Proceedings of ICGPSH 2026 Symposium: Global Governance, Digital Politics, and the Transformation of Public Policy Systems
DOI: 10.54254/2753-7048/2026.ZJU33775

Judicial Trends in EU Cross-Border Data Flow

Ziyue Wang

Law School, Dalian Maritime University, Dalian, China
wangziyue0571@163.com

Abstract. The European Union has built the world's most influential regulatory system for cross-border data flow through the *General Data Protection Regulation,* and the judicial practices of the Court of Justice of the European Union and the courts of member states have played a crucial role in the evolution of this system. This paper systematically examines the latest trends in the judicial application of EU cross-border data flow rules. At the level of review standards, the Court of Justice of the European Union has completed a paradigm shift from formal compliance to dynamic standardization: starting with the principle of "substantial equivalence" established in the Schrems series of cases, followed by the proceduralization of this principle into due diligence obligations in the European Data Protection Board guidelines, and finally the continuous monitoring obligations affirmed in the EU-U.S. Data Privacy Framework and the *Latombe* case. The scope of review has also been extended to intergovernmental treaty-based data exchange. Through contextual application and proportionality assessment, the courts of member states have judicially corrected zero-risk enforcement, introduced a contextual perspective, and struck a balance between rights protection and commercial realities. At the level of remedies and enforcement, the *Bindl* case lowered the threshold for finding non-material damage, the *WhatsApp* case confirmed enterprises' direct right of action against binding decisions of the European Data Protection Board, and the *EEvidence Regulation* has transformed judicial authorities from passive recipients relying on administrative assistance into proactive subjects that can issue evidence orders directly to global service providers. These developments have strengthened the effectiveness of remedies and the accessibility of enforcement from the dimensions of data subjects, enterprises, and judicial authorities.

Keywords: Cross-border data flow, GDPR, Substantial equivalence, Judicial review, Soft data localization

1. Introduction

The EU regulatory system for the cross-border flow of personal data is centered on Chapter V of the *General Data Protection Regulation,* aiming to ensure that data enjoys a "substantially equivalent" level of protection after transfer outside the EU as it does within the EU. Existing studies generally hold that since the *Schrems I* case, the Court of Justice of the European Union has infused the protection standards established by the *Charter of Fundamental Rights of the European Union* into the review logic of cross-border data flow through a series of landmark rulings, driving the judicial

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2026.ZJU33775

review in this field from declaratory statements to case-by-case substantive assessment. Scholars further point out that fundamental rights-oriented judicial practices have reshaped the institutional foundation of EU-U.S. data flow and exerted a profound impact on the global digital governance landscape through the "Brussels Effect" [1-3]. However, with the deepening of regulatory practices, the EU judiciary is showing a trend of dynamic balance between maintaining high-standard protection and responding to the realities of digital economic development.

Based on the latest judicial practices after the *Schrems II* case, this paper aims to analyze the new trends of EU cross-border data flow rules in review standards, regulatory discretion, and remedy enforcement. By examining the judicial evolution from the dynamic construction of "substantial equivalence" to contextual adjustment of judicial correction, and then to the strengthening of procedural rights and enforcement capacity, this paper attempts to reveal how the EU judiciary prudently reconciles the tension between zero-risk polarized enforcement and the free movement of data while adhering to the bottom line of fundamental rights, so as to provide a theoretical reference for understanding the judicial logic of EU data governance.

2. Dynamic construction of review standards

Under the rights framework based on the EU Charter, the judicial review standards for EU cross-border data flow have evolved from one-off adequacy determination to continuous monitoring [4].

