
This is the **published version** of the master thesis:

Viecelli, Bruna; Blasi Casagran, Cristina (tut.). *Transatlantic data transfers under the GDPR : Essential equivalence, adequacy, and the unresolved challenges of EU-US data flows*. (Universitat Autònoma de Barcelona), 2026 (Màster Universitari en Integració Europea). 41 pàg.

This version is available at <https://ddd.uab.cat/record/331588>

under the terms of the  license.



**MÁSTER UNIVERSITARIO EN
INTEGRACIÓN EUROPEA**

Curso 2025-2026

TRABAJO DE FIN DE MÁSTER

**Transatlantic Data Transfers under the GDPR:
Essential Equivalence, Adequacy, and the Unresolved
Challenges of EU–US Data Flows**

AUTHOR: BRUNA VIECELLI

TUTOR: Dra. CRISTINA BLASI CASAGRAN

UAB Campus, June 18, 2026

ABSTRACT:

This study examines the legal and constitutional framework governing transatlantic personal data transfers under European Union law. Using a doctrinal and analytical methodology, it traces the historical development of privacy and data protection, analyzes the European Union rights-based transfer regime under Directive 95/46/EC, the Charter of Fundamental Rights, and the General Data Protection Regulation, and evaluates the instability of EU–US transfer mechanisms through Safe Harbor, Privacy Shield, *Schrems II*, and the EU–US Data Privacy Framework. The study focuses on three central questions: the meaning of “essential equivalence,” the role of effective judicial protection in international transfers, and the extent to which the current DPF resolves the structural conflict between EU fundamental rights standards and US surveillance law. This study argues that the central weakness of the EU–US transfer regime is not merely the imperfect design of successive adequacy instruments, but the deeper attempt to reconcile EU constitutional standards with a US surveillance framework that remains structurally incompatible with the requirements of necessity, proportionality, independent supervision, and effective judicial protection. It concludes that the DPF, although formally operative and institutionally more developed than its predecessors, should not be understood as a satisfactory constitutional settlement, and that EU–US data flows should remain limited, strictly conditioned, and subject to renewed judicial scrutiny until substantive convergence on surveillance limits, accountability, and redress is achieved.

KEYWORDS:

Transatlantic data transfers; essential equivalence; *Schrems II*; adequacy; Data Privacy Framework.

INDEX:

INTRODUCTION.....	3
1. THE HISTORICAL AND NORMATIVE BACKGROUND OF TRANSATLANTIC DATA TRANSFERS.....	6
1.1 The emergence of privacy and data protection concerns in the international legal order.	6
1.2 The recognition of data protection as a fundamental right in European Union law.....	8
1.3 Digital globalization and the centrality of cross-border personal data flows.....	9
1.4 Early EU–US data transfers and the absence of a common regulatory framework.....	10
2. THE GDPR AND THE CONSTRUCTION OF A RIGHTS-BASED MODEL FOR INTERNATIONAL DATA TRANSFERS.....	11

2.1 The evolution of EU data protection law and the limits of pre-GDPR legislation.....	11
2.2 The GDPR as a response to technological change and regulatory fragmentation.....	13
2.3 The principle of an essentially equivalent level of protection.....	13
2.4 Adequacy, safeguards, and derogations as expressions of EU constitutional standards.	15
2.5 The extraterritorial reach of the GDPR and its implications for third countries.....	16
3. THE DATA TRANSFER REGIME BETWEEN THE EUROPEAN UNION AND THE UNITED STATES AND ITS STRUCTURAL FRAGILITIES.....	17
3.1 The Safe Harbor framework and its underlying assumptions.....	17
3.2 Schrems I and the judicial rejection of formal adequacy.....	18
3.3 The Privacy Shield framework and the persistence of structural incompatibilities.....	19
3.4 US surveillance law and the limits of executive and administrative safeguards.....	20
4. SCHREMS II AND THE UNRESOLVED CONFLICT BETWEEN FUNDAMENTAL RIGHTS AND TRANSATLANTIC DATA FLOWS.....	22
4.1 Schrems II and the requirement of effective judicial protection.....	22
4.2 The conditional validity of Standard Contractual Clauses after Schrems II.....	23
4.3 The later refinement of “essential equivalence” in CJEU jurisprudence.....	24
4.4 Legal uncertainty and the fragmentation of compliance mechanisms.....	26
5. THE EU–US DATA PRIVACY FRAMEWORK AND THE PERSISTENCE OF THE ADEQUACY DILEMMA.....	27
5.1 The EU–US Data Privacy Framework as a new adequacy attempt.....	27
5.2 Risks of renewed judicial invalidation and regulatory instability.....	29
5.3 Possible normative paths toward a more sustainable transatlantic data transfer regime.	33
CONCLUSIONS.....	34
BIBLIOGRAPHY.....	36

INTRODUCTION

The digitalization of economic, social, and governmental activity has intensified the cross-border circulation of personal data and, with it, the legal problems associated with privacy, surveillance, and the protection of fundamental rights in networked environments.¹

Within that setting, the European Union has developed a particularly dense regime of personal data protection. The General Data Protection Regulation, adopted in 2016 and applicable since 25 May 2018, consolidated a rights-based model of digital governance designed both to respond to technological change and to preserve a high level of protection

¹ Kuner, Christopher. 2015. “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, *International Data Privacy Law*, vol. 5, n.º 4, pp. 235-245, especially pp. 235-236; Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2020, p. 18.

for personal data under conditions of globalization.²

International data transfers occupy a central place in that model. Although the GDPR facilitates the free movement of personal data within the internal market, it subjects transfers to third countries to conditions intended to ensure that the protection guaranteed under European Union law is not undermined once data leave Union territory.³

Those tensions are especially visible in the transatlantic relationship, as EU–US data flows have long been operationally indispensable to the digital economy, yet legally unstable, given the contrast between the EU’s comprehensive rights-based framework and the United States’ fragmented approach to privacy, combined with extensive intelligence-gathering powers under US law.⁴

Schwartz and Peifer describe the transatlantic divide as a contrast between an EU model structured around rights-bearing data subjects and a US model more closely connected to marketplace discourse, consumer protection, and sectoral intervention.⁵ That instability found its clearest expression in the case law of the Court of Justice of the European Union. In *Schrems I* and *Schrems II*, the Court invalidated Safe Harbor and Privacy Shield on the ground that they failed to secure a level of protection essentially equivalent to that required by EU law, particularly in light of the Charter of Fundamental Rights and the requirement of effective judicial protection.⁶

The EU–US Data Privacy Framework, adopted in 2023, represents the most recent attempt to restore stability to those transfers. Yet the concerns that undermined earlier arrangements

² 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, OJ L 119, 4 May 2016; Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, Tese de Doutoramento, Universidade Nova de Lisboa, Lisboa, 2018, pp. 92-93.

³ Regulation (EU) 2016/679, cit., arts. 44-49; Kuner, Christopher, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, cit., p. 236.

⁴ Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da, *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, cit., p. 155; Kuner, Christopher, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, cit., p. 236.

⁵ Schwartz, Paul M.; Peifer, Karl-Nikolaus. 2017. “Transatlantic Data Privacy Law”, *Georgetown Law Journal*, vol. 106, n.º 1, pp. 115-180.

⁶ Court of Justice of the European Union. *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, Judgment of 6 October 2015; Court of Justice of the European Union. *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, Case C-311/18, Judgment of 16 July 2020.

have not disappeared, as reflected in the reservations expressed by the European Data Protection Board, the continuing review of the framework, and the persistence of broader doctrinal controversy concerning surveillance, redress, and essential equivalence.⁷

This study adopts a doctrinal and analytical methodology. By doctrinal methodology, it understands the systematic interpretation of legal norms, institutional acts, and judicial decisions in order to determine the content, scope, and limits of the EU legal regime governing international transfers of personal data. The primary sources examined are Directive 95/46/EC, the GDPR, the Charter of Fundamental Rights of the European Union, Commission adequacy decisions, the case law of the Court of Justice and the General Court, and institutional materials issued by the EDPB, the EDPS, and the Article 29 Working Party. US legal instruments, including FISA 702, Executive Order 12333, Executive Order 14086, and the regulations establishing the Data Protection Review Court, are considered only insofar as they are relevant to the EU adequacy assessment.⁸

The analysis is also supported by selected academic doctrine, but doctrine is not treated as a substitute for the legal materials themselves. The study does not provide an empirical assessment of corporate compliance practices, nor a full account of US constitutional or intelligence law. Its more limited contribution is to argue that the central defect of the

⁷ 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-U.S. Data Privacy Framework, OJ L 231, 20 September 2023; European Data Protection Board. *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-U.S. Data Privacy Framework*, adopted on 28 February 2023; European Data Protection Board. *Report on the first review of the European Commission Implementing Decision on the adequate level of protection of personal data under the EU-U.S. Data Privacy Framework*, adopted on 4 November 2024; General Court of the European Union. *Philippe Latombe v European Commission*, Case T-553/23, Judgment of 3 September 2025; Murphy, Maria Helen. 2022. “Assessing the Implications of Schrems II for EU-US Data Flow”, *International and Comparative Law Quarterly*, vol. 71, n.º 1, pp. 245-262; Batlle, Sergi; van Waeyenberge, Arnaud. 2024. “EU-US Data Privacy Framework: A First Legal Assessment”, *European Journal of Risk Regulation*, vol. 15, n.º 1, pp. 191-200.

⁸ 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, OJ L 281, 23 November 1995; Regulation (EU) 2016/679, cit.; Charter of Fundamental Rights of the European Union, OJ C 326, 26 October 2012; Court of Justice of the European Union, *Schrems*, Case C-362/14, cit.; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit.; General Court of the European Union, *Latombe v Commission*, Case T-553/23, cit.; European Data Protection Board, *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-U.S. Data Privacy Framework*, cit.; Article 29 Data Protection Working Party. *Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, WP 238, adopted on 13 April 2016; European Data Protection Supervisor. *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, 30 May 2016; Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a; Executive Order 12333 of 4 December 1981, “United States Intelligence Activities”, 46 Fed. Reg. 59941, 8 December 1981; Executive Order 14086 of 7 October 2022, “Enhancing Safeguards for United States Signals Intelligence Activities”, 87 Fed. Reg. 62283, 14 October 2022; United States Department of Justice. Data Protection Review Court, 28 C.F.R. Part 201.

