

This Bestao Translation is provided as a working tool. No warranty of any kind, either expressed or implied, is made as to its accuracy, correctness, or reliability. Only the original official version should prevail as a source of reference.

Data Security Law of the PRC

(2021 年 6 月 10 日第十三届全国人民代表大会常务委员会第二十九次会议通过)

Contents

Chapter I: General Provisions

Chapter II: Data Security and Development

Chapter III: Data Security Systems

Chapter IV: Obligations of Data Security Protection

Chapter V: Security and Openness in Government Affairs Data

Chapter VI: Legal Liability

Chapter VII: Supplementary Provisions

Chapter I: General Provisions

Article 1: This Law is formulated so as to regulate the handling of data, ensure data security, promote the development and exploitation of data, protect citizens' and organizations' lawful rights and interests, and preserve state sovereignty, security, and development interests.

Article 2: This law applies to data handling activities and security regulation carried out within the [mainland] territory of the People's Republic of China.

Data handling activities carried out outside the [mainland] territory of the P.R.C. that harming the national security of the P.R.C., the public interest, or the lawful rights and interests of citizens and organizations, are to be pursued for legal responsibility in accordance with law.

Article 3: "Data" as used in this Law, refers to any record of information in electronic or other forms.

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

Data security refers to employing necessary measures to ensure that data is effectively protected and legally used, as well as possessing the capacity to ensure a sustained state of security.

Article 4: The preservation of data security shall adhere to the overall national security perspective, establish and complete data security governance systems, and increase capacity to ensure data security.

Article 5: The Central Leading Institution on National Security is responsible for major decision-making, deliberating and coordinating the nation's data security work; researching, drafting, and guiding the implementation of the national data security strategy and related major policy directives; planning and coordinating major matters and efforts in national data security, and establishing a coordination mechanism for national data security work.

Article 6: Each region and department is responsible for the data collected and produced by that region or department's work and for data security.

Regulatory departments such as for industry, telecommunications, communications, finance, natural resources, health, education, science and technology are to undertake data security regulatory duties in the corresponding sector.

Public security organs, state security organs, and so forth are to undertake data security regulation duties within the scope of their duties in accordance with the provisions of this Law, relevant laws, and administrative regulations.

The State internet information departments are to take responsibility for the overall coordination of online data security and relevant regulatory efforts in accordance with this Law, relevant laws, and administrative regulations.

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

Article 8: The carrying out of data handling activities shall obey laws and regulations, respect social mores and ethics, comply with commercial and professional ethics, be honest and trustworthy, perform obligations to protect data security and take on social responsibility; it must not endanger national security, the public interest, or individuals' and organizations' lawful rights and interests.

Article 9: The state is to support the development of publicity spreading knowledge on data security, elevating the entire society's awareness and level of data security protections, pushing relevant departments, industry organizations, scientific research bodies, enterprises, and individuals to jointly participate in efforts to protect data security, and forming a positive environment for the entire society to jointly preserve data security and promote development.

Article 10: In accordance with their charters, relevant industry organizations are to draft data security conduct specifications and group standards in accordance with law, strengthen industry self-discipline, guide members to strengthen data security protections, increase the level of data security protections, and promote the healthy development of the industry.

Article 11: That state is to actively develop international exchanges and cooperation in fields such as data security governance and data exploitation and use, participating in the drafting of international rules and standards for data security, and promoting the cross-border security and free flow of data.

Article 12: All individuals and organizations have the right to make complaints or reports to the relevant departments regarding violations of the provisions of this Law. Departments receiving complaints or reports shall handle them promptly and in accordance with law.

The relevant regulatory departments shall preserve the confidentiality of complainants' or informants' information and protect the complainants' or informants' lawful rights and interests.

Chapter II: Data Security and Development

Article 13: The state is to make overall plans for development and security, persisting using the development and use of data and industry development to promote data security, and using data security to ensure the development and use of data and industry development.

Article 14: The state is to implement a big data strategy, advancing the establishment of data infrastructure, and encouraging and supporting innovative applications of data in each industry and field.

