Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.33695

Compliance Paths and Institutional Improvement for Personal Information Protection in Cross-Border Data Flows

Ruiyan Zhang

Institute for Advanced Studies in Humanities and Social Sciences, Beihang University, Beijing, China
2791084273@qq.com

Abstract. Against the backdrop of the globalization of the digital economy, cross-border data flows have made significant contributions to the integration of the global industrial chain and the development of digital trade. As a sensitive data type in cross-border flows, the protection of personal information is deeply linked to national data sovereignty and the protection of individuals' basic rights. China has achieved phased results in the institutional construction of personal information protection in cross-border data flows, forming a "1+3+N" legal regulatory system, and establishing three statutory compliance paths: data exit security assessment, personal information protection certification, and standard contract for personal information exit. It has also explored a regulatory model adapted to China's digital economic development stage through the pilot programs of negative lists and white lists for data exit in free trade pilot zones. However, practical problems still exist, such as difficulties in implementing protection mechanisms, unclear regulatory rules, hidden dangers in legal convergence and data development. Therefore, this paper puts forward practical and systematic suggestions for institutional improvement from four dimensions: precisely defining the scope of sensitive personal information, refining supporting rules for data exit, preventing potential risks from technological development, and optimizing certification rules for international cooperation networks.

Keywords: Cross-border data flows, Personal information protection, Data developmentalism, Sensitive personal information

1. Introduction

Relevant research from the McKinsey Global Institute shows that data flows were rare more than a decade ago, while the rapid growth of cross-border data flows is profoundly reshaping the evolution of globalization. With the advent of a series of technological changes, cross-border data flows have shifted from occasional to normal, with significant expansion in coverage, volume and content composition, and increasingly prominent influence and radiation scope [1].

As an important type of big data, personal information accounts for a large proportion in large-scale cross-border data flows. In 2013, the U.S. PRISM scandal shocked the world, triggering strong public protests against government infringement of citizens' privacy rights and international condemnation of the U.S. for violating the data sovereignty of citizens of other countries. This

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2026.33695

incident has drawn global attention to the security of personal data in cross-border flows and promoted in-depth discussions on data privacy protection and data sovereignty worldwide. Personal information has stronger personal attributes and higher sensitivity than other types of data. In terms of the ownership of personal information, most scholars at home and abroad tend to believe that personal information should be owned by individuals and is closely related to personal privacy rights. Therefore, for the purpose of protecting national data sovereignty and individuals' basic rights, this paper aims to explore the compliance paths and institutional improvement for personal information protection in cross-border data flows.

2. Overview of cross-border data flows and personal information protection

The concept of "cross-border data flows" was proposed and used as early as the 1970s, and there have been many discussions on its definition in academic circles. Defined from the perspective of the evolution of international information policies, the core definition of Transborder Data Flow can be summarized as: the activities of data storage, transmission, processing and retrieval in electronic form across national or judicial jurisdiction boundaries, whose core feature is that the control or processing subjects of data involve the legal and regulatory systems of different sovereign jurisdictions [2]. The Organisation for Economic Co-operation and Development (OECD) first gave a legal interpretation of "cross-border data flows" in the OECD Declaration on Cross-Border Data Flows, namely "the international flow of computerized data or information". The UN Transnational Corporation Center defines cross-border data flows as "activities such as processing, storing and reading machine-readable data across national borders" [3]. In a U.S. Congress report, this concept is described as "the act of processing and storing electronic data in computers across national borders" [4]. In Article 1, Paragraph 3 of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data issued in 1980, the OECD redefined cross-border flows of personal data as "the movement of personal data across national borders". The Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection issued by China in 2012 defines personal electronic information as "electronic information that can identify citizens' personal identities and involves citizens' personal privacy". Meanwhile, as an important data type in cross-border data flows, personal information has attracted much attention from scholars at home and abroad. In his article Data Autonomy, Cesare Fracassi proposed that personal data is the digital extension of personal will, a mixed form of will, personality, freedom and private property, and the circulation of personal data is a manifestation of respecting and realizing individual personality will. Strengthening data circulation centered on individual autonomy and self-determination is conducive to promoting personality protection [5]. Chinese scholars have also conducted in-depth research on the balance between personal data protection and circulation interests. Some scholars believe that the interest in personal data protection belongs to the category of basic human rights, and it is necessary to enhance the protection of the interests of data subjects and strictly restrict the industrial practice of personal data [6]. Some scholars hold that there is a widespread risk of personal data infringement in the data market, and unregulated data circulation will face a crisis of trust, so it is necessary to build a rule-based data transaction system centered on personal data protection [7]. Other scholars argue that no matter how data elements develop, the security value should be prioritized as the primary value of China's personal data circulation governance to guarantee and promote human dignity and freedom [8].

Many countries internationally have issued laws and regulations to regulate cross-border data flows and personal information protection. The EU's General Data Protection Regulation (GDPR)

DOI: 10.54254/2753-7048/2026.33695

issued in 2018 sets strict conditions for cross-border data transmission, and guarantees the security of cross-border data transmission through mechanisms such as the white list system, standard contractual clauses, and binding corporate rules. In terms of personal information protection, it grants data subjects multiple rights such as the right to know, the right to access, and the right to be forgotten, and sets high fines for violations. The United States has not formulated a unified comprehensive personal information protection law, but relies on industry self-regulation and specific field legislation for corresponding regulation [9]. China has constructed a "1+3+N" legal system and regulatory mechanism. Article 37 of the Cybersecurity Law of the People's Republic of China (hereinafter referred to as the Cybersecurity Law) adopted in 2016 stipulates the specific applicable scenarios of security assessment and establishes the cyber security classified protection system. The promulgation of the Data Security Law of the People's Republic of China (hereinafter referred to as the Data Security Law) in 2021 not only inherits the provisions on the exit security management of important data collected and generated by operators of critical information infrastructure in their operations within the People's Republic of China in the Cybersecurity Law, but also regulates the collection and acquisition of data by individuals and organizations, as well as the exit of important data [10]. The Personal Information Protection Law of the People's Republic of China (hereinafter referred to as the Personal Information Protection Law) came into effect in November of the same year. Its Chapter III specifically stipulates the conditions and methods for information processors to obtain information, adopts a relatively strict national protectionism, and requires the cyberspace administration to conduct security assessments on the flowing information and data. In response to a series of new problems brought about by cross-border data flows, the Cyberspace Administration of China has successively promulgated the Measures for the Security Assessment of Data Exit (hereinafter referred to as the Assessment Measures) and the Provisions on the Promotion and Regulation of Cross-Border Data Flows (hereinafter referred to as the Flow Provisions), which carefully regulate cross-border data flows in different scenarios. At present, China has formulated a series of legal regulations on cross-border data flows and prevented and controlled their main risk points, striving to reduce infringement and damage from the source of data exit.

