This is an Accepted Manuscript of Lucas Maldonado Diz Latini and Edoardo Celeste, 'The European General Data Protection Regulation: Origins, Objectives and Impact' in Olivier Delas et al (eds), L'Espace transatlantique à l'épreuve du numérique global (Larcier 2025), 101-129, https://www.larcier-intersentia.com/fr/l-espace-transatlantique-l-epreuve-numerique-global-9782802776598.html#product.info.tab.details

The European General Data Protection Regulation: Origins, Objectives and Impact

Lucas Maldonado Diz Latini and Edoardo Celeste*

I. Introduction

In today's digital age, where personal data is a valuable commodity, the need for robust data protection measures is nothing less than crucial. The General Data Protection Regulation (GDPR), enacted in May 2018, marks a pivotal advancement in the European Union's (EU) approach to safeguarding individual privacy and data protection rights[1]. This regulation establishes stringent data processing standards and aims to unify data protection law across EU member states, fostering trust and accountability in the digital marketplace.

This chapter aims to provide an overview of the origins, objectives and impact of the GDPR within and beyond the EU. Section II will focus on the historical origins of EU data protection law by analysing the evolution of privacy rights and the foundational contributions of early legal thinkers. We will present the first national and supranational data protection initiatives that emerged in Europe and the EU's first attempt to harmonise the data protection framework via the Data Protection Directive of 1995[2].

Section III will delve into the GDPR's key objectives. We will explain why a regulation was needed after more than twenty years of the Data Protection Directive's life and provide an aerial

* Lucas Latini is a Research Intern at the Law and Tech Research Cluster of Dublin City University, Ireland. Edoardo Celeste is an Associate Professor of Law, Technology and Innovation at the School of Law and Government of Dublin City University, Ireland, where is the Deputy Director of the Dublin European Law Institute (DELI), the Coordinator of the DCU Law and Tech Research Cluster and the Programme Chair of the Erasmus Mundus Master in Law, Data and AI (EMILDAI).

[1] 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.

[2] 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.

view of the GDPR's key rights and principles, highlighting the main differences from the previous regime.

Section IV will examine the GDPR's impact both within the EU and globally, illustrating how its standards have influenced data protection law worldwide. Before concluding, Section V will explore two significant case studies, Canada and the United States, showing how EU data protection standards influence foreign legislation. In the Canadian case, we observe that EU standards are proactively taken as a model and incorporated into national law. The US conversely represents a case where convergence in data protection standards results from a more laborious and tense process, which has been triggered by repeated interventions from civil society actors and EU courts' case law.

II. The origins of EU data protection law

A. From the right to privacy to data protection

The discussions about privacy have gained greater focus from the second half of the 20th century[3]. The idea of privacy has undergone a significant transformation, at least since the end of the 19th century, mainly after the publication of the landmark article «The Right to Privacy» by Samuel D. Warren and Louis Brandeis[4]. In this work, the authors argued that privacy was an implicit right within existing common law, primarily concerned with protecting individuals from unwarranted public disclosure of personal information. They posited that privacy was initially perceived as a physical concept, strongly emphasising safeguarding one's personal space and property.

The «right to privacy» was never explicitly added to the US Federal Constitution. The evolution of the right to privacy in the US occurred through case law, and the Supreme Court explicitly recognised such a right for the first time in 1965, in a context where it was discussed whether states could make contraception by married couples illegal[5]. According to the US Supreme Court, «a right to privacy can be inferred from several amendments in the Bill of Rights»[6].

[3] Our literature review did not find relevant work on this matter before the end of the 1800s.
[4] S. D. WARREN AND L. D. BRANDEIS, «The Right to Privacy» (1890) 4:193, *Harvard Law Review, online:* <https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html> [Accessed 28 July 2024].
[5] US Supreme Court, *Griswold v Connecticut,* [1965].
[6] *Ibid.*

As technology advanced, the understanding of privacy began to shift. The development of photography and the spreading of newspapers in the late 19th and early 20th centuries introduced new ways for personal information to be disseminated without consent, thus demanding broader legal protections[7]. This is why Warren and Brandeis posited the existence of a right «to be let alone», a term first coined by Judge Cooley, and suggested that the law should evolve to address new threats posed by technology, laying the groundwork for modern privacy law[8].

From this moment on, it was apparent that it would not be possible to guarantee a right to privacy, understood as a «static, negative kind of protection»[9] for an individual to keep their personal life and information hidden from public view. It would also be necessary to guarantee a right to data protection, i.e., a «dynamic kind of protection»[10] that gives individuals control over how their information is used, even without their explicit consent.

Interestingly, the terminology «right to privacy» was never adopted in Europe. However, a right to the protection of «private life» was included in the 1950 European Convention on Human Rights, which stated that «everyone has the right to respect for his private and family life, his home and his correspondence»[11]. In 1983, the German Federal Constitutional Court issued a landmark decision establishing the concept of «informational self-determination», recognising that individuals should control their personal data collection, storage, use, and disclosure to protect their dignity and freedom[12]. This decision was made in the context of a general census that was going to be conducted by the German federal government and led to the population's fear of surveillance and invasion of privacy[13].

Even before the *Bundesverfassungsgericht*'s decision, several national data protection initiatives emerged in Europe in the 1970s. In 1970, the German Land of Hessen adopted the first data protection law[14]. In 1973, the Swedish Data Act was enacted, the first specific piece

---

[7] S. D. WARREN AND L. D. BRANDEIS, «The Right to Privacy», *op. cit*.
[8] *Ibid.*
[9] S. RODOTÀ, «Data Protection as a Fundamental Right» (2009) in S. GUTWIRTH AND OTHERS (eds), *Reinventing Data Protection?*, *online:* <http://link.springer.com/10.1007/978-1-4020-9498-9_3> [Accessed 28 July 2024].
[10] *Ibid.*
[11] Council of Europe, European Convention on Human Rights, Art 8 (1950).
[12] BVerfG, *Order of the First Senate of 15 December 1983* - 1 BvR 209/83 -, paras. 1-214, *online:* <https://www.bverfg.de/e/rs19831215_1bvr020983en.html> [Accessed 28 July 2024].
[13] G. HORNUNG AND C. SCHNABEL, «Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination» (2009) 25:1, *Computer Law & Security Review, online:* <https://www.sciencedirect.com/science/article/abs/pii/S0267364908001660> [Accessed 28 July 2024].
[14] G. G. FUSTER, «The Surfacing of National Norms on Data Processing in Europe» (2014) in *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Springer Science & Business, *online:* <https://link.springer.com/chapter/10.1007/978-3-319-05023-2_3> [Accessed 28 July 2024].

of legislation issued by a Western country at the national level[15]. It defined the concepts of «personal information» and «personal register», the last one being «any register or any other notes made by automatic data processing and containing personal information that can be assigned to the individual concerned»[16]. Thus, it is worth noting that the Swedish Data Act was only applied to personal data run by a computer and not by physical means.

In 1977, Germany also enacted its Federal Data Protection Act[17]. Like Swedish law, the German Act focused on the processing of personal data by automatic means, therefore leaving data processed manually outside its scope[18]. One year later, France enacted its own Data Protection Act[19].

The emergency of these and other national data protection laws led to regulatory fragmentation in Europe, with countries having very different data protection standards and thus hampering the free flow of data. This is one of the reasons why, since the 1970s, the OECD, the Council of Europe, and the EU have progressively intervened in this field, aiming to harmonise national provisions.