People's governments at the provincial level or higher shall include the development of the digital economy in the people's economic and social development plans for that level, and draft development plans for the digital economy as needed.

Article 15: The state is to support the development and use of data to increase the level of smart technology in public services. The provision of smart public services shall fully consider the needs of the elderly and persons with disabilities, to avoid creating obstacles in their daily lives.

Article 16: The state is to support research into data use and development and data security techniques, encourage the spread and commercial innovation in areas such as the use and development of data and data security, to foster and develop the use and development of data, data security products, and industrial systems.

Article 17: The state is to advance the establishment of a system of standards for data development and exploitation technologies and data security. Within the scope of their respective duties, the State Council departments in charge of standardization and other relevant State Council departments are to organize the formulation and appropriate revision of standards related to technology and products for the development and use of data and to data security. The state is to support enterprises and social groups, educational or research bodies, and so forth, participating in drafting standards.

Article 18: The state is to promote the development of services such as data security testing, appraisals, and certification, and support professional institutions carrying out data security testing, appraisals, and certification service activities.

The state is to support relevant departments, industry organizations, enterprises, educational or scientific research bodies, relevant professional bodies, and so forth in carrying out collaboration in areas such as assessments, prevention, and handling of data security risks.

Article 19: The state is to establish and complete management systems for data transactions, regulating data exchange conduct, and cultivating data exchange markets.

Article 20: The State is to support educational and scientific research bodies, enterprises, and so forth, in carrying out education and training related to data use and development and data security, employing diverse methods to cultivate professional data use and development and data security talent, and promote professional exchanges.

Chapter III: Data Security Systems

Article 21: The state is to establish a categorical and hierarchical system for data protection and carry out categorized and graded data protections based on the importance of the data in economic and social development as well as the extent of harm to national security, the public interest, or the lawful rights and interests of individuals or organizations that would be caused once the data is altered, destroyed, leaked, or illegally obtained or used. The national mechanism for coordinating data security work is to plan and coordinate relevant departments' drafting of catalogs of important data and strengthen protections of important data.

Data related to national security, the lifeline of the national economy, important aspects of people's livelihoods, and major public interests are core state data, and are to implement a stricter management system.

Each region and department shall determine the catalog of important data within that region and department and corresponding industries and sectors on the basis of the categoric and hierarchical protection system, and conduct key protection for data entered in the catalog.

Article 22: The state is to establish uniform, highly effective, and authoritative systems for data security risk assessment, reporting, information sharing, monitoring, and early warnings. The national coordination mechanism for data security work is to plan and coordinate relevant departments to strengthen the acquisition, analyses, assessment, and early warnings for information on data security risks.

Article 23: The state is to establish a data security emergency response and handling system. Relevant regulatory departments shall initiate emergency response plans in accordance with law when data security incidents occur, employing the corresponding emergency response and handling measures to prevent the harm from increasing and eliminate security risks, and promptly issue relevant alerts to the public.

Article 24: The state is to establish systems for data security reviews and conduct national security reviews of data handling activities that impact or might impact national security.

Security review decisions made in accordance with law are final decisions.

Article 25: The state is to implement export controls in accordance with law for data that are controlled items related to preserving national security and performing international obligations.

Article 26: Where any nation or region employs discriminatory, restrictive, or other similar measures against the PRC in terms of areas such as investment or trade in data and technology for the exploitation and development of data, the P.R.C. may employ equal measures against that nation or region based on the actual circumstances.

Chapter IV: Obligations of Data Security Protection

Article 27: The carrying out of data handling activities shall be in accordance with laws and regulations, establishing and completing data security management systems for the entire process, organizing and carrying out education on data security, and employing corresponding technical measures and other necessary measures to safeguard data security. The use of the internet or other information networks to carry out data handling activities shall be done on the basis of the multi-level protection system for cybersecurity, and carry out the data security protection obligations described above.

Those processing important data shall clearly designate persons responsible for data security and data security management bodies to implement responsibilities for data security protection.

Article 28: The carrying out of data handling activities as well as research into new technology for developing data shall be conducive to promoting economic development, improving the well-being of the people, and complying with social mores and ethics.

