[English] [中文版]

Home About Us Contact Us August 9, 2022

Tools: Save | Print | E-Mail

Data Security Law of the People's Republic of China

Posted: June-10-2021 Adjust font size:

Order of the President of the People's Republic of China

No. 84

The *Data Security Law of the People's Republic of China*, adopted at the 29th Meeting of the Standing Committee of the Thirteenth National People's Congress of the People's Republic of China on June 10, 2021, is hereby promulgated, and shall go into effect on September 1, 2021.

Xi Jinping
President of the People's Republic of China
June 10, 2021

Data Security Law of the People's Republic of China

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

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 enacted for the purpose of regulating data processing, ensuring data security, promoting development and utilization of data, protecting the lawful rights and interests of individuals and organizations,

and safeguarding the sovereignty, security, and development interests of the state.

Article 2 This Law shall apply to data processing activities and security supervision and regulation of such activities within the territory of the People's Republic of China.

Where data processing outside the territory of People's Republic of China harms the national security, public interests, or the lawful rights and interests of individuals 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, the term "data" refers to any record of information in electronic or any other form.

"Data processing" includes the collection, storage, use, processing, transmission, provision, and disclosure of data, among others.

"Data security" refers to ensuring that data is effectively protected and lawfully used through adopting necessary measures, and to possessing the capacity to guarantee the continuous security of data.

Article 4 In preserving data security, the holistic approach to national security shall be adopted, sound data security governance systems shall be established, and data security and protection capabilities shall be improved.

Article 5 The central leading authority for national security shall be responsible for the decision-making, deliberation and coordination of the national data security work; researching, formulating, and guiding the implementation of the national data security strategy and related major guidelines and policies; coordinating major matters and important work in respect of national data security; and establishing a coordination mechanism for national data security.

Article 6 All localities and departments shall bear responsibility for the management of the data collected or generated in their work as well as for the data security thereof.

The competent departments of industry, telecommunications, transport, finance, natural resources, health, education, technology and other relevant competent departments shall assume the responsibilities of supervising and regulating data security in their respective trades and sectors.

Public security organs and national security organs, etc. shall assume the responsibilities of supervising and regulating data security within the scopes of

their respective duties in accordance with the provisions of this Law and other relevant laws and administrative regulations.

The national cyberspace affairs department shall be in charge of the overall planning and coordination of network data security and the related supervision and regulation in accordance with the provisions of this Law and other relevant laws and administrative regulations.

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

Article 8 Whoever processes data shall observe laws and regulations, respect social morality and ethics, observe business and professional ethics, uphold honesty and trustworthiness, fulfill data security protection obligations, and undertake social responsibilities; and shall not endanger national security and public interests, nor harm the lawful rights and interests of individuals and organizations.

Article 9 The state supports the dissemination and popularization of knowledge of data security to raise public awareness in this regard and ability to protect data security, and promotes the joint participation by relevant departments, industry organizations, research institutions, enterprises, and individuals in data security protection, so as to create a good environment for members of the whole society to jointly protect data, ensure data security and promote development of relevant industries.

Article 10 Relevant industry associations shall, in accordance with their articles of association, formulate the code of conduct and standards to ensure data security according to the law, strengthen self-regulation in their respective industries, guide members to strengthen data security protection, improve their protection level and promote the healthy development of the industries.

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

Article 12 Any individual or organization shall have the right to file complaints about or report violations of this Law to the competent departments. The departments receiving such complaints or reports shall deal with them in a timely manner in accordance with the law.

The competent departments shall keep confidential the relevant information of those making such complaints or reports, and protect their lawful rights and interests.

Chapter II
Data Security and Development

Article 13 The state shall make an overall plan to coordinate development and security, to promote data security through data development and utilization and through industrial development on one hand, and on the other hand, to ensure that data security facilitates data development and utilization as well as industrial development.

Article 14 The state shall implement the big data strategy, advance the construction of data infrastructure, and encourage and support the innovative application of data in all industries and fields.

People’s governments at or above the provincial level shall incorporate the development of digital economy into their national economic and social development plans, and formulate development plans for the digital economy as needed.

Article 15 The state supports development and utilization of data to render public services smarter. In providing smarter public services, the needs of the elderly and the disabled shall be taken into full account to avoid posing obstacles to their daily lives.

