Data Security Law of the People’s Republic of China

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 Systems 2

Chapter IV — Data Security Protection Obligations 3

Chapter V — Security and Protection of Government Data 3

Chapter VI — Legal Liability 3

Chapter VII — Supplementary Provisions 4

Adopted June 10, 2021; Effective September 1, 2021

Effective: September 1, 2021

Table of Contents

- Chapter I — General Provisions
- Chapter II — Data Security and Development
- Chapter III — Data Security Systems
- Chapter IV — Data Security Protection Obligations
- Chapter V — Security and Protection of Government Data
- 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 data development and utilization, protecting the lawful rights and interests of individuals and organizations, and safeguarding national sovereignty, security, and development interests.

Article 2. This Law applies to data processing activities and security supervision and administration 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 harm national security, the public interest, or the lawful rights and interests of citizens or organizations of the People’s Republic of China, legal liability shall be investigated in accordance with law.

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 adopting necessary measures to ensure that data is effectively protected and lawfully utilized, and to possess the capability to maintain a continuous state of security.

Article 4. The State shall uphold a holistic approach to national security, establish a sound data security governance system, and enhance data security protection capabilities.

Article 5. The central national security leadership body shall be responsible for the decision-making, deliberation, and coordination of national data security work; it shall research, formulate, and guide the implementation of national data security strategies and relevant major guidelines and policies.

Article 6. Each region and each department shall bear primary responsibility for the data security of data collected and generated by their own regions, departments, entities, and individuals within their respective work scopes.

Article 7. The State shall protect the rights and interests of individuals and organizations related to data, encourage the lawful, reasonable, and effective use of data, safeguard the free flow of data in accordance with law, and promote the development of the digital economy with data as a key factor of production.

Chapter II — Data Security and Development

Article 8. The State shall implement a big data strategy, promote the construction of data infrastructure, and encourage and support the innovative application of data in various industries and fields. 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.

Article 9. The State shall support the development and utilization of data to enhance the level of intelligent public services. When providing intelligent public services, the needs of the elderly and persons with disabilities shall be taken into consideration to avoid creating barriers to their daily lives.

Article 10. The State shall support the lawful and compliant circulation and use of data, promote the establishment of a data property rights system, and regulate data trading markets.

Chapter III — Data Security Systems

Article 11. The State shall establish a system of categorized and graded data protection. Based on the importance of data to national security, economic development, and the public interest, as well as the degree of harm that would be caused to national security, the public interest, or the lawful rights and interests of individuals or organizations in the event of tampering, destruction, leakage, or illegal acquisition or use, data shall be classified and graded for protection. The specific catalogues for important data shall be formulated by the relevant regional and sectoral authorities.

Article 12. The State shall establish a centralized, unified, highly efficient, and authoritative data security risk assessment, reporting, information sharing, monitoring, and early warning mechanism. The national data security coordination mechanism shall coordinate relevant departments to strengthen data security intelligence and information gathering, analysis, and assessment.

Article 13. The State shall establish a data security emergency response mechanism. Relevant departments shall initiate emergency response plans in accordance with law upon occurrence of data security incidents, take corresponding emergency response measures, and eliminate security hazards.

Article 14. The State shall establish a data security review system. Data processing activities that affect or may affect national security shall undergo national security review organized by the national data security coordination mechanism in accordance with law. Security review decisions made in accordance with law shall be final.

Source: https://www.danyoungcpa.com/data-security-law-prc-2021-english-translation/

Article 15. The State shall implement export controls over data that are controlled items and those related to safeguarding national security and interests and fulfilling international obligations.

Article 16. Where any country or region adopts discriminatory prohibitions, restrictions, or other similar measures against the People's Republic of China in respect of investment or trade related to data and data development and utilization technology, the People's Republic of China may, based on actual circumstances, adopt proportionate countermeasures against that country or region.

Chapter IV — Data Security Protection Obligations

Article 17. Entities and individuals conducting data processing activities shall establish and improve data security management systems throughout the entire data lifecycle, organize and carry out data security education and training, and adopt corresponding technical and other necessary measures to ensure data security.

Article 18. Where data processing is conducted using the internet or other information networks, the data processor shall fulfill the data security protection obligations specified in this Law on the basis of the graded cybersecurity protection system.

Article 19. Processors of important data shall specify the persons responsible for data security and establish data security management bodies to perform data security protection responsibilities.

Article 20. Processors of important data shall conduct regular risk assessments of their data processing activities and submit risk assessment reports to the relevant competent authorities. Risk assessment reports shall include: (1) the categories, quantity, and scope of important data processed; (2) the circumstances and security risks associated with the important data processing activities; (3) the state of implementation of data security protection measures; and (4) other matters requiring explanation.

Article 21. The State shall establish a data security review system for the cross-border transfer of important data. Processors of important data that need to provide important data abroad shall undergo a data security review organized by the national cyberspace administration authority in conjunction with relevant departments under the State Council.

Article 22. No entity or individual may collect or acquire data by illegal means such as theft, fraud, or coercion. No entity or individual may provide data abroad without the approval of the competent authorities where such provision is subject to approval under laws or administrative regulations.

Article 23. The State shall provide equal protection to the lawful data-related rights and interests of domestic and foreign-invested enterprises. Data processors shall implement a system for receiving and handling complaints and reports regarding data security.

Chapter V — Security and Protection of Government Data

Article 24. The State shall promote the openness of government data and establish a government data catalogue that distinguishes between data that is open and data that is not open, with the principle of openness as the norm and non-openness as the exception.

Article 25. State organs shall fulfill their data security protection obligations and must not disclose or illegally provide government data to others without authorization. State organs shall take necessary measures to ensure the security of government data processed on their behalf by third parties.

Chapter VI — Legal Liability

Article 26. Where data processing activities are conducted in violation of this Law without causing harm, the competent authority may order correction and issue a warning; where serious consequences arise, a fine of not less than CNY 50,000 and not more than CNY 500,000 may be imposed on the entity, and a fine of not

Source: https://www.danyoungcpa.com/data-security-law-prc-2021-english-translation/

less than CNY 10,000 and not more than CNY 100,000 may be imposed on the directly responsible person in charge.

Article 27. Where data processing activities violate this Law and cause substantial harm to national security, the public interest, or the lawful rights and interests of individuals or organizations, the competent authority may impose a fine of not less than CNY 500,000 and not more than CNY 2 million on the entity, and may order suspension of relevant business, cessation of business for rectification, revocation of relevant business permits, or revocation of business licenses; a fine of not less than CNY 50,000 and not more than CNY 200,000 may be imposed on the directly responsible persons.

Article 28. Where data is provided abroad in violation of the provisions of this Law, the relevant competent authorities may order correction and impose a fine of not less than CNY 100,000 and not more than CNY 1 million on the entity; where the circumstances are serious, a fine of not less than CNY 1 million and not more than CNY 10 million may be imposed, and business permits or business licenses may be revoked.

Chapter VII — Supplementary Provisions

Article 29. This Law shall take effect as of September 1, 2021.

Source: https://www.danyoungcpa.com/data-security-law-prc-2021-english-translation/