大成 DENTONS

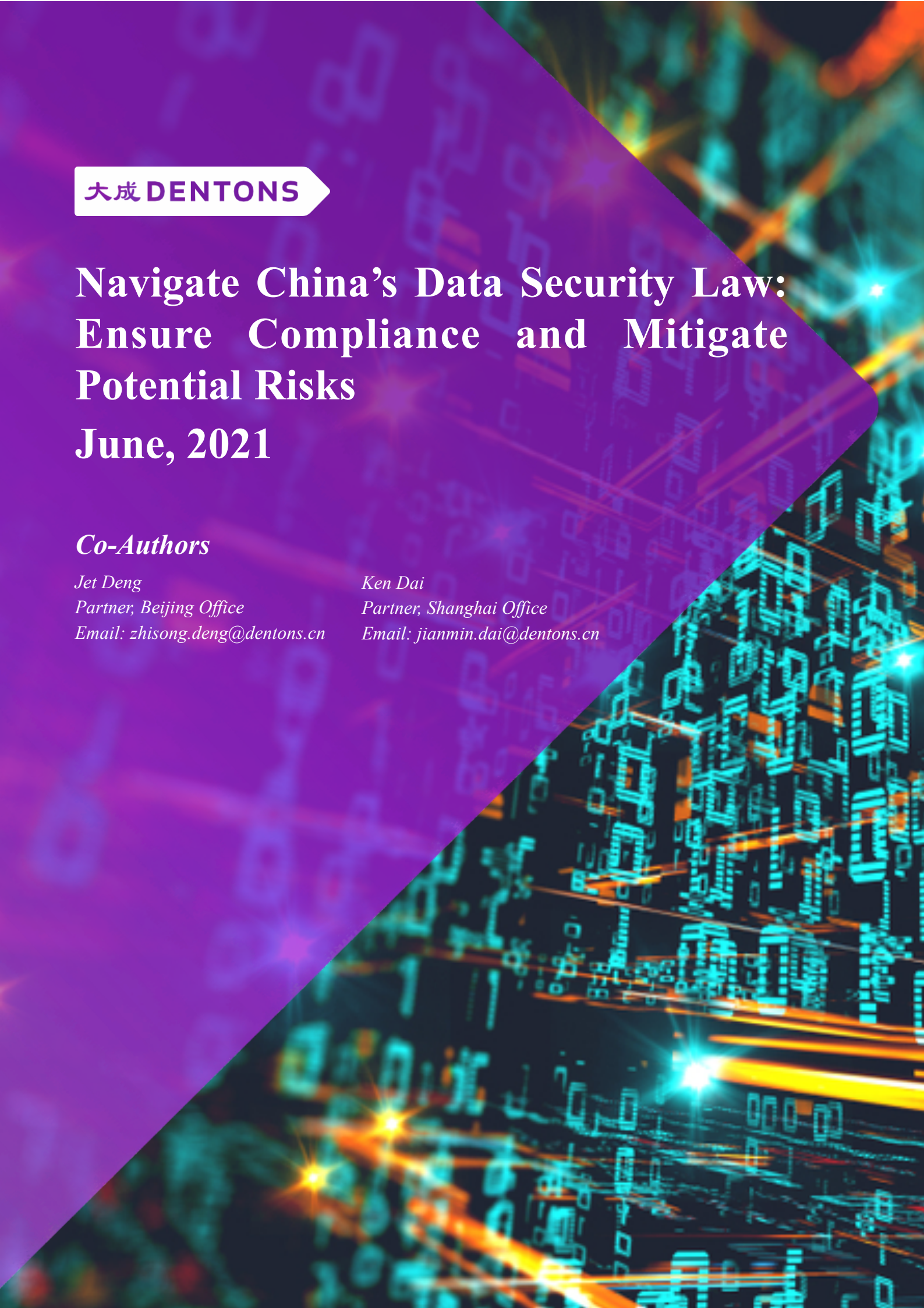
Navigate China's Data Security Law: Ensure Compliance and Mitigate Potential Risks

June, 2021

Co-Authors

Jet Deng
Partner, Beijing Office
Email: zhisong.deng@dentons.cn

Ken Dai
Partner, Shanghai Office
Email: jianmin.dai@dentons.cn



Content

Overview

China is to reach a new height in enhancing national security in data area. On June 10, 2021, China adopted the widely concerned *Data Security Law* (the "**DSL**") at the 29th Meeting of the Standing Committee of the 13th National People's Congress, China's top legislature.

