Proceedings of ICMRED 2026 Symposium: Financial Innovation, Risk Governance, and the Dynamics of Global Capital Flows
DOI: 10.54254/2754-1169/2026.BL32674

The Theoretical Framework of Fiduciary Duties in Data Trusts and Their Applicability Limitations

Tianao Tan

School of Law, Beijing Jiaotong University, Beijing, China
24261055@bjtu.edu.cn

Abstract. Currently, data trusts mainly develop along two paths: the "information trustee model" and "third-party data trusts", and compared with conventional trust relationships, the introduction of the data controller role differs. When exercising rights on behalf of data subjects, data trustees should neither abuse their power nor supervise the compliance of data controllers' behaviours; At the same time, they need to participate in strategic interactions around data use rights. Considering that different trust objects have specific economic benefits; At the same time, because it involves personal information privacy and other rights issues, the interest demands of the participants cannot be overlooked. Therefore, the purposes for setting up a trust no longer solely encompass the protection of assets; instead, they now include the safeguarding of privacy rights. Given this situation, the fiduciary obligation of the data trustee will cover the entire life cycle of the data. The fiduciary obligations of data trustees mainly include: the obligation to ensure the security of personal data, the obligation to ascertain that there is no illegality in the purpose of using personal data, the obligation to specify the scope of exercising rights over personal data, and the obligation to avoid conflicts of interest. In actual application, the fiduciary obligations of data trusts are constrained by public interest factors and limits on the disposition rights of data owners.

Keywords: data trust, trustee, fiduciary duty

1. Introduction

With the rapid development of the digital economy, data has become a new driver of progress in the information age. Therefore, the balance of interests among data utilisation, application and protection has become a hot issue for academic research, industrial practice and governmental regulation; Both the European Union's General Data Protection Regulation (GDPR) and China's Personal Information Protection Law have imposed strict legal responsibilities on individuals who control or process personal data, forming an upper-lower level constraint network. This model is unable to address the inequality of status among data subjects and data controllers, nor does it really build a sense of trust between them. Data trusts introduce independent data trustees and replace legal obligations with fiduciary duties to achieve a new balance of rights and interests. How to define the specific content of these fiduciary duties in the data trust governance framework has become an urgent new problem.

© 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: 10.54254/2754-1169/2026.BL32674

Scholars have different opinions on the fiduciary duty of data trustees. Some people believe that this duty includes only prohibitory norms, while others think that, different from traditional fiduciary duties, data trustees under the data trust mechanism should also take the initiative to act in order to maximize the interests of data subjects [1,2]. Some people believe that the dual-track system of combining general fiduciary obligations with specific duties should be established [3]. Research existing provides some basis for this paper to examine the problems it addresses, but there is still room for improvement. On the one hand, academic research has focused more on economic interests and failed to reveal the moral connotation of the fiduciary duty and the necessity of protecting personality rights; On the other hand, when it comes to personality protection in e-commerce platform-based transactions, there is no systematic discussion yet. On the other hand, apart from inspecting the content of the duty of care, existing research has not taken into account any limitations on it.

First of all, this paper will explain the nature of the fiduciary obligation. Then it will analyse, based on the specific content of this duty for data trustees, how to protect the personal rights of data subjects. Finally, it examines the restrictions on fulfilling this duty from two angles: public interest and the data subject's right to dispose of their own data. The objective of this paper is, based on existing literature research at home and abroad, to construct a theory reference system for developing the fiduciary obligation and guiding governance pattern within the data trust structure.

2. Conceptual definition of data trustees and fiduciary duties

In traditional trust relationships, the settlor transfers property based on trust, and the trustee has a fiduciary duty to benefit the beneficiary. A clear division of authority and responsibility is formed among the three parties with regard to full control, maintenance and management, as well as the appreciation or increase in value of the property. A data trust is a new form of trust that modifies traditional trust relationships to meet the features of data. On the one hand, data rights as trust assets have a double ownership structure; On the other hand, the trust purpose extends beyond the asset appreciation function to incorporate privacy protection. These modifications alter not only the nature but also the direction of the trust obligation of the data trustee. Therefore, before elaborating on the specific aspects of the data trustee's fiduciary obligation, it is necessary to first clarify these two concepts.

