



Editorial

- Into the Great Wide Open: Celebrating 250 Years of the United States of America
James H. Boykin / Kulsum Gulamhusein / Andjela Mikanovic / Stephan Wilske

Articles

- The Trump Tariffs: From "Liberation Day" to – Well – Liberation Day
John M. Barkett
- Europe's Bold Space Law Gambit? What the EU Space Act Means for Global Space Commerce
Marc Ruttloff / Christoph Goller / Friederike Niemann
- Tariffs and Other Trade Restrictions: Contractual and Statutory Remedies under German Law for Disrupted Supply Chain Contracts
Tino Schneider / Julia Becker
- Access by U.S. Authorities to Data Stored in European Clouds
Annina Fittkau / Robert Grüner
- Schrems, Trump and the Growing Rift Between the United States and the European Union in the Digital Economy
Fabian Anheier
- A Thumbs Up for Emojis in Contracting and Legal Communication (Part 2)
Camilla Baasch Andersen / Marilyn Bromberg / Matthias Pendl
- Sanctions Against the Russian Federation in a Transnational Frame
Vladyslav Holopapa

Cases

- Not-So-Smart Glasses: AI and the Integrity of Witness Evidence
Barney Stannard / David Bufton / Eleanor McCann

Editorial Board

George A. Bermann, James H. Boykin, Charles N. Brower, Franco Ferrari, Stephan Harbarth, Claudia Junker, Juliane Kokott, Alexander Lorz, Thomas Meiers, Thomas Pfeiffer, Catherine Rogers, Norbert Röttgen, Giesela Rühl, Anahita Thoms, Stephan Wilske, Diane P. Wood

Editors-in-Chief

Stephan Wilske and James H. Boykin

Annina Fittkau and Robert Grüner, Berlin*

Access by U.S. Authorities to Data Stored in European Clouds

I. Introduction

The use of cloud computing services has become a defining feature of contemporary data processing within the European Union. Public authorities, private enterprises, and multinational corporations increasingly rely on infrastructure, platform, and software services provided by a limited number of globally operating cloud service providers. A significant proportion of these providers – such as *Microsoft*, *Amazon Web Services* (“AWS”), and *Google Cloud* – are headquartered in the United States or otherwise subject to U.S. jurisdiction.

From a European data protection perspective, this reliance on U.S.-based cloud services has raised persistent legal questions. Central among them is whether, and under what conditions, U.S. public authorities may lawfully access personal data processed in the EU when such data is stored or otherwise controlled by U.S. service providers.

This issue has already been addressed in the literature of the *Transatlantic Law Journal*, in particular by Boris P. Paal, who analyzed the implications of U.S. surveillance law for EU data transfers, as well as by Roland Marko and Johannes Sekannina, who discussed the interaction between EU data protection law and transatlantic cloud services.¹

These questions arise against the background of U.S. statutory frameworks that impose legally binding disclosure and preservation obligations on providers, in some cases irrespective of the data’s physical location.² At the same time, EU law, as codified in the General Data Protection Regulation (“GDPR”), establishes a comprehensive framework governing international transfers of personal data and explicitly addresses situations in which third country authorities seek access to data processed under EU jurisdiction.³

The resulting tension between U.S. access mechanisms and EU data protection requirements has been the subject of sustained legal scrutiny over the past decade. This scrutiny has been shaped most visibly by the jurisprudence of the Court of Justice of the European Union (“CJEU”), in particular its landmark decisions in *Schrems I* and *Schrems II*, which invalidated successive EU–U.S. data transfer frameworks.⁴ These judgments did not merely assess the adequacy of specific transatlantic arrangements but articulated broader principles concerning the level of protection required when personal data is transferred to, or becomes accessible from, a third country.

Against this background, this article pursues three objectives. First, it briefly traces the historical development of the EU–U.S. data transfer debate, with a focus on the *Schrems* case law as the central doctrinal turning point. Second, it analyzes the current legal framework under EU law, paying particular attention to the rules on international data transfers in Chapter V GDPR, the specific role of Article 48 GDPR, and the guidance issued by the European Data Protection Board (“EDPB”). Third, it examines the practical implications of this framework for companies that rely on cloud services provided by U.S.-based providers and considers compliance-oriented approaches grounded in existing legal instruments and supervisory practice.

