Data Security Law of the People's Republic of China

Table of Contents

Chapter I: General Provisions

Article 1: This Law is formulated in order to standardize data handling activities, ensure data security, promote data development and use,[1] protect the lawful rights and interests of individuals and organizations, and safeguard national sovereignty, security, and development interests.

Article 2: This Law applies to data handling activities and their security regulation within the mainland territory of the People's Republic of China (PRC).[2]

When data handling activities outside the mainland territory of the PRC harm the national security, the public interest, or the lawful rights and interests of citizens or organizations of the PRC, legal liability is to be pursued according to the law.

Article 3: As used in this Law, "data" refers to any information record in electronic or other form.

"Data handling" includes the collection, storage, use, processing, transmission, provision, disclosure, etc., of data.[3]

"Data security" refers to ensuring data is in a state of effective protection and lawful use through adopting necessary measures, and to possessing the capacity to ensure a persistent state of security.

Article 4: In safeguarding data security, the overall national security concept shall be upheld, data security governance systems established and completed, and data security protection capacities increased.

Article 5: The central leading institution for national security is responsible for: policy-making, deliberation, and coordination in national data security work; researching, formulating, and guiding the implementation of national data security strategy and related

major directives and policies; comprehensively coordinating major matters and important work in national data security; and establishing a national data security work coordination mechanism.[4]

Article 6: Each locality and department is responsible for data collected and created, as well as data security, in the respective locality or department's work.

Departments in charge of such sectors as industry, telecommunications, transportation, finance, natural resources, hygiene and health, education, and technology are to undertake data security regulatory duties in their respective field.

Public security authorities and national security authorities, etc., are to undertake data security regulatory duties within the scope of their respective duties, in accordance with the provisions of this Law and relevant laws and administrative regulations.

The national cybersecurity and informatization department[5] is responsible for the comprehensive coordination of network data security and related regulatory work, in accordance with the provisions of this Law and relevant laws and administrative regulations.

Article 7: The State is to protect the data-related rights and interests of individuals and organizations; encourage lawful, reasonable, and effective data use; ensure the lawful and orderly free flow of data; and promote the development of the digital economy with data as a key factor.[6]

Article 8: In the conduct of data handling activities, laws and regulations shall be followed, social public morals and ethics respected, business ethics and professional ethics observed, honesty and trustworthiness [practiced], data security protection obligations fulfilled, and social responsibility assumed; national security and the public interest must not be endangered; and the lawful rights and interests of individuals and organizations must not be harmed.

Article 9: The State is to support the launch of data security knowledge propagation and popularization; raising the entire society's consciousness and level of data security protection; pushing relevant departments, industry organizations, scientific research institutions, enterprises, individuals, etc., to jointly participate in data security protection work; and forming a positive environment for the entire society to jointly safeguard data security and promote development.

Article 10: Relevant industry organizations, in accordance with their charters, are to formulate data security standards of conduct and group standards, strengthen industry self-discipline, guide members to strengthen data security protection, raise data security protection levels, and promote the healthy development of the industry.

Article 11: The State is to actively engage in international exchanges and cooperation in fields such as data security governance and data development and use, participating in the formulation of international rules and standards related to data security, and promoting the secure and free flow of data across borders.

Article 12: Any organization or individual has the right to file a complaint about or report acts violating the provisions of this Law to the relevant department in charge. Departments receiving complaints or reports shall handle them promptly and in accordance with law.

Relevant departments shall preserve the confidentiality of information related to persons filing complaints or reports and protect the lawful rights and interests of persons filing complaints or reports.

Chapter II: Data Security and Development

Article 13: The State is to coordinate overall development and security, persist in the promotion of data security through data development and use and industrial development, and ensure the development and use of data and industrial development through data security.

Article 14: The State is to implement a big data strategy, advancing data infrastructure construction, and encouraging and supporting the innovative application of data in all industries and all fields.

Provincial-level and higher people's governments shall include digital economy development in their respective level's people's economic and social development plans, and formulate digital economy development plans as needed.

Article 15: The State is to support the development and use of data to increase the intelligentization[7] level of public services. When providing intelligentized public services, the needs of elderly people and people with disabilities shall be fully considered, to avoid creating obstacles in the daily lives of elderly people and people with disabilities.

