Proceedings of ICILLP 2026 Symposium: Comparative Politics and Legal Frameworks in Policy Development
DOI: 10.54254/2753-7048/2026.JO39451

Institutional Causes of Compliance Dilemmas in Cross-Border Data Transfer by Chinese Enterprises and Coordinated Pathways

Manxia Wang

Law School, Hubei University of Police, Wuhan, China
20250401146@hbpa.edu.cn

Abstract. Chinese enterprises increasingly transfer data abroad in the course of overseas business expansion. When they do so, they are subject to two sets of rules at the same time: Chinese data transfer rules and the EU General Data Protection Regulation (GDPR). The two sets of rules are not fully compatible. This paper studies the institutional causes of the compliance dilemma that enterprises face under this dual regulatory framework. The research object is the relationship between China's security assessment and standard contract systems and the GDPR's adequacy decision and standard contractual clause mechanisms. The paper uses literature analysis, normative analysis, and comparative analysis. It finds that the root cause of the compliance dilemma is not that domestic rules are too strict, nor that GDPR standards are too high, but that the two sets of rules lack a coordination mechanism. They differ in compliance standards, procedural nature, and assessment of compliance effects. Enterprises must satisfy two parallel and incompatible rule systems at the same time. The paper suggests that the direction of reform is not unilateral improvement of domestic institutions, but coordination and mutual recognition between the two rule systems, possibly through regional frameworks such as RCEP. The paper also notes the limits of its analysis and the need for further research on specific industries.

Keywords: Cross-border data transfer, GDPR, compliance dilemma, institutional coordination, standard contractual clauses

1. Introduction

Legally, cross-border data transfer refers to the situation in which a data processor transfers or stores data that are collected and generated in domestic operations to a foreign country, or in which data are stored domestically but can be accessed or called by foreign institutions, organizations, or individuals. In recent years, Chinese enterprises have accelerated their pace of expanding into overseas markets, and cross-border data transfer activities have become increasingly frequent. At present, when Chinese enterprises transfer data abroad, they are simultaneously subject to two sets of rules: Chinese law and the EU General Data Protection Regulation (GDPR). On the Chinese side, a regulatory system has been built with three basic laws--the Cybersecurity Law, the Data Security

© 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.JO39451

Law, and the Personal Information Protection Law--as its core, and with departmental rules such as the Measures for Security Assessment of Data Cross-border Transfer and the Measures for Standard Contracts for Cross-border Transfer of Personal Information as supporting rules. This has formed a management system that is centered on security assessment and standard contracts.

From the perspective of institutional division of labor, security assessment mainly targets important data and personal information transfer that reaches certain quantity thresholds, and the review intensity is relatively high; standard contracts cover small- and medium-scale cross-border data transfer activities that do not reach the security assessment threshold, and the procedure is relatively simple. Together, the two constitute a layered and classified management system whose original intention is to provide enterprises with operable compliance paths under the premise of controllable risks. However, this system, designed on the basis of domestic risks, also needs to face another set of international rules that are based on the level of data protection. On the EU side, Chapter V of the GDPR establishes cross-border data transfer rules centered on "adequacy decisions". The two sets of rules apply simultaneously to Chinese enterprises' cross-border data transfer activities, but they are not fully compatible with each other.

This raises a question: what is the root cause of the compliance dilemma that enterprises face in cross-border data transfer? This paper argues that the deep cause is not that domestic rules themselves are too strict, but that there is a lack of coordination between domestic rules and the GDPR. On this basis, this paper analyzes the tension between the two sets of rules from the perspective of institutional coordination and explores possible coordinated pathways. The analysis stays at the institutional level. It does not attempt to quantify the actual compliance cost of individual enterprises, nor does it compare how data transfer rules are implemented in different industries.

2. Literature review

Around the compliance issue of cross-border data transfer, some research results have been accumulated in academia.

Domestic research mostly analyzes the compliance difficulties that enterprises face in cross-border data transfer from the perspective of institutional construction. Some studies point out that enterprises face multiple difficulties when transferring data abroad, including unclear compliance paths and high compliance costs [1]. Other studies focus on the governance of cross-border data security and argue that the current governance framework still has multiple dilemmas that need to be addressed [2]. Some studies further examine the relationship among the three paths--security assessment, standard contracts, and protection certification--and point out that the systemic connection among them has not yet been clearly established, so that enterprises lack clear guidance when applying them [3]. Foreign research focuses more on the governance of cross-border data flows under the GDPR framework, and discusses how the GDPR rules interact with data governance in practice [4].

