Research on the Compliance Path and Trust Law Improvement for Trustor Personal Information Protection in Trust Business in the Big Data Era

Chao Yang[1, a], Zhibo Xue[2*]

[1]Tianjin University of Commerce, Tianjin, China
[2]Ministry of Transport Waterway Science and Technology Institute, Beijing, China

[a]13504465905@163.com
[*]929249520@qq.com

Abstract. Under the new circumstances, fulfilling trust management responsibilities requires the support of big data in the refined development of trust business. However, this move increases the risk and probability of trustor information being leaked or exploited by trust companies. Currently, trust companies lack internal compliance awareness and systems, have unclear legal responsibilities for external cooperation, and lack effective division of labor and coordination in administrative supervision. Furthermore, the Trust Law lacks specific provisions for protecting trustor personal information, resulting in poor coordination with regulations protecting trustors' use of trust property. These factors complicate the protection of trustor information. This study examines the practical and existing challenges of trustor information protection in the context of big data and explores a compliance path for trustor personal information protection that involves "trustor self-optimization, trustor collaborative management, and joint supervision by regulatory agencies." Based on this, the study proposes the following recommendations: adding a dedicated section to the Trust Law on protecting trustor personal information, specifying the special legal obligations of trustors, establishing a reverse burden of proof, establishing a trustor compensation fund, and developing and improving supporting laws and regulations alongside the Personal Information Protection Law and the Financial Stability Law. This study aims to provide practical assistance to trust companies' compliance practices and contributes positively to filling the gaps in the legal system for trustor information protection.

Keywords: big data era; trust business; trustor’s personal information; compliance path; trust law improvement

1 Current Status and Challenges of Protecting Trustor’s Personal Information in Trust Business in the Big Data Era

Under the background of big data, the practical predicament of protecting the personal information of trustor in trust business has permeated multiple levels such as internal

H. Dai et al. (eds.), *Proceedings of the 2025 5th International Conference on Business Administration and Data Science (BADS 2025)*, Advances in Computer Science Research 125,
https://doi.org/10.2991/978-94-6463-980-3_9

management, external cooperation and regulatory coordination, and echoes the information scope, circulation characteristics and negative impacts of big data mentioned earlier. Internally, most trust companies have yet to establish a suitable technical and institutional system[1]. According to industry research data, among the 68 domestic trust companies, only 35% have completed the construction of a hierarchical management system corresponding to the four types of information: identity, income and expenditure, transactions, and privacy. Small and medium-sized trust companies are particularly lagging behind, with approximately 68% not having integrated lightweight privacy computing tools. This has led to a 38% rate of duplicate storage of core information such as customer asset certificates and risk preferences during internal departmental circulation, which not only violates the principle of "necessary circulation" but also magnifies the risk of leakage[2].

The issue of ambiguous responsibilities at the external cooperation level is more prominent. In 2023, a trust company in East China cooperated with a third-party investment advisor who did not meet the third-level data security qualification. Due to the failure to clearly define the boundaries of data usage, the information on the benefit distribution intentions of 217 family trust trustees was leaked. Subsequently, as the cooperation agreement did not stipulate the compensation ratio, Trust companies can only bear 72% of their clients' losses on their own, which confirms the pain point of "unclear legal responsibilities for external cooperation"[3].

There are also obstacles in the regulatory and rights relief links. A joint inspection by the banking and insurance regulatory department and the Cyberspace Administration of Guangdong Province in 2024 revealed that due to differences in data statistics standards between the two sides, the behavior of three trust companies transmitting customer transaction information beyond the scope was not discovered until 48 hours after it occurred, making real-time control impossible. In addition, the imbalance of rights and interests caused by algorithmic black boxes is not uncommon. A certain client in Beijing once questioned the trust company for using its risk tolerance data for non-trust marketing. However, as the company was unable to disclose the algorithmic logic, it ultimately failed to protect its rights due to insufficient evidence. This is consistent with the conclusion that "black box algorithms exacerbate the imbalance of rights and interests", and also provides a realistic basis for the subsequent construction of compliance paths and improvement of laws.

2 Construction of a Compliance Path for Protecting Trustors' Personal Information in Trust Business in the Big Data Era

2.1 Optimization of trust companies' internal compliance systems

In terms of technology, we need to overcome the barriers to implementation. For small and medium-sized companies that lack technology, on the one hand, we need to share lightweight privacy computing tools. For example, we can promote the Trust Industry Association to build a unified federated learning module resource pool within 1 year, supporting small and medium-sized trust companies to complete the integration of

existing business systems within 3 months after access, so that only model parameters are transmitted without presenting original data during the customer profiling process, thus streamlining the repeatedly collected "big data"; on the other hand, we need to develop a middle platform for industry-shared data security, complete the preliminary construction of the middle platform (integrating real-time risk control algorithms and blockchain evidence storage functions) within 2 years, achieve complete traceability of the information chain and generate abnormal alarms within 15 minutes [4]. Large companies can open technical solution templates of leading companies within 1.5 years to provide cost reduction capabilities.