Throughout the article, U.S. law is addressed only to the extent necessary to explain the source of the legal conflict with EU law. The focus remains on the European legal response to third country access risks and on the mechanisms available under EU law to address such risks in practice.

II. Historical Development: From *Safe Harbor* to *Schrems II*

The legal conflict surrounding access by U.S. authorities to personal data transferred from the EU did not begin with *Schrems I*, but the judgment marked the decisive turning point at which concerns regarding U.S. surveillance powers and inadequate judicial redress were first addressed systematically by the CJEU.

1. *Schrems I* and the Invalidation of the *Safe Harbor* Framework

The modern legal debate on access by U.S. authorities to data transferred from the EU can be traced back to the judgment of the CJEU in *Schrems I*.⁵ The case originated from a complaint lodged with the Irish Data Protection Commissioner concerning the transfer of personal data by *Facebook Ireland* to servers located in the United States. The complainant argued that U.S. law did not ensure an adequate level of protection for personal data, particularly in light of access by U.S. intelligence authorities.⁶

At the time, such transfers were legitimized under Commission Decision 2000/520/EC, commonly referred to as the “*Safe Harbor*” decision.⁷ This decision declared that organizations adhering to the *Safe Harbor* Privacy Principles ensured an adequate level of protection within the meaning of EU data protection law then in force.

In its judgment of 6 October 2015, the court invalidated the *Safe Harbor* decision. The court held that the European Commission had failed to establish that U.S. law ensured a level of protection “*essentially equivalent*” to that guaranteed within the European Union.⁸ It further emphasized that U.S. public authorities were able to access personal data

* Annina Fittkau is a Partner at gunnercooke, specializing in technology risk, IT compliance and data protection. She advises international clients on the compliant implementation of software, AI and digital platforms, with a particular focus on complex IT environments and regulatory frameworks. Prior to joining gunnercooke, she worked at PwC, Deloitte and KPMG Law. Robert Grüner works at the Umweltbank AG and is responsible for IT Strategy & Governance, IT Security as well as Provider Management. He is responsible for implementing the latest technology into the IT Portfolio and the accompanying IT Compliance. He also takes the lead in case of audits and the continuous monitoring of the IT security threat landscape. Prior to the Umweltbank he worked for PwC and Accenture.

1 Boris P. Paal, *Transatlantic Data Transfers After Schrems II*, TLJ 3/2025, 113; Roland Marko/Johannes Sekannina, *Cloud Services and EU Data Protection Law*, TLJ 2/2023, 63.

2 18 U.S.C. § 2713 (CLOUD Act).

3 Regulation (EU) 2016/679 (General Data Protection Regulation).

4 Case C-362/14, *Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650; Case C-311/18, *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, ECLI:EU:C:2020:559.

5 *Schrems*, *id.*

6 *Id.*, paras 26–30, 73–74.

7 Commission Decision 2000/520/EC, O.J. L 215 (25 August 2000).

8 *Schrems*, *supra* note 4, paras 73–74.

transferred from the EU on a generalized basis for national security purposes, without limitations that were strictly necessary and proportionate.⁹ It also found that EU data subjects lacked effective judicial redress against such access.¹⁰

While *Schrems I* was decided under the pre-GDPR legal framework, its reasoning laid the foundation for the later interpretation of EU data transfer rules. Notably, the court articulated the standard of “*essential equivalence*” as the benchmark for assessing third country protection, a concept that would later be explicitly reflected in the GDPR’s provisions on adequacy decisions.¹¹

2. *Schrems II* and the Reassessment of Third Country Access Risks

The second *Schrems* judgment, delivered on 16 July 2020, marked a decisive development in the EU’s approach to third country access to data.¹² In *Schrems II*, the court was again asked to assess the legality of data transfers from *Facebook Ireland* to the U.S. This time, the transfers were based on Commission Implementing Decision (EU) 2016/1250 on the EU–U.S. Privacy Shield and on the use of Standard Contractual Clauses (“SCCs”) pursuant to Article 46 GDPR.¹³

The court invalidated the Privacy Shield adequacy decision, holding that U.S. law – particularly in the area of signals intelligence – continued to permit access to personal data in a manner incompatible with EU fundamental rights.¹⁴ The court again pointed to the absence of limitations satisfying the requirements of necessity and proportionality and to the lack of effective judicial redress for EU data subjects.¹⁵ Importantly, the judgment did not amount to a general prohibition of transfers to the United States, but addressed specific deficiencies relating to U.S. surveillance powers and the lack of effective judicial redress for EU data subjects.