B. International and EU instruments

In 1980, the OECD introduced the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data to increase the level of harmonisation of data protection law at an international level. They established eight basic principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability[20]. These principles aimed to set a minimum standard for privacy protection and ensured that personal data was handled responsibly, regardless of where it was processed or stored. The Guidelines were intended to be flexible and adaptable, allowing for their implementation in diverse legal and cultural contexts[21]. Over the years, the OECD Privacy

---

[15] J. PILA, «Privacy Legislation and Social Research in Sweden» (1979) in Ekkehard Mochmann and Paul J. Müller (eds), *Data Protection and Social Science Research*, Campus Verlag GmbH.
[16] *Ibid*.
[17] J. L. RICCARDI, «The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?» (1983) 6:1, *Boston College international and comparative law review*, *online:* <https://core.ac.uk/download/pdf/80399406.pdf> [Accessed 16 July 2024].
[18] *Ibid.*
[19] France, *La loi Informatique et Libertés,* 1978.
[20] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2002).
[21] M. KIRBY, «The History, Achievement and Future of the 1980 OECD Guidelines on Privacy» (2011) 1:6, *International Data Privacy Law, online:* <https://academic.oup.com/idpl/article-abstract/1/1/6/759637?redirectedFrom=fulltext> [Accessed 17 July 2024].

Guidelines have influenced numerous national and international data protection frameworks, contributing to the global dialogue on privacy and data protection despite their non-legally binding nature[22]. The Guidelines were revised in 2013 to address new challenges posed by technological advancements[23].

In 1981, Convention No. 108, formally known as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, was adopted by the Council of Europe[24]. It was the first binding international treaty dedicated to data protection[25], aiming to safeguard individuals' privacy and personal data amidst the growing use of computers and data processing technologies. The Convention established core principles such as data quality, purpose specification, security, and the rights of data subjects. It also required signatory states to implement these standards in their national law[26]. Similarly to the OECD Privacy Guidelines, in response to technological advancements and new privacy challenges, the Convention was modernised in 2018, resulting in the so-called Convention 108+[27]. This updated version includes enhanced provisions such as more robust data subject rights, increased transparency, mandatory notification of data breaches and strengthening the powers of data protection authorities («DPAs»)[28]. To date, fifty-five countries have adopted Convention 108+, 9 of them being non-members of the Council of Europe[29].

Despite helping to harmonise data protection law, the OECD Privacy Guidelines and the Convention 108 were still relatively general instruments, and more detailed rules were needed in a highly integrated market such as the EU. Thus, in 1995, the EU adopted a pivotal legislative framework designed to regulate the processing of personal data: the Data Protection Directive

---

[22] G. GREENLEAF, «It's Nearly 2020, so What Fate Awaits the 1980 OECD Privacy Guidelines? (A Background Paper for the 2019 OECD Privacy Guidelines Review)» (2019), *SSRN Electronic Journal*, *online:* <https://www.ssrn.com/abstract=3405156> [Accessed 17 July 2024].
[23] *Ibid.*
[24] Council of Europe, Convention 108 and Protocols (1981).
[25] *Ibid.*
[26] C. D. TERWANGNE, «Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data» (2021) 40, *Computer Law & Security Review, online:* <https://www.sciencedirect.com/science/article/abs/pii/S0267364920301023> [Accessed 26 July 2024].
[27] Council of the European Union, Convention 108 + - Convention for the protection of individuals with regard to the processing of personal data (2018).
[28] C. D. TERWANGNE, «Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data», *op. cit.*
[29] Council of Europe, Chart of Signatures and Ratifications of Treaty 108 (2024) [Accessed 27 July 2024].

(Directive 95/46/EC). This legislation entered into force in 1998 and required EU member states to transpose its provisions into national laws[30].

The Data Protection Directive established several key provisions, including requirements for data quality, data subject rights, and the responsibilities of data controllers. It mandated that personal data should be processed fairly and lawfully, collected for specified, legitimate purposes[31], and kept secure against unauthorised access or disclosure[32]. One of the Directive's critical goals was to harmonise data protection law across EU member states to prevent disparities that could hinder the free movement of data[33]. Even though national regulations were slightly different, this harmonisation was achieved by setting a high standard of data protection that member states had to implement in their national laws, thus creating a level playing field and facilitating cross-border data exchanges[34].

One of the main innovations of the Directive was its international data transfer mechanisms, as stipulated in Article 25. In principle, personal data could only be transferred to third countries, intended as non-EU countries, if they provided an «adequate level of [data] protection». Intra-EU data transfers were no longer considered international and were thus freely allowed without any obstacles. Some derogations were provided in Article 26 (e.g. if the data subject consented to the transfer)[35]. This provision encouraged non-EU countries to adopt similar data protection standards to facilitate data exchanges with EU member states and de facto fostered the extraterritorial influence of the Directive[36].

It is worth noting that the Data Protection Directive was adopted in a context where digital technologies were still at an embryonal stage. As technology evolved, some challenges were faced when enforcing the Data Protection Directive, mainly in a context where the online and offline environments became more intertangled. To tackle these new challenges and ensure

---

[30] UE, *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] OJ, L 281.
[31] *Ibid.*
[32] *Ibid.*
[33] UK, Information Commissioner's Office, N. ROBINSON AND OTHERS, *Review of the European Data Protection Directive,* 2009, *online:* <https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf> [Accessed 27 July 2024].
[34] *Ibid.*
[35] UE, 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, *op. cit*.
[36] M. D. BIRNHACK, «The EU Data Protection Directive: An Engine of a Global Regime» (2008) 24:6, *Computer Law & Security Review, online:* <https://www.sciencedirect.com/science/article/abs/pii/S0267364908001337#:~:text=The%201995%20EU%20Directive%20on,the%20export%20of%20such%20data.> [Accessed 27 July 2024].

privacy in the digital age, specifically in the context of electronic communications, in 2002, the European Union adopted the e-Privacy Directive, formally known as Directive 2002/58/EC, which is still in force[37]. Like the Data Protection Directive, member states should also transpose the provisions of the e-Privacy Directive into their national laws.

A significant provision of the e-Privacy Directive is the regulation of cookies and similar technologies for tracking online behaviour. In the first version of this Directive, as a rule, cookies were only allowed if the user was (i) provided with clear and comprehensive information about the purposes of the processing and (ii) offered the right to refuse such processing by the data controller[38]. After an amendment in 2009, Article 5(3) of the e-Privacy Directive mandates that the processing of personal data using cookies is only allowed, as a rule, if the user has (i) given their consent and (ii) been provided with clear and comprehensive information about the purposes of the processing, in accordance to the Data Protection Directive. This shift from an «opt-out» to an «opt-in» approach was designed mainly due to concerns about online tracking, thus enhancing user privacy and control over personal data[39].

Another key provision of the e-Privacy Directive is Article 13, which deals with unsolicited communications, i.e., direct electronic marketing via email, SMS, and other similar means of communication. The general rule for processing personal data for this purpose also relies on collecting the user's affirmative consent (opt-in)[40], which can be withdrawn at any time[41]. As a derogation, the provider does not need to gather consent for direct marketing of its similar products or services provided that users are allowed to object each time the marketing message is sent (opt-out)[42].

As seen, the e-Privacy Directive dealt with more detailed technological issues regarding the processing of personal data in the digital environment, whereas the Data Protection Directive provided a broader scope of application, not explicitly mentioning technologies such as

---

[37] UE, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, [2002] OJ, L 201.
[38] *Ibid.*
[39] UK, Information Commissioner's Office, *Guidance on the Rules on Use of Cookies and Similar Technologies*, May 2012, *online:* <https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf> [Accessed 28 July 2024].
[40] UE, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *op. cit*.
[41] Ireland, Data Protection Commission, *Rules for Direct Electronic Marketing,* n.d., *online:* <https://www.dataprotection.ie/organisations/rules-electronic-and-direct-marketing> [Accessed 28 July 2024].
[42] *Ibid.*

cookies, spam, etc. Both Directives were directly impacted by the adoption of the GDPR, as will be detailed later in this chapter.