2.2 Improvement of regulatory coordination and compliance supervision mechanisms

A unified national trust information supervision platform will be established. The China Banking and Insurance Regulatory Commission (CBIRC) shall take the lead, and jointly with the Cyberspace Administration of China (CAC) and the People's Bank of China (PBC) to complete the platform's project approval, development and testing within 2 years, and realize the full access of business data of 68 trust companies nationwide and shared records of cooperative institutions within 2.5 years [5]. The platform will embed big data risk control models to automatically issue warnings for behaviors such as over-range collection and abnormal data flow, thus realizing a closed loop of "real-time monitoring - risk identification - violation handling"; the platform shall complete the connection with the blockchain evidence storage system within 3 months after launch to retain traces of regulatory operations and ensure that supervision is traceable.

3 Paths to Improve Trust Law for Protecting Trustor’s Personal Information in the Big Data Era

The coordinated improvement of supporting legal systems needs to focus on the characteristics of trust business and build a multi-layered protection system of "special legislation + judicial interpretation + industry norms", with clear implementation time limits:

First, promote the in-depth integration of the Personal Information Protection Law with trust scenarios. The Standing Committee of the National People's Congress shall launch the research and drafting of a special decision in the short term (1-2 years), and formally issue it in the medium term (2-3 years), refining the "minimum necessary" exceptions for trust due diligence and information use during the trust term, and clarifying the specific conditions for exempting sensitive information of family trusts (such as inheritance arrangements) from routine disclosure. Trust companies shall complete the compliance self-examination and adjustment of internal information collection processes within 3 months after the release of the special decision to avoid the general application of general legal provisions.

Second, improve the supporting rules of the Data Security Law. The Ministry of Industry and Information Technology (MIIT) shall jointly with the CBIRC complete the project approval and draft formulation of the national standard "Guidelines for Data Classification and Grading in the Trust Industry" within 1 year, and complete the solicitation of opinions and formal implementation within 1.5 years. The guidelines shall incorporate the four-level data classification into the legal framework, clarify the transmission encryption standards for core data (such as client asset privacy) and the audit frequency of sensitive data (e.g., quarterly audits for core asset data, monthly audits for sensitive transaction data), providing a legal basis for the application of internal compliance technologies. Trust companies shall complete the upgrade of data encryption technologies and the landing of audit mechanisms within 6 months after the implementation of the guidelines.

Third, optimize the legal basis for coordinated financial supervision. Add trust data security clauses in the revision of the Financial Stability Law (to be completed in the medium term (2-3 years)), clarifying the joint law enforcement powers and responsibilities of the CBIRC and the CAC, and stipulating the time limit for cross-departmental regulatory information sharing (no more than 24 hours) to resolve the obstruction of "multiple management"; meanwhile, the Trust Industry Association shall complete the formulation of the "Information Protection Operational Guidelines" within 1 year, refining the industry standards for partner qualification review (e.g., re-verification of ISO 27001 certification every 3 years) and emergency response (e.g., joint traceability process for leakage incidents). The Association shall organize industry-wide training within 3 months after the release of the guidelines, ensuring that trust companies and cooperative institutions complete the adaptation of operating processes within 6 months.

There are significant limitations in the compliance path: small and medium-sized trust companies find it difficult to bear the costs of data classification encryption and the deployment of privacy computing tools, and their technical adaptation capabilities are insufficient. Cross-departmental supervision, such as the collaboration between CBIRC and CAC, is prone to barriers, and standards are difficult to unify, which affects the efficiency of supervision. Moreover, technologies such as blockchain evidence storage are insufficiently compatible with the independence rules of trust properties, and the implementation of some compliance requirements lags behind, weakening the effectiveness of personal information protection.

4 Conclusion

In the new journey of the trust industry's transformation and development under the power of the digital economy, the protection of trustors' personal information will become a practical and strategic issue faced by the trust industry's innovative development and risk management and control. This has important theoretical and practical significance for promoting the construction of a financial data security governance system and achieving compliant digital transformation in the trust industry. In the future, the full traceability of trust data can be achieved by relying on blockchain, and

data desensitization can be carried out through federated learning and homomorphic encryption to balance security and sharing. It is also necessary to adapt to the independence of trust property, build a technical compliance system, and defuse the risks of data rights confirmation and transfer.

References

1. Liddell, Kathleen Mary, and J. M. Skopek. "Informed Consent for Research Using Biospecimens, Genetic Information and Other Personal Data." Social Science Electronic Publishing (2018).
2. Chen, Jiajun, et al. "A Trust-Based Personalized Differential Privacy Guarantees for Online Social Networks." IEEE Transactions on Network and Service Management (2025):1-1.
3. Svenson, Frithiof, Eva Ballová Mikuková, and M. A. Launer. "Credibility and trust of information privacy at the workplace in Slovakia. The use of intuition." Journal of Information, Communication and Ethics in Society 21.3(2023):302-321.
4. Lomotey, Richard K., et al. "Synthetic data digital twins and data trusts control for privacy in health data sharing." Proceedings of the 2024 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems. 2024.
5. Zhu, FangBing, and Zongyu Song. "Systematic regulation of personal information rights in the era of big data." SAGE Open 12.1 (2022): 21582440211067529.