At the same time, the court upheld the validity of SCCs in principle, while imposing significant conditions on their use. According to the court, data exporters and, where appropriate, supervisory authorities are required to verify, prior to any transfer, whether the law of the recipient third country ensures adequate protection under the SCCs. Where this is not the case, supplementary measures must be adopted, or the transfer must be suspended or prohibited.¹⁶

Schrems II is significant not only because of the invalidation of the Privacy Shield, but because of the court’s systemic reasoning. The judgment made clear that contractual safeguards cannot compensate for structural deficiencies in third country law, particularly where public authorities enjoy extensive access powers.¹⁷ As a result, the assessment of third country access risks became an integral element of the EU data transfer regime.¹⁸

III. The Current EU Legal Framework Governing Third Party Access to Data

Following the judicial developments outlined above, the central legal question shifted from the validity of specific transatlantic transfer frameworks to the broader structure of EU law governing transfers of personal data to third countries and access requests originating outside the Union.

1. Chapter V GDPR: Structure and Objective

The legal framework governing international transfers of personal data under EU law is primarily contained in Chapter V (Articles 44–50) of the GDPR. Article 44 GDPR establishes the general principle that any transfer of personal data to a third country or international organization shall take place only if the conditions laid down in Chapter V are

complied with, thereby ensuring that the level of protection guaranteed by the GDPR is not undermined.¹⁹

Chapter V provides for a structured system of transfer mechanisms. Firstly, under Article 45 GDPR, the European Commission may adopt an adequacy decision declaring that a third country ensures an adequate level of protection. Where such a decision exists, transfers may take place without the need for specific authorization.²⁰ Secondly, in the absence of an adequacy decision, Article 46 GDPR permits transfers subject to appropriate safeguards, including SCCs, binding corporate rules, or other approved instruments, provided that enforceable data subject rights and effective legal remedies are available.²¹ Thirdly, Article 49 GDPR sets out specific derogations for particular situations, such as explicit consent or important reasons of public interest.²²

Recitals 101 to 104 GDPR clarify that transfers to third countries may occur only where the conditions of Chapter V are met and emphasize that the level of protection of natural persons guaranteed within the Union must not be undermined.²³ The CJEU expressly relied on this structure in *Schrems II*, stating that the effectiveness of transfer mechanisms must be assessed in light of the legal framework of the recipient third country, including access by public authorities.²⁴

2. Article 48 GDPR: Judgments and Decisions of Third Country Authorities

In addition to the general transfer regime, Article 48 GDPR addresses a specific scenario: the situation in which a court or administrative authority of a third country requires a controller or processor to transfer or disclose personal data.

Article 48 provides that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring such disclosure may be recognized or enforceable only if based on an international agreement in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to Chapter V.²⁵

The provision therefore links the recognition of third country disclosure orders to the existence of an international agreement and situates the rule within the broader framework of Chapter V. The wording does not create an autonomous transfer mechanism; instead, it clarifies the conditions under which third country decisions may be recognized under EU law.²⁶

The EDPB has adopted Guidelines 02/2024 on Article 48 GDPR, finalized in June 2025, which explain the scope and application of this provision. The Guidelines state that Arti-

9 *Id.*, paras 87–91.

10 *Id.*, paras 95–98.

11 GDPR, Art. 45; *Schrems*, *supra* note 4, para. 73.

12 *Schrems II*, *supra* note 4.

13 Commission Implementing Decision (EU) 2016/1250, O.J. L 207 (1 August 2016).

14 *Schrems II*, *supra* note 4, paras 168–185.

15 *Id.*, paras 191–197.

16 *Id.*, paras 133–135.

17 *Id.*, paras 126–131.

18 *Id.*

19 GDPR, Art. 44.

20 GDPR, Art. 45.

21 GDPR, Art. 46.

22 GDPR, Art. 49.

23 GDPR, Recitals 101–104.

24 *Schrems II*, *supra* note 4, paras 92–96.