3. Regulatory mechanisms and practical measures for personal information protection in China's cross-border data flows

Based on the current relevant domestic laws mentioned above, it is not difficult to find that China has adopted relatively strict exit control over personal information, a sensitive type of data. Different countries adopt different protection strategies and intensities for personal information data: the U.S. personal information protection measures are relatively flexible, while the EU adopts strict protection measures; China's personal information protection measures are more neutral, taking into account both flow security and freedom [11], and are mainly composed of three legally specified data exit paths and systems such as white lists and negative lists.

First, statutory data exit paths. At present, China's legislation has established three paths for data exit: data exit security assessment, personal information protection certification, and standard contract for personal information exit. The data exit security assessment system refers to determining whether data can flow freely through risk assessment of data exit in specific scenarios, and is an important precondition for cross-border data flows. The personal information protection certification and standard contract systems adapt to the trend of frequent data flows. Both parties can agree on rights and obligations in protecting personal information by signing a standard contract; or obtain recognition for enterprises or institutions that meet specific personal information protection

DOI: 10.54254/2753-7048/2026.33695

standards and requirements through certification, so as to achieve legal compliance. Adopting the above two methods can reduce enterprises' compliance costs and improve the efficiency of cross-border data flows.

Second, data exit negative list and white list systems. In addition to the above three specific paths, China has carried out pilot programs of data exit negative lists and white lists in multiple free trade pilot zones. The Flow Provisions issued in March 2024 revised some clauses and empowered each free trade zone to formulate data exit negative lists. The negative list clearly specifies the types and scopes of data that can only exit after government supervision and approval; other data outside the list can accordingly simplify or omit the exit approval process. At present, the Lingang New Area of Shanghai Free Trade Zone and the Pingtan Area of Fujian Free Trade Zone have implemented general data lists, while Tianjin and Beijing Free Trade Zones have launched their own negative lists for pilot operation. Corresponding to the negative list, the white list system grants greater freedom of data exit to each free trade zone, that is, data types on the white list have statutory exemptions. The Flow Provisions systematically established the white list system for the first time, covering six exemption scenarios. In some common low-risk data flow scenarios, such as cross-border e-commerce enterprises providing consumers' personal information overseas to fulfill shopping contracts, or enterprises transmitting employees' information for cross-border human resource management, the white list can be considered for certain exemptions, which has improved the efficiency of compliant data flows to a certain extent.

4. Existing problems and challenges of personal information protection in China's cross-border data flows

With China's deeper participation in cross-border data flows, a series of problems have emerged. From the perspective of legal regulations, the informed consent protection mechanism defined in China's laws and regulations may become a mere formality due to cumbersome and complex operations in actual operation, greatly reducing operational efficiency; the lack of specific regulations on some sensitive personal information may lead to their dereliction of supervision in cross-border flows. Meanwhile, there are problems in the convergence and coordination of domestic and foreign legal systems and the response to new risks brought about by the development of new technologies.

4.1. Practical dilemma of the informed consent protection mechanism

As an important part of personal information protection norms, informed consent is stipulated in both the Civil Code and the Personal Information Protection Law. Although China's relevant laws stipulate that "where a personal information processor provides personal information outside the People's Republic of China, it shall inform the individual of the name or title, contact information, processing purpose, processing method, type of personal information of the overseas recipient, as well as the methods and procedures for the individual to exercise the rights prescribed by this Law against the overseas recipient, and obtain the individual's separate consent" [12]. However, in the huge volume of cross-border data flows, it is obviously impossible to obtain the separate consent of every individual from whom personal information data is collected, which is undoubtedly a huge problem in terms of cost and practical implementation.

First, difficulties in the substantive implementation of "informed-consent". Although the "informed-consent" regulation endows natural persons with the right to choose and process personal information at the institutional level, it still exists as a mere formality in the actual process of data

DOI: 10.54254/2753-7048/2026.33695

collection and processing. On the one hand, the unclear connotation of personal information leads to the uncertainty of the scope of informed consent, which restricts the flow of personal information data to a certain extent and increases the cost of data collection and processing, contrary to the current trend of enhanced data flows. On the other hand, the rigid requirement of the "informed-consent" mechanism forces network service providers to obtain the full consent and explicit expression of users when collecting or processing user data. In practice, most platforms or websites tend to let users directly check the service agreement, while most users do not browse the agreement and can hardly be fully informed of the content and scope of data collected and processed. Therefore, there is a regulatory gap in whether natural persons can fully understand how their personal information will be processed and used, as well as the scope of their consent. At the same time, informed-consent has become an agreement between data providers and collectors, leading to a certain degree of supervision absence and vacuum [13]. If data infringement does occur, it is impossible to take preventive measures in advance, and only remedial measures and punishment mechanisms can be taken afterwards, resulting in unnecessary data leakage and infringement of personal rights.