EU–US transfer regime is structural rather than merely technical: an executive-based, largely secret, and *ex post* remedial architecture cannot fully compensate for a surveillance framework that continues to place non-US persons in a constitutionally weaker position than EU law permits.⁹

1. THE HISTORICAL AND NORMATIVE BACKGROUND OF TRANSATLANTIC DATA TRANSFERS

1.1 The emergence of privacy and data protection concerns in the international legal order

The protection of privacy has long occupied a significant place in international human rights law, even before the emergence of a distinct vocabulary of data protection. Although the earliest instruments did not yet speak in the language of algorithmic processing, automated profiling, or cross-border infrastructures, they articulated principles that later became indispensable to modern data protection law. The contemporary law of personal data therefore did not arise from an entirely new normative field, but from an older concern with shielding individuals against unjustified intrusions into private life, even as data protection later acquired autonomy as a distinct legal field.¹⁰

That concern appears already in the foundational texts. Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights protect individuals against arbitrary or unlawful interference with privacy, family, home, and correspondence. Although these provisions did not anticipate the technological environment in which personal data are now collected, aggregated, retained, exported, and reused, the Human Rights Committee later clarified that privacy protection extends to surveillance, the collection of personal information, and forms of automated processing, thereby giving classical privacy a clearer connection with contemporary data

⁹ Zalnieriute, Monika. 2022. “Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security”, *Vanderbilt Journal of Transnational Law*, vol. 55, n.º 1, pp. 1-74; Rotenberg, Marc. 2020. “Schrems II, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection”, *European Law Journal*, vol. 26, n.º 1-2, pp. 141-152; Tzanou, Maria; Vogiatzoglou, Plixavra. 2023. “In Search of Legal Certainty Regarding ‘Effective Redress’ in International Data Transfers: Unpacking the Conceptual Complexities and Clarifying the Substantive Requirements”, *Review of European Administrative Law*, vol. 16, n.º 1, pp. 11-30; Docksey, Christopher. 2023. “Government Access to Personal Data and Transnational Accountability”, *Oslo Law Review*, vol. 10, n.º 1.

¹⁰United Nations. Universal Declaration of Human Rights, adopted 10 December 1948, art. 12; United Nations. International Covenant on Civil and Political Rights, adopted 16 December 1966, entered into force 23 March 1976, art. 17; Lynskey, Orla. *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015.

governance.¹¹

During the second half of the twentieth century, conceptions of privacy organized around home, correspondence, and communicative intrusion encountered new risks generated by computerized databases and automated information systems. The 1973 American report *Records, Computers and the Rights of Citizens* captured that shift by treating computerized records not merely as instruments of administrative efficiency, but as a transformation in institutional power over the individual, requiring fair information practices capable of limiting abuse and restoring a measure of control to data subjects.¹²

Doneda's account of the "generations" of data protection law is useful because it shows that data protection did not emerge through a single legislative breakthrough, but through successive responses to changing technological and institutional risks. The field moved from early concern with centralized public-sector databases toward private-sector processing, transparency, participation by the data subject, and eventually the recognition that personal data could no longer be regulated within purely domestic borders.¹³

In parallel with national developments, international organizations began to formulate more systematic responses. The OECD Privacy Guidelines of 1980 articulated influential principles such as purpose limitation, use limitation, security safeguards, openness, and individual participation, while expressly linking privacy protection to transborder data flows. Convention 108 then gave binding international form to many of those principles, including data quality, purpose specification, security, access, rectification, and remedies, while also recognizing that transborder flows should remain legitimate only insofar as they did not become vehicles for circumventing protection.¹⁴

¹¹ Directive 95/46/EC, cit., art. 1; Kuner, Christopher, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law", cit., pp. 235-245, especially pp. 236-237; Council of Europe, Convention 108, cit., art. 12; Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, cit., pp. 11-14.

¹² United States Department of Health, Education, and Welfare. *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, Washington, D.C., 1973.

¹³ Doneda, Danilo. 2011. "A proteção dos dados pessoais como um direito fundamental", *Espaço Jurídico Journal of Law*, vol. 12, n.º 2, pp. 91-108.

¹⁴ Organisation for Economic Co-operation and Development. *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, 1980; Organisation for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, 2002; Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, Strasbourg, 28 January 1981, arts. 5-10 and Chapter III; Council of Europe, Convention 108, cit., art. 12; Office of the United Nations High Commissioner for Human Rights. *The*

1.2 The recognition of data protection as a fundamental right in European Union law

Within the European legal order, the protection of personal data did not begin as a fully constitutional concept, instead it became one. That transformation is central to the law of international transfers because it explains why the movement of personal data outside the Union is treated not merely as a commercial or administrative operation, but as a matter capable of affecting the substance of fundamental rights.¹⁵

Directive 95/46/EC marked the first comprehensive attempt to organize EU data protection law around both fundamental-rights protection and internal-market integration. It created a shared legal vocabulary, introduced concrete rights, obligations, supervisory mechanisms, and transfer conditions, and placed international transfers within a structured legal framework. Article 25 was especially important because it allowed transfers to third countries only where an adequate level of protection was ensured, thereby making clear that EU protection should not disappear once personal data crossed a territorial border.¹⁶

The constitutional status of data protection was strengthened with the Charter of Fundamental Rights of the European Union. Article 7 protects respect for private and family life, home, and communications, while Article 8 recognizes the protection of personal data as a distinct fundamental right, linked to fairness, specified purposes, legal basis, access, rectification, and independent supervision.¹⁷

Lynskey and Hijmans help clarify the constitutional significance of that development: EU data protection law became a distinct regulatory and constitutional field, and the Union's role in this area came to involve not only market regulation, but also the protection of a fundamental right in the digital environment.¹⁸

Right to Privacy in the Digital Age, U.N. Doc. A/HRC/31/64, Geneva, 3 February 2016.

¹⁵ Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da, *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, cit., pp. 92-93.

¹⁶ 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, OJ L 281, 23 November 1995, art. 1; Kuner, Christopher, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law", cit., pp. 235-245, especially pp. 236-237; Council of Europe, Convention 108, cit., art. 12; Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, cit., pp. 11-14.

¹⁷ Charter of Fundamental Rights of the European Union, cit., arts. 7-8.

¹⁸ Lynskey, Orla, *The Foundations of EU Data Protection Law*, cit.; Hijmans, Hielke, *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU*, Springer, Cham, 2016.

Once personal data protection was constitutionalized, questions that might otherwise have been treated as regulatory or administrative became constitutional questions. That shift explains the strictness of the Court of Justice in the *Schrems* line of cases, where the Court insisted that international transfer mechanisms must comply not only with secondary legislation, but also with Articles 7, 8, and 47 of the Charter.¹⁹

Against that backdrop, the GDPR appears less as an abrupt beginning than as the culmination of a longer constitutional and regulatory trajectory. By replacing Directive 95/46/EC, strengthening enforcement, and projecting EU standards more clearly beyond Union territory, it deepened a framework whose constitutional foundations had already been laid.²⁰

1.3 Digital globalization and the centrality of cross-border personal data flows

Digital globalization transformed both the scale of personal data processing and its legal significance. Internet services, cloud infrastructures, platforms, mobile ecosystems, and data-driven business models made the continuous transfer of personal information across jurisdictions routine, often without the data subject perceiving that territorial movement had occurred. In that environment, personal data became a strategic resource of the global economy, used to provide services, coordinate internal operations, personalize interfaces, outsource storage, manage risk, refine advertising systems, train computational models, and expand across markets²¹

The legal difficulty is intensified by the fact that EU and US law do not always conceptualize the protected object in the same way. Schwartz and Solove show that the European notion of personal data and the American category of personally identifiable information rest on different assumptions about identifiability, risk, and regulatory

¹⁹ Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da, *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, cit., p. 92; Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 91-95; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 168-176.

²⁰ Regulation (EU) 2016/679, cit., art. 1; Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da, *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, cit., pp. 92-93.

²¹ Kuner, Christopher, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, cit., pp. 235-236; Bradford, Anu, *The Brussels Effect: How the European Union Rules the World*, cit., p. 18.

intervention.²²

For that reason, the regulation of international transfers has become one of the most delicate problems in contemporary data protection law. Cross-border transfers sit at the intersection of data protection, trade, and national security, since what appears to be a private transfer between companies may expose the individual to the public-law powers of the destination state. The European Union's response has been to insist that protection must travel with the data themselves, so that transfers outside the Union remain conditional upon mechanisms capable of preserving the level of protection guaranteed by EU law, particularly in light of Articles 7, 8, and 47 of the Charter.²³

Within this broader landscape, the EU–US relationship occupies a particularly prominent position. The two digital economies are deeply connected, and a substantial portion of personal data generated in Europe has long been processed, stored, or made accessible in the United States; yet the European and American legal traditions evolved very differently in their treatment of privacy, data protection, surveillance, and remedies.²⁴

1.4 Early EU–US data transfers and the absence of a common regulatory framework

The early development of transatlantic data transfers took place under conditions of evident regulatory asymmetry. On the European side, personal data protection was progressively shaped as a general legal framework closely tied to privacy, dignity, and individual rights. On the American side, by contrast, privacy regulation developed through a more fragmented combination of sectoral statutes, consumer protection enforcement, and self regulatory commitments, without consolidating into a comprehensive federal data protection regime comparable to that of the European Union.²⁵

²² Schwartz, Paul M.; Solove, Daniel J. 2014. “Reconciling Personal Information in the United States and European Union”, *California Law Review*, vol. 102, pp. 877-916.

