDPR. To illustrate the impact of the GDPR on global data protection trends, the examples of third countries joining the GDPR path are used to demonstrate self-reinforcement of network effects and GDPR path dependence. The countries illustrated in Fig. 2 are merely for illustrative purposes and do not represent a conclusive list.

Phase 1 represents the pattern of data protection laws, when there was no legal harmonization, and countries pursued their own independent data protection policies. At this stage, some countries may not yet have enacted a data protection law (these are marked with an asterisk). When transitioning to Phase 2, the EU introduced a regional instrument, the DPD 95/46/EC. This has led to the establishment of a distinct pattern of EU data protection law, prompting third countries to join the EU path. Countries situated between the dashed line of Phase 2 and the straight line of Phase 3 have already been granted the

adequacy decisions.[42] Third countries placed next to the main line are also on the GDPR path, with their laws influenced by the GDPR, but not yet achieving adequacy status. Clearly, an increasing number of countries are entering the EU data protection network in Phase 3, thereby establishing the GDPR as the dominant global standard.

The preformation phase

In the early days of the first phase of the data protection regime, the introduction of data protection laws in several countries was initiated by the Organization for Economic Co-operation and Development (OECD), beginning with its Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data in 1980 (OECD Guidelines).[43] The OECD Guidelines recommend that member countries develop national privacy strategies and enact privacy laws.[44] This can be regarded as an early attempt to coordinate data protection regimes on an international level.

In 1981, the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). This was a significant development as it was the first legally binding international instrument for data protection,[45] although it took many years to come into force. It also provided a significant link between data protection and the right to privacy.[46] Both the OECD Guidelines and Convention 108 highlighted the transborder data flow[47] and exerted a clear influence on the development of national data protection regulations.[48]

However, there was no harmonized European data protection law in this first phase. There was a great diversity of laws and regulations on the national level. For example, the German Land of Hessen was recognized in 1970 as the first in the EU to introduce personal data protection.[49] Between 1973 and 1978, Sweden (SE), Germany (DE), and France (FR) enacted national data protection laws consecutively.[50] Consequently, in the 1980s, a growing number of countries introduced national data protection laws in response to the adoption of the OECD Guidelines[51] and the Convention 108, such as the UK (1984) and Finland (1987).[52]

The USA enacted the Federal Privacy Act in 1974, which was designed to prohibit and regulate the disclosure of personal information by federal agencies.[53] Canada (CA) established its first public sector privacy protection in 1977 as part of the Canadian Human Rights Act. This was followed by the development of specific legislation of the Privacy Act and the Access to Information Act in 1983.[54] While the OECD Guidelines covered both the public and private sectors, the USA and Canada initially only imposed laws on the actions of governments. Switzerland (CH) and New Zealand (NZ), both distant from the legislation of the EU and North America, also experienced a push of their data protection through the OECD Guidelines and enacted their privacy laws in 1992 and 1993.[55]

In Phase 1, there was fragmentation between data protection laws among countries. Some covered only government activities, while others covered both private and public sectors. Obviously, it was the early stage of privacy protection. Even among EU Member States, national laws remained diverse, with some members not having their own legislation on the issue. Therefore, there is an absence of a clearly defined pattern in data protection law. The OECD Guidelines and the Convention 108 provided some directions, but the overall trend was unclear at that time.

The formation phase

In 1995, the Data Protection Directive 95/46/EC (DPD) was introduced as the first EU data protection instrument. Even though the DPD did not fully harmonize the

42 Andorra (AD), Argentina (AR), Canada (CA), Faroe Islands (FO), Guernsey (GG), Israel (IL), Isle of Man (IM), Japan (JP), Jersey (JE), New Zealand (NZ), the Republic of Korea (KR), Switzerland (CH), the United Kingdom (UK), the United States (US), and Uruguay (UY).

43 Organisation for Economic Co-operation and Development (OECD), 'Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' OECD/LEGAL/0188 (23 September 1980) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188> accessed 20 January 2026.

44 ibid.

45 'Background to Convention 108' (*Council of Europe*) <https://www.coe.int/en/web/data-protection/1108/background> accessed 10 January 2026.

46 Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer International Publishing 2014) 89.

47 Birnhack (n 6) 511.

48 'Background to Convention 108' (*Council of Europe*) <https://www.coe.int/en/web/data-protection/convention108/background> accessed 10 January 2026; See also Fuster (n 46) 92.

49 Hendrik Mildebrath, 'Understanding EU data protection policy' (*European Parliament*, January 2025) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf> accessed 1 November 2025, 2.

50 ibid.

51 ibid.

