WEP Warwick Evans Publishing

International Journal of Global Economics and Management

ISSN: 3005-9690 (Print), ISSN: 3005-8090 (Online)
Volume 10, Number 10, Year 2026
DOI: https://doi.org/10.62051/ijgem.v10n10.05



Regulatory Compliance and Financial Regulation Challenges in Cross-border Financial Data Flows under AI Governance

Xingyu Jin

Inner Mongolia University of Finance and Economics, Hohhot, China

ABSTRACT

This paper studies regulatory compliance and financial regulation issues in cross-border financial data flows under the new circumstances of increased application of artificial intelligence (AI), cloud computing and data-intensive analysis in finance. Although it does not provide new empirical data, cross-border financial data activities can be viewed in light of data protection, trade in services, prudential supervision, digital operational resilience and internal governance. AI is not the reason for the legal dispute; rather, it may have increased the scale and speed of data processing and increased dependence on external technology providers. Therefore, this paper will investigate the impact of the current cross-border data regulations, financial supervision requirements and regimes for digital operational resilience on AI-powered and cloud-based financial activities, as well as coordination deficiencies. Based on legal texts, materials from international standard-setting organisations and peer-reviewed research, this paper conducts a normative and conceptual analysis to distinguish between binding legal obligations and non-binding regulatory guidance or suggestions for compliance put forward in this paper. Several levels of context-aware reading for cross-border financial data governance have been provided, but no new global governance system has been proposed, and there is no claim or presentation of a causal effect of specific regulatory measures.

KEYWORDS

Cross-border financial data; AI governance; Regulatory compliance; Digital operational resilience; Financial regulation; Data governance

1. INTRODUCTION

Artificial intelligence, cloud computing and data-intensive analysis are being applied to risk management, customer evaluation, fraud detection and cross-border services in finance more and more often. The activities will need to obtain data from various financial institutions, technology companies and other places. Therefore, the flow of cross-border financial data has led to problems of operational efficiency and personal data protection, supervisory access to information, third-party technology risk, and digital operational resilience. AI is not responsible for all of these legal problems; instead, it may have expanded the scale and speed of data processing, increased reliance on external models, cloud platforms and other technology suppliers, etc.

Cross-border financial data are used here for convenience and do not refer to a particular legal provision. Based on the type of activity, the relevant materials may include personal information, non-personal operating data, transaction and risk data, supervisory information, model-related records, etc. Therefore, the relevant legal provisions will differ according to the type of data, the purpose and location of processing, the recipient, financial services involved, and the relevant regulatory system. Therefore, either unrestricted data flow or localisation should not be selected for the analysis of financial-sector compliance.

Content from this work may be used under the terms of CC BY-NC 4.0 licence (https://creativecommons.org/licenses/by-nc/4.0/).
Published by Warwick Evans Publishing.

This paper examines the combined impact of the existing cross-border data rules, financial prudential requirements and digital operational-resilience regimes on the use of AI and cloud services in cross-border finance, and identifies current coordination gaps. The normative and conceptual analysis are based on public legal materials, reports by international organisations and standard-setting bodies, and peer-reviewed research. No bank-internal data, regulatory interviews or quantitative data sets are used, and the paper does not present causal inferences about the effect of specific regulatory policies. Separate the binding legal obligations from the non-binding policy or supervisory documents and from compliance models that have not been empirically validated.

2. CROSS-BORDER DATA FLOW FRAMEWORKS AND FINANCIAL DATA

Discussions of cross-border data flows globally occurred prior to the current wave of AI in finance. The OECD Privacy Guidelines were released in 1980 and updated in 2013. They want to protect their privacy and avoid excessive restrictions on the cross-border flow of personal data; therefore, the 2013 amendment has increased the emphasis on accountability and interoperability [1]. The Guidelines are recommendations, and the international treaties do not have binding force. For financial activities, the relevant scope also depends on whether the data in question are personal data; not all financial-sector information is subject to the same legal provisions.