²³ Kuner, Christopher, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, cit., p. 236; Directive 95/46/EC, cit., art. 25; Regulation (EU) 2016/679, cit., arts. 44-49; Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 72-74; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 168-176.

²⁴ Kuner, Christopher, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, cit., p. 236; Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da, *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, cit., p. 155.

²⁵ Kuner, Christopher, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, cit., p. 236; Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da, *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, cit., p. 155; Schwartz, Paul M.; Peifer, Karl-Nikolaus, “Transatlantic Data Privacy Law”, cit.

This divergence reflected, at a deeper level, a distinct legal imagination, and this contrast became especially consequential once EU law linked international transfers to the existence of an adequate level of protection in the destination country. While European data protection law proceeded on the assumption that the processing of personal information by both public and private actors required general rules and rights-based constraints, the United States addressed privacy concerns in a more compartmentalized way, through specific interventions rather than a unified normative structure.²⁶

The divergence also appears at the level of the protected object. Whereas EU law adopts a broad concept of personal data, US law has traditionally relied more heavily on narrower and more context-dependent categories of personally identifiable information, a difference that complicates any claim of straightforward regulatory equivalence.²⁷

Article 25 of Directive 95/46/EC transformed that divergence into a legal problem for transfers. The Commission could recognize a third country as adequate only where its legal order preserved protection sufficiently compatible with EU standards; yet the United States' technological centrality made transatlantic transfers practically indispensable even though its fragmented privacy model did not map neatly onto the comprehensive rights-based framework contemplated by EU law.²⁸

Safe Harbor was the pragmatic response to that dilemma. Rather than requiring full legislative convergence, it relied on voluntary certification by participating US companies to privacy principles recognized by the European Commission.²⁹

2. THE GDPR AND THE CONSTRUCTION OF A RIGHTS-BASED MODEL FOR INTERNATIONAL DATA TRANSFERS

2.1 The evolution of EU data protection law and the limits of pre-GDPR legislation

²⁶ Directive 95/46/EC, cit., art. 25; Kuner, Christopher, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law", cit., p. 236.

²⁷ Schwartz, Paul M.; Solove, Daniel J., "Reconciling Personal Information in the United States and European Union", cit.

²⁸ Directive 95/46/EC, cit., art. 25; Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da, *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, cit., p. 155; Kuner, Christopher, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law", cit., p. 236.

²⁹ Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the United States Department of Commerce, OJ L 215, 25 August 2000.

The EU architecture governing international transfers did not begin with the GDPR. It developed through a longer process of legislative accumulation, institutional adjustment, and normative deepening, through which the Union moved from minimum harmonization and differentiated national implementation toward a more integrated, directly applicable, and constitutionally denser regime.³⁰

Directive 95/46/EC established the first comprehensive EU framework for data protection, defining central notions such as personal data, controller, processing, and recipient, while linking fundamental-rights protection to the free movement of personal data within the internal market. It also treated international transfers as a core data protection problem: Article 25 required that personal data be transferred only to third countries ensuring an adequate level of protection, thereby affirming that the protective logic of EU law should not disappear once data crossed the Union's territorial borders.³¹

The Directive's limits became increasingly visible over time. Its dependence on national implementation produced uneven interpretation, supervisory practice, procedural requirements, and enforcement intensity, while its 1995 architecture was increasingly strained by social media platforms, large-scale cloud outsourcing, mobile applications, behavioral advertising, and data-intensive infrastructures. By the early 2010s, reform had become difficult to postpone, since EU law needed a regime capable of reducing fragmentation, strengthening enforceability, and preserving protection in a transnational digital environment.³²

The GDPR, adopted in 2016, marked that shift. As a regulation, it became directly applicable in all Member States, strengthening harmonization, reducing interpretive divergence, and seeking to ensure that data subjects throughout the Union would enjoy a more consistent level of protection.³³

³⁰ Directive 95/46/EC, cit.; Regulation (EU) 2016/679, cit., arts. 44-49.

³¹ Directive 95/46/EC, cit.

³² Regulation (EU) 2016/679, cit., recitals 6-13; Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da, *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, cit., p. 93; Bradford, Anu, *The Brussels Effect: How the European Union Rules the World*, cit., p. 18.

³³ Regulation (EU) 2016/679, cit.; Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da, *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, cit., p. 93.

2.2 The GDPR as a response to technological change and regulatory fragmentation

The GDPR was designed to respond simultaneously to technological transformation and to the fragmentation that had characterized the era of Directive 95/46/EC. These two problems were closely connected: the more personal data circulated across services, devices, jurisdictions, corporate groups, and technical infrastructures, the less adequate it became to govern them through uneven national implementation. At the same time, platforms, analytical tools, and machine-learning techniques expanded the capacity of public and private actors to collect, cross-reference, retain, and exploit personal information, making the legal challenge both quantitative and qualitative.³⁴

The GDPR responded by articulating a more demanding architecture of principles, rights, and obligations. Article 5 requires processing to comply with lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. The Regulation also strengthened rights of access, rectification, erasure, portability, transparency, and objection, while requiring controllers and processors not merely to comply with the Regulation, but to demonstrate compliance through documentation, technical design, risk assessment, and supervisory engagement.³⁵

The Regulation also responded directly to the territorial mismatch that increasingly characterizes digital activity. Article 3 extends the GDPR to controllers and processors established outside the Union where they offer goods or services to individuals in the Union or monitor their behavior there.³⁶ As Kuner observes, from the perspective of international transfer law, extraterritoriality becomes difficult to avoid once rights based protection and globalized processing are placed within the same legal frame.³⁷

2.3 The principle of an essentially equivalent level of protection

One of the most significant doctrinal developments in the European Union law of

³⁴ Regulation (EU) 2016/679, cit., recitals 6-13; Lynskey, Orla, *The Foundations of EU Data Protection Law*, cit.

³⁵ Regulation (EU) 2016/679, cit., art. 3; Kuner, Christopher, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, cit., pp. 237-239.

³⁶ Regulation (EU) 2016/679, cit., art. 3.

³⁷ Kuner, Christopher, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, cit., pp. 237-239.

international transfers is the principle that personal data transferred outside the Union must continue to enjoy a level of protection that is essentially equivalent to that guaranteed under EU law. Although the General Data Protection Regulation itself speaks primarily in terms of adequate protection in Article 45, the more precise standard of essential equivalence was developed and clarified through the case law of the Court of Justice, most decisively in *Schrems*.³⁸

This standard should not be understood as a requirement of formal duplication. The Court did not require third countries to reproduce the GDPR article by article, nor to organize their institutions in the same way as the European Union; it required protection comparable in substance and effectiveness. If EU law treats data protection as a fundamental right, adequacy cannot be reduced to institutional resemblance, but must preserve the substance of that right under conditions of external transfer.³⁹

That inquiry is inseparable from the Charter of Fundamental Rights, and the Court has repeatedly insisted that international data transfers must not undermine Articles 7 and 8 of the Charter, which protect private life and personal data, nor Article 47, which guarantees effective judicial protection.⁴⁰

Once the test is framed in Charter terms, the legality of an international transfer mechanism depends not only on private commitments or supervisory language on paper, but also on the broader public-law environment of the destination state, including surveillance powers, necessity and proportionality, and access to remedies effective in law and in practice. This became especially clear in the EU–US context, where the central difficulty concerned the insufficiency of safeguards and redress mechanisms available to EU data subjects.⁴¹

This became especially clear in later critiques of the transfer framework between the European Union and the United States, where the central difficulty concerned the fact that

³⁸ Regulation (EU) 2016/679, cit., art. 45; Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 72-74.

³⁹ Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 72-74; Hijmans, Hielke, *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU*, cit.

⁴⁰ Charter of Fundamental Rights of the European Union, cit., arts. 7, 8 and 47; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 168-176.

⁴¹ Charter of Fundamental Rights of the European Union, cit., arts. 7, 8 and 47; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 121-147, 168-185 and 191-197.

the safeguards and redress mechanisms available to EU data subjects did not satisfy the standards of effective judicial protection that EU law treats as fundamental.⁴²

It is precisely because essential equivalence is a substantive standard, and not merely a comparative metaphor, that it later destabilized both Safe Harbor and Privacy Shield. Once the Court connected adequacy to the practical preservation of Charter rights, the space for formal, diplomatic, or institutionally optimistic solutions became considerably narrower.⁴³

2.4 Adequacy, safeguards, and derogations as expressions of EU constitutional standards

The General Data Protection Regulation structures international transfers through a layered framework composed of adequacy decisions, appropriate safeguards, and exceptional derogations.⁴⁴ That framework should be understood as the legal expression of a broader constitutional commitment according to which personal data may continue to circulate internationally only under conditions that preserve the substance of the rights attached to them.

At the highest level stand adequacy decisions under Article 45. Through such decisions, the Commission may determine that a third country, territory, sector, or international organization ensures an adequate level of protection, allowing transfers to proceed without additional authorization. That assessment must consider the rule of law, respect for fundamental rights, relevant legislation, independent supervision, and effective administrative and judicial redress for data subjects.⁴⁵

Where no adequacy decision exists, Article 46 permits transfers on the basis of appropriate safeguards, including Standard Contractual Clauses, Binding Corporate Rules, approved codes of conduct, and certification mechanisms. These instruments are indispensable to ordinary cross-border flows, but *Schrems II* made clear that contractual commitments cannot by themselves neutralize incompatible powers of public authorities in the

⁴² Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 168-185 and 191-197.

⁴³ Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 72-74; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 168-176.

⁴⁴ Regulation (EU) 2016/679, cit., arts. 44-49.

