Proceedings of the 3rd International Conference on Management Research and Economic Development
DOI: 10.54254/2754-1169/181/2025.22954

Research on the Compliance Path of Cross-border Data Flow under EU Law

Jiaran Gong

Institute of LAW University Of Sheffield, Sheffield, UK
JGong18@Sheffield.ac.uk

Abstract: In an increasingly digitized global economy, the seamless transfer of data across national borders has become integral to facilitating international commerce, digital service delivery, and economic progress. This study critically examines the legal structure established by the European Union (EU) for regulating international transfers of personal data, emphasizing key aspects of the General Data Protection Regulation (GDPR). Recognized globally for its rigorous protection standards, GDPR's extraterritorial application and reliance on adequacy determinations have nonetheless intensified global regulatory divergence. Despite widespread adoption, compliance instruments such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) encounter notable operational difficulties when navigating diverse international legal contexts. The study identifies key challenges—such as lack of international harmonization, enforcement barriers, and the disproportionate compliance burden on SMEs—and offers recommendations to enhance legal interoperability and policy convergence. Through comparative analysis and policy proposals, the paper calls for strengthened international coordination, global standardization of data transfer mechanisms, and integration of SCCs/BCRs into multilateral trade and governance frameworks. These efforts are essential for building a secure, transparent, and legally robust global data protection ecosystem.

Keywords: cross-border data transfers, regulatory fragmentation, EU data protection law, adequacy decision, privacy governance

1. Introduction

In digital landscape, data has become as an essential catalyst for economic expansion, technological innovation, and worldwide interconnectedness. The rapid expansion of digital trade, cloud computing, and artificial intelligence has necessitated the cross-border flow of data, facilitating business operations, international collaboration, and consumer services. However, the internationl data transfers face significant regulations. Concerns over national security, data sovereignty, personal privacy, and regulatory compliance have led major global economies to implement stringent regulations governing such transfers [1].

Different jurisdictions have developed distinct regulatory frameworks to oversee cross-border data transfers. The European Union (EU) has established a rigorous and comprehensive legal standard for personal data protection with its implementation of the General Data Protection Regulation (GDPR). GDPR imposes rigorous obligations on data controllers and processors, requiring that personal data may only be transferred outside the EU if an adequate level of protection is ensured, either through

DOI: 10.54254/2754-1169/181/2025.22954

adequacy decisions, Standard Contractual Clauses (SCCs), or Binding Corporate Rules (BCRs)[2]. Non-compliance can result in significant penalties, with fines reaching 4% of a company's global annual turnover or €20 million, whichever is higher [3].

In contrast, the United States (US) takes a more market-driven and sectoral approach to data governance. While there is no comprehensive federal data protection law, the California Consumer Privacy Act (CCPA) and sector-specific laws regulate data privacy in areas such as healthcare and finance. The US generally promotes the free flow of data, except in cases related to national security or law enforcement [2].

China has taken a security-first approach with stringent data localization requirements under its Cybersecurity Law (CSL), Data Security Law (DSL), and Personal Information Protection Law (PIPL). Companies must conduct security assessments before transferring critical data or large amounts of personal data abroad, and certain data transfers require explicit government approval. This regulatory framework reflects China's emphasis on data sovereignty and cybersecurity, making cross-border data transfers significantly more complex [4].

This divergence in regulatory approaches creates complexities for multinational enterprises seeking to engage in cross-border business operations, in the meantime, the regulation under the EU have more rigorous and complete so companies investing in the EU must navigate the GDPR's stringent requirements to avoid legal risks and financial penalties. Non-compliance can result in severe sanctions, including fines amounting to 4% of annual global turnover or €20 million, whichever is higher [5]. Therefore, businesses must implement comprehensive compliance strategies to align with EU regulations while maintaining operational efficiency.

This paper seeks to examine the EU's legal framework for cross-border data flows, analyzing its impact on businesses and offering compliance recommendations. By reviewing key legal instruments, enforcement mechanisms, and emerging challenges, the study aims to provide a roadmap for organizations to navigate the complexities of EU data protection laws. The findings will contribute to a deeper understanding of how businesses can achieve compliance while fostering innovation and global data exchange within the constraints of legal and regulatory requirements [1].

