PRC Data Security Law

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 Protection System 3

Chapter III — Obligations of Data Security Protection 4

Chapter IV — Security and Openness of Government Data 5

Chapter V — Development of Data Security Industry and Services 6

Chapter VI — Legal Liability 7

Chapter VII — Supplementary Provisions 8

Adopted at the 29th Session of the Standing Committee of the Thirteenth National People's Congress on June 10, 2021

Effective: September 1, 2021

Table of Contents

- Chapter I — General Provisions
- Chapter II — Data Security and Protection System
- Chapter III — Obligations of Data Security Protection
- Chapter IV — Security and Openness of Government Data
- Chapter V — Development of Data Security Industry and Services
- Chapter VI — Legal Liability
- Chapter VII — Supplementary Provisions

Chapter I — General Provisions

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

Article 2 — This Law shall apply to the conduct of data processing activities and the security supervision and administration of such activities within the territory of the People's Republic of China. Where data processing activities conducted outside the territory of the People's Republic of China damage the national security, public interest, 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.

Source: https://www.danyoungcpa.com/data-security-law-peoples-republic-of-china-2021-en/

Article 3 — For the purposes of this Law, "data" means any record of information in electronic or non-electronic form. "Data processing" includes the collection, storage, use, processing, transmission, provision, disclosure, and deletion of data. "Data security" means taking necessary measures to ensure that data is effectively protected and lawfully utilized, and has the capacity to maintain a state of continuous security.

Article 4 — The state shall adhere to the overall concept of national security, implement the big data strategy, promote the construction of data infrastructure, and encourage and support the rational and effective use of data to ensure the security of data in accordance with the law, promote the development of the digital economy, and improve the modernization level of the public service system. The state shall establish a sound data security governance system and enhance the data security protection capability.

Article 5 — The central leading institution for national security shall be responsible for the decision-making, deliberation, and coordination of national data security work, research, formulation, and guidance of the implementation of national data security strategies and relevant major guidelines and policies, overall planning and coordination of major national data security matters and work, and establishment of a national data security work coordination mechanism.

Article 6 — All regions and departments shall assume the main responsibility for the security of the data generated by them and in their respective regions, departments, and industries, as well as the data collected and generated by various data processors in their respective industries and fields. The relevant departments in charge of industry, telecommunications, transport, finance, natural resources, health, education, science and technology, and other competent authorities shall assume the responsibility for data security supervision in their respective industries and fields. Public security authorities and national security authorities shall, within the scope of their respective functions and duties, assume the responsibility for data security supervision. The national cyberspace administration authority shall, in accordance with the provisions of this Law and relevant laws and administrative regulations, be responsible for the overall planning and coordination of network data security and the related supervision and administration.

Article 7 — The state shall protect the rights and interests of individuals and organizations relating to data, encourage the reasonable and effective use of data in accordance with the law, ensure the orderly and free flow of data in accordance with the law, and promote the development of the digital economy with data as a key factor.

Article 8 — When conducting data processing activities, data processors shall comply with laws and regulations, respect social morality and ethics, observe business ethics and professional ethics, be honest and trustworthy, fulfill their data security protection obligations, assume social responsibility, and shall not endanger national security or the public interest, nor shall they damage the lawful rights and interests of individuals or organizations.

Article 9 — The state shall support the publicity and education on data security, raise the awareness of data security protection of the whole society, and promote the formation of a good environment for the whole society to jointly safeguard data security and promote development.

Article 10 — Relevant industry organizations shall, in accordance with their articles of association, formulate data security codes of conduct and group standards in accordance with the law, strengthen industry self-discipline, guide their members to strengthen data security protection, raise the level of data security protection, and promote the sound development of the industry.

Article 11 — The state shall actively carry out international exchanges and cooperation in data governance, the development and utilization of data, and other fields, participate in the formulation of international rules and standards for data security, and promote the safe and free flow of data across borders.