⁴⁵ Regulation (EU) 2016/679, cit., art. 45.

destination state.⁴⁶

Article 49 retains a narrow set of derogations, including explicit consent and necessity for the performance of a contract. Their exceptional character reinforces the general logic of the system: derogations are not an alternative transfer regime, but limited exceptions for specific circumstances.⁴⁷

Read as a whole, Articles 44 to 49 reveal that the law of international transfers occupies a central position within the EU data protection regime. It is one of the points at which the Union's constitutional commitment to privacy, personal data protection, and effective redress is translated into operational legal categories.⁴⁸

2.5 The extraterritorial reach of the GDPR and its implications for third countries

One of the most distinctive features of the GDPR is its explicit extraterritorial scope. Article 3 applies the Regulation to controllers and processors established within the Union, and also to those established outside it where they offer goods or services to individuals in the Union or monitor their behavior there. In a digital environment defined by border-crossing infrastructures, the protection of rights cannot depend solely on the formal location of establishment.⁴⁹

The limits of this extraterritorial projection have been emphasized by Greze, who argues that the GDPR's reach beyond EU territory raises a genuine enforcement problem rather than a merely theoretical question of jurisdiction. That observation matters for international transfers because it shows why the Union cannot rely solely on the extraterritorial application of its own rules.⁵⁰ Chapter V mechanisms remain necessary precisely because EU law may project standards outward more easily than it can enforce them abroad.

The global influence of the GDPR is visible in the way non-EU organizations adapt their

⁴⁶ Regulation (EU) 2016/679, cit., art. 46; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 121-134.

⁴⁷ Regulation (EU) 2016/679, cit., art. 49.

⁴⁸ Regulation (EU) 2016/679, cit., arts. 44-49; Charter of Fundamental Rights of the European Union, cit., arts. 7, 8 and 47.

⁴⁹ Regulation (EU) 2016/679, cit., art. 3; Greze, Benjamin, "The extra-territorial enforcement of the GDPR", cit.

⁵⁰ Greze, Benjamin, "The extra-territorial enforcement of the GDPR", cit.

processing practices to retain access to the European market. Yet that external influence does not make the transfer regime secondary. On the contrary, once personal data are processed through infrastructures that do not respect territorial neatness, the conditions under which data move to third countries become central to global digital governance.⁵¹

That is the setting in which the transatlantic transfer regime evolved. The real problem was whether personal data could flow from Europe to the United States without exposing EU data subjects to a legal environment insufficiently constrained by the standards of necessity, proportionality, independent supervision, and effective redress that EU law treats as fundamental.⁵²

3. THE DATA TRANSFER REGIME BETWEEN THE EUROPEAN UNION AND THE UNITED STATES AND ITS STRUCTURAL FRAGILITIES

3.1 The Safe Harbor framework and its underlying assumptions

The regulation of transatlantic data transfers has long been shaped by the structural mismatch between the European and American approaches to privacy and data protection. While the European legal order gradually constructed a comprehensive framework grounded in general principles, independent supervision, and enforceable rights, the United States relied on a more sectoral model, combining consumer protection, administrative enforcement, and firm-level commitments in the absence of a single comprehensive federal data protection statute.⁵³

Once Directive 95/46/EC made adequate protection a condition for transfers to third countries, the absence of a generally adequate US framework became a practical and legal problem. Safe Harbor, adopted through Commission Decision 2000/520/EC, attempted to resolve that problem through voluntary self-certification by participating US companies, backed by Department of Commerce administration and Federal Trade Commission

⁵¹ Bradford, Anu, *The Brussels Effect: How the European Union Rules the World*, cit.; Kuner, Christopher, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, cit.

⁵² Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 168-185; European Data Protection Board. Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020.

⁵³ Kuner, Christopher, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, cit.

enforcement.⁵⁴

That model was attractive because it avoided full legislative convergence while preserving economically necessary transatlantic flows. Its weakness, however, lay in the fact that private commitments could not fully answer the public-law implications of US surveillance powers.⁵⁵

The difficulty, therefore, lay in the fact that Safe Harbor attempted to resolve a systemic problem through a partial and administratively mediated workaround. So long as the rights of EU data subjects depended on corporate conduct as well as on the broader legal environment of the United States, especially in relation to public access to data, the arrangement remained exposed to a deeper kind of challenge.⁵⁶

3.2 *Schrems I* and the judicial rejection of formal adequacy

That deeper challenge emerged after the Snowden revelations, which brought renewed attention to the scale of US intelligence access to electronic communications. The legal question was no longer only whether participating companies complied with Safe Harbor principles, but whether the US legal environment itself allowed interferences with EU fundamental rights that were incompatible with the adequacy standard.⁵⁷

Against that background, Maximilian Schrems challenged the transfer of his Facebook data from Ireland to the United States, arguing that the Safe Harbor arrangement did not, in fact, provide adequate protection because US law permitted broad governmental access to data without sufficient safeguards or judicial remedies.⁵⁸ The dispute ultimately reached the Court of Justice, which used the case to assess the Commission decision and to restate, with considerable clarity, the constitutional boundaries of European Union transfer law.

⁵⁴ Directive 95/46/EC, cit., art. 25; Commission Decision 2000/520/EC, cit.

⁵⁵ Commission Decision 2000/520/EC, cit.; Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 86-88.

⁵⁶ Commission Decision 2000/520/EC, cit.; Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 86-88; Schwartz, Paul M.; Peifer, Karl-Nikolaus, “Transatlantic Data Privacy Law”, cit.

⁵⁷ Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da, *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, cit., p. 155; Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 26-30.

⁵⁸ Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 28-30.

In its 2015 judgment, the Court invalidated Safe Harbor because the Commission had failed to establish that the United States ensured a level of protection essentially equivalent to that guaranteed within the Union. The Court emphasized that access by public authorities to personal data must be limited by clear and precise rules, and that individuals must have access to effective legal remedies.⁵⁹

Schrems I can therefore be read as the moment in which the Court made explicit that adequacy under EU law cannot be satisfied by a diplomatic arrangement or a corporate compliance framework if the surrounding legal system permits disproportionate state access to personal data.⁶⁰

The judgment also has to be read against the post-Snowden context. Rotenberg emphasizes that the transatlantic dispute exposed not merely weaknesses in a particular adequacy decision, but the absence in the United States of a comprehensive privacy framework, an independent data protection authority, and stronger rights for foreign persons affected by surveillance.⁶¹

The judgment was, in this sense, a judicial refusal to accept form in place of substance, since the Commission's assessment of Safe Harbor as sufficient could not survive scrutiny once the Charter was treated as the relevant constitutional frame.⁶²

The invalidation of Safe Harbor disrupted transatlantic data flows and made clear that adequacy under EU law could not rest on formal institutional assurances where the structure of the third-country legal order failed to preserve the substance of Charter rights.⁶³

3.3 The Privacy Shield framework and the persistence of structural incompatibilities

⁵⁹ Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 90-95.

⁶⁰ Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 90-95.

⁶¹ Rotenberg, Marc. 2020. "Schrems II, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection", *European Law Journal*, vol. 26, n.º 1-2, pp. 141-152.

⁶² Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 91-95.

⁶³ Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 72-74 and 90-95; Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da, *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, cit., p. 155.

Privacy Shield was adopted as the political and legal successor to Safe Harbor, but it preserved the same basic architecture: participating US companies committed to privacy principles, while the Commission treated the framework as providing an adequate level of protection. The arrangement added written assurances, oversight commitments, and an Ombudsperson mechanism, yet it still depended on the assumption that an adequacy framework could stabilize transfers without requiring deeper convergence in US surveillance law.⁶⁴

Nevertheless, doubts emerged almost immediately, and the Article 29 Data Protection Working Party, in Opinion 01/2016, welcomed certain improvements but criticized the draft Privacy Shield decision for its lack of clarity, insufficient safeguards in relation to onward transfers, and unresolved issues concerning mass surveillance and redress.⁶⁵ The European Data Protection Supervisor voiced similar concerns in Opinion 4/2016, emphasizing that the arrangement still left significant uncertainty as to whether data transferred to the United States would be protected against disproportionate access by public authorities and whether the available redress architecture satisfied EU constitutional expectations.⁶⁶

Those reservations show that the problems later identified in *Schrems II* were visible from the beginning. The question was whether the broader US legal environment, especially Section 702 FISA, Executive Order 12333, and the intelligence-collection framework, had changed sufficiently to satisfy EU constitutional standards. Because Privacy Shield did not fundamentally alter those surveillance powers, and because the Ombudsperson model remained vulnerable from the standpoint of independent judicial protection, the framework was juridically fragile from the start.⁶⁷

⁶⁴ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1 August 2016.

⁶⁵ Article 29 Data Protection Working Party. Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision, WP 238, adopted on 13 April 2016.

⁶⁶ European Data Protection Supervisor. Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision, 30 May 2016.

⁶⁷ Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, cit.; European Data Protection Supervisor, *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, cit.; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 180-197; Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a; Privacy and Civil Liberties Oversight Board. *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Washington, D.C., 2 July 2014; Executive Order 12333, cit.; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 180-185.

3.4 US surveillance law and the limits of executive and administrative safeguards

At the heart of the transatlantic conflict lies the structure of United States surveillance law, together with the absence of a comprehensive federal privacy statute comparable to the European model. In practical terms, this means that the legality of transfers between the European Union and the United States cannot be evaluated solely by examining private sector obligations. It also requires attention to the public-law framework governing access by US authorities to personal data once those data are transferred to, stored in, or otherwise made available through infrastructures subject to US legal control.⁶⁸

Section 702 of the Foreign Intelligence Surveillance Act is among the most significant instruments in this regard. It authorizes the targeting of non-US persons reasonably believed to be located outside the United States for foreign intelligence purposes, and has served as the legal basis for major collection programs involving access to electronic communications.⁶⁹ Executive Order 12333, meanwhile, governs a broader range of intelligence activities conducted outside the United States, including activities affecting communications in transit, and has therefore occupied an important place in European concerns regarding data transfers and state access.⁷⁰

After the Snowden disclosures, the United States adopted measures intended to respond to criticism, including Presidential Policy Directive 28 and the Judicial Redress Act of 2015. These reforms were not irrelevant, but the central European concern remained whether they cured the underlying defects from the standpoint of necessity, proportionality, and effective judicial protection under EU fundamental-rights law.⁷¹

From the perspective of EU law, the difficulty was twofold. First, surveillance powers had

⁶⁸ Schwartz, Paul M.; Peifer, Karl-Nikolaus, “Transatlantic Data Privacy Law”, cit.; Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a; Executive Order 12333, cit.; Swire, Peter. U.S. Surveillance Law, Safe Harbor, and Reforms Since 2013, Georgia Tech Scheller College of Business Research Paper No. 36, Atlanta, Georgia Institute of Technology Scheller College of Business, 2015.