The widely applicable DSL with extraterritorial effect clarifies the State's regulatory system for data security, requires data security protection obligations to be performed, and further increases the penalties based on the second draft of the DSL.

Considering that the DSL will come into effect as of September 1, 2021, during the short grace period, entities to which the law applies are suggested to establish the relevant compliance systems and perform data security protection obligations as required as soon as possible, in order to be prepared for the upcoming implementation of the new legislation.

This alert aims to provide a general picture of the DSL, and to discuss the possible impacts of this law on entities operating in China, as well as the highlights to be paid attention to when conducting data compliance in accordance with this law for kind reference.

I. Scope of Application

According to Article 2 of the DSL, the law applies to data processing activities and their security regulations carried out within the territory of China. Meanwhile, data processing activities carried out outside of the territory of China that harm the national security, public interests or lawful interests of citizens or organizations of China, will be held liable in accordance with the law.

This provision reflects the law's certain degree of extraterritorial application effect, which is consistent with the practice of countries around the world to extend their jurisdiction over data through legislation. That means, entities processing data outside of China may also be governed by this law.

Besides, under the DSL, "data" is broadly defined as any record of information in electronic or non-electronic form, and "data processing" widely includes activities such as collection, storage, use, refinery, transfer, provision and disclosure of data.

II. Enforcement Authorities

Similar to the regulation of personal information protection in China, data security is also regulated by multiple parties. On this basis, the DSL clarifies that the central national security leadership agency (namely the National Security Commission) is responsible for the decision-making and coordination of data security-related works; and other regulatory departments like the Cyberspace Administration of China and the Ministry of Public Security, competent authorities of industries like finance and healthcare, and local governments are responsible for the relevant regulation of data security within their respective scope of duties.

As the DSL does not change the current polycentric supervision on data security, but maintains such status quo to some extent, the data processing activities of an entity may be subject to multiple law enforcement authorities' regulations with different perspectives in practice.

III. Highlights for Data Security Compliance

The DSL creates a series of data security systems, including data categorization and classification, data security review, etc., and establishes a basic framework for data security. At the same time, this law puts forward some data security protection obligations for entities carrying out data processing activities, and stipulates penalties for violations to ensure that they are complied with. As such, for the relevant companies, it is suggested to pay attention to the following highlights when conducting compliance work in accordance with the law.

1. Data Categorization and Classification

Data categorization and classification is not a new concept, but has been mentioned in

several regulatory documents, such as the *Industrial Data Categorization and Classification Guide (Trial)* issued by the Ministry of Industry and Information Technology of China in 2020. The DSL reiterates it as a data security system.

Further, the DSL provides that data categorization and classification protection shall be implemented according to the level of importance to the State's economic and social development, as well as the degree of harm to the national security, social interests or lawful interests of citizens and organizations, if the data is tampered with, destroyed, leaked or illegally obtained or used.

According to the new law, a catalog of important data will be formulated at the national level, and each region and department will make specific catalogs of important data in their own region and department on this basis. The relevant entities shall be subject to the above-mentioned catalogs when categorizing and classifying data. For now, before the catalogs are released, it is recommended that the relevant companies could sort out and identify internal data at first, and prepare for the following categorization and classification work.

2. Important Data Protection

The DSL proposes to strengthen the protection of important data, which is generally understood as data closely related to national security, economic development, and social public interests; and puts forward the following special requirements for the processor of important data.

a) Responsible Person and Department for Data Security

The DSL requires that the processor of important data shall designate a person in charge and set up a management department, to fulfill data security protection responsibilities.