2.1. Evolution from fundamental rights orientation to case-by-substantive review

The *General Data Protection Regulation* systematically regulates the cross-border transfer of personal data through Articles 44-50. The *Schrems I* (C-362/14) case marks the starting point of the "substantial equivalence" standard, and the Court of Justice of the European Union also shifted its judicial focus from "expansive interpretation" to "effectiveness review" for the first time [5]. In this case, the Court of Justice of the European Union reviewed the constitutionality of the European Commission's 2000 Safe Harbor Decision, holding that U.S. domestic law lacked sufficient restrictions and effective remedies for the surveillance activities of intelligence agencies, especially that the *Patriot Act* allowed mass surveillance, which violated the *Charter of Fundamental Rights of the European Union,* and thus declared the decision invalid [5]. It can be seen that the adequacy determination in the EU data protection system is not merely a technical administrative judgment, but a constitutional matter directly bound by EU fundamental rights and subject to comprehensive judicial review. In *Schrems II* (C-311/18), the Court held that under frameworks such as FISA Section 702 and Executive Order 12333, U.S. intelligence agencies could conduct mass collection of foreigners' data without sufficient proportional constraints and effective remedies, and that the Privacy Shield Ombudsperson lacked sufficient independence, thus declaring it invalid [5, 6]. The Court also required enterprises to conduct a Transfer Impact Assessment when relying on Standard Contractual Clauses to judge whether they can provide data subjects with an equivalent level of protection in specific circumstances. National supervisory authorities of member states shall take the initiative to suspend or prohibit transfers when determining that a third country cannot comply with Standard Contractual Clauses and there are no sufficient supplementary measures [1, 7]. *Schrems II* essentially clarified "substantial equivalence" as a process requiring case-by-case substantive review, continuous monitoring, and dynamic assessment. Within this framework, the European Data Protection Board's *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* issued in 2020 further refined the cross-border data transfer framework, providing practical reference standards for circumstances in which

DOI: 10.54254/2753-7048/2026.ZJU33775

technical measures can be deemed sufficient in principle to identify surveillance risks in third countries [8].

2.2. From one-off adequacy determination to continuous monitoring

On the basis of the "substantial equivalence" standard, EU judicial review does not stop at the assessment of a single adequacy decision or a certain type of transfer tool. In July 2023, the European Commission adopted the adequacy decision for the EU-U.S. Data Privacy Framework, attempting to rebuild the institutional foundation for transatlantic data flow [9]. However, the Data Privacy Framework has undeniable limitations. First, the United States only made commitments through executive orders and did not substantially amend core intelligence legislation such as Section 702 of the *Foreign Intelligence Surveillance Act.* Second, the Privacy and Civil Liberties Oversight Board is under the Office of the Director of National Intelligence, and the Data Protection Review Council is still part of the administrative system, so the independence of the dual remedy mechanism remains questionable. French Member of Parliament Latombe immediately filed a lawsuit challenging whether the Data Privacy Framework meets the "substantial equivalence" standard. In the 2025 judgment of *Latombe v Commission,* the General Court explicitly emphasized that the European Commission has an obligation to conduct long-term monitoring of U.S. laws and practices, and shall promptly amend or revoke the decision in the event of material regression [10]. This means that the stability of the Data Privacy Framework depends on the European Commission's continuous monitoring and subsequent judicial review by the EU courts. Instead of rashly overturning the European Commission's adequacy determination, the Court has returned part of the space for environmental assessment to administrative authorities, seeking a new balance between the protection of fundamental rights and the stability of cross-border data flow.

In addition, Belgian courts have referred a preliminary ruling request to the Court of Justice of the European Union regarding the U.S. *Foreign Account Tax Compliance Act,* reviewing whether the arrangement for transferring financial account information to the United States under the tax treaty framework complies with the *General Data Protection Regulation* and the Charter. Although there is no final judgment yet, this means that the "substantial equivalence" standard formed in the Schrems system is expanding from commercial platform data flow to intergovernmental treaty-based data exchange and beginning to intervene in fiscal information cooperation mechanisms between sovereign states. This helps prevent large-scale data abuse in the name of taxation, but it may also be regarded as a secondary review of the existing bilateral and multilateral treaty systems by EU justice, thus triggering vigilance among sovereign states against judicial spillover.

