China Insight

China Releases Regulations on Network Data Security Management

On 30 September 2024, the State Council of China released the *Regulations on Network Data Security Management* ("Regulations"), which will come into effect on 1 January 2025.

1. Background

The Regulations are the first administrative-level legal instrument in China following the establishment of the basic framework of China's three fundamental laws in the field of data protection, i.e. the *PRC Cybersecurity Law* ("CSL"), the *PRC Personal Information Protection Law* ("PIPL"), and the *PRC Data Security Law* ("DSL"). After the release of the draft version for public comments in November 2021, following three years of anticipation, the Regulations have been finally published and will take effect on 1 January 2025.

The Regulations, overall, provide detailed stipulations of the three fundamental data laws, but many provisions have already been reflected and covered in previously issued laws, regulations, and national standards. Therefore, our article will focus on some new and key content from the perspective of company's obligations.

2. Scope of application

According to Article 2 of the Regulations, the Regulations apply to network data processing activities and their safety supervision and management within the territory of China. The activities processing personal information of Chinese natural persons, as well as the processing activities that would harm China's national security, public interests, or the lawful rights and interests of citizens or organizations, carried out outside China, are also subject to the Regulations.

Based on the definitions in the Regulations, "network data" refers to "all kinds of electronic data processed and created through networks", which theoretically excludes any data processed by physical means, such as on paper. The term "network data processor"[1] refers to "a person or organization that decides on its own purpose and processing method in network data processing activities".

[1] The companies mentioned below are all referred to as network data processors.

Therefore, considering the widespread use of network processing data and the growing degree of digitization, most companies are subject to the Regulations and should attach importance to the Regulations.

3. Key obligations for companies

a) General obligations

(1) Report of security defects and vulnerability

Previously, according to Article 7 of the *Provisions on the Management of Security Vulnerabilities on Network Products* released in September 2021, when a company discovers that security defects or vulnerability exists in its provided network product or service, all these security defects and vulnerabilities should be reported to Information Sharing Platform for Network Security Threats and Vulnerabilities of the Ministry of Industry and Information Technology within two days.

On this basis, Article 10 of the Regulations further requires that if the identified security defects or vulnerability could jeopardize national security or public interests, the company shall report the situation to the relevant competent authority within a shorter timeframe, i.e. within 24 hours.

(2) Notice of network data security incident to affected parties and report to competent authorities

It is specified in the Regulations that companies are required to notify affected individuals and organizations when harm is caused to the legitimate rights and interests of individuals and organizations. In terms of notification methods, the Regulations allow the way of phone calls, text messages, instant messaging tools, electronic mail, or announcements, etc.

In addition, the Regulations require that companies shall also report to competent authorities in accordance with relevant regulations. For details of the reporting deadline and reporting content, etc., companies may refer to *Measures for the Administration of Cybersecurity Incident Reporting (Draft for comments)* issued in December 2023.

(3) Supervision of data recipients

As to the processing of personal information and important data, Article 12 of the Regulations specifies the obligation of companies to supervise data recipients when processing data. A company shall agree with the recipient of the concerned personal information and important data on the purpose, method, scope, and security protection obligations of the processing through a contract or by other means, and supervise the performance of fulfilling obligations by the data recipient. In addition, the company is required to keep records of related processing for at least three years.

b) Obligations related to handling of personal information

(1) Refined requirements regarding notification and consent

On the basis of the "notification and consent" requirement stipulated in the PIPL, the Regulations refine the required matters that shall be included in a notification to be distributed to the concerned individuals. In particular, the notification should:

- include the specific personal information rights, including the rights to inspect, copy, transfer, correct, supplement, delete, restrict the processing of personal information, as well as to deactivate accounts and withdraw consent;

- specify the purpose, method, and type regarding the processing relevant personal information, as well as the information on the data recipient, in the form of a list, if personal information is provided to other network data processors;

- clearly define the method for determining the retention period, if a specific retention period is difficult to determine.

(2) Rule of the right to data portability

Article 25 of the Regulations first clarifies the rule of the right to data portability stipulated in the PIPL. Specifically, for requests to transfer personal information that meet the following conditions, the network data processor should provide means for other network data processors designated by the individual to access and obtain relevant personal information:

- The identity of the individual requester can be verified;

- The transfer is of personal information that the individual has consented to provide or that has been collected based on a contract;

- The transfer of personal information is technically feasible;

- The transfer of personal information does not infringe upon the legitimate rights and interests of others.

(3) Overseas processors' obligation on establishing specialized bodies

Previously, according to Article 53 of the PIPL, foreign data processors who directly process the personal information of natural persons within China from abroad for the purpose of providing products and services to natural persons within the territory of China or for analyzing and assessing the behavior of natural persons within the territory of China, shall establish a dedicated body or designate a representative in China. Article 26 of the Regulation reiterates this obligation and clarifies that the name and contact information of the body or representative should be reported to the local municipal-level cyberspace authority where the agency or representative is located.

(4) New exemption scenario for cross-border transfer

Article 35 of the Regulations adds a newly applicable exemption scenario compared to the scenarios stipulated in Article 5 of the *Provisions on Promoting and Regulating Cross-border Flow of Data*, i.e. where there is a need to provide personal information outside China in order to perform statutory duties or legal obligations, the processor is allowed to transfer the personal information without the declaration for the security assessment, the conclusion of the standard contract, or the personal information protection certification. However, the scope of its application, such as whether the legal obligations referred to here solely pertain to Chinese laws and regulations, still needs further clarification.

c) Obligations related to handling of important data

(1) Threshold for personal information processors deemed as important data processors

As stipulated in Article 28 of the Regulations, if a company processes more than 10 million people's personal information, it is required to perform the security protection responsibilities as a processor of important data, e.g. appointment of the person in charge of network data security and the network data security management organization, as well as reporting obligations in the event of merger, demerger, dissolution, bankruptcy, etc. of the company.

Besides, it is necessary to analyze the application situation on a case-by-case basis for specific industry. For example, in the automotive industry, personal information involving more than 100,000 individuals is important data according to the *Regulations on the Safe Management of Automotive Data (Trial Version)*.

(2) Important data risk assessment

The Regulations stipulate a new requirement for specialized risk assessment of important data, i.e., companies should carry out a risk assessment before providing, commissioning, or co-processing important data. In addition, companies are required to conduct a risk assessment of their network data processing activities on an annual basis. Such risk assessment report shall be submitted to relevant competent authorities at or above the provincial level.

d) Obligations for companies in specific industries

(1) Companies in AI industry

Article 19 of the Regulations stipulates that companies providing generative artificial intelligence services shall strengthen the security management of training data and related processing activities, as well as take effective measures to prevent and address network data security risks. For other compliance requirements regarding training data processing activities, reference can be made to the previously released *Interim Measures for the Administration of Generative Artificial Intelligence Services* and *Basic Requirements for the Security of Generative Artificial Intelligence Services*.

In addition, the legitimacy and restrictions of automated collection techniques such as crawling and robotic process automation have been fully discussed as a hot topic. Previously, automated collection techniques were regulated from the perspective of the *PRC Anti-Unfair Competition Law*. The Regulations require that when using automated tools to access and collect network data, companies should assess the impact on the data service, and not infringe upon other's networks or interfere with the normal network service operation. Article 24 of the Regulations further clarifies the requirements for handling personal information through automated collection techniques. If automated collection techniques are used to obtain relevant training data, companies should delete or anonymize the personal information contained therein.

(2) Companies involved in online platform services

The Regulations impose many safety supervision and management obligations on providers of network platform services and providers of large-scale network services. A "large-scale data platform" is defined as a network platform that owns a registered user base of 50 million or more, or an active user base of 10 million or more in a month. The platform also has a complex business type, and whose network data processing activities have a significant impact on national security, economic operations and national economy. According to Article 44 of the Regulations, the providers of large-scale network platform services should publish an annual social responsibility report on personal information protection.

(3) Companies involved in government-related services

The Regulations clarify that companies providing services to government departments, critical information infrastructure operators and other public infrastructure or public service systems shall adopt a higher and stricter level of security protection. It is explicitly required that without the consent of the entrusting party, the service provider is not allowed to access, obtain, retain, use, disclose or provide network data to others, or to conduct correlation analysis of network data.

4. Legal liabilities

The Regulations stipulate legal liabilities for three types of illegal activities, including violation of data security protection obligations, data processing endangering national security, and violation of important data management regulations. For scenarios which are not covered by the Regulations, the *PRC Cybersecurity Law*, the *PRC Data Security Law*, and the PIPL shall be applied.

The current maximum fine for companies is capped at RMB 10 million, but only for situations where network data processing activities affect national security. In addition, Article 59 of the Regulations introduce the principles of "no penalty for the first violation" and "no penalty for minor violations", making it clear that the primary purpose of stipulating penalties is not to impose fines, but to avoid the harm of illegal data activities.

5. Conclusion

The Regulations address the outstanding issues of network data security management, scientifically summarize past governance experience, and take into account new security issues brought about by new technologies and applications. Since the Regulations will be formally implemented next year, we recommend that relevant companies should actively identify their compliance obligations and proactively assess their compliance efforts based on the Regulations during the transition period of three months.

In case you have questions or for further information, please contact the authors of this newsletter:

Panpan Tang
Senior Associate
CMS, China

T +86 21 6289 6363
E Panpan.Tang@cmslegal.cn

Daisy Lv
Junior Associate
CMS, China

T + 86 21 6289 6363
E Daisy.Lv@cmslegal.cn

CMS Hasche Sigle Shanghai
Representative Office (Germany)
3108 Plaza 66, Tower 2
1266 Nanjing Road West
Shanghai 200040, China

CMS Cameron McKenna LLP Beijing
Representative Office (UK)
Room 1909, China Youth Plaza,
No. 19 Dongsanhuan North Road,
Chaoyang District
Beijing 100026, China