2.1. Data trustee

Compared with traditional trust relationships, the data-trust Relationship has introduced the role of "data controller". Since data rights have a double-ownership structure of "nominal ownership of the data subject and substantive control over the data controller", it is necessary for the data trustee to pay attention to whether there has been any non-compliant use by the data controller during their execution of powers, and carry out strategic interaction with the controller about the rights over the use of data. The relationship between these two parties is complex and key, which is the core of understanding the data trustee's role.

Currently, there are two predominant models for the development of data trusts: One is Balkin's "information fiduciaries theory," which seeks to regulate data controllers through fiduciary duty obligations, requiring them to protect user information and thus alleviate the imbalance in rights relationships due to information asymmetry [4]. Second, there is an "operational model of third-party data trust" proposed by the UK Open Data Institute that introduces a neutral third-party institution as the data trustee to fulfill fiduciary responsibilities for the data subject [5].

DOI: 10.54254/2754-1169/2026.BL32674

In the "information fiduciaries" model, the data controller is the trustee. During the trust-building period, the data controller needs to inform the data subject of the relevant rules for trust management. Only with the consent of the data subject can personal information be processed legally. Once consent is given, a relationship of trust based on the right to data is formed between the parties, and the fiduciary duty of the data controller as trustee is thus generated.

In terms of content, there is no significant difference between the "information fiduciaries" model and traditional data-sharing platforms in terms of participants and transaction methods. The main difference is that the data controller enjoys more power but is subject to stricter obligations. In terms of authority, after the delegation of rights over personal data to the data controller, although nominally belonging to the data subject, it is actually controlled by the data controller using technical means and operational mechanisms. In the subsequent stages of collection, mining, analysis and trading, the data controller utilises its information advantages to achieve full control over the data, and realises an increase in value through management and disposal. In terms of obligation, the law has imposed strict fiduciary obligations on the trustee. For information leaks due to third parties, the law assumes fault on the part of the data controller to achieve equilibrium in the burden of proof between the principal and the trustee. If the data controller cannot prove that it has fulfilled its fiduciary duties to a high standard, it will be held jointly liable in cases of data infringement.

In the "third-party data trust" model, the data trustee is an independent third party. In addition to having a statutory fiduciary obligation towards the data subject, assuming the duty of safeguarding and utilising the data, the Data Trustee will enter into an agreement with the Data Controller, using professional technical means to supervise its use. In the trust-building stage, the data trustee will negotiate with the settlor about matters such as the purpose of trust, access authority, and benefits distribution, and accept the transfer of data rights. The data trustee will then review whether the processed data meets the privacy standard; if not, they will perform tiered anonymisation operations. Finally, the trustee will process the data into products based on their features; selectively sell data resources to demand parties according to the trust purpose specified by the settlor; and continually track privacy leak risks during use by the data controller. In a word, third-party institutions that act as data trustees are the link of trust between upstream suppliers and downstream consumers. By selling data to consumers, they maintain their fiduciary obligations toward the consumer as an entity that entrusted the information and facilitate secure and trustworthy multi-party use of data.

2.2. Fiduciary duty in data trust

The fiduciary obligation is intended to compel trustees to act in the best interests of the beneficiaries for their own sake. The fiduciary duty generally has the following features: first, as a higher-order obligation, it demands that trustees place the interests of the beneficiaries ahead of their own and those of third parties. Second, it is all-encompassing and involves every aspect of trust management. The third is that it is not waivable, so the basic needs cannot be excluded in the agreement made by both parties.