Overall, the "substantial equivalence" standard has enhanced the substantive protection of data rights, but the EU's "substantial equivalence" review standard has also given rise to the following problems while strengthening data protection: First, it has resulted in de facto soft data localization. The "adequacy determination" standard of the *General Data Protection Regulation* is strict with an extremely low pass rate; after the *Schrems II* case, enterprises using Standard Contractual Clauses are burdened with case-by-case assessment of the legal risks of surveillance in third countries and the design of technical remedial measures; the scope of application of the exception clause (Article 49) is strictly limited to "occasional" and "small-scale" transfers [11]. These mechanisms constitute a de facto barrier to data outflow, forcing enterprises to choose to store data within the EU or restrict cross-border transfers to avoid legal risks and huge fines. Second, the surge in compliance costs caused by soft data localization imposes a heavy burden on small and medium-sized enterprises. A survey shows that more than 90% of Standard Contractual Clauses users consider the relevant assessment costs too high, which constitutes a bottleneck to technological development. A 2023

DOI: 10.54254/2753-7048/2026.ZJU33775

World Bank study indicates that data restriction measures can reduce GDP by up to 1.7%, investment growth by 4.2%, and export growth by 1.7% [2]. Third, the effectiveness of the "Brussels Effect" relies on its institutional credibility, fairness and predictability, and appeal of values, that is, global recognition of the moral legitimacy of EU rules [2, 3]. However, the EU's rapid approval for allied countries and high thresholds for developing countries in the above institutional framework reflect discriminatory protectionism, which deviates from its value of protecting the free movement of data.

3. Contextual adjustment of judicial remedies under regulatory polarization

3.1. Tension balance between enforcement polarization and judicial correction

Some courts of EU member states have to a certain extent judicially corrected the zero-risk interpretation in judicial practice. In the *Cookiebot* case, the Administrative Court of Wiesbaden, Germany, issued an interim injunction prohibiting the use of the tool in summary proceedings on the grounds that the U.S. *Clarifying Lawful Overseas Use of Data Act* might apply and Akamai servers were potentially under U.S. jurisdiction, holding that the embedding of Cookiebot on university websites violated the *General Data Protection Regulation* [12]. The legality of the transfer was denied as long as there was a theoretical path to access the data. Although the higher court ultimately revoked the injunction on procedural grounds without giving a fundamentally different answer on the merits, it indirectly expressed a more prudent judicial attitude, that is, it is not advisable to negate the complex legal environment of third countries through simple reasoning in interim proceedings [1].

In some cases involving Google Analytics, local courts such as those in Cologne have begun to adopt more refined contextual review. The courts examine the identifiability of dynamic IP addresses in specific contexts, review whether supplementary measures such as the specific content of Standard Contractual Clauses between exporters and Google, encryption, and access control can substantially reduce the realistic possibility of government access, as well as the specific methods of user notification and consent [1]. Instead of directly declaring that all uses of Google Analytics necessarily violate the *General Data Protection Regulation*, the courts take risk controllability as the measurement standard. This eases the one-size-fits-all trend of risk judgment after *Schrems II* and provides space for risk classification and remedial measures.

In a relevant judgment, the Regional Court of Traunstein further gave a concrete interpretation of the "necessity of contract performance" from the perspective of contractual purpose and service functions. In the case, a user sued a social media platform for violating the *General Data Protection Regulation* when processing and transferring his personal data to its U.S. parent company [13]. The Court pointed out that for platforms advocating global connectivity, cross-border data transfer to a certain extent can be regarded as objectively necessary to achieve the contractual purpose on the condition of complying with the principles of data minimization and transparency, and the necessity of contract cannot be denied simply on the ground that there are technically decentralized or local alternatives [13]. This approach provides an intermediate zone reconciled by the principle of proportionality between rights protection and business models and technological realities at the level of judicial application. The judgment reflects that the scope of application of the legal basis of "contract performance" is not fixed, but adjusts with the nature of services, technical architecture, and user expectations.