Yet both types of research share the same problem: they discuss their respective systems separately and rarely put the two sets of rules together in order to analyze their impact on enterprises. Domestic research asks how the domestic system should be improved. Foreign research asks how the GDPR should be understood. Neither asks how the two rule systems interact when they apply to the same transfer activity. This paper tries to fill this gap by treating the two rule systems as one analytical object. This is not to say that existing studies lack value. Their analyses of domestic institutions and GDPR rules remain necessary. What they do not explain is why an

DOI: 10.54254/2753-7048/2026.JO39451

enterprise that has complied with one system may still fail to comply with the other. This is the question that this paper addresses.

3. Analysis of the institutional causes of compliance dilemmas in cross-border data transfer by enterprises

3.1. The internal logic of China's cross-border data transfer system

The core of China's cross-border data transfer management system consists of two paths: security assessment and standard contracts.

The security assessment system follows the logic of prior review. Data processors that meet certain thresholds must apply to the national cyberspace administration for security assessment before transferring data abroad. The assessment focuses on the purpose and scope of cross-border data transfer, the data protection level of the overseas recipient, and the risks that cross-border data transfer may bring [5]. The design intention of this mechanism is to have the regulatory authority review the legality and security of the transfer activity before the cross-border data transfer occurs, so as to prevent possible risks.

The standard contract system follows the logic of contract filing plus impact assessment. Data processors that do not reach the security assessment threshold may complete compliance by signing standard contracts and filing them, and at the same time must carry out personal information protection impact assessments [6]. The design intention of this mechanism is to replace administrative review with contractual tools for cross-border data transfer activities with relatively low risks, thereby reducing compliance costs while maintaining necessary supervision.

From the perspective of application relations, security assessment and standard contracts are not parallel options, but form a progressive structure that is based on thresholds. Data processors that reach the security assessment threshold cannot replace the filing obligation by signing standard contracts; only entities that do not reach the threshold may complete compliance through standard contracts. This progressive structure can achieve differentiated allocation of regulatory resources at the domestic level, but it also means that enterprises must first accurately determine whether they have reached the threshold before choosing the correct compliance path. The data classification and quantity standards on which threshold judgments depend are also uncertain in practice [5]. An enterprise may know the general categories of important data, but it may not know whether a specific data set falls into one of those categories. It may also be uncertain about how to count the number of individuals whose personal information is transferred. These uncertainties do not arise from a single unclear clause. They arise from the fact that the threshold itself depends on lower-level rules that are not yet fully in place. This lays the groundwork for the later analysis of corporate compliance dilemmas. This uncertainty has practical consequences. When an enterprise cannot determine whether its data falls within the scope of important data, it may choose to file a security assessment even when the transfer is low-risk. This increases the time and cost of compliance. Alternatively, it may decide not to file and later face administrative penalties if the data are later classified as important data. Neither choice is based on a clear legal standard. The problem is therefore not simply that enterprises lack information. It is that the legal standard itself relies on lower-level rules that are not yet complete. Some enterprises therefore treat the threshold as something to be judged case by case, not as a rule that can be applied mechanically. Some research reflects on the legitimacy basis of the security assessment system from a jurisprudential perspective. It argues that the institutional logic on which this system relies still needs further clarification, and that the relationship between security review and the free flow of data has not been fully settled [7].

DOI: 10.54254/2753-7048/2026.JO39451

Together, the two paths reflect the institutional concept of "security first, classification and grading". Security first means that the primary consideration of cross-border data transfer activities is security, and that only after security is guaranteed is the convenience of flow considered. Classification and grading means that different compliance requirements are set according to differences in data types and quantities. This institutional design has internal rationality at the domestic level. However, when this system faces another set of international rules that are equally internally rational, a question arises: whether this system has the ability to coordinate with external rules.

3.2. Additional constraints of the GDPR on Chinese enterprises

Chapter V of the GDPR establishes a cross-border data transfer framework centered on "adequacy decisions". The basic logic of this framework is that only when the European Commission determines that the recipient country provides an adequate level of data protection may data be transferred freely; if an adequacy decision has not been obtained, the data transfer party must use alternative transfer tools such as Standard Contractual Clauses (SCC) [8].