52 Fuster (n 46) 92.

53 'The Evolution of Privacy: A Look at the Past, Present, and Future' (*Connecticut General Assembly*) <https://www.cga.ct.gov/PS98/rpt%5Colr%5Chtm/98-R-1455.htm#:~:text=The%20Federal%20Privacy%20Act%20of,personally%20identifying%20number%20or%20symbol> accessed 30 November 2024.

54 'Research publications – Canada's Federal Privacy Laws' (*Library of Parliament*, 1 October 2013) <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/200744E#a2> accessed 30 November 2024.

55 Paul Roth and Blair Stewart, *Privacy and Data Protection Law in New Zealand* (Kluwer Law International BV 2022), 46.

national data protection laws of the EU Member States, it attracted significant attention and exerted considerable influence on global data protection. Particularly, the set of rules limiting data transfers outside the EU, as outlined in Article 25 of the DPD regarding the adequacy decision, prompted jurisdictions outside the EU to revise their laws and align with the DPD standards.[56]

Switzerland was the first country to achieve the adequacy standards in 2000,[57] with Canada following closely in 2001.[58] New Zealand experienced several attempts to amend its Privacy Act 1993 and succeeded in its 2010 amendment, leading to the adequacy decision in 2012.[59] The Privacy (Cross-Border Information) Amendment Act 2010 was aimed at providing sufficient standards to address EU concerns about cross-border data transfers.[60]

Since 2000, following the adoption of the DPD in 1995, the EU and the USA made several attempts to establish a framework based on the adequacy requirement set out in the DPD. The initial endeavor was the inception of the Safe Harbour Privacy Principles.[61] Any company in the USA that committed itself to comply with the principles would be permitted to transfer data to the EU and was assumed to meet the EU standards. However, in October 2015, the CJEU ruled in *Schrems I*[62] that the Safe Harbour agreement was invalid.[63] For reasons of national security, the US authorities were allowed to access foreign intelligence data without a warrant,[64] which was considered a risk to the protection of personal data transfers from the EU to the USA. Consequently, another initiative, the EU–US Privacy Shield, was launched in 2016 between the USA and the EU.[65] It was aimed at addressing deficiencies of the previous Safe Harbour agreement. The US authorities agreed to refrain from surveillance and access to the personal data of EU citizens.[66] However, the new attempt was still not deemed satisfactory by the CJEU and was again held to be invalid in *Schrems II*.[67] The two attempts to agree on the adequacy standards allowing the free flow of data from the listed companies in the USA to the EU demonstrated the significant efforts by the USA to adjust and join the EU adequacy network.

Japan (JP) is a good example of efforts to implement appropriate measures to facilitate active information exchange with the EU.[68] In 2014, Japan issued the Policy Outline of the Institutional Revision for Utilization of Personal Data, which explicitly affirmed the objective of achieving international harmonization and cross-border data transfer between Japan and third countries.[69] This was presumed to be the fulfillment of aligning its policy with the EU.[70] Nevertheless, during Phase 2, Japan was unable to obtain an adequacy decision.

Furthermore, from 1995 to 2018, a number of newcomers entered the data protection path. Jurisdictions such as the Republic of Korea (KR) and Singapore (SG) enacted their original data protection laws around 2011 and 2012, respectively. For Thailand (TH), the Freedom of Official Information Act was implemented in 1997, encompassing the activities of government and public agencies.[71]

Despite the 11 countries that have already received adequacy decisions, a number of other countries have expressed an interest in achieving EU standards, including Japan, Chile, Colombia, Australia, Mexico, and Turkey.[72] The laws of third countries, such as China, Dubai, India, the Philippines, and Singapore, are also influenced by the EU standards.[73] Greenleaf has identified ten unique elements of EU standards that are

56 See also Birnhack (n 6).

57 Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland [2000] OJ L 215 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0518>.

58 Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act [2002] OJ L2/13.

59 Roth and Stewart (n 55) 27.

60 Roth and Stewart (n 55) 51.

61 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7 <https://eur-lex.europa.eu/eli/dec/2000/520/oj/eng>.

62 Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.

63 Court of Justice of the European Union, 'The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid' Press Release No 117/15 (6 October 2015).

64 Peter Margulies, 'Defining Foreign Affairs in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on US Surveillance Policy' (2015) 72 Washington and Lee Law Review 1283.

65 European Commission, 'EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield' Press Release (2 February 2016) <https://ec.europa.eu/commission/presscorner/detail/en/ip_16_216> accessed 12 January 2025.

66 ibid.

67 Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems [2020] ECLI:EU:C:2020:559, para 186.