In terms of its essence, the fiduciary duty is divided into two aspects. On the other hand, it is forbidden to have conflicts of interest and to acquire benefits in the trust relationship, such as self-dealing or using trust property to benefit others, at the same time It is not allowed to use trust property to obtain benefits other than compensation for oneself. On the positive side, the trustee is required to act for the benefit of the beneficiary; and this clause serves as a general exception. Different trusts have distinct requirements for the duty of care. Tending to prohibit transactions

DOI: 10.54254/2754-1169/2026.BL32674

involving conflicts of interest absolutely, civil trusts allow for fair transactions if they have been made public and accepted [6].

In the relationship of data trusts, given that the object of trust and the interests of beneficiaries have special properties, they not only include economic benefits but also personal rights such as privacy. Therefore, the purpose of building trust has shifted from raising property values to protecting personal information rights. Under this change, the fiduciary duty of the data trustee runs through the entire life cycle of the data. In addition to prohibiting self-dealing, it is required to make public detailed information and pass strict compliance reviews. To ensure data security, avoid the damage or unlawful use of data in any form; At the same time, guarantee that every operation on this big data aims to achieve the intended goals for the subjects.

3. Content of the data trustee's fiduciary duty

The subject matter of a data trust is not traditional property but rather data rights, which are closely associated with the privacy, emotions, and social reputation of the data subject. Since economic interests and personal rights coexist on the premise of exercising the right over data, it is reasonable to require the trustee of data to perform stricter and more complete fiduciary obligations. Based on this definition, how can obligations be specified to manage and dispose of the data of trustees? How should the boundary between economic interests and personal rights be drawn to achieve a balance among the circulation of data, its security, privacy safeguards for individuals, etc.? There is still some ambiguity about what qualifies as a fiduciary duty in substance that needs to be clarified further.

3.1. Obligation to ensure data security

In the data age, data leakage undoubtedly causes harm to the rights and interests of individuals in terms of property, spirit, and social reputation. Considering the above risks, in order to enhance people's voluntary participation in the flow of data, it is necessary to strengthen protection for data security at the same time. Therefore, the most all-encompassing and essential duty under a data trustee's fiduciary responsibility is the obligation to guarantee the security of trust-kept data.

With the primary objective of safeguarding data security, the duty of a data trustee includes two aspects: On the one hand, it is self-regulation to avoid data leakage during storage and management; on the other hand, it is supervisory responsibility to prevent data leaks when data controllers use it for processing or transactions. The self-discipline of data trustees is centred around the initial stage of establishing data trusts. At the contract formation stage, the data trustee should establish legitimate trust objectives and truthfully inform the data subject; At the same time, based on both parties' agreement, define the trustee's powers over specific matters. At this time, based on anonymisation technology developed using more matured trust and protection strategies as part of data security efforts in the blockchain's decentralised framework, flexible implementation becomes possible during the handling phase of that information. Grant different levels of security processing permissions for personal data according to the privacy and confidentiality requirements; Ultimately, adopt a "trusted third-party isolated storage" mechanism to achieve effective isolation between data management and data storage [7].

In terms of the audit and oversight of data controllers, because there are more kinds of supervised subjects in combination with a wider range of management processes, the responsibilities that data trustees must bear have become stricter and richer. The primary responsibilities of these reviews and supervisions mainly cover the two aspects. In terms of access review, the data trustees are

DOI: 10.54254/2754-1169/2026.BL32674

responsible for verifying the qualifications of the data controllers before they can access the data; At the same time, require controllers to submit relevant supporting documents and specific security protection schemes to guarantee that the accessed data has been protected in accordance with the required scale and sensitivity during use [8]. Regarding the monitoring of data use, the data trustee needs to set up an anomaly detection mechanism for data access, conduct full-process supervision on the application of data utilisation, and implement dynamic authorisation. If a data controller exceeds their authorised permissions in any way, the data access interface should be immediately disabled to reduce risk exposure and maintain the separation of data control authority [9].

