

Construction of Access Rules for Data Transaction Subjects

Simin Li¹

¹ School of Cyber Science and Engineering, Wuhan University, Wuhan, Hubei 430072, China

Correspondence: Simin Li, School of Cyber Science and Engineering, Wuhan University, Wuhan, Hubei 430072, China.

doi:10.56397/LE.2024.11.08

Abstract

At present, data exchanges have been set up in various provinces and cities in China, but China has not yet established uniform rules for data transactions. As an important threshold to ensure the security of data transactions, it is of great significance to construct access rules for data transaction subject. By building access rules for data transaction subjects, data transaction rules will be gradually improved, which is also a positive response to China's policy requirements. Adhering to the principle of ensuring data security and promoting the release of data value, this paper analyzes the existing rules of data exchanges and explores the construction ideas of access rules for data transaction subjects. Data transaction subjects can be divided into data providers and data demanders. In addition to examining the basic situation of the subject of the transaction, a more detailed examination is needed. For data providers, it is necessary to review whether they have any recent data-related violations and whether they have a sound data compliance management system. For data demanders, it is also necessary to review their data-related breaches, cybersecurity protection capabilities, and data security protection capabilities.

Keywords: data transaction, data transaction rules, access rules for subjects, data security

1. Introduction

With the advent of the digital economy era, data has become a new engine for economic development. In October 2019, the Fourth Plenary Session of the 19th Communist Party of China (CPC) Central Committee included data as a production factor for the first time, laying the foundation for subsequent market-based allocation of data elements and related policy formulation. The Opinions on Improving the Systems and Mechanisms for Market-based Allocation of Factors of Production released in April 2020 explicitly stated the need to accelerate the cultivation of the data element market. In December 2022, the Opinions on Establishing a Data Base System to Maximize a Better Role of Data Elements clearly proposed the introduction of management methods for data exchanges and the establishment of comprehensive data transaction rules. In July 2024, Resolution of the Central Committee of the Communist Party of China on Further Deepening Reform Comprehensively to Advance Chinese Modernization clearly indicated the need to work faster to set up a system for data market transaction. Currently, the Chinese government is vigorously promoting the construction of data transaction rules, but unified data transaction regulations have not yet been formed.

The admission rules for data transaction participants are crucial gatekeepers for ensuring the security of data transactions. At present, big data transaction platforms only conduct formal reviews to verify the authenticity of the identities of both transaction parties but do not establish corresponding admission mechanisms for data transaction participants, which cannot meet data security and management requirements. Therefore, this paper discusses the necessity of the construction of access rules for data transaction subjects and proposes specific ideas for rule construction.

2. The Necessity of Establishing Access Rules for Data Transaction Subjects

Due to the replicability and unbounded dissemination of data, the absence or low threshold of participant admission regulations can lead to hidden risks such as data breaches and tampering. Establishing access rules for data transaction subjects is essential for ensuring data security, unlocking data value, and developing the data element market. Therefore, this regulatory gap urgently needs to be filled.

Establishing access rules for data transaction subjects is a necessary requirement to ensure data security. In the digital age, data security has become the key foundation for the long-term stable development of the data element market. According to Article 3 of the Data Security Law of the People's Republic of China, data security refers to employing necessary measures to ensure that data is effectively protected and legally used, as well as having the capacity to ensure a sustained state of security. Entities that breach data security are no longer limited to individuals and organizations taking attack measures but also extend to those who fail to take necessary protective measures. For example, data breaches due to technical vulnerabilities or poor management, and illegal data transactions driven by profit motives. Whether data is secure is closely related to the rights and interests of data providers, suppliers, and users. Establishing access rules for data transaction subjects can limit data security risks to a controllable range and effectively prevent illegal data transactions.

Establishing access rules for data transaction subjects is a practical need to fully unlock the value of data. The system of the data element market should both ensure data security and promote data development. Constructing clear and flexible access rules for data transaction subjects helps support the circulation and trading of different levels of data within a controllable range, fully mining and amplifying the value of data while ensuring security. For entities with stronger data security capabilities, the scope of data they can trade is greater. In practice, the Beijing International Data Exchange divides data buyers into four levels, with different levels corresponding to different data purchasing capabilities.