25 GDPR, Art. 48.

26 *Id.*

cle 48 applies whenever a controller or processor in the EU is required by a third country authority to disclose personal data and emphasize that such requests must be assessed under EU law independently of the foreign legal obligation.²⁷

3. Recital 115 GDPR: Extraterritorial Application of Third Country Law

The regulatory context of Article 48 GDPR is further clarified in Recital 115 GDPR. Recital 115 states that some third countries adopt laws or regulations that purport to directly regulate processing activities of natural and legal persons under the jurisdiction of Member States. It further indicates that such extraterritorial application may conflict with international law and may impede the attainment of the protection of natural persons guaranteed within the Union.²⁸

Recital 115 also provides that transfers of personal data to third countries may take place only where the conditions laid down in the GDPR are complied with. This recital explicitly acknowledges the existence of extraterritorial claims by third country authorities and situates the response to such claims within the framework of Chapter V.²⁹

4. The Role of the European Data Protection Board

Under Article 68 GDPR, the EDPB is established to ensure the consistent application of the Regulation throughout the Union.³⁰ In the context of third country access risks, the EDPB has adopted several relevant instruments.

Most notably, the EDPB issued Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, finalized on 18 June 2021. These recommendations were adopted following the *Schrems II* judgment and provide a structured approach for assessing third country law and identifying supplementary measures where necessary. The document outlines a step-by-step methodology for data exporters and importers, including the assessment of third country access powers and the effectiveness of transfer tools.³¹

The EDPB explicitly recognizes that third country public authority access powers must be examined when assessing whether the chosen transfer mechanism ensures an essentially equivalent level of protection.³² The recommendations also identify categories of potential supplementary measures, including technical, contractual, and organizational safeguards.³³

Together, Chapter V GDPR, Article 48 GDPR, Recital 115, and the guidance issued by the EDPB form the core of the EU legal architecture addressing the risks associated with third country authority access to personal data, including in cloud computing environments.

IV. U.S. Access Mechanisms Relevant to EU Cloud Data: An Overview

U.S. access mechanisms assume particular relevance for EU cloud processing insofar as they impose legally binding obligations on service providers that may operate irrespective of, and potentially alongside, the EU's transfer regime. From the perspective of EU law, their importance lies less in their internal doctrinal configuration than in their normative and practical effect: they may compel providers subject to U.S. jurisdiction to preserve or disclose data within their possession, custody, or control, including data stored on servers located within the European Union.

1. The Stored Communications Act and the CLOUD Act

The principal statutory framework governing law enforcement access to data held by electronic communication and remote computing service providers is the **Stored Communications Act** ("SCA"), codified at 18 U.S.C. §§ 2701–2713. § 2703 establishes the circumstances under which U.S. governmental entities may require providers to disclose stored communications or related records.³⁴

In 2018, the **Clarifying Lawful Overseas Use of Data Act** ("CLOUD Act") amended the SCA and introduced 18 U.S.C. § 2713. This provision states that a service provider subject to U.S. jurisdiction must comply with obligations to preserve, backup, or disclose data within its "*possession, custody, or control*," regardless of whether the data is located within or outside the United States.³⁵ The statutory text therefore establishes that the physical location of the data is not determinative for the applicability of disclosure obligations.

For EU cloud constellations, this provision is relevant where a provider operating data centres within the European Union is nevertheless subject to U.S. jurisdiction. In such cases, disclosure obligations may arise independently of whether the data has been transferred to the U.S. within the meaning of Chapter V GDPR.³⁶

2. National Security Access: Section 702 FISA

Section 702 of the **Foreign Intelligence Surveillance Act** ("FISA"), codified at 50 U.S.C. § 1881a, authorizes the targeting of non-U.S. persons reasonably believed to be located outside the United States for the acquisition of foreign intelligence information.³⁷ The statute provides that the Attorney General and the Director of National Intelligence may jointly authorize such targeting, subject to procedures reviewed by the Foreign Intelligence Surveillance Court.³⁸

Section 702 further provides that electronic communication service providers must comply with directives issued under this provision.³⁹ The statutory framework thus establishes a legally binding mechanism through which U.S. intelligence authorities may obtain data from providers subject to U.S. jurisdiction.