DOI: 10.54254/2753-7048/2026.ZJU33775

3.2. Relational reinterpretation of the scope of application

The core of data protection lies in the control relationship rather than data attributes [14]. In the *SRB v. EDPS* case, the Court of Justice of the European Union conducted a contextual consideration of whether pseudonymized data constitutes "personal data", introducing a "recipient's capacity" perspective into the scope of application of the *General Data Protection Regulation*. First, to judge whether data is related to an individual, we can start from the relationship between the controller and the data subject; second, to judge whether data is identifiable, we should examine whether the recipient has reasonably available additional information and technical capabilities. If measures such as encryption, key separation, and access control make it legally and technically difficult for the recipient to associate data with a specific natural person, the data processed by the recipient can be regarded as "non-personal data" in specific circumstances [7, 14]. The same data is personal data for the Single Resolution Board, which holds the decryption key, but anonymous information for Deloitte, which has no access to the key. This judgment exchanges a certain degree of regulatory leniency by proving the recipient's inability to identify individuals, avoiding the one-size-fits-all inclusion of all data into the highest regulatory intensity and preventing technical intermediaries from evading protection obligations at will. However, this path faces challenges of information asymmetry and insufficient technical assessment capacity. Issues such as who judges the recipient's identification capacity and how to prevent enterprises from diluting their liability under the cover of technical complexity must be addressed.

4. Strengthening of judicial remedies and enforcement

4.1. Procedural strengthening of regulated entities' rights

In the *Bindl v Commission* (T-354/22) case, a German citizen filed a lawsuit because the "Sign in with Facebook" widget embedded on the European Commission's website transferred his IP address and browser information to Meta platforms in the United States. The General Court held that the European Commission failed to ensure appropriate cross-border transfer safeguards, constituting a serious infringement within the meaning of Article 44 of the *General Data Protection Regulation,* and that the plaintiff's constant sense of anxiety due to losing control of personal data was sufficient to constitute non-material damage, ordering the European Commission to pay 400 euros in compensation [15]. First, this judgment affirms that EU institutions themselves, as controllers, are subject to the obligations of Chapter V of the *General Data Protection Regulation* without institutional privileges; second, it extends the threshold for finding damage from traditional incurred economic loss to the subjective psychological level, broadening the space for data subjects to seek compensation through judicial channels, which is consistent with the personality rights emphasized in the Charter. However, a broad interpretation of the damage standard may give rise to a large number of small-value but complex lawsuits and impose high compliance pressure on public institutions. Striking a balance between justiciability and judicial affordability will be a further issue for subsequent precedents.

In addition, the *WhatsApp v EDPB* (C-97/23 P) case focuses on the procedural space of enterprises in the integrated enforcement structure. The core issue is whether an enterprise can bypass the courts of member states and directly file an action for annulment with the EU courts to challenge a binding decision of the European Data Protection Board that directly affects its rights and obligations under the highly centralized enforcement framework composed of the *General Data Protection Regulation's* one-stop-shop mechanism and binding decisions of the European Data

DOI: 10.54254/2753-7048/2026.ZJU33775

Protection Board. The Court of Justice of the European Union held that a binding decision of the European Data Protection Board has a direct and clear binding effect on the legal status of an enterprise, meeting the standard of an "actionable administrative act" under Article 263 of the *Treaty on the Functioning of the European Union,* and enterprises have the right to directly file an action for annulment with the EU courts [16]. Thus, enterprises have transformed from passive subjects waiting for the initiation of procedures into entities that can actively trigger judicial review at the EU level. This to a certain extent prevents the integrated enforcement of the *General Data Protection Regulation* from sliding towards strong administrative centralization.

4.2. Enhancement of judicial authorities' enforcement capacity

The *EEvidence* Regulation has completed a more structural transformation in the enforcement link [17]. Designed in accordance with this Regulation, judicial authorities of member states may directly issue a "European Production Order" to electronic service providers providing services in the EU, requiring them to provide specified electronic evidence within 10 days, or 8 hours in emergencies, without going through traditional judicial assistance or diplomatic channels. The *EEvidence* Regulation reflects a paradigm shift from the "state-to-state" model to the "court-to-enterprise" model in the judicial dimension, pushing judicial authorities from the end of the cross-border evidence acquisition chain to the front end. This efficiency optimization is obviously positive for combating serious illegal acts, but such a unilateral evidence-gathering mechanism inevitably leads to institutional frictions in data governance, and its long-term effect still depends on whether the EU and third countries can establish a more inclusive coordination framework for evidence sharing and jurisdictional conflicts [9].