Second, the risk of concession of informed-consent at the public interest level. Cross-border data flows play an important role in transnational economic cooperation, combating terrorism, maintaining public security and other aspects. Under specific circumstances, for the sake of public interest, it is necessary to impose certain restrictions on the principle of informed consent to ensure the maximum maintenance of security and order [14]. Article 13 of China's Personal Information Protection Law lists exemption scenarios related to public interest, providing a legal basis for public interest-oriented cross-border flows of personal information; Article 36 also stipulates that when state organs provide personal information across borders, they only need to pass security assessment and do not need to perform the "informed-consent" procedure to individuals. It is worth noting that although it is more efficient and in line with the maintenance of public interest that the strict application of the informed-consent rule is no longer applied to personal information data in cross-border data flows at the group or national level; this concession also hides the risk of abuse and leakage of personal information. At present, the "informed-consent" rule has been hollowed out. If the definition of public interest is vague, it may become an excuse for enterprises or organs to evade this rule and arbitrarily transmit personal information across borders. Meanwhile, in this scenario, individuals are unaware of where their personal information data will be transmitted and how it will be collected and used, and a sound individual post-incident relief path has not yet been established, making it impossible to grasp the balance between public interest protection and personal information rights and interests protection.

4.2. Unclear regulations on sensitive personal information protection

The unclear legal definition model of sensitive personal information makes it difficult to clarify which data fall under the strict protection category in the process of cross-border data flows. Globally, there are significant differences among countries in the definition, protection standards and levels of sensitive personal information, and different subjects such as data exporting and receiving countries have different regulations. Some data may not fall within the scope of sensitive personal information according to the laws of the receiving country, but belong to it for the provider, thus increasing the protection risk in the flow. China defines sensitive personal information by means of "definition + enumeration" [15], but this definition method has exposed drawbacks with the emergence and development of new business forms and the expansion of data flow scope.

DOI: 10.54254/2753-7048/2026.33695

First, lack of consensus on regulatory standards. The first appearance of the concept of sensitive personal information in the international vision can be traced back to the 1980s, when the OECD drafted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The formal establishment of "sensitive personal information" as a legal concept in Europe can be traced back to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted in 1981 [16]. Article 9, Paragraph 1 of the EU's General Data Protection Regulation (hereinafter referred to as "GDPR") also defines sensitive personal information by enumeration, specifically including "personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; data concerning health; data concerning a natural person's sex life or sexual orientation". Japan also added the concept of "sensitive personal information" in the amendment to the Act on the Protection of Personal Information (Act No. 57 of 2003 as amended), refined it in various regulations issued by its departments, and adopted a strict statutory protection mechanism. The United States has provisions on sensitive personal information in both the Freedom of Information Act and the USA PATRIOT ACT. Different from the countries and regions listed above, the United States defines sensitive personal information and ordinary personal information by means of "contextual balancing" and adopts a model combining decentralized legislation and industry norms [17]. It can be seen that countries have different definitions and legislative provisions for "sensitive personal information", which may lead to the risk of protection vacancy due to legislative differences in specific scenarios of cross-border personal information flows.

Second, unclear definition and confusion of "sensitivity". In addition to the several types listed in specific laws, the definition of "sensitivity" is also affected by the subjective will of natural persons. Based on the legislative experience of different countries and regions mentioned above, it is not difficult to find that the definition of sensitive personal information is closely related to national conditions and reality. For example, the EU emphasizes information such as race and personal trade union membership, which is not included in sensitive information in China. In addition, the definition of sensitive personal information is easily confused with privacy and private information. For natural persons, these are all "information unwilling to be known by others" that requires special consent, but in the process of cross-border data flows, different category definitions point to different assessment difficulties and even whether data can exit. Therefore, the unclear definition of sensitive personal information or blind adoption of personal subjective judgment will lead to difficulties in the implementation of this system, hindering the free flow of data or hiding risks of personal information protection. In addition, with the development of society and the Internet, more "sensitive personal information" closely related to personal relations may emerge in the future, and how to regulate such data is also a question worth thinking about.

4.3. Convergence and coordination of international law

The convergence and coordination of cross-border data flow regulations can be divided into the extraterritorial application of Chinese law and the formulation of inter-state agreements and treaties.

First, different countries have different positions and specific rules on cross-border data flows, leading to disputes over jurisdiction and legal application in transnational cases. The Data Security Law and the Personal Information Protection Law clearly stipulate extraterritorial jurisdiction clauses for cross-border flows of personal information. Although the Cybersecurity Law does not explicitly declare the validity of jurisdiction clauses, its extraterritorial effect can be inferred through the interpretation of other legal provisions. Cases arising from differences in legal regulations and

DOI: 10.54254/2753-7048/2026.33695

jurisdiction disputes in cross-border data flows are common. Max Schrems, an Austrian privacy activist, filed a lawsuit claiming that the United States failed to prevent large-scale surveillance by U.S. intelligence agencies and could not provide "adequate protection" for European citizens' data. Based on this, the Court of Justice of the European Union (CJEU) ruled the invalidity of the long-used "Safe Harbor" agreement and "Privacy Shield" agreement in 2015 and 2020 respectively. This judgment directly put U.S. tech giants (such as Meta, Google) relying on these agreements for transatlantic data transmission into legal dilemmas. In 2023, the Data Protection Commission (DPC) of Ireland relied on this to order Meta to stop transmitting data to the United States and issued a record fine of 1.2 billion euros. Although the U.S. cross-border data flow model emphasizes "free flow", its Cloud Act and data restriction orders issued in recent years in the name of national security show a strong tendency of unilateralism and expansion of extraterritorial jurisdiction. For example, in 2013, U.S. law enforcement agencies demanded that Microsoft hand over email content stored on servers in Dublin, Ireland. Microsoft argued that "data is stored in other countries, the law of the storage place should apply, and U.S. search warrants should not have extraterritorial effect", but the U.S. Congress quickly passed the Cloud Act clearly stipulating that "as long as data is controlled by U.S. companies, the United States has the right to obtain it no matter where it is stored", thus completely overturning the original judgment at the legal level and establishing the jurisdiction principle of "controllerism".

