

Trustee's Obligation of Data Trust from the Perspective of Balancing Personal Information Protection and Data Circulation

Tao Liu *

School of Humanities, Beijing University of Posts and Telecommunications, Beijing, China

* Corresponding Author Email: liutao5789@bupt.edu.cn

Abstract. Data plays a key role in current society with its security facing challenges. In this context, data trusts have emerged, but the trustee's obligations are vague. The theory and practice of data trust in Britain, the United States, Japan and other countries are developing vigorously. However, China has not yet established a relevant legal system with different views on the trustee's obligations in academia. According to the further analysis of a tripartite legal relationship of data trust, the significance of the data controller as the settlor, the admission standards of the trustee, and the multi-beneficiary theory are emphasized. From the perspective of balancing personal information protection and data circulation, it is proposed that personal information protection is the foundation of data trust. Meanwhile, data circulation with public goods and economic value attributes is the driving force for the development of data trust. Finally, the trustee's legal obligations during the establishment, continuance and termination of the trust should be further refined, including reasonable negotiation obligations, fiduciary obligations for data management, data confidentiality obligations, and income distribution obligations.

Keywords: Data Trust; Personal Information Protection; Data Circulation; Trustee's Obligations.

1. Raise of the Question

Data plays a key role in current society, which supports decision-making, drives innovation, provides personalized services, predicts future trends, and optimizes resource utilization. However, data, as the treasure of the 21st century, is encountering difficulties such as illegal abuse and improper development. Thus, it is urgent to build a more complete data governance to solve the present dilemma. In 2022, the Central Committee of the Communist Party of China and the State Council issued the *Opinions on Building a Basic Data System to More Effectively Maximize the Role of Data Elements* (hereinafter referred to as *Twenty Data Measures*). According to the sixth measure, the mechanism for the trustee should be explored to supervise the collection, processing, and use of personal information data by market players on behalf of personal interests. This is very similar in composition to the foreign data trust mechanism, so numerous scholars have studied the introduction of the data trust system into the Chinese data governance system. Data trust has mainly developed two foreign theories in Britain and the United States. Jack M. Balkin, a professor at Yale Law School, took the lead in proposing the specific concept of "data trust" and then proposed the scheme of information trustee. Such a scheme relies on imposing fiduciary obligations on data controllers. In other words, the trust trustee is to achieve a balance between the data subject and the data controller. The data trust scheme proposed by Britain proposed to set up a third-party organization as a trustee, which integrates the scattered data information of the data subject and transacts with the data user. In the process, it shoulders fiduciary obligations to balance the legal relationship of the data trust. The Japanese approach is the same as the British solution of data trust, but it is called "information bank", which aims to manage personal data and all kinds of data through personal accounts. The data provider stores the data in the personal data storage system by signing a data use contract, and the information bank acts as an intermediary to provide the data to a third party according to the individual instructions. A third-party enterprise can use data to conduct commercial activities, and part of the proceeds will be returned to individuals to promote data circulation. The data subject entrusts the information bank to manage the data based on the trust legal relationship, so as to protect

personal information while promoting data circulation. Most countries prefer the British data trust scheme, so this paper is mainly premised on the British data trust scheme for in-depth analysis.

Data trust has a lot of experience in foreign countries, but China has not yet established a legal system for data trust. Regarding the issue of the trustee's obligations in data trust, the academia also holds different views without consensus. Some scholars believe that the trustee's obligations should give priority to protecting personal information and maintaining privacy and security [1]. Some other scholars hold that the trustee's obligations should be more inclined to efficient data circulation [2]. However, balancing these two aspects, this paper proposes how to establish the trustee's obligation during the data trust to ensure the protection of personal information privacy for natural persons and enterprises during the circulation, and to ensure that data can be carried out at a high speed under a safe channel to promote data transactions by circulation.

2. Tripartite Legal Relationship of Data Trust

Before analyzing the trustee's obligations, we need to clarify the composition and structure of the legal relationship of data trust. From the theoretical perspective, the data trust scheme was originally managed by Shane McDonald through the citizen trust in 2015 [3]. In June 2016, Neil Lawrence proposed a scheme for independent management of personal data through data trusts in *Data Trust Could Allay Our Privacy Fears* [4]. Since then, Britain has initiated the practice of data trust theory [5].

