Data Security Law of the People's Republic of China [1]

Authority: **Standing Committee of the National People's Congress**

Document Number: No.84

Promulgation date: 10 June, 2021

Effective date:1 September, 2021

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

The Data Security Law of the People's Republic of China, as adopted at the 29th session 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 come into force 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 session of the Standing Committee of the Thirteenth National People's Congress on June 10, 2021)

Contents

[1] Translated by Health Law Asia – Pharmaceutical, Medical Device, and Cosmetics Law

Chapter I: General Provisions

Article 1

This Law is enacted for the purposes of regulating data processing activities, safeguarding data security, promoting data development and utilization, protecting the lawful rights and interests of individuals and organizations, and maintaining national sovereignty, security, and development interests.

Article 2

This Law shall apply to data processing activities and the security supervision thereof conducted within the territory of the People's Republic of China. Entities that conduct data processing activities outside the territory of the People's Republic of China to the detriment of national security, public interest, or the lawful rights and interests of citizens and organizations of the People's Republic of China shall be held legally liable in accordance with the law.

Article 3

For the purposes of this Law, "data" means any record of information in electronic or any other form. "Data processing" includes, but is not limited to, the collection, storage, use, processing, transmission, provision, and public disclosure of data. "Data security" means that necessary measures are taken to ensure the state of effective protection and lawful utilization of data and to maintain the capability to safeguard the continuing state of security.

Article 4

In the maintenance of data security, a holistic approach to national security shall be adhered to, a data security governance system shall be established and improved, and the capability to safeguard data security shall be enhanced.

Article 5

The central leading body for national security shall be responsible for coordinating policymaking and deliberations on national data security work, researching, developing, and

guiding the implementation of national data security strategies and relevant major guidelines and policies, conducting overall coordination of significant affairs and important tasks concerning national data security, and establishing a national data security work coordination mechanism.

Article 6

Each region or department shall be responsible for the data collected and generated in its work and for ensuring data security. Industrial sectors, including telecommunications, transportation, finance, natural resources, health, education, science and technology, and other departments shall undertake the duty to supervise data security within their respective industries and fields. Public security authorities and national security authorities, among others, shall, in accordance with the provisions of this Law and relevant laws and administrative regulations, undertake the duty to supervise data security within their respective purviews. The national cyberspace authority shall, in accordance with the provisions of this Law and relevant laws and administrative regulations, be responsible for conducting overall coordination of cyber data security and related supervisory work.

Article 7

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

Article 8

When conducting data processing activities, one shall comply with laws and regulations, respect social norms and ethics, observe business and professional ethics, act in good faith, perform data security protection obligations, and undertake social responsibilities, and shall neither compromise national security and public interest nor harm the lawful rights and interests of any organization or individual.

Article 9

The State shall support the publicity and dissemination of knowledge on data security, raise the awareness and level of data security protection in the whole society, and encourage relevant departments, industry organizations, scientific research institutions, enterprises, and individuals, among others, to jointly participate in data security protection work, so as to create a favorable environment for the whole society to jointly maintain data security and promote development.

Article 10

A relevant industry organization shall, in accordance with its articles of association, formulate a code of conduct and group standards for data security in conformity with the law, strengthen industry self-regulation, guide its members in enhancing data security protection, elevate the level of data security safeguards, and promote the sound and orderly development of the industry.

Article 11

The State shall proactively engage in international exchanges and cooperation in the fields of data security governance, data development and utilization, and other related areas, participate in the formulation of international rules and standards pertaining to data security, and promote the secure and unrestricted cross-border flow of data.

Article 12

Any individual or organization shall be entitled to lodge complaints or reports with the competent department regarding any violation of this Law. The department receiving such complaints or reports shall handle them promptly in accordance with the law. The competent department shall maintain the confidentiality of information concerning the complainant or reporting party and safeguard the lawful rights and interests of the complainant or reporting party.

Chapter II: Data Security and Development

Article 13

The State shall coordinate data development and security, and shall adhere to the principle of promoting data security in conjunction with data development and utilization as well as industry development, while safeguarding data development and utilization and industry development in conjunction with data security.

Article 14

The State shall implement a big data strategy, advance the construction of data infrastructure, and encourage and support the innovative application of data across various industries and sectors.

People's governments at or above the provincial level shall incorporate the development of the digital economy into the national economic and social development plan at the corresponding level, and shall formulate, as necessary, a comprehensive plan for the development of the digital economy.