Establishing access rules for data transaction subjects is a requirement for improving the development of the data element market. By establishing access rules for data transaction subjects which can clarify the access threshold for the data transaction market, it helps to establish subsequent universal technical standards and rules for data delivery. And this is also a legal response to calls for establishing sound data transaction rules and improving the data element market. Additionally, setting access rules for data transaction subjects will effectively promote the standardization of data transaction processes, reduce transaction costs, and improve the transparency and efficiency of transactions.

3. Establishing Access Rules for Data Transaction Subjects

According to most of local data transaction management measures, data transaction participants include not only the supply and demand sides but also data merchants, data intermediaries, and data transaction service institutions. According to the principle of privity of contract, the actual subjects in a data transaction are the data provider and the data demander. When conducting data transactions, the identities of other participants like data merchants and data intermediaries correspond to that of either the data providers or the data demanders. At other times, they merely assist in the conduct of data transactions rather than being the actual subjects in the transaction.

3.1 Access Rules for Data Providers

A data provider, also known as a data seller, refers to a civil subject that provides data and receives corresponding payment.

The examination of transaction subjects by data exchanges can be divided into formal examination and substantive examination. According to local management measures or the practices of various data exchanges, the focus of the examination for sellers is primarily on the data they provide, while the sellers themselves are generally only subject to a formal examination. Specifically, sellers should register at the exchange and submit legal proof of their data sources. Only after the exchange has reviewed and approved the above information can they proceed with data transactions. The Interim Measures for Data Transaction Management in Shenzhen impose higher requirements on the qualifications of data sellers. To engage in data transactions, data sellers must first become data merchants or be recommended by data merchants. However, there are some data exchanges conducting substantive examinations of sellers. For instance, the Jiangsu Big Data Exchange conducts a review of providers' compliance management systems for data. The key aspects of the review include basic information, credit status, qualifications, data security protection capabilities, and compliance commitment to services.

It is necessary to impose more qualification restrictions on data sellers in the entity registration process at data exchanges. In addition to conducting a review of basic information such as legal establishment, effective continuance, credit status, and qualifications, it is also essential to perform a substantive examination of the overall data compliance situation. Firstly, examine whether the data seller has engaged in any recent data-related violations. For example, the Shanghai Data Exchange requires confirmation that the applicant has not received any administrative penalties or industry sanctions related to data transactions or privacy protection over the past

three years, and that there are no significant data-related legal or regulatory violations by the applicant's legal representatives, directors, or supervisors. The existence of data violations can reflect the seller's awareness and ability to ensure data legality and compliance from a results-oriented perspective. Secondly, review whether the data seller has a comprehensive data compliance management system. For data exchanges, a comprehensive data compliance management system serves as an endorsement of good corporate governance and effective risk control. The establishment and improvement of a data compliance management system not only reflects the seller's awareness of data protection but also effectively prevents data compliance risks, contributing to safe and orderly transactions within trading venues. For data buyers, it is impossible to fully understand and investigate the data before a transaction; therefore, compared to confirming that the purchased data has no compliance issues, buyers often place more emphasis on whether the data seller possesses a comprehensive data compliance management system.

3.2 Access Rules for Data Demanders

A data demander, also known as a data buyer, refers to a civil subject that pays for and obtains corresponding data.

There is a consensus among local management measures on the requirements for data buyers: they should have the technical ability to protect and apply data securely. In practice, the review of data buyers is essentially substantive. For example, the Beijing International Data Exchange categorizes data buyers into four levels, with different levels of data demanders corresponding to different data procurement capabilities. On top of meeting the basic qualification requirements, demanders' levels are comprehensively determined based on their capabilities which include network security protection ability, data security protection ability, and other abilities. Similarly, the Jiangsu Big Data Exchange requires a review of the data demander's basic information, transaction motivation, purpose or goal, expected derivative data, transaction contracts, and delivery methods.