Second, the signing of relevant international treaties. China formulated laws and regulations on data flow regulation relatively late, and its international cooperation in this field is also insufficient. In terms of the signing of bilateral agreements, China and Germany signed the Memorandum of Understanding on Sino-German Cooperation in Cross-Border Data Flows in 2024, focusing on cross-border data protection and enterprise compliance convenience, which partially mentions the protection rules of sensitive information. Apart from this, China has not explicitly reached or signed bilateral rules on personal information protection in cross-border data flows with other countries [18]. In terms of the signing of international agreements, China officially signed the Regional Comprehensive Economic Partnership (RCEP) on November 15, 2020, but its supervision of cross-border flows of personal data mostly relies on the domestic legal frameworks of each contracting party [19]. In 2021, China officially applied to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). However, some provisions of this agreement conflict with China's current laws, so there are difficulties in its application and it is difficult to achieve the desired cooperation effect. At the same time, China's information cross-border restriction measures cannot fully meet the exception requirements of the CPTPP, and there are differences between China's provisions and CPTPP clauses in specific applicable conditions and scopes, which may make China face doubts about non-compliance with rules in relevant cross-border data flow scenarios, thus limiting the types and degrees of cross-border data flows and affecting the competitiveness of Chinese enterprises in the international market.

4.4. New risks brought by technological development

With the rapid development of information technology, new technologies such as cloud computing, big data and artificial intelligence have emerged continuously, making cross-border flows of personal information data increasingly frequent. Although these new technologies provide new development opportunities for the globalization of the digital economy, they also bring many severe problems to the protection of personal information data.

First, data privacy and security risks. The emergence and development of new technologies have greatly increased the scale of data collection, storage and transmission. In a cloud computing

DOI: 10.54254/2753-7048/2026.33695

environment, a large amount of user data is centrally stored on cloud servers. Once there are loopholes in the security protection measures of cloud service providers, it may lead to large-scale leakage of personal information data. In 2017, Dropbox, a U.S. cloud storage service provider, was exposed to have security vulnerabilities, putting user data at risk of leakage and tampering. In cross-border data flows, data often needs to pass through multiple network nodes and different legal jurisdictions, with complex transmission paths, which further increases the risk of data leakage. At present, some enterprises and websites are good at using big data analysis technology to deeply mine massive personal information, so as to profile user preferences and accurately push relevant products or services to obtain greater benefits. Driven by such interests, some enterprises may use high-tech to obtain cross-border flowing personal information and analyze it without sufficient user authorization, further infringing users' privacy rights. In addition, when artificial intelligence algorithms process cross-border personal information, defects in algorithm design or malicious use may also lead to improper disclosure of personal privacy information and adverse consequences [20].

Second, regulatory and enforcement difficulties. The complexity of new technologies, the global nature of cross-border data flows, and the limited authority of each regulatory department make it difficult to fully grasp the flow and processing of data, and also provide opportunities for some infringers. The application of blockchain technology makes data storage and transmission more decentralized and anonymous, making it difficult for regulatory authorities to track the accurate flow path of data. The emergence of a large number of mobile applications in recent years has made cross-border data flows more hidden and frequent. Regulatory authorities need to invest a lot of resources to monitor and review massive applications, greatly reducing the efficiency of regulatory investigation. At the same time, cross-border data flows involve regulatory agencies of multiple countries, and different countries have different regulatory policies and law enforcement intensities, leading to many difficulties in cross-border law enforcement cooperation. Some countries may also relax the supervision or cooperation of cross-border data flows for reasons such as protecting the interests of domestic enterprises or national security, adversely affecting the protection of personal information.

Third, lack of standards and mutual recognition. In the new technological environment, there is a lack of unified technical standards in data formats, encryption technologies, security assessments and other aspects involved in cross-border flows of personal information data. Different enterprises adopt different data encryption algorithms and key management methods, making it difficult to achieve mutual trust and secure docking in the process of cross-border data transmission and sharing. The lack of unified technical standards also leads to the lack of scientific basis for data security assessment, increasing the uncertainty of data protection. At present, the certification system for cross-border flows of personal information data is not perfect, and some countries and regions still lack mutual recognition on the basis of establishing data protection certification mechanisms, leading to increased operation and certification costs for enterprises in cross-border businesses.

5. Suggestions for improving the personal information protection system in cross-border data flows

At present, the dilemmas of China's cross-border data flows mainly focus on three aspects: unclear specific regulations, potential risks brought by technological development, and differences between domestic and international standards. Therefore, corresponding measures need to be taken in the refinement and improvement of regulations, response to potential risks, and strengthening of

DOI: 10.54254/2753-7048/2026.33695

international cooperation to improve flow efficiency and reduce the risk of personal information data leakage.

5.1. Precisely define the exit of sensitive personal information data

At present, the choice of review and restriction methods for data exit mainly depends on the data type and content involved in the information. As mentioned above, sensitive personal information requires stronger review and protection due to its special nature, but there are still problems in the unclear definition of sensitive personal information in practice. Therefore, it is necessary to formulate specific definition plans to clarify boundaries and make its connotation development match data development.

First, the connotation definition of sensitive personal information. The problems of ambiguity and insufficient scene adaptability in the definition of sensitive personal information in current laws can be solved by establishing a clear and unified definition benchmark, applying bottom clauses, and implementing graded and classified regulation. Article 28 of China's Personal Information Protection Law [21] defines sensitive personal information from the perspective of harmful consequences, which guides us to take objective rights infringement risks as the core basis for judging sensitive personal information, avoiding confusion of definition standards caused by differences in personal subjective feelings [22]. The law ends with the word "etc." as an expansion window of the concept, adding a similar bottom clause to provide a path for the inclusion of new types of sensitive personal information, which is more in line with the needs of data development. Typical examples include physiological sensing data, which can be included in the scope of sensitive personal information through the "etc." clause if it meets the objective rights infringement risk standard. In the public power scenario of government information disclosure, the definition of sensitive personal information also needs to balance public interest and personal rights and interests. For information involving specific identities, whereabouts and other information in government-disclosed information, judgment should not be made only according to unified standards, but the gain of disclosure to public interest and the damage to personal rights and interests should be additionally considered and compared. If the harm to personal rights and interests after disclosure far exceeds the value of public interest, it should be identified as sensitive personal information and the disclosure and cross-border transmission and acquisition should be restricted [23].