Lastly, besides these two landmark pieces of legislation, it is worth remembering that, in 2009, for the first time, privacy and data protection were recognised as two distinct fundamental rights in the Charter of Fundamental Rights of the EU (Articles 7 and 8)[43]. After the 2009 Lisbon Treaty, the Charter acquired a constitutional status within the EU[44]. This development highlighted the importance of protecting both the «physical» and the «electronic» body of individuals when interacting with digital technologies[45].

III. Objectives of the GDPR

A. The need for a regulation

The transition from the Data Protection Directive to the GDPR marked a significant shift in the EU's approach to data protection[46]. In this context, it is essential to differentiate a directive from a regulation within the EU legal framework. A regulation is a binding legislative act that applies directly across all member states without the need for national transposition[47]. It does not need to be implemented by national laws, although certain matters can be left to the member states to implement further. This ensures uniformity and consistency in applying the law across the entire EU. A directive is also a binding legal instrument. However, it sets out goals that all EU member states must achieve, allowing them flexibility in implementing these objectives through their national laws[48].

The need for member states to implement the provisions of the Data Protection Directive led to some inconsistencies in the application and enforcement of data protection law across the EU[49]. These variations created challenges for businesses operating across multiple EU countries as they had to navigate different legal requirements. To address these issues and

[43] UE, *Charter of Fundamental Rights of the European Union*, [2012] OJ, C 326/391.
[44] UE, European Data Protection Supervisor, *Data Protection*, n.d., *online:* <https://www.edps.europa.eu/data-protection/data-protection_en> [Accessed 27 July 2024].
[45] S. RODOTÀ, «Data Protection as a Fundamental Right», *op. cit*.
[46] C. TIKKINEN-PIRI, A. ROHUNEN AND J. MARKKULA, «EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies» (2018) 34:134, *Computer Law & Security Review, online:* <https://www.sciencedirect.com/science/article/abs/pii/S0267364917301966> [Accessed 28 July 2024].
[47] EU, *Types of Legislation*, n.d., *online:* <https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en> [Accessed 29 July 2024].
[48] *Ibid.*
[49] K. NOLAN, «GDPR: Harmonization or Fragmentation? Applicable Law Problems in EU Data Protection Law» (2018), *Berkeley Technology Law Journal*, *online:* <https://btlj.org/2018/01/gdpr-harmonization-or-fragmentation-applicable-law-problems-in-eu-data-protection-law/> [Accessed 18 August 2024].

ensure a more uniform and coherent approach[50], the GDPR was introduced as a regulation in 2016, becoming directly applicable in all member states without the need for national transposition in 2018. This eliminated legal fragmentation and provided a single set of rules for data protection across the EU.

B. Normative innovations

Besides harmonising the data protection provisions across the EU, the GDPR also introduced essential innovations within the EU data protection framework[51]. Below, we will further explore seven of those innovations.

1. Clarifying the extraterritorial scope of application

The first significant innovation from the Data Protection Directive to the GDPR is related to its territorial scope of application. A first reading of the Data Protection Directive could lead to an interpretation that this piece of legislation was only applicable to organisations that had a «physical presence» in a specific member state or to personal data processed within the EU (Article 4), which led to variations in data protection rules across member states. This matter was analysed at least twice by the Court of Justice of the European Union (CJEU)[52], which ruled that the Data Protection Directive could apply to a foreign-registered company if that company exercises real and effective activities in a member state, even if the organisation is not actually «established» within a member state. These decisions had to clarify that the

[50] Spain, Agencia Española de Protección Datos, *Approach to Data Spaces From GDPR Perspective*, May 2023, *online:* <https://www.aepd.es/documento/approach-to-data-spaces-from-gdpr-perspective.pdf> [Accessed 18 August 2024].
[51] G. PRIYADHARSHINI AND K. SHYAMALA, «Strategy and Solution to Comply with GDPR : Guideline to Comply Major Articles and Save Penalty from Non-Compliance», *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), online:* <https://ieeexplore.ieee.org/document/8653696/> [Accessed 18 August 2024].
[52] CJEU, *Google Spain, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* C-131/12, [2014]; *Weltimmo s r o v Nemzeti Adatvédelmi és Információszabadság Hatóság,* C-230/14, [2015].

territorial scope of the Directive could extend beyond the simple location of a company's registration.

In contrast with the provision of the Data Protection Directive, so that there would be no doubt about this extraterritorial application, the GDPR expressly extends (Article 3(2)) its application to organisations not established in the EU, provided that the personal data processing activities are related to (i) the offering of goods or services to data subjects in the Union, or (ii) the monitoring of their behaviour as far as their behaviour takes place within the Union[53].

2. Excluding law enforcement from the material scope of application

Both the Data Protection Directive (Article 3(1)) and the GDPR (Article 2(1)) explicitly provide that the legislation should apply «to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system».

However, in contrast to the Data Protection Directive, the GDPR explicitly states that it does not apply to personal data processing activities related to law enforcement, which is governed by the Law Enforcement Directive (Directive EU 2016/680)[54]. This Directive explicitly regulates the processing of personal data by competent authorities to prevent, investigate, detect, or prosecute criminal offences. It establishes rules for law enforcement agencies to balance privacy rights with public security needs[55].

3. Introducing the principle of accountability

Another relevant innovation that the GDPR introduced is the principle of accountability (Article 5(2)). Under the Directive, organisations were primarily required to comply with data protection law, but there was no explicit requirement to demonstrate compliance. The GDPR

---

[53] UE, *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)*, [2016] OJ, L 119. See F. FABBRINI, E. CELESTE AND J. QUINN (eds), *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty,* UK, Hart, 2021.

[54] UE, *Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA,* [2016] OJ, L 119.

[55] J. SAJFERT AND T. QUINTEL, «Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities» (2017), *SSRN Electronic Journal*, *online:* <https://www.ssrn.com/abstract=3285873> [Accessed 18 August 2024].

conversely made accountability a central principle, requiring organisations to comply with data protection rules and document and demonstrate their compliance[56].

This shift reflects a more proactive approach to data protection. It compels organisations to maintain transparency with stakeholders, including DPAs and data subjects, ensuring they can provide proof of compliance whenever necessary[57]. The accountability principle has fundamentally changed the data protection landscape by making compliance an ongoing responsibility rather than a reactive measure. The introduction of accountability has had far-reaching effects on the data protection ecosystem, shifting the burden of proof to data controllers and making it a cornerstone of the GDPR's regulatory framework[58].

4. Making consent rules more stringent

The GDPR also introduced more stringent rules on consent to process special categories of personal data, what was formerly known as 'sensitive' data, requiring it to be explicit (Article 9(2)(a)), informed, and freely given (Article 7), a considerable upgrade from the more lenient requirements under the Data Protection Directive[59]. This means that organisations, in some instances, must obtain explicit, clear and unambiguous consent from data subjects before processing their personal data, and the consent must be actively given[60], such as by checking a box rather than through pre-checked boxes or implied actions.