3.2. Obligation of legitimate purpose in data processing

The obligation to guarantee data security is part of a general duty that covers the whole operational cycle of trust-based data business. At the same time, the duty-bearers of data must take on corresponding responsibility for trust management in all aspects. The duty of legitimate purpose is primarily applied at the beginning of establishing a data trust agreement to regulate the nature of such a trust relationship. Based on the current legal system, the legitimate basis for data processing is still the consent of individuals. Based on this assumption, it is assumed that individuals can exercise full control over their own privacy information by making reasonable decisions. Due to the lack of recognisable technical bottlenecks, individuals are unable to understand the privacy statement and also do not possess the power to oversee its execution. As a result, they often select to "agree" merely for the purpose of using the service [10]. For example, If The Dynamic Data Field Responds Differently In various applications; At this time, all parties need to re-consent On the circulation And Use of Data. This practice is at odds with the efficiency requirements of the digital economy [11].

In response to the imbalance in the rights structure of the empowerment-based regulatory model, the legitimacy of purpose for data trustees sets out two supplementary evaluation standards. On the one hand, the transfer of trust property management and disposal rights between data subjects and trustees is still accomplished based on the principle of informed consent, endowing data trustees with necessary independent property management authority. On the one hand, it demands that the Data Trustee take on their primary duty to ensure the safety of the data; On the other hand, they must incorporate protecting Data Security into some scope during routine examination according to legal requirements. On one hand, it restricts the trustor's subsequent rights over the data, such as management and disposal; On the other hand, there is still some room left for them to exercise their power in other ways, which means a change from empowerment to behavioural regulation [10].

3.3. Obligations regarding permission boundaries for data usage

If the obligation of legitimate purpose is considered the starting point of the fiduciary relationship, then the obligation of authority boundaries constitutes the specific limit on the management process. The authority of the data trustee is established in two ways: First, based on the independent will expressed by the data subject in a contract; Second, supplemented by legal norms. The authority of a data trustee is different from the objective set in a data trust. The trust purpose both represents that the data subject has delegated its rights and assumes corresponding data security obligations under the trust relationship. Both the rights and obligations are limited to the data trustee. On the other hand, the authority boundary set by the data subject over the data trustee has an expanding effect. The binding force has extended to the data controller via the oversight and regulation of the data trustee. Therefore, it cannot be concluded that there will be a link between breaching the authority

DOI: 10.54254/2754-1169/2026.BL32674

boundary obligation and bearing liability. When the data trustee is the subject, the breach not only violates the trust agreement but also infringes upon legal norms. Where the data controller is the subject, the data trustee shall bear supplementary liability to the extent of their responsibilities undertaken [12].

3.4. Obligation to prevent conflicts of interest

The obligation to ensure the security of data is essentially a concrete form of the duty that a data trustee owes to protect personal rights and interests; At the same time, the obligation to avoid conflicts of interest serves as the central aspect of the trustee's duty over economic interests. Fiduciary duties require data trustees to prioritise the interests of the data subjects, which can be further broken down into three aspects: First is the prohibition of conflicts of interest; The data trustee's own interests should not conflict with those of the data subject. In case of a conflict, the data subject should be informed immediately, and all management and disposal activities should be stopped; if required, the data rights need to be returned. Secondly, in terms of self-interest prohibition, the data trustee cannot profit from their own management at the expense of the data subject's interests. Thirdly, there is an obligation to review; the data trustee needs to evaluate the risk that may arise from the use of data by the data controller [13,14].

The third requirement is, in essence, a deviation from the prohibition on conflicts of interest. The application objectives of data trust go far beyond the storage of data; conflicts may occur when data controllers are required to generate economic benefits based on their exercise of data rights. The objective of the data controller is to enhance the use efficiency of personal information, increase its application extent, and cut down on security costs; while these goals do not align with what the data subject seeks. Therefore, the conflict-of-interest prevention obligation should pursue "maximum priority interests" in status and hierarchy rather than an absolute "sole interest," which requires prioritising personal rights over economic interests in the data trust framework and positioning the interests of the data subject above those of the data controller [15].

