A Brief Review of PRC Administrative Regulation of Network Data Security

By Xun Yang | Olivia Huang

On September 24, 2024, the State Council of the People's Republic of China promulgated the *Administrative Regulation of Network Data Security* (the "**Network Data Regulation**"), which will take effect from January 1, 2025. This regulation represents a significant legislative advancement in data protection, building upon the foundation laid by the Cyber Security Law, Data Security Law, and Personal Information Protection Law.

This article will provide a concise overview of how the Network Data Regulation has evolved the data law framework. It will also discuss the regulation's application to innovative data operations and outline the compliance obligations for network data operators.

1. Development of Data Law Regime by Network Data Regulation

The Network Data Regulation marks a significant milestone in the realm of data law, harmonizing fragmented regulations concerning data security, data exportation, and personal information protection. It further refines the rules in these critical areas.

The promulgation of the Cyber Security Law by the Standing Committee of the National People's Congress (the "**Standing Committee**") in 2017 heralded the commencement of an era of intensive legislative activity in data-related matters. Subsequently, a plethora of national standards and ministerial regulations concerning data were introduced. In 2021, the Standing Committee promulgated the Data Security Law and the Personal Information Protection Law, which respectively bolstered provisions on data protection and personal information protection under the Cyber Security Law. During 2023, the measures for security assessment and standard

如果您需要本出版物的中文本,
请联系:

Publication@llinkslaw. com

For more Llinks publications,
please contact:

Publication@llinkslaw.com

contract filing for data exportation were finally solidified, while the rules for compliance review of personal information protection continued to evolve. Consequently, a comprehensive data protection regime has begun to take shape.

However, the data law regime still presents several issues that necessitate further development, and the Network Data Regulation aims to address these challenges.

Firstly, the Network Data Regulation harmonizes the rules for protecting personal information and non-personal data. Previous regulations for data security and personal information protection were largely governed by separate laws and regulations. Yet, in practice, businesses often handle data that combines both personal and non-personal elements, necessitating a unified approach to data legislation. The Network Data Regulation strives to align the rules for both types of data.

Secondly, the Network Data Regulation complements the Data Security Law and the Personal Information Protection Law. Despite numerous legislative amendments in the form of ministerial rules and national standards, gaps persist in data protection. For instance, while the Personal Information Protection Law grants data subjects the right to data portability, it lacks detailed provisions for exercising this right. Similarly, the Data Security Law mandates risk assessments for handling important data but does not provide detailed guidelines for conducting such assessments. The Network Data Regulation includes provisions to fill these gaps.

Thirdly, the Network Data Regulation "amends" existing rules in light of real-world practices. Some data-related rules are so stringent that they are challenging to enforce. For example, the Personal Information Protection Law requires the collection of only necessary information, a stipulation that may be difficult to adhere to when employing automatic data collection technologies that incidentally gather unnecessary data. The Network Data Regulation reconciles such technical or practical challenges and establishes rules to accommodate them.

Fourthly, the Network Data Regulation introduces rules for innovative technologies and their applications. For example, Articles 18 and 19 of the Network Data Regulation outline regulations for the use of automatic data collection technologies (e.g., web crawlers) and artificial intelligence.

2. Key Content of Network Data Regulation

The Network Data Management Regulations encompass the full spectrum of network data activities, including collection, storage, utilization, processing, transmission, provision, publication, and deletion. "Network data" is broadly defined as any electronic data that is either processed or generated through network operations. The essence of these regulations is summarized below:

A. Data Governance

The Network Data Regulation provides for detailed guidelines for the establishment of robust data protection governance, building upon the foundational requirements of the Data Security Law and Personal Information Protection Law.

In the context of processing personal information of Chinese residents outside China, the Network Data Regulation mandates the appointment of a dedicated agent or the designation of a representative, in accordance with the Personal Information Protection Law. This agent or representative must be registered with the local cyber security administration, including their name and contact information, to serve as the primary point of contact for all matters pertaining to personal information protection.

For entities that process personal information of 10 million individuals or more, the Network Data Regulation equates such activities to the handling of important data. This categorization necessitates the appointment of a responsible individual with extensive knowledge and experience in data administration, empowered with the authority to report directly to governmental authorities about data handling practices. The Network Data Regulation also delineates the responsibilities of the data security management division, which include:

(1) The development and enforcement of comprehensive network data security management systems, operational protocols, and emergency response plans to address network data security incidents.
(2) The regular conduct of network data security risk monitoring, assessments, emergency drills, and educational outreach programs, ensuring prompt mitigation of network data security risks and incidents.
(3) The management and resolution of complaints and reports concerning network data security.