2. General provisions on cross-border data transfers in the EU

2.1. Legal framework

The European Union (EU) has implemented an extensive regulatory framework governing international data transfers, predominantly through Regulation (EU) 2016/679, known as the General Data Protection Regulation (GDPR). Effective since May 25, 2018, the GDPR replaced the earlier Data Protection Directive (95/46/EC) from 1995, establishing stringent standards for protecting personal data and setting clear requirements and procedures for data transfers across borders [2].

Significantly, GDPR possesses extraterritorial applicability, meaning it governs any organization, irrespective of geographical location, that processes personal data relating to individuals residing in the EU. This extensive jurisdictional reach positions GDPR as a leading global benchmark for data protection standards [6].

Specifically, Chapter V of GDPR delineates explicit guidelines for transferring personal data beyond the EU and European Economic Area (EEA), mandating that external data recipients must uphold protection standards comparable to those within the EU. Fundamental principles underlying GDPR include lawful, fair, and transparent data processing; clearly defined and limited processing purposes; minimization of collected data; ensuring accuracy; restrictions on data storage duration; and maintaining integrity and confidentiality [4].

DOI: 10.54254/2754-1169/181/2025.22954

In addition to GDPR, the EU's broader data governance framework incorporates legislation such as the Data Governance Act (DGA) and the Data Act, which address the cross-border circulation of non-personal data, complementing the GDPR's focus on personal data.

2.2. Specific provisions

GDPR imposes strict limitations on cross-border data transfers and offers three primary compliance pathways:

2.2.1. Adequacy decision (article 45 GDPR)

The European Commission conducts evaluations to determine if a third country, territory, or international organization provides a sufficient level of data protection. If such an entity is recognized as having adequate data protection standards, transfers of personal data may occur freely, without the need for supplementary protective measures. To date, adequacy decisions have been granted to jurisdictions including Andorra, Argentina, Canada (limited to commercial entities), Israel, Japan, New Zealand, South Korea, Switzerland, the United Kingdom, and Uruguay [7].

2.2.2. Appropriate safeguards (article 46 GDPR)

If a recipient country does not have an adequacy decision, GDPR mandates that data controllers implement alternative safeguards, including:

The European Union's legal framework for international data transfers includes various mechanisms designed to uphold compliance with the General Data Protection Regulation (GDPR). Among these mechanisms, Standard Contractual Clauses (SCCs) are notably prevalent. SCCs comprise contractual terms pre-authorized by the European Commission, obligating data recipients outside the European Economic Area (EEA) to maintain GDPR-compliant standards. These clauses provide enforceable protections, ensuring that personal data transferred internationally continues to receive adequate safeguarding, particularly in situations where an Adequacy Decision is not applicable [4].

Another significant mechanism is Binding Corporate Rules (BCRs), which are internal corporate policies designed to enable multinational organizations to transfer personal data within their corporate structure while ensuring compliance with GDPR standards. BCRs provide a framework for intra-group data transfers and must be approved by the competent data protection authorities within the EU before implementation. Unlike SCCs, which apply to external data transfers, BCRs are tailored for multinational enterprises seeking a harmonized internal data transfer regime across jurisdictions [6].

Additionally, the GDPR introduces certification mechanisms and codes of conduct as alternative compliance measures. These mechanisms involve industry-wide certifications and sector-specific codes of conduct, which, once approved by EU supervisory authorities, allow organizations to demonstrate compliance with GDPR requirements. By adhering to these standards, companies can establish a recognized level of data protection, thereby facilitating lawful data transfers while reinforcing transparency and accountability in data processing operations [8].

These mechanisms must be approved by the European Commission or national Data Protection Authorities (DPAs)to ensure GDPR compliance.

2.2.3. Derogations (article 49 GDPR)

In situations where an Adequacy Decision or suitable protective measures, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), are not available, the General Data Protection Regulation (GDPR) allows specific derogations for cross-border data transfers under

DOI: 10.54254/2754-1169/181/2025.22954

exceptional circumstances. These derogations are carefully crafted to strike a balance between safeguarding personal data and addressing the practical operational requirements of businesses and governmental entities. Consequently, they facilitate certain lawful data transfers even when the recipient jurisdiction lacks formally recognized data protection standards[9].