The manifestation of this scheme is to replace the various subjects of the data in the trust legal relationship. Specifically, a third-party subject is introduced between the data subject and the data user, which must have the ability to process data and qualifications to be trusted. Such a third-party subject is generally called data controllers in academia. The data subject, that is, the matrix of the data generation, hands over the data to the trustee data controller as the settlor. Meanwhile, the data controller integrates and processes the data, enabling the personal data of several settlors to be a dataset with certain economic value. After that, the data controller transacts with the data user who uses the acquired data to generate commercial benefits and pays a reasonable consideration to the data controller. The beneficiary is the client himself. The tripartite structure in the trust legal system is fixed, with the following elaborated from the perspective of the tripartite subjects.

(1) Settlor

In a data trust, the settlor tends to be the data subject, that is, the vast number of network users and data providers. Some scholars believe that the settlor of data trust only includes individuals, but this paper denies this view [6]. The data controller can also become the settlor of the data trust [7]. The original purpose of data trust is to solve the inefficient personal data protection and data circulation, and the data service capabilities of data controllers also vary. Using the data controller as the settlor and other data controllers as the trustee can promote the essential purpose of data trust. Firstly, the cost of transferring data between the settlor and the trustee should be reduced, so as to decrease the aggregation of scattered data subjects to a few data controllers and improve the efficiency of data circulation. In other words, it reduces the distance of data flow. Secondly, the cost of trustees processing data should be reduced. The data received by the data controller as the trustee must not be absolutely scattered and disorderly information, which is beneficial for the trustee to better process, analyze, and process data. Finally, the value conversion rate of data should be improved to stimulate the potential of data elements, optimize production capacity attributes of data obtained by data users from data controllers, and use a certain capacity of data to create more data benefits [8]. Hence, the existence of the data trust settlor should be in the following forms including the data subject, the data controller, and the data subject with the data controller as the settlor.

(2) Trustee

The trustee of a data trust is a data controller, which needs to have two characteristics. On the one hand, it must have sufficient ability to analyze, process, and utilize numerous personal data. On the

other hand, the allocation of public goods such as data should be adjusted for social public interests [9].

As a third party, data controllers have little practice in China. Based on the opinions of some scholars, some existing trust companies are used as trustees to expand data trust business to cater to the growing data society. These trust companies need to obtain trust licenses with relevant qualifications that meet the requirements of the *Measures for the Administration of Trust Companies* and *Measures of China Banking Regulatory Commission for the Implementation of Administrative Licensing Matters for Non-bank Financial Institutions*. Besides, these trust companies need to expand their data service business and foster data processing capabilities, so as to become a qualified data trust trustee. Based on the opinions of some other scholars, a data service organization should be established to undertake the digital work of collecting, handling and processing. These data service organizations need to apply to the government for relevant qualification documents, which requires them to exercise their rights as much as possible for the benefit of the client. Undoubtedly, their premise lies in a trust foundation between the settlor and the trustee. Only when the data controller demonstrates to the data subject that it has the ability to protect the data security and is willing to undertake fiduciary obligations can it fully obtain the trust of the data subject and then promote the trust establishment. It is not appropriate to set too strict or loose entry thresholds for data service capabilities. To balance personal information protection and data circulation, an entry threshold is needed to improve the professionalism of data trust trustees, thereby protecting personal information. The excessively high capacity entry threshold is to allow more data trust trustees who meet the requirements to perform their functions in the market and ensure data circulation.

As for the public service capacity, since the data trust trustee is a third-party platform, the intermediary agency between the data subject and the data user has to conduct transactions with the data user. Given that the data user is a profit-making legal person, the private subject is willing to make a profit. Excessive pursuit of profit-seeking may lead to infringement of the personal information of the data subject. Hence, the data controller, as a trustee, must be entrusted and loyal to others, protect the public goods of data intact, and protect it from infringement as much as possible within the autonomy of the data subject. Moreover, when abundant data on the data subject is gathered in the data controller, it holds most of the data information of the society, which is related to the public interest. When the public interest of the society conflicts with the interests of the data controller itself, the data controller needs to make concessions. How to ensure concessions? The government can be introduced as a supervisory agency, which requires governmental intervention and social supervision. Through legislation intervention and public power, this unequal status quo can be eliminated, and the platform can be urged to fulfill its obligations, providing a foundation for forming a trust system with a strong guarantee [10].