⁶⁹ Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a; Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, cit.

⁷⁰ Executive Order 12333, cit.; Court of Justice of the European Union, Schrems II, Case C-311/18, cit., paras. 180-185.

⁷¹ Presidential Policy Directive 28 of 17 January 2014, “Signals Intelligence Activities”; Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282; Swire, Peter, U.S. Surveillance Law, Safe Harbor, and Reforms Since 2013, cit.

to satisfy standards of necessity and proportionality rather than permit undifferentiated or generalized access. Second, individuals whose rights were affected had to enjoy remedies that were effective, independent, and practically usable. It is precisely on these points that the transatlantic frameworks repeatedly encountered difficulty, since executive and administrative safeguards, however useful they may have been politically, did not necessarily amount to the legally guaranteed judicial protection required by the Charter.⁷²

Christakis and Terpan show that EU–US negotiations on access to data for law enforcement reveal deeper divergences over procedure, fundamental rights, and the institutional conditions under which state access to data can be legitimized.⁷³ Docksey’s work on government access and transnational accountability is equally relevant, since it frames the problem as one of accountability across legal orders rather than merely one of domestic surveillance powers.⁷⁴

This explains why the Ombudsperson mechanism under Privacy Shield attracted persistent criticism. Located within the executive branch and lacking the independence associated with a court or tribunal, it appeared insufficient to remedy the deficit of effective judicial protection identified in *Schrems I* and later reiterated more forcefully in *Schrems II*.⁷⁵

4. SCHREMS II AND THE UNRESOLVED CONFLICT BETWEEN FUNDAMENTAL RIGHTS AND TRANSATLANTIC DATA FLOWS

4.1 *Schrems II* and the requirement of effective judicial protection

The second *Schrems* judgment arose out of a complaint that, while formally continuous with the earlier dispute, operated in a markedly altered legal environment. Maximilian Schrems once again challenged Facebook Ireland’s transfers of personal data to the United States. By then, however, the regulatory setting had shifted: Safe Harbor had already been

⁷² Charter of Fundamental Rights of the European Union, cit., arts. 7, 8 and 47; European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, cit.; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 168-185 and 191-197.

⁷³ Christakis, Theodore; Terpan, Fabien. 2021. “EU-US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options”, *International Data Privacy Law*, vol. 11, n.º 2, pp. 81-106.

⁷⁴ Docksey, Christopher. 2023. “Government Access to Personal Data and Transnational Accountability”, *Oslo Law Review*, vol. 10, n.º 1.

⁷⁵ European Data Protection Supervisor, Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision, cit.; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 194-197.

invalidated, Privacy Shield had taken its place, and Standard Contractual Clauses had become one of the principal legal mechanisms on which transatlantic transfers depended.⁷⁶

When the Court invalidated Privacy Shield in July 2020, it did so on grounds that went directly to the heart of the European Union constitutional order. The Court concluded that the legal framework governing United States intelligence activities did not provide safeguards essentially equivalent to those guaranteed under EU law, particularly in relation to necessity, proportionality, and effective judicial protection.⁷⁷ It was not enough that the Commission had secured representations from US authorities, but what mattered here is whether the rights of individuals transferred into that legal environment were actually protected in a manner compatible with the Charter.

A central part of the Court's reasoning concerned the adequacy of the existing remedies. Articles 7 and 8 of the Charter protect privacy and personal data, and Article 47 insists that rights must be judicially protectable in practice. The Ombudsperson mechanism introduced under Privacy Shield, however, was deemed insufficient because it did not provide guarantees of independence and enforceability comparable to those associated with a judicial body.⁷⁸

The centrality of redress in *Schrems II* is consistent with the broader uncertainty surrounding the meaning of effective remedy in international data transfers. Tzanou and Vogiatzoglou argue that effective redress in this context cannot be treated as a simple procedural formality, because it raises difficult questions concerning access, independence, enforceability, and the projection of Article 47 beyond the Union's territorial setting.⁷⁹

The insistence on judicial protection is one of the most consequential features of *Schrems II*: adequacy is not satisfied by procedural appearances or institutional assurances where the underlying remedial structure remains deficient.⁸⁰

⁷⁶ Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 121-134.

⁷⁷ Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 168-185 and 191-197.

⁷⁸ Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 194-197.

⁷⁹ Tzanou, Maria; Vogiatzoglou, Plixavra. 2023. "In Search of Legal Certainty Regarding 'Effective Redress' in International Data Transfers: Unpacking the Conceptual Complexities and Clarifying the Substantive Requirements", *Review of European Administrative Law*, vol. 16, n.º 1, pp. 11-30.

⁸⁰ Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 194-197; Tzanou, Maria; Vogiatzoglou, Plixavra, "In Search of Legal Certainty Regarding 'Effective Redress' in International Data Transfers", cit.

4.2 The conditional validity of Standard Contractual Clauses after *Schrems II*

However, *Schrems II* did not invalidate Standard Contractual Clauses, but it transformed their legal significance. SCCs remained valid in principle, yet no longer as a merely standardized compliance tool; their use now depends on whether the legal context of the recipient country allows the importer to comply with them in substance.⁸¹

The Court made clear that contractual clauses cannot, by themselves, neutralize the powers of public authorities in the destination state. If the legal environment of the third country permits access to personal data in ways that are incompatible with Articles 7, 8, and 47 of the Charter, the clauses may be insufficient unless supplemented by additional measures, and in some cases no supplementary measure may be enough.⁸² Thus, the Court transformed SCCs from a largely formal transfer tool into an instrument whose validity depends on contextual legal assessment.

Zalnieriute and Churches capture this weakness in terms of the “outsourcing” of data protection. Their critique is particularly apt after *Schrems II*: private contractual clauses may regulate the conduct of exporters and importers, but they cannot by themselves restrain the surveillance powers of the recipient state.⁸³

Exporters and importers must therefore assess, case by case, whether the law of the destination country permits compliance with the clauses in practice. Where that cannot be ensured, the transfer must be suspended or prohibited, which explains the post-*Schrems II* emphasis on transfer impact assessments, supplementary technical measures, and closer scrutiny of surveillance exposure.⁸⁴

4.3 The later refinement of “essential equivalence” in CJEU jurisprudence

⁸¹ Regulation (EU) 2016/679, cit., art. 46; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 121-147.

⁸² Charter of Fundamental Rights of the European Union, cit., arts. 7, 8 and 47; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 125-146.

⁸³ Zalnieriute, Monika; Churches, Genna. 2021. “Rejecting the Transatlantic Outsourcing of Data Protection in the Face of Unrestrained Surveillance”, *The Cambridge Law Journal*, vol. 80, n.º 1, pp. 8-11.

⁸⁴ Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 134-146; European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on 18 June 2021.

The significance of *Schrems II* lies not in introducing the doctrine of essential equivalence for the first time, but in refining its practical and constitutional operation. Earlier case law had already established that adequacy does not require identity between legal systems, but rather a level of protection comparable in substance and effectiveness to that guaranteed within the Union,⁸⁵ and what *Schrems II* added was a more exacting account of how that standard must be applied, through an integrated assessment of how the recipient legal order functions in practice.

In the US context, this required the Court to move beyond formal legislative assurances and examine surveillance authorities, institutional oversight, and available remedies as parts of a single legal structure. FISA 702, Executive Order 12333,⁸⁶ and the means available to non-US persons to challenge intelligence-related access to their data could not be considered in isolation, because the adequacy inquiry turned precisely on their combined effect. The Court's conclusion was not that the United States lacked every relevant safeguard, but that the framework, taken as a whole, failed to satisfy the Charter-based standard required for lawful transfers.⁸⁷

What *Schrems II* therefore contributed was a more operational understanding of essential equivalence, and the decisive question here became whether individuals whose data entered that legal environment would in fact be protected against disproportionate interference and afforded access to independent and effective redress, turning essential equivalence into less a formula of comparative resemblance than a method for testing whether protection remains real once data leave the Union.⁸⁸

This post-*Schrems II* understanding is also reflected in the literature. Murphy emphasizes the judgment's practical consequences for EU-US data flows,⁸⁹ while Zalnieriute reads it as exposing a deeper disagreement about national security, human rights, and the data-driven state.⁹⁰ Their readings support the conclusion that essential equivalence after *Schrems II* is not satisfied by legal vocabulary or institutional appearance alone, and

⁸⁵ Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 72-74.

⁸⁶ Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a; Executive Order 12333, cit.

⁸⁷ Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 180-197.

⁸⁸ Fonseca, Diogo Brito; Aires, Inês Pereira; Chowdhury, Isabel; Pereira, Margarida, "The international data transfer framework and its political consequences: a practical approach", cit., pp. 165-166.

⁸⁹ Murphy, Maria Helen, "Assessing the Implications of *Schrems II* for EU-US Data Flow", cit.

⁹⁰ Zalnieriute, Monika, "Data Transfers after *Schrems II*", cit.

requires scrutiny of the actual conditions under which rights can be invoked, enforced, and protected in the third country.

The doctrine thereby acquires a sharper constitutional function, requiring EU institutions, supervisory authorities, and private actors engaged in transfers to look beyond institutional reassurance and to confront the possibility that structural asymmetry between legal systems cannot always be repaired by contractual clauses, administrative redesign, or executive undertakings.⁹¹ This is the point at which my own analysis departs from a merely descriptive account: if the relevant interference arises from the public-law powers of the recipient state, then the adequacy inquiry must focus on the structure of those powers, not only on the procedural mechanisms created after the fact to review them.