One such exception is the explicit consent of the data subject (Article 49(1)(a) GDPR), which allows data transfers if the individual concerned has been fully informed of the potential risks associated with the transfer and has provided unambiguous and specific consent. This exception, however, requires that the consent be freely given, informed, and revocable, thereby reinforcing the principle of data subject autonomy [8].

Another significant derogation under GDPR is the necessity to transfer personal data for contractual purposes, as outlined in Article 49(1)(b)-(c). This derogation applies specifically when data transfers are indispensable to fulfil contractual obligations between the data subject and the data controller, such as processing personal data for services like international travel bookings. It also covers scenarios involving pre-contractual measures undertaken at the explicit request of the data subject [10].

Moreover, GDPR permits cross-border transfers on public interest grounds (Article 49(1)(d)), which applies when the transfer is necessary to serve essential public policy objectives, such as international cooperation in law enforcement, health emergencies, or economic policies. These transfers must be based on explicit legal provisions, ensuring alignment with fundamental rights and proportionality principles [9].

Additionally, legal claims and proceedings (Article 49(1)(e)) constitute another valid exception, allowing personal data to be transferred if it is necessary for the establishment, exercise, or defence of legal claims. This derogation is particularly relevant in cross-border litigation, arbitration, and regulatory investigations, where data disclosure is essential for legal compliance and procedural fairness [10].

While these derogations enable certain data transfers, they are strictly interpreted and should not be relied upon for large-scale or repetitive data transfers. Organizations invoking these exceptions must demonstrate necessity, proportionality, and compliance with GDPR’s overarching principles, reinforcing the EU’s commitment to safeguarding data subjects' rights while facilitating legitimate international data flows.

2.3. Challenges

Despite being one of the strictest data protection frameworks worldwide, GDPR's cross-border data transfer system faces several challenges:

2.3.1. Regulatory fragmentation

The General Data Protection Regulation (GDPR) has established a highly stringent legal framework for cross-border data transfers, aimed at ensuring robust personal data protection. However, the rigorous requirements imposed by GDPR have led to regulatory fragmentation, particularly in cases where third countries have not received an Adequacy Decision from the European Commission. As a result, businesses engaging in international data transfers face significant legal uncertainty, increased compliance costs, and operational inefficiencies when dealing with jurisdictions that lack recognized data protection standards [6].

For multinational enterprises (MNEs), the establishment of a harmonized global data protection framework is essential for reducing compliance burdens and ensuring a more predictable and consistent regulatory environment. While the European Union's General Data Protection Regulation (GDPR) is broadly recognized for establishing a robust word privacy framework, its approach to

DOI: 10.54254/2754-1169/181/2025.22954

international data transfers—relying heavily on adequacy decisions and supplementary measures like Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs)—has inadvertently exacerbated regulatory fragmentation in global data governance. This fragmented regulatory environment presents challenges for international compliance and highlights the need for greater harmonization in cross-border data protection standards [2].

The current international landscape lacks a cohesive and enforceable global framework for governing cross-border data flows. National regulations often reflect divergent interests—ranging from data sovereignty to national security—resulting in incompatible and multilayered legal regimes that complicate international compliance. The EU's regionally oriented legal model poses significant challenges for global interoperability, functioning more as a barrier than a bridge to free data movement [6].

If such regulatory divergence remains unaddressed, it will likely to hinder the establishment of a stable, transparent, and secure framework for international data transfers. This scenario could disproportionately affect small and medium-sized enterprises (SMEs), which are typically short of sufficient information to drive complex and varied regulatory landscapes. Therefore, there is an urgent need to accelerate international efforts toward a harmonized and mutually recognized global standard, balancing robust privacy protections with the need for efficient and lawful data flows.