Article 16: The State is to support research into data development and use and data security technology, encourage dissemination and commercial innovation of technology in fields such as data development and use and data security, and foster and develop products and industrial systems for data development and use and data security.

Article 17: The State shall promote the construction of technical and data security standards systems for data development and use. The administrative department for standardization under the State Council and the relevant departments of the State Council shall, in accordance with their respective duties, organize the formulation and timely revision of standards relating to data development and use technologies, products, and data security. The State is to support the participation of enterprises, social organizations, and educational or scientific research institutions in the formulation of standards.

Article 18: The State is to promote the development of services such as data security testing and assessment, certification, etc., and to support specialized institutions for data security testing and assessment, certification, etc., to carry out service activities in accordance with law.

The State is to support relevant departments, industry organizations, enterprises, educational or scientific research institutions, relevant professional bodies, etc., in carrying out collaboration in areas such as assessment, prevention, and handling of data security risks.

Article 19: The State is to establish and complete data transaction management systems, standardize data transaction behavior, and cultivate a data transaction market.[8]

Article 20: The State is to support education and scientific research institutions, enterprises, etc., to carry out education and training in data development and use technologies and data security, adopting diverse methods to cultivate professional talent in data development and use technology and data security, and promoting talent exchanges.

Chapter III: Data Security Systems

Article 21: The State is to establish a categorized and graded protection system for data,[9] implementing categorized and graded protection according to the data's degree of importance in economic and social development, as well as the degree of danger to national security, public interests, or the lawful rights and interests of individuals or organizations brought about if it is altered, destroyed, leaked, or illegally obtained or used. The national data security work coordination mechanism is to comprehensively coordinate relevant departments in formulating catalogs of important data and strengthen the protection of important data.

Data related to national security, the lifelines of the national economy, important aspects of people's livelihoods, major public interests, etc., constitute core national data,[10] for which a stricter management system is to be implemented.

Each region and department, in accordance with the categorical and graded protection system for data, shall determine a specific catalog of important data for the respective region, department, or relevant industry, and engage in special protection of data listed in the catalog.

Article 22: The State is to establish a centralized and integrated, highly effective, and authoritative mechanism for data security risk assessment, reporting, information sharing, monitoring, and early warning. The national data security work coordinating mechanism is to comprehensively coordinate relevant departments to strengthen data security risk information acquisition, analysis, determination, and early warning work.

Article 23: The State is to establish data security emergency response mechanism. When data security incidents occur, relevant departments in charge shall activate emergency response plans in accordance with law, taking corresponding emergency response and handling measures to prevent further harm and eliminate security gaps, and promptly release warning information relevant to the public.

Article 24: The State is to establish a data security review system and conduct national security reviews for data handling activities that affect or may affect national security.

Security review decisions made according to law are final decisions.

Article 25: The State is to implement export controls in accordance with law for data belonging to controlled categories in order to safeguard national security and interests and fulfill international obligations.

Article 26: When any country or region adopts discriminatory prohibitions, restrictions, or other similar measures against the PRC relevant to investment, trade, etc., in data, data

development and use technology, etc., the PRC may take reciprocal measures against that country or region based on the actual circumstances.

Chapter IV: Data Security Protection Obligations

Article 27: The conduct of data handling activities shall be in compliance with the provisions of laws and administrative regulations, establishing and completing a data security management system for the entire workflow, organizing and conducting data security education and training, and adopting corresponding technical measures and other necessary measures to ensure data security. The conduct of data handling activities using the Internet or other such information networks shall perform the data security protection obligations described above on the basis of the cybersecurity Multi-Level Protection System.

Important data handlers shall clearly designate persons responsible for data security, and management bodies to implement data security protection responsibilities.

Article 28: The conduct of data handling activities and research and development of new data technologies shall be beneficial to promoting economic and social development, enhance the people's well-being, and conform to social morals and ethics.

Article 29: The conduct of data handling activities shall strengthen risk monitoring, and when data security shortcomings, leaks, or other such risks are discovered, remedial measures shall be taken immediately; when data security incidents occur, methods to address them shall be taken immediately, promptly notifying users and reporting to relevant departments in charge as provided.