68 Yuko Suda, 'Japan's Personal Information Protection Policy Under Pressure' (2020) 60 Asian Survey 510, 517.

69 'Policy Outline of the Institutional Revision for Utilization of Personal Data' (*Prime Minister's Office of Japan*, 24 June 2014) <https://japan.kantei.go.jp/policy/it/20140715_2.pdf> accessed 20 October 2024, 8–9.

70 Suda (n 68) 517.

71 See 'Responses to the Questionnaire on the Right of Access to Information in the Field of Hazardous Substances and Wastes' (*Office of the High Commissioner for Human Rights*) <https://www.ohchr.org/sites/default/files/Documents/Issues/ToxicWaste/RightToInformation/Thailand.pdf> accessed 20 October 2024.

72 Birnhack (n 6) 516.

73 ibid.

considered higher or stricter standards, as they are not present in other data protection instruments, specifically the OECD Guidelines and the Privacy Framework introduced by the Asia-Pacific Economic Cooperation (APEC Framework) in 2004.[74] Thirty-three laws from third countries outside the EU were found to be influenced by EU standards to varying degrees.

During this formation phase, there were some other available alternatives to the DPD, such as the Convention 108 and the APEC Framework.[75] Even though APEC economies span four continents, they lack mechanisms to create network effects, as there are no implementation requirements or regulations for data export.[76] The framework, therefore, proved unsuccessful in generating impact and was subject to criticism.[77] This obviously emphasizes that the growth of the DPD network was significantly driven by limitations on data transfer through mechanisms such as adequacy decisions. The DPD developed the main trend and became predominant over the others.[78]

In Fig. 2, third countries that are more integrated with the EU through adequacy decisions are positioned between the lines. Countries that have initiated their data protection laws, but have not yet achieved the adequacy standards, are placed adjacent to the line representing the emerging EU path. Interestingly, there are currently fifteen countries pertaining to the EU adequacy decisions, with eleven of them adopted during Phase 2. This suggests that the trajectory of EU data protection law began to impact the global trend even before the GDPR's implementation in 2018.

The lock-in phase

The path of the GDPR became increasingly dominant with the attraction of third countries. Even those countries placed outside the main dashed line were heavily influenced by the GDPR. As of 2017, the European Commission negotiated with key trading partners in East and Southeast Asia an alignment of their data protection regimes with the GDPR, commencing with Japan and the Republic of Korea.[79]

The Republic of Korea is an example of a country that initially diverged from the EU standard but later converged with the GDPR framework. At the outset of the EU–Republic of Korea discussions, a key challenge emerged regarding the absence of an independent supervisory authority in the Republic of Korea, which led to the suspension of the adequacy discussion.[80] It took until 2022 for the Republic of Korea to adapt its data privacy regulation, leading to the European Commission's adequacy decision.[81]

For Japan, discussions concerning the adequacy standard commenced in 2017, before Japan achieved adequacy status in 2019. Japan has introduced a number of substantial amendments, including the establishment of an independent authority, the Personal Information Protection Commission.[82] This reflects a strong degree of convergence with the EU standard. To achieve agreement on the mutual and smooth transfer of data between Japan and the EU, several amendments to the Japanese Act on the Protection of Personal Information (APPI) were required to ensure compliance with the GDPR standards. The amendments included information on sexual orientation, trade union membership, the guarantee of the right of data subjects to access their data, and the adoption of anonymization standards.[83] Finally, in a letter dated 14 September 2018, the Japanese Minister of Justice affirmed that 'government access to personal information transferred from the EU to Japan will be limited to what is necessary and proportionate'.[84] However, Yuko Suda observes that 'policy adjustment for the mutual adequacy findings seems to be rather one-sided', with most of the data protection issues resolved due to unilateral adjustments of Japanese law.[85]

Recently, in 2023, the European Commission and the USA reached an agreement on the new Data Privacy

74 Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108' (2012) 2 International Data Privacy Law 68, 74.

75 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2004/AMM/014rev1, 29 October 2004) <https://www.apec.org/docs/default-source/press/newsrelease/2004/04_amm_014rev1.pdf>.

76 Graham Greenleaf, *Asia-Pacific Developments in Information Privacy Law and its Interpretation* (UNSW Law Research Paper No 2007-5, 2012) 8.

77 ibid; See also Graham Greenleaf, 'APEC's Privacy Pathfinders – A Dead End for Consumers?' (2008) 91 Privacy Laws & Business International Report 12.

78 Greenleaf (n 74).

79 European Commission, 'Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World' COM (2017) 7 final (10 January 2017) <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0007> accessed 20 October 2024.