The CJEU examined Section 702 in *Schrems II* when assessing whether U.S. law ensured a level of protection essentially equivalent to that guaranteed within the EU. In that judgment, it analyzed the scope of intelligence access under Section 702 in the context of the adequacy of the Privacy Shield framework.⁴⁰

For individuals whose data is processed in cloud infrastructures operated by providers subject to U.S. jurisdiction, Section 702 is relevant because the obligation to comply with directives is directed at the provider and is not limited by the physical storage location of the data. The court's analysis in

27 EDPB, Guidelines 02/2024 on Article 48 GDPR (Version 2.1, June 2025), paras 6–12.

28 GDPR, Recital 115.

29 *Id.*

30 GDPR, Art. 68.

31 EDPB, Recommendations 01/2020 (Version 2.0, 18 June 2021).

32 *Id.*, paras 42–45.

33 *Id.*, Annex 2.

34 18 U.S.C. § 2703.

35 18 U.S.C. § 2713.

36 *Id.*

37 50 U.S.C. § 1881a (a).

38 50 U.S.C. § 1881a.

39 50 U.S.C. § 1881a (h).

40 *Schrems II*, *supra* note 4, paras 168–185.

Schrems II makes clear that, when assessing the level of protection afforded to personal data transferred to or accessible from a third country, it is necessary to consider not only contractual safeguards but also the broader legal environment of the recipient country, including the scope of public authorities' powers to access such data, particularly for law enforcement or national security purposes.⁴¹

3. Executive Order 12333

U.S. intelligence activities are further organized under Executive Order 12333, which establishes the general framework for intelligence operations conducted by U.S. agencies.⁴² While the Executive Order itself does not create provider-directed disclosure obligations in the same manner as the SCA or FISA, it forms part of the overall legal framework governing signals intelligence activities.

The CJEU referred to intelligence activities conducted under Executive Order 12333 when analyzing the broader U.S. legal regime in *Schrems II*.⁴³ Similarly, when adopting the EU-U.S. Data Privacy Framework adequacy decision, the European Commission assessed the broader U.S. intelligence framework, including surveillance activities conducted under Executive Order 12333.⁴⁴

In the context of EU cloud services, Executive Order 12333 is relevant insofar as it forms part of the legal environment that EU institutions have taken into account when assessing third country access risks under Article 45 and Article 46 GDPR.

V. The EU-U.S. Data Privacy Framework

Following the invalidation of the EU-U.S. Privacy Shield by the CJEU in *Schrems II*, the European Commission and the United States initiated negotiations aimed at establishing a new legal framework for transatlantic data transfers. These negotiations resulted in the adoption of Commission Implementing Decision (EU) 2023/1795 of 10 July 2023, commonly referred to as the EU-U.S. Data Privacy Framework ("DPF").⁴⁵

The decision was adopted pursuant to Article 45 GDPR and finds that organizations in the U.S. that self-certify under the Framework ensure an adequate level of protection for personal data transferred from the EU. The adequacy finding applies only to organizations that participate in the Framework and commit to comply with its principles, as administered by the U.S. Department of Commerce.⁴⁶

1. Safeguards Concerning U.S. Intelligence Access

A central element of the DPF concerns safeguards relating to access to personal data by U.S. intelligence authorities. These safeguards are primarily based on Executive Order 14086, issued on 7 October 2022 and entitled "*Enhancing Safeguards for United States Signals Intelligence Activities*".⁴⁷

Executive Order 14086 introduces requirements governing the conduct of U.S. signals intelligence activities, providing that such activities may be undertaken only to advance validated intelligence priorities and only to the extent and in a manner that is necessary and proportionate. The Order further requires U.S. intelligence agencies to adopt policies and procedures designed to ensure compliance with these principles.⁴⁸

2. Redress Mechanism for Individuals

Executive Order 14086 also establishes a redress mechanism for individuals who believe their personal data has been accessed unlawfully by U.S. intelligence authorities. This mechanism consists of two layers.

First, complaints are examined by the Civil Liberties Protection Officer ("CLPO") within the Office of the Director of National Intelligence. Second, individuals may seek review before the Data Protection Review Court ("DPRC"), an independent body created within the U.S. Department of Justice.⁴⁹

3. Current Legal Status

The Data Privacy Framework adequacy decision remains in force at the time of writing. However, the decision has been challenged before the courts of the EU.