4. Limitations on the fiduciary duty

In terms of trust management, the data trustee needs to perform two types of obligations simultaneously: one is the fiduciary duty that arises out of the trust relationship; The other is a statutory obligation. How to handle the conflict between these two kinds of identities? At this time, it may need to restrict the data trustee's fiduciary obligations.

4.1. Public interest

When public interests conflict with the rights of data subjects, the former will take precedence. For example, in the fight against crimes that threaten national security, data custodians need to provide data to relevant departments beyond what is authorised by criminal procedure law. Statutory obligations have universal enforceability, and as they take precedence over fiduciary duties in the legal hierarchy, data custodians cannot refuse to perform their statutory obligations on the grounds that they are acting in a fiduciary capacity.

Of course, when making decisions that harm the rights and interests of data subjects, comprehensive and reasonable considerations should be given; and the application of legal obligations needs to meet several conditions. First, the statutory and specific definition of public interest is not open to broad interpretation. Second, both the purpose and means need to conform to

DOI: 10.54254/2754-1169/2026.BL32674

the proportionality rule; necessity is deemed met only if the public interest surpasses the harm done to the data subject's right and interests and no other superior alternative exists. Third, the scope of the breach of the duty of loyalty should be reduced as much as possible and used preferentially for less privacy-sensitive personal data. Finally, the Data Trustee also undertakes a confidentiality obligation; and when required, the data subject must be provided with remedy or compensation.

4.2. Disposition of the data subject

According to whether the data trustee's authority has increased or decreased, the restrictions on the data trustee's fiduciary obligation set by the data subject's action can be divided into two categories. First, exercise the right to withdraw consent to reduce the power of the data trustee. The second is to agree on an increase in the scope of authority for the data trustee. In the first situation, under the obligation of the data trustee to safeguard the data, respect the data subject's intention to destroy or delete the entrusted data. Maintain the original authority of the authorised Data. Although there is occasionally a limit on the exercise of the fiduciary obligation due to the duty for data security, this does not fundamentally contradict it. On the other hand, there is a binding rule of legality for data trusts. The obligation to ensure data security is naturally included in the fiduciary duty, and its restriction on the other is essentially to protect individual rights more importantly than economic interests within the trust subject matter. On the other hand, there is no such thing as perfect trust property. Damage to trust property caused by pre-existing defects does not belong to the data trustee's failure to perform its fiduciary duties.

Similarly, the data subject may also consent to the data trustee managing trust assets outside the scope of its authority. According to the Uniform Trust Code of the United States, breaches of the sole interest may be permitted if otherwise provided for in the contract [16]. This shows that the data subject has control over the economic benefits in the trust relationship. However, such limitations are not absolute; even if the duty to prevent conflicts of interest does not require "sole interest", it must uphold the priority of personal rights over economic interests. In terms of personal rights and interests that should be protected in legal norms, the fiduciary's obligation of loyalty cannot be weakened or abolished because of the data subject's autonomous will [9].

5. Conclusion

Human development is no longer following the path foreseen by people in terms of technological progress. Data has inevitably become an integral part of the social and economic system, which carries great value in the society. Compared with the traditional empowerment model, the data trust mechanism achieves a balance of rights and obligations among all three parties through the fiduciary obligation. In addition to emphasising the moral dimension of the fiduciary obligation, it should also be clearly stated that preserving data security is an essential duty for trustees; Give priority to individual rights over economic benefits in order to protect the vulnerable group on the Internet. Of course, with the development of technology, new problems in the governance of data trust will continue to emerge. How to motivate the trustees of data trusts to perform their fiduciary obligations and how to design profit-sharing mechanisms that align with the interests of all three parties - the trustor, the trustee, and the beneficiary - are urgent problems that need to be addressed urgently.