Second, adopt a graded and classified method to regulate sensitive personal data, focusing on the refined definition of special fields and groups. For minors, a special group, China's legal system has special protection for them. In the field of personal information protection, the academic community generally supports the direct inclusion of personal information of minors under the age of 14 into the scope of sensitive personal information, and proposes to strengthen the participation of guardians [24]. In special fields such as medical health and financial accounts, the definition should be refined combined with industry characteristics, and derivative information such as genetic testing data and diagnosis and treatment behavior trajectories in addition to medical record information should also be included in the scope of sensitive definition. In terms of grading, a risk gradient definition is adopted to adapt to classified processing, and a gradient definition scheme with the degree of damage risk as the core. The definition of sensitive personal information should not be a binary judgment of "either/or", but different levels of sensitive information should be divided according to the damage risk level after leakage or abuse. For example, biometric information has a higher damage risk than general medical records, so the definition standard should be stricter and the corresponding processing rules should be more stringent. This scheme can achieve precise connection between definition and subsequent processing rules [25].

DOI: 10.54254/2753-7048/2026.33695

Third, improve legal interpretation and system convergence, and strengthen the legal adaptability of definition. For scenarios where sensitive personal information is processed not based on personal consent, the definition should be combined with factors such as purpose and scope of use, and a strict interpretation method should be adopted. For example, in information processing related to public interest, whether a certain type of information belongs to the sensitive category should be defined combined with the necessity of processing purpose. If the processing behavior exceeds the "specific purpose", such information is more likely to be judged as sensitive personal information [26]. The convergence of the legal system and the formation of definition synergy with relevant legal norms also play an important role in the definition of sensitive personal information data. In legal application, Articles 28-30 of the Personal Information Protection Law should be taken as the core, connecting with relevant legal norms such as the Civil Code and the Data Security Law, expanding applicable scenarios and strengthening rights protection. When defining sensitive personal information in judicial scenarios, reference should be made to the identification standards of electronic data evidence in criminal proceedings. For example, the definition of sensitive attributes of financial accounts, whereabouts and other information in cross-border telecom and network fraud cases should match the legality requirements of evidence, so as to avoid confusion in judicial identification caused by conflicts in definition standards [27].

5.2. Refine supporting regulatory rules

At present, the Flow Provisions specify three permitted paths for personal information exit: applying for data exit security assessment, signing a standard contract for personal information exit, and passing personal information protection certification.

First, data exit security assessment system. Data exit security assessment is now widely used in cross-border data flows. On the one hand, this system safeguards data sovereignty and adheres to the position of national security; on the other hand, it balances the legitimate rights and interests of data processors. At present, some concepts in this system are defined too broadly, leading to frequent assessments, reduced assessment efficiency, and restrictions on data flows and digital trade development. Therefore, it is necessary to narrow its scope, clarify definition standards, and enhance the operability of the system [27]. In addition, a variety of guarantee methods should be fully utilized, and appropriate certification standards and contract templates can be formulated by drawing on international experience and combining with China's actual situation. Furthermore, the implementation of negative list and white list systems should be further promoted. Through early definition and classification of data nature, a fast track is provided for data subjects or data types meeting specific security standards and conditions to improve data exit efficiency, which can alleviate the current problem of excessive assessment burden to a certain extent. At the same time, the effective convergence between the domestic regulatory system and international treaty frameworks must be further promoted. China should take the initiative to align with international rules such as CPTPP and DEPA, break down barriers to cross-border data flows on the premise of ensuring national security, build smooth data circulation paths, and thus enhance China's competitive position and right to speak in rule-making in global digital trade [28].

Second, personal information protection certification system. From the perspective of institutional attributes, personal information protection certification is a "socialized regulatory tool", which makes up for the lack of administrative regulatory resources through the review of professional third-party certification institutions, and guides enterprises to take the initiative to comply with regulations through market-oriented incentives. Certification institutions should have the qualifications of impartiality and professionalism, adhere to the principle of objectivity and

DOI: 10.54254/2753-7048/2026.33695

neutrality in performing their duties, and practically reflect the professional level matching their functions. From international experience, different countries and regions have different certification institution setting models. France's CNIL privacy certification adopts a national certification model, with certification institutions operating at the national level; the U.S. TRUSTe privacy certification is a third-party certification model, carried out by independent third-party institutions away from the government [29]. China's certification system is still in the stage of development and improvement, and the main problems currently faced include the dependence of some certification institutions on administrative organs, lack of due independence, and the restriction of the professional capabilities of relevant institutions to a certain extent due to the unity of management. In the future, China should gradually establish a third-party certification model under government supervision, which not only maintains the flexibility of the third-party certification in the operating mechanism, but also effectively makes up for its institutional shortcomings through government supervision.

Third, standard contract filing system. Although China has formulated a relatively complete standard contract for personal information exit through legislation, it may have problems such as narrow application scope, single clause structure, and lack of review of personalized clauses. Specifically, it excludes large platforms and enterprises in key fields from the subject provisions [30], and does not set a dynamic adjustment mechanism, making it unable to adapt to complex businesses such as data sharing within transnational enterprise groups and sub-processing entrustment. Secondly, the review boundary of personalized clauses added on the basis of the standard contract is not clear, neither distinguishing between mandatory and arbitrary clauses nor stipulating whether the cyberspace administration needs to conduct substantive review. In practice, enterprises may weaken security obligations through supplementary clauses. If the cyberspace administration only conducts formal review, it is difficult to find potential risks.