Article 16 The state supports research on development and utilization of data and on data security related technologies, encourages popularization and commercial innovation of technologies in the foregoing fields, and fosters and develops products and industrial systems for development and utilization of data and for data security.

Article 17 The state shall advance the forming of the standards for data development and the standards for data utilization technologies and data security. The department in charge of standardization under the State Council and other relevant departments under the State Council shall, within the scopes

of their respective duties and functions, organize the establishment of, and make revisions in due time to the standards for technologies and products for data development and data utilization and the standards for data security. The state shall support enterprises, social groups, and education or research institutions, etc. in their participation in the establishment of such standards.

Article 18 The state encourages the development of services such as data security testing, evaluation, and accreditation, and supports agencies specialized in data security testing, evaluation, accreditation, etc. to provide services according to the law.

The state supports collaboration among relevant departments, industry associations, enterprises, education and research institutions, relevant specialized agencies, etc. in the fields such as data security related risk assessment, prevention, and disposal .

Article 19 The state shall establish sound systems for data trading management, standardize data trading activities, and foster a data trading market.

Article 20 The state supports education and research institutions, enterprises, and other entities in carrying out education and training on technologies for data development and utilization and on data security, cultivates professionals in data development and utilization technologies and in data security by a variety of means, and promotes talent exchanges.

Chapter III
Data Security Systems

Article 21 The state shall establish a categorized and classified system and carry out data protection based on the importance of the data in economic and social development, as well as the extent of harm to national security, public interests, or the lawful rights and interests of individuals or organizations that will be caused once the data are altered, destroyed, leaked, or illegally obtained or used. The coordination mechanism for national data security shall coordinate the relevant departments to formulate a catalog of important data and strengthen protection of important data.

Data concerning national security, lifelines of the national economy, important aspects of people’s lives, major public interests, ect., are core data of the state, for which a stricter management system shall be implemented.

All localities and departments shall, in accordance with the categorized and

classified data protection system, prepare specific catalogs of important data for their respective regions, departments, and relevant industries and sectors, and give priority to the data listed in the catalogs in terms of data protection.

Article 22 The state shall establish a centralized, unified, highly effective, and authoritative mechanism for assessing, reporting, information sharing, monitoring, and early alert of data security risks. The coordinating mechanism for national data security shall make an overall plan on and coordinate relevant departments in strengthening the work about acquiring, analyzing, researching and evaluating information of data security risks and the work about early alert of such risks.

Article 23 The state shall establish a data security emergency response mechanism. Where a data security incident occurs, the relevant competent departments shall initiate emergency response in accordance with the plan and the law, take corresponding measures to prevent further harm and eliminate security hazards, and send out warnings to the public by publishing information relevant thereto in a timely manner.

Article 24 The state shall establish a review system for data security, conducting national security reviews of data processing that affects or may affect national security.

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

Article 25 The state shall apply export control in accordance with the law on data that are controlled items and concern national security and interests and the performance of international obligations.

Article 26 Where any country or region adopts discriminatory prohibitions, restrictions, or other similar measures against the People’s Republic of China in respect of investment, trade or any other field related to data and data development and utilization technologies, the People’s Republic of China may take countermeasures against that country or region in light of the actual circumstances.

Chapter IV
Data Security Protection Obligations

Article 27 In data processing, the laws and regulations shall be complied

with, a sound data security management system throughout the whole process shall be established, data security education and training shall be organized and conducted, and corresponding technical measures and other necessary measures shall be adopted to ensure data security. In data processing by making use of the internet or any other information networks, the abovementioned data security obligations shall be fulfilled on the basis of the classified protection system for cyber security.

Processors of important data shall be clear about their persons responsible for data security and the data security management bodies, and fulfill the responsibilities for data security.

Article 28 Data processing as well as research and development of new data technologies shall be conducive to furthering economic and social development, and improving the well-being of people, and shall conform to social morals and ethics.

Article 29 Closer risk monitoring shall be applied in data processing. Where data security defects, bugs, or other risks are discovered, remedial measures shall be taken immediately. Where a data security incident occurs, measures shall be taken immediately to address it, and users shall be notified and reports made to relevant competent departments in a timely manner in accordance with relevant provisions.

Article 30 Processors of important data shall, in accordance with the relevant provisions, conduct risk assessments of their data processing on a regular basis and submit risk assessment reports to relevant competent departments.

Risk assessment reports shall include the types and amounts of important data processed, information on data processing, data security risks and the response measures for them.

