

Data Security Law of the People's Republic of China

Promulgation date	2021-06-10	Effective region	NATIONAL
Promulgator	Standing Committee of the National People's Congress	Document number	Order of the President of the People's Republic of China No. 84
Effectiveness	Effective	Effective date	2021-09-01
Taxonomy	Public Security Law (Public Security Law) ,Computer & Internet (Science & Technology Law->Computer & Internet)		
Industry category	Software & Information Technology		

Data Security Law of the People's Republic of China

Order of the President of the People's Republic of China No. 84

June 10, 2021

The Data Security Law of the People's Republic of China, which has been adopted at the 29th session of the Standing Committee of the 13th National People's Congress on June 10, 2021, is hereby promulgated and shall come into effect from September 1, 2021.

Xi Jinping President of the People's Republic of China

Data Security Law of the People's Republic of China

(Adopted at the 29th session of the Standing Committee of the 13th National People's Congress on June 10, 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 Openness of Government Data

Chapter VI Legal Liability

Chapter VII Supplementary Provisions

Chapter I General Provisions

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

Article 2 This Law shall apply to the data handling activities carried out within the territory of the People's Republic of China as well as the security regulation thereof.

Where any data handling activity carried out outside of the territory of the People's Republic of China harms the national security, public interests, or the legitimate rights and interests of citizens or organizations of the People's Republic of China, legal liability shall be investigated in accordance with the law.

Article 3 For the purpose of this Law, data shall refer to any record of information in electronic or other form. Data handling shall refer to the collection, storage, use, processing, transmission, provision and disclosure of data.

Data security shall refer to the ability to ensure that data are being effectively protected and lawfully used and to keep the secure state by adopting necessary measures.

Article 4 In ensuring data security, the overall national security concept shall be upheld, with data security governance systems established and perfected, and data security protection capabilities increased.

Article 5 The central leadership organ of national security is responsible for the decision-making, deliberation and coordination in respect of data security work, and for researching, formulating, and guiding the implementation of national data security strategies and related significant guidelines and policies; coordinating the major matters and key work regarding national data security and establishing a national data security coordination mechanism.

Article 6 All regions and departments assume primary responsibility for the data collected and generated in the work of their respective regions or departments as well as for data security.

Competent departments of industries such as industry, telecommunications, transport, finance, natural resources, hygiene and health, education, and science and technology are responsible for the supervision of data security in respective industries or sectors.

Public security organs and national security organs are, in accordance with this Law and the relevant laws and administrative regulations, responsible for the supervision of data security within their respective scope of duties.

The national cyberspace administration authority is, in accordance with this Law and the relevant laws and administrative regulations, responsible for the comprehensive coordination of online data security and related supervision work.

Article 7 The State shall protect the data-related rights and interests of individuals and organizations; encourage lawful, reasonable, and effective data use; ensure the lawful, orderly, and free flow of data; and stimulate the development of a digital economy with data as a key factor.

Article 8 When conducting data handling activities, laws and administrative regulations shall be observed, social public morals and ethics respected, commercial and professional ethics followed, sincerity and trustworthiness upheld, data security protection obligations fulfilled, and social responsibilities undertaken. It is prohibited to harm national security or public interests or to harm the legitimate rights and interests of individuals and organizations.

Article 9 The State shall support the promotion and publicity of data security knowledge, raise the awareness and capability of the whole society in data security protection, and urge the relevant departments, industrial organizations, research institutions, enterprises, and individuals to jointly participate in data security protection work, so as to create a beneficial environment in which all walks of life jointly safeguard data security and boost development.

Article 10 Relevant industrial organizations shall, in accordance with their articles of association, legally formulate the code of conduct in and the group standards for data security, enhance industrial self-discipline, guide their members to strengthen data security protection, improve the level of data security protection and promote the healthy development of the industry.

Article 11 The State shall actively engage in international exchange and cooperation in such areas as data security governance and data development and use, participate in the formulation of international rules and standards related to data security, and promote the secure and free flow of data across borders.

Article 12 Any individual or organization has the right to file a complaint or tip-off about violations of this Law with the relevant competent departments. Departments receiving complaints or tip-offs shall handle them promptly in accordance with the law.

Relevant competent departments shall keep confidential the information on those filing the complaint or tip-off and protect their legitimate rights and interests.

Chapter II Data Security and Development

Article 13 The State shall coordinate both development and security, and adhere to promoting data security through data development and use and through industrial development, and ensuring data development and use and industrial development through data security.