80 George Christou and Ji Soo Lee, 'EU–South Korea Cooperation on Cybersecurity, Data Protection and Emerging Technologies' in Gertjan Boulet, Michael Reiterer and Ramon Pacheco Pardo (eds), *Cybersecurity Policy in the EU and South Korea: From Consultation to Action – Theoretical and Comparative Perspectives* (Springer 2022) 41, 57.

81 Commission Implementing Decision (EU) 2022/254 of 17 December 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act [2022] OJ L44/1 <http://data.europa.eu/eli/dec_impl/2022/254/oj/eng> accessed 20 October 2024.

82 Suda (n 68) 516.

83 Suda (n 68) 520.

84 Letter from Yoko Kamikawa to Ms. Věra Jourová <https://www.ppc.go.jp/files/pdf/letter_government_access.pdf> accessed 30 November 2024.

85 Suda (n 68).

Framework, which implied the USA's adequacy status.[86] In contrast to other adequacy decisions, the free flow of data from the EU to the USA is constrained to companies participating in the EU–U.S. Data Privacy Framework, rather than being equally applied to all companies in the USA. The new framework takes steps to ensure the protection of personal data from the EU to participating companies in the USA. The collection and interference of personal data for national security purposes are restricted to what is necessary and proportionate.[87] The USA has established an independent redress mechanism to ensure the rights of data subjects. Complaints can be filed with the Civil Liberties Protection Officer of the US intelligence community or challenged at the Data Protection Review Court.[88] However, despite the European Commission's favourable assessment of the first-year review, it remains to be seen whether the CJEU would reach the same positive conclusion if the framework is challenged before it.[89]

In addition to countries fully aligned with the GDPR through the adequacy decision, many new countries are entering the GDPR path in Phase 3. They are considered part of the GDPR path dependence, and as such, they are positioned within the dashed line right next to the primary adequacy trend. Even though there is some strong influence of the GDPR towards their data protection laws, it should be noted that their integration with the GDPR is not as comprehensive as that observed in countries with the adequacy decision. For instance, Vietnam (VN), Brazil (BR), and Nigeria (NG) have all introduced their data protection legislation in 2023, thereby converging on the GDPR standard. Furthermore, Thailand (TH) and Indonesia (ID) have fully enforced their personal data protection laws in 2022. Prior to the implementation of the Personal Data Protection Act B.E. 2562, Thailand had only a law governing the handling of personal information by the government and state agencies.[90] For Indonesia, the Director General of the Ministry of Communications and Information stated that the Law on Personal Data Protection has a majority of its provisions in common with the GDPR, such as the rights of data subjects, the limitation of data transfer, and the notification of data breaches.[91]

As a prospective alternative to the GDPR, the Global Cross-Border Privacy Rules (Global CBPR) Forum was established in 2022.[92] While it has not yet become as prominent as the GDPR or a serious competitor, it does share some similarities with the GDPR in terms of facilitating free movement of data. Nevertheless, it is unlikely that the Global CBPR Forum will supersede the lock-in effect of the GDPR. For a country, data controllers and processors, it is costly to follow two data protection regimes simultaneously. To break the GDPR path, the Global CBPR Forum would need a significant advantage to justify the switching cost to its regime.

During the lock-in phase, the law of third countries is mostly influenced by the GDPR. The GDPR's predominant position within the global economy and the global data protection trend are underscored by the increasing number of countries aligning with the EU path. Obviously, sixteen of the top seventeen countries with the highest World Gross Domestic Product ranking in 2024 are either EU Member States, countries with adequacy decisions, or countries whose laws are influenced by EU standards.[93] Furthermore, data protection lawyers and legal professionals are already familiar with and specialized in the GDPR. It is difficult for countries, controllers, processors, or legal practitioners to switch to a new set of data protection laws when it is unknown whether it will become dominant in the future. Therefore, direct and indirect network effects obviously play a decisive role in the path dependence of GDPR.

The GDPR legal mechanisms and network effects

The introduction of the GDPR in 2018 has had a profound impact on the global data protection framework. Countries have aligned their laws with the GDPR requirements, and companies have adopted these

86 'Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows' (European Commission Press release, 10 July 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721> accessed 1 December 2024.

87 Giovanni Tricco, 'The New Transatlantic Data Agreement Placed in Context: Decoding the Schrems Saga within the Digital Economy' (2024) 3 Journal of Law, Market and Innovation 82, 106.

88 Bureau of Intelligence and Research, 'Executive Order 14086 – Policy and Procedures' (US Department of State, 3 July 2023) <https://www.state.gov/executive-order-14086-policy-and-procedures> accessed 12 December 2024.