Article 30: Those handling important data shall periodically conduct risk assessments of such data handling activities as provided and submit risk assessment reports to the relevant departments in charge.

Risk assessment reports shall include the type and amount of important data being handled, the circumstances of the data handling activities, the data security risks faced and measures to address them, etc.

Article 31: The provisions of the Cybersecurity Law of the PRC apply to the outbound security management[11] of important data collected or produced by critical information infrastructure operators operating within the mainland territory of the PRC; outbound security management measures for other data handlers collecting or producing important data within the mainland territory of the PRC are to be jointly formulated by the national cybersecurity and informatization department and relevant departments of the State Council.

Article 32: Any organization or individual collecting data shall adopt lawful and proper methods and must not steal or otherwise obtain data through illegal methods.

Where laws or administrative regulations have provisions on the purpose or scope of data collection and use, data shall be collected and used for the purpose and within the scope provided for by those laws and administrative regulations.

Article 33: When institutions engaged in data transaction intermediary services provide services, they shall require the party providing the data to explain the source of the data,

examine and verify the identities of both parties to the transactions, and retain verification and transaction records.

Article 34: Where laws and administrative regulations provide that administrative permits shall be acquired for the provision of services related to data handling, service providers shall obtain permits in accordance with law.

Article 35: Where public security authorities and national security authorities obtain data as necessary to safeguard national security or investigate crimes in accordance with law, they shall undergo strict approval procedures according to relevant State provisions and proceed in accordance with law, and relevant organizations and individuals shall cooperate.

Article 36: The competent authorities of the PRC are to handle foreign justice or law enforcement institution requests for the provision of data, according to relevant laws and treaties or agreements concluded or participated in by the PRC, or in accordance with the principle of equality and reciprocity. Domestic organizations and individuals must not provide data stored within the mainland territory of the PRC to the justice or law enforcement institutions of foreign countries without the approval of the competent authorities of the PRC.

Chapter V: Security and Openness of Government Data

Article 37: The State is to forcefully advance the construction of e-government; increase the scientific nature, accuracy, and efficacy of government data; and enhance capabilities to use data in service of economic and social development.

Article 38: State authorities that need to collect or use data to perform their legally-prescribed duties shall do so within the scope of their legally-prescribed duties and in accordance with the conditions and procedures provided by law and administrative regulations; they shall preserve the confidentiality, in accordance with law, of data such as personal private [data], personal information, commercial secrets, and confidential commercial information; and they must not divulge or illegally provide it to others.

Article 39: State authorities shall, in accordance with the provisions of laws and administrative regulations, establish and complete data security management systems, implement data security protection responsibilities, and ensure government data security.

Article 40: State authorities entrusting others to construct or maintain e-government systems, or to store or process government data, shall undergo strict approval procedures, and shall supervise entrusted parties' performance of data security protection obligations. Entrusted parties shall perform data security protection obligations according to the provisions of laws, administrative regulations, and contractual agreements, and must not retain, use, divulge, or provide others with government data without authorization.

Article 41: State authorities shall abide by the principles of fairness, impartiality, and convenience for the people and promptly and accurately disclose government data according to provisions, except that which according to law is not to be disclosed.

Article 42: The State is to: formulate government data openness catalogs; build a uniform and standard, interconnected and interactive, secure and controllable government data openness platform; and promote the use of open government data.

Article 43: The provisions of this Chapter apply to the conduct of data handling activities in the performance of legally prescribed duties by organizations authorized by laws and administrative regulations to have public affairs management duties.

Chapter VI: Legal Liability

Article 44: Where relevant departments in charge, in the course of performing data security supervision and management duties, discover the existence of relatively major risks in data handling activities, they may arrange talks with relevant organizations and individuals in accordance with the limits of authority and procedures provided, and require relevant organizations and individuals to adopt measures to carry out reforms or eliminate risks.