Article 14 The State shall implement a big data strategy to enhance data infrastructure construction, to encourage and support the innovative application of data in all industries and sectors.

People's governments at or above the provincial level shall include the digital economy development in the national economic and social development planning at the respective level and formulate digital economy development plans as needed.

Article 15 The State shall support the data development and use to make public services more intelligent. When providing such intelligent public services, it is required to fully consider the needs of the elderly and the handicapped and avoid causing any obstacle to their daily life.

Article 16 The State shall support the research on data development and use technologies and data security technologies; support the dissemination and commercial innovation of technologies in such areas as data development and use and data security; and foster and develop products and industry systems for data development and use and for data security.

Article 17 The State shall advance the construction of the standard systems for the data development and use technology and those for data security. The administrative department of standardization under the State Council and the relevant departments of the State Council shall, according to their respective duties, organize the formulation and timely revision of standards concerning data development and use technologies and products and data security. The State shall support enterprises, social organizations, and education and research institutions to participate in the formulation of standards.

Article 18 The State shall promote the development of services such as data security monitoring and assessment, and certification, and support specialized institutions to perform data security monitoring and assessment, and certification in providing services in accordance with the law.

The State shall support relevant departments, industrial organizations, enterprises, education and research institutions, and relevant specialized institutions to conduct coordination in such areas as data security risk assessment, prevention and disposal.

Article 19 The State shall establish and perfect the data transaction management systems, standardize data transaction activities, and cultivate a data transaction market.

Article 20 The State shall support education and research institutions, enterprises and other organizations in carrying out education and training in respect of data development and use technology and data security,

and in adopting a variety of methods to cultivate talent in data development and use technology and data security, and to promote talent exchange.

Chapter III Data Security Systems

Article 21 The State shall establish a classified and graded data protection system, and carry out classified and graded data protection in accordance with the degree of importance of data to economic and social development, and the damage to national security, public interests, or the legitimate rights and interests of individuals or organizations in the event that data are tampered with, destroyed, leaked, or illegally obtained or used. The national data security coordination mechanism shall make overall planning for and coordinate relevant departments in formulating the catalogues for important data and strengthening the protection of important data.

Data that have a bearing on national security, the lifelines of national economy, important aspects of people's livelihood and major public interests shall constitute the core data of the State and shall be subject to stricter management system.

Each region and department shall, in accordance with the classified and graded data protection system, determine the specific catalogue for important data for the respective region and department, and in relevant industries and areas, and undertake special protection for the data included in the catalogue.

Article 22 The State shall establish a centralized, efficient, and authoritative mechanism for data security risk assessment, reporting, information sharing, supervision, and early warning. The national data security coordination mechanism shall make overall planning for and coordinate relevant departments in strengthening their work in the collection, analysis, determination, and early warning of the data security risk information.

Article 23 The State shall establish a data security emergency response mechanism. In the event of a data security incident, the relevant competent department shall, in accordance with the law, activate a contingency plan, adopt appropriate emergency response measures, prevent expansion of harms, eliminate security hazards, and promptly publish the warning information related to the public.

Article 24 The State shall establish a data security review system, where data handling activities that affect or may affect the national security will undergo national security review. Security review decisions issued in accordance with the law are final decisions.

Article 25 The State shall implement export controls in accordance with the law on data belonging to controlled categories and those relevant to safeguarding national security and interests and fulfilling international obligations.

Article 26 For any country or region that adopts discriminatory prohibitions, limitations, or other similar measures related to data and data development and use technology, against the People's Republic of China, in investment, trade and other areas, the People's Republic of China may, depending on the actual circumstances, adopt the equivalent measures against such country or region.

Chapter IV Data Security Protection Obligations

Article 27 Those conducting data handling activities shall, in accordance with laws and regulations, establish and perfect a data security management system across the entire workflow, organize and conduct data security education and training, and adopt the corresponding technical measures and other necessary measures to ensure data security. Those conducting data handling activities by using the internet or other information networks shall, based on the graded cybersecurity protection system, perform the aforesaid data security protection obligations.

Those handling important data shall clearly specify responsible personnel and management bodies for data security and fully implement data security protection responsibilities.

Article 28 Any data handling activity as well as the research and development of new data technologies shall benefit the advancement of economic and social development, enhance the people's welfare, and conform to social morals and ethics.