Recently, the OECD has carried out research and shown that the measures affecting non-personal data may include rules that promote data sharing, require regulatory access, demand local-storage conditions or restrict cross-border transfer [2]. The Scope of the Measures may be the same, but their Objectives are different. Therefore, when analysing the flow of financial data, it is necessary to determine the specific type and regulatory purposes of the data, and not assume that all restrictions and transfer paths are the same.

Cross-border financial data activities may also be subject to international services-trade rules. The general obligations and specific commitments on restrictive measures to trade in services are contained in the General Agreement on Trade in Services (GATS); whether a particular data-related measure falls within the scope of these restrictions depends on the mode of supply and the schedule of commitments for that country. GATS Article XIV(c)(ii) provides for measures required to ensure compliance with laws or regulations on the protection of personal data and the protection of confidentiality of individual records and accounts in the processing and dissemination of personal data, subject to the Article XIV chapeau, which lists conditions under which such measures should not be applied in a manner that constitutes arbitrary or unjustifiable discrimination or a disguised restriction on trade in services. Prudential measures are covered separately in paragraph 2(a) of the Annex on Financial Services and should not be combined with the privacy exception [3]. New digital trade agreements may contain special provisions on cross-border data transfer and localisation, as well as guarantees for regulatory autonomy [4]. The legal consequences of the prudential exception will vary in different places and do not grant a general exemption [5].

Scholarly studies have examined how economic interests, individual rights and the objectives of state governance shape different ideas of cross-border data governance [6]. They should not be regarded as fixed or independent national models; instead, they can help to explain the differences in data-transfer rules of various jurisdictions and regulatory systems. Cross-border financial data may be subject to data protection laws, services-trade rules and other sector-specific financial regulations. Thus, the data in the above section should not be considered general data-flow problems.

3. AI GOVERNANCE, DATA GOVERNANCE AND FINANCIAL SECTOR RISKS

Data Governance is Required for AI Governance in Finance. Financial AI can increase efficiency, but there are also defects, such as poor-quality data, bias, a lack of interpretability, market risk, and financial instability [7]. The IMF's research on the data economy has also highlighted the problems of privacy and access, interoperability, and policy coordination in cross-border data flows [8]. The reliability of a model is also influenced by the quality and representativeness of the training and operating data, their sources, and how current they are in practice.

The digitalisation of finance has also increased the demand for third-party technology services. The 2024 report by the Basel Committee on AI, Cloud Computing and Other Technologies' Impact Assessment of Technology-enabled Service Providers for Banks and Supervisors [9]. In 2025, the Basel Committee's Principles for the Sound Management of Third-Party Risk will offer non-binding supervisory guidance and a common reference for identifying, assessing, monitoring and managing risks arising from all kinds of third-party arrangements beyond traditional outsourcing [10]. The above materials indicate a low risk of cloud and external-model dependence, and not all third-party arrangements are equally risky.

Recently, the FSB has pointed out some potential risks of artificial intelligence, including third-party dependencies and service-provider concentration, market correlations, cyber risk, model risk, data-quality problems and governance deficiencies [11]. According to the 2025 monitoring report, monitoring is still in its early days, there are data deficiencies, classification problems and third-party concentration risks [12]. The OECD has also reported in its work on the supervision of AI in finance that supervisors may face difficulties interpreting and implementing relevant rules, acquiring information, scrutinising complex models, and possessing sufficient technical skills [13].

These developments do not support the construction of all-encompassing financial AI governance systems. Research in academia on AI in finance has focused more on responsibility and meaningful human involvement as possible responses to opacity and accountability problems [14]. Meaningful human participation can be introduced as a governance mechanism to enhance accountability and model supervision, but not all model risks will be eliminated. A narrow conclusion is that AI-enabled cross-border finance needs to coordinate data governance, model governance, third-party risk management and supervisory access, and the specific obligations will differ according to the applicable legal and institutional environment.

4. CROSS-BORDER FINANCIAL DATA, SUPERVISORY ACCESS AND AI

Cross-border flows of financial data continue to be problematic for supervision, accountability and information access. Financial institutions need to process data and use various areas of technological services, and the regulator requires extensive information to determine whether these institutions and their service providers are operating safely and stably. According to the IMF and Basel Committee materials, cross-border cooperation and access to relevant records for supervision are needed to effectively regulate technology-driven banking activities [8-10].