For the existing supporting regulations, the future improvement direction should be to broaden the application scope and establish a dynamic adjustment mechanism. The personal information exit standard contract system can appropriately relax its subject restrictions and include some large platforms and key field enterprises meeting certain security guarantee conditions to adapt to the diverse needs of cross-border data flows [31]. At the same time, drawing on relevant international experience, regularly evaluate and dynamically adjust the application scope according to data types, risk levels and other factors to ensure that the system is consistent with the development of actual businesses. For the review of personalized clauses, systematic interpretation can be used for normative analysis, emphasizing the importance of subdividing rights and obligations of different subjects, and clarifying the review methods of clauses of different natures. For mandatory clauses, the cyberspace administration should conduct substantive review to ensure that they meet the requirements of data security and personal information protection; for arbitrary clauses, on the basis of formal review, enterprises can be required to conduct self-risk assessment and file [32].

5.3. Prevent potential risks in line with data developmentalism

The collection and acquisition of personal information data are closely related to technological development. In terms of data right protection and governance, China is different from the EU's data conservatism and the U.S.'s information utilization liberalism. Instead, it studies data law from the perspective of data developmentalism, adhering to the people as the main body of the rule of law and developing for the benefit of the people; at the same time, it adheres to grasping the objective laws of data utilization and digital economic development, and guaranteeing the right to a better life in the digital era [33]. Therefore, the risks brought by technological development must be prevented

DOI: 10.54254/2753-7048/2026.33695

and resolved through effective ways, mainly including technical compliance, regulatory coordination and mutual recognition certification.

First, technology is the information and algorithm infrastructure embedded in the governance process of cross-border data flows. Its role is not only reflected in the support capacity for processes such as data collection, processing, encryption, sharing and cross-border transmission, but also in the governance integration in rule embedding, authority allocation and behavior constraint [34]. Technology empowerment and compliance embedding can resolve data privacy and security risks to a certain extent. In terms of implementation means, Privacy Enhancing Technologies (PETs) are used to build a technical defense line, and anti-leakage means such as homomorphic encryption, data desensitization and zero-trust architecture are promoted to realize that cross-border data is available but not visible, computable but not identifiable, and balance data utilization and privacy protection. At the same time, the main security responsibilities of cloud service providers and data processors should be implemented, and a normalized vulnerability detection, penetration testing and emergency response mechanism should be established to prevent centralized storage and cross-border transmission leakage risks. For personal information data that may be obtained and leaked in AI training, it is necessary to strengthen AI algorithm ethical review and whole-process supervision, establish and implement the principles of minimal necessity and full authorization, prohibit cross-border data mining and commercial utilization without effective user consent, and curb privacy infringement from the source.

Second, regulatory coordination is an important means to prevent new technologies from infiltrating and stealing personal data, which is mainly reflected in the use of regulatory technology to achieve penetrating supervision, building a cross-border data flow monitoring platform, and conducting full-process traceability and dynamic control of hidden flow behaviors such as blockchain and mobile applications. The existing data regulatory structure is unable to fully cope with new problems caused by big data such as new artificial intelligence technologies [35]. Therefore, it is necessary to establish a relatively complete and independent data regulatory structure at the macro level, and update regulatory countermeasures at the micro level to deal with continuously iterative data technologies and make up for regulatory loopholes. The data regulatory structure should be composed of the cyberspace administration, the National Data Administration and other relevant functional departments. All departments should cooperate on the basis of performing their original duties, tackle key problems for new technologies and effectively prevent possible personal information acquisition behaviors. In the process of data exit, data desensitization and anonymization can be used to reduce the exposure of personal information. For the sensitive data graded and classified processing mechanism, different desensitization strategies can be adopted according to the degree of data sensitivity, and machine learning can be used to meet different data desensitization needs [20].

Third, connecting global data governance rules extraterritorially and establishing a cross-border data law enforcement coordination mechanism can effectively resolve jurisdiction conflicts and local protectionism and improve regulatory enforcement. Integrating into the global governance system requires establishing unified standards and mutual recognition certification with foreign countries to make up for the shortcomings of the governance system. China should participate in and even lead the formulation of global unified technical standards as much as possible, and promote the integration of data formats, encryption algorithms, security assessments, cross-border transmission rules and other aspects with international standards. Specifically, it can align with the EU GDPR, the U.S. Data Privacy Framework, and China's data exit rules, unify the bottom-line standards for personal data protection for new technology scenarios such as cloud storage, AI cross-border

DOI: 10.54254/2753-7048/2026.33695

training, and big data cross-border analysis, and avoid repeated enterprise compliance and repeated regulatory intervention. For incidents such as cloud service leakage, AI algorithm privacy abuse, and illegal blockchain data circulation, sign cross-border data law enforcement mutual assistance agreements, clarify a series of processes such as personal data retrieval, investigation cooperation, evidence solidification, and penalty notification, and solve the problems of difficult query, control and punishment after cross-border data under new technologies.

5.4. Strengthen international cooperation and unify certification rules

China's cross-border flows of personal information data still face many challenges in the convergence and coordination of laws and regulations, especially in rule identification in international cooperation. For differentiated regulatory content, efforts should be made to seek common ground while reserving differences and strengthen the coordination of domestic and foreign legal regulations; or take the initiative to seek international cooperation to take the initiative, establish agreement clauses in line with the trend of data development, and balance bilateral or multilateral interests.

First, strengthen the convergence of domestic law and international law. Domestic law is the foundation for China to regulate cross-border flows of personal data, while international law provides a framework for international cooperation. From the perspective of international law, there is no unified global rule for cross-border flows of personal data, but some international organizations and regional agreements have formed relevant norms. For example, the EU's General Data Protection Regulation (GDPR) has established cross-border data flow regulatory principles such as "adequate protection" and "appropriate safeguards". China can draw on such mature experience and consider the trend of international law regulation and adapt to relevant international regulations in the formulation and revision of domestic law. For the protection of data subject rights, domestic law should clearly grant data subjects full rights to know and control; in certification rules, the assessment of requirements for overseas recipients can refer to internationally recognized data protection standards such as ISO27001 to ensure the security of data transmission and protection as much as possible [36]. In terms of dispute settlement mechanisms, domestic law should reserve space for docking with international law. When international disputes involving cross-border flows of personal data occur, handle them in accordance with international law rules to protect China's rights and interests in global data governance.

