Llinks Client Alert - October 2024
Why is this new PRC data security regulation important to your 2025 data compliance work

By David Pan | Nigel Zhu | Susan Deng | Eric Zuo | Jackie Li

On September 30, 2024, China's State Council officially published the long-anticipated *Regulations on Network Data Security Management* ("**Network Data Regulations**"), which will take effect on January 1, 2025. It has been almost three years since the draft of the Network Data Regulations were originally issued by the Cyberspace Administration of China ("**CAC**") in November 2021. The Network Data Regulations appear to be a summary of the CAC's regulatory insights gained from its law enforcement of the *Cybersecurity Law* ("**CSL**"), *Data Security Law* ("**DSL**"), and the *Personal Information Protection Law* ("**PIPL**"). The Network Data Regulations heralds a new era of regulatory compliance for all businesses operating in and outside of China.

Because the Network Data Regulations in essence is NOT a new regulation, the "heads-up" is given on relatively short notice (three months from now to the beginning of 2025). Therefore, we expect that the "grace period" after the Network Data Regulations officially take effect will be relatively short, if any. This alert aims to help clients better understand the Network Data Regulations, and to prepare for key compliance objectives highlighted therein, so that they can be prepared to face regulatory challenges coming up in the near future.

For more Llinks publications, please contact:

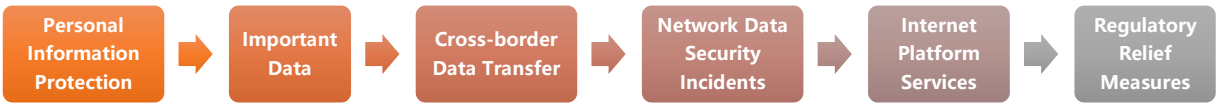
Publication@llinkslaw.com

I. Scope of Application

The Network Data Regulations applies to "network data processing activities" and to "network data processors". Please don't be misguided by the word "network" and think it only applies to Internet and telecommunication companies. Just like the concept of "network operator" in the CSL covers pretty much every company that uses the Internet, it is safe to equal "network data" to data and "network data processors" to data controllers under the Network Data Regulations. Consequently, the application scope of the Network Data Regulations covers all business sectors.

II. Year 2025 compliance obligations indicated by the Network Data Regulations

The Network Data Regulations generally follow the framework set by the CSL, DSL and PIPL, and reflect the principles in these laws. We anticipate that provisions in the Network Data Regulations that reiterate or supplement these three laws are likely to become future regulatory initiatives and law enforcement priorities. Therefore, we draw your attention to the compliance obligations in the following special scenarios prescribed by the Network Data Regulations. Clients are advised to prioritize these compliance tasks in the year of 2025.



Major Compliance Obligations under the Network Data Regulations

1. Personal Information Protection

1.1 Prepare for personal information compliance audits

The PIPL mandates that personal information controllers shall conduct regular personal information compliance audits. Article 27 of the Network Data Regulations reiterates this requirement.

This reiteration shall be read in conjunction with the *Personal Information Protection Compliance Audit Management Measures (Draft for Comments)* published last year, and the national standard "*Data Security Technology - Personal Information Protection Compliance Audit Requirements (Draft for Comments)*" ("**PI Audit Measures**") published recently this year. Together, these regulations further indicate that personal information audit-related laws and obligations are imminent.

We suggest that companies start ASAP to prepare for personal information compliance audit by conducting data mapping and due diligence into the company's personal information processing scenarios and activities. Otherwise, companies may likely be overwhelmed by the magnitude of workload after the PI Audit Measures becomes effective. For more on personal information audit, please refer to our illustrative guidelines, in which we briefly analyze the relevant rules through videos and charts:

- *Too complex? – We've drawn graphs of the Personal Information Compliance Audit for you*

1.2 Appoint domestic representatives and prepare for information submission (foreign entities only)

For data controllers outside China but process personal information of data subjects in China, Article 26 of the Network Data Regulations reiterates the PIPL that foreign data controllers shall establish a

dedicated institution or appoint a representative in China for information submission, and further clarifies that the reporting shall be made to a "municipal-level CAC".