Article 31 The provisions of the Cyber Security Law of the People’s Republic of China shall apply to the outbound security management of the important data collected or produced by critical information infrastructure operators during their operation within the territory of the People’s Republic of China, and the measures for the outbound security management of the important data collected or produced by others data processors during their operation within the territory of the People’s Republic of China shall be formulated by the national cyberspace authority in conjunction with the relevant departments under the State Council.

Article 32 An organization or individual shall collect data by lawful and proper means, and shall not acquire data by theft or in other illegal manners.

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

Article 33 When providing services, data transaction intermediaries shall require data providers to specify the sources of the data, verify the identities of both parties to the transactions, and retain the verification and transaction records.

Article 34 Where laws or administrative regulations require that administrative permissions be acquired for providing services related to data processing, service providers shall obtain such administrative permissions in accordance with these provisions.

Article 35 Where a public security organ or national security organ needs to obtain data for the sake of national security or for investigating crimes in accordance with the law, strict approval formalities shall be completed in accordance with the relevant provisions of the state and data be obtained in accordance with the law, and the relevant organizations and individuals shall cooperate.

Article 36 The competent authorities of the People’s Republic of China shall handle requests for data made by foreign judicial or law enforcement authorities, in accordance with the relevant laws and international treaties or agreements concluded or acceded to by the People’s Republic of China, or in accordance with the principles of equality and reciprocity. Without the approval of the competent authorities of the People’s Republic of China, organizations or individuals in the People’s Republic of China shall not provide data stored within the territory of the People’s Republic of China to any overseas judicial or law enforcement body.

Chapter V
Security and Openness of Government Data

Article 37 The state shall make great efforts to promote the development of e-government, make government database more scientific, accurate, and

time-efficient, and improve the ability of using data to serve economic and social development.

Article 38 Where state organs need to collect or use data to perform their statutory duties, they shall collect or use data within the scope as needed for performance of their statutory duties and under the conditions and procedures provided by laws and administrative regulations. They shall, in accordance with the law, preserve the confidentiality of the data accessed in the course of performing their duties, such as personal privacy, personal information, trade secrets, and confidential business information, and shall not divulge such data or illegally provide them to others.

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

Article 40 Where a state organ entrusts others to construct or maintain e-government systems, or to store or process government data, the state organ shall go through strict approval procedures, and shall supervise the entrusted party in the performance of data security protection obligations. The entrusted party shall perform its data security protection obligations in accordance with the provisions of laws, regulations, and contracts signed, and shall not retain, use, divulge, or provide others with government data without authorization.

Article 41 State organs shall, under the principles of fairness, equality and convenience for the people, disclose government data in a timely and accurate manner in accordance with the provisions, except those which shall not be disclosed in accordance with the law.

Article 42 The state shall formulate the catalog of open government data, build an open, uniform, standardized, interconnected, safe and controllable government data platform, and promote the release and utilization of government data.

Article 43 The provisions of this Chapter shall apply to the data processing carried out by the organizations with the functions of administering public affairs as authorized by laws and regulations for the purpose of performing their statutory duties.

Chapter VI
Legal Liability

Article 44 Where competent departments discover the existence of major security risks in data processing when they perform their regulatory duties as regards data security, they may, in accordance with the prescribed limits of authority and procedures, conduct regulatory talks with the relevant organizations and/or individuals, and require the relevant organizations and/or individuals to adopt measures to make rectifications and eliminate potential hazards.

Article 45 Where an organization or individual that processes data fails to perform the data security protection obligations provided in Articles 27, 29 and 30 of this Law, the organization or individual shall be ordered to make rectifications and be given a warning, and may be concurrently fined not less than RMB 50,000 yuan but not more than RMB 500,000 yuan by the competent department, and the directly liable persons in charge and other directly liable persons may be fined not less than RMB 10,000 yuan but not more than RMB 100,000 yuan. Where the organization or individual refuses to make rectifications or has caused serious consequences such as a massive data breach, the organization or individual shall be fined not less than RMB 500,000 yuan but not more than RMB 2 million yuan, and may be ordered to suspend the relevant business or suspend operations for rectification, or have relevant business permits or the business license revoked, and the directly liable persons in charge and other directly liable persons shall be fined not less than RMB 50,000 yuan but not more than RMB 200,000 yuan.

