A New Chapter in Data Security Governance – Commentary on the Data Security Law

Authors: Kevin DUAN | Kemeng CAI | Minzhe HU[1]

On June 10, 2021, the *Data Security Law of the People's Republic of China* (the "**Data Security Law**") was adopted at the 29th meeting of the Standing Committee of the 13th National People's Congress. The law will officially enter into force on September 1, 2021. The Data Security Law is a fundamental law in the area of data security and is also a key component of the entire national security legal system. In this article, we provide a preliminary analysis of the changes and key issues in the final draft of the Data Security Law, and then further analyze the relationship between the Data Security Law and other related regulations as well as challenges for corporate compliance.

What are the important changes compared to the second reading draft?

The final draft of Data Security Law is generally consistent with the April 29 second reading draft that preceded it. The primary changes are as follows:

- **Strengthens the top-level design of data security management.** According to Article 5 of the final draft, the National Security Commission of the CPC will coordinate major issues and work related to national data security. The article also establishes a coordination mechanism for national data security work and strengthens the top-level design of data security management.
- **Core state data appears for the first time, strengthening classified and graded data protection.** The final draft at Article 21 introduces the concept of "core state data" based on the establishment of classified and graded data protection systems and the development of an important data catalogue. In this regard, the Article 21 provides that core state data is "data related to national security, lifelines of the national economy, important matters related to people's livelihood and major public interests and such data will be subject to a stricter management system."

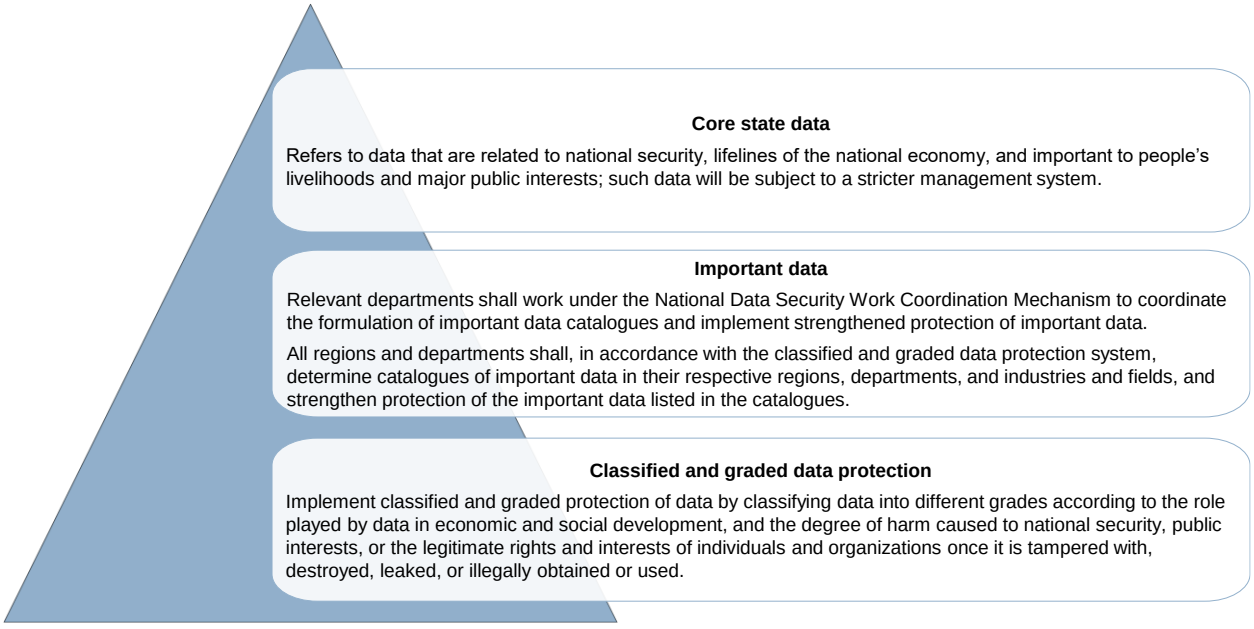
[1] Intern Zihuan XU has also contributed to the writing of this article.