Source: https://www.danyoungcpa.com/data-security-law-peoples-republic-of-china-2021-en/

Article 12 — Every individual and organization shall have the right to lodge a complaint or report to the relevant competent authority for acts that violate the provisions of this Law. The authority receiving the complaint or report shall handle it in a timely manner in accordance with the law. The relevant competent authority shall keep confidential the information on the complainant or reporter and protect the lawful rights and interests of the complainant or reporter.

Chapter II — Data Security and Protection System

Article 13 — The state shall establish a data classification and hierarchical protection system, and shall, on the basis of the importance of the data in economic and social development and the degree of harm to national security, the public interest, or the lawful rights and interests of individuals and organizations that may be caused if the data is tampered with, destroyed, leaked, illegally obtained, or illegally used, implement classified and hierarchical protection of data.

Article 14 — The state shall establish a data security risk assessment, reporting, information sharing, monitoring, and early warning mechanism. The national data security work coordination mechanism shall coordinate the relevant authorities in strengthening the collection, analysis, research, and assessment of data security risk information. The relevant authorities shall, in accordance with the provisions of the state, promptly report to the national data security work coordination mechanism on the data security risks discovered by them in the course of performing their functions and duties.

Article 15 — The state shall establish a data security emergency response mechanism. The relevant authorities shall, in accordance with the provisions of the state, formulate emergency response plans for data security incidents, and in the event of a data security incident, the relevant competent authorities shall initiate the emergency response plan in accordance with the law, adopt corresponding emergency response measures, eliminate the security risks, prevent the expansion of the harm, and promptly release warning information related to the public.

Article 16 — The state shall establish a national security review system for data processing activities that affect or may affect national security. The security review decisions made in accordance with the law shall be final.

Article 17 — The state shall, on the basis of the principle of equality and reciprocity, carry out export control of data that is subject to export control such as controlled items under the Export Control Law of the People's Republic of China and data related to the safeguarding of national security and interests and the fulfillment of international obligations.

Article 18 — Where a country or region adopts discriminatory prohibitions, restrictions, or other similar measures against the People's Republic of China in the areas of investment and trade related to data or the development and utilization of data and technology, the People's Republic of China may, on the basis of the actual circumstances, adopt countermeasures against such country or region.

Article 19 — The state shall promote the openness, sharing, and utilization of public data such as government data in accordance with the law, and promote the development of the digital economy. The state shall formulate policies and measures to support the cultivation of the data factor market, encourage value-added development and utilization of data, and support the lawful use of data by individuals and organizations for innovation and business development.

Article 20 — The state shall support education and scientific research institutions and enterprises in carrying out research on data security technologies and products, promoting the innovation of data security technologies, and cultivating and developing data security products and industrial systems. The state shall support the establishment of specialized data security technology assessment institutions and promote the development of data security testing, assessment, certification, and other services. The state shall support the relevant departments, industry organizations, enterprises, education and scientific research institutions,

Source: https://www.danyoungcpa.com/data-security-law-peoples-republic-of-china-2021-en/

and relevant professional institutions in carrying out data security education and training, adopt various methods to cultivate specialized data security talents, and promote the exchange of data security talents.

Chapter III — Obligations of Data Security Protection

Article 21 — The state shall, on the basis of the importance of the data in economic and social development and the degree of harm to national security, the public interest, or the lawful rights and interests of individuals and organizations that may be caused if the data is tampered with, destroyed, leaked, illegally obtained, or illegally used, implement classified and hierarchical protection of data. The national data security work coordination mechanism shall coordinate the relevant authorities in formulating the catalogue of important data and strengthening the protection of important data. Data related to national security, the lifeline of the national economy, important aspects of people's livelihood, major public interests, and other core state data shall be subject to a stricter management system. All regions and departments shall, in accordance with the data classification and hierarchical protection system, determine the specific catalogues of important data for their respective regions, departments, and relevant industries and fields, and give priority to the protection of the data listed in the catalogues.

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 work coordination mechanism shall coordinate the relevant authorities in strengthening the collection, 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 authorities shall initiate the emergency response plan in accordance with the law, adopt corresponding emergency response measures to prevent the expansion of the harm, eliminate the security risks, and promptly release warning information related to the public.