Cloud computing, external models and other third-party arrangements can be added to increase the complexity of the relationship; for example, the location of the data, confidentiality obligations, contractual terms or transfer restrictions may affect access to the information. For the above reasons, there will be limitations in the scope of supervision in some cases; however, supervision should not be entirely avoided. The question is whether the relevant laws, contracts and supervisory powers provide sufficient access to the particular activity and jurisdiction in question [9, 10].

Some of the AI-related supervisory risks are already known problems from the traditional model risk, outsourcing risk and information asymmetry; however, AI may increase the scale, complexity,

concentration and difficulty of supervision. FSB and OECD have listed some possible deficiencies in the information system, provider concentration and audit difficulties of complex models; however, these are monitoring and supervision problems, not signs of regulatory failure [11-13]. Financial institutions should assign particular responsibilities within the organisation for data, models and third-party services, and supervisors need to be well-versed in the relevant risks and services. Academic research on human responsibility in financial AI has also pointed out the requirement for identifiable accountability arrangements [14].

Cross-border financial data flow has generated a dual demand. Build a practical system for data processing and cross-border use of technology services, and ensure that the relevant information can be reliably obtained by supervisors for prudential supervision. Whether both requirements can be met depends on the legal basis for processing and transmitting the data, the nature of the financial activities, contractual arrangements, supervisory powers and the role of third-party providers. Therefore, this paper does not assume uninterrupted global interoperability or unavoidable regulatory conflicts.

5. DIGITAL OPERATIONAL RESILIENCE AND SECTOR-SPECIFIC FRAMEWORKS

The Digital Operational Resilience Act (DORA) came into force on January 16, 2023, and took effect on January 17, 2025. It sets the same requirements for ICT risk management, incident management and reporting, digital operational-resilience testing, ICT third-party risk and oversight of critical ICT third-party service providers for covered financial institutions [15]. Therefore, DORA should be viewed as an existing framework in use rather than a future system.

Commission Delegated Regulation (EU) 2024/1774 sets out binding final regulatory technical standards for ICT risk management tools, methods, processes and policies and supplements DORA [16]. These standards are already in effect and will not be replaced by draft RTS in the future. Although the framework puts forward the ideas of governance and documented risk management, it does not directly regulate all AI models or provide a single system for cross-border data legality.

Third-party governance under DORA will also distribute the responsibilities of financial institutions and public supervisory authorities. Financial institutions should address their own ICT third-party risks by means of contracts, registers of information, access and audit rights, continuity plans and exit strategies [15-16]. DORA has also created a supervision system for certain essential ICT third-party service providers and introduced Lead Overseer arrangements. The Lead Overseer directly supervises the designated critical providers, and the financial institutions are still responsible for their own ICT risk management, contractual, registration, audit and exit obligations and are still supervised by their competent authorities.

DORA, the General Data Protection Regulation (GDPR), and the EU Artificial Intelligence Act have different regulatory objects and legal purposes, and may apply simultaneously in light of the facts. Chapter V of the GDPR provides for the transfer of personal data to third countries or international organisations [17]. The EU Artificial Intelligence Act sets out standardised requirements for AI systems and related parties [18], and the implementation schedule and other provisions have been revised in Regulation (EU) 2026/1744 [19]. Application of one of these instruments does not automatically imply the application of the others; each needs to be determined based on the actual circumstances and scope.

Therefore, DORA should be regarded as a type of industry-specific operational resilience system rather than a general rule for cross-border data transfer or particular legislation on AI. The Regulatory Systems of GDPR, DORA and the AI Act may overlap in practice. Therefore, a financial institution using an AI model hosted by a cross-border cloud provider must independently meet requirements

for personal data transfer, ICT and third-party risk, and any other relevant obligations of AI systems, and should not believe that a single framework can address all these problems [15-19].