89 Tricco (n 87) 109.

90 Official Information Act B.E. 2540 (1997) (Thailand).

91 See also Corning (n 5).

92 'Global Cross-Border Privacy Rules Declaration' (*US Department of Commerce*) <https://www.commerce.gov/global-cross-border-privacy-rules-declaration> accessed 5 March 2025.

93 United States, China, Germany, Japan, India, United Kingdom, France, Italy, Canada, Brazil, Republic of Korea, Mexico, Australia, Spain, Indonesia, Turkey; See 'GDP Ranking' (*World Bank Group*, 15 December 2025) <https://datacatalog.worldbank.org/search/dataset/0038130/gdp-ranking> accessed 20 January 2026; Graham Greenleaf, 'Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance' (2021) 169 Privacy Laws & Business International Report 1, 3–5; UNSW Law Research Paper No 21-60; Birnhack (n 6) 516.

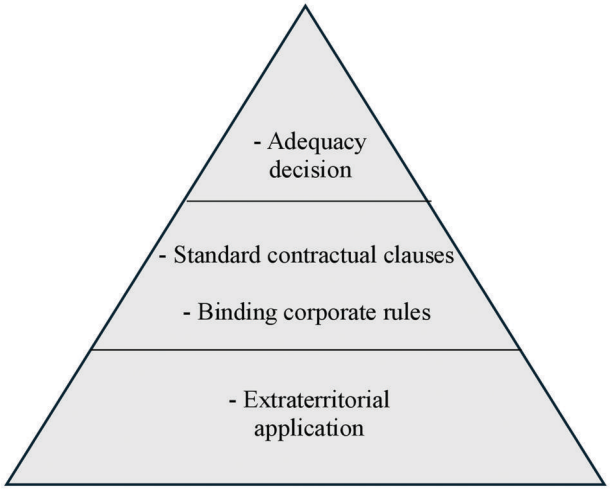

Figure 3. Triangle of the GDPR mechanisms contributing to the network effects.

standards as their data protection policies, not only for doing business in the EU but worldwide.

This section examines further the legal mechanisms under the GDPR that have created network effects and formed the GDPR's path dependence. The four principal mechanisms—the adequacy decision, the SCCs, the BCRs, and the extraterritorial application—are selected because they involve an expansion of the GDPR networks beyond the EU border. These mechanisms allow third countries, data controllers, or processors in third countries to adopt and comply with the GDPR standards, even though they are not located within the EU. The network effects of the GDPR involve all relevant players, including states, companies, and individuals acting as controllers or processors, as they all contribute to explaining how the GDPR shapes the global data protection trend at every level.

The triangle in Fig. 3 depicts the four mechanisms. The apex of the pyramid represents the highest degree of integration with the GDPR. Only a limited number of third countries can attain this level of compliance and become members of the GDPR network at the highest tier. The SCCs and the BCRs are placed at the second rank of the pyramid, indicating a lesser level of integration. In countries without an adequacy decision, parties may opt for incorporation under SCCs or BCRs to facilitate cross-border transfers. Lastly, the extraterritorial application forms the base of the triangle representing the broadest and overarching application of the GDPR. The EU applies this measure to all countries without requiring any consent. The four mechanisms motivate third countries and overseas parties to comply with the GDPR in either way. If their countries are not under an adequacy decision, they may choose to adopt SCCs or BCRs. Even in the absence of the first three, they may still be subject to the extensive GDPR's extraterritorial application. Consequently, powerful network effects unfold, reinforcing the dominance of the GDPR.

Adequacy decision

The most evident mechanism through which the EU has reinforced the GDPR network is the legal concept of an adequate level of protection. Article 45 of the GDPR sets out conditions for the transfer of personal data from the EU to third countries. The transfer is permitted without any limitation if a third country is deemed by the European Commission to have an adequate level of protection in accordance with the GDPR, and has obtained an adequacy decision from the European Commission.[94] The possibility of unlimited data sharing is a key motivator for states to adopt the GDPR standards into their own data protection laws.

In June 2024, the first international high-level meeting about safe data flows took place.[95] The meeting was joined by Didier Reynders, the EU Commissioner for Justice, Věra Jourová, the Vice-President of the EU Commission and Commissioner for Values and Transparency (until November 2024), Anu Talus, the Chair of the European Data Protection Board (EDPB), and ministers and heads of data protection authorities from fifteen adequacy countries. Jourová emphasized the significance of collaboration and network effects in data protection law.

> In digital era where the innovation is often powered by personal data, we are facing similar challenges across the globe, this is why it would be mutually beneficial to work towards a network effect and common understanding of the challenges.[96]

Similarly, Reynders' remarks underscore the importance and necessity of adequacy networks.