- **Strengthens the management for provision of data to overseas institutions, raises maximum penalties.** The second reading draft for the first time stipulated penalties for companies that unlawfully provide domestic data to overseas law enforcement agencies and judicial authorities. The final draft at Article 48 significantly raises the maximum penalties for enterprise violations – if an enterprise provides domestic data to overseas law enforcement agencies and judicial authorities and causes serious consequences, it may be subject to a fine of up to RMB 5 million, and may be ordered to suspend its relevant business, close business for rectification, and may have its relevant business permits or business licenses revoked. Persons in charge and others directly responsible may be subject to fines of up to RMB 500,000.

- **Advances requirements to adapt to the needs of the elderly, ensuring the digital rights and interests of the elderly.** Since last year, the Ministry of Industry and Information Technology has successively issued plans requiring internet websites and mobile apps to better accommodate the needs of the elderly, including the *Special Action Plan for Aging People Adaptation and Barrier-free Transformation of Internet Applications*, and the *Circular on Further Implementing the Special Action Plan for Aging People Adaptation and Barrier-free Transformation of Internet Applications*. The final draft at Article 15 adapts to the aging demographic trend in Chinese society, stipulating for the first time under law to "take into account the needs of the elderly" and requiring providers of intelligent public services take into full consideration the needs of the elderly and the disabled and to ensure accessibility for these groups.

What are the grades of data protection?

The Data Security Law sets forth the concept of "core state data," based on the establishment of classified and graded data protection systems and the development of an important data catalogue, and stipulates a complete graded data protection system by grading data in terms of importance. Based upon the Data Security Law, data is to be graded and protected according to the following:



What important supporting systems does the Data Security Law establish?

The Data Security Law establishes basic systems for data protection, laying a foundation for data security management and protection as well as administration of data circulation and application in China. These basic systems mainly include:

- **Data transaction management system**: China will establish a data transaction management system, in order to standardize data transactions and facilitate development of the data transactions market (Article 19). Agencies that provide data trading intermediary services must request data providers to explain their data sources, verify the identities of both transaction parties, and maintain verification and transaction records (Article 33).
- **Important data protection system**: The Data Security Law puts forward special requirements for the processing of important data. These requirements include: processors of important data must specify the person(s) responsible for important data security and the relevant responsible department, and should undertake responsibilities for data security protection (Article 27); processors of important data must regularly conduct risk assessments of their data processing activities in accordance with the relevant provisions and submit risk assessment reports to the relevant competent authorities. Risk assessment reports are to specify the types and quantities of important data processed, the description of the data processing activities, and the data security risks possibly arising from the data processing activities and the countermeasures thereto (Article 30).
- **Data security risk management and control system**: China will establish centralized, unified, efficient, and authoritative data security risk assessment, reporting, information sharing, monitoring, and early warning mechanisms. China will also establish a national data security work coordination mechanism, under which the relevant departments will cooperate to strengthen the work of acquiring, analyzing, researching, judging, and early warning of data security risk information (Article 22).
- **Data security emergency response mechanism**: China will establish a data security emergency response mechanism. Under this mechanism, in the event of a data security incident, the relevant competent authorities will activate an emergency response plan in accordance with law and take appropriate emergency response measures to prevent the spread of damage, eliminate potential security risks, and promptly give warnings to the public (Article 23).
- **Data security review system**: China will establish a data security review system, under which data processing activities that affect or may affect national security will be subject to national security review. Decision made by the relevant departments on data security reviews in accordance with the law will be final. This means that the data security review system will exclude remedies such as administrative review and administrative litigation (Article 24).

What important systems govern cross-border data exchanges?

- **CII operators obligated to localize data**: According to the Data Security Law, the cross-border transfer of important data collected and generated in the operation of critical information infrastructure ("**CII**") within China is governed by the Cybersecurity Law (Article 31). According to Article 37 of the Cybersecurity Law, personal information and important data collected and generated in the operation of CII in China must be stored in China. If it is necessary to provide such data and information to overseas parties due to business needs, a security assessment must be conducted in accordance with the measures jointly formulated by the national cyberspace administration and relevant departments under the State Council, unless otherwise provided by laws and administrative regulations.