Article 24 — The state shall establish a national security review system for data processing activities that affect or may affect national security. Security review shall be conducted in accordance with the law for data processing activities that affect or may affect national security. The security review decisions made in accordance with the law shall be final.

Article 25 — When conducting data processing activities, data processors shall, in accordance with the provisions of laws and regulations and the mandatory requirements of national standards, establish and improve the data security management system for the entire data processing workflow, organize and carry out data security education and training, adopt corresponding technical measures and other necessary measures to ensure data security. Those who use the internet and other information networks to conduct data processing activities shall fulfill the data security protection obligations on the basis of the cybersecurity protection tiered system. Important data processors shall specify the persons responsible for data security and the management institution, and implement the responsibility for data security protection.

Article 26 — Where any data processing activity is carried out, the purpose of data processing shall be legitimate and necessary, the processing shall be conducted in a proper manner, and the processing shall be limited to the minimum scope necessary for the realization of the purpose, and shall not be excessively collected or used.

Article 27 — When conducting data processing activities, data processors shall, in accordance with the provisions of laws and regulations, adopt corresponding technical measures and other necessary measures to ensure data security. Where any risk such as a data security defect or vulnerability is discovered, remedial measures shall be taken immediately; where a data security incident occurs, remedial measures shall be taken immediately in accordance with the provisions, the users shall be notified, and the matter shall be reported to the relevant competent authority.

Article 28 — When conducting data processing activities and research and development of new data technologies, the data processors shall be conducive to promoting economic and social development, improving the well-being of the people, and complying with social morality and ethics. Data processing activities shall not endanger national security or the public interest, nor shall they damage the lawful rights and interests of individuals or organizations.

Article 29 — Data processors shall strengthen risk monitoring, and when discovering data security defects, vulnerabilities, or other risks, they shall immediately adopt remedial measures; where a data security incident occurs, they shall immediately adopt remedial measures, notify users in a timely manner, and report the same to the relevant competent authority in accordance with the provisions.

Article 30 — Important data processors shall, in accordance with the provisions, periodically carry out risk assessments of their data processing activities and submit risk assessment reports to the relevant competent authority. The risk assessment reports shall include information on the types and quantities of important data processed, the situation of conducting data processing activities, the data security risks discovered, and the countermeasures adopted.

Article 31 — The security management of the cross-border transfer of data by operators of critical information infrastructure and important data processors shall be governed by the provisions of the Cybersecurity Law of the People's Republic of China. The measures for the security management of the cross-border transfer of important data by other data processors shall be formulated by the national cyberspace administration authority in conjunction with the relevant authorities under the State Council.

Article 32 — No organization or individual may collect data by stealing or other illegal means. Where data is collected or obtained by other means, data shall not be stolen or obtained by illegal means from others. No organization or individual shall provide data collection services or other related services for others' illegal collection or acquisition of data.

Article 33 — Data trading intermediary service institutions shall require the data providers to explain the sources of the data, verify the identities of both parties to the transaction, and retain records of the verification and the transaction. Data trading intermediary service institutions shall require the data providers to explain the sources of the data and shall retain records of the verification, review, and transaction.

Article 34 — Where laws or administrative regulations provide that the provision of data processing-related services shall be subject to administrative licensing, the service providers shall obtain the license in accordance with the law.

Article 35 — Public security authorities and national security authorities shall, in accordance with the law, obtain data needed for safeguarding national security or investigating crimes; they shall, in accordance with the relevant provisions of the state, go through strict approval procedures and carry out the data acquisition in accordance with the law. Relevant organizations and individuals shall provide cooperation.

Article 36 — The competent authorities of the People's Republic of China shall, in accordance with relevant laws and international treaties and agreements concluded or acceded to by the People's Republic of China, or on the basis of the principle of equality and reciprocity, handle the requests of foreign judicial authorities and 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 the People's Republic of China may provide data stored within the territory of the People's Republic of China to foreign judicial authorities or law enforcement authorities.