This reiteration and refinement may indicate that the reporting obligations mandated by the PIPL will be enforced in the near future. ***We suggest that foreign data controllers that fall into the scope of the PIPL take prompt actions to determine the type of entity/the individual that will serve as their representative in China and gather the information to be submitted.*** Considerations may include: how familiar is the representative with Chinese law and regulatory framework; the representative's understanding of the data controller's personal information processing and cross-border transmission; the relationship between the representative and the foreign data controller (affiliated entity, executive/employee, or independent third party); the efficiency and smoothness of communication; and whether the appointment of the representative will bring additional risks to the foreign data controller.

1.3 Improve supporting mechanism for personal information transfer requests

Article 25 of the Network Data Regulations clarifies for the first time the specific conditions for individuals to exercise their "right to data portability" under the PIPL, which is likely to increase the frequency of user requests for transferring their personal information.

Data controllers are advised to:

- assess and refine the data portability section of their privacy policies related to the right of transfer (e.g., add the company's review standards for accepting personal information transfer requests, and emphasize that the company has the right to charge reasonable fees for unreasonable transfer requests);
- timely communicate and collaborate with IT and information security departments to ensure that data portability is technically feasible and supported;
- refer to the specific rules for data portability in the national standard "*Data Security Technology - Requirements for personal information transfer based on request of personal information subject (Draft for Comments)*" released in April 2024.

1.4 Data controller processing over 10 million people's personal information

Article 28 of the Network Data Regulations requires that data controllers processing over 10 million people's personal information must comply with some of the obligations imposed on controllers of important data. This is the first time that a general regulation defines personal information that meets a certain quantity level as important data.

Data controllers that meet the quantity threshold are advised to prepare for compliance with the following new obligations in a timely manner:

- Clearly define the person in charge of network data security, establish a network data security management committee, and fulfill the data security protection responsibilities prescribed by law (such as the MLPS);
- In case of merger, division, dissolution, bankruptcy, etc., which may affect the security of over 10 million people's personal information, they should:
  (a) Take data security protection measures;
  (b) Report to their relevant industrial regulators at or above the provincial level on the important data disposal plan, the name or name and contact information of the data receiver, etc.; in case where the industrial regulator is not clearly defined, report to a data security authority at or above the provincial level.

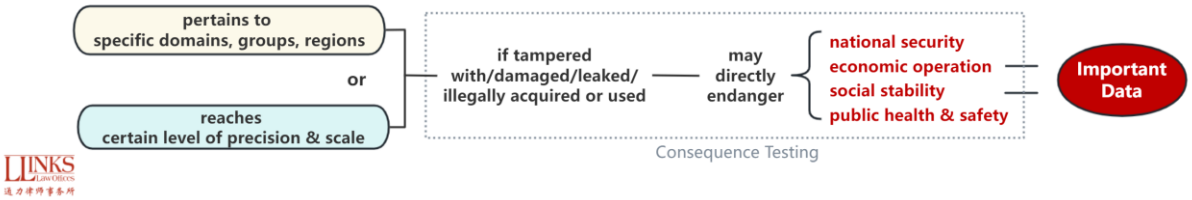
According to the Network Data Regulations, companies processing over 10 million people's personal information are relieved from other important data-related obligations, such as important data risk assessment and annual risk assessment and reporting (however, note that a personal information impact assessment must be carried out for the sharing, contracted processing and joint processing of personal information, and the large amount of personal information shall be taken into consideration in such assessments).

2. Important Data

2.1 Timely identify and declare important data

Article 29 of the Network Data Regulations echoes the DSL regarding the development of a directory of important data by the government, and once again emphasizes data controllers' obligation to identify and declare important data, following the *Provisions on Regulating and Promoting Cross-border Data Flow*.

The identification of important data is the cornerstone of the fulfillment of subsequent compliance obligations. Since neither the DSL nor the CSL provides a definition of important data, regulations such as the *Measures for Security Assessment of Data Exports*, *Provisional Regulations on Data Security Management of Automotive Data*, and the national standard *Data Security Technology - Data Classification and Grading Rules (GB/T 43697-2024)* played an important role in the identification. The Network Data Regulations give the definition of important data at the level of administrative regulations, integrating the identification rules in the previous regulations and national standards (see chart below).