Article 15

The State shall support the development and utilization of data to enhance the intelligence level of public services. In the provision of intelligent public services, due consideration shall be given to the needs of the elderly and persons with disabilities, so as to avoid creating obstacles to their daily lives.

Article 16

The State shall support technological research on data security and data development and utilization, encourage technological promotion and commercial innovation in the fields of data development and utilization as well as data security, and foster and develop product and industry systems pertaining to data development and utilization and data security.

Article 17

The State shall advance the construction of a standards system for data development and utilization technology and for data security. The standardization department of the State Council and other relevant departments of the State Council shall, within their respective jurisdictions, organize the formulation and timely revision of standards related to data development and utilization technologies and products, as well as data security. The State shall support enterprises, social organizations, and educational and scientific research institutions, among others, in participating in the formulation of such standards.

Article 18

The State shall promote the development of data security testing, assessment, certification, and other related services, and shall support professional institutions engaged in data security testing, assessment, certification, and other such activities to conduct their services in accordance with the law. The State shall support collaboration among relevant departments,

industry organizations, enterprises, educational and scientific research institutions, and other relevant professional bodies in the assessment, prevention, and handling, among other aspects, of data security risks.

Article 19

The State shall establish and improve a data trading management system, regulate the conduct of data trading, and cultivate and develop data trading markets.

Article 20

The State shall support educational and scientific research institutions, enterprises, and other relevant entities in providing education and training in data development and utilization technologies as well as data security, foster professionals in these fields through diverse means, and promote the exchange of talent.

Chapter III: Data Security Systems

Article 21

The State shall establish a categorized and hierarchical data protection system to provide protection based on the importance of data in economic and social development and the extent of harm that may result from data tampering, destruction, disclosure, or illegal acquisition or utilization affecting national security, public interest, or the lawful rights and interests of individuals and organizations. The national data security work coordination mechanism shall coordinate relevant departments in formulating a catalog of important data to strengthen the protection of such data. Data that is critical to national security, the lifeline of the national economy, essential aspects of people's livelihood, or material public interests shall constitute national core data and shall be subject to a more stringent management system. Each region or department shall, in accordance with the categorized and hierarchical data protection system, determine specific catalogs of important data within the region, department, or relevant industries and fields, and shall provide priority protection for data listed in such catalogs.

Article 22

The State shall establish a centralized, unified, efficient, and authoritative mechanism for data security risk assessment, reporting, information sharing, monitoring, and early warning. The national data security work coordination mechanism shall coordinate relevant departments in

strengthening efforts related to the acquisition, analysis, research, and evaluation of data security risk information, as well as the issuance of early warnings.

Article 23

The State shall establish a data security emergency response and management mechanism. Upon the occurrence of a data security event, the competent department shall, in accordance with the law, activate its emergency response plan, adopt corresponding emergency response and management measures, prevent the escalation of harm, eliminate potential security risks, and timely release to the public relevant warning information.

Article 24

The State shall establish a data security review system to conduct national security reviews of data processing activities that affect, or may affect, national security. Decisions rendered in accordance with law pursuant to such security reviews shall be final.

Article 25

The State shall implement export control in accordance with the law with respect to data that constitutes controlled items related to safeguarding national security and interests, and fulfilling international obligations.

Article 26

Where any country or region adopts discriminatory prohibitions, restrictions, or other analogous measures against the People's Republic of China in relation to investment, trade, data, or data development and utilization technology, the People's Republic of China may, based on the actual circumstances, adopt reciprocal measures against such country or region.

Chapter IV: Data Security Protection Obligations

Article 27

In the course of conducting data processing activities, any entity shall, in accordance with the provisions of laws and regulations, establish and improve a comprehensive data security management system, organize data security education and training, and adopt corresponding

technical measures and other necessary measures to safeguard data security. When conducting data processing activities via the Internet or any other information network, such entity shall fulfill the foregoing data security protection obligations in accordance with the hierarchical cybersecurity protection system. A processor of important data shall designate a person responsible for data security and establish a data security management body, and shall implement and enforce responsibilities for data security protection.

Article 28

Data processing activities and research and development of new data technologies shall be conducted in a manner that promotes economic and social development, enhances the well-being of the people, and complies with social norms and ethical standards.

Article 29

In the course of conducting data processing activities, entities shall strengthen risk monitoring. Upon discovering any data security defect, vulnerability, or other risk, they shall immediately adopt remedial measures; and upon the occurrence of a data security event, they shall immediately implement appropriate disposition measures, notify users, and report to the competent department in a timely manner as required.