4.4 Legal uncertainty and the fragmentation of compliance mechanisms

The immediate consequence of *Schrems II* was the invalidation of Privacy Shield, but its broader effect was a more fragmented model of compliance. Because the Court conditioned the continued use of SCCs on case-by-case assessment of the destination country's legal framework, responsibility for judging transfer legality was redistributed among exporters, importers, and supervisory authorities, producing the legal uncertainty emphasized by Christakis and Murphy.⁹²

That redistribution has had predictable effects. International transfers now often require detailed transfer impact assessments, analysis of surveillance regimes, evaluation of technical and organizational supplementary measures, and ongoing reassessment where the relevant legal environment changes.⁹³

At the same time, supervisory authorities across the Union have emphasized encryption, pseudonymization, and data minimization as potential supplementary safeguards, while

⁹¹ Murphy, Maria Helen, "Assessing the Implications of Schrems II for EU-US Data Flow", cit.; Zalnieriute, Monika, "Data Transfers after Schrems II", cit.

⁹² Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 134-146; Christakis, Theodore. 2020. "After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe", *European Law Blog*, 21 July 2020; Murphy, Maria Helen, "Assessing the Implications of Schrems II for EU-US Data Flow", cit.

⁹³ European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, cit.

others have adopted a more restrictive posture when surveillance exposure appears difficult to mitigate in practice, thereby producing a compliance landscape that is more demanding and not always uniform.⁹⁴

5. THE EU-US DATA PRIVACY FRAMEWORK AND THE PERSISTENCE OF THE ADEQUACY DILEMMA

5.1 The EU-US Data Privacy Framework as a new adequacy attempt

Following the invalidation of Privacy Shield, the Commission and the United States again sought to stabilize transatlantic transfers through an adequacy arrangement. Commission Implementing Decision (EU) 2023/1795 concluded that the United States ensures an adequate level of protection for transfers to participating organizations under the DPF. The framework was built in the shadow of *Schrems II* and therefore sought to respond to two defects identified by the Court: the limits of US surveillance law and the absence of effective redress for EU data subjects.⁹⁵

The DPF preserves the basic institutional logic of its predecessors insofar as it remains centered on certification by participating US companies, whose obligations are enforced under US law and administered through the Department of Commerce and related oversight structures. It therefore still depends on public recognition and private commitment rather than on full harmonization of transatlantic data protection law.⁹⁶

What differentiates the DPF from Privacy Shield is not the abandonment of that architecture, but the set of additional measures adopted on the US side after *Schrems II*. The Commission grounded its adequacy finding in a package of reforms linked to Executive Order 14086, which, in the Commission's account, introduces the principles of necessity and proportionality into the US legal framework on signals intelligence and establishes a new two-level redress mechanism culminating in the Data Protection Review Court.⁹⁷

⁹⁴ European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, cit.; European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, cit.

⁹⁵ Commission Implementing Decision (EU) 2023/1795, cit.; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 168-185 and 191-197.

⁹⁶ Commission Implementing Decision (EU) 2023/1795, cit.

⁹⁷ Commission Implementing Decision (EU) 2023/1795, cit.; Executive Order 14086, cit.

The DPRC was created in accordance with Executive Order 14086 and Attorney General regulations as the second level of the new redress mechanism, following an initial civil liberties review within the US intelligence oversight structure. Its judges are appointed by the Attorney General, after consultation with other executive actors, and the mechanism is housed within the executive branch rather than within the ordinary Article III judiciary.⁹⁸

The DPRC should therefore be treated as the central institutional innovation of the post-*Schrems II* framework. Propp and Swire had already argued that the individual redress deficit identified by the Court could be addressed through a more structured mechanism capable of combining fact-finding, independent review, and binding corrective measures.⁹⁹

Christakis, Propp and Swire later developed that argument specifically in relation to the DPRC, emphasizing its proposed independence and effective powers.¹⁰⁰ That more optimistic reading, however, must be placed alongside the Article 47 concerns identified by Tzanou and Vogiatzoglou, for whom effective redress in international transfers cannot be reduced to the existence of a complaint channel, but must be assessed through independence, accessibility, and enforceability.¹⁰¹

The Commission presented the DPF as a framework capable of addressing the constitutional concerns that proved fatal to Privacy Shield, but that remains the Commission's position rather than a settled conclusion.¹⁰²

The EDPB did not dismiss the new mechanism outright. In Opinion 5/2023, it accepted that a redress body created under Executive Order 14086 is not *per se* insufficient, but emphasized that the decisive question is whether the safeguards contained in the Executive

⁹⁸ Executive Order 14086, cit.; United States Department of Justice. Data Protection Review Court, 28 C.F.R. Part 201.

⁹⁹ Propp, Kenneth; Swire, Peter. 2020. "After Schrems II: A Proposal to Meet the Individual Redress Challenge", Lawfare, 13 August 2020.

¹⁰⁰ Christakis, Theodore; Propp, Kenneth; Swire, Peter. 2022. "The Redress Mechanism in the Privacy Shield Successor: On the Independence and Effective Powers of the DPRC", Cross-Border Data Forum, 24 October 2022.

¹⁰¹ Tzanou, Maria; Vogiatzoglou, Plixavra, "In Search of Legal Certainty Regarding 'Effective Redress' in International Data Transfers", cit.

¹⁰² Commission Implementing Decision (EU) 2023/1795, cit.; European Data Protection Board, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-U.S. Data Privacy Framework, cit.; noyb. 2023. "European Commission gives EU-US data transfers third round at CJEU", noyb, 10 July 2023.

Order and the Attorney General regulation ensure the DPRC's independence *vis-à-vis* the executive, especially in light of Article 47's requirements.¹⁰³

noyb has taken a sharper view, arguing that the DPF again presents an executive mechanism as judicially sufficient despite the Court's rejection of the Privacy Shield Ombudsperson model. The objection is therefore not merely semantic: what is called a "court" may still fall short of the independence expected of one if it remains executive-created, executive-appointed, and structurally opaque.¹⁰⁴

The same caution applies to necessity and proportionality. The Commission, and to a significant extent the EDPB, regarded Executive Order 14086 as a substantial improvement because it introduces those concepts into the US legal framework on signals intelligence. Yet the relevant question is no longer whether the vocabulary appears in the text, but whether it is operationally implemented in intelligence policies and procedures in a manner comparable to EU fundamental-rights law.¹⁰⁵

The critical literature therefore treats the DPF as improved but unresolved. Drechsler, Elbi, Kindt, Kun, Meszaros and Vranckaert question whether the third framework can avoid the fate of its predecessors, while Batlle and van Waeyenberge frame the decisive issue as whether the DPF satisfies the expectations generated by *Schrems II*, rather than whether it merely improves upon Privacy Shield.¹⁰⁶

5.2 Risks of renewed judicial invalidation and regulatory instability

It would be premature to describe the DPF as a stable settlement. The history of EU–US transfers suggests that political and institutional innovation does not automatically resolve structural legal divergence, especially where the benchmark remains the Charter as

¹⁰³ European Data Protection Board, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-U.S. Data Privacy Framework, cit.

¹⁰⁴ Noyb, "European Commission gives EU-US data transfers third round at CJEU", cit.

¹⁰⁵ European Data Protection Board, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-U.S. Data Privacy Framework, cit.; European Data Protection Board, Report on the first review of the EU-U.S. Data Privacy Framework, cit.

¹⁰⁶ Drechsler, Laura; Elbi, Abdullah; Kindt, Els; Kun, Eyup; Meszaros, Janos; Vranckaert, Koen. 2023. Third Time Is the Charm? The Draft Data Privacy Framework for International Personal Data Transfers From the European Union to the United States, CiTiP Working Paper 2023, Leuven, KU Leuven Centre for IT & IP Law; Batlle, Sergi; van Waeyenberge, Arnaud, "EU-US Data Privacy Framework: A First Legal Assessment", cit.

interpreted in *Schrems I* and *Schrems II*. The adequacy question turns not on whether a new framework is more elaborate than its predecessor, but on whether the recipient legal order preserves, in substance and in practice, the protection required by EU law.¹⁰⁷

The EDPB's position already pointed in that direction before the Framework entered into operation. In Opinion 5/2023, the Board welcomed several improvements in the draft adequacy decision, including the additional safeguards connected to signals intelligence and the new redress architecture, but it also identified unresolved issues concerning onward transfers, bulk collection, and the practical operation of the new safeguards. The DPF was primarily criticized because improvement alone does not answer the constitutional question. A framework may be institutionally more sophisticated and still fall short of essential equivalence.¹⁰⁸

That scrutiny continued after the adequacy decision was adopted. Article 3 of Commission Implementing Decision (EU) 2023/1795 requires periodic review, and the first review meeting took place in Washington on 18 and 19 July 2024 with the participation of EDPB representatives. In its report of 4 November 2024, the EDPB acknowledged that the commercial dimension of the Framework had been implemented and that the new multi-layered redress system was formally in place, but it also emphasized that the decisive issue had shifted from textual commitment to practical implementation. The relevant question is therefore whether those concepts operate in a manner genuinely comparable to their function under EU fundamental-rights law.¹⁰⁹

The most important development since then is the General Court's judgment of 3 September 2025 in *Latombe v Commission*. The case is significant precisely because it is the strongest argument against the critical position defended in this study. The applicant challenged the 2023 adequacy decision on grounds that went to the center of the post-*Schrems II* debate: first, that the Data Protection Review Court was not truly

¹⁰⁷ Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 72-74; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 168-176; Battle, Sergi; van Waeyenberge, Arnaud, "EU-US Data Privacy Framework: A First Legal Assessment", cit.; Drechsler, Laura et al., *Third Time Is the Charm?*, cit.

¹⁰⁸ European Data Protection Board, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-U.S. Data Privacy Framework, cit.