(3) Beneficiary: Multi-beneficiary Theory

According to the *Trust Law of the People's Republic of China*, the settlor can be the beneficiary or the sole beneficiary of the same trust. The trustee can be the beneficiary, but must not be the sole beneficiary of the same trust. In other words, when the data subject or the data controller is the settlor, it can become the beneficiary. When the data controller is not the settlor, it cannot be the sole beneficiary. Xu Tianxi, a scholar who supported a single beneficiary, believed that the data subject (as the beneficiary), the data user (company, as the trustee) and a third-party public or private legal person (as the settlor) constitute a tripartite trust relationship [11]. This view ignores the diversity of beneficiary identities, which is not desirable.

Scholars supporting the multi-beneficiary theory hold that the settlor of a data trust should realize the transformation from a data subject to a data controller. In other words, the data controller is the settlor and becomes a trust co-beneficiary with the data subject, which does not exclude the data subject from bringing their personal information to the data trust alone [9]. The beneficiary of a data trust should be a multi-subject model, which can be understood as the only data subject or the only data controller or the only third party designated by the settlor. Beneficiaries can include both data subjects

and data controllers, which is consistent with the overall architecture of balancing personal information protection and data circulation. If the beneficiary can only be the data subject, then the protection loss of the interests of the data controller during the data trust will reduce the quality of data circulation. If the data subject cannot be the beneficiary, then the protection of personal data is out of the question. Therefore, data subjects, data controllers, and a third party selected by the settlor should be included in the beneficiary subjects of data trusts, so as to strengthen the balance between personal information protection and data circulation of data trusts.

3. Trustee's Obligations of the Data Trust in the Whole Process

(1) Trustee's Obligations of the Data Trust at the Establishment Stage

The establishment of a trust is the initial stage, where the trustee of a data trust has the following three obligations. Firstly, assist the settlor to achieve the settlor's trust purpose in the trust agreement, which must conform to the settlor's wishes. The trustee needs to provide the settlor with the necessary advice to ensure that the trust establishment goes smoothly. As an organization or trust company with data service capabilities, the trustee is obliged to provide a pre-drafted standard contract, and negotiate with the settlor on individual terms during the establishment stage. Secondly, the trustee is obliged to review the compliance of the trust establishment to ensure that it complies with applicable laws and regulations. Thirdly, the trustee needs to be responsible for registering the trust assets to ensure that all data assets are accurately included in the management of the trust. Meanwhile, data rights need to be registered as trust property. Although the law does not stipulate that data rights need to be registered as trust property, personal information can be better protected in the system after registration, so that data rights can be publicly certified by specialized agencies. Data provides the necessary guarantee in circulation. As for registration agencies, there is currently no agency specializing in data asset registration in China. Existing institutions such as the National Data Bureau can be ideal, whose responsibilities are to coordinate and promote the construction of basic data systems, coordinate the integration, sharing, development and utilization of data resources, and enhance digital China, digital economy as well as digital society planning and construction. Hence, it is suitable to be a registration agency for data rights.

The issue of trust property is quite controversial in the data trust. The mainstream view in academia is that the property of data trust should be the personal data rights established by the *Civil Code*, *Personal Information Protection Law* and other laws, instead of personal data [6]. Some scholars hold that data trust property is personal data, which is not advisable. As mentioned above, the data of data trust has particularity, which leads to the far-reaching impact of data circulation on various market players, and then promotes the development of data trust. Thus, data has a certain economic value only when it is circulated and exchanged. Data rights as intangible property have been confirmed by civil law [7]. The subordinate concept of property rights of data trust objects is expanded and interpreted as property attributes, which is more conducive to taking data rights as trust objects [6] and proves the adaptability of data trusts to the Chinese legal system. The trustee needs to cooperate with the settlor to register data rights and strive to fulfill its fiduciary obligations. For trust property, if relevant laws and administrative regulations stipulate that registration procedures should be handled, trust registration shall be handled according to law.