Article 30

A processor of important data shall, as required, conduct regular risk assessments with respect to its data processing activities and submit risk assessment reports to the competent department.

Such risk assessment reports shall include information regarding the type and quantity of important data processed, the nature of data processing activities, data security risks encountered, and corresponding countermeasures.

Article 31

The security management of cross-border transfer of important data collected and generated by operators of key information infrastructure during their operations within the territory of the People's Republic of China shall be governed by the Cybersecurity Law of the People's Republic of China.

The measures governing the security management of cross-border transfer of important data collected and generated by other data processors during their operations within the territory

of the People's Republic of China shall be formulated by the national cyberspace authority in conjunction with the relevant departments of the State Council.

Article 32

Any organization or individual shall collect data by lawful and proper means and shall not steal or otherwise illegally acquire data. Where prescribed by laws and administrative regulations, data shall be collected and used solely for the purpose and within the scope so prescribed.

Article 33

An institution engaged in data trading intermediary services shall, in the course of providing such services, require the data provider to disclose the source of the data, verify the identity of both parties to the transaction, and maintain records of the verification and trading process.

Article 34

Where provision of data processing-related services requires the obtaining of an administrative license under any law or administrative regulation, the service provider shall obtain such license in accordance with the law.

Article 35

As necessary for safeguarding national security or investigating crimes, a public security authority or national security authority shall, in accordance with relevant state provisions and strictly following approval procedures, legally access data, and the relevant organizations and individuals shall provide necessary cooperation.

Article 36

The competent authority of the People's Republic of China shall process any request for data from a foreign judicial or law enforcement authority in accordance with relevant laws, or under international treaties and agreements to which the People's Republic of China is a party, or under the principle of equality and reciprocity. Without the approval of the competent authority of the People's Republic of China, no domestic organization or individual shall provide data stored within the territory of the People's Republic of China to any foreign judicial or law enforcement authority.

Chapter V: Security and Public Availability of Government Data

Article 37

The State shall vigorously promote the construction of e-government, improve the scientific rigor, accuracy, and timeliness of government data, and enhance the capability to utilize such data in serving economic and social development.

Article 38

A state authority shall, in performing its statutory duties, collect and use data in accordance with the conditions and procedures prescribed by laws and administrative regulations and only to the extent necessary for the fulfillment of its statutory functions. Such authority shall, in accordance with the law, maintain the confidentiality of individual privacy, personal information, trade secrets, confidential business information, and other data that comes to its knowledge, and shall not divulge or provide such data to others unlawfully.

Article 39

A state authority shall, in accordance with laws and administrative regulations, establish and improve a data security management system, enforce responsibilities for data security protection, and safeguard the security of government data.

Article 40

When commissioning others to construct or maintain an e-government system, or to store or process government data, a state authority shall comply with strict approval procedures and shall oversee the commissioned party's performance of corresponding data security protection obligations.

The commissioned party shall fulfill its data security protection obligations in accordance with the provisions of laws and regulations and as stipulated in contracts, and shall not retain, use, disclose, or provide government data to others without authorization.

Article 41

A state authority shall, in accordance with the principles of equity, fairness, and convenience for the public, publicly disclose government data in a timely and accurate manner as required, except where public disclosure is prohibited by law.

Article 42

The State shall formulate catalogs of open government data, establish uniform, standardized, interconnected, secure, and controllable platforms for the disclosure of government data, and promote the public availability and utilization of such data.

Article 43

Where an organization authorized by laws and regulations to manage public affairs conducts data processing activities for the performance of its statutory duties, the provisions of this Chapter shall apply.

Chapter VI: Legal Liability

Article 44

Where, in the performance of its duty to supervise data security, the competent department discovers that any data processing activities present a relatively significant security risk, it may, in accordance with its prescribed authority and procedures, interview the relevant organizations and individuals, and require such organizations and individuals to take corrective measures to address the issues and eliminate potential risks.

Article 45

Where an organization or individual conducting data processing activities fails to perform any of the data security protection obligations stipulated in Articles 27, 29, and 30 of this Law, the competent department shall order the violator to take corrective action and issue a warning, and may impose a fine of not less than 50,000 yuan and not more than 500,000 yuan on the violator, and a fine of not less than 10,000 yuan and not more than 100,000 yuan on any directly liable executive in charge or other directly liable person.