Article 29 Those conducting data handling activities shall strengthen risk monitoring, and where they discover risks such as data security flaws and vulnerabilities, immediately adopt remedial measures; when data security incidents occur, they shall immediately take disposal measures, notify the users as required and report the matter to the relevant competent department.

Article 30 Those handling important data shall, in accordance with relevant provisions, periodically conduct risk assessments for their data handling activities, and submit a risk assessment report to the relevant competent department.

The risk assessment report shall include the categories and quantities of important data handled by the said organization, how data are handled, the data security risks faced and their countermeasures.

Article 31 The security administration of the cross-border transfer of important data collected and generated by operators of critical information infrastructure during their operation in China shall be subject to the provisions of the Cybersecurity Law of the People's Republic of China; the administrative measures for the cross-border transfer of important data collected and generated by other data handlers during their operation in the People's Republic of China shall be formulated by the national cyberspace administration authority in collaboration with relevant departments of the State Council.

Article 32 Any organization or individual collecting data shall adopt lawful and proper methods and shall not steal data or obtain them by other illegal means.

Where any law and administrative regulation contains provisions on the purpose or scope of data collection or use, data shall be collected and used for the purpose and within the scope prescribed by such law and administrative regulation.

Article 33 Institutions engaging in data transaction intermediary services shall, when providing their services, require the data providers to explain the source of data, examine and verify the identity of both parties to the transaction, and retain examination, verification, and transaction records.

Article 34 Where any law and administrative regulation stipulates that administrative license shall be obtained before providing any service related to data handling, the service providers shall obtain such license in accordance with the law.

Article 35 Where public security organs and national security organs need to consult any data in order to safeguard national security or investigate a crime in accordance with the law, they shall, in accordance with the relevant provisions of the State, undergo strict approval procedures and proceed with the matter in accordance with the law; and the relevant organizations and individuals shall render cooperation.

Article 36 The competent authority of the People's Republic of China shall handle the request for providing any data from a foreign judicial body and law enforcement body in accordance with relevant laws and the international treaty or agreement which the People's Republic of China has concluded or acceded to, or under the principle of equality and mutual benefit. Any organization or individual within the territory of the People's Republic of China shall not provide any foreign judicial body and law enforcement body with any data stored within the territory of the People's Republic of China without the approval of the competent authority of the People's Republic of China.

Chapter V Security and Openness of Government Data

Article 37 The State shall vigorously advance the construction of e-government, increases the rationality, accuracy, and timeliness of government data, and enhance the capabilities to use data to serve economic and social development.

Article 38 Where any state organ needs to collect or use data to perform its statutory duties, it shall do so within the scope of its statutory duties and according to the conditions and procedures prescribed in laws and administrative regulations; any data it comes to know in the course of performing its duties, including personal privacy, personal information, trade secret and confidential business information, shall be kept confidential and shall not be leaked or illegally provided to others.

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

Article 40 Where state organs entrust others maintain and construct any government system, or to store or process government data, they shall undergo strict approval procedures, and shall supervise the entrusted parties in terms of their fulfillment of the corresponding data security protection obligations. The entrusted parties shall perform their data security protection obligations in accordance with laws, regulations and any contractual agreement, and shall not retain, use, leak or provide to others any government data without permission.

Article 41 State organs shall promptly and accurately publish government data as required under the principles of fairness, impartiality, and convenience for the people, except where the data shall not be disclosed in accordance with the law.

Article 42 The State shall formulate open catalogues for government data, and build a uniform and standard, interconnected and interactive, secure and controllable government data open platform, to promote the open use of government data.

Article 43 Where organizations with public affairs management functions, as authorized by laws and regulations, conduct data handling activities in order to perform their statutory duties, this chapter shall apply.

Chapter VI Legal Liability

Article 44 When the relevant competent departments discover any major security risk in data handling activities in the course of performing their data security supervision duties, they may, according to the prescribed authority and procedures, conduct interviews with the relevant organizations and individuals, and require them to take measures for rectification to eliminate hazards.

Article 45 Where any organization and individual fails to fulfill the data security obligations stipulated in Articles 27, 29, and 30 hereof in conducting data handling activities, relevant competent departments shall order such organization and individual to make correction, give warnings, and may impose a fine of no less than CNY50,000 but no more than CNY500,000 concurrently; the directly responsible officers and other persons directly liable may be imposed a fine of no less than CNY10,000 but no more than CNY100,000; those who refuse to make correction or cause major data leakages or other serious consequences shall be imposed a fine of no less than CNY500,000 but no more than CNY2 million, and may concurrently be ordered to suspend relevant business or stop operation for rectification, or be subject to revocation of relevant

business permits or business license; and the directly responsible officers and other persons directly liable shall be imposed a fine of no less than CNY50,000 but no more than CNY200,000.