(2) Trustee's Obligations of the Data Trust at the Continuance Stage

Firstly, the trustee needs to distinguish the data of the settlor to avoid confusion. According to Article 29 of the *Trust Law of the People's Republic of China*, the trustee must manage and record the trust property and its inherent property separately, which is the same for the trust property of different settlors. This article stipulates the independence of trust property, and the trustee needs to distinguish the trust property from other inherent property and the trust property of other settlors. In other words, in the process of collecting and processing data, the trustee will generate "associated data" and "predictive data" in addition to the "active data" provided by the data subject [12]. In this case, the trustee must add these data rights as new trust property to the same trust legal relationship and become

the beneficiary. Then the trustee is obliged to properly manage these three types of data statically, store them reasonably, and provide network defense means when necessary, such as setting up firewalls to protect data security and maintain data rights.

Secondly, the trustee shall handle trust affairs for the best interests of the beneficiaries. When managing trust property, the trustee must fulfill his duties of honesty, credit, prudence and effective management, which is also a fiduciary duty in a trust. The subdivision of fiduciary duty in academia includes two aspects: the duty of loyalty and the duty of diligence. At the establishment stage of data trust, fiduciary obligations should include six aspects. Firstly, confidentiality. The trustee is responsible for ensuring that the trustee's data is properly confidential and not accessed, used, or compromised by unauthorized persons or entities. Secondly, integrity. The trustee shall take measures to ensure the entrusted data is not tampered with, damaged or modified during storage and transmission. Thirdly, availability. The trustee needs to ensure that the trustee data is available to meet the requirements of the trustee. Fourthly, legitimacy. The trustee needs to ensure that laws and regulations are complied with during the collection and processing of data, and that the integrated data collection comply with the provisions of laws and regulations. Fifthly, transparency. The trustee shall provide the settlor with transparency and visibility of data processing activities, including information on how the data is handled, security measures and risk management measures. Sixthly, restrictive. The trustee shall process the data only in accordance with the purposes and conditions specified by the settlor, and shall not conduct any additional data processing beyond the settlor's authority.

Thirdly, if the trustee resigns, he shall still perform the duties of managing trust affairs until a new trustee is elected. The trustee can resign if he meets the conditions in accordance with the *Trust Law of the People's Republic of China*. However, when the new trustee is selected, he needs to store the data in his hands reasonably and perform relevant obligations. When he needs to trade with other data users, he cannot shirk responsibility. When a new trustee is selected, it is also necessary to complete the handover of the data processing process, results, and distribution, which is the obligation the trustee of the data trust should undertake when he resigns.

Fourthly, as for the obligation of income distribution, in traditional trusts, the income generated by the trust is generally listed as fructus and distributed to the beneficiaries as trust income. However, data trust is relatively special. Its special feature is that after receiving the personal data of the data subject, the trustee has to reasonably process and integrate a lot of data, resulting in "active data", "associated data" and "predictive data" [12]. It includes the processing and work of the trustee, which makes the trust property change from the original "active data" as the settlor's property to a union of "active data", "associated data" and "predictive data". Therefore, the data controller, as the trustee and beneficiary under the same trust relationship, must participate in the distribution of trust income. Hence, the trustee must fairly distribute the income in strict accordance with certain distribution principles, taking into account the interests of the beneficiaries agreed upon when the trust was created and its own interests. Concerning the specific method, agreement should be realized on the distribution ratio of trust income between the settlor and the trustee when signing the trust document. As completely equal civil subjects, the distribution can be conducted in accordance with the principle of party autonomy. As one of the parties, the trustee should actively cooperate and engage in the distribution, and put forward distribution suggestions according to the specific situation.

Fifthly, the obligation to allocate public goods. Based on the above-mentioned, personal data can be understood as "public goods" in a broad sense. Public goods are in the hands of the trustee, and the trustee naturally enjoys the obligation to rationally allocate resources such as data. Because the data is rationally allocated, the data user can create more income, which in turn can generate more trust income and the beneficiary (including the trustee) can get more benefits. At that time, the data of the settlor can be protected, the interests of the data controller can be improved, the benefits of the beneficiary can be realized, the needs of the data user can be met, and the data circulation can be smoother. There is no reason for the data controller not to undertake the obligation of this reasonable allocation.