B. Consent to Data Collections

The Network Data Regulation meticulously outlines the protocols for obtaining individuals' consent regarding the management of their personal information, enhancing the "informed consent" principle established by the Personal Information Protection Law.

The Network Data Regulation specifies the minimum information that must be disclosed to individuals, which includes: (1) the name and contact details of the data handler; (2) the objectives, techniques, and categories of personal information processing, along with the rationale for processing sensitive data and its potential effects on individual rights and interests; (3) the data retention duration and the procedures for data handling post-expiration, with a clear methodology for determining retention periods when they cannot be predefined; and (4) the processes available for individuals to access, duplicate, transfer, amend, augment, erase, limit the use of their personal information, as well as to deactivate accounts and rescind consent.

Furthermore, the Network Data Regulation solidifies the guidelines for obtaining individual consent, stipulating that: (1) consent must be secured without the use of deception, deceit, or duress; (2)

explicit consent is mandatory for processing sensitive personal information, including biometric data, religious affiliations, unique identifiers, medical records, financial data, or geographic location information; (3) for minors under the age of fourteen, consent must be obtained from their parents or legal guardians; (4) personal information should not be processed beyond the boundaries of the predefined purposes, methods, categories, and retention timeframes; (5) once an individual has clearly rejected the processing of their personal information, they should not be subjected to repeated requests for consent; and (6) any alterations to the objectives, methods, or types of personal information processing necessitate the reacquisition of consent from the individual concerned.

C. Data Transfers

The Network Data Regulation streamlines the regulations governing the transfer of both personal and non-personal critical data.

The Network Data Regulation mandates that during the transfer of personal information or non-personal important data—whether it be for data provision or entrusted data processing purposes—the data transferor must: (1) enter into a contract with the recipient that clearly defines the objectives, methodologies, extent, and security obligations associated with the personal or vital data, (2) ensure compliance with these obligations by the data recipients, and (3) maintain records of the provision or processing of personal or significant data to third parties for a minimum of three years. Concurrently, the data recipient is obligated to safeguard the personal or significant data received and to process this data strictly within the agreed-upon parameters.

Moreover, the Network Data Regulation extends its purview to encompass the transfer of non-personal data in scenarios such as mergers, acquisitions, divisions, dissolutions, and similar contexts, thereby ensuring that the transfer of non-personal data is also subject to the same stringent rules as personal data. As a result, the Network Data Regulation necessitates that a recipient of data assumes the associated data security responsibilities upon gaining control over the data during such corporate transitions.

Furthermore, the Network Data Regulation delineates the detailed procedures for individuals to exercise their right to data portability. A data handler is required to facilitate the transfer of personal information to another data handler designated by the individual, provided that: (1) the individual's identity has been authenticated; (2) the personal information to be transferred was either consensually provided by the individual or collected for the fulfillment of a contract; (3) the technical feasibility of transferring the personal information is ensured; and (4) the transfer does not infringe upon the legitimate rights and interests of third parties. Additionally, should an individual make requests for data transfers at an unreasonable frequency, the data handler may impose a reasonable fee to cover the associated costs.

D. Cross-border Data Transfers

The Network Data Regulation standardizes the protocols for data exportation, taking into the practice, and aligning with the objectives of the Personal Information Protection Law.

This Personal information Protection Law outlines three primary avenues for the export of personal information: through security assessments, standard contract filings, and professional certifications. It further delegates authority to the cyber security administration to establish additional channels as appropriate. In practice during 2023, the administration has recognized the impracticality of scrutinizing every data export scenario and has therefore exempted certain low-risk export situations from stringent oversight. The Network Data Regulation codifies these exemptions into law, specifying the following scenarios:

(1) When it is essential to provide personal information to an overseas entity for the conclusion or performance of a contract to which an individual is a party;
(2) When the provision of employees' personal information to an overseas entity is required for the implementation of cross-border human resource management, in compliance with legally established labor regulations and collective labor agreements;
(3) When the fulfillment of legal duties or obligations mandates the provision of personal information to an overseas entity;
(4) When personal information must be provided to an overseas entity in emergency situations to safeguard the life, health, or property of an individual.

As such, the Network Data Regulation achieves a balanced approach that upholds data security while accommodating legitimate and low-risk international data transfers.

E. Risk Assessment

In alignment with the protocols for managing personal information, the Network Data Regulation has instituted comprehensive guidelines for risk assessment when dealing with important data.