Regarding whether a data buyer can enter the market for data transactions, firstly, the examination of whether there are any data-related violations applies equally to the data buyer. This is not only key to establishing a trust relationship between buyers and sellers but also concerns compliance risk issues during the data utilization phase, which, meanwhile, align with the requirement to strengthen the full-process compliance governance of data market entities. Secondly, it is necessary to examine the network and data security protection capabilities of the data buyer during entities access phase because this directly concerns the security issues after the data transaction. To fully protect the interests of the data provider, especially in transactions involving raw data, it is essential to require the data buyer to have security protection capabilities commensurate with the level of transaction data. This rule helps minimizing risks such as data tampering and leakage beforehand as much as possible.

In the case of the data buyer's transaction motivation, purpose, transaction contracts, delivery methods, and whether they have a data compliance management system, there is no need to review these aspects during entities access phase. After the data buyer obtains access to the exchange, they will engage in various data transactions. As the market environment changes, the data buyer's transaction motivation and purpose are likely to change. The content of the transaction contracts reached through negotiations between the parties varies with each transaction. These details, which can only be finalized during specific transactions, do not require immediate or comprehensive review upon the data buyer's entry but should be reviewed when signing the transaction contract. Additionally, taking into account that the buyer may not directly process data but outsource data processing to third parties or sellers may maintain data within their domain through special delivery methods, it can be decided on a case-by-case basis whether to require the buyer to have a data compliance management system.

Lastly, it should be noted that some exchanges stipulate that individual entities are temporarily not allowed to conduct transactions. It is believed that this provision is inappropriate. Currently, except for the Henan Province Data Transaction Management Measures (Trial) (Draft for Comments), which states that data transaction subjects only include legal persons and other organizations, management measures in Tianjin, Guizhou, Hubei, and other places recognize that citizens can also act as data transaction subjects and engage in transactions at exchanges. Although in practice, individuals may be unable to gain access to exchanges due to lacking data processing and security protection capabilities. However, national-level documents have not explicitly excluded individuals from data exchanges. Therefore, data exchanges have no justifiable reason to refuse individuals from conducting transactions and should establish a dedicated access channel for individuals.

When individuals apply to enter data exchanges, they should provide materials proving their creditworthiness, financial status, and other basic information. The main challenge when applying the established access rules for data transaction subjects to individuals is that individuals find it difficult to establish a data compliance management system alone; however, no obstacles present when other rules, such as reviewing for any data-related violations and assessing network and data security protection capabilities, are applied to individuals.

The purpose of requiring data transaction subjects to have a data compliance management system is to demonstrate good data management capabilities and prevent data compliance risks. When reviewing individual entities for access, it is acceptable as long as individuals can provide corresponding alternative proofs. Admissible alternative proofs include individuals having technical abilities to ensure data security, establishing a technical safeguard system capable of preventing basic risks, or receiving data security services from industry-recognized third parties.

4. Conclusion

Data transaction rules are not built overnight. When constructing access rules for data transaction subjects, it is necessary to consider both data security and the release of data value. Setting no restrictions is impractical, and a one-size-fits-all rule is even more so. As to how to manage data transaction subjects, it is essential to strike a balance between liberalization and regulation, maintaining market vitality while upholding order in the data element market through effective supervision. We must base our approach on practical needs, summarize the practical experiences of various data trading venues, and explore access rules for data transaction subjects that is adapted to Chinese conditions.

References

- Beijing International Data Exchange, (n.d.). Buyer Tier Management? <https://www.bjidex.com/guide>.
- Chen Bing, (2024). Legal Advancements in the Market-Oriented Allocation of Data Elements — A Discussion on the Design of the “Twenty Articles on Data”. *Journal of Shanghai University (Social Sciences Edition)*, 41(01), 1-13.
- Xu Zhongyuan, Zheng Huangjie, (2024). The Institutional Construction of Empowering New Quality Productivity through the Marketization of Data Elements. *Theory and Reform*, 1-18 [2024-11-13]. <http://kns.cnki.net/kcms/detail/51.1036.D.20241030.1411.008.html>.
- Yan Haoyu, (2023). Institutional Requirements and Legal Guarantees for Cultivating the Data Element Market. *Journal of China University of Mining and Technology (Social Sciences Edition)*, 25(03), 73-90. DOI:10.20089/j.cnki.issn.1009-105x.2023.03.007.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).