Second, explore bilateral rule-making negotiations. At present, the main international data cross-border flow agreement joined by China is the RCEP agreement. However, due to the large differences in the development levels of the contracting parties, the RCEP data cross-border flow rules have a small number of provisions and relatively basic content, which cannot well meet the needs of China's vigorous development of cross-border data flows. Against this background, the one-on-one negotiation mechanism adopted by the Data Privacy Framework points out another feasible path for negotiations in the field of cross-border data flows. For neighboring countries and regions with large-scale data flow exchanges with China (such as ASEAN, Japan, South Korea, etc.), we can try to transcend the traditional governance paradigm of multi-party value conflicts and explore the introduction of a bilateral negotiation mechanism similar to the "Data Privacy Framework" to promote bilateral cooperation in the field of cross-border data flows on the basis of seeking common ground while reserving differences [37]. Taking the cooperation between China and Japan as an example, China and Japan have extensive cooperation needs in the digital economy field. Through bilateral negotiation to formulate certification rules for cross-border flows of personal data, the safe and orderly flow of data between the two sides can be promoted [38]. In the specific

DOI: 10.54254/2753-7048/2026.33695

negotiation process, clarify the data protection standards and certification processes of both parties, reach a consensus on core issues such as data subject rights protection, data storage and use specifications; at the same time, establish a bilateral data regulatory sharing mechanism, and the regulatory agencies of both parties can conduct regular exchanges on the implementation of certification rules and jointly investigate and deal with violations.

Third, actively participate in regional rule-making. Regional rule-making provides a platform for China to promote the optimization of certification rules for cross-border flows of personal data on a larger scale. In regional cooperation, China can jointly formulate certification rules in line with regional characteristics with neighboring countries and regional organizations. In the formulation of regional regulations, China upholds the core position of attaching equal importance to security and development, advocates the establishment of inclusive goals taking into account regional cooperation and domestic supervision, and proposes to reserve reasonable exceptions for public policy objectives and basic security interests. In terms of regulatory paths, China tends to adopt a gradual model of "principle framework + transition mechanism + special legislation". First, establish basic principles of data protection at the regional level, then build transition mechanisms such as enterprise certification, and finally form a unified and flexible regulatory system [39]. ASEAN has led the establishment of the CAFTA cross-border data flow "dual-track mechanism". China can join in in-depth cooperation based on this: on the one hand, promote the establishment of a regional data governance committee to coordinate the rules of member states, unify the interpretation standards of vague concepts such as legitimate public policies and basic security interests, and avoid the abuse of exception clauses; on the other hand, build an Enterprise Personal Data Protection Authentication System (EPDPAs), in which China-ASEAN joint institutions certify enterprises meeting regional standards, and certified enterprises can enjoy the convenience of cross-border data flows as a transition plan before the implementation of unified regulations.

6. Conclusion

Under the wave of digital economy globalization, cross-border data flows have become the core driving force promoting the integration of the global industrial chain, scientific and technological collaborative innovation and trade liberalization. As the core sensitive type in cross-border data flows, the protection of personal information is not only related to the basic civil rights of natural persons, but also deeply bound to national data sovereignty, network security and the high-quality development of the digital economy. The institutional improvement of personal information protection in cross-border data flows is not achieved overnight, but needs continuous dynamic adjustment according to the development of digital technology and changes in the global governance pattern. Guided by data developmentalism, China's personal information protection system for cross-border data flows is neither purely "protection priority" nor absolute "flow priority", but seeks a dynamic balance between personal information protection, national data security and the release of data element value. This governance idea is not only in line with China's national conditions and development stage, but also provides a Chinese solution for global data governance. From the perspective of future development, the construction of China's personal information protection system for cross-border data flows first needs to continuously deepen the refinement and dynamism of the system to solve the dilemma of hollowing out, and include relevant personal information into legal protection in a timely manner to keep the system in step with technological development; second, it needs to strengthen the in-depth application of regulatory technology, break through cross-departmental and cross-regional regulatory data barriers, and achieve full-process and penetrating supervision of cross-border data flows; finally, it needs to deepen the breadth and depth of

DOI: 10.54254/2753-7048/2026.33695

international cooperation, promote from current bilateral negotiations and regional pilots to form a new global data governance pattern that takes into account national data sovereignty, personal information rights protection and digital economy globalization, so that cross-border data flows can release greater economic and social value on the premise of security.

References

[1] Qi Aimin. "On the Improvement of the Comprehensive Legal Protection of Data Security in the Big Data Era——From the View of Cyber Security Law." Journal of Northeast Normal University (Philosophy and Social Sciences Edition), no. 04 (2017): 108-114.

[2] Pipe, G. R. "International information policy: Evolution of transborder data flow issues." Telematics and Informatics (1984).

[3] Chandran, R., Phatak, A., & Sambharya, R. "Transborder data flows: Implications for multinational corporations." Business Horizons 30 (1987): 74, 75-76.

[4] Congress of the U.S. International Barriers to Data Flows: Staff Background Report. Washington: Government Printing Office, 1982.

[5] Fracassi, Cesare, and William Magnuson. "Data Autonomy." Vanderbilt Law Review (2021).

[6] Min Fengjin. "The Research of the Legal Boundary of Personal Data Right Protection: Based on the Analysis of 50 Human Rights Cases of European Court." Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), vol. 30, no. 04 (2018): 56-66.