Similar to the Personal Information Protection Law, which mandates conducting a personal information protection impact assessment in various scenarios, the Network Data Regulation enforces an equivalent requirement. It stipulates that a risk assessment must be carried out prior to any provision, entrustment, or joint management of important data with a third party. The critical elements to be examined in this assessment encompass:

(1) The legality, justifiability, and necessity of the data transfer, as well as the objectives, techniques, and extent of the data recipient's intended use of the network data.
(2) Potential risks of data tampering, destruction, leakage, or unauthorized access and utilization, alongside the possible threats to national security, public welfare, and the legitimate rights and interests of individuals and organizations.
(3) The trustworthiness and adherence to legal standards of the data recipient.

(4) The efficacy of contractual agreements concerning network data security in ensuring that the recipient meets their data protection obligations.
(5) The sufficiency of existing and planned technical and managerial measures to safeguard against the aforementioned risks to network data.

Furthermore, handlers of important data are obligated to conduct an annual risk assessment of their data handling practices and submit a report to the provincial-level or higher regulatory authority. This risk assessment report should encompass:

(1) Fundamental information about the network data handler, details about the network data security management division, and contact information for the designated network data security officer.
(2) The objectives, categories, volumes, techniques, extent, duration of storage, and storage locations concerning the processing of important data, excluding the actual content of the network data.
(3) An overview of the network data security management system and its enforcement, along with the implementation and efficacy of technical measures such as encryption, data backup, tagging, access control, and security certification.
(4) A record of identified network data security risks, occurrences of network data security incidents, and the measures taken to address them.
(5) The results of the risk assessment for activities involving the provision, entrustment, or shared management of important data.
(6) Details regarding the cross-border transfer of network data.

F. Incident Management

The Network Data Regulation consolidates the incident management responsibilities of data handlers, clarifying and reinforcing the provisions previously outlined in the Data Security Law and the Personal Information Protection Law. The obligations include:

(1) The creation and execution of a comprehensive contingency plan to address cyber incidents, with the goals of reducing losses and resolving risks promptly.
(2) The duty to promptly inform individuals or organizations at risk about the cyber incident and any potential risks that may impact their legitimate interests.
(3) The requirement to report the incident to the relevant regulatory authority in accordance with the legal procedures.
(4) The necessity to report to the police or national security authorities if any suspicious criminal activities are detected during the incident resolution process.

Furthermore, operators have a responsibility to take immediate corrective measures if they discover any defects or vulnerabilities in their network products or services. They must notify the affected users and report such issues to the government. Where the defect or vulnerability poses a threat to national security or public interest, a report must be submitted within a 24-hour period.

G. Applications of Innovative Technology

The Network Data Regulation addresses the application of innovative technologies with several specific provisions.

(1) Crawler Technology: To regulate the prevalent practice of employing crawler technology for data collection, the Network Data Regulation establishes boundaries. It mandates that any network data handler utilizing automated tools for data collection must evaluate the potential impact of such tools on network services. Furthermore, it prohibits any unauthorized intrusion into third-party networks or any actions that may disrupt the normal functioning of network operations.

(2) Artificial Intelligence: The regulation includes a principle-based stipulation for network data handlers providing content-generating AI services. It demands the enhancement of security management protocols for training data and the processing activities associated with it. Additionally, it necessitates the implementation of effective measures to preempt and mitigate network data security risks.

(3) Auto-collecting Technology: Recognizing the potential for auto-collecting technology to gather unnecessary personal information or data beyond the scope of consent, the Network Data Regulation does not ban the technology. Instead, it mandates that collected data exceeding the necessary or consented scope must be deleted or anonymized. Should deletion or anonymization be technically challenging, the collecting operator is restricted from using the data beyond storage or implementing protective measures.

(4) Auto-decision Technology: For operators engaged in customized advertising or those pushing notifications to individuals based on auto-decision technology, the Network Data Regulation requires the establishment of clear, accessible, and user-friendly options to opt-out of personalized recommendations. Users must be empowered to decline push notifications and to remove user tags that are targeted based on their personal characteristics.

3. Implication on Business

The enactment of the Network Data Regulation marks a pivotal milestone in the legislative landscape of data protection. Businesses must now ensure readiness to comply with it.

A. Risk Assessment Procedures

The Network Data Regulation underscores the necessity of conducting robust risk assessment procedures, marking a strategic shift towards a more nuanced and proactive approach to data protection compliance. It mandates that network data handlers perform self-assessments of potential risks across a variety of scenarios, thereby personalizing their compliance efforts to the specifics of their operations.

Essentially, these operators are tasked with evaluating the risks arising from their data handling activities or the network services they provide. In cases where substantial risks are detected, operators

are obligated to implement corrective actions to alleviate these risks. Moreover, if the identified risks are deemed to exceed the benefits derived from the data processing activities or network services, a thorough reconsideration of their continuation is mandated.