Those who violate the management system for core data of the State and cause harm to the national sovereignty, security and development interests shall be imposed a fine of no less than CNY2 million but no more than CNY10 million by relevant competent departments, and shall be ordered to suspend relevant business or stop operation for rectification, or be subject to revocation of relevant business permits or business license, as appropriate; if a crime is constituted, they shall be held criminally liable in accordance with the law.

Article 46 Those who provide any important data to a party outside the territory of the People's Republic of China in violation of Article 31 hereof shall be ordered to make correction and given warnings by relevant competent departments, and may be imposed a fine of no less than CNY100,000 but no more than CNY1 million concurrently; the directly responsible officers and other persons directly liable may be imposed a fine of no less than CNY10,000 but no more than CNY100,000. In case of serious circumstances, they shall be imposed a fine of no less than CNY1 million but no more than CNY 10 million, and may be ordered to suspend relevant business or stop operation for rectification, or be subject to revocation of relevant business permits or business license; the directly responsible officers and other persons directly liable shall be imposed a fine of no less than CNY100,000 but no more than CNY1 million.

Article 47 Where any data transaction intermediary organization fails to perform the obligations stipulated in Article 33 hereof, relevant competent departments shall order it to make correction, confiscate any illegal income, and impose a fine of no less than one but no more than ten times the illegal income; where there is no illegal income or the illegal income is less than CNY100,000, a fine of no less than CNY100,000 but no more than CNY1 million shall be imposed, and the relevant competent departments may order such organization to suspend relevant businesses, stop its operation for rectification, or revoke the relevant business permits or business licenses; the directly responsible officers and other persons directly liable shall be imposed a fine of no less than CNY10,000 but no more than CNY100,000.

Article 48 Those who refuse to cooperate in data access in violation of Article 35 hereof shall be ordered to make correction and given warnings and may be imposed a fine of no less than CNY50,000 but no more than CNY500,000 concurrently by relevant competent departments; their directly responsible officers and other persons directly liable shall be imposed a fine of no less than CNY10,000 but no more than CNY100,000. Those who provide any data to any foreign judicial or law enforcement body without approval of competent departments in violation of Article 36 hereof shall be given warnings, and may be imposed a fine of no less than CNY100,000 but no more than CNY1 million concurrently by relevant competent departments; their directly responsible officers and other persons directly liable may be imposed a fine of no less than CNY10,000 but no more than CNY100,000. In case of serious consequences, they shall be imposed a fine of no less than CNY1 million but no more than CNY5 million, and may be ordered to suspend relevant business or stop operation for rectification, or be subject to revocation of relevant business permits or business license; their directly responsible officers and other persons directly liable shall be imposed a fine of no less than CNY50,000 but no more than CNY500,000.

Article 49 Where any state organ fails to perform its data security protection obligations provided for herein, the directly responsible officers and other persons directly liable shall be sanctioned in accordance with the law.

Article 50 Where any government functionary with the duties of overseeing data security neglects his or her duties, abuses his or her powers, or engages in malpractice for selfish ends, he or she shall be sanctioned in accordance with the law.

Article 51 Any act of stealing or illegally obtaining data, and any data handling activity that excludes or

restricts competition, harms national security or public interests, or damages the legitimate rights and interests of individuals or organizations, shall be subject to punishment in accordance with the relevant laws and administrative regulations.

Article 52 Anyone who violates this Law, causing harm to others, shall bear civil liability in accordance with the law.

If anyone violates this Law, constituting a violation of public security administration, he or she shall be given a public security administration penalty in accordance with the law. If a crime is constituted, he or she shall be held criminally liable in accordance with the law.

Chapter VII Supplementary Provisions

Article 53 For data handling activities involving state secrets, such laws and administrative regulations as the Law of the People's Republic of China on Protecting State Secrets shall apply.

The data handling activities in the work of statistics and archiving, and those involving personal information shall abide by the relevant laws and administrative regulations.

Article 54 Measures for protecting military data will be separately formulated by the Central Military Commission.

Article 55 This Law shall come into force as of September 1, 2021.