China is currently not included in the list of countries and regions that have obtained an adequacy decision under Article 45 GDPR [8]. The adequacy decision procedure usually involves a systematic assessment of the recipient country's data protection legislation, the independence of regulatory authorities, and remedy mechanisms. For countries without an adequacy decision, SCC are one of the commonly used alternative tools for enterprises. Some research points out that the EU's regulation of cross-border data flows carries a clear motive of rule export. Adequacy decisions and standard contractual clauses are typical channels through which this legal export is carried out. As a result,enterprises in third countries do not face technical compliance problems alone. They also face tensions between different rule systems [9]. SCC are formulated and continuously updated by the European Commission, adopt a modular clause design, and apply respectively to different data transfer scenarios such as controller-to-controller and controller-to-processor. Enterprises must choose the corresponding module according to their role in the data transfer chain and ensure that the contract clauses are consistent with the actual situation. This requirement increases the technical burden on enterprises in contract drafting and review. In practice, the choice of module often requires judgment rather than a simple matching of role labels. A Chinese enterprise may act as a controller in one business line and as a processor in another. It may also receive data from an EU controller and then transfer the data to a third country. Each situation may require a different module or a different combination of clauses. The enterprise must therefore map its data flows before it can draft the contract. The module choice also affects the content of the contract. A controller-to-processor module requires the processor to act only on the controller's instructions, while a controller-to-controller module requires both parties to assume independent obligations. If the enterprise chooses the wrong module, the contract may not reflect the actual data flow, and the filing may be rejected. The enterprise may then need to renegotiate the contract and refile, which adds another round of delay. This is a technical issue, but it has direct consequences for the timetable of cross-border data transfer.

This means that when Chinese enterprises receive personal data from the EU, they must rely on alternative transfer mechanisms such as SCC. On the surface, this only adds one compliance procedure: originally only Chinese law requirements needed to be met, but now SCC must additionally be signed. However, the substance of the problem cannot be reduced to "one more procedure".

DOI: 10.54254/2753-7048/2026.JO39451

What SCC add is not just one more layer of supervision, but a different compliance logic. The core question of China's security assessment system is "why the data are transferred abroad", and it reviews the purpose and scope of the transfer activity. The core question of SCC is "to whom the data are transferred and whether the recipient can protect them", and it reviews the protection level of the data recipient. The former focuses on the legality of the transfer activity, while the latter focuses on the protection capacity of the recipient. The two logics emphasize different things. When they apply to the same act at the same time, the enterprise has to answer two questions. These questions do not point in the same direction. The enterprise therefore cannot treat the documents prepared for one procedure as substitutable for those required by the other.

3.3. The institutional tension between the two sets of rules

The tension between the two sets of rules is mainly reflected in three aspects.

First, the logic of compliance standards is different. Security assessment requires enterprises to prove the legality of the purpose and scope of transfer, while SCC require enterprises to ensure that the protection level of the data recipient meets EU standards. Completing security assessment according to Chinese standards does not mean that the data recipient automatically meets the protection level requirements of SCC; conversely, signing SCC does not mean that the transfer activity can pass the review of China's security assessment. The two sets of standards are independent and do not replace each other.

Second, the nature of compliance procedures is different. Security assessment is an administrative review procedure, that is, enterprises apply to the national cyberspace administration and wait for the approval result, and the review cycle and result are subject to certain uncertainty. SCC are contractual tools, that is, enterprises negotiate and sign with the data recipient and file with the provincial cyberspace administration. The pace of administrative review is controlled by the regulatory authority, while the pace of contractual tools is decided by negotiation between the parties. When the two procedures run in parallel, the compliance cost of enterprises is not simply additive, but mutually constraining. If the security assessment is not passed, signing SCC has no practical benefit; if SCC are not properly signed, the security assessment may also be affected. In practice, an enterprise may complete the SCC first and then wait for the security assessment. If the assessment takes longer than expected, the enterprise may have to delay the transfer even though the contract is ready. Or it may pass the security assessment first and then find that the SCC module it chose does not match the actual data flow. In either case, the enterprise bears a cost that neither procedure would have produced on its own. The time cost is more than the sum of the two procedures. The enterprise may need to coordinate internal legal, technical, and business teams at the same time. The security assessment may require a data map, while the SCC may require a transfer impact assessment. If the two documents are prepared separately, the enterprise may produce inconsistent descriptions of the same data flow. If the two documents describe the same data flow in different ways, the inconsistency itself may be treated as a compliance problem.

Third, the assessment of compliance effects is different. Satisfying one set of rules does not necessarily satisfy the other. For example, an enterprise has passed China's security assessment, but if the country where the data recipient is located has not obtained a GDPR adequacy decision and the parties have not signed SCC, the transfer activity is still non-compliant under the GDPR framework. Conversely, if an enterprise has signed SCC but has not applied for security assessment as required by Chinese law, it also constitutes a violation under Chinese law. The two sets of rules independently judge compliance, and enterprises must pass the test of both sets of rules at the same time in order to achieve complete compliance.