Chapter IV — Security and Openness of Government Data

Article 37 — The state shall make great efforts to promote the development and utilization of e-government, improve the scientific nature, accuracy, and effectiveness of government decision-making, and enhance the

Source: https://www.danyoungcpa.com/data-security-law-peoples-republic-of-china-2021-en/

modernization level of the public service system. State organs shall, in accordance with the provisions of laws and administrative regulations, establish and improve the data security management system, implement the data security protection responsibility, and ensure the security of government data.

Article 38 — State organs shall collect and use data within the scope of their statutory functions and duties in accordance with the conditions and procedures prescribed by laws and administrative regulations, and shall not collect or use data beyond the scope and limits of their statutory functions and duties. Where state organs entrust others to construct or maintain e-government systems, or to store or process government data, they shall go through strict approval procedures, and shall supervise the entrusted party's fulfillment of the data security protection obligations. The entrusted party shall fulfill its data security protection obligations in accordance with the provisions of laws, regulations, and the contractual agreement, and shall not retain, use, disclose, or provide government data to others without authorization.

Article 39 — State organs shall establish and improve the data security management system, and implement the data security protection responsibility for data security in accordance with the provisions. The persons responsible for data security shall be designated, and the data security protection responsibilities of each person shall be defined.

Article 40 — State organs shall keep confidential the personal privacy, personal information, trade secrets, and confidential business information they come to know in the performance of their functions and duties, and shall not disclose or illegally provide the same to others.

Article 41 — State organs shall, in accordance with the principles of fairness, impartiality, and openness, open government data to the public in a timely and accurate manner in accordance with the provisions of laws and administrative regulations, except for data that shall not be disclosed in accordance with the law. The state shall formulate policies and measures to encourage and support the opening of government data, promote the opening, sharing, and utilization of government data, and promote the development of the digital economy.

Article 42 — The state shall formulate catalogues for the opening of government data and establish a unified, standardized, interconnected, secure, and controllable mechanism for the opening of government data. State organs shall, in accordance with the provisions, promptly and accurately open government data. The state shall support the lawful use of public data by individuals and organizations for innovation and business development.

Article 43 — Where laws or regulations provide that the opening of government data is subject to security review, the review shall be conducted in accordance with the provisions.

Chapter V — Development of Data Security Industry and Services

Article 44 — The state shall implement the big data strategy, promote the construction of data infrastructure, encourage and support the innovation and application of data security technologies and data development and utilization technologies, promote the cultivation and development of the data factor market, and promote the development of the digital economy with data as a key factor.

Article 45 — The state shall support education and scientific research institutions and enterprises in carrying out research on data security technologies and related products, and promote the innovation of data security technologies. The state shall support the development of data security testing, assessment, certification, and other services, and support specialized institutions in providing such services in accordance with the law. The state shall support the relevant departments, industry organizations, enterprises, education and scientific research institutions, and relevant professional institutions in carrying out data security education, training, and publicity, and in cultivating specialized data security talents.

Source: https://www.danyoungcpa.com/data-security-law-peoples-republic-of-china-2021-en/

Article 46 — The state shall support data development, utilization, and data security technologies research, encourage value-added development and utilization of data, promote the construction of data factor market, and cultivate data trading markets and data factor market systems.

Article 47 — The state shall, on the basis of the principle of equality and reciprocity, carry out international exchanges and cooperation in the field of data security and development, promote the safe and free flow of data across borders, and promote the development and prosperity of the global digital economy.

Chapter VI — Legal Liability

Article 48 — Where any organization or individual violates the provisions of Article 12 of this Law by retaliating against a complainant or reporter, the relevant competent authority shall order it to make corrections and give it a warning; where it refuses to make corrections or the circumstances are serious, sanctions shall be imposed on the directly responsible person in charge and other directly responsible persons in accordance with the law.