In Case T-553/23 (*Latombe v. Commission*), the applicant sought the annulment of Commission Implementing Decision (EU) 2023/1795. The General Court dismissed the action by judgment of 3 September 2025, thereby upholding the validity of the adequacy decision.⁵⁰

An appeal against that judgment has been lodged before the CJEU and registered as Case C-703/25 P. Until a final judgment is rendered, the adequacy decision continues to apply as a valid transfer mechanism under Article 45 GDPR.

VI. Practical Implications for Companies Using U.S.-Based Cloud Services

The legal framework described above has direct implications for organizations within the EU that rely on cloud services provided by companies headquartered in the U.S. or otherwise subject to U.S. jurisdiction. In practice, widely used cloud infrastructures – such as those operated by *Microsoft*, *AWS*, and *Google Cloud* – may involve processing environments in which personal data is stored within the EU but remains under the operational control of a provider subject to U.S. law.

This distinction between the physical location of data and the legal control exercised by the provider has been identified in both case law and legal scholarship as a central element of the transatlantic data protection conflict. The relevance of this constellation arises from the interaction between two legal regimes. On the one hand, U.S. law establishes mechanisms through which authorities may request or compel access to data held by providers subject to U.S. jurisdiction. On the other hand, EU data protection law regulates the conditions under which personal data may be transferred to, or otherwise disclosed to authorities in, third countries.

The CJEU addressed this interaction in *Schrems II*, emphasizing that the level of protection guaranteed by EU law must not be undermined where personal data becomes accessible from a third country.⁵¹ The court further held that

41 *Id.*, paras 104–105, 126.

42 Executive Order No. 12333, 46 Fed. Reg. 59941 (4 December 1981).

43 *Schrems II*, *supra* note 4, paras 178–183.

44 Commission Implementing Decision (EU) 2023/1795 of 10 July 2023, Recitals 74–84.

45 *Id.*

46 *Id.*

47 Executive Order No. 14086, 87 Fed. Reg. 62283 (14 October 2022).

48 *Id.*

49 *Id.*, Sec. 3.

50 Case T-553/23, *Latombe v. Commission*, Judgment of 3 September 2025.

51 *Schrems II*, *supra* note 4, paras 92–96.

controllers and processors relying on transfer mechanisms under Article 46 GDPR must verify whether the law of the third country may affect the effectiveness of those safeguards.⁵² This interaction between provider-based access obligations and EU data protection law has also been identified in legal scholarship as a central structural tension in transatlantic data governance.

1. Structural Characteristics of Cloud Processing

Cloud computing is characterized by a distributed and layered technical architecture, including features such as multi-tenancy, remote access administration, redundancy across multiple data centers, and dynamic allocation of computing resources.⁵³

These characteristics may result in personal data being processed across different systems and jurisdictions, even where contractual arrangements specify data localization within the EU.

In this context, the relevance of U.S. access mechanisms does not depend on whether data is transferred in the traditional sense, but on whether the provider falls within the scope of U.S. jurisdiction and is therefore subject to legally binding obligations under U.S. law.

2. Technical and Legal Complexity of Cloud Infrastructures

The legal assessment of third country access risks in cloud environments is further complicated by the technical architecture of modern cloud computing infrastructures. Cloud services are typically characterized by virtualization, multi-tenancy, distributed storage, and remote administrative access, which together result in a decoupling of data location, processing, and control.⁵⁴

In particular, data may be replicated across multiple data centers for redundancy and performance purposes, while administrative access may be exercised remotely by personnel located in different jurisdictions. This architecture challenges traditional territorial concepts underlying data protection law, as the physical storage location of data does not necessarily determine the applicable legal framework or the effective control over the data.

From a compliance perspective, this implies that organizations cannot rely solely on contractual data localization clauses but must assess the technical and organizational structure of the cloud service, including access control mechanisms, encryption models, and key management arrangements.