2.3.2. Uncertainty of adequacy decisions

The adequacy decision process under the General Data Protection Regulation (GDPR) is designed to support international data transfers by verifying that third countries uphold data protection standards similar to those of the EU. However, the sustainability and dependability of these adequacy decisions have faced growing scrutiny, particularly concerning EU-US data transfers. This concern intensified after the EU-US Privacy Shield framework, established to facilitate GDPR-compliant transatlantic data exchanges, was invalidated by the Court of Justice of the European Union (CJEU) in the 2020 Schrems II case. The Court determined that US surveillance practices did not sufficiently protect the personal data of EU residents, creating significant legal ambiguity for businesses and organizations reliant on data transfers between the EU and the US [11].

In response to this legal void, the EU and the US have initiated negotiations to establish a new "Trans-Atlantic Data Privacy Framework". While this framework in order to solve the deficiencies identified in the Schrems II case by introducing additional safeguards for EU data subjects, concerns remain regarding its long-term viability and compliance with EU fundamental rights. Legal experts and privacy advocates continue to question whether the new framework can withstand future legal scrutiny by the CJEU, or whether it will face similar challenges leading to its eventual invalidation [6].

As a result, organizations conducting EU-US data transfers must remain vigilant in their compliance strategies, closely monitoring regulatory developments while implementing robust data protection measures to mitigate potential risks associated with the ongoing legal uncertainties surrounding adequacy decisions [4].

2.3.3. Enforcement challenges

The General Data Protection Regulation (GDPR) enforces obligations on data controllers to ensure that foreign data recipients adhere to EU data protection standards when engaging in international data transfers. However, despite these legal requirements, the supervision and enforcement of compliance remain significant challenges in practice. One of the primary difficulties arises from the jurisdictional limitations of EU regulators, as enforcement actions against non-EU entities often face

DOI: 10.54254/2754-1169/181/2025.22954

procedural obstacles, including complex legal cooperation frameworks, lack of direct oversight, and difficulties in verifying compliance in foreign jurisdictions[5].

Furthermore, small and medium-sized enterprises (SMEs), representing a significant segment of the digital economy, often encounter challenges in complying with GDPR requirements due to considerable financial and technical constraints involved in implementation. Unlike large multinational corporations that have dedicated compliance teams and legal resources, SMEs often lack the necessary expertise and infrastructure to effectively assess the adequacy of third-country data protection measures, implement Standard Contractual Clauses (SCCs), or conduct Data Protection Impact Assessments (DPIAs). As a result, SMEs are disproportionately affected by GDPR's enforcement mechanisms, as non-compliance penalties can impose severe financial consequences on businesses with limited resources [6].

2.3.4. Challenges from technological advances

Emerging technologies such as cloud computing, artificial intelligence (AI), and blockchain increase the complexity of cross-border data flows [4]. One of the primary concerns is decentralized data storage, particularly in blockchain-based systems and multi-regional cloud environments. Unlike traditional centralized databases, blockchain operates on distributed ledger technology (DLT), where data is stored across multiple nodes in various jurisdictions. This decentralized nature raises fundamental legal questions regarding data controller accountability, the right to be forgotten, and jurisdictional applicability, as GDPR primarily assumes centralized data management models. Similarly, cloud computing services that store data across multiple data centres globally further complicate the identification of data transfer routes, making it difficult for organizations to ensure GDPR compliance in real-time [12].

Additionally, the rise of Privacy-Enhancing Technologies (PETs)—such as homomorphic encryption, federated learning, and differential privacy—has sparked debates on whether GDPR can effectively regulate and integrate these innovations into existing data protection frameworks. While PETs aim to enhance privacy protections, their integration into GDPR compliance remains unclear, particularly in terms of accountability, data minimization, and consent management [2].

These challenges highlight that while GDPR remains the global standard for data protection, its cross-border data transfer framework requires continuous legal adaptation and international cooperation to balance data security, business efficiency, and digital trade [13].

3. Suggestions for the cross-border data transfers framework in the EU

While the European Union's framework for international data transfers under the General Data Protection Regulation (GDPR) is recognized globally as one of the most robust data protection regimes, it nevertheless contains certain shortcomings and potential loopholes. This section aims to identify these areas for improvement and propose recommendations to enhance the comprehensiveness and effectiveness of the EU's regulatory framework.