Article 49 — Where a state organ fails to fulfill its data security protection obligations as provided for in this Law, the authority at a higher level or the relevant competent authority shall order it to make corrections; sanctions shall be imposed on the directly responsible person in charge and other directly responsible persons in accordance with the law. Where any staff member of a state organ responsible for the supervision and administration of data security neglects his or her duties, engages in malpractice for personal gain, or abuses his or her power, he or she shall be sanctioned in accordance with the law.

Article 50 — Where a state organ performs its data security regulatory functions and duties without fulfilling its obligations under this Law, the authority at a higher level or the relevant competent authority shall order it to make corrections; sanctions shall be imposed on the directly responsible person in charge and other directly responsible persons in accordance with the law.

Article 51 — Where a data processor that steals data or obtains data by other illegal means, or conducts data processing activities that endanger national security or the public interest, or damages the lawful rights and interests of individuals or organizations, the relevant competent authority shall order it to make corrections, give it a warning, and may also impose a fine of not more than RMB 50,000 on the entity or a fine of not more than RMB 10,000 on the directly responsible person; where the circumstances are serious, a fine of not less than RMB 50,000 but not more than RMB 500,000 may be imposed on the entity, and a fine of not less than RMB 10,000 but not more than RMB 100,000 may be imposed on the directly responsible person in charge. Where the violation is relatively serious, the relevant competent authority may order it to suspend the relevant business, suspend business for rectification, close down the website, or revoke the relevant business permit or business license; and a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed on the directly responsible person in charge and other directly responsible persons.

Article 52 — Where a data processor violates the provisions of this Law by failing to fulfill its data security protection obligations, the relevant competent authority shall order it to make corrections and give it a warning, and may also impose a fine of not more than RMB 50,000; where it refuses to make corrections, which causes harm such as a large-scale data leakage, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed, and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible person in charge; where the circumstances are serious, the relevant competent authority may order it to suspend the relevant business, suspend business for rectification, close down the website, or revoke the relevant business permit or business license, and shall impose a fine of not less than RMB 50,000 but not more than RMB 500,000 on the directly responsible person in charge and other directly responsible persons.

Source: https://www.danyoungcpa.com/data-security-law-peoples-republic-of-china-2021-en/

Article 53 — Where a data processor that is an important data processor fails to conduct a risk assessment in accordance with the provisions of this Law and submit a risk assessment report, the relevant competent authority shall order it to make corrections and give it a warning, and may also impose a fine of not less than RMB 50,000 but not more than RMB 200,000; where it refuses to make corrections, a fine of not less than RMB 100,000 but not more than RMB 500,000 shall be imposed, and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible person in charge.

Article 54 — Where a data processor violates the provisions of Article 36 of this Law by providing data to foreign judicial authorities or law enforcement authorities without the approval of the competent authorities of the People's Republic of China, the relevant competent authority shall give it a warning and may also impose a fine of not less than RMB 50,000 but not more than RMB 500,000, and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible person in charge; where serious consequences are caused, a fine of not less than RMB 100,000 but not more than RMB 5,000,000 shall be imposed, and the relevant competent authority may order it to suspend the relevant business, suspend business for rectification, close down the website, or revoke the relevant business permit or business license; and a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed on the directly responsible person in charge and other directly responsible persons.

Article 55 — Where any act violates the provisions of this Law and constitutes a crime, criminal liability shall be pursued in accordance with the law. Where any act violates the provisions of this Law and causes damage to others, civil liability shall be borne in accordance with the law.

Chapter VII — Supplementary Provisions

Article 56 — This Law shall come into force as of September 1, 2021.

Disclaimer: This English translation is provided for reference purposes only. While every effort has been made to ensure accuracy, the official Chinese text shall prevail in all legal matters. Dan Young Business Consultancy makes no warranty, express or implied, as to the accuracy, completeness, or fitness for any particular purpose of this translation. Users should consult qualified legal professionals for advice on specific data security compliance matters. The translation reflects the law as adopted on June 10, 2021, and may not incorporate subsequent amendments or interpretations.