> We form, together with fifteen other countries, the world's broadest networks for safe and free data flows. With the development of Artificial Intelligence and global challenges

94 General Data Protection Regulation, art 45.

95 'Daily News 04/03/2024' *European Commission* (Brussels, 4 March 2024) <https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307#11> accessed 5 March 2025.

96 ibid.

> arising from new technologies, our cooperation to promoting the responsible use of data and trusted data flows is more important than ever. I look forward to discussing these opportunities in the first ever international summit between like-minded partners on privacy.[97]

The two statements not only mention the general idea of networks, but also that countries with adequacy decisions are emphasized as partners from whom it is expected to follow the EU path of data protection. The total of 15 countries with an adequacy decision is a diverse group with a strong local or commercial affiliation with the EU. Countries are attracted by the EU market access and the free flow of data. At the same time, an adequacy decision also serves to guarantee that these countries adhere to rigorous data protection standards in the context of global business. It successfully encourages countries to revise and enact their laws to reach the GDPR standard. The concept of the adequacy decision has existed since the precursor of the GDPR, the DPD. Therefore, several countries, including New Zealand, Canada, and Argentina, have long been recognized as having an adequate level of protection under the DPD. In contrast, some countries, such as Japan, the Republic of Korea, and the USA, have only recently been granted the adequacy decisions under Article 45 of the GDPR. To ensure the legacy and compatibility of the data protection regime over time, the European Commission is required by the GDPR to review the adequacy decision every 4 years.[98]

The adequacy decision ensures that 15 countries with their data protection regimes are regarded as equivalent to the GDPR, allowing free data flows between the EU and those countries. Furthermore, Chander and Schwartz's paper notes that more than 60 countries outside the EU have adopted an approach similar to the EU adequacy decision, limiting cross-border data transfers from their country to others with equivalent protection standards.[99] Third countries are trying to align their laws with the GDPR to attain the adequacy status. At the same time, they are adopting a similar adequacy approach to data transfers from their countries. If a significant number of countries adhere to the GDPR, it becomes a *de facto* global standard, allowing countries to transfer data freely even among themselves. Consequently, the network effects of the GDPR are reinforced.

Standard contractual clauses

The SCCs have been in place since the DPD. In June 2021, the European Commission adopted the new SCCs, replacing the previous SCCs under the DPD. The SCCs address the relationship between data controllers and processors on the one hand, and the transfer of personal data from the EU to third countries on the other.[100] The SCCs for data transfers to countries outside the EU have a significant impact on the dominance of the GDPR through network effects. The incorporation of SCCs ensures that controllers and processors in third countries comply with the GDPR as a unified data protection standard (direct network effect). Meanwhile, it attracts legal services from outside the EU to be trained in the application and interpretation of the GDPR, enabling them to provide legal advice on the SCCs and the cross-border data transfers (indirect network effect).

The SCCs are a set of legal clauses to be included in the main agreement when parties from the EU wish to transfer personal data to any third country that has not yet met the GDPR adequacy standard.[101] More precisely, companies or individuals in third countries can voluntarily commit themselves under the SCCs to manage data in accordance with the GDPR standard. The clauses function as a template to be incorporated into an agreement, in which parties cannot amend the template except to add a higher level of data protection.[102] The purpose of the SCCs is to guarantee that data flows from the EU receive the high level of protection set out in the GDPR.[103]

Interestingly, the template of the SCCs even requires parties to agree to be subject to the jurisdiction of EU data protection authorities and courts.[104] As third-party beneficiaries, data subjects whose rights are infringed may lodge a complaint with the data protection authority or the responsible court of the EU country.[105] Furthermore, parties are required to conduct a transfer impact assessment regarding the law of the country of destination and the protection of the personal data transferred.[106]

While the clauses appear to be non-obligatory, controllers or processors based in third countries without an

97 ibid.

98 General Date Protection Regulation, art 97

99 See Anupam Chander and Paul M Schwartz, 'Privacy and/or Trade' (2023) 90 University of Chicago Law Review 50.

100 'The New Standard Contractual Clauses – Questions and Answers Overview' (*European Commission*) <https://commission.europa.eu/document/download/b9d3d16b-9003-45e7-acef-409562b4bf8b_en?filename=questions_answers_on_sccs_en.pdf> accessed 28 November 2024, 4.

101 'Standard Contractual Clauses (SCC): Standard contractual clauses for data transfers between EU and non-EU countries' (*European Commission*) <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en> accessed 28 November 2024.