3.1. Recommendations for enhancing data protection adequacy assessments

To enhance the scientific rigour, impartiality, and consistency of adequacy assessments in data protection, it is advisable for the European Union (EU) to refine its evaluation criteria further. These criteria should be made more transparent, quantifiable, and flexible, enabling them to adapt effectively to ongoing developments in the global data protection environment. The current adequacy decision mechanism serves to assess whether third countries provide a level of data protection equivalent to the General Data Protection Regulation (GDPR). However, there is room for

DOI: 10.54254/2754-1169/181/2025.22954

improvement, particularly in enhancing objectivity, defining clear evaluation metrics, and strengthening enforcement oversight [10].

Firstly, it is recommended to clearly define and operationalize criteria grounded in fundamental data protection principles, such as purpose limitation, data accuracy, proportionality, transparency, and security.These principles should be supplemented by concrete assessment benchmarks to ensure a more precise evaluation of a third country's data protection framework. Additionally, assessments should not only focus on the legal provisions of the target country but also emphasize actual implementation and enforcement effectiveness, ensuring that theoretical protections are effectively applied in practice [14].

Second, a continuous monitoring and periodic review mechanism should be introduced to ensure that countries granted adequacy status maintain their compliance with GDPR standards over time [9]. If significant changes in the legal framework or enforcement practices of a third country occur, an immediate reassessment of its adequacy decision should be conducted to uphold the stability and integrity of the EU's data protection framework [13].

Finally, improving the transparency of the adequacy assessment process is essential. Clearly defined evaluation criteria and quantifiable indicators should be made publicly available to provide legal certainty for businesses and individuals. Furthermore, the EU should explore stronger international collaboration to promote the convergence of global data protection standards, thereby enhancing the predictability and compliance of cross-border data flows [15].

By refining its adequacy assessment framework, the EU can not only strengthen its own data protection regime but also play a more proactive role in shaping the global data governance landscape, fostering greater international harmonization in data protection regulations.

3.2. Enhancing international regulatory coordination and cooperation in data governance

In the context of increasing digitalization and globalized data flows, regulatory fragmentation poses great challenges to international data transfers. To address these challenges, the European Union (EU) should strengthen its engagement in international regulatory coordination, particularly with major data-exporting jurisdictions such as the United States. Establishing structured bilateral and multilateral frameworks would facilitate greater harmonization of data governance standards, thereby minimizing legal inconsistencies and enhancing regulatory predictability [10].

Given the divergent approaches to data protection—where the EU emphasizes privacy as a fundamental right under the General Data Protection Regulation (GDPR), while the United States relies on a more sector-specific and self-regulatory model—there is a need for structured regulatory dialogues to identify common principles. These discussions should prioritize mutual recognition of adequacy mechanisms, the development of interoperable cross-border transfer frameworks, and mechanisms for ensuring equivalence in privacy protection standards [14].

Furthermore, regulatory cooperation should balance commercial interests with privacy protection, ensuring that businesses can operate in a stable and predictable legal environment while safeguarding individuals' data rights. Initiatives such as the OECD’s efforts to map commonalities in data governance regulations highlight the potential for international best practices and frameworks to facilitate convergence. The Schrems II ruling by the Court of Justice of the European Union (CJEU) has further underscored the necessity for robust safeguards in international data transfers, reinforcing the urgency for enhanced transatlantic cooperation [13].

To achieve meaningful harmonization, the EU should pursue enhanced multilateral engagement through existing international trade and data governance platforms, including the OECD, G7, and WTO digital trade initiatives. By aligning regulatory principles through legally binding agreements or sectoral cooperation mechanisms, regulatory fragmentation can be reduced, promoting both economic efficiency and robust privacy protection [16].

DOI: 10.54254/2754-1169/181/2025.22954

Such a coordinated approach would not only strengthen transatlantic and global data governance but also set a precedent for emerging economies, ensuring that international data transfer mechanisms align with high privacy and security standards while facilitating the growth of the digital economy [10].

3.3. Recommendations for strengthening Standard Contractual Clauses (SCCs) and other legal safeguards

In today's global data governance environment, ensuring the legality and security of cross-border data transfers remains a critical priority for regulatory bodies and enterprises alike. When the European Union (EU) has not recognized a third country through an Adequacy Decision, it becomes particularly important to enhance and actively support the application of Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) as reliable legal mechanisms to manage international data flows [13]. These measures will ensure that data transferred internationally continues to meet high privacy and security standards, thereby maintaining compliance with evolving global data protection requirements.