¹⁰⁹ Commission Implementing Decision (EU) 2023/1795, cit., art. 3; European Data Protection Board, Report on the first review of the EU-U.S. Data Privacy Framework, cit.

independent because it remained institutionally connected to the executive; and second, that bulk collection by US intelligence agencies remained insufficiently circumscribed because it was not subject to prior authorization by a court or independent administrative authority. The General Court rejected both arguments and dismissed the action in its entirety.¹¹⁰

The judgment therefore confronts the two elements on which the post-*Schrems II* reform rests: the independence of the DPRC and the legality of bulk collection subject to *ex post* review. On the first point, the General Court held that the appointment and functioning of DPRC judges were surrounded by safeguards sufficient to reject the allegation of lack of independence. It emphasized that DPRC judges may be dismissed by the Attorney General only for cause and that neither the Attorney General nor the intelligence agencies may hinder or improperly influence their work. It also attached importance to the Commission's continuing duty to monitor the US framework and, if necessary, suspend, amend, repeal, or limit the adequacy decision.¹¹¹

On the second point, the General Court adopted a reading of *Schrems II* that is especially consequential. It held that nothing in *Schrems II* requires bulk collection as such to be subject to prior authorization by a court or independent administrative authority. In its view, the relevant minimum requirement is the availability of *ex post* judicial review, which the Court considered to be satisfied through the DPRC. On that basis, it concluded that US bulk collection could not be regarded, solely because of the absence of prior authorization, as incompatible with the requirements arising from *Schrems II*, nor as preventing the United States from ensuring a level of protection essentially equivalent to that guaranteed under EU law.¹¹²

This is precisely where the present study takes a different position. The difficulty with *Latombe* is not that the General Court failed to identify the relevant safeguards, but that it treated those safeguards as capable of neutralizing a deeper institutional asymmetry. An executive-created body may be insulated from day-to-day interference, and yet still fail to offer the kind of structural independence that Article 47 requires when the rights at stake

¹¹⁰ General Court of the European Union, *Latombe v Commission*, Case T-553/23, Judgment of 3 September 2025.

¹¹¹ General Court of the European Union, *Latombe v Commission*, Case T-553/23, cit.; Bissacco, Francesco. 2025.

“Case T-553/23 *Latombe*: Overturning *Schrems*... and *Plaumann*?”, European Law Blog, 19 November 2025.

¹¹² General Court of the European Union, *Latombe v Commission*, Case T-553/23, cit.

concern secret intelligence access to foreign persons' data. Similarly, *ex post* review may be relevant, but it is a weak substitute for prior independent authorization where the interference consists of bulk access to personal data in transit, where the individual will normally not know that the interference occurred, and where the remedial process itself remains necessarily opaque.¹¹³

For that reason, *Latombe* does not eliminate the constitutional objection; it exposes it. If essential equivalence can be satisfied by an executive-based redress body and by *ex post* review of bulk collection, the standard risks being diluted into institutional deference to the Commission's assessment. The question is not whether the DPRC is better than the Ombudsperson mechanism; it almost certainly is. The decisive question is whether it transforms the position of EU data subjects sufficiently to make US surveillance law compatible with Articles 7, 8, and 47 of the Charter. In my view, it does not.¹¹⁴

The fact that an appeal is pending before the Court of Justice as Case C-703/25 P is therefore important, but it should not be used as an escape from the substance of the General Court's reasoning. Even if the judgment were ultimately upheld, the normative problem would remain. The DPF normalizes transfers to a legal order in which broad intelligence powers, limited prior control, executive-based redress, and the weaker remedial position of non-US persons continue to define the structure within which EU data are processed. The persistence of that structure is what makes the adequacy dilemma unresolved.¹¹⁵

For these reasons, regulatory instability remains a defining feature of the transatlantic transfer regime. The DPF has survived an important judicial test, but survival is not constitutional settlement. The stronger reading is that it mitigates the most visible defects of Privacy Shield while preserving the deeper incompatibility between EU fundamental-rights standards and US surveillance law, which supports a more restrictive approach to EU–US transfers.¹¹⁶

¹¹³ General Court of the European Union, *Latombe v Commission*, Case T-553/23, cit.

¹¹⁴ General Court of the European Union, *Latombe v Commission*, Case T-553/23, cit.; Court of Justice of the European Union, *Latombe v Commission*, Case C-703/25 P, appeal brought on 31 October 2025.

¹¹⁵ European Data Protection Board, Report on the first review of the EU-U.S. Data Privacy Framework, cit.; Court of Justice of the European Union, *Latombe v Commission*, Case C-703/25 P, cit.; Bissacco, Francesco, "Case T-553/23 *Latombe*: Overturning Schrems... and Plaumann?", cit.

¹¹⁶ European Data Protection Board, *Report on the first review of the EU-U.S. Data Privacy Framework*, cit.;

5.3 Possible normative paths toward a more sustainable transatlantic data transfer regime

If the recurring invalidation cycle of transatlantic transfer mechanisms teaches anything, it is that procedural design cannot indefinitely substitute for structural convergence. A more sustainable regime would require deeper legislative reform within the United States, including a comprehensive federal privacy law, clearer statutory limits on intelligence access, stronger remedies for non-US persons, and a more independent institutional framework. Rotenberg's proposals are especially relevant in this respect, since they show that durable adequacy cannot rest indefinitely on executive commitments alone.¹¹⁷

A second path lies in a more disciplined use of supplementary safeguards and transfer-specific risk assessment under the GDPR. Transfer impact assessments, organizational controls, encryption, data minimization, and access restrictions may reduce risk, but they cannot cure structural deficiencies in the recipient state's law where those deficiencies concern public authority access and ineffective remedies.¹¹⁸

A third path lies in stronger transatlantic oversight and accountability. The DPF already contains review mechanisms, but sustainability requires oversight that is transparent, responsive to legal change, and tied to measurable benchmarks concerning government access and redress. Docksey's account of transnational accountability reinforces this point: the issue is not whether some review exists, but whether accountability mechanisms preserve meaningful protection across legal orders.¹¹⁹

A sustainable transatlantic regime must acknowledge that cross-border data transfers are constitutional questions situated at the intersection of privacy, state power, market

General Court of the European Union, *Latombe v Commission*, Case T-553/23, cit.; Court of Justice of the European Union, *Latombe v Commission*, Case C-703/25 P, cit.; Zalnieriute, Monika, "Data Transfers after Schrems II", cit.; Rotenberg, Marc, "Schrems II, from Snowden to China", cit.

¹¹⁷ Zalnieriute, Monika, "Data Transfers after Schrems II", cit.; Rotenberg, Marc, "Schrems II, from Snowden to China", cit.; European Data Protection Board, *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-U.S. Data Privacy Framework*, cit.; Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da, *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, cit., p. 155.

¹¹⁸ European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, cit.; Zalnieriute, Monika; Churches, Genna, "Rejecting the Transatlantic Outsourcing of Data Protection in the Face of Unrestrained Surveillance", cit.

¹¹⁹ Commission Implementing Decision (EU) 2023/1795, cit.; General Court of the European Union, *Latombe v Commission*, Case T-553/23, cit., para. 292; Docksey, Christopher, "Government Access to Personal Data and Transnational Accountability", cit.

integration, and digital sovereignty. The position defended here is therefore more restrictive than a call for better institutional management. So long as EU personal data remain exposed to a foreign surveillance architecture that lacks fully equivalent limits, independent prior control, and judicially effective remedies for non-US persons, broad adequacy should not be the default legal basis for transatlantic transfers.¹²⁰

CONCLUSIONS

The regulation of transatlantic data transfers under the GDPR reveals a central tension of contemporary digital governance: personal data move globally, while EU law continues to attach their protection to demanding constitutional standards. The United States, although institutionally sophisticated in many respects, remains normatively distinct from that model.¹²¹

The first question addressed in this study concerned the meaning of “essential equivalence”. The analysis has shown that essential equivalence does not require identical legal systems, nor formal symmetry between the European Union and the United States. What it requires is a level of protection that remains comparable in substance and in practical effect. Adequacy under EU law therefore cannot be reduced to technical similarity, diplomatic reassurance, or the formal existence of transfer mechanisms. It is a constitutional standard directed to the preservation of rights once data become mobile.¹²²

The second question concerned the role of effective judicial protection in international transfers. *Schrems II* is decisive because it clarified that lawful transfers depend not only on substantive safeguards against disproportionate interference, but also on remedies capable of operating independently and effectively in practice. Articles 7 and 8 of the Charter protect privacy and personal data, while Article 47 gives those guarantees institutional force by requiring genuine and effective redress. Effective judicial protection is therefore not accessory to the transfer regime, but one of the constitutional conditions

¹²⁰ Docksey, Christopher, “Government Access to Personal Data and Transnational Accountability”, cit.; Zalnieriute, Monika, “Data Transfers after Schrems II”, cit.

¹²¹ Regulation (EU) 2016/679, cit.; Charter of Fundamental Rights of the European Union, cit., arts. 7, 8 and 47; Schwartz, Paul M.; Peifer, Karl-Nikolaus, “Transatlantic Data Privacy Law”, cit.