References

[1] Li Zhi, Zhou Zhihao (2024). Development Dilemma and Institutional Design of Personal Data Trusts. Academic Exchange, 8, 43-58. https: //doi.org/10.3969/j.issn.1000-8284.2024.08.004

DOI: 10.54254/2754-1169/2026.BL32674

[2] Zhang Chunyu., Zhang Chunyu (2025). The Dilemma and Resolution of Dual-Obligation Conflicts for Data Trust Trustee. South China Finance, 9, 71-84. https: //doi.org/10.3969/j.issn.1007-9041.2025.09.006
[3] Cao Pantian (2024). The Generative Logic, Predicament Analysis and Optimization Path of Chinese-style Data Trust. Political Science and Law, 10, 113-130. https: //doi.org/10.15984/j.cnki.1005-9512.2024.10.004
[4] Zhai Zhiyong (2021). Data Trust: A New Approach to Data Governance. Oriental Law, 4, 61-74. https: //doi.org/10.19404/j.cnki.dffx.20210722.014
[5] Xin Yuan, Tian Xinmin (2025). The Mechanism and Implementation Pathways of Third-Party Data Trust Models in Data Sharing. Jiangxi Social Sciences, 2, 47-58. https: //doi.org/10.3969/j.issn.1004-518X.2025.2.jxshkx202502006
[6] Cao Xingquan (2019). An Interpretation on Beneficiary's Interests in Trustees' Duty of Fidelity: Monoscientism vs.Measurementism. SJTU Law Review, 2, 23-35. https: //doi.org/10.19375/j.cnki.31-2075/d.2019.02.002
[7] Wang Zhong, Wang Mengye (2024). Balancing Data Circulation and Privacy Protection: Operation Mechanism of Third-Party Data Trusts. Economic Review Journal, 1, 101-109. https: //doi.org/10.16528/j.cnki.22-1054/f.202401101
[8] Wei Yuanshan, Liu Yan (2023). On the Type Choice and System Design of Personal Data Trust. Library Tribune, 11, 70-78. https: //doi.org/10.3969/j.issn.1002-1167.2023.11.009
[9] Mei Yizhe, Dong Xinyi (2024). Constructing Personal Data Trust: A Data Governance Framework Based on Interest Balancing. South China Finance, 8, 61-73. https: //doi.org/10.3969/j.issn.1007-9041.2024.08.006
[10] He Xiaoshi (2022). Data Trust: A New Program for Personal Online Behavior Information Protection. Exploration and Free Views, 12, 197-202. https: //doi.org/10.3969/j.issn.1004-2229.2022.12.025
[11] CAI Linan (2022). Data Trust Participates in Data Governance: Theoretical Logic and Implementation Mechanism. Chinese Review of Financial Studies, 1, 66-79.
[12] Zhang Li, He Yuze (2024). Theoretical Proof and Institutional Development of Data Trust. Journal of Shenzhen University(Humanities & Social Sciences), 2, 121-131. https: //doi.org/10.3969/j.issn.1000-260X.2024.02.012
[13] Di Liya (2023). Governance Function, Mode and Development Strategy of Personal Data Trust. Information Studies: Theory & Application, 5, 90-98.
[14] Ye Jiamin (2022). Research on the Hermeneutics of Data Trust from the Perspective of Personal Information Collection. Inner Mongolia Social Sciences, 2, 94-103. https: //doi.org/10.14137/j.cnki.issn1003-5281.2022.02.012
[15] Fu Xiaoxing (2025). On the Data Trust Model in the Distribution of Personal Data Interests. Oriental Law, 1, 60-74. https: //doi.org/10.3969/j.issn.1007-1466.2025.01.006
[16] Xu Huageng (2021). Research on Fiduciary Duties. Tsinghua University Press.