DOI: 10.54254/2753-7048/2026.JO39451

From the above three aspects, it can be seen that the root cause of the compliance dilemma in cross-border data transfer is not that Chinese rules are too strict, nor that GDPR standards are too high, but that there is a lack of coordination mechanism between the two sets of rules. Both sets of rules have their own institutional rationality, but their institutional logic, procedural nature, and assessment standards are not connected with each other, causing enterprises to repeatedly weigh between two parallel and incompatible rule systems. This is the institutional cause of the dilemma. The cause lies in the relationship between the two systems, not in either system taken alone.

4. Coordinated pathways

Some research points out that the security assessment system has systemic defects in terms of regulatory hierarchy, compliance pathways, and identification standards, which further shows that merely improving domestic institutions cannot solve the problem [10].

Based on the above analysis, the direction of solving the problem is not to unilaterally improve domestic institutions or require the GDPR to lower standards, but to establish coordination and mutual recognition mechanisms between the rules. Regional cooperation frameworks provide possible pathways for this. For example, the Regional Comprehensive Economic Partnership (RCEP) contains provisions on cross-border data flows in Chapter 12 (Electronic Commerce), Article 12.15, and allows parties to adopt measures for public policy objectives. This does not create a full mutual recognition mechanism, but it provides a starting point for discussion. The specific institutional design of this direction needs to be further explored in subsequent research. The point here is not that RCEP already solves the problem, but that regional frameworks may offer a less costly path than unilateral reform or bilateral negotiation. Such frameworks do not remove the differences between the two rule systems. What they may do is to create a space for discussion, in which those differences can be addressed over time.

5. Conclusion

This paper analyzes the causes of compliance dilemmas in cross-border data transfer from the perspective of institutional coordination. The study finds that the problem is not that domestic rules themselves are too strict, but that there is a lack of effective coordination between domestic rules and the GDPR. The two sets of rules have institutional contradictions in three aspects: compliance standards, procedural nature, and effect assessment. Enterprises must simultaneously satisfy two parallel and incompatible sets of rule requirements, and compliance difficulties arise therefrom.

The significance of this finding is that it shifts the focus of reform. If the problem were simply that domestic rules are too strict, the solution would be to relax them. If the problem were simply that GDPR standards are too high, the solution would be to negotiate exemptions. However, if the problem is a lack of coordination between two rule systems, then the solution must involve coordination mechanisms. This paper suggests that regional frameworks such as RCEP may provide a starting point, although the specific design needs further study. This finding also has practical value for enterprises. If the problem is coordination rather than strictness, enterprises should not simply wait for domestic rules to be relaxed. They should monitor how regional frameworks develop and prepare internal compliance documents that can be adapted to different rule systems. This does not remove the double compliance burden, but it may reduce the cost of adjusting to future changes.

The paper has limitations. It does not measure the actual compliance cost of enterprises, nor does it examine how different industries experience the tension between the two rule systems. It also does

DOI: 10.54254/2753-7048/2026.JO39451

not discuss in detail how coordination mechanisms would work in practice. Future research could focus on specific industries, such as cross-border e-commerce or financial services, and examine how enterprises in those industries choose between different compliance paths. Future research could also examine whether and how regional frameworks can be used to reduce the double compliance burden without lowering data protection standards.

References

[1] Huang, Q. X. (2025). On the compliance dilemma and optimization path of corporate data cross-border transfer. *Wuhan University International Law Review, 9*(1), 36-52.
[2] Guo, D. X. (2024). Multiple dilemmas and path innovation in China's data cross-border security governance. *Law Review, 42*(3), 170-181.
[3] Zhao, J. W. (2023). On the systematization of rules for cross-border data assessment, contracts, and certification. *Administrative Law Review, 1*, 78-94.
[4] Voss, W. G. (2020). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal, 29*(3), 485-531.
[5] Measures for security assessment of data cross-border transfer. (2022). Order No. 11 of the Cyberspace Administration of China.
[6] Measures for standard contracts for cross-border transfer of personal information. (2023). Order No. 13 of the Cyberspace Administration of China.
[7] Ding, X. D. (2023). Jurisprudential reflection and institutional reconstruction of cross-border data flows: A comment on the measures for security assessment of data cross-border transfer. *Administrative Law Review, 1*, 62-77.
[8] European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.
[9] Jin, J. (2023). EU rules, global standards? "Race to the top" in cross-border data flow regulation. *Peking University Law Journal, 1*, 46-65.
[10] Wang, D. (2025). The institutional construction of data cross-border security assessment. *Legal Science, 43*(5), 100-111.