3.3.1. Adapting to global data flow challenges: Optimizing SCCs and BCRs

To effectively address the legal and regulatory challenges associated with global data flows, the European Union (EU) should enhance Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) to ensure compliance while improving their adaptability and practicality [13]. To achieve this, the following measures are recommended:

Regularly update SCCs to align with evolving data protection requirements across different jurisdictions. In particular, following the Schrems II ruling, data exporters are required to conduct more rigorous assessments of the legal environment in recipient countries. Therefore, SCCs should be dynamically adjusted to meet changing global data protection standards [14].

Enhance compatibility between SCCs and other international data protection frameworks. Efforts should be made to strengthen coordination between SCCs and the APEC Cross-Border Privacy Rules (CBPRs) to ensure a more unified compliance framework across different regions. This would reduce regulatory burdens on businesses and facilitate smoother international data transfers [10].

3.3.2. Enhancing oversight of SCCs and BCRs implementation

To ensure the effectiveness of Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) in practice, stronger regulatory measures should be implemented to ensure they serve as robust data protection mechanisms [14]. The following recommendations are proposed:

Strengthen corporate compliance obligations: Data exporters should not only sign SCCs but also conduct legal assessments of the recipient country’s regulatory environment. Additionally, they should adopt supplementary safeguards, such as data encryption, anonymization, and access control, to mitigate risks associated with government surveillance and legal uncertainties [10].

Establish a cross-border regulatory cooperation mechanism: Encourage collaboration among data protection authorities worldwide to share best practices for SCCs and BCRs enforcement, ensuring greater regulatory consistency and advancing the harmonization of global data compliance frameworks [10].

3.3.3. Promoting international coordination and strengthening legal certainty

To lower compliance expenses for enterprises involved in international data transfers and maintain uniformity in global privacy protection standards, it is essential to encourage greater harmonization

DOI: 10.54254/2754-1169/181/2025.22954

and standardization of Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) internationally [11].The following measures are recommended:

Facilitate the global standardization of SCCs and BCRs: Encourage international organizations such as the OECD, G7, and WTO to promote SCCs and BCRs as universally recognized data protection mechanisms, ensuring their broader applicability and legal certainty across different jurisdictions [16].

Strengthen the legal recognition of SCCs and BCRs in trade agreements and data governance frameworks: Governments should be encouraged to incorporate SCCs and BCRs provisions into bilateral and multilateral trade protocols, thereby reinforcing the legal foundation for international data flows and providing businesses with a clearer compliance framework [12].

By implementing these initiatives, a more unified, stable, and transparent global data protection system can be established, ensuring the seamless flow of data while safeguarding privacy and security, ultimately supporting the sustainable growth of the digital economy.

4. Conclusion

In an increasingly interconnected digital economy, ensuring the security, legality, and efficiency of internationl data transfers remains a critical challenge for regulators and businesses alike. This study underscores the regulatory fragmentation that characterizes the current global data protection landscape, where divergent legal approaches—ranging from the fundamental rights-based model of the European Union (EU) to sectoral frameworks in the United States and state-controlled governance in China—create significant legal uncertainties. While the EU's adequacy decision mechanism offers a structured approach for recognizing third countries with equivalent data protection standards, its limited scope and the dynamic feature of data protection laws necessitate continuous reassessment. In cases where an adequacy decision is not granted, Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) serve as the primary legal instruments for international data transfers. However, these mechanisms alone are insufficient to address evolving compliance challenges, particularly following the Schrems II ruling, which emphasized the need for supplementary safeguards to mitigate risks associated with inadequate third-country protections.