Sixthly, balance the obligations of personal information protection and data circulation. In Chapter 3, the balance between personal information protection and data circulation is proposed. To this end, there are two situations: (1) emphasize personal information protection over data circulation; (2) emphasize data circulation over personal information protection.

“Emphasizing protection over circulation” usually occurs when the data of the data subject is not allowed to be properly used or used by the data controller and data user. For example, it restricts the circulation and sharing of data. Only after multiple authorizations can personal information be accessed and processed. Strict requirements of encryption and security for data high trigger increases data transmission and storage costs. Meanwhile, rigid restrictions on the use of personal information purposes make data only be used for specific and limited purposes, which hinders the circulation and application of data, overemphasizing the rights of data subjects, including the right to know, access, correction and deletion, etc. It may make it difficult for data controllers to legally process and use personal information. In addition, overly strict data protection policies and regulatory mechanisms make it difficult for data controllers to comply with and implement, thus impeding the legal circulation and use of data, etc. In this case, first of all, the trustee can request the data subject to perform its obligations based on the agreed trust documents in accordance with the relevant provisions of the *Civil Code*. Secondly, the trustee should actively promote the rationalization of data circulation, ensure that the circulation and sharing of personal information complies with the provisions of laws and regulations, so as to simultaneously protect the privacy rights and personal information security of data subjects as much as possible. Thirdly, the trustee should establish an effective data management system and process, including data collection, storage, processing, transmission and destruction, to ensure the security and compliance of personal information. Finally, the trustee should continuously monitor data processing activities, assess the risks of personal information protection and data circulation, and take necessary improvement measures to maintain the legality, compliance and effectiveness of data processing activities.

“Emphasizing circulation over protection” often occurs when the personal data of the data subject is abused or infringed by the data controller or data user. For example, it can be data leakage, misuse of personal information such as sending spam, manipulating personal data of data subjects, tampering or fabricating data, etc. Chinese laws and regulations can be combined to find the applicable legal norms, such as the provisions of the *Civil Code* and *Personal Information Protection Law*. On the one hand, if the personal data of the data subject is abused by the data controller, it can be punished in combination with the relevant legal responsibilities of Chapter 7 of the *Personal Information Protection Law*, including Articles 66 to 71. The fiduciary duty of loyalty in this scenario should be detailed to two aspects. It is necessary to prohibit the abuse of trust property, and to strengthen the protection measures for personal data to prevent similar abuse incidents and ensure the safe and compliant use of data. On the other hand, when the personal data of a data subject is infringed by a data user, the relevant provisions of the *Civil Code* on infringement can be applied for regulation. At this time, the trustee needs to fulfill its duty of diligence. Firstly, stop data circulation. The trustee should immediately stop providing data to data users to prevent further infringements or damage to the rights of data subjects. Secondly, cooperate with data subjects and safeguard the rights of data subjects. Thirdly, record and report the infringement situation. The trustee should record the relevant information of the infringement incident, report to the client and relevant regulatory agencies timely, and cooperate with the investigation and handling.

(3) Trustee’s Obligations of the Data Trust at the Termination Stage

During the termination stage of a data trust, the trustee has the following three obligations.

Firstly, stop data processing activities and notify interested parties. The trustee shall immediately stop any processing activities on the data, including the collection, storage, use, transmission and destruction of the data. At the same time, notify the settlor and other relevant parties of the termination of the data trust in a timely manner, and explain the reasons for the termination and follow-up measures.

Secondly, handle data properly. The trustee shall properly handle the data that has been collected, including securely storing, archiving or deleting personal information, so as to ensure that the data is not misused or compromised and process the data according to the client's request. If requested by the settlor, the trustee should hand over the data to the settlor or other designated data manager at the direction of the settlor, ensuring the security and integrity of the data.

Thirdly, settlement and liquidation. The trustee shall complete the settlement and liquidation related to the data trust, including paying the remaining trust funds to the beneficiary, liquidation-related expenses, etc. The repayment obligation at this stage is similar to the obligation of income distribution at the survival stage. The trustee must faithfully judge the distribution of trust benefits in accordance with the trust agreement and the actual situation for fair distribution with honesty and trustworthiness.