¹²² Court of Justice of the European Union, *Schrems*, Case C-362/14, cit., paras. 72-74; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 168-176.

without which essential equivalence cannot be meaningfully satisfied.¹²³

The third and final question asked whether the current EU–US Data Privacy Framework resolves the structural conflict between EU fundamental-rights standards and US surveillance law. The answer defended in this study is negative. The DPF undoubtedly introduces relevant institutional adjustments, particularly through Executive Order 14086 and the creation of the Data Protection Review Court. It is also formally operative, has undergone initial review by the EDPB, and has survived a first challenge before the General Court in *Latombe*. Yet these developments do not eliminate the deeper asymmetries that have historically destabilized transatlantic transfers. The DPF mitigates some of the deficiencies identified in earlier frameworks, but it does not fully resolve the structural tension between the EU’s constitutional requirements and the surveillance architecture of the United States.¹²⁴

The General Court’s judgment in *Latombe* makes that conclusion more difficult, but also more necessary. The Court accepted that the DPRC was accompanied by sufficient safeguards of independence and that bulk collection need not necessarily be subject to prior authorization where *ex post* review is available. Nevertheless, an executive-based redress mechanism cannot fully substitute for structurally independent judicial protection where the interference concerns secret intelligence access to personal data; nor can *ex post* review fully answer the risks created by bulk collection where the data subject is unlikely to know that the interference occurred. *Latombe* may uphold the DPF as a matter of first-instance legality, but it does not prove that the US framework is substantively compatible with EU fundamental-rights law.¹²⁵

From a broader normative standpoint, the transatlantic experience shows that international data transfer law has become a site in which competing constitutional visions of the digital order are negotiated. The conflict is not merely technical; it concerns whether the legal

¹²³ Charter of Fundamental Rights of the European Union, cit., arts. 7, 8 and 47; Court of Justice of the European Union, *Schrems II*, Case C-311/18, cit., paras. 194-197; Tzanou, Maria; Vogiatzoglou, Plixavra, “In Search of Legal Certainty Regarding ‘Effective Redress’ in International Data Transfers”, cit.

¹²⁴ Commission Implementing Decision (EU) 2023/1795, cit.; European Data Protection Board, Report on the first review of the EU-U.S. Data Privacy Framework, cit.; General Court of the European Union, *Latombe v Commission*, Case T-553/23, cit.

¹²⁵ General Court of the European Union, *Latombe v Commission*, Case T-553/23, cit.; Court of Justice of the European Union, *Latombe v Commission*, Case C-703/25 P, cit.

protection attached to a person can survive the territorial movement of that person's data.¹²⁶

For that reason, the long-term sustainability of transatlantic transfers will not be achieved through provisional compliance mechanisms, executive commitments, or institutional redesign alone. It requires substantive convergence regarding limits on state access, independent oversight, and enforceable remedies for non-US persons. Until that convergence is achieved, broad adequacy for EU-US transfers should be treated with caution rather than confidence, and transatlantic data flows should remain limited, strictly conditioned, and open to suspension where the substance of EU protection cannot be preserved.¹²⁷

BIBLIOGRAPHY

Article 29 Data Protection Working Party. *Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, WP 238, adopted on 13 April 2016.

Battle, Sergi; van Waeyenberge, Arnaud. 2024. "EU-US Data Privacy Framework: A First Legal Assessment", *European Journal of Risk Regulation*, vol. 15, n.º 1, pp. 191-200.

Bissacco, Francesco. 2025. "Case T-553/23 Latombe: Overturning Schrems... and Plaumann?", *European Law Blog*, 19 November 2025. Available at: <https://www.europeanlawblog.eu/pub/20d2hhrr>. Accessed: 12 June 2026.

Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2020.

Charter of Fundamental Rights of the European Union, OJ C 326, 26 October 2012.

Christakis, Theodore. 2020. "After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe", *European Law Blog*, 21 July 2020. Available at: <https://www.europeanlawblog.eu/pub/after-schrems-ii-uncertainties-on-the-legal-basis-for->

¹²⁶ Schwartz, Paul M.; Peifer, Karl-Nikolaus, "Transatlantic Data Privacy Law", cit.; Zalnieriute, Monika, "Data Transfers after Schrems II", cit.

¹²⁷ Rotenberg, Marc, "Schrems II, from Snowden to China", cit.; Docksey, Christopher, "Government Access to Personal Data and Transnational Accountability", cit.

data-transfers-and-constitutional-implications-for-europe. Accessed: 11 June 2026.

Christakis, Theodore; Propp, Kenneth; Swire, Peter. 2022. “The Redress Mechanism in the Privacy Shield Successor: On the Independence and Effective Powers of the DPRC”, *Cross-Border Data Forum*, 24 October 2022. Available at: <https://www.crossborderdataforum.org/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc>. Accessed: 11 June 2026.

Christakis, Theodore; Terpan, Fabien. 2021. “EU-US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options”, *International Data Privacy Law*, vol. 11, n.º 2, pp. 81-106.

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the United States Department of Commerce, OJ L 215, 25 August 2000.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1 August 2016.

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-U.S. Data Privacy Framework, OJ L 231, 20 September 2023.

Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, Strasbourg, 28 January 1981.

Court of Justice of the European Union. *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, Case C-311/18, Judgment of 16 July 2020.

Court of Justice of the European Union. *Latombe v Commission*, Case C-703/25 P, appeal brought on 31 October 2025.

Court of Justice of the European Union. *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, Judgment of 6 October 2015.

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, OJ L 281, 23 November 1995.

Docksey, Christopher. 2023. “Government Access to Personal Data and Transnational Accountability”, *Oslo Law Review*, vol. 10, n.º 1.

Doneda, Danilo. 2011. “A proteção dos dados pessoais como um direito fundamental”, *Espaço Jurídico Journal of Law*, vol. 12, n.º 2, pp. 91-108.

Drechsler, Laura; Elbi, Abdullah; Kindt, Els; Kun, Eyup; Meszaros, Janos; Vranckaert, Koen. 2023. *Third Time Is the Charm? The Draft Data Privacy Framework for International Personal Data Transfers From the European Union to the United States*, CiTiP Working Paper 2023, KU Leuven Centre for IT & IP Law, Leuven.

European Data Protection Board. *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-U.S. Data Privacy Framework*, adopted on 28 February 2023.

European Data Protection Board. *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, version 2.0, adopted on 18 June 2021.

European Data Protection Board. *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, adopted on 10 November 2020.

European Data Protection Board. *Report on the first review of the European Commission Implementing Decision on the adequate level of protection of personal data under the EU-U.S. Data Privacy Framework*, adopted on 4 November 2024.

European Data Protection Supervisor. *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, 30 May 2016.

Executive Order 12333 of 4 December 1981, “United States Intelligence Activities”, 46 Fed. Reg. 59941, 8 December 1981.

Executive Order 14086 of 7 October 2022, “Enhancing Safeguards for United States Signals Intelligence Activities”, 87 Fed. Reg. 62283, 14 October 2022.

Fonseca, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia: manifestações e limites*, Tese de Doutoramento, Universidade Nova de Lisboa, Lisboa, 2018.

Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a.

General Court of the European Union. *Philippe Latombe v European Commission*, Case T-553/23, Judgment of 3 September 2025.

Greze, Benjamin. 2019. “The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives”, *International Data Privacy Law*, vol. 9, n.º 2, pp. 109-128.

Hijmans, Hielke. *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU*, Springer, Cham, 2016.

Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282.

Kuner, Christopher. 2015. “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, *International Data Privacy Law*, vol. 5, n.º 4, pp. 235-245.

Lynskey, Orla. *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015.

Murphy, Maria Helen. 2022. “Assessing the Implications of Schrems II for EU-US Data Flow”, *International and Comparative Law Quarterly*, vol. 71, n.º 1, pp. 245-262.

noyb. 2023. “European Commission gives EU-US data transfers third round at CJEU”, *noyb*, 10 July 2023. Available at: <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu>. Accessed: 14 June 2026.

Office of the United Nations High Commissioner for Human Rights. *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/31/64, Geneva, 3 February 2016.

Organisation for Economic Co-operation and Development. *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, 1980.

Organisation for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, 2002.

Presidential Policy Directive 28 of 17 January 2014, “Signals Intelligence Activities”.

Privacy and Civil Liberties Oversight Board. *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Privacy and Civil Liberties Oversight Board, Washington, D.C., 2 July 2014.

Propp, Kenneth; Swire, Peter. 2020. “After Schrems II: A Proposal to Meet the Individual Redress Challenge”, *Lawfare*, 13 August 2020. Available at: <https://www.lawfaremedia.org/article/after-schrems-ii-proposal-meet-individual-redress-challenge>. Accessed: 12 June 2026.

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, OJ L 119, 4 May 2016.

Rotenberg, Marc. 2020. “Schrems II, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection”, *European Law Journal*, vol. 26, n.º 1-2, pp. 141-152.

Schwartz, Paul M.; Peifer, Karl-Nikolaus. 2017. “Transatlantic Data Privacy Law”, *Georgetown Law Journal*, vol. 106, n.º 1, pp. 115-180.

Schwartz, Paul M.; Solove, Daniel J. 2014. “Reconciling Personal Information in the United States and European Union”, *California Law Review*, vol. 102, pp. 877-916.

Swire, Peter. *U.S. Surveillance Law, Safe Harbor, and Reforms Since 2013*, Georgia Tech Scheller College of Business Research Paper No. 36, Georgia Institute of Technology Scheller College of Business, Atlanta, 2015.

Tzanou, Maria; Vogiatzoglou, Plixavra. 2023. “In Search of Legal Certainty Regarding ‘Effective Redress’ in International Data Transfers: Unpacking the Conceptual Complexities and Clarifying the Substantive Requirements”, *Review of European Administrative Law*, vol. 16, n.º 1, pp. 11-30.

United Nations. International Covenant on Civil and Political Rights, adopted 16 December 1966, entered into force 23 March 1976.

United Nations. Universal Declaration of Human Rights, adopted 10 December 1948.

United Nations Human Rights Committee. *General Comment No. 16: Article 17, The right to respect of privacy, family, home and correspondence, and protection of honour and reputation*, adopted on 8 April 1988.

United States Department of Health, Education, and Welfare. *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, United States Department of Health, Education, and Welfare, Washington, D.C., 1973.

United States Department of Justice. Data Protection Review Court, 28 C.F.R. Part 201.

Zalnieriute, Monika. 2022. "Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security", *Vanderbilt Journal of Transnational Law*, vol. 55, n.º 1, pp. 1-74.

Zalnieriute, Monika; Churches, Genna. 2021. "Rejecting the Transatlantic Outsourcing of Data Protection in the Face of Unrestrained Surveillance", *The Cambridge Law Journal*, vol. 80, n.º 1, pp. 8-11.