Article 29: The carrying out of data handling activities shall strengthen risk monitoring, and when data security flaws, vulnerabilities, or other risks are discovered, remedial measures shall be immediately employed; and when data security incidents occur, methods for addressing them shall be immediately employed, users are to be promptly notified as provided, and reports are to be made to the relevant regulatory departments.

Article 30: Those handling important data shall follow periodically carry out risk assessments of their data handling activities as provided, and send risk assessment reports to the relevant regulatory departments.

Risk assessment reports shall include the types and amounts of important data being handled; the circumstances of the data handling activities; the data risks faced, methods for addressing them, and so forth.

Article 31: The provisions of the Cybersecurity Law of the P.R.C. apply to the security management for exporting of data from the [mainland] territory that was collected or produced by critical information infrastructure operators inside the [mainland] territory of the PRC; security management measures for the export of important data from the mainland territory that was collected or produced by other

data handlers within the [mainland] territory of the PRC are to be drafted by the State internet information department in conjunction with the relevant departments of the State Council.

Article 32: Any organization or individual collecting data shall employ lawful and appropriate methods and must not steal or obtain data through other illegal methods.

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

Article 33: The provision of services by institutions engaged in data transaction intermediary services shall require the party providing the data to explain the data's origins, and shall review and verify both parties to the transactions' identities, and store records of the verifications and transactions.

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

Article 35: Public security organs and state security organs collecting data as necessary to lawfully preserve national security or investigate crimes shall follow relevant state provisions and complete strict approval formalities to do so, and relevant organizations and individuals shall cooperate.

Article 36: The competent organs of the PRC are to handle requests for the provision of data from foreign justice or law enforcement based on relevant laws and international treaties and agreements concluded or participated in by the PRC, or in accordance with the principle of reciprocity. Domestic organizations and individuals must not provide data stored within the PRC to foreign justice or law enforcement bodies without the permission of the competent organs of the PRC.

Chapter V: Security and Openness in Government Affairs Data

Article 37: The state is to forcefully advance the establishment of e-governance, increasing the scientific nature, accuracy, and efficacy of government affairs data, and increasing the use of data in service of economic and social development.

Article 38: State organs that need to collect or use data for the performance of their legally-prescribed duties shall do so within the scope of their legally-prescribed duties and in accordance with the requirements and procedures provided by laws and administrative regulations; and preserve the confidentiality in accordance with law of personal private information, personal information, commercial secrets, confidential commercial information, and other such data that they learn of in the performance of their duties; and they must not leak or illegally provide it to others.

Article 39: In accordance with the provisions of laws and administrative regulations, state organs shall establish and complete data security management systems, implement responsibility for data security protection, and ensure the security of government affairs data.

Article 40: State organs entrusting others to establish or maintain electronic government affairs systems or to store or process government affairs data shall go through strict approval procedures, and shall oversee the performance of data security protection obligations by the entrusted parties. The entrusted party shall perform data security protection obligations in accordance with laws, regulations, and contractual agreements, and must not store, use, leak, or provide others with government affairs data without authorization.

Article 41: State organs shall follow the principles of justice, fairness, and convenience for the people, to promptly and accurately disclose government affairs data as provided. Except for that which is not to be disclosed in accordance with law.

Article 42: The state is to create a catalog of open government affairs data, building a uniformly standardized, interconnected, secure and controllable platform for opening government affairs data, and promoting the use of open government affairs data.

Article 43: The provisions of this chapter apply to the carrying out of data handling activities by organizations authorized by laws or regulations to have public affairs management duties in order to perform their legally-prescribed duties.

Chapter VI: Legal Responsibility

Article 44: Where relevant regulatory departments performing data security oversight and management duties discover that data handling activities have larger security risks, they may give the relevant organizations and individuals a talking to in accordance with the authority and procedures provided, and require the relevant organizations or individuals to employ measures to correct or eliminate the risks.