Network Data Regulations' definition of important data

It is worth noting that Article 37 of the Network Data Regulations also clarifies that no security assessment is necessary for any data that is not officially declared as important data. This will effectively reduce the compliance costs of companies with data export needs.

Although by law important data will be determined by the government, in practice, authorities constantly organize companies in their jurisdiction to "brainstorm" the identification of important data and request them to declare the types of important data they have identified. Therefore, ***we suggest that critical infrastructure related companies refer to the identification rules of important data to conduct the classification and grading of data as ASAP, and communicate with the competent authorities about the progress of the important data directory on a regular basis.*** We will closely follow the development of the important data directory and keep you posted.

2.2 Special Risk Assessment for Important Data

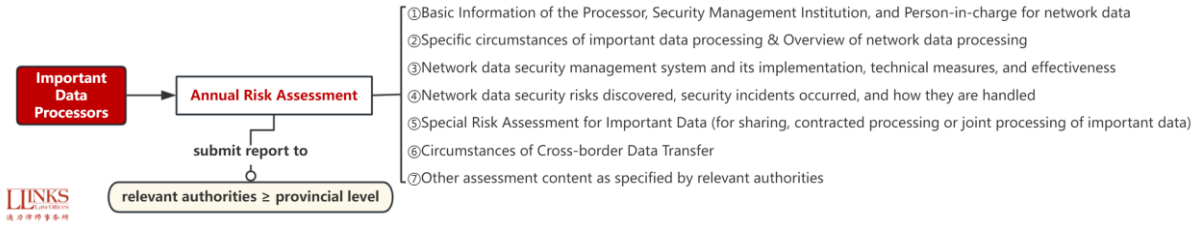
Article 31 of the Network Data Regulations introduces a new requirement called "Special Risk Assessment" for important data - in addition to performing legal duties or obligations, controllers of important data must conduct a risk assessment before **(i) sharing, (ii) contracted processing, or (iii) joint processing** of important data (in contrast, the impact assessment for personal information is triggered in all of the three scenarios above, and also where a data controller is processing sensitive personal information and data export. However, since important data is inherently "sensitive data", and its cross-border transfer requires a security assessment, the Network Data Regulations limit the scope of the risk assessment to the above three circumstances). The key contents of the assessment include:

Special Risk Assessment Requirements for Important Data

We suggest that companies that may possess important data should draw reference from the impact assessment of personal information and prepare for the special risk assessment for important data, such as assessing the overall project risk, drafting or reviewing contracts related to the sharing/contracted processing/joint processing of important data, and improving network data security protection measures.

2.3 Annual Risk Assessment & Reporting for Important Data Controllers

For companies processing important data, Article 33 of the Network Data Regulations introduces new requirements for an annual risk assessment and reporting:



Annual Risk Assessment and Reporting Requirements for Important Data Processors

Annual risk assessment and reporting for important data have already become routine work in certain industries (such as the automotive industry). Therefore, companies in other industries can proactively draw on the assessment and reporting experience of these specific industries.

3. Cross-border Data Transfer

In terms of cross-border data transfer, the Network Data Regulations mainly reiterates and supplements the existing rules:

3.1 Expansion of Personal Information Export Pathways

The Network Data Regulations not only reiterate the pathways for personal information exports as stipulated in the PIPL, but also re-establish the 3 exemptions specified in the *Provisions on Regulating and Promoting Cross-border Data Flow* as official pathways from the level of administrative regulations (for details, please refer to our previous review *A Brief Review of China's New Data Export Regulation*).

Personal Information Export Pathways under the Network Data Regulations

Furthermore, reading in conjunction with the *Memorandum of Understanding on China-Germany Data Cross-border Flow Cooperation* signed between the CAC and the German Federal Ministry of Digital Affairs and Transport in June this year, we believe that China will continue to deepen international cooperation in promoting data cross-border flow in the future. We also look forward

to these new pathways bringing better solutions to the actual needs of foreign clients in the fields of financial data cross-border supervision and inspection.