Finally, maintain confidentiality. The trustee should continue to perform the obligation of confidentiality and not disclose the relevant information of the data trust to unauthorized third parties, so as to protect the privacy and trade secrets of the settlor and data users. The obligation of confidentiality does not only appear at the termination stage. Before the termination stage, it acquiesces that it cannot disclose the data of the data subject at will because of its fiduciary duty. After the termination of the data trust, some people may think that they are no longer under any obligations, so the processing of the data becomes casual, which may lead to the data being compromised or misused. It should be emphasized that even after the termination of the data trust, personal information cannot be processed at will. Meanwhile, relevant laws, regulations and obligations to protect personal information must still be strictly abided by, which is also the continuity of the trustee's confidentiality.

4. Conclusion

In the current digital age, the importance of data has been increasingly prominent. Correspondingly, there is data abuse and governance. The release of *Twenty Data Measures* and the research on data trust theory in academia have provided new ideas and possibilities for Chinese data governance. Based on the balance between personal information protection and data circulation, this paper puts forward the vital obligations that data trust trustees should undertake, aiming at promoting the legal and efficient conduct of data transactions, and protecting the rights and interests of data subjects and social public interests.

The theoretical exploration and legal system construction of data trust is a complex and long-term task that requires the joint efforts of the government, academia, industry and all sectors of society. We should continue to improve relevant laws and regulations, establish a sound supervision mechanism, and ensure the compliant operation of data trusts and the effective rights protection and interests of beneficiaries. At the same time, it is necessary to strengthen the training and access management of data trustees, enhance their professionalism and sense of responsibility, and cope with increasingly complex data governance challenges. In this process, it is crucial to balance the protection of personal privacy and the needs of data circulation. Only by adhering to this balancing principle can the desirable development of the data ecosystem be realized, thus promoting the sustainable and healthy development of the digital economy and society.

References

- [1] He, X. S. (2022). Data trust: A new program for personal online behavior information protection. *Exploration and Free Views*, 12:197-204+214.
- [2] Xia, Y. K., Guan, Q. & Li, G. (2022). The connotation, generation logic and implementation path of data trusts: Analysis from the perspective of data circulation. *Documentation, Information & Knowledge*, 39(05): 109- 119. doi:10.13366/j.dik.2022.05.109.
- [3] McDonald, S. & Porcaro, K. (2021). The civic trust [EB/OL]. <https://medium.com/@dig-italpublic/the-civic-trust-e674f9aeab43>.

- [4] Lawrence, N. (2021). Data trusts could allay our privacy fears[EB/OL]. <https://www.theguardian.com/media-network/2016/jun/03/data-trustsprivacy-fears-feudalism-democracy>.
- [5] Zhai, Z. Y. (2021). Data trust: A new approach to data governance. *Oriental Law*, 04: 61-76. doi: 10.19404/j.cnki.dffx.20210722.014.
- [6] Ding, F. L. & Peng, J. (2023). Returning personal data to the people: “Emerging” data intermediaries for realizing self-determination of personal data. *Journal of Huazhong University of Science and Technology (Social Science Edition)*, 37(04): 74-84. doi: 10.19648/j.cnki.jhustss.1980.2023.04.08.
- [7] Xi, Y. M. (2021). Data security: The purpose of data trust and its realization mechanism. *Law Science Magazine*, 42(09): 29-41+52. doi: 10.16092/j.cnki.1001-618x.2021.09.003.
- [8] Wei, Y. S. & Liu, Y. (2023). On the type choice and system design of personal data trust. *Library Tribune*, 43(11): 70-78.
- [9] Yang, Y. W. (2023). Data trust: A new path of legal regulation of data transaction. *Journal of Southeast University (Philosophy and Social Science)*, 25(S1): 120- 124.
- [10] Jia, Y. H. & Li, X. R. (2023). Financial innovation in the context of digitalization: Data trust. *Northern Finance Journal*, 10: 57-61. doi: 10.16459/j.cnki.15-1370/f.2023.10.018.
- [11] Xu, T. X. (2024). The reciprocal logic and trust mechanization of personal data utilization in China. *Law and Economy*, 02: 19-36. doi: 10.16823/j.cnki.10-1281/d.2024.02.002.
- [12] Tian, A. N. (2022). Data trust in the form of a third party: The dilemma of data cotrollers obligations and its solution. *Library Tribune*, 42(08): 100-109.