To bridge these regulatory gaps, stronger international coordination and legal harmonization are required. The EU should actively engage in multilateral initiatives led by organizations such as the OECD, G7, and WTO, which play a significant role in fostering regulatory interoperability and standardizing cross-border data governance frameworks. Encouraging the integration of SCCs and BCRs into trade agreements and multilateral governance frameworks can further strengthen legal certainty, ensuring that businesses operate within a predictable and enforceable compliance environment. Additionally, to improve the practical enforceability of SCCs and BCRs, regulatory authorities must enhance supervisory cooperation mechanisms and cross-border enforcement protocols to address jurisdictional inconsistencies in data protection oversight. Moreover, considering the disproportionate compliance burden placed on small and medium-sized enterprises (SMEs), policymakers should explore streamlined regulatory pathways that maintain high data protection standards while reducing unnecessary legal complexities.

A harmonized global data protection framework is essential to ensuring the secure and legally compliant flow of data while supporting digital economic growth. Future efforts should focus on updating SCCs and BCRs to align with technological and regulatory advancements, enhancing cross-border cooperation to standardize data protection laws, and integrating these mechanisms into international trade and data governance agreements. By leading efforts in global regulatory convergence, the EU can set a precedent for a more resilient, interoperable, and transparent global data ecosystem, balancing the imperatives of privacy protection, legal certainty, and economic innovation in an increasingly digitalized world.

DOI: 10.54254/2754-1169/181/2025.22954

References

[1] *Han, X., 'Paradigm Shift of European Union (EU) in Cross-Border Data Flow Supervision – From the Perspective of Digital Services Legislation' (2023) 13 Journal of WTO and China 69.*

[2] *Chin, Y.-C. and Zhao, J.(2022)Governing Cross-Border Data Flows.https://doi.org/10.3390/laws11040063*

[3] *Guamán, D.S.(2021)del Alamo, J.M. and Caiza, J.C., 'GDPR Compliance in Android Apps' IEEE Access. https://doi.org/10.1109/ACCESS.2021.3053130*

[4] *Arroyo, V., Hess, K., Grünbaum, N. and Ribeiro, G. (2023) Policy Brief: What Specific Measures Could the US, the EU and China Take to Foster and Facilitate Cross-Border Data Flows?Comparative Approach to Big Tech Regulation.*

[5] *Guamán, D.S., del Alamo, J.M. and Caiza, J.C., 'GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps' (2021) IEEE Access. https://doi.org/10.1109/ACCESS.2021.3053130*

[6] *Kong, L.(2010) 'Data Protection and Transborder Data Flow in the European and Global Context' 21(2) European Journal of International Law 441. https://doi.org/10.1093/ejil/chq025*

[7] *European Commission, 'Adequacy Decisions' https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en accessed 30 January 2022.*

[8] *Guamán, D.S., del Alamo, J.M. and Caiza, J.C. (2023) GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps.Computers & Security,130,103262.*

[9] *de Miguel Asensio, P.A. (2021) Cross-Border Data Transfers Between the EU and the U.S.Santa Clara Journal of International Law,19(2) , 1–45.*

[10] *Zheng, W.(2020) Comparative Study on the Legal Regulation of Cross-Border Flow of Personal Data and Its Inspiration to China .Frontiers of Law in China, 15(3), 280–312.*

[11] *Coche, E., Kolk, A. and Ocelík, V.(2024)Unravelling Cross-Country Regulatory Intricacies of Data Governance: The Relevance of Legal Insights for Digitalization and International Business. Journal of International Business Policy,7(1) , 112–127.*

[12] *Court of Justice of the European Union, Schrems II Judgment, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, [2020] ECLI:EU:C:2020:559.*

[13] *Jimenez-Gomez, B.S.(2021) Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic Dispute.Santa Clara Journal of International Law,19(2) ,1–45.*

[14] *Reimsbach-Kounatze, C., Enhancing Access to and Sharing of Data: Striking the Balance between Openness and Control over Data (OECD, 2019). https://doi.org/10.5771/9783748924999-25 accessed 12 March 2025.*

[15] *Zetzsche, D.A., Arner, D.W., Buckley, R.P. and Puschmann, T.(2021)DLT-Based Enhancement of Cross-Border Payment Efficiency – A Legal and Regulatory Perspective.Law and Financial Markets Review. https://doi.org/10.1080/17521440.2022.2065809 accessed 14 March 2025.*

[16] *OECD Trade and Agriculture Directorate, 'Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers' (2021) OECD Trade Policy Paper No. 248.*