102 European Commission (n 100) 6.

103 European Commission (n 100) 4.

104 European Commission (n 100) 11.

105 European Commission (n 100) 17.

106 'International data transfers' *European Data Protection Board* <https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en> accessed 30 November 2024.

adequacy decision are indirectly compelled to adopt the clauses if they wish to receive personal data transfers from the EU. In the absence of the SCCs being incorporated into the contract, controllers or processors will be excluded from the data flow from the EU. Furthermore, the EU SCCs allow the EU a relatively high level of control over potential disputes between parties by prescribing EU law as the governing law in the event of a dispute.

Binding corporate rules

Similar to the SCCs, the BCRs apply to cross-border transfers from the EU to third countries without an adequacy decision. However, while the SCCs address the transfer of data between controllers and processors of different entities, the BCRs concern corporate policies within the same group of undertakings, or group of enterprises engaged in a joint economic activity for their internal data transfer.[107] The BCRs need to be approved by the supervisory authority to ensure compliance with the GDPR.[108] It facilitates the internal transfer of data within the group of entities that adhere to the same standards.

In terms of network effects, it attracts some entities based outside the EU to comply with the GDPR standards for the free flow of data. Without the BCRs or SCCs, cross-border data transfers to third countries that lack an adequacy decision would be subject to strict limitations. Currently, 180 BCRs for controllers and 59 BCRs for processors have been approved.[109] This serves as primary evidence of the success in expanding the network of GDPR compliance through the BCRs.

Extraterritorial application

One of the most distinctive provisions of the GDPR is its extraterritorial scope,[110] as set out in Article 3(2).[111] This provision allows the unilateral application of the GDPR to data controllers or processors in foreign countries, without the necessity that countries or companies have consented somehow to the applicable data protection regime.[112]

While adequacy decisions, SCCs, and BCRs primarily concern the rules facilitating cross-border data transfer on a voluntary basis, the extraterritorial application governs all data collection or processing of personal data of data subjects in the EU, when it meets the condition set forth in Article 3(2) of the GDPR. The objective of this stipulation is to control the activities of data collection and data processing, rather than the transfer of data to third countries. Once Article 3(2) is applied to any given activity, there is no requirement to consider the incorporation of SCCs or BCCs, given that such activity would always be obliged to comply with the GDPR.[113] However, one could say that Article 3(2) is a unilateral extraterritorial application of the GDPR.[114] This, in turn, gives rise to the question of whether it can be justified under public and private international law.[115]

According to Article 3(2), the GDPR is applicable if the data subject is in the EU at the time of data collection or data processing, irrespective of their citizenship or residence.[116] However, it is important to consider whether the GDPR should apply to a data subject who is present in the EU only for a temporary purpose, such as for transit, as it establishes only a minimal connection with the EU.[117]

The primary reason for the extraterritorial scope of the GDPR is the prevalence of internet-based data processing, which complicates identifying the location where the data is stored or indexed.[118] Today, businesses may have the place of establishment, place of registration, and place of data processing all in different jurisdictions.[119] Hence, the extraterritorial application under Article 3(2)

107 'Binding Corporate Rules (BCR)' (*European Commission*) <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en> accessed 15 January 2026.

108 Article 29 Data Protection Working Party, *Working Document Setting Forth a Co-Operation Procedure for the Approval of "Binding Corporate Rules" for Controllers and Processors under the GDPR* (2018) WP263 rev.01.

109 'Binding Corporate Rules (BCR)' (*European Data Protection Board*) <https://www.edpb.europa.eu/our-work-tools/accountability-tools/bcr_en> accessed 15 January 2026.

110 See Christopher Kuner, 'Extraterritoriality and regulation of international data transfer in EU data protection law' (2015) 5 International Data Privacy Law 235; Dan Jerker B Svantesson, 'The Extraterritoriality of the EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on US Business' (2014) 50 Stanford Journal of International Law 53.

111 General Data Protection Regulation, art 3
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (i) the offering of goods or services, irrespective of whether a payment from the data subject is required, to such data subjects in the Union; or (ii) the monitoring of their behavior as far as their behavior takes place within the Union.

112 See Christopher Kuner, 'Data Protection Law and International Jurisdiction on the Internet (Part 1)' (2010) 18 International Journal of Law and Information Technology 176; Cedric Ryngaert, *Jurisdiction in International Law* (2nd edn, OUP 2015).

113 European Commission (n 100) 13.

114 See Oskar Josef Gstrein and Andrej Janko Zwitter, 'Extraterritorial Application of the GDPR: Promoting European Values or Power?' (2021) 10 Internet Policy Review 1.