The Network Data Regulation delineates several scenarios where risk assessments are mandatory:

(1) Personal Information Protection Impact Assessment: This must be carried out prior to handling sensitive personal information, engaging in automated decision-making processes, data processing, data provision, public disclosure of personal information, and the transfer of personal information to foreign entities, as dictated by both the Personal Information Protection Law and the Network Data Regulation.

(2) Important Data Risk Assessment: Handlers of important data are required to perform a risk assessment prior to any provision, entrustment, or joint processing of such data. This assessment primarily includes the evaluation of the legality, legitimacy, and necessity of the data handling, as well as the potential risks to national security, public interest, and the legal rights and interests of individuals or organizations.

(3) Cross-border Data Transfer Risk Assessment: When transferring network data across borders, especially personal and important data, a thorough security assessment is necessary. This assessment must determine whether the transfer's purpose, method, and scope are legal, legitimate, and necessary, and it must also consider the potential risks.

(4) Regular Risk Assessment: The Network Data Regulation enforces annual risk assessments of network data handling activities by important data handlers, with a requirement to submit risk assessment reports to the relevant provincial-level or higher authorities.

(5) Risk Assessment for the Use of Automated Tools: Network data handlers utilizing automated tools for accessing and collecting data must assess the potential impact on network services, ensuring non-interference and non-intrusion into the networks of others.

Despite the diverse scenarios requiring risk assessment, the fundamental factors considered are consistent. Integrating risk assessment procedures into the internal management systems of operators would streamline the process. This integration would allow for assessments to be conducted seamlessly during routine internal reviews and decision-making, preventing the repetitive evaluation of the same factors and thus enhancing overall efficiency.

B. Compliance Review

The Network Data Regulation mandates that operators conduct autonomous compliance reviews and integrate compliance considerations into the product development lifecycle. This stipulation reinforces the Personal Information Protection Law's demand for personal information protection compliance audits, with the Network Data Regulation reiterating and expanding upon this necessity. Importantly, the risk assessment procedures for handlers of important data also encompass an evaluation of the adherence to data handling regulations.

Furthermore, the Network Data Regulation insists on the compliance of network products and services. Operators must guarantee that their offerings align with the obligatory national standards and proactively address any uncovered vulnerabilities. Besides, for operators presenting network products or services to the public, establishing avenues for receiving complaints and reports is imperative. This implies that operators must incorporate these channels into the design phase of their products or services.

Additionally, operators are obliged to adhere to the guidelines of the platforms that host their products and the protocols of third-party distribution services that disseminate their offerings. Under the Network Data Regulation, network platform operators are tasked with establishing data security protocols for products on their platform and supervising compliance with these rules. Similarly, application distribution service providers are responsible for creating and executing compliance checks on the products distributed via their services. Non-compliance with these regulations can lead to the disconnection of the relevant products from the platform or a suspension in their distribution. Consequently, operators must ensure that their network product or service designs are in accordance with platform and distribution guidelines, in addition to legal and regulatory requirements

.

C. Retention of Records

Under the Network Data Regulation, data handlers are legally obligated to maintain detailed records to facilitate potential government inspections. These records are not only essential for fulfilling legal duties, but they also serve as critical evidence that may defend against claims stemming from data-related incidents.

As stipulated by the Network Data Regulation, data handlers must retain the following records:

(1) Data Handling Activity Records: This includes: (a) for personal information collected with consents, a record of the consents obtained, (b) for data provision, entrustment, or joint handling of data, records of contracts with data recipients and documentation of the supervision over the data recipients' activities, and (c) for the handling of important data, a record of annual risk assessments.

(2) Compliance Review Records: This entails: (a)for personal information handling, a record of compliance audits, (b) for any data handling activities potentially impacting national security, a record of national security reviews, and (c) a comprehensive collection of risk assessment reports demonstrating the performance of due diligence.

(3) Incident Management Records: This involves: (a) a contingency plan along with records of training sessions related to the plan, (b) documentation of the execution of the contingency plan to prevent the expansion of losses and mitigate risks.

These meticulous record-keeping requirements ensure that data handlers are transparent, accountable, and prepared to address any issues that may arise in the course of their operations.

If you would like to know more information about the subjects covered in this publication, please contact:

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

SHANGHAI
19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli,
Chaoyang District
Beijing 100020 P.R.China
T: +86 10 5081 3888
F: +86 10 5081 3866

SHENZHEN
18F, China Resources Tower
2666 Keyuan South Road,
Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG
Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON
1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD