

Data Security Law of the PRC

Dan Young Business Consultancy — www.danyoungcpa.com
Unofficial English translation prepared for reference only. The official Chinese text prevails.

Contents

Table of Contents	1
Chapter I — General Provisions	1
Chapter II — Data Security and Development	2
Chapter III — Data Security Protection Obligations	3
Chapter IV — Data Security Protection Obligations of State Organs	5
Chapter V — Legal Liability	5
Chapter VI — Supplementary Provisions	7

Adopted at the 29th Session of the Standing Committee of the 13th National People's Congress on June 10, 2021
Effective: September 1, 2021

Table of Contents

- Chapter I — General Provisions
- Chapter II — Data Security and Development
- Chapter III — Data Security Protection Obligations
- Chapter IV — Data Security Protection Obligations of State Organs
- Chapter V — Legal Liability
- Chapter VI — Supplementary Provisions

Chapter I — General Provisions

Article 1 — This Law is enacted for the purposes of regulating data processing activities, ensuring data security, promoting data development and utilization, protecting the lawful rights and interests of individuals and organizations, and safeguarding the sovereignty, security and development interests of the State.

Article 2 — This Law shall apply to data processing activities and security supervision and administration within the territory of the People's Republic of China. Where data processing activities outside the territory of the People's Republic of China harm the national security or public interest of the People's Republic of China, or the lawful rights and interests of citizens or organizations of the People's Republic of China, legal liability shall be pursued in accordance with the law.

Article 3 — For the purposes of this Law, "data" means any record of information by electronic or other means. "Data processing" includes the collection, storage, use, processing, transmission, provision and disclosure of data. "Data security" means the adoption of necessary measures to ensure that data is effectively protected and lawfully used, and to have the capacity to ensure a sustained state of security.

Article 4 — The State shall safeguard the security of data, protect the lawful rights and interests of citizens and organizations in relation to data, and promote the lawful, reasonable and effective use of data. The State shall promote the establishment of a data security governance system with data security policies, data security technologies, data security standards, data security management and data security services as the main elements.

Article 5 — The Central National Security Leadership Institution shall be responsible for the decision-making, deliberation and coordination of national data security work, researching, formulating and guiding the implementation of national data security strategies and relevant major guidelines and policies, and making overall plans and coordinating major matters and important work of national data security.

Article 6 — All regions and departments shall bear the primary responsibility for the security of the data collected and generated by them and the data in the data processing activities within their respective regions, departments and industries. The departments in charge of industry, telecommunications, transportation, finance, natural resources, public health, education, science and technology and other relevant competent departments shall undertake the data security supervision duties within their respective industries and fields. The public security organs and national security organs shall, in accordance with the provisions of this Law and relevant laws and administrative regulations, undertake data security supervision duties within their respective scope of duties. The national cyberspace administration authority shall, in accordance with the provisions of this Law and relevant laws and administrative regulations, be responsible for overall planning and coordination of network data security and relevant supervision and administration work.

Article 7 — The State shall protect the lawful collection and use of data by individuals and organizations, and protect the rights and interests of individuals and organizations in connection with data that are formed in accordance with the law. The State shall encourage innovation in the application of data and the rational use of data to promote the development of the digital economy. The State shall establish a sound data trading management system, cultivate a data trading market, and standardize data trading conduct.

Article 8 — Data processing activities shall comply with laws and regulations, respect social morality and ethics, observe business ethics, be honest and trustworthy, fulfill data security protection obligations, bear social responsibility, and shall not endanger national security or public interests, or damage the lawful rights and interests of individuals or organizations.

Article 9 — The State shall support the research and development of data security technologies, promote the protection of data security, and strengthen publicity and education on data security, enhance the awareness of data security protection in the whole society, and promote the formation of a favorable environment for jointly safeguarding data security and promoting development.

Article 10 — Relevant industry associations shall, in accordance with their articles of association, strengthen self-discipline and integrity building in accordance with the law, guide members in strengthening data security protection, improve the level of data security protection, and promote the healthy development of the industry.

Article 11 — The State shall actively carry out international exchanges and cooperation in the fields of data security governance, data development and utilization and other fields, and participate in the formulation of international rules and standards on data security.

Article 12 — Where any country or region adopts any discriminatory prohibitions, restrictions or other similar measures against the People's Republic of China in respect of investment or trade related to data or data development and utilization technologies, the People's Republic of China may, in light of the actual circumstances, adopt corresponding measures against such country or region.

Chapter II — Data Security and Development

Article 13 — The State shall make overall plans for development and security, adhere to promoting the development and utilization of data and the development of industries on the premise of ensuring data security, promote the construction of a data infrastructure, and encourage and support the innovative application of data in various industries and fields. The people's governments at or above the provincial level shall incorporate the development of the digital economy into their national economic and social development plans and formulate development plans for the digital economy as needed.

Article 14 — The State shall implement the big data strategy, promote the construction of data infrastructure, and encourage and support the innovative application of data in various industries and fields. The people's governments at or above the provincial level shall incorporate the development of the digital economy into their national economic and social development plans and formulate development plans for the digital economy as needed.

Article 15 — The State shall support the development and utilization of data to enhance the level of intelligent public services. When providing intelligent public services, the special needs of the elderly and the disabled shall be fully considered to prevent creating barriers to their daily lives.

Article 16 — The State shall support the research on data development and utilization technologies and data security technologies, encourage the commercial circulation and use of data in accordance with the law, and foster the development and growth of data-related industries.

Article 17 — The State shall promote the construction of a data standards system. The standardization administrative department under the State Council and the relevant departments under the State Council shall organize the formulation and timely revision of standards on data development and utilization technologies, products, services and security in accordance with their respective duties. The State shall support enterprises, social organizations, educational and scientific research institutions and other parties in participating in the formulation of data security standards.

Article 18 — The State shall promote the development of services such as data security testing and assessment, certification and other services, and support specialized institutions such as those providing data security testing and assessment and certification services in carrying out service activities in accordance with the law.

Article 19 — The State shall establish a sound data trading management system, standardize data trading conduct, and cultivate data trading markets.

Article 20 — The State shall support institutions of higher education, secondary vocational schools and scientific research institutions in establishing data development and utilization technologies and data security-related disciplines and specialties, and shall promote the combination of industry, academia and research to jointly cultivate professionals in data development and utilization technologies and data security.

Chapter III — Data Security Protection Obligations

Article 21 — The State shall establish a system for categorized and graded data protection, and implement categorized and graded protection of data based on the importance of data to economic and social development, and the degree of harm that may be caused to national security, public interests or the lawful rights and interests of individuals or organizations once data is tampered with, destroyed, divulged or illegally obtained or used. The State shall coordinate the relevant departments to formulate a catalog of important data and strengthen the protection of important data. The relevant departments shall, in accordance with their respective duties, specify their respective catalogs of important data and implement special protection of the important data included in the catalog.

Article 22 — The State shall establish a centralized, unified, efficient and authoritative data security risk assessment, reporting, information sharing, monitoring and early warning mechanism. The National Data

Security Coordination Mechanism shall coordinate the relevant departments in strengthening the acquisition, analysis, research and assessment of data security risk information.

Article 23 — The State shall establish a data security emergency response mechanism. Where a data security incident occurs, the relevant competent departments shall initiate the emergency response plan in accordance with the law, take corresponding emergency response measures, prevent the expansion of harm, eliminate security hazards, and release early warning information related to the public in a timely manner.

Article 24 — The State shall establish a data security review system and conduct national security reviews of data processing activities that affect or may affect national security. The decision on a security review made in accordance with the law shall be final.

Article 25 — The State shall implement export control on data that falls within the categories subject to export control in accordance with the law and perform international obligations.

Article 26 — Where any country or region adopts any discriminatory prohibitions, restrictions or other similar measures against the People's Republic of China in respect of investment in data-related industries, the People's Republic of China may, in light of the actual circumstances, adopt corresponding measures against such country or region.

Article 27 — Data processing activities shall be carried out in accordance with the provisions of laws and regulations. Important data processors shall designate a person in charge of data security and a management body, and implement the responsibility for data security protection. Data processing shall comply with the requirements of the categorized and graded data protection system, and corresponding technical and administrative measures shall be adopted in accordance with the law to ensure data security. Data processors shall organize data security education and training for employees.

Article 28 — Data processing activities and research and development of new data technologies shall be conducive to promoting economic and social development, enhancing the well-being of the people, and complying with social morality and ethics. Data processors shall use technical and other necessary measures to ensure data security and shall strengthen risk monitoring. Where data security defects, vulnerabilities and other risks are discovered, remedial measures shall be taken immediately; where a data security incident occurs, immediate measures shall be taken; and the matter shall be reported to the relevant competent authority and the user shall be notified in accordance with the provisions.

Article 29 — Data processors shall assess risks in data processing activities in accordance with the law, strengthen the acquisition, analysis, research and early warning of data security risk information, and promptly report to the relevant competent authority when discovering potential data security risks or defects.

Article 30 — Important data processors shall, in accordance with the provisions, regularly carry out risk assessments of 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 circumstances of data processing activities, the data security risks faced and the countermeasures, and other matters.

Article 31 — The security management of cross-border data transfer by critical information infrastructure operators under the Cybersecurity Law of the People's Republic of China and other data processors shall be governed by the provisions of the Cybersecurity Law of the People's Republic of China and other laws and administrative regulations. Where important data collected and generated by other data processors during their operations within the territory of the People's Republic of China is to be transferred abroad, the security management measures shall be formulated by the national cyberspace administration authority in conjunction with the relevant departments under the State Council.

Article 32 — No organization or individual shall illegally collect or acquire data, or instigate or induce others to illegally collect or acquire data. No organization or individual shall provide data collection, storage, trading, publishing, analysis or other services for illegal data collection and acquisition by others.

Article 33 — Organizations and individuals engaged in data trading intermediary services shall require the data provider to explain the source of the data, verify the identities of both parties to the transaction, and keep the verification and transaction records.

Article 34 — Where laws or administrative regulations provide that an administrative license is required for the provision of services relating to data processing, the service provider shall obtain such administrative license in accordance with the law.

Article 35 — Where a public security organ or national security organ needs to obtain data for the purpose of safeguarding national security or investigating crimes in accordance with the law, it shall go through strict approval procedures in accordance with the relevant provisions of the State and shall carry out data retrieval in accordance with the law. No relevant organization or individual shall refuse the same.

Article 36 — Competent authorities of the People's Republic of China shall, in accordance with relevant laws and international treaties or agreements concluded or acceded to by the People's Republic of China, or on the principle of equality and reciprocity, handle requests from foreign judicial or law enforcement authorities for the provision of data. Without the approval of the competent authorities of the People's Republic of China, no organization or individual within the territory of China shall provide data stored within the territory of the People's Republic of China to any foreign judicial or law enforcement authority.

Chapter IV — Data Security Protection Obligations of State Organs

Article 37 — State organs shall perform their data security protection obligations in accordance with the provisions of laws and administrative regulations. The state organs and their staff shall keep confidential the state secrets, trade secrets, personal privacy and personal information they come to know in the course of performing their duties, and shall not divulge or illegally provide the same to others.

Article 38 — State organs shall implement a security management system for data collection and use, and specify the purpose, scope, method and time limit for data collection and use in accordance with the law. The data provided by the data subject shall be obtained in a lawful and proper manner, shall be processed within the statutory scope of duties in accordance with the provisions of laws and administrative regulations and in accordance with the necessary conditions and procedures, and shall not be obtained beyond the scope of duties or the conditions and procedures.

Article 39 — State organs shall establish a sound data security management system, specify the person responsible for data security, and implement the responsibility for data security protection.

Article 40 — The entrustment of data processing by a state organ to another party shall be subject to strict approval procedures and the entrusted party shall be supervised to perform its corresponding data security protection obligations. The entrusted party shall perform its data security obligations in accordance with the provisions of laws and regulations and the agreement, and shall not retain, use, divulge or provide others with government affairs data without authorization.

Article 41 — State organs shall strengthen that government affairs data shall be made public and used in accordance with the law and in a secure and orderly manner, open government affairs data in accordance with the law, promote data sharing, and eliminate data barriers. The State shall formulate rules for the opening of government affairs data, establish a catalog of government affairs data open to the public, build an open platform for government affairs data, and promote the lawful, secure, orderly and free flow of government affairs data.

Chapter V — Legal Liability

Article 44 — Where a relevant competent authority discovers in performing its data security supervision duties that data processing activities involve a relatively large security risk, it may, in accordance with the prescribed competence and procedures, interview the relevant organization or individual and require them to take measures for rectification and to eliminate hidden dangers.

Article 45 — Where an organization or individual fails to perform its data security protection obligations as provided in Articles 27, 29 and 30 of this Law, the relevant competent authority shall order rectification and give a warning, and may concurrently impose a fine of not more than RMB 50,000; a fine of not less than RMB 10,000 and not more than RMB 100,000 shall be imposed on the directly responsible person in charge and other directly responsible personnel. Where rectification is refused or a relatively large data security risk or other serious consequences are caused, a fine of not less than RMB 50,000 and not more than RMB 500,000 shall be imposed, and a fine of not less than RMB 50,000 and not more than RMB 200,000 shall be imposed on the directly responsible person in charge and other directly responsible personnel.

Article 46 — Where the provisions of Article 31 of this Law are violated by providing important data outside the territory of China, the relevant competent authority shall order rectification, give a warning, and may concurrently impose a fine of not less than RMB 100,000 and not more than RMB 1,000,000; a fine of not less than RMB 10,000 and not more than RMB 100,000 shall be imposed on the directly responsible person in charge and other directly responsible personnel. Where the circumstances are serious, a fine of not less than RMB 1,000,000 and not more than RMB 10,000,000 shall be imposed, and may concurrently order the suspension of relevant business, cessation of business operations for rectification, or revocation of relevant business permits or business licenses; a fine of not less than RMB 100,000 and not more than RMB 1,000,000 shall be imposed on the directly responsible person in charge and other directly responsible personnel.

Article 47 — Where an organization or individual engaged in data trading intermediary services fails to require the data provider to explain the source of the data, verify the identities of both parties to the transaction, or keep the verification and transaction records, the relevant competent authority shall order rectification, give a warning, confiscate the illegal gains, and impose a fine of not less than one time but not more than ten times the illegal gains; where there are no illegal gains, a fine of not more than RMB 1,000,000 shall be imposed; a fine of not less than RMB 10,000 and not more than RMB 100,000 shall be imposed on the directly responsible person in charge and other directly responsible personnel.

Article 48 — Where a violation of the provisions of Article 35 of this Law is committed by refusing or obstructing data retrieval in accordance with the law, the relevant competent authority shall order rectification, give a warning, and impose a fine of not more than RMB 50,000; a fine of not less than RMB 5,000 and not more than RMB 50,000 shall be imposed on the directly responsible person in charge and other directly responsible personnel.

Article 49 — Where a state organ fails to perform its data security protection obligations as provided in this Law, the directly responsible person in charge and other directly responsible personnel shall be subject to sanctions in accordance with the law.

Article 50 — Where a department performing data security supervision duties abuses its powers, neglects its duties, or engages in malpractices for personal gain in performing its data security supervision duties, the directly responsible person in charge and other directly responsible personnel shall be subject to sanctions in accordance with the law.

Article 52 — Where a violation of the provisions of this Law causes damage to others, civil liability shall be borne in accordance with the law. Where a violation of the provisions of this Law constitutes a violation of public security administration, public security administration penalties shall be imposed in accordance with the law; where a crime is constituted, criminal liability shall be pursued in accordance with the law.

Chapter VI — Supplementary Provisions

Article 53 — Where data processing activities involving state secrets are conducted, the provisions of the Law of the People's Republic of China on Guarding State Secrets and other laws and administrative regulations shall apply. Where personal information is processed in the form of data, the provisions of the Personal Information Protection Law of the People's Republic of China shall apply in addition to the provisions of this Law.

Article 54 — The security management of data used for military purposes shall be separately prescribed by the Central Military Commission in accordance with the provisions of this Law.

Article 55 — This Law shall come into force on September 1, 2021.

Disclaimer: This translation is provided for informational purposes only and is not an official translation. While every effort has been made to ensure accuracy and completeness, this translation may contain errors or omissions. Readers should consult the official Chinese text for legal purposes. Dan Young Business Consultancy makes no representations or warranties, express or implied, regarding the accuracy, completeness or fitness for a particular purpose of this translation and shall not be liable for any loss or damage arising from reliance on this translation.