6. CROSS-BORDER PAYMENTS AND DATA-FRAMEWORK COORDINATION

Cross-border payments are a typical case of the integration of data rules, financial regulations and operational requirements. According to the FSB's 2024 final report on alignment and interoperability of data frameworks for cross-border payments, differences in laws, rules and regulatory requirements for collecting, storing and using payment-related data result in friction [20]. The above differences may affect the cost, speed, transparency and convenience of cross-border payments, as well as the ability of authorities and enterprises to obtain or use related information.

The FSB's report hopes to reduce unintended frictions in cross-border payments while keeping the original regulatory goals of transaction security, anti-money laundering and counter-terrorist financing, sanctions compliance and personal-data protection [20]. Therefore, the relevant public authorities need to strengthen coordination and interoperability, correct unreasonable inconsistencies in the data, promote cross-sectoral cooperation, and not assume that all data restrictions are unjustified.

Financial institutions need to comply with the horizontal legal provisions and the risk control requirements for data handling in cross-border payments in the industry, etc. Determine the type and purpose of the payment data, the place and party for processing, relevant transfer restrictions, and the role of external technology providers for the company. Where AI or cloud services are used, the problems are also linked to third-party risk, documentation and supervisory access issues mentioned above [10, 13, 15].

Therefore, cross-border payments are employed here as an application case rather than as the subject of independent research. As shown in the example above, coordination of data frameworks is required; otherwise, none of the individual international instruments would meet all the legal requirements. All kinds of payment services, different types of data, various areas of operation and various regulatory purposes have their own compliance requirements.

7. COMPLIANCE, GOVERNANCE CHOICES AND AI RISK MANAGEMENT

The above analysis shows some compliance and governance choices for the AI-powered cross-border financial data activity. The above selections should be classified according to the kind of law. Requirements in binding legislation such as DORA and GDPR should be treated as legal obligations; materials from the Basel Committee, FSB and OECD should be regarded as supervisory principles, standards or policy recommendations; and the additional organisational measures proposed in this paper should be presented as feasible compliance practices rather than mandatory legal duties.

Financial institutions should map the corresponding data categories and sources at the institutional level, along with processing purposes, locations, recipients and applicable legal basis, keep such records for internal control and supervisory review, etc. Review and monitor the third-party arrangements in light of relevant laws and regulations to ensure contractual access, audit rights, service continuity, and an exit plan [10-16]. If the relevant processing falls within the material and territorial scope of the GDPR, and a transfer of personal data to a third country or international organisation is involved, then the requirements of GDPR, including those in Chapter V, must also be met [17].

A compliance-by-design approach can be employed in this paper as a descriptive governance concept to identify legal requirements, internal controls and responsibility arrangements during the design and

operation of business, data and technology systems. It is similar in spirit to the concept of privacy by design in Article 25 of the GDPR, but not the same [17]. 'Algorithmic compliance' is also used exclusively to refer to the governance controls for data quality, documentation, testing, auditing, human supervision and accountability of models. It is not a fixed legal term and does not automatically apply to all national laws [13-15].

These ways should not give false hope. Although the current legal and supervisory system has added some restrictions, not all conflicts among data protection, trade, prudential supervision, operational resilience and AI governance have been addressed. This paper has not considered the cost or efficacy of compliance-by-design and algorithmic governance, etc., of external controls. The review, documentation and coordination of the institution's preparations are ongoing but have not been tested in practice or verified.

8. SUMMARY AND LIMITATIONS

Cross-border flows of financial data in the era of AI and cloud services are subject to multiple levels of regulation for various reasons. The same set of financial activities may be subject to data protection laws, services-traded standards, prudential supervision and digital operational resilience requirements at the same time. No single framework can solve all the problems of data transmission, supervision access, third-party dependency, model governance and operational risk independently.

Therefore, the analysis does not present a choice between free flow of data and localisation for cross-border financial data governance. A full-coverage assessment will consider the category of the data, business scenario, scope of the treaty, domestic legal basis, prudential purpose, supervisory information requirements and the role of external technology providers. Financial institutions can turn external demands into internal controls by means of data classification, third-party risk management, model documentation, audit records, human responsibility and business-continuity arrangements, but these should not be assumed to be universally applicable in all jurisdictions.