5. Conclusion

The judicial trend of EU cross-border data flow rules is shifting from a single role of protecting fundamental rights to a more adaptive governance balancer. The "substantial equivalence" standard established by the Court of Justice of the European Union through the *Schrems II* case has been continuously deepened. On the one hand, it strengthens the protection of individual rights and extends the scope of review to intergovernmental data exchange; on the other hand, it has also triggered concerns about regulatory polarization and soft data localization. In response, judgments of local courts of member states have shown a trend of contextual correction based on the principle of proportionality. The *Bindl and WhatsApp* cases have improved the judicial remedy system from the perspectives of individual remedies and enterprises' procedural rights respectively, while the *EEvidence* Regulation reflects a paradigm leap in enforcement collaboration. The authority of future EU cross-border data judicial review will depend both on adhering to high standards of rights protection and on continuously delivering prudent and pragmatic solutions between rights protection, the stability of digital trade, and legal pluralism.

The limitations of this paper are as follows: the analysis focuses on typical precedents and does not fully cover the differences in regulatory practices of member states and their interaction with justice; it focuses on review standards and remedy mechanisms, with limited discussion of other transfer tools such as codes of conduct and certification mechanisms, and does not involve the institutional divergence between the UK and the EU system after Brexit; it is based on normative analysis and lacks a technical dimension discussion on the validity assessment of technical measures such as encryption and pseudonymization. These shortcomings need to be supplemented by follow-up research.

DOI: 10.54254/2753-7048/2026.ZJU33775

References

[1] Yang Fan. Evolution of EU Legal Regulation on Cross-Border Data Flow After the Schrems II Case and China's Countermeasures [J]. Global Law Review, 2022, 44(1): 178-192.
[2] Jin Jing. EU Rules, Global Standards? "Race to the Top" in the Regulation of Cross-Border Data Flow [J]. Chinese Journal of International Law, 2023, 35(1): 46-65.
[3] Bradford A. The Brussels Effect: How the European Union Rules the World [M]. Oxford: Oxford University Press, 2020.
[4] Kuner C, Bygrave L, Docksey C, eds. The EU General Data Protection Regulation (GDPR): A Commentary [M]. Oxford: Oxford University Press, 2020.
[5] European Court of Justice. Judgment of 6 October 2015, C-362/14, Maximillian Schrems v Data Protection Commissioner (Schrems I) [ECLI: EU: C: 2015: 650].
[6] European Court of Justice. Judgment of 16 July 2020, C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II) [ECLI: EU: C: 2020: 559].
[7] General Court of the European Union. Judgment of 26 April 2023, T-557/20, Single Resolution Board v European Data Protection Supervisor [ECLI: EU: T: 2023: 219]; Court of Justice, Judgment of 5 December 2024, C-413/23 P [ECLI: EU: C: 2024: 998].
[8] 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.
[9] General Court of the European Union. Judgment of 3 September 2025, T-553/23, Latombe v Commission [ECLI: EU: T: 2025: 553].
[10] Liu Yideng, Song Ge. Game of EU-U.S. Cross-Border Data Flow Rules Under the Data Privacy Framework and Its Reference [J]. Chinese Journal of International Law, 2025, 12(3): 29-48.
[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1.
[12] Verwaltungsgericht Wiesbaden. (2021). Beschluss vom 1. Dezember 2021, 6 L 738/21.WI. Decision on the use of Cookiebot. Retrieved from https: //doi.org/10.1007/s11623-022-1584-9
[13] Landgericht Traunstein. (2024). Urteil vom 8. Juli 2024, Az. 9 O 173/24. Judgment on data transfer compliance. Retrieved from https: //nrwe.justiz.nrw.de/lgs/bonn/lg_bonn/j2025/13_O_156_24_Urteil_20250603.html
[14] Lynskey O. The Foundations of EU Data Protection Law [M]. Oxford: Oxford University Press, 2015.
[15] General Court of the European Union. Judgment of 8 January 2025, T-354/22, Bindl v Commission [ECLI: EU: T: 2025: 1].
[16] Court of Justice of the European Union. Judgment of 10 February 2026, C-97/23 P, WhatsApp Ireland Ltd v European Data Protection Board [ECLI: EU: C: 2026: 97].
[17] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production and Preservation Orders for electronic evidence in criminal proceedings (EEvidence Regulation) [2023] OJ L191/118.