The law does not further elaborate on the duties and responsibilities of the person in charge and the management department. In addition, whether the person in charge of data security can concurrently serve as the person in charge of network security required by the *Cybersecurity Law* and the person in charge of personal information protection that may be required by the coming *Personal Information Protection Law* remains to be further clarified as well.

b) Risk Assessment

The processor of important data shall conduct risk assessment of its data processing activities regularly, and submit a risk assessment report to the competent authority according to the DSL. Such risk assessment report shall include the categories and quantities of important data processed, how data processing activities are conducted, and the potential data security risks and responding measures.

c) Cross-border Transfer of Important Data

The *Cybersecurity Law* has stipulated the requirements on the export of important data by critical information infrastructure operators ("**CIIOs**"). The DSL extends the restriction on the cross-border transfer of important data to general data processors, namely non-CIIOs. According to this law, the national cybersecurity and informatization department will take the lead to formulate the security management measures for important data export by non-CIIOs, which shall be highly concerned by the relevant entities, especially multinationals.

Notably, the *Hainan Free Trade Port Law*, which was approved on the same day as the DSL and took effect concurrently, proposes for the first time at the level of law that China supports Hainan Free Trade Port to explore and implement a regional international data flow system. It is speculated that the policies and regulations on cross-border transfer of data in free trade zones and ports in China may be more flexible in the future, therefore be more benefit for the relevant entities.

In addition, the DSL, puts forward a new concept of "national core data", which is defined as data related to national security, the lifeline of the national economy, important people's livelihood, and major public interests. Also, the law indicates that national core data shall be protected with a more stricter management system. However, the DSL does not elaborate in this regard, and further requirements remain to be clarified in the future.

3. Data Security Review

Pursuant to the DSL, China will establish data security review system, to review the data processing activities that affect or may affect national security. As no detailed rules

has been made in this regard, it is supposed that such system may share a similar idea to the existing cybersecurity review of China, which is conducted when CIIOs purchase network products or services that affect or may affect national security.

4. Export Control and Reciprocating Measures

In the context of the current international situation, China states in the DSL that it implements export control on data that constitutes controlled items, and imposes reciprocating measures against the countries and regions that adopt discriminatory prohibitions, restrictions or other similar measures against China. The above provisions are in line with China's *Export Control Law* promulgated in 2020 and the *Anti-foreign Sanctions Law* which was approved on the same day as the DSL and took effect on that day. As such, the relevant companies should pay great attention and make corresponding compliance arrangements in this regard.

5. MLPS-based Data Security Protection Obligations

The DSL requires entities carrying out data processing activities to perform data security protection obligations on the basis of the establishment of multi-level protection scheme ("**MLPS**"). Those obligations include setting up and improving data security management system across the entire workflow; organizing and conducting data security training, and adopting technical measures and other necessary measures to ensure data security.

MLPS is a system provided under the *Cybersecurity Law* that requires network operators to perform related obligations to protect network security and prevent data breach. The relevant entities need to file MLPS with the local public security organs in accordance with the relevant regulations and national standards. After the implementation of the DSL, it is expected that the enforcement activities against failing to file MLPS may increase accordingly.

6. Risk Monitoring and Security Incident Handling

Pursuant to the DSL, when carrying out data processing activities, entities shall strengthen risk monitoring, and immediately adopt remedial measures when data security defects and vulnerabilities are found. Meanwhile, when data security incidents

occur, entities shall promptly take responding measures, notify users and report to the competent authorities.

Obviously, the above provisions are similar to those regarding cybersecurity incident response mechanism provided under the *Cybersecurity Law*, and those regarding personal information breach response mechanism under the draft of the *Personal Information Protection Law*. As such, the relevant entities may establish a set of emergency plans to deal with different security incidents in the future.

7. Request for Data by Law Enforcement Organs in and outside China

Countries around the world are strengthening their own data sovereignty. China follows such trend and makes it clear in the DSL that, on one hand, the relevant organizations and individuals are obliged to cooperate with public security agencies and national security agencies' request for data for the purpose of maintaining national security or investigating crimes; on the other hand, organizations and individuals in China are not allowed to provide data stored within the territory of China to foreign judicial or law enforcement agencies without the approval of the competent authority.

In this regard, when the relevant entities participate in judicial procedures or confront administrative investigations outside of China, attentions shall be paid to abide by the relevant provisions and consider the requirements under the laws and regulations such as the *International Criminal Judicial Assistance La*w of China.