Where the organization or individual violates the national core data management rules and endangers national sovereignty, security, or development interests of the state, the competent department shall impose upon the organization or individual a fine of not less than RMB 2 million yuan but not more than RMB 10 million yuan, and may, based on the circumstances, order a suspension of relevant business or a suspension of operations for rectification, or revoke relevant business permits or the business license. Where a crime is constituted, criminal responsibilities shall be investigated in accordance with the law.

Article 46 Whoever, in violation of the provisions of Article 31 of this Law, provides important data abroad, shall be ordered to make rectifications and be given a warning by the competent department, and may be concurrently fined not less than RMB 100,000 yuan but not more than RMB 1 million yuan,

and the directly liable persons in charge and other directly liable persons may be fined not less than RMB 10,000 yuan but not more than RMB 100,000 yuan. Where the circumstances are serious, the violator shall be fined not less than RMB 1 million but not more than RMB 10 million yuan, and may also be ordered to suspend the relevant business or suspend operations for rectification, or have relevant business permits or the business license revoked, and the directly liable persons in charge and other directly liable persons shall be fined not less than RMB 100,000 yuan but not more than RMB 1 million yuan.

Article 47 Where a data transaction intermediary fails to perform the obligations prescribed in Article 33 of this Law, it shall be ordered by the competent department to make rectifications, its illegal gains, if any, shall be confiscated, and it shall also be fined not less than the amount of but not more than ten times the amount of the illegal gains; if there are no illegal gains or the illegal gains are less than RMB 100,000 yuan, it shall be fined not less than RMB 100,000 yuan but not more than RMB 1 million yuan. It may be concurrently ordered to suspend the relevant business or suspend operations for rectification, or have relevant business permits or the business license revoked. The directly liable persons in charge and other directly liable persons shall be fined not less than RMB 10,000 yuan but not more than RMB 100,000 yuan.

Article 48 Whoever in violation of Article 35 of this Law, refuses to cooperate when a public organ or national security organ needs to access the data, shall be ordered by the competent department to make rectifications and be given a warning, and shall be concurrently fined not less than RMB 50,000 yuan but nor more than RMB 500,000 yuan, and the directly liable persons in charge and other directly liable persons may be fined not less than RMB 10,000 yuan but not more than RMB 100,000 yuan.

Whoever, in violation of Article 36 of this Law, provides data to an overseas judicial or law enforcement body without the approval of the competent authorities, shall be given a warning by the competent department, and may be concurrently fined not less than RMB 100,000 yuan but not more than RMB 1 million yuan, and the directly liable persons in charge and other directly liable persons may be fined not less than RMB 10,000 yuan but not more than RMB 100,000 yuan. If serious consequences are caused, the violator shall be fined not less than RMB 1 million yuan but not more than RMB 5 million yuan, and may be ordered to suspend the relevant business or suspend operations for rectification, or have relevant business permits or the business license revoked. The directly liable persons in charge and other directly liable persons shall be fined not less than RMB 50,000 yuan but not more than RMB

500,000 yuan.

Article 49 Where a state organ fails to perform data security obligations as provided for in this Law, the directly liable persons in charge and other directly liable persons shall be given a sanction in accordance with the law.

Article 50 Any state functionary performing data security related regulation regulation neglects his duty, abuses power, or engages in malpractice for personal gain, shall be given a sanction in accordance with the law.

Article 51 Whoever obtains data through theft or by any other illegal means, or eliminates or restricts competition in data processing, or harms the lawful rights and interests of individuals or organizations, shall be punished in accordance with the provisions of relevant laws and administrative regulations.

Article 52 Whoever, in violation of this Law, causes damages to others shall bear civil liability in accordance with the law.

Where a violation of the provisions of this Law constitutes a violation of public security administration, a public security administrative penalty shall be given in accordance with the law. Where a crime is constituted, criminal responsibility shall be investigated in accordance with the law.

Chapter VII
Supplementary Provisions

Article 53 The provisions of the Law of the People's Republic of China on Guarding State Secrets and other relevant laws and administrative regulations shall apply to data processing that involves state secrets.

The provisions of relevant laws and administrative regulations shall also be observed when data are processed in statistical or archival work and in data processing involving personal information.

Article 54 Measures for the military data security and protection shall be separately formulated by the Central Military Commission in accordance with this Law.

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

Source: Editor:

Tools: Save | Print | E-Mail

Related Topics