Article 45: Where organizations or individuals carrying out data handling activities do not perform the data security protection obligations provided for in articles 27, 29, and 30 of this Law, the relevant regulatory departments are to order corrections and give warnings, and may give a concurrent fine of between 50,000 and 500,000 RMB, and may give directly responsible managers and other directly responsible personnel a concurrent fine of between 10,000 and 50,000 RMB; where corrections are refused or a large data leak or other serious consequences are caused, a fine of between 500,000 and 2,000,000 RMB is to be given, and they may be ordered to stop relevant operations, suspend operations for rectification, cancel relevant business permits or licenses, and the directly responsible managers and other directly responsible personnel are to be given a fine of between 50,000 and 200,000 RMB.

Where systems for the management of core state data are violated, endangering the nation's sovereignty, security, or development interests, the relevant regulatory departments are to give fines of between 2,000,000 and 10,000,000 RMB, and in light of the circumstances, order a suspension of operations, a suspension for rectification, cancel relevant permits or cancel business licenses; and where a crime is constituted, criminal responsibility is pursued in accordance with law.

Article 46: Where organizations or individuals violate article 31 of this Law by providing important data abroad, the relevant regulatory departments are to order corrections and give warnings, and may give a concurrent fine of between 100,000 and 1,000,000 RMB, and may give directly responsible managers and other directly responsible personnel a concurrent fine of between 10,000 and 50,000 RMB; where the circumstances are serious, a fine of between 1,000,000 and 10,000,000 RMB is to be given, and they may be ordered to stop relevant operations, suspend operations for rectification, cancel relevant business permits or licenses, and the directly responsible managers and other directly responsible personnel are to be given a fine of between 100,000 and 1,000,000 RMB.

Article 47: Where establishments engaged in services as intermediaries in data transactions fail to perform the obligations in article 33 of this Law, the relevant regulatory departments are to order corrections, confiscation the unlawful gains, and give a fine of between 1 and 10 times the value of the unlawful gains, or where there are no unlawful gains or the unlawful gains are less than 100,000 RMB, a fine of between 100,000 and 1,000,000 RMB is to be given, and they may be ordered to stop relevant operations, suspend operations for rectification, or cancel related business permits or licenses; a fine of between 10,000 and 100,000 RMB is to be given to the directly responsible managers and other directly responsible personnel.

Article 48: Where article 35 of this Law is violated by a refusal to cooperate with the collection of data, the relevant regulatory departments are to order corrections and give warnings, and give a concurrent fine of between 50,000 and 500,000 RMB, and give directly responsible managers and other directly responsible personnel a fine of between 10,000 and 100,000 RMB.

Where article 36 of this Law is violated by providing data to foreign justice or law enforcement bodies without the approval of the organs in charge, the relevant regulatory departments are to give warnings, may give a concurrent fine of between 100,000 and 1,000,000 RMB, and may give directly responsible managers and other directly responsible personnel a concurrent fine of between 10,000 and 50,000 RMB; where serious consequences result, a fine of between 1,000,000 and 5,000,000 RMB is to be given, and they may be ordered to suspend relevant operations, suspend operations for rectification, or cancel relevant business permits or licenses, and the directly responsible managers and other directly responsible personnel are to be given a fine of between 50,000 and 500,000 RMB.

Article 49: Where state organs do not perform obligations to protect data security as provided for in this Law, the directly responsible managers and other directly responsible personnel are to be given sanctions in accordance with law.

Article 50: Where state personnel with duties for regulating data security derelict their duties, abuse their authority or twist the law for personal gain, they are to be sanctioned in accordance with law.

Article 51: Where the theft or other illegal acquisition of data or carrying out 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 laws and administrative regulations.

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

Where provisions of this Law are violated, constituting a violation of public security management, public security administrative sanctions are given in accordance with law; where a crime is constituted, criminal responsibility is pursued in accordance with law.

Chapter VII: Supplementary Provisions

Article 53: The "P.R.C. Law on the Protection of State Secrets" and other relevant laws and administrative regulations apply to the carrying out of data handling activities that involve state secrets.

The carrying out of data handling activities in statistics or archival work, or involving personal information shall also comply with relevant laws and administrative regulations.

Article 54: Measures for military data security are to be separately drafted by the Central Military Commission on the basis of this Law.

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