- **Cross-border data transfers by other data processors to be subject to administrative rules issued by the cyberspace administration and other authorities**: The cyberspace administration and relevant departments under the State Council will formulate administrative measures for the security review of cross-border transfers of important data collected and generated during the operation of facilities within China (Article 31). After the adoption of the Data Security Law, relevant supporting regulations will be successively formulated and improved so as to provide clear guidance to data operators.

- **Requests for domestic data by overseas law enforcement or judicial authorities**: Chinese competent authorities will process requests for domestic data from overseas law enforcement or judicial authorities in accordance with relevant laws and international treaties or agreements concluded or acceded to by China, or in accordance with the principles of equality and mutual benefit. No organization or individual within China may provide overseas law enforcement or judicial authorities with data stored in China without the approval of the Chinese competent authorities (Article 36).

- **Data export control system**: China will implement export controls over data that is categorized as a controlled item and is relevant to safeguarding national security and interests and to fulfilling international obligations (Article 25).

- **Anti-discrimination system**: Where any country or region takes, on discriminatory basis, prohibitive, restrictive, or other similar measures against China in terms of investment or trade related to data, data development, and technology utilization, etc., China may take reciprocal measures against such country or region according to actual circumstances (Article 26).

Important enterprise data security compliance obligations

Under the Data Security Law, enterprises have the following primary obligations in terms of data compliance and may be subject to the following punishments in the event of violation of relevant obligations.

Article	Obligations	Punishments for violation
Article 27 Data security protection obligations and important data security protection obligations	In order to conduct data processing activities, enterprises shall establish a sound data security management system, organize data security education and training, and take appropriate technical measures and other necessary measures in accordance with laws and regulations, so as to protect data security. When data processing activities are conducted through information networks such as the Internet, the above data security protection obligations shall also be followed, subject to compliance with requirements under the classified data protection system. Processors of important data shall specify the person(s) responsible for data security and the department in charge of data security protection.	**In general:** (1) Enterprises: ■ Corrections; ■ Warnings; ■ Fines of RMB 50,000-500,000. (2) Persons in charge and others directly responsible: ■ Fines of RMB 10,000-100,000. **In cases of refusal to make corrections or the violation results in serious consequences, such as a large data leakage:** (1) Enterprises: ■ Fines of RMB 500,000-2,000,000; and ■ Being ordered to suspend relevant business or to close for rectification; ■ Revocation of relevant business operating permits or business licenses. (2) Persons in charge and others directly responsible: ■ Fines of RMB 50,000-2,000,000.
Article 29 Risk monitoring and emergency response	Enterprises shall strengthen risk monitoring when conducting data processing activities and shall take remedial measures immediately upon discovery of data security defects, bugs, and other risks. In the event of a data security incident, enterprises shall take responsive measures in accordance with regulations, notify users, and report to the relevant competent authorities immediately in accordance with law.	
Article 30 Risk assessment and reporting of important data	Processors of important data shall, in accordance with regulations, conduct risk assessment of their data processing activities on a regular basis and submit risk assessment reports to the relevant competent authorities. A risk assessment report shall specify the types and quantities of important data processed, descriptions of data processing activities, data security risks possibly arising and the countermeasures therefor.	
Article 21 Core state data protection obligations	Core state data refers to data relating to national security, lifelines of the national economy, and that is important to people's livelihoods and major public interests, and such data shall be subject to a stricter management system.	■ Fines of RMB 2 million-10 million; ■ Being ordered to suspend relevant business or to close for rectification; ■ Revocation of relevant business operating permits or business licenses; ■ If a crime is constituted, criminal liability shall be investigated in accordance with the law.
Article 31 Restrictions on the cross-border	If an operator of critical information infrastructure intends to export important data collected and generated in the operation of critical information infrastructure within the territory of China, the Cybersecurity Law of the People's Republic of China	**In general:** (1) Enterprises:

Article	Obligations	Punishments for violation
provision of important data	shall apply. The export of other important data collected and generated within the territory of China shall subject to management of administrative regulations formulated by the cyberspace administration authority together with relevant departments under the State Council.	■ Corrections; ■ Warnings; ■ Fines ranging from RMB 100,000 to 1 million. (2) Persons in charge and others directly responsible: ■ Fines ranging from RMB 10,000 to 100,000. **In serious cases:** (1) Enterprises: ■ Fines ranging from RMB 1 million to 10 million; ■ Being ordered to suspend relevant business or to close for rectification; ■ Revocation of relevant business operating permits or business licenses. (2) Persons in charge and others directly responsible: ■ Fines ranging from RMB 100,000 to 1 million.
Article 33 Obligations of data transaction intermediary service providers for data source review and maintenance of transaction records	Agencies that provide data transaction intermediary services shall request data providers to explain data sources, verify the identities of both transaction parties, and maintain verification and transaction records.	(1) Enterprises: ■ Corrections; ■ Confiscation of illegal gains; ■ Imposition of fines ranging from one to ten times the illegal gains; if there are no illegal gains or the illegal gains are less than RMB 100,000, a fine ranging from RMB 100,000-1 million shall be imposed; ■ Being ordered to suspend relevant business or to close for rectification; ■ Revocation of relevant business operating permit or business license. (2) Persons in charge and others directly responsible: ■ Fines ranging from RMB 10,000 to 100,000.
Article 35 Cooperation in the provision of data	Where public security organs or national security organs need certain data to be provided for purposes of safeguarding national security or investigating crimes in accordance with the law, they shall, in accordance with the relevant provisions of the State, strictly go through approval procedures, and relevant organizations or individuals shall cooperate with the provision of data.	(1) Enterprises: ■ Corrections; ■ Warnings; ■ Fines ranging from RMB 50,000 to 500,000. (2) Persons in charge and others directly responsible:

Article	Obligations	Punishments for violation
		■ Fines ranging from RMB 10,000 to 100,000.
Article 36 No data may be provided to foreign judicial or law enforcement authorities without approval of the Chinese competent authorities	The Chinese competent authorities shall process requests for the provision of data from foreign judicial or law enforcement authorities in accordance with relevant laws and international treaties or agreements concluded or acceded to by China, or in accordance with the principles of equality and mutual benefit. No organization or individual within the territory of China may provide foreign judicial or law enforcement authorities with data stored within the territory of the China without the approval of the Chinese competent authorities.	**In general:** (1) Enterprises: ■ Warnings; ■ Fines ranging from RMB 100,000 to 1 million. (2) Persons in charge and others directly responsible: ■ Fines ranging from RMB 10,000 to 100,000. **In serious cases:** (1) Punishments for enterprises include: ■ Fines ranging from RMB 1 million to 5 million; ■ Being ordered to suspend relevant business or to close for rectification; ■ Revocation of relevant business permits or business licenses. (2) Persons in charge and others directly responsible: ■ Fines ranging from RMB 50,000 to 500,000.

Conclusion

The Data Security Law systematically echoes the requirements of pursuing a holistic approach to national security and comprehensively establishing a basic legal framework for data security governance. However, the Data Security Law mainly specifies the general principles and direction for data security governance and does not generally address detailed rules and obligations. Therefore, the regulatory authorities will need to further formulate supporting rules and regulations in order to assist with implementation of important systems under the law. It also remains to be further clarified the relationships among these systems, including the data security protection system, important data protection system, data security incident and emergency response system, anti-discrimination system, data export control system, data security review system, and other relevant systems and measures, particularly those under the Personal Information Protection Law, the Cybersecurity Law, the Anti-foreign Sanctions Law, the Export Control Law, the Foreign Investment Law, and the Measures for Examination of Cybersecurity, among others. We foresee these relevant supporting rules being soon released with the gradual implementation of the relevant systems. We recommend companies to closely watch legal developments in this area and prepare to make the changes necessary to come into compliance.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123
Email: kevin.duan@hankunlaw.com