Where the violator refuses to take corrective action, or where serious consequences occur, such as the disclosure of a large amount of data, the competent department shall impose a fine of not less than 500,000 yuan and not more than 2,000,000 yuan on the violator, and may order suspension of the related business, suspension of business for overhaul, revocation of the

related business permit, or revocation of the business license, and impose a fine of not less than 50,000 yuan and not more than 200,000 yuan on any directly liable executive in charge or other directly liable person.

Where violations involve the national core data management system, thereby compromising national sovereignty, security, or development interests, the competent department shall impose a fine of not less than 2,000,000 yuan and not more than 10,000,000 yuan on the violator, and shall order suspension of the related business, suspension of business for overhaul, revocation of the related business permit, or revocation of the business license according to the circumstances. Where the violation constitutes a criminal offense, the offender shall be held criminally liable in accordance with the law.

Article 46

Where any important data is provided to any overseas recipient in violation of Article 31 of this Law, the competent department shall order the violator to take corrective action and issue a warning, and may impose a fine of not less than 100,000 yuan and not more than 1,000,000 yuan on the violator, and a fine of not less than 10,000 yuan and not more than 100,000 yuan on any directly liable executive in charge or other directly liable person. Where the circumstances are serious, the competent department shall impose a fine of not less than 1,000,000 yuan and not more than 10,000,000 yuan on the violator, and may order suspension of the related business, suspension of business for overhaul, revocation of the related business permit, or revocation of the business license, and impose a fine of not less than 100,000 yuan and not more than 1,000,000 yuan on any directly liable executive in charge or other directly liable person.

Article 47

Where an institution engaged in data trading intermediary services fails to perform the obligations prescribed under Article 33 of this Law, the competent department shall order the violator to take corrective action and impose a fine of not less than one times and not more than ten times the illegal income derived therefrom, which shall be confiscated. Where there is no illegal income, or the illegal income is less than 100,000 yuan, the competent department shall impose a fine of not less than 100,000 yuan and not more than 1,000,000 yuan, and may order suspension of the related business, suspension of business for overhaul, revocation of the related business permit, or revocation of the business license, and impose a fine of not less than 10,000 yuan and not more than 100,000 yuan on any directly liable executive in charge or other directly liable person.

Article 48

Where an entity refuses to provide cooperation in the access of data in violation of Article 35 of this Law, the competent department shall order the violator to take corrective action, issue a warning, and impose a fine of not less than 50,000 yuan and not more than 500,000 yuan on the violator, and a fine of not less than 10,000 yuan and not more than 100,000 yuan on any directly liable executive in charge or other directly liable person.

Where data is provided to a foreign judicial or law enforcement authority without the approval of the competent authority in violation of Article 36 of this Law, the competent department shall issue a warning to the violator, and may impose a fine of not less than 100,000 yuan and not more than 1,000,000 yuan on the violator, and a fine of not less than 10,000 yuan and not more than 100,000 yuan on any directly liable executive in charge or other directly liable person.
Where serious consequences arise, the competent department shall impose a fine of not less than 1,000,000 yuan and not more than 5,000,000 yuan on the violator, and may order suspension of the related business, suspension of business for overhaul, revocation of the related business permit, or revocation of the business license, and impose a fine of not less than 50,000 yuan and not more than 500,000 yuan on any directly liable executive in charge or other directly liable person.

Article 49

Where a state authority fails to perform its data security protection obligations under this Law, any directly liable official in charge or other directly liable person shall be subjected to disciplinary action in accordance with the law.

Article 50

A state employee responsible for supervising data security who neglects duty, abuses power, or falsifies information for personal gain shall be subjected to disciplinary action in accordance with the law.

Article 51

Where data is stolen or otherwise illegally obtained, or where data processing activities are conducted to preclude or restrict competition, or in a manner prejudicial to the lawful rights and interests of any individual or organization, the violator shall be subject to punishment in accordance with relevant laws and administrative regulations.

Article 52

Where any violation of this Law causes damage to another person, the violator shall bear civil liability in accordance with the law.

Where a violation of this Law constitutes a breach of public security administration, the violator shall be subject to administrative punishment in accordance with the law; and where the violation constitutes a criminal offense, the offender shall be held criminally liable in accordance with the law.

Chapter VII: Supplemental Provisions

Article 53

Where data processing activities involve any state secrets, the Law of the People's Republic of China on Guarding State Secrets and other relevant laws and administrative regulations shall apply.

Data processing activities conducted in statistical or archival work, or involving personal information, shall also comply with applicable laws and administrative regulations.

Article 54

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

Article 55

This Law shall come into force on September 1, 2021.