This paper is a normative and conceptual study based on public legal materials, foreign regulatory and standard-setting documents, and prior research by scholars. There are no data from financial institutions, supervisory interviews or other quantitative evidence; thus, the cost, technical performance and regulatory effectiveness of a specific compliance mechanism cannot be verified. In the future, more particular comparisons and case studies of some areas and financial activities will be conducted to study these problems. Only the regulatory system and points of overlap/potential compliance conflicts will be identified in this paper; a single-solution global system will not be proposed.

REFERENCES

[1] OECD. (2013). The OECD Privacy Framework. Paris: OECD Publishing.

[2] López González, J., Del Giovane, C., & Ferencz, J. (2025). A Preliminary Mapping of Measures Affecting the Cross-Border Flow of Non-Personal Data. OECD Trade Policy Papers, No. 295. Paris: OECD Publishing. https://doi.org/10.1787/0825c57c-en

[3] World Trade Organization. (1994). General Agreement on Trade in Services (GATS), including Article XIV and the Annex on Financial Services. Geneva: WTO.

[4] Burri, M., & Kugler, K. (2024). Regulatory autonomy in digital trade agreements. Journal of International Economic Law, 27(3), 397–423. https://doi.org/10.1093/jiel/jgae025

[5] Mitchell, A. D., Hawkins, J. K., & Mishra, N. (2016). Dear Prudence: Allowances under International Trade and Investment Law for Prudential Regulation in the Financial Services Sector. Journal of International Economic Law, 19(4), 787–820. https://doi.org/10.1093/jiel/jgw069

[6] Gao, R. Y. (2023). A Battle of the Big Three?—Competing Conceptualizations of Personal Data Shaping Transnational Data Flows. Chinese Journal of International Law, 22(4), 707–787. https://doi.org/10.1093/chinesejil/jmad040

[7] Boukherouaa, E. B., Shabsigh, G., AlAjmi, K., Deodoro, J., Farias, A., Iskender, E. S., Mirestean, A. T., & Ravikumar, R. (2021). Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance. IMF Departmental Paper 2021/024. Washington, DC: International Monetary Fund.

[8] Haksar, V., Carrière-Swallow, Y., Islam, E., Giddings, A., Kao, K., Kopp, E., & Quirós-Romero, G. (2021). Toward a Global Approach to Data in the Digital Age. IMF Staff Discussion Note 2021/005. Washington, DC: International Monetary Fund.

[9] Basel Committee on Banking Supervision. (2024). Digitalisation of Finance. Basel: Bank for International Settlements.

[10] Basel Committee on Banking Supervision. (2025). Principles for the Sound Management of Third-Party Risk. Basel: Bank for International Settlements.

[11] Financial Stability Board. (2024). The Financial Stability Implications of Artificial Intelligence. Basel: Financial Stability Board.

[12] Financial Stability Board. (2025). Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector. Basel: Financial Stability Board.

[13] OECD. (2026). Supervision of Artificial Intelligence in Finance: Challenges, Policies and Practices. OECD Artificial Intelligence Papers, No. 54. Paris: OECD Publishing. https://doi.org/10.1787/92743dc1-en

[14] Buckley, R. P., Zetzsche, D. A., Arner, D. W., & Tang, B. W. (2021). Regulating Artificial Intelligence in Finance: Putting the Human in the Loop. Sydney Law Review, 43(1), 43–81.

[15] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector (DORA). Official Journal of the European Union.

[16] Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying ICT risk management tools, methods, processes and policies and the simplified ICT risk management framework. Official Journal of the European Union.

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation, GDPR). Official Journal of the European Union.

[18] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

[19] Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulation (EU) 2024/1689 and related legislation as regards simplification of the implementation of harmonised rules on artificial intelligence. Official Journal of the European Union.

[20] Financial Stability Board. (2024). Recommendations to Promote Alignment and Interoperability Across Data Frameworks Related to Cross-border Payments: Final Report. Basel: Financial Stability Board.