3. Transfer Assessments and Supplementary Measures

Following the *Schrems II* judgment, the EDPB issued guidance addressing how organizations should assess third country access risks when transferring personal data. In its Recommendations 01/2020, the EDPB describes a process through which exporters should evaluate whether the law and practice of the third country may affect the protection afforded by the chosen transfer mechanism.⁵⁵

The recommendations state that organizations must assess whether public authorities in the third country may access transferred data in a manner that goes beyond what is considered necessary and proportionate under EU law. Where such risks are identified, exporters may adopt supplementary measures, which may include technical, contractual, or organizational safeguards.⁵⁶

Examples discussed in the recommendations include technical measures such as encryption or pseudonymization, contractual commitments concerning the handling of government access requests, and organizational policies governing transparency and documentation. The EDPB emphasizes that the effectiveness of such measures must be assessed on a case-by-case basis.⁵⁷

Legal and technical literature further emphasizes that the effectiveness of such supplementary measures depends in particular on their concrete implementation, including encryption architecture and key management structures.⁵⁸

Academic and policy-oriented analyses emphasize that technical measures – particularly strong encryption combined with exclusive control over cryptographic keys – may in certain constellations effectively mitigate third country access risks, whereas purely contractual measures are generally insufficient.⁵⁹

4. Handling Requests from Third Country Authorities

Where a controller or processor receives a request from a third country authority seeking disclosure of personal data, Article 48 GDPR provides that such a judgment or administrative decision may be recognized or enforceable only if based on an international agreement between the requesting country and the Union or a Member State.⁶⁰

The EDPB Guidelines 02/2024 on Article 48 GDPR clarify that organizations receiving requests from third country authorities must independently assess whether compliance with such requests is permissible under EU law. The guidelines further explain that any disclosure of personal data in response to such orders must be assessed considering the GDPR's rules on international data transfers and the safeguards laid down in Chapter V.⁶¹

In practice, this requires organizations to implement internal procedures for identifying, documenting, and legally assessing such requests, including coordination with processors and cloud service providers.

VII. Conclusion: Use of Cloud Services under the Current Legal Framework

Recently, political discussions within the EU have increasingly focused on strengthening European technological sovereignty in cloud computing, particularly in response to concerns regarding third country access to data.⁶²

In this context, several initiatives have emerged, including GAIA-X as an initial framework for federated data infrastructures, as well as more recent developments such as the *European Alliance for Industrial Data, Edge and Cloud* and the *EU Cloud Rulebook* under the EU Data Act. These initiatives aim to promote interoperability, transparency, and European control over cloud infrastructures, including requirements relating to data localization, governance structures, and compliance with EU law.

⁵² *Id.*, paras 133–135.

⁵³ *European Union Agency for Cybersecurity* (“ENISA”), *Cloud Security Guide for SMEs* (2023).

⁵⁴ *Id.*

⁵⁵ EDPB, *supra* note 31.

⁵⁶ *Id.*

⁵⁷ *Id.*

⁵⁸ ENISA, *supra* note 53.

⁵⁹ ENISA, *Cloud Security for Healthcare Services* (2021).

⁶⁰ GDPR, Art. 48.

⁶¹ EDPB, Guidelines 02/2024 on Article 48 GDPR.

⁶² *European Commission*, *A European Strategy for Data*, COM(2020) 66 final (19 February 2020).

At the same time, legal and policy analyses emphasize that such initiatives do not in themselves remove the relevance of third country access mechanisms where cloud providers remain subject to foreign jurisdiction.⁶³

Accordingly, current discussions increasingly focus on hybrid compliance models combining legal safeguards under Chapter V GDPR with technical and organizational measures designed to limit access risks, rather than relying solely on geographic data localization.⁶⁴

While these developments reflect a significant policy shift towards strengthening European control over cloud infrastructures, recent scholarship and policy analyses emphasize that the underlying legal tension identified in *Schrems II* persists.⁶⁵ In particular, it is highlighted that the decisive factor for assessing third country access risks is not the

geographic location of data processing, but the legal exposure of the cloud provider to foreign jurisdiction.

Accordingly, even cloud offerings marketed as “sovereign” or “EU-only” must be assessed in light of the provider’s corporate structure, applicable legal obligations, and technical access possibilities.⁶⁶ From a practical perspective, this has led to an increased focus on governance-based and technical mitigation strategies, including strict access controls, customer-managed encryption keys, and organizational separation models within cloud infrastructures.⁶⁷ ■

63 EDPB, *supra* note 31.

64 *Id.*

65 *Schrems II*, *supra* note 4, paras 121–123.