115 See Maja Brkan, 'Data Protection and European Private International Law' (2015) Brkan, Maja, Data Protection and European Private International Law (July 2015). Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS 2015/40, Maastricht Faculty of Law Working Paper, accessed 10 November 2024.

116 European Data Protection Board, 'Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) Version 2.1' (12 November 2019) 14.

117 Claes G Granmar, 'Global applicability of the GDPR in context' (2021) 11 International Data Privacy Law 225, 234.

118 Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317.

119 Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639, paras 28–29.

of the GDPR is designed to prevent any circumvention of EU law by companies that have their business operations based entirely in third countries but target EU data subjects.[120] The extensive extraterritorial application of the GDPR serves as an example of a legal instrument that demonstrates the EU's attempt to expand its jurisdiction and to enforce its legal standards.

Third countries are under no obligation to adopt the extraterritorial principle, as it is not a criterion for determining the adequacy status. However, the provision of extraterritorial application is present in many countries' data protection laws, including those of Japan, Singapore, and Thailand. This is partly in addition to the attempt of third countries to amend or introduce laws in alignment with the GDPR. Many of its provisions have been adopted and incorporated into the national legislation of several countries in various regions around the world. This highlights the significant global impact of the extraterritorial application of the GDPR, affecting not only companies and individuals within its scope but also third states influenced to adopt similar provisions.

Conclusion

The GDPR has grown from being a regional EU law into a comprehensive legal framework with international outreach. Direct and indirect network effects have triggered a legal path dependence, which has led the GDPR to become the worldwide dominant data protection regime. The explanatory power of path dependence is evident on the macro-level, facilitating comprehension of the longer processes and adaptations over time, which brought the GDPR into its dominating position. This article has delved more profoundly into the analysis of path dependence by identifying the triggers of the success of the GDPR and linking those findings to the concrete legal developments of data protection over time. As a result, the lock-in into the GDPR as the world's leading data protection framework becomes analytically tangible.

The GDPR has emerged as a global legal platform involving multiple jurisdictions, transnational companies, and multinational data subjects. The adequacy decision, the SCCs, the BCRs, and the extraterritorial application are the most crucial mechanisms for facilitating the expansion of the GDPR network and maintaining the GDPR's integrity. At present, the network of countries that have already gained the adequacy decision is very strong.[121] The network is supported by a considerable number of countries that are close to attaining adequacy status. Moreover, data controllers and processors have strong incentives to comply with the GDPR standard as a global standard, as it simplifies their task considerably. Therefore, they prefer a unified set of rules that allows them to process their activities across all jurisdictions.

The article's findings raise several key discussion points for future consideration: whether the GDPR, which was originally designed for the specific needs of the EU, faces future challenges in maintaining its status as the world-leading data protection law, and what adjustments might be needed to avoid a path-breaking in the future. A dominant platform may be difficult for an innovator to compete with at a given time. However, once a disruption takes place, it is rather sudden and groundbreaking. To sustain its dominant position, the EU needs to maintain the network effects of the GDPR. It is essential to strike a balance between the protection of data subjects and enabling the free flow of data. Notably, if the EU keeps raising the bar and establishing exceedingly rigorous standards that only a few countries can meet, it will preclude the opportunity for the majority of third countries from joining the network. Hence, to grow the number of countries adhering to the GDPR, the EU must allow greater legal flexibility. The simplification of the GDPR[122] may be beneficial as a starting point for readjusting its position from a regional to a global standard. With a less rigorous threshold, its networking members will be able to comprehend and follow with greater ease. The recent communication and proposal by the European Commission proposing the simplification of certain aspects of the GDPR could be a significant step towards the future of the GDPR to adapt itself to 'a more volatile world',[123] while maintaining its dominance.

120 Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (OUP 2013).

121 Didier Reynders, the EU Commissioner for Justice, Opening Remarks - High-Level Roundtable on Safe Data Flows, (4 March 2024) <https://ec.europa.eu/commission/presscorner/detail/en/speech_24_1310> accessed 28 November 2024).

122 See Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM (2025) 837 final, 19 November 2025; See also Helen Dixon, 'GDPR Is Not Loved, But Does It Work?' (2025) 15 International Data Privacy Law 101.

123 See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A simpler and faster Europe: Communication on implementation and simplification, COM (2025) 47 final (11 February 2025); Digital Omnibus (n 122).

Acknowledgements

We would like to thank the reviewers for their valuable feedback, which has helped us to improve the article substantially.

Conflict of interest statement

None declared.

https://doi.org/10.1093/idpl/ipag009

International Data Privacy Law, 2026, 16, 1–14
https://doi.org/10.1093/idpl/ipag009
Article