Article 45: Where organizations or individuals conducting data handling activities do not perform the data security protection obligations provided for in Articles 27, 29, and 30 of this Law, the relevant departments in charge are to order corrections and give warnings, and may also impose a fine of between 50,000 and 500,000 yuan, and a fine of between 10,000 and 100,000 yuan on directly responsible management personnel and other directly responsible personnel. Those who refuse to make corrections or caused serious consequences such as a large-scale data leak are to be fined between 500,000 and 2,000,000 yuan and may be ordered to suspend relevant operations, suspend operations for rectification, or have relevant business permits or licenses revoked; directly responsible management personnel and other directly responsible personnel are to be fined between 50,000 and 200,000 yuan.

Where core national data management systems are violated, endangering national sovereignty, security, or development interests, relevant departments in charge are to impose a fine of between 2,000,000 and 10,000,000 yuan and, according to the circumstances, order a suspension of relevant operations, suspension of operations for rectification, or the revocation of relevant business permits or licenses; where a crime is constituted, criminal liability is to be pursued in accordance with law.

Article 46: Where important data is provided abroad in violation of the provisions of Article 31 of this Law: relevant departments in charge are to order corrections and give warning; a a fine of between 100,000 and 1,000,000 yuan may be imposed; a suspension of relevant operations, suspension of operations for rectification, or revocation of relevant business permits or licenses may be ordered; and directly responsible management personnel and other directly responsible personnel are to be fined between 100,000 and 1,000,000 yuan.

Article 47: Where institutions engaged in data transaction intermediary services fail to perform obligations provided by Article 33 of this Law: relevant departments in charge are to order corrections, confiscate unlawful gains, and impose a fine of between the amount of the unlawful gains and 10 times the amount of the unlawful gains; where there are no unlawful gains or the unlawful gains are less than 100,000 yuan, a fine of between 100,000 and 1,000,000 yuan is to be imposed; a suspension of relevant operations, a suspension of business for rectification, or the revocation of relevant business permits or licenses may be ordered; and directly responsible management personnel and other directly responsible personnel are to be fined between 10,000 and 100,000 yuan.

Article 48: Where the provisions of Article 35 of this Law are violated through refusal to cooperate with the obtaining of data, the relevant departments in charge are to order correction, give warnings, impose a fine of between 50,000 and 500,000 yuan, and fine

directly responsible management personnel and other directly responsible personnel between 10,000 and 100,000 yuan.

Where the provisions of Article 36 of this Law are violated through the provision of data to foreign justice or law enforcement institutions without the approval of managing authorities, relevant departments in charge are to order corrections, may impose a fine of between 100,000 and 1,000,000 yuan, and may impose a fine of between 10,000 and 100,000 yuan on directly responsible management personnel and other directly responsible personnel; where serious consequences result, a fine of between 1,000,000 and 5,000,000 yuan is to be imposed, and a suspension of relevant operations, a suspension of business for rectification, or the revocation of relevant business permits or licenses may be ordered, and directly responsible management personnel and other directly responsible personnel are to be fined between 50,000 and 500,000 yuan.

Article 49: Where State authorities do not perform data security protection obligations provided by this Law, the directly responsible management personnel and other directly responsible personnel are to be sanctioned according to law.

Article 50: Where State personnel with data security regulatory duties are derelict, abuse their authority, or abuse their position for private gain, they are to be sanctioned according to law.

Article 51: Where data is obtained through theft or other illegal means, or the conduct of data handling activities eliminates or restricts competition or harms the lawful rights and interests of individuals or organizations, punishment is to be given in accordance with the provisions of relevant laws and administrative regulations.

Article 52: Where violations of the provisions of this Law harm others, civil liability is to be borne in accordance with law.

Where violations of the provisions of this Law constitute a violation of public security management, public security administrative sanctions are to be given in accordance with law; where a crime is constituted, criminal liability is to be pursued in accordance with law.

Chapter VII: Supplementary Provisions

Article 53: The provisions of the Law of the PRC on the Protection of State Secrets and other laws and administrative regulations apply when conducting data handling activities involving state secrets.

The conduct of data handling activities in statistical or archival work, and the conduct of data handling activities that involve personal information, shall also comply with the provisions of relevant laws and administrative regulations.

Article 54: Measures for military data security protection are to be formulated by the Central Military Commission according to provisions separate from this Law.

Article 55: This Law is to be implemented beginning Sept. 1, 2021.