66 EDPB, *supra* note 31.

67 ENISA, *supra* note 53.

Fabian Anheier, Cologne*

Schrems, Trump and the Growing Rift Between the United States and the European Union in the Digital Economy

I. Introduction – Schrems, FISA, and the Problem of Data Transfer to the U.S.

The U.S. and EU share a common market in the digital economy. According to the U.S. Chamber of Commerce, the U.S. exported \$199.35 billion in digitally-deliverable services to the EU in 2023 which accounted for about 31 % of U.S. worldwide digitally-delivered exports.¹ In the other direction, EU digital services exports to the U.S. were valued at \$93.97 billion, giving the U.S. a trade surplus in digitally-deliverable services of \$105.38 billion.² When it comes to the platform economy, European reliance on the U.S. becomes even clearer. U.S. companies lead the score on monthly active users of online platforms in the EU with Google’s combined services averaging 1.4 billion monthly users followed by Meta’s 518 million and Amazon with 181 million.³ While U.S. based platform services make up for 86 % of global market share, Europe’s market share sits at only 2 %.⁴

The first cracks in this business model started to appear in 2015 when the Court of Justice of the European Union (“CJEU”) handed down its judgment in *Maximilian Schrems v. Data Protection Commissioner*,⁵ finding that the transfer of personal data of EU citizens to the United States under the at the time EU-U.S. Safe Harbor agreement did not provide for an adequate level of protection under EU Directive 95/46.⁶ The CJEU’s finding of an inadequate level of protection was based on the fact that the Safe Harbor principles did not apply to the U.S. government and that the underlying agreement further stated that “national security, public interest, or law enforcement requirements” should have primacy over these principles.⁷

In the wake of this decision the EU and the U.S. were quick to negotiate a new agreement – Privacy Shield – which in 2020, was struck down as well by the CJEU in *Schrems II*.⁸ This time the court voiced its concerns over an inadequate level of protection in the U.S. more clearly by addressing specific laws that it deemed to be in violation of the EU Charter of Fundamental Rights. Specifically, the court criticized two provisions: Section 702 of the Foreign Intelligence

Surveillance Act (“FISA”) and Executive Order 12.333. While the EU and the U.S. have since negotiated yet another agreement, called the EU-U.S. Data Privacy Framework,⁹ both Section 702 and E.O. 12.333 still remain in force to this day.¹⁰ Unsurprisingly, this development sparked criticism from data privacy activists who called the validity of the EU-U.S. Data Privacy Framework into question.¹¹

While the CJEU’s decisions in *Schrems* are yesterday’s news, another statute has sparked more recent concerns from Europeans over the extent to which U.S. intelligence agencies

* Fabian Anheier is a research associate at the chair for U.S.-Law, Prof. Dr. Kirk W. Junker, at the University of Cologne. He holds an LL.M. from Mitchell Hamline School of Law in St. Paul, Minnesota. This article is based on a previous publication in German in ZD 2025, 557.

1 See U.S. Chamber of Commerce, Transatlantic Economy Report 2025, p. 50, https://www.uschamber.com/assets/documents/Transatlantic_Economy_2025.pdf.

2 *Id.*

3 See European Commission, Supervision of the designated very large online platforms and search engines under DSA (December 2025), <http://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vlos>.

4 U.S. Chamber of Commerce, *supra* note 1, p. 55.

5 CJEU Judgment of 6 October 2015, *Maximilian Schrems v. Data Protection Commissioner*, Case No. C-361/14, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362>.

6 See Art. 25(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J.L 281, 31. The predecessor to the EU’s General Data Protection Regulation (“GDPR”) – prohibited the transfer of personal data to third countries outside the EU not ensuring an adequate level of protection for this data.

7 *Id.* at 86.

8 CJEU Judgment of 16 July 2020, *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems*, Case No. C-311/18, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311>.

9 U.S. Department of Commerce, International Trade Administration, EU-U.S. Data Privacy Framework, <https://www.dataprivacyframework.gov/EU-US-Framework> (last accessed: 15 July 2026).

10 For an in-depth explanation of U.S. surveillance powers under FISA and EO 12.333, see Anheier/Nau, ZD 2025, 557 (in German).

11 NOYB – European Center for Digital Rights, European Commission gives EU-U.S. data transfers third round at CJEU (10 July 2023), <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu>. The organizations acronym “NOYB” stands for “none of your business.”