勤理.
Qinli Legal

Legal Comment

Authors:
Weiheng Jia
weihengjia@qinlilegal.com

Sean Xu
seanqu@qinlilegal.com

Zheyu Yang
eryang@qinlilegal.com

For more information, please contact:
Patrick Yip
Senior International Advisor
patyipqinli@qinlilegal.com

Cody Chen
codychen@qinlilegal.com

Alexander Fischer
alexfischer@qinlilegal.com

Clare Lu
cllu@qinlilegal.com

Ron Ma
roma@qinlilegal.com

Jolin Song
jolsong@qinlilegal.com

Xiangyang Ge
xyge@qinlilegal.com

Zhen Han
zhenhan@qinlilegal.com

Ping Liu
liuping@qinlilegal.com

Jason Lin
jasonlinzj@qinlilegal.com

Jason Ma
jasonma@qinlilegal.com

Lizhong Jiang
lzjiang@qinlilegal.com

Start of a New Era in Data Compliance – Analysis on the Key Points of the PRC Data Security Law

China's Data Security Law was adopted by the Standing Committee of the Thirteenth National People's Congress of the People's Republic of China on June 10, 2021, and will come into force on September 1, 2021. The Data Security Law is one of a series of laws focusing on the subject of network, data and information security, together with the Cyber Security Law and the forthcoming Personal Information Protection Law constitutes three fundamental laws in this field. In particular, the Data Security Law establishes the general principles of data security management, as well as the administration and punishment.

I. Analysis on the Key Points of the PRC Data Security Law

(i) Scope of Application

Article 2 of the Data Security Law stipulates that the law applies to "carrying out data processing activities and conducting security supervision within the territory of the People's Republic of China". That is to say, the law mainly regulates "data processing activities" and "security supervision" of data processing activities by government bureaus. It is not a law regulating civil rights and obligations relating to data. In other words, any organization or individual that carries out data processing activities in China must comply with the provisions of the Data Security Law. Meanwhile, in line with a series of recently promulgated laws concerning national security, Article 2 of the Data Security Law clearly stipulates that China will pursue the legal liability against any oversea data processing activity that harms PRC national security and public interest.

The Data Security Law also broadly defines the scope of "data processing" and defines data processing as "including data collection, storage, use, processing, transmission, provision, publication and etc." The definition enumerates known and common data processing activities, using the definitions of "including" and "etc.", leaving room for further expansion of the application of the law by judicial or administrative interpretation.

(ii) Supervision Authorities and Their Functions and Powers

Articles 5 and 6 of the Data Security Law stipulates that the data security supervision authorities and their functions and powers.

1. **The central leadership organ of national security** is responsible for the decision-making, deliberation and coordination in respect of national data security work, and establishes a national data security coordination mechanism. Through legislation, China has raised the data security and network security to the height of national security. At present, the highest leadership body responsible for China's national security is the National Security Commission of the Central Committee of the Communist Party of China.

2. **The competent industrial government departments** undertake the responsibility for data security supervision in their respective industries and fields. According to this authorization rule, the competent industrial government departments are eligible to formulate detailed rules for data security supervision based on the actual situations of different industries. For example, the Ministry of Industry and Information Technology can formulate detailed rules for data security supervision in internet and automobile industries.

3. **The public security organs and national security organs** shall undertake the duties of data security supervision within the scope of their respective duties. According to the provisions of the PRC National Security Law, the public security organs and national security organs shall have the authority to collect intelligence information related to national security, and exercise investigation, detention, preliminary hearing and execution of arrest and other functions and powers stipulated in accordance with the relevant laws and regulations. In the meantime, the public security organs have set up Cyber Security Monitoring and Cyber Security Safeguarding departments to supervise the internet.

4. **The national cyberspace administration authority** is responsible for the overall coordination of **network data security** and relevant supervision. At present, China's national cyberspace administration authority refers to the "Office of the Central Cyberspace Affairs Commission of the Communist Party of China" and the "Cyberspace Administration Office of PRC State Council", they are actually the same

organization with two brands, and are directly subordinate to the Central Commission of the Communist Party of China and the PRC State Council.

(iii) Data Security System

1. Data Protection System based on Hierarchical Classification

Article 21 of the Data Security Law provides that China shall establish a data protection system based on hierarchical classification. The basic principle is to provide classified protection according to the degree of importance of data and the degree of harm caused by an infringement. According to the Data Security Law, data can be classified into three categories for protection and management: (1) national core data, (2) important data and (3) normal data. As for the scope and definition of the national core data, the Data Security Law only provides one broad principle, it does not make clear that any institution has or will have the power to identify "national core data", to issue a more operational catalogue and etc. We speculate that the catalogue of national core data may be defined in the "important data catalogue".

The Data Security Law provides that the national data security coordination mechanism will coordinate to issue the "important data catalogue" and requires to give priority protection towards important data. We anticipate that there will be further clarification on the management and protection requirements for important data in the future.

Although the Data Security Law does not mention the normal data, according to understanding of the law, data other than national core data and important data shall be treated as normal data.

2. Data Security Review System

Article 24 of the Data Security Law stipulates that China shall establish a data security review system, under which data processing activities that affect or may affect national security are subject to national security review, and the lawful decision made on security review shall be the final decision. However, the Data Security Law does not provide detailed rules for data security review and their scope of application. This article is also an authorization rule, which authorizes the data supervisory institution to conduct national security review. It remains unclear whether any prior or subsequent approval is required or any action should be taken to mitigate risk.

3. Data Export Control

Article 25 of the Data Security Law provides that China shall implement export control over data related to items which fall under controlled categories for safeguarding

national security and interests and fulfilling international obligations. Such provision in the Data Security Law links with the corresponding regulation in the PRC Export Control Law. The Export Control Law stipulates the export control requirements for the relevant goods, technologies, services and other items, including technical information and data related to the items. Therefore, if the data to be exported fall under the export control list, the export of data shall also be approved by the Export Administration Department of the State Council or the Central Military Commission according to the Export Control Law.

(iv) Obligations of Data Security Protection

1. Data Security Management

Article 27 of the Data Security Law stipulates that the following shall be done to carry out data processing activities:

a. Establish and improve **a whole-process data security management system** according to the law, organize **data security education and training**, and take appropriate **technical measures and other necessary measures** to ensure data security.

b. **Data processing activities carried out by use of information networks such as the Internet** shall fulfill the data security protection obligations based on the **classified protection system for cyber security**.

c. In addition, **important data processors** shall specify their respective **data security officer and management department**, to implement their data security protection responsibilities.

As for the classified protection system for cyber security applicable to network data processing, this article of the Data Security Law corresponds with Article 21 of the PRC Cyber Security Law which stipulates that network operators shall perform the relevant security protection obligations in accordance with the requirements of the classified protection system for cyber security. The PRC Ministry of Public Security once issued the Regulations on Classified Protection of Cybersecurity (Draft for Comments) for public comments. According to such regulation, networks are classified into five levels of security protection based on the importance and the degree of harm caused by an infringement; a network with a higher level of security protection shall be subject to higher level of security protection measures; and a network at or above Level II must also pass the expert review, obtain approval by the competent industrial authority and file record with the public security authority.

The draft Regulations on Classified Protection of Cybersecurity is yet to be formally promulgated. In addition, it should be noted that the PRC Standardization Committee has issued the Information Security Technology – Baseline for Classified Protection of Cybersecurity (GB/T 22239-2019), the Information Security Technology – Technical Requirements of Security Design for Classified Protection of Cybersecurity (GB/T 25070-2019), the Information Security Technology – Evaluation Requirement for Classified Protection of Cybersecurity (GB/T/28448-2019) and other relevant standards, which have formed a system of standards for the classified protection of cyber security.

2. Data Security Risk and Response to Security Incidents

Article 29 of the Data Security Law stipulates that the following shall be done to carry out data processing activities:

a. Strengthen risk monitoring, and immediately take remedial measures upon discovery of data security defects, bugs and other risks;

b. In the event of data security incident, immediately take measures to deal with the incident, notify users in a timely manner and report the incident to the relevant competent authority in accordance with laws.

3. Risk Assessment

Article 30 of the Data Security Law stipulates that **important data processors** shall, in accordance with the relevant provisions, **conduct regular risk assessments** over their data processing activities and submit risk assessment reports to the relevant competent authorities. The risk assessment report shall include the types and quantities of important data processed, the data processing activities carried out, and the data security risks faced and the countermeasures taken.

4. Administration of Data Cross-Border Transfer

Article 31 of the Data Security Law stipulates that:

a. The security administration of the cross-border transfer of important data collected and generated during the operation by critical information infrastructure operators within China shall be subject to the provisions of the Cyber Security Law;

b. The security administration measures for the cross-border transfer of important data collected and generated during the operation by other data processors

within China shall be formulated by the national cyberspace administration authority in collaboration with relevant departments of the State Council.

The Article 37 of the Cyber Security Law requires that the cross-border transfer of important data (as well as personal information) generated and collected by critical information infrastructure operators within China shall be subject to security assessment in accordance with the measures formulated by the national cyberspace administration authority in collaboration with relevant departments of the State Council. The measures for the security assessment of important data to be transmitted overseas were once released for public comment by the national cyberspace administration authority, but are yet to be released.

In addition, Article 36 of the Data Security Law also stipulates that no organization or individual within China can provide foreign judicial or law enforcement authorities with any data stored within China without the approval of the PRC competent authorities. The PRC competent authorities shall, in accordance with the relevant PRC laws, the international treaties and agreements concluded or acceded to by China, or based on the principle of equality and mutual benefit, handle the request of supply of data from foreign judicial or law enforcement authorities.

(v) Legal Liability

Article 45 of the Data Security Law provides the legal liability that shall be borne by organizations and individuals conducting data processing activities who fail to perform the relevant data security protection obligations (obligations under Articles 27, 29 and 30 of the Data Security Law); Article 46 of the Data Security Law stipulates the legal liability for illegal cross-border transfer of important data (in violation of Article 31 of the Data Security Law); and Article 48 of the Data Security Law stipulates the legal liability for provision of data to foreign judicial or law enforcement authorities without obtaining approval from PRC authority (in violation of Article 36 of the Data Security Law). Such legal liability, depends on the severity of the illegal acts and consequences caused, includes:

a. Ordering to make correction, warning, imposing a fine, and ordering to suspend the relevant business, shut down business for rectification, and revoke the relevant business permit or business license against the enterprise.

b. Imposing a fine against the officer(s) directly in charge and other individual(s) directly responsible.

It is worth noting that a fine of up to RMB 10 million can be imposed against an illegal act that: (i) violates the national core data administration regulation and endangers national sovereignty, security and development interests; (ii) severely violates the administration regulations on data cross-border transfer.

In addition to the above penalties, the Data Security Law also stipulates that the corresponding legal liability shall be borne by anyone whose conduct constitutes a criminal offence, violates public security administration or causes damage to others. However, the Data Security Law does not specify how shall the criminal liability, public security administrative penalty and civil liability be applied. In this regard, the PRC Criminal Law, the PRC Law of Administrative Penalties for Public Security, the PRC Civil Code and other relevant laws and regulations shall be followed to judge on a case-by-case basis.

II. Our Insights

On the one hand, the Data Security Law establishes the basic systematic framework of data security governance, and provides the fundamental legal basis for administration of data security by PRC authority. On the other hand, several key issues in relation to data security preliminarily dealt by the Data Security Law, such as the definition and scope of important data as well as administration of the cross-border data transfer, are yet to be clarified in the future regulations.

With regard to the definition and scope of important data, now the Data Security Law and the Cyber Security Law have not provided the definition of important data. A catalogue of important data shall be issued in future according to the Data Security Law. Regarding to the concept and scope of important data, the Cyberspace Administration Office of State Council has issued the Administrative Measures for Data Security (Draft for Comments), the Measures for Security Assessment on Cross-border Transfer of Personal Information and Important Data (Draft for Comments), and the National Information Security Standardization Technical Committee has issued the Information Security Technology – Guidelines for Date Cross-border Transfer Security Assessment (Draft for Comments) to attempt to define the concept and scope of important data. In addition, the National Information Security Standardization Technical Committee also plans to compile the Information Security Technology – Guidelines for Identification of Important Data to formulate standards for the identification of important data. The concept, scope and catalogue of important data are to be further specified in following official regulations.

Regarding to the administration of cross-border data transfer, in terms of important data, compared with the Cyber Security Law, the Data Security Law newly includes provisions on the administration of the cross-border transfer of important data controlled (collected and generated within China, the same below) by data processors other than critical information infrastructure operators, and provides that detailed measures shall be formulated by the national cyberspace

administration authority in collaboration with relevant departments of the State Council. Based on the Cyber Security Law and other relevant regulations, the Cyberspace Administration Office of State Council has issued the Measures for Security Assessment on Cross-border Transfer of Personal Information and Important Data (Draft for Comments), and the National Information Security Standardization Technical Committee has issued the Information Security Technology – Guidelines for Date Cross-border Transfer Security Assessment (Draft for Comments) as an attempt to formulate rules on the security assessment of cross-border transfer of important data. Data cross-border transfer security administration, especially detailed rules for data cross-border transfer security assessment, are yet to be finalized in official documents in the future.

Data is commonly regarded as the core competitiveness of countries and economic organizations in the next era. Issues such as national security, personal privacy and data ownership are constantly emerging. Laws and regulations, which are the general principles of data security management, are imperative. After the enactment of the Data Security Law, the Personal Information Protection Law and other relevant administrative regulations, rules and standards will be promulgated intensively. In view of this, all enterprises and relevant personnel must initiate data compliance work as early as possible, follow up the issuance of new laws and regulations, sort current data processing procedures, and perfect the data processing compliance measures.

Legal Analysis is published for the clients and professionals of Shanghai Qin Li Law Firm. The contents are of a general nature only. Readers are advised to consult their advisors before acting on any information contained in this newsletter. For more information or advice on the above subject or analysis of other issues, please contact:

Patrick Yip
Senior International Advisor
patyipqinli@qinlilegal.com

Cody Chen
codychen@qinlilegal.com

Alexander Fischer
alexfischer@qinlilegal.com

Weiheng Jia
weihengjia@qinlilegal.com

Clare Lu
cllu@qinlilegal.com

Ron Ma
roma@qinlilegal.com

Jolin Song
jolsong@qinlilegal.com

Xiangyang Ge
xyge@qinlilegal.com

Zhen Han
zhenhan@qinlilegal.com

Ping Liu
liuping@qinlilegal.com

Jason Lin
jasonlinzj@qinlilegal.com

Jason Ma
jasonma@qinlilegal.com

Lizhong Jiang
lzjiang@qinlilegal.com

About Shanghai Qin Li Law Firm

Shanghai Qin Li Law Firm is a member of the Deloitte Legal global network. Shanghai Qin Li Law Firm prepares and publishes "Legal Analysis", which includes introduction and commentaries on newly issued legislations, regulations and circulars. For more information, please contact:

Shanghai Qin Li Law Firm
15/F Bund Center,
222 Yan An Road East
Shanghai 200002, PRC
Telephone: +86 21 6141 1718
Fax: +86 21 6141 1758
www.qinlilegal.com

If you prefer to receive future issues by soft copy or update us with your new correspondence details, please notify us by either email at inquiries@qinlilegal.com or by fax to +86 21 6335 0003.