The Regulation explicitly gives data subjects the right to withdraw their consent at any time, making the consent process more dynamic and giving individuals greater control over their personal data[61]. This contrasts with the Directive, where withdrawal of consent was not as

---

[56] T. KARJALAINEN, «All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm» (2022) 8:1, *European Data Protection Law Review, online:* <https://edpl.lexxion.eu/article/edpl/2022/1/6> [Accessed 19 August 2024].
[57] *Ibid.*
[58] *Ibid.*
[59] D. CLIFFORD, I. GRAEF AND P. VALCKE, «Pre-Formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections» (2019) 20:5, German Law Journal, *online:* <https://www.cambridge.org/core/journals/german-law-journal/article/preformulated-declarations-of-data-subject-consentcitizenconsumer-empowerment-and-the-alignment-of-data-consumer-and-competition-law-protections/293BB74ABDC953F88ECB10895755589B> [Accessed 18 August 2024].
[60] S. BREEN, K. OUAZZANE AND P. PATEL, «GDPR: Is Your Consent Valid?» (2020) 37:1, *Business Information Review*, *online:* <https://journals.sagepub.com/doi/full/10.1177/0266382120903254> [Accessed 18 August 2024].
[61] E. POLITOU, E. ALEPIS AND C. PATSAKIS, «Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions» (2018) 4:1, *Journal of Cybersecurity*, *online:* <https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyy001/4954056> [Accessed 18 August 2024].

clearly defined or enforced. Additionally, the consent under the GDPR must be «granular»[62], meaning individuals should be able to consent to different types of processing separately, ensuring that consent is not bundled with other conditions or coerced.

5. Establishing new data subject rights

The Data Protection Directive (Articles 12 and 14) explicitly provided the data subjects' basic rights, such as access, processing confirmation, rectification, and objection[63]. The GDPR delved deeper into this topic and dedicated an entire chapter to this matter, expanding on existing rights and introducing new rights for data subjects[64].

One of the most popular provisions introduced in the GDPR is the so-called «right to be forgotten» (Article 17), where the data subject has the right to obtain from the controller the erasure of personal data under specific conditions (e.g. if the personal data are no longer necessary to the purposes for which they were collected or otherwise processed)[65]. In the Data Protection Directive, this right was not as broad and explicit as in the GDPR. Still, it was already recognised by the CJEU based on the right to object to the processing of personal data and the right to rectification, erasure or blocking of personal data[66].

One new right can be found in Article 20 of the GDPR, which explicitly grants the data subject the right to portability, allowing individuals to transfer their personal data from one controller to another in a structured, commonly used, machine-readable format. By allowing individuals to transfer their data from one data controller to another, the right to data portability reduces the so-called «lock-in effect», where consumers find it challenging to switch between service

---

[62] UK, Information Commissioner's Office, *Consent,* 19 May 2023, *online:* <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/> [Accessed 18 August 2024].
[63] UE, 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, *op. cit*.
[64] G. PRIYADHARSHINI AND K. SHYAMALA, «Strategy and Solution to Comply with GDPR : Guideline to Comply Major Articles and Save Penalty from Non-Compliance», *op. cit*.
[65] F. FABBRINI AND E. CELESTE, «The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders», (2020) 21:S1, *German Law Journal*, *online:* <https://www.cambridge.org/core/journals/german-law-journal/article/right-to-be-forgotten-in-the-digital-age-the-challenges-of-data-protection-beyond-borders/3E3E182352F1AD555CBB788E2380E23F> [Accessed 28 August 2024].
[66] U. KOHL, «The Right to Be Forgotten in Data Protection Law and Two Western Cultures of Privacy» (2023) 72:3, *International and Comparative Law Quarterly*, *online:* <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/right-to-be-forgotten-in-data-protection-law-and-two-western-cultures-of-privacy/31D2EDDE753A64F40FAFBF4B76CEA89C> [Accessed 28 August 2024].

providers due to the inability to transfer their data easily[67]. Therefore, the right to data portability has a pro-competitive character, facilitating the entry of new competitors into the market by enabling them to attract users who can bring their data along with them, thus reducing barriers to entry.

Moreover, Article 22 of the GDPR provides that data subjects have the right not to be subject to a decision based solely on automated processing. This is especially relevant in a context where organisations increasingly use Artificial Intelligence (AI) systems to make decisions that impact people in several areas of life (e.g., credit scoring, insurance, etc.)[68]. When automated decision-making mechanisms are used, the controller must grant the data subject the right to obtain human intervention to express their point of view and contest the decision.

6. Ensuring data protection by default and by design

One of the GDPR's most innovative provisions compared to the Data Protection Directive is Article 25: the principle of Data Protection by Design and by Default[69]. According to Article 25(1) of the GDPR (Data protection by design), the controller shall, both at the time of determining the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to effectively implement data protection principles and integrate the necessary safeguards into the processing.

According to the European Data Protection Board (EDPB), this means that organisations shall adopt such appropriate technical and organisational measures from the earliest stage of the data processing activity, that is, «when the controller is deciding how the processing will be conducted and the manner in which the processing will occur and the mechanisms which will be used to conduct such processing»[70]. The same measures shall be maintained «at the time of

[67] I. GRAEF, M. HUSOVEC AND N. PURTOVA, «Data Portability and Data Control: Lessons for an Emerging Concept in EU Law» (2018) 19:6, German Law Journal, *online:* <https://www.ssrn.com/abstract=3071875> [Accessed 11 September 2024].

[68] M. PURDY AND A. M. WILLIAMS, «How AI Can Help Leaders Make Better Decisions Under Pressure» (2023), *Harvard Business Review*, *online:* <https://hbr.org/2023/10/how-ai-can-help-leaders-make-better-decisions-under-pressure> [Accessed 7 September 2024]. See also E. CELESTE AND G. D. GREGORIO, «Digital Humanism: The Constitutional Message of the GDPR» (2022) 3:4, *Global Privacy Law Review*, *online:* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4045029> [Accessed 7 September 2024].

[69] G. PRIYADHARSHINI AND K. SHYAMALA, «Strategy and Solution to Comply with GDPR : Guideline to Comply Major Articles and Save Penalty from Non-Compliance», *op. cit*.

[70] EU, European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0,* 20 October 2020, p 10, *online* <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> [Accessed 18 August 2024].

the processing», meaning that the controller shall keep adopting effective measures to comply with the GDPR's principles effectively[71].

Article 25(2) of the GDPR provides that organisations shall, by default, implement appropriate technical and organisational measures to process only personal data which are strictly necessary for each specific purpose (Data protection by default). The EDPB clearly states that it is the organisation's responsibility to implement default processing settings (e.g. in a software application) to ensure that only strictly necessary processing activities are carried out by default[72]. This is closely related to the data minimisation principle of the GDPR (Article 5(1)(c)), which provides that personal data shall be adequate, relevant and limited to what is necessary concerning the purposes for which they are processed.

7. Reporting personal data breaches

The Data Protection Directive did not have a specific provision regarding data breach notification obligation, although local authorities advised organisations to do so[73]. After the GDPR (Article 33), controllers shall, as a rule, report personal data breaches to the respective supervisory authority within 72 hours of becoming aware of it.

However, not all personal data breaches must be notified. As recognised by the EDPB, notifying the competent supervisory authority is not required if a breach is unlikely to result in a risk to the rights and freedoms of individuals. Similarly, communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms[74]. Some points to be considered when assessing the risk of the breach are the type of breach; the nature, sensitivity, and volume of personal data; ease of identification of individuals; severity of consequences for individuals; special characteristics of individuals and the data controller; and the number of affected individuals[75].

This obligation is closely related to the principle of accountability illustrated above since Article 33(5) of the GDPR provides that «the controller shall document *any* personal data

---

[71] *Ibid.*
[72] *Ibid.*
[73] EU, European Data Protection Board, *Guidelines 9/2022 on Personal Data Breach Notification under GDPR Version 2.0*, 28 March 2023, *online:* <https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf> [Accessed 18 August 2024].
[74] *Ibid.*
[75] *Ibid.*

breaches». In this context, the supervisory authority can request the respective documentation[76].