8. Data-related Anti-unfair Competition and Anti-monopoly

The final version of the DSL adds a new provision compared with the previous two drafts, according to which entities grabbing or illegally collecting data in other ways, or carrying out data processing activities that eliminate or restrict competition or damage the lawful rights and interests of individuals and organizations, shall be punished in accordance with the relevant laws and regulations.

In the era of Internet economy, platforms may use crawlers and other technical measures to access others' data, and Internet giants that have a large amount of data may use data combined with algorithms to gain competitive advantages. The above provisions mainly target illegal data crawling and abuse of data to restrict competition,

which is in line with and echoes the ideas and requirements under the *Anti-unfair Competition Law* and the *Anti-monopoly Law*, especially the *Anti-monopoly Guidelines on Platform Economy* newly released in February 2021.

IV. Legal Liabilities

For violations of data security protection obligations and other data security requirements, the DSL stipulates two-level legal liabilities based on the severity of circumstances, for both entities/individuals that violate the law and the directly responsible persons of the violators, as follows.

	Violations	**In General Circumstances**		**In Severe Circumstances**	
		Entities/ Individuals	**Responsible Persons**	**Entities/ Individuals**	**Responsible Persons**
Art. 45	Failing to perform data security protection obligations; failing to conduct risk monitoring and report incidents; (CIIOs) failing to conduct risk assessment and submit report	• Order to rectify • Warning • A fine ranging from CNY50,000 to CNY500,000 (about USD 78,150)	A fine ranging from CNY10,000 to CNY100,000 (about USD 15,630)	• Suspension of related business • Suspension for rectification • Revocation of business license • A fine ranging from CNY500,000 to CNY 2 million (about USD 312,600)	A fine ranging from CNY50,000 to CNY200,000 (about USD 31,260)
Art. 46	Failing to fulfill the requirements	• Order to	The same as	• Suspension of related	A fine ranging from

	regarding important data export	rectify • Warning • A fine ranging from CNY100,000 to CNY 1 million (about USD 156,300)	above	business • Suspension for rectification • Revocation of business license • A fine ranging from CNY 1 million to CNY 10 million (about USD 1.56 million)	CNY100,000 to CNY1 million
Art. 48	Failing to cooperate with Chinese agencies' request for data	• Order to rectify • Warning • A fine ranging from CNY50,000 to CNY500,000	The same as above	N/A	N/A
Art. 48	Providing data to foreign agencies without approval	• Order to rectify • Warning • A fine ranging from CNY100,000 to CNY 1 million	The same as above	• Suspension of related business • Suspension for rectification • Revocation of business license	A fine ranging from CNY50,000 to CNY500,000 (about USD 78,150)

				• A fine ranging from CNY 1 million to CNY 5 million (about USD 781,500)	

Notably, the DSL also provides that where the national core data management system is violated, and national sovereignty, security and development interests are endangered, the violator shall be fined up to CNY10 million (about USD 1.56 million), and imposed penalties such as suspension of related business, suspension for rectification, and revocation of business license.

Besides, it is specified in the DSL that, any violation of this law that constitutes a crime, shall be investigated in accordance with the criminal law, and if damage is caused to others, civil liability shall be borne correspondingly.

V. Conclusion and Looking Forward

As mentioned above, the grace period of the DSL is less than three months, the relevant entities are suggested to start or at least prepare for compliance work as quickly as possible, including but not limited to conducting data categorization and classification, establishing important data/core data protection systems, and fulfilling data security protection obligations. Meanwhile, given that many provisions under the DSL remain to be further clarified and detailed, close attention should be paid to the promulgation of supporting rules and measures as well.

After the implementation of the DSL, it is expected that the law enforcement activities based on this law will be carried out and gradually normalized, so the relevant entities may face more risks in their business operations. On the other hand, the DSL states that China establishes and improves data transaction management system and cultivates data transaction markets, entities may, in this regard, usher in opportunities and development in the coming future.