3.2 Clarify Scale of Data Export When Conducting a Security Assessment

The *Measures for Security Assessment of Data Exports* stipulated that if the purpose, method, scope, and type of data processed by the data processor change, a new data outbound security assessment must be re-declared (for a complete interpretation, please refer to *Dust Settled: Measures for Security Assessment of Data Exports*).

In this regard, the Network Data Regulations further add a restriction on "scale". That is, data exporters are required to transfer personal information and important data to overseas entities only in accordance with the purpose, method, scope, and type that filed with the authority in the data export security assessment.

To avoid the compliance costs brought by re-doing the assessment, we suggest that data exporters clearly define the scale of their data export before conducting the security assessment.

4. Network Data Security Incident Response

4.1 Report significant risks of network products within 24 hours

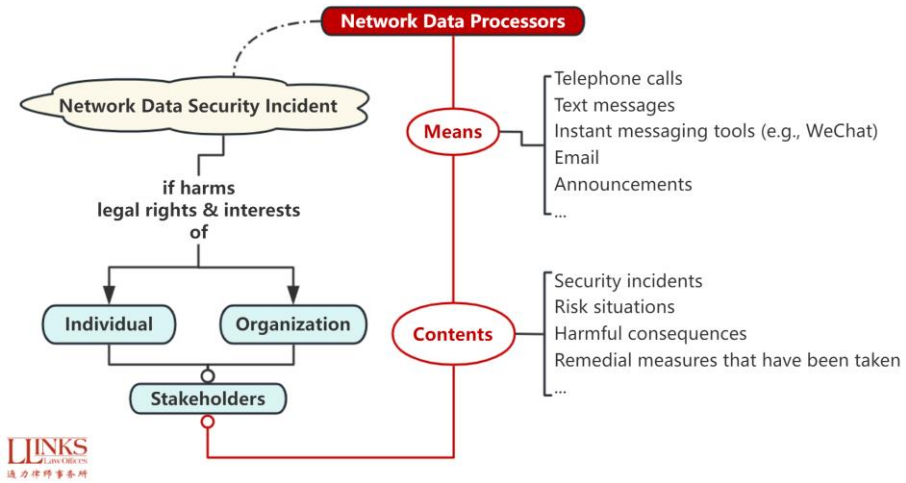
Article 10 of the Network Data Regulations introduces new reporting requirements for network products or services that pose a threat to national security or public interests. Data controllers must report to the authorities **within 24 hours** when they discover that their network products or services **may threaten national security or public interests**. To make the compliance with this obligation more pragmatic, we anticipate authorities to clarify the specific form and reporting channels required for this reporting.

Compared to the 2-day reporting time-limit prescribed in the *Network Product Security Vulnerability Management Regulations* previously issued by the Ministry of Industry and Information Technology, this clause focuses more on protecting national security and public interests so that it has a shorter time limit.

4.2 Reporting and notification obligations for network data security incidents

Article 11 of the Network Data Regulations reiterates the reporting obligations for cybersecurity incidents under the DSL and CSL, requiring reporting to the relevant authorities when a network data security incident occurs. Since the clause still lacks details, we suggest that companies prepare for incident reporting in accordance with the *Cybersecurity Incident Reporting Management Measures (Draft for Comments)* released by the CAC in December 2023.

Furthermore, Article 11 also introduces new **notification obligations** for network data security incidents. Except as otherwise provided by law or administrative regulations, when a network data security incident harms the legal rights and interests of individuals or organizations, network data processors shall notify the stakeholders **in a specific manner** as shown in the figure below:



Notification Requirements for Network Data Security Incidents

5. Internet Platform Services

5.1 Strengthen supervision on third-party product/service providers on the platform

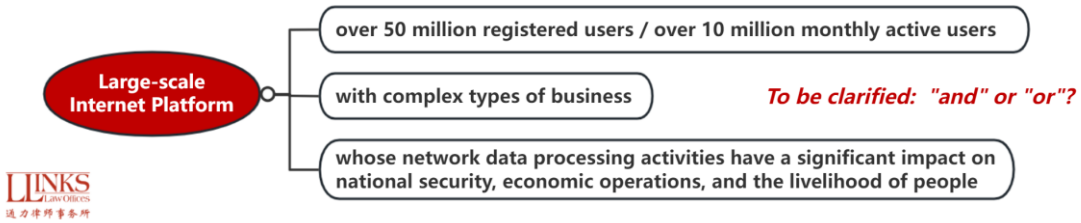
Article 40 of the Network Data Regulations stresses that Internet platform service providers have a supervisory duty and may be jointly liable for third-party product and service providers on their platforms:

- They should specify in their platform rules or contracts the network data security protection obligations of third-party product and service providers accessing their platforms.
- They should procure third-party product and service providers to strengthen network data security management (e.g., if a third party carries out network data processing activities illegally, in violation of regulations, or in breach of contract, causing damage to users, the internet platform service provider and the third-party product and service provider will bear corresponding responsibilities).

In addition, this clause also specifically states that "manufacturers of smart terminal devices such as pre-installed application devices" are also subject to the above regulations. We advise companies engaged in the production of smart home appliances, medical and chemical equipment (e.g., analyzer programs pre-installed in laboratory equipment), and other similar devices to update their agreements in a timely manner, ramp up supervision, and consider purchasing liability insurance.

5.2 Large-scale Network Platforms

The Network Data Regulations set the criteria for "Large-scale Network Platform" at the level of administrative regulations (as shown in the figure below, but it is not clear whether the relationship between the three conditions is "and" or "or", which needs to be further clarified (we are inclined to understand it as "or")). However, the regulation is unclear in terms of whether companies need to carry out their own identification or whether the competent authorities will subsequently publish a corresponding list.



Identification Criteria for large-scale Internet platform

Large-scale Network Platforms must fulfill the following obligations:

- Publish the "Personal Information Protection Social Responsibility Report" annually (which includes the measures and effectiveness of personal information protection, the handling of individual rights exercise applications, and the performance of duties by the personal information protection supervision organization mainly composed of external members, etc.)
- Comply with the national data cross-border security supervision requirements when exporting data.
- Must not use network data, algorithms, and platform rules, etc., to harm the legitimate rights and interests of users.
- When processing important data, it should also fully explain the network data security of key businesses and supply chains in its annual risk assessment report (see the aforementioned "Annual Risk Assessment & Reporting for Important Data Processors").

In addition, after the official introduction of the *Personal Information Protection Compliance Audit Management Measures*, large-scale platforms will also need to fulfill the personal information audit obligations specifically targeting them, such as establishing an independent supervision organization mainly composed of external members, and focusing on auditing the rules of large Internet platforms and the content of the "Personal Information Protection Social Responsibility Report".

6. Relief of Compliance Burden

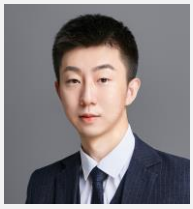
It is worth noting that in order to reasonably connect the existing regulatory rules in the field of network security and data compliance, Article 52 of the Network Data Regulations specially emphasizes the "burden relief principle". Specifically:

- When the competent authorities carry out supervision and inspection of network data security, they should **avoid unnecessary inspections and redundant inspections**.
- Personal information protection compliance audits, risk assessments of important data, and security assessments of important data going abroad should be better coordinated to **avoid repetitive assessments and audits**.
- When there is an overlap between the risk assessment of important data and the network security level assessment, **the relevant results can be mutually recognized**.

We look forward to these requirements effectively reducing the compliance burden on companies after the implementation of the Network Data Regulations, and we will continuously follow the subsequent law enforcement trends of various regulatory authorities.

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

David Pan
+86 21 3135 8701
david.pan@llinkslaw.com



Nigel Zhu
+86 21 3135 8683
nigel.zhu@llinkslaw.com

SHANGHAI	BEIJING	SHENZHEN
19F, ONE LUJIAZUI 68 Yin Cheng Road Middle Shanghai 200120 P.R.China T: +86 21 3135 8666 F: +86 21 3135 8600	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	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	LONDON
Room 3201, 32/F, Alexandra House 18 Chater Road Central, Hong Kong T: +852 2592 1978 F: +852 2868 0883	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