IV. Impact of the GDPR: within the Union and beyond

A. Internal enforcement and broader societal effects

Since it became fully applicable in May 2018, the GDPR has had significant impact within the EU. One of the main consequences has been the increased activity of national DPAs, which are responsible for investigating GDPR violations. In the first twenty-four months after the GDPR's implementation, DPAs across the EU have investigated hundreds of cases[77]. As of 2020, national authorities had already publicly issued over 261 enforcement orders concerning GDPR violations[78].

At the time of writing, DPAs across the EU issued 2185 fines for GDPR infractions, totalling approximately € 4,920,000,000[79]. The highest fine (€ 1,200,000,000) was imposed in 2023 by the Irish Data Protection Commission due to an insufficient legal basis for data processing by the US company Meta[80]. This type of violation represents the rationale for most of the fines imposed by DPAs (654 fines to date)[81].

Ireland is the country that imposed the highest total *amount* of fines (almost € 2,860,000,000 at 27 fines), followed by Luxembourg (almost € 750,000,000 at 32 fines) and France (more than € 370,000,000 at 62 fines)[82]. Most «big tech» companies have established their headquarters in Ireland due to low taxes and easy access to the EU market[83]. Therefore, according to Articles 55 and 56 of the GDPR, the Irish Data Protection Commission is the competent authority to enforce the Regulation vis-à-vis these companies. Regarding the highest *number* of fines, Spain leads with 890 fines imposed (€ 82,154,990 in total). Italy occupies the

---

[76] *Ibid.*
[77] J. WOLFF AND N. ATALLAH, «Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020» (2020), *TPRC48: The 48th Research Conference on Communication, Information and Internet Policy*, *online:* <https://www.ssrn.com/abstract=3748837> [Accessed 11 September 2024].
[78] *Ibid.*
[79] CMS Law.Tax, «GDPR Enforcement Tracker», (2024), *online:* <https://www.enforcementtracker.com> [Accessed 11 September 2024].
[80] *Ibid.*
[81] *Ibid.*
[82] *Ibid.*
[83] C. GOUJARD, «Ireland Gambles on China's Big Tech Billions», *POLITICO* (19 March 2024), *online:* <https://www.politico.eu/article/ireland-big-tech-china-economy/> [Accessed 11 September 2024].

second place with 384 fines imposed (€ 236,297,858 in total), followed by Germany in the third place (€ 55,578,933 in total)[84].

The GDPR also had an educational impact within the EU. Article 57 of the GDPR explicitly provides that each supervisory authority shall, in its own territory, «promote public awareness and understanding of the risks, rules, safeguards and rights in relation to [personal data] processing». From the public perspective, the GDPR represented a critical vehicle to spread a data protection culture across the EU and raise awareness among businesses and citizens[85].

In 2020, 69% of the people in the EU already heard about the GDPR[86]. 60% of the citizens knew about provisions allowing them to access their data processed by public administrations, and 51% knew about the possibility of exercising this right vis-à-vis private companies[87]. In selected countries[88], citizens' awareness of the GDPR has more than doubled from 2018 to 2022[89].

However, there is still work to be done. 2020 research shows that only one in five respondents in the EU always read the terms and conditions when using online services[90], highlighting that people are not always fully aware of the means and purposes for which controllers process their personal data.

B. Global influence: the Brussels effect

As observed above, EU data protection law has exercised an extraterritorial effect since at least the Data Protection Directive by extending its scope of application to organisations established in non-EU countries offering products and services in the EU and by influencing data protection legislation of countries that aim to receive EU data. Various scholars have been studying the

---

[84] CMS Law.Tax, «GDPR Enforcement Tracker», *op. cit*.
[85] EU, European Union Agency for Fundamental Rights, *Your Rights Matter: Data Protection and Privacy: Fundamental Rights Survey,* 2020, *online:* <https://data.europa.eu/doi/10.2811/031862> [Accessed 11 September 2024].
[86] *Ibid.*
[87] *Ibid.*
[88] France, Germany, Netherlands, Spain, UK and Belgium.
[89] A. PETROSYAN, «GDPR Awareness Level in Selected European Markets 2018-2022», *Statista* (7 July 2022), *online:* <https://www.statista.com/statistics/1311126/gdpr-awareness-european-countries/> [Accessed 11 September 2024].
[90] EU, European Union Agency for Fundamental Rights, *Your Rights Matter: Data Protection and Privacy: Fundamental Rights Survey, op. cit*.

impact of applying EU law outside its borders; in 2012, Anu Bradford coined the successful expression «Brussels effect» to reflect this phenomenon[91].

The Brussels effect refers to the European Union's capacity to influence non-EU companies and foreign regulations[92]. This phenomenon arises due to the EU's economic power: to access its large internal market, foreign businesses are compelled to comply with EU standards[93]. This trend is not only the result of the architecture of EU law but of global corporations voluntarily adopting EU regulations. This occurs because it is often cheaper and more efficient for companies to follow a single standard, usually the stricter one, across all markets rather than adopting different practices across their targeted regions[94]. This principle applies to various policy sectors, including data protection[95].

The Brussels Effect operates in two forms: *de facto* and *de jure*[96]. The *de facto* Brussels effect occurs when companies alter their practices globally to meet EU standards without any legal mandate from their home countries to adhere to do so[97]. This has been especially common in sectors such as data protection, where tech companies operating globally conform to GDPR standards even in jurisdictions with less stringent regulations[98]. The same is expected regarding

---

[91] D. J. B. SVANTESSON, «Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation» (2015) 5:4, *International Data Privacy Law, online:* <https://academic.oup.com/idpl/article-abstract/5/4/226/2404462?redirectedFrom=fulltext> [Accessed 11 September 2024]; See also C. KUNER, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5, *International Data Privacy Law*, *online:* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2644237> [Accessed 11 September 2024]; and F. FABBRINI AND E. CELESTE, «The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders», *op. cit*. In relation to the concept of 'Brussels effect', see A. BRADFORD, «The Brussels Effect» (2012) 107, *Northwestern University Law Review*, *online:* <https://northwesternlawreview.org/issues/the-brussels-effect/> [Accessed 11 September 2024].

[92] A. BRADFORD, «Exporting Standards: The Externalization of the EU's Regulatory Power via Markets», (2015) 42, *International Review of Law and Economics*, *online:* <https://www.sciencedirect.com/science/article/abs/pii/S0144818814000659> [Accessed 7 September 2024]; See also A. BRADFORD, *The Brussels Effect: How the European Union Rules the World,* UK, Oxford University Press, 2020.

[93] *Ibid.*

[94] L. M. D. LATINI, *Frameworks Para a Governança de Inteligência Artificial: Uma Análise Comparativa*, (2023), *online:* <https://repositorio.fgv.br/items/6a48c0a0-9c1e-474e-8da0-0efecfeaa41b> [Accessed 8 September 2024].

[95] A. BRADFORD, *Digital Empires: The Global Battle to Regulate Technology,* UK, Oxford University Press, 2023); See also A. BRADFORD, «Exporting Standards: The Externalization of the EU's Regulatory Power via Markets», *op. cit*.

[96] A. BRADFORD, «Exporting Standards: The Externalization of the EU's Regulatory Power via Markets», *op. cit*.

[97] *Ibid.*

[98] C. SIEGMANN AND M. ANDERLJUNG, «The Brussels Effect and Artificial Intelligence», (2022) 1, *APSA Preprints*, *online:* <https://preprints.apsanet.org/engage/apsa/article-details/634849133e8d99f02d18b1d2> [Accessed 8 September 2024].

AI since the EU AI Act entered into force on August 1, 2024, and some provisions became applicable in February 2025[99].

On the other hand, the *de jure* Brussels effect occurs when non-EU countries adopt EU-like legislation as national organisations impacted by the *de facto* Brussels Effect lobby their local governments to incorporate these same standards into national law. According to Bradford, this phenomenon occurs mainly for competition reasons, as an attempt to create a fairer playing field against their local competitors who are not focused on exports[100].

While some authors interpret the Brussels effect as a form of modern regulatory imperialism or colonialism[101], other scholars regard it as a natural outcome of the EU internal market goals and the voluntary nature of global corporate compliance[102]. According to this interpretation, the Brussels Effect would play a protective function vis-à-vis the EU internal market, preventing access from companies adopting different standards and potentially violating EU rules.

V. Two case studies: data protection across the Atlantic

A. Following the EU model: Canada

Even before the GDPR, EU standards on data protection had already influenced several countries around the globe. As of the end of May 2018, when the GDPR was still coming into force, at least 126 countries had already enacted data protection laws that met international standards, such as the Council of Europe's Convention 108, with 60% of these pieces of legislation coming from outside Europe[103]. In the two decades since the adoption of the Data Protection Directive, there has been a considerable degree of global convergence towards the

---

[99] T. HICKMAN AND OTHERS, «Long Awaited EU AI Act Becomes Law after Publication in the EU's Official Journal», *White & Case* (16 July 2024), *online:* <https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal> [Accessed 8 September 2024].

[100] A. BRADFORD, «The Brussels Effect», *op. cit*.

[101] R. A. PINTO, «Digital Sovereignty or Digital Colonialism?» (2018) 15, *SUR international human rights journal*, *online:* <https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/> [Accessed 15 September 2024]; cf. E. CELESTE, «Digital Sovereignty in the EU: Challenges and Future Perspectives.», in F. FABBRINI, E. CELESTE AND J. QUINN (eds), *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty,* UK, Hart, 2021.

[102] A. EUSTACE, «The European Union's Forced Labour Regulation: Putting the «Brussels Effect» to Work for International Labour Standards» (2024) 15:1, *European Labour Law Journal*, *online:* <https://journals.sagepub.com/doi/10.1177/20319525231221097> [Accessed 15 September 2024].

[103] G. GREENLEAF, «Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018» (2018), *online:* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3184548> [Accessed 8 September 2024].

EU standards, and data protection law adopted outside Europe embraced more than half of the higher standards required in Europe since the 1990s[104].

By September 2023, five years after the full entry into force of the GDPR, at least 18 countries worldwide had already adopted GDPR-like data protection laws[105]. This includes big economies on different continents, such as Canada, Brazil, Japan, India, Australia, and the UK (after Brexit). While more work can be found in each of these countries, our analysis will focus on one example: Canada.

Following the introduction of the Data Protection Directive, Canada was one of the many countries outside the EU that enacted a comprehensive piece of legislation on data protection. The Personal Information Protection and Electronic Documents Act (PIPEDA) was passed in 2000 and became effective in January 2001, much influenced by the European framework[106]. Before the PIPEDA, privacy and data protection in Canada were primarily focused on the public sector, leaving gaps in the private sector[107].

The primary goal of PIPEDA was to establish a wide-ranging framework for protecting personal data in commercial activities. In December 2001, the European Commission recognised Canada as a country with an adequate level of protection for personal data transferred from the EU to recipients subject to the PIPEDA, thus limiting the possibility of freely transferring EU data to Canadian commercial organisations[108].

The GDPR significantly impacted Canada's data protection framework. Following its introduction in 2018, Canada undertook legislative reviews and amendments to align its data protection standards with the GDPR's stringent requirements, aiming to maintain its adequacy

---

[104] *Ibid.*

[105] F. ZAFAR, «18 Countries with GDPR-like Data Privacy Laws», *Yahoo Finance* (14 September 2023), *online:* <https://finance.yahoo.com/news/18-countries-gdpr-data-privacy-121428321.html> [Accessed 8 September 2024].

[106] R. MAHIEU AND OTHERS, «Measuring the Brussels Effect through Access Requests: Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens?» (2021) 11, *Journal of Information Policy*, *online:* <https://scholarlypublishingcollective.org/psup/information-policy/article/doi/10.5325/jinfopoli.11.2021.0301/292024/Measuring-the-Brussels-Effect-through-Access> [Accessed 9 September 2024].

[107] L. E. FRAZIER, «Extraterritorial Enforcement of Pipeda: A Multi-Tiered Analysis» (2004) 36, George Washington International Law Review, *online:* <https://heinonline-org.dcu.idm.oclc.org/HOL/Page?handle=hein.journals/gwilr36&id=227&collection=journals&index=> [Accessed 9 September 2024].

[108] EU, European Commission, *2002/2/EC: Commission Decision 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,* 20 December 2001, *online:* <https://eur-lex.europa.eu/eli/dec/2002/2(1)/oj/eng> [Accessed 9 September 2024].

status with the EU[109]. One of the main adjustments to PIPEDA aimed to address concerns about obtaining individuals' consent[110]. After PIPEDA's reform, organisations are generally required to obtain meaningful consent to process personal data[111]. Similarly to the GDPR, consent under PIPEDA's regime can only be collected to fulfil an explicitly specified and legitimate purpose. It will only be valid if data subjects are informed about and understand the nature, purpose, and consequences of processing their personal data[112]. Also like the GDPR, consent for processing special categories of personal data (known as «sensitive information» under PIPEDA) must be explicit[113]. In January 2024, the European Commission issued a Report concluding that Canada «continues to provide an adequate level of protection for personal data transferred from the EU to recipients subject to PIPEDA»[114].

Nowadays, Canada is discussing a comprehensive reform of its legislation regarding digital matters, called «Bill C-27» or the «Digital Charter Implementation Act»[115]. It intends to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act in a single legislation and make amendments to other acts[116].

If passed, this new legislation will substitute PIPEDA and establish even more stringent data protection obligations. For example, under PIPEDA's regime, the Office of the Privacy Commissioner of Canada (OPC) can only initiate audits where there are reasonable grounds that an organisation *is infringing* legislation[117]. According to the new proposal, the Canadian Authority could initiate an investigation if the organisation *has contravened, is contravening*

---

[109] A. THOROGOOD, «Canada: Will Privacy Rules Continue to Favour Open Science?» (2018) 137:8, Human Genetics, *online:* <https://pmc.ncbi.nlm.nih.gov/articles/PMC6132649/> [Accessed 8 September 2024].
[110] EU, European Commission, *REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the First Review of the Functioning of the Adequacy Decisions Adopted Pursuant to Article 25(6) of Directive 95/46/EC*, 15 January 2024, *online:* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024DC0007> [Accessed 9 September 2024].
[111] Canada, Office of the Privacy Commissioner of Canada, *PIPEDA Fair Information Principle 3 – Consent*, 8 January 2018, *online:* <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/> [Accessed 9 September 2024].
[112] *Ibid.*
[113] *Ibid.*
[114] EU, European Commission, *Report From The Commission To The European Parliament And The Council on the First Review of the Functioning of the Adequacy Decisions Adopted Pursuant to Article 25(6) of Directive 95/46/EC*, *op. cit*.
[115] Canada, *Bill C-27 (44-1) - Digital Charter Implementation Act,* 2022.
[116] *Ibid.*
[117] Canada, Office of the Privacy Commissioner of Canada, *Issue Sheets on the Study of Bill C-27*, 16 February 2024, *online:* <https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/indu_20231019/is_c27_20231019/> [Accessed 12 September 2024].

or is likely to contravene the law[118]. This aligns with the powers granted by the EU to DPAs, who expressly have independence and autonomy to conduct investigations under the GDPR (Articles 52 and 57(f)(h)).

Another proposal regarding Bill C-27 by the OPC includes a right to contest decisions taken by automated systems. The original text of the Bill provides that organisations using automated decision systems to make predictions, recommendations or decisions must provide individuals with an explanation of that decision[119]. However, the OPC understands that besides explaining the decision, individuals should have the right to contest such an automated decision and seek human intervention, as in Article 22 of the GDPR[120].

Furthermore, the OPC expressly mentions the need for the Canadian AI and Data Act to be aligned with the EU legislation, particularly the GDPR and the EU AI Act[121]. This shows that while Canada is advancing in regulating digital matters, it is putting efforts into maintaining the country's data protection framework aligned with the EU's standards, which is relevant to keeping the status of a country with an adequate level of protection for personal data.

B. A laborious convergence: the United States

Whereas many countries have adopted legislation aligned with the EU approach, the US, one of the world's leading economic players, has followed a significantly different path in data protection. The country has a more liberal approach to this matter. It does not rely on a comprehensive federal data protection law equivalent to the GDPR but only on sector-specific regulations[122]. Some US states have specific privacy laws, such as the California Consumer Protection Act (CCPA) and the Colorado Privacy Act (CPA)[123]. Still, these only impact mainly local undertakings and are less comprehensive than the GDPR.

In addition to this very different regulatory approach, the EU has expressed serious concerns about the possibility of US federal agencies accessing personal data coming from the EU for

---

[118] *Ibid.*
[119] *Ibid*.
[120] *Ibid*.
[121] *Ibid*.
[122] N. O'CONNOR, «Reforming the U.S. Approach to Data Protection and Privacy» (2018), Council on Foreign Relations, *online:* <https://www.cfr.org/report/reforming-us-approach-data-protection> [Accessed 10 September 2024].
[123] A. FOLKS, «US State Privacy Legislation Tracker» (2024), IAPP Research Center, *online:* <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> [Accessed 10 September 2024].

surveillance purposes[124]. These factors impacted the US' capability to secure and maintain a stable data transfer mechanism with the EU. Three mechanisms have been progressively introduced to ensure personal data transfer from the EU to the US: (i) the Safe Harbor Agreement (2000), (ii) the Privacy Shield (2016)[125], and (iii) the Data Privacy Framework (EU-US DPF)[126]. For two times, the CJEU invalidated the adequacy decision adopted by the EU Commission to allow for a free transfer of personal data to selected US entities under the first two of these mechanisms. The US has gradually introduced measures to satisfy EU requirements, but one cannot speak of a spontaneous process of imitating EU law: it is rather a laborious exercise of limited convergence.

1. The Safe Harbor Agreement and the *Schrems I* case

The Safe Harbor was a set of privacy guidelines and standards established to facilitate the transfer of personal data between the EU and the US. It was designed mainly because the Data Protection Directive could restrict the EU-US commercial partnership[127]. This Agreement was certified as providing an adequate level of protection with a decision adopted by the European Commission in July 2000[128].

---

[124] See ex multis E. CELESTE, «The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios» (2019) 15:1, *European Constitutional Law Review, online:* <https://www.cambridge.org/core/journals/european-constitutional-law-review/article/court-of-justice-and-the-ban-on-bulk-data-retention-expansive-potential-and-future-scenarios/6FA1FB501FB00670DF8361CDD657FBC2> [Accessed 11 September 2024]; E. CELESTE AND F. FABBRINI, «Targeted Surveillance: Can Privacy and Surveillance Being Reconciled?» in S. CARRERA, D. CURTIN AND A. GEDDES (eds), *20 Year Anniversary of the Tampere Programme. Europeanisation Dynamics of the EU Area of Freedom, Security and Justice,* Italy, European University Institute, 2020; E. CELESTE AND G. FORMICI, «Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia» (2024) 25:3, *German Law Journal, online:* <https://www.cambridge.org/core/journals/german-law-journal/article/constitutionalizing-mass-surveillance-in-the-eu-civil-society-demands-judicial-activism-and-legislative-inertia/DED870C0CC8F43D6A8CDDC1923EB09CA> [Accessed 11 September 2024].

[125] EU, European Parliament, S. MONTELEONE AND L. PUCCIO, *From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU-US Data Transfer Rules,* January 2017, *online:* <https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf> [Accessed 10 September 2024].

[126] EU, European Commission, *Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, 10 July 2023, *online:* <https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj/eng> [Accessed 11 September 2024].

[127] D. GREER, «Safe Harbor—a Framework That Works» (2011) 1:3, *International Data Privacy Law*, *online:* <https://academic.oup.com/idpl/article-abstract/1/3/143/688691?redirectedFrom=fulltext> [Accessed 11 September 2024].

[128] EU, European Commission, *2000/520/EC: Commission Decision 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*, 26 July 2000, *online:* <https://eur-lex.europa.eu/eli/dec/2000/520/oj/eng> [Accessed 11 September 2024].

The Safe Harbor consists of seven core principles and fifteen Frequently Asked Questions (FAQs). The adherence to the principles was only supported by a self-certification mechanism[129]. After self-certifying adherence to the Safe Harbor principles, US companies could receive personal data from the EU without needing additional measures to legitimise the data transfer. Many critics of Safe Harbor, mainly regarding this self-certification mechanism, were concerned that it was only a «check the box» exercise and that there was no real oversight to guarantee the enforcement and respect for the principles[130]. Concerns grew after Edward Snowden's revelations in 2013, which led to a complaint filed before the Irish Data Protection Commission (DPC) and to the consequent invalidation of the agreement by the CJEU.

The case that invalidated the Safe Harbor Agreement is known as the «Schrems I» case[131]. It started with a complaint filed by Maximilian Schrems before the DPC, where he intended to prohibit Facebook Ireland from transferring his personal data to Facebook US since the US did not provide the same level of personal data protection as the EU, mainly because of potential surveillance activities[132]. The DPC rejected the complaint, and Schrems filed a lawsuit before the Irish High Court. The High Court then referred two questions to the CJEU for a preliminary ruling. The questions regarded whether the national DPAs are bound by an adequacy decision issued by the Commission about the level of data protection of a third country or if the DPAs can conduct independent investigations involving the international data transfer to a country that the Commission once considered with an adequate level of personal data protection[133]. Because of Schrems' arguments before the High Court, the CJEU also addressed the validity of the Safe Harbor adequacy decision.

In the 2015 judgement, the CJEU understood that the Commission did not provide concrete elements proving that the US had an adequate level of data protection under the requirements of Article 25(6) of the Data Protection Directive[134] and invalidated the Safe Harbor Agreement. The CJEU highlighted that the Safe Harbor adequacy decision gave margin to interferences by US national security authorities vis-a-vis the European fundamental right to respect private life[135]. The Court also considered the Commission's adequacy decision to limit the power of

[129] *Ibid.*
[130] *Ibid.*
[131] CJEU, *Maximillian Schrems v Data Protection Commissioner,* C-362/14 [2014].
[132] *Ibid.,* para 28.
[133] *Ibid.,* para 36.
[134] *Ibid.,* para 98.
[135] *Ibid,* para 86.

the DPAs regarding the possibility of them «taking action to ensure compliance with Article 25 of that directive» (i.e., transfers of personal data)[136].

2. The Privacy Shield and the *Schrems II* case

Not long after the Safe Harbor Agreement was invalidated, a new privacy framework was introduced in 2016: the Privacy Shield[137]. It was also based on seven core principles, similar to Safe Harbor. The self-certification approach remained the same in the new agreement, but three differences between these two transfer mechanisms are worth mentioning. The first concerns the Onward Transfer principle. Under the new rule, US organisations sharing EU personal data with third parties should ensure that such a third party provides the same level of data protection as stipulated in the Privacy Shield, regardless of whether the third party is an agent performing tasks on behalf and under the instructions of the organisation that first collected the data[138]. The second difference was the more robust oversight and enforcement mechanisms under the Privacy Shield. US organisations were subject to regular compliance checks by the US Department of Commerce. The Federal Trade Commission (FTC) played a more active role in monitoring and enforcing compliance, including bringing enforcement actions against non-compliant companies[139]. The third difference regarded the limitation imposed on the US Government to access EU personal data for surveillance. This included a commitment letter from the US Director of National Intelligence[140] and creating an oversight mechanism: the Privacy Shield Ombudsperson. This Ombudsperson would ensure that «individual complaints are properly investigated and addressed, and that individuals receive independent confirmation that U.S. laws have been complied with or, in case of a violation of such laws, the non-compliance has been remedied»[141].

---

[136] *Ibid,* para 101.
[137] EU, European Commission, *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, 12 July 2016, *online:* <https://eur-lex.europa.eu/eli/dec_impl/2016/1250/oj/eng> [Accessed 12 September 2024].
[138] Otava, «How Does Safe Harbor Compare to the EU-US Privacy Shield?» *OTAVA®*, (4 November 2019), *online:* <https://www.otava.com/reference/how-does-safe-harbor-compare-to-the-eu-us-privacy-shield/> [Accessed 10 September 2024].
[139] EU, European Commission, *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, *op. cit*.
[140] *Ibid.,* Annex VI.
[141] *Ibid.,* Introduction para 117.

Despite its differences from Safe Harbor, the Privacy Shield was also invalidated by the CJEU[142]. After Maximilian Schrems filed a new complaint before the DPC, this Authority brought an action before the Irish High Court, which made another reference for a preliminary ruling to the CJEU[143]. The case C-311/18 became known as «Schrems II».

The CJEU considered the Privacy Shield adequacy decision invalid because there was no equivalent level of data protection in the US compared to the EU. In the Court's view, the limitations on EU personal data protection regarding access and use of such data by US public authorities did not satisfy requirements «that are essentially equivalent to those required, under EU law»[144]. The CJEU also considered that the US did not provide adequate redress mechanisms for EU data subjects to ensure the exercising of their rights, which is fundamental in assessing the adequate level of data protection[145]. Even the Privacy Shield Ombudsperson mechanism was considered inadequate because it could not «provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent» to those provided in the EU legislation[146].

3. The Data Privacy Framework

In July 2023, the European Commission issued a Decision regarding a new transatlantic personal data transfer mechanism that US organisations can rely on without needing additional safeguards: the EU-US Data Privacy Framework (EU-US DPF)[147].

The new framework has many similarities to its predecessors, such as the self-certification approach, scope of application, and principles that US companies must commit to. However, there are also some changes worth mentioning. Firstly, despite the certification mechanism remaining the same, the US Department of Commerce commits to actually verify, «prior to finalizing an organization's initial self-certification or annual re-certification», whether an organisation complies with the framework's principles[148]. Secondly, following the Schrems II decision, the EU-US DPF provides more robust redress mechanisms to ensure the exercise of

---

[142] CJEU, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems,* C-311/18 [2020].
[143] *Ibid.,* para 57.
[144] *Ibid.,* para 185.
[145] *Ibid.,* paras 187-189.
[146] *Ibid.,* para 197.
[147] EU, European Commission, *Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, *op. cit*.
[148] *Ibid.,* p. 103.

EU data subjects' rights. The new framework states that US organisations must implement effective mechanisms to deal with data subjects' complaints. As a last resort, if the mechanisms adopted by organisations are unsuccessful, the EU data subject has the right to invoke an arbitration procedure by a new body called «EU-U.S. DPF Panel», consisting of 10 arbitrators appointed by the US Department of Commerce and the Commission[149]. Thirdly, the EU-US DPF tries to introduce more limitations and oversight regarding US national agencies accessing EU personal data, mainly for criminal law enforcement and national security purposes. Some additional safeguards are provided in this context, such as limitation on data retention periods and the obligation to keep documentation about processing activities for the abovementioned purposes[150]. However, it should be noted that very general safeguards are also mentioned, and it is unclear how they will be put in place and enforced.

Lastly, the EU-US DPF provides that the adequacy decision will be periodically revised, with the first revision occurring in July 2024[151]. The new framework also states that further reviews will be conducted, mainly where there are indications that (i) US organisations are not complying with the EU-US DPF principles and US authorities are not addressing measures to tackle this non-compliance; (ii) US public authorities are not complying with the conditions and limitations to access EU personal data, and (iii) complaints from EU data subjects are not being effectively addressed by US organisations[152]. In such cases, the Commission can initiate a procedure to suspend or repeal the adequacy decision.

Although it is currently in force, the EU-US DPF could be challenged before the CJEU. According to the Court in the *Schrems I* case, all acts of EU institutions can be reviewed, and the Commission's adequacy decisions «cannot escape such review»[153]. The competence for reviewing and eventually invalidating EU institutions' acts, including adequacy decisions, lies only with the CJEU[154].

VI. Conclusion

The GDPR has played a crucial role in data protection, strengthening the awareness and factual implementation of the duty to adequately manage and safeguard personal data within the EU

[149] *Ibid.,* p. 22.
[150] *Ibid.,* p. 45-46.
[151] Until the finishing of this article, no revisions of the EU-US DPF were found.
[152] *Ibid.,* p. 63.
[153] CJEU, *Maximillian Schrems v Data Protection Commissioner, op. cit.,* para. 60.
[154] *Ibid,* paras 61-62.

and beyond. This chapter has explored the GDPR's origins, objectives, and impact. Firstly, we traced the historical evolution from the concept of privacy to data protection, highlighting the foundational contributions of early legal thinkers such as Warren and Brandeis, whose advocacy for privacy rights laid the groundwork for modern data protection frameworks. This historical context illustrates how societal values surrounding privacy have evolved to shape an autonomous right to data protection, first through the establishment of national initiatives within the EU (e.g., Sweden and Germany), then through international instruments (e.g., Convention 108), and finally with the attempt of the EU to harmonise the data protection framework across its member states first with the Data Protection Directive and, subsequently, with a more robust legal instrument such as the GDPR.

Secondly, the chapter identified the core objectives of the GDPR, emphasising its commitment to empowering data subjects through enhanced rights and protections. Key innovations, such as the principles of accountability, data protection by design and by default, more stringent consent requirements, and the creation of new ones, reflect a proactive approach to data management that prioritises individual autonomy and transparency. These principles shift the burden of compliance onto organisations, requiring them to adhere to EU law actively and demonstrate their commitment to data protection.

Thirdly, we illustrated how the impact of the GDPR is not only limited to an increased regulatory coherence at the EU level but extends beyond the EU, influencing global data protection standards and prompting countries worldwide to reassess their privacy and data protection laws and practices. In summary, the GDPR represents a significant advancement in protecting personal data and addressing the complexities of a rapidly evolving technological landscape. Its emphasis on individual rights, organisational accountability, and global influence underscores its role as a cornerstone of the contemporary digital constitutionalism agenda[155]. As we continue to navigate the challenges posed by digital innovation, the principles enshrined in the GDPR will remain vital in ensuring that individual rights are upheld and respected, fostering a secure and trustworthy digital environment for all. The ongoing evolution of data protection legislation will continue to be shaped by the foundational principles established by the GDPR, guiding future efforts to balance innovation needs with the imperative of safeguarding privacy and personal data protection.

---

[155] E. CELESTE, «Digital Constitutionalism: A New Systematic Theorisation» (2019) 33:1, *International Review of Law*, Computers & Technology, *online:* <https://www.tandfonline.com/doi/abs/10.1080/13600869.2019.1562604> [Accessed 11 September 2024]; E. CELESTE AND G. D. GREGORIO, «Digital Humanism: The Constitutional Message of the GDPR», *op. cit*.