Appendix: Data Security Law of the People's Republic of China

Chapter I General Provisions	**第一章 总则**
Article 1 This Law is promulgated in order to regulate data processing activities, ensure data security, promote data development and use, protect the lawful rights and interests of individuals and organizations, and safeguard national sovereignty, security, and development interests.	**第一条** 为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。
Article 2 This Law applies to data processing activities and their security regulations carried out within the territory of the People's Republic of China. Data processing activities carried out outside of the territory of the People's Republic of China that harm the national security, the public interests, or the lawful interests of citizens or organizations of the People's Republic of China, will be held liable in accordance with law.	**第二条** 在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。 在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。
Article 3 "Data" as mentioned in this Law, refers to any record of information in electronic or non-electronic form. "Data processing" include activities such as the collection, storage, use, refinery, transfer, provision, or public disclosure of the data. "Data security" refers to the ability to ensure that data remains in the condition of being effectively protected and lawfully used, and to safeguard data remaining in a continually secure state through adopting necessary measures.	**第三条** 本法所称数据，是指任何以电子或者非电子形式对信息的记录。 数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。 数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。
Article 4 To ensure data security, the holistic view of national security shall be upheld,	**第四条** 维护数据安全，应当坚持总体国家安全观，建立健全数据安全

data security governance systems shall be established and completed, and data security protection capabilities shall be increased.	治理体系，提高数据安全保障能力。
Article 5 The leading central national security agency is responsible for the decision making and coordination related to national data security works. The agency researches, drafts, and guides the implementation of national data security strategies and related major policies and plans；it also coordinates major issues and important tasks of national data security and establishes a National Data Security Coordination Mechanism.	**第五条** 中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。
Article 6 Each region and department bears primary responsibility for the data security and the data created and collected through the work of that region or department. Regulatory departments such as industry, telecommunications, transportation, finance, natural resources, public health, education, scientific technology, and finance are responsible for the regulation of data security in their respective industries or sectors. The public security agency and national security agency are responsible for the regulation of data security within their respective scope of duties in accordance with this Law, other relevant laws and administrative regulations. The state cyberspace administration is responsible for the comprehensive coordination and relevant regulation of data security in accordance with this Law, other relevant laws and administrative regulations.	**第六条**各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。 工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。 公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。 国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。
Article 7 The State protects the data-related rights of individuals	**第七条** 国家保护个人、组织与数据有关的权益，鼓励数据依法合理有

and organizations; encourages lawful, reasonable, and effective use of data; ensures the lawful and orderly free flow of data; and promotes the development of the digital economy with data as a key factor.	效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。
Article 8 Entities carrying out data processing activities shall comply with laws and regulations, respect morals and ethics, comply with commercial and professional ethics, be honest and responsible, fulfill data security protection obligations, and undertake social responsibilities. It is prohibited to harm national security interests, public interests, or the lawful rights and interests of individuals and organizations.	**第八条** 开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。
Article 9 The State supports the promotion and popularization of data security knowledge to improve the awareness and level of data security protection; promotes relevant departments, sectoral organizations, enterprises, and individuals to jointly participate in data security protection work, and; creates a beneficial environment in which the whole society jointly safeguards data security and promotes development.	**第九条** 国家支持开展数据安全知识宣传普及，提高全社会的数据安全保护意识和水平，推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全和促进发展的良好环境。
Article 10 Relevant industry organizations may formulate codes of conducts and organization standards for data security by laws; strengthen self-regulation within respective industries; guide member entities to improve data security protection; enhance data security protection standard; and promote the healthy development of the industry.	**第十条** 相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。
Article 11 The state actively carries out international exchanges and cooperation in the fields of data security governance, data	**第十一条** 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国

development and utilization; participates in the formulation of international rules and standards related to data security, and promotes the safe and free flow of data across borders.	际规则和标准的制定，促进数据跨境安全、自由流动。
Article 12 Any individual or organization has the right to file a complaint about or report acts violating the provisions of this Law to departments responsible for data security duties. The departments receiving complaints or reports shall handle them in a timely manner and in accordance with law.	**第十二条** 任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。 有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。
Chapter II Data Security and Development	**第二章 数据安全与发展**
Article 13 The State makes overall planning of the development and security; promoting data security through data development and use as well as through industrial development and ensuring data development and use as well as industrial development through data security.	**第十三条** 国家统筹发展和安全，以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。
Article 14 The State implements 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 provincial level or above shall incorporate digital economy development into their economic and social development plans, and stipulate digital economy development plan according to their needs.	**第十四条** 国家实施大数据战略，推进数据基础设施建设， 鼓励和支持数据在各行业、各领域的创新应用。 省级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划，并根据需要制定数字经济发展规划。
Article 15 The State supports the development and utilization of data to improve the level of intelligence in public services. The needs of the elderly and the disabled should be fully	**第十五条** 国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑老

considered, and intelligent public services should be provided to them to avoid obstacles to the daily lives.	年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。
Article 16 The State supports research on data development and use as well as data security technologies; encourages the dissemination and commercial innovation of technologies in areas such as data development and use, data security; and fosters and develops products and industrial systems for data development and use, and for data security.	**第十六条** 国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。
Article 17 The State promotes the construction of data development and use technology and data security standards systems. The administrative department for standardization of the State Council and relevant departments of the State Council shall organize the stipulation and timely revision of standards concerning data development and use technologies and products and data security standards, according to their respective duties and responsibilities. The State supports entities such as enterprises, society organizations, as well as education and scientific research institutions, to participate in the formulation of standards.	**第十七条** 国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。
Article 18 The State promotes the development of services such as data security assessment, and certification. It supports professional institutions to provide services such as data security assessment, and certification in accordance with law. The State supports relevant departments, industry organizations, enterprises, education and scientific research institutions, and professional institutions to collaborate in the assessment, prevention, and disposal of data security risk.	**第十八条** 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。 国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

Article 19 The State establishes and completes data trading management systems, standardizes data trading activities, and cultivates a data trading market.	**第十九条** 国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。
Article 20 The State supports entities such as education, scientific research institutions and enterprises to develop education and training in data development and use technologies and data security, to adopt various methods to train talents in data development and use technologies and data security, to promote talents exchange.	**第二十条** 国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。
Chapter III Data Security Systems	**第三章 数据安全制度**
Article 21 The State shall establish a data categorization and classification protection system, implement data categorization and classification protection, according to the level of importance to the State's economic and social development, as well as the degree of damages to the national security, social interests or the lawful interests of citizens and organizations, if the data is tampered, damaged, leaked or illegally obtained or used. The State shall stipulate the important data catalogue and The National Data Security Coordination Mechanism coordinates relevant departments to develop an important data catalogues; strengthen the protection of important data. The data related to national security, the lifeblood of the national economy, people's wellbeing, and public interests is categorized as the national core data, which needs to be implemented with a stricter management system. Each region and department, shall stipulate a regional, departmental, as well as relevant industrial and sectoral important	**第二十一条** 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者公民、组织合法权益造成的危害程度，对数据实行分类分级保护。– 国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。 各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

data specified catalogue, according to the data categorization and classification protection system, and shall undertake special protections for data listed in the catalog.	
Article 22 The State establishes a centralized, efficient, and authoritative mechanism for data security risk assessment, reporting, information sharing, supervision, and warning. The National Data Security Coordination Mechanism coordinates relevant departments to strengthen work on data security risk information acquisition, analysis, determination, and warning.	**第二十二条** 国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。
Article 23 The State establishes a data security emergency response mechanism. In the event of a data security incident, departments responsible for data security duties shall implement the emergency plan, adopt appropriate emergency response measures, prevent expansion of harms, eliminate security risks, and publicly release warning information relevant to the public in accordance with laws	**第二十三条** 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。
Article 24 The State establishes a data security review system, and conducts national security review on data processing activities that affect or may affect national security. Security review decisions issued in accordance with laws are final decisions.	**第二十四条** 国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。依法作出的安全审查决定为最终决定。
Article 25 The State imposes export controls on types of data which are controlled items and related to the protection of national security and interests, as well as the fulfillment of international obligations in accordance with law.	**第二十五条** 国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

Article 26 For any country or region that adopts discriminatory prohibitions, limitations or other similar measures against the People's Republic of China with respect to matters such as investment or trade related to data, data development and use technology, the People's Republic of China may adopt measures reciprocally toward that country or region according to the actual circumstances.	**第二十六条** 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。
Chapter IV Data Security Protection Responsibilities	**第四章 数据安全保护义务**
Article 27 Entities carrying out data processing activities shall establish and complete a data security management system across the entire workflow, organize and conduct data security training, and adopt corresponding technical measures and other necessary measures to safeguard data security in accordance with laws and regulations. When using the Internet and other information networks to carry out data processing activities, they should perform the above-mentioned data security protection obligations, based on the network security level protection system. Entities processing important data shall designate a data security officer and set up a management office, to fulfill data security protection responsibilities.	**第二十七条** 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。 重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。
Article 28 Entities carrying out data processing activities as well as researching and developing new data technologies, shall benefit the economic and social development, enhance people's welfare, and conform with morals and ethics.	**第二十八条** 开展数据处理活动以及研究开发数据新技术， 应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

Article 29 Entities carrying out data processing activities shall strengthen risk monitoring. Where entities discover risks such as data security defects or leaks, they shall immediately adopt remedial measures; when data security incidents occur, entities shall immediately take responding measures, promptly notify users and report to the regulatory departments according to regulations.	**第二十九条** 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。
Article 30 Entities processing important data shall periodically conduct risk assessments of their data processing activities, and submit a risk assessment report to departments responsible for data security duties in accordance with regulations. The risk assessment report shall include content such as: the categories and quantities of important data processed by entities; how data processing activities are conducted; and the data security risks and responding measures.	**第三十条** 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。
Article 31 The cross-border transfer of important data collected and generated in the operation by the operator of the Critical Information Infrastructure within the territory of the People's Republic of China shall follow the requirements under the Cybersecurity Law of the People's Republic of China; the cross-border transfer of important data collected and generated in the operation by other data processing entities within the People's Republic of China shall follow the rules to be formulated by State Cyberspace Administration and relevant departments of the State Council.	**第三十一条** 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。
Article 32 All organizations and individuals collecting data shall adopt lawful and justified methods; they shall not steal or obtain data by other illegal means.	**第三十二条** 任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

Where laws and administrative regulations contain requirements 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 laws and administrative regulations.	法律、行政法规对收集、使用数据的目的、范围有规定的， 应当在法律、行政法规规定的目的和范围内收集、使用数据。
Article 33 When providing data trading intermediary services, intermediary agency shall require data providers to explain the source of the data, examine and verify the identity of both parties, and retain review and transaction records.	**第三十三条** 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。
Article 34 If laws or administration regulations require a data processing related service to obtain an administrative license, the service provider shall obtain the license in accordance with laws.	**第三十四条** 法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。
Article 35 Where the public security agency and national security agency need to access data for safeguarding national security or investigating crimes, they shall follow strict approval procedures and proceed in accordance with relevant law and state regulations; relevant organizations and individuals shall cooperate with them.	**第三十五条** 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。
Article 36 The competent authorities of the People's Republic of China shall handle requests for data provision by foreign judicial or law enforcement agencies in accordance with relevant laws and international treaties and agreements concluded or acceded by the People's Republic of China, or in accordance with the principle of equality and reciprocity. Where foreign judicial or law enforcement organs request for data stored within the territory of the People's Republic of China, organizations and	**第三十六条** 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

individuals within China are prohibited to provide them with the data unless competent authorities of the People's Republic of China have issued approval.	
Chapter V Government Data Security and Openness	**第五章 政务数据安全与开放**
Article 37 The State promotes the construction of e-government, increases the scientific nature, accuracy, and efficacy of government data, and enhances capabilities to use data to serve economic and social development.	**第三十七条** 国家大力推进电子政务建设，提高政务数据的科学性、准确性、时效性，提升运用数据服务经济社会发展的能力。
Article 38 Where State agencies need to collect or use data to fulfill their legal duties, they shall proceed within the scope of their legal duties and shall follow conditions and procedures provided in laws and administrative regulations; they shall keep personal privacy, personal information, business secrets, confidential business information and other data confidential in accordance with the law, and shall not disclose or illegally provide them to others in the process of performing their duties.	**第三十八条** 国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。
Article 39 State agencies shall, establish and complete data security management systems, distribute data security protection responsibilities, and ensure the security of government data, in accordance with requirements in laws and administrative regulations.	**第三十九条** 国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。
Article 40 Where State agencies entrust others to set up or maintain electronic government management systems, retain or process government data, the State agencies shall	**第四十条** 