[7] Miao Zeyi. "Research on Personal Information Protection under the Background of Data Trading Market Construction." Tribune of Political Science and Law, vol. 40, no. 06 (2022): 55-65.

[8] Ling Xia. "Security Value First: Legal Path of Personal Information Protection in the Big Data Era." Social Sciences in Hunan, no. 06 (2021): 83-91.

[9] Cao Bo. "Legislative Model and Perfect Path of Cross-border Data Transmission: Pitching-in from Article 37 of the Cyber Security Law." Journal of Southwest Minzu University (Humanities and Social Science), vol. 39, no. 09 (2018): 94-100.

[10] Hu Keyang, and Yuan Hao. "Deconstructing and Reshaping of China's Data Outbound Transfer Rules—Considering Adapt to International Agreements." Information Security and Communications Privacy, no. 11 (2023): 46-53.

[11] Xiong Guangqing, and Zhang Sumin. "The Extraterritorial Application of China's Personal Information Protection Norms: An International Comparative Study." Journal of Harbin Institute of Technology (Social Sciences Edition), no. 5 (2025).

[12] Personal Information Protection Law of the People's Republic of China, Article 39.

[13] Shi Chao. "Rational Correction of the Implementation of the Informed Consent Rule for Personal Information Processing." Studies on Socialism with Chinese Characteristics, no. 1 (2024).

[14] Gao Zhihong. "Practical Dilemma and Institutional Optimization of 'Informed-Consent' Mechanism in the Era of Big Data." Law Review, no. 2 (2023).

[15] Personal Information Protection Law of the People's Republic of China, Article 28, Paragraph 1.

[16] He Zhicheng. "A Study on the Definition and Legal Protection of Sensitive Personal Information." Master's thesis, Southwest University of Political Science & Law, 2017.

[17] Deng Lingbin. "Comparative Study on the Legal Regulation of Sensitive Personal Information Protection in the European Union and the United States and Analysis on the Characteristics of Chinese Legislation." Library, no. 3 (2023).

[18] Lu Lu, and Qi Meijuan. "Security Governance and Supervision of Cross-border Data Flow." Jiang-huai Tribune, no. 1 (2025).

[19] Wu Qiwei. "RCEP's Protection of Transborder Flow of Personal Data and China's Response Path." Foreign Economic Relations & Trade, no. 10 (2022).

[20] Peng Sheng, Luo Fu, and Chen Qingmei. "Research on Privacy Protection Technology and Application in Cross-border Data Flow." China Venture Capital, no. 2 (2025).

[21] Personal Information Protection Law, Article 28.

[22] Chen Xi. "Analysis of the Approach to Improve China's Sensitive Personal Information Protection Rules——Based on Articles 28-30 of the Personal Information Protection Law." Social Sciences in Hunan, no. 6 (2023).

[23] Yang Shangdong. "On the Protection of Sensitive Personal Information in Government Information Disclosure in the Big Data Era." Administrative Law Review, no. 4 (2025).

DOI: 10.54254/2753-7048/2026.33695

[24] Ning Yuan. "The Legal Attributes and Definition of Sensitive Personal Information: Centered on the First Paragraph of Article 28 of Personal Information Protection Law of PRC." Journal of Comparative Law, no. 5 (2021).
[25] Xia Qingfeng. "Interpretation and Application of Personal Information Classification Processing Rules: A Risk-Based Perspective." Law Review, no. 4 (2025).
[26] Zhang Jianwen, and Zhang Rui. "On the Legal Basis of the Sensitive Personal Information." Inner Mongolia Social Sciences, no. 5 (2025).
[27] Ma Guang. "On the Construction of China's Outbound Data Transfer Security Assessment System." Journal of Shanghai University of Political Science and Law (The Rule of Law Forum), no. 3 (2023).
[28] Mei Ao, and Li Huaijun. "Discussion on the Convergence of Regulation of Cross-border Data Flow of Measures of Data Cross-border Transfer Security Assessment and DEPA." Journal of Shanghai University of International Business and Economics, no. 2 (2023).
[29] Nie Leilei. "Understand and improve the personal information protection certification system from the perspective of the whole certification process." Cyber Security And Data Governance, no. 11 (2023).
[30] Measures on the Standard Contract for Outbound Transfer of Personal Information (Cyberspace Administration of China Order No. 13), Article 4.
[31] Mei Ao, and Xie Bingzi. "Research on the Standard Contract for the Outbound Transfer of Personal Information in China under the Global Data Regulatory Competition." Intertrade, no. 6 (2024).
[32] Chen Hengcong. "Research on the Standard Contract for Outbound Transfer of Personal Information in Cross-border Data Flow." Journal of Yulin Normal University, no. 6 (2024).
[33] Zhou Kunlin. "China's Independent Knowledge System of Data Rule of Law under Data Developmentalism." Tribune of Economic Law, no. 2 (2023).
[34] Xu Wanxiu, and Zuo Xiaodong. "China's Approach to Cross-Border Data Flow Governance in the Context of Global Competition." Strategic Study of CAE, no. 1 (2025).
[35] Liu Quan, and Liao Jialin. "Reflection and Restructuring of the Horizontal Allocation of Data Regulatory Authority." Journal of Hunan University of Science and Technology, no. 3 (2025).
[36] Zou Jun. "The Regulation and Mechanism of Transborder Flows of Personal Data Based on GDPR." Journalism Research, no. 12 (2019).
[37] Yang Zishuo. "Analysis of data cross-border flow rules from the perspective of Data Privacy Framework system and its implications for China." Cyber Security And Data Governance, no. 8 (2024).
[38] Xue Zhihua, Zeng Dehua, and Meng Qixun. "Institutional Practice of Cross-Border Data Flows Regulation in Japan and Prospects for Sino-Japanese Cooperation." Intertrade, no. 6 (2024).
[39] Wang Chongyu. "Research on regulation of cross-border Data Flow in Digital Trade of China-Asean Free Trade." Master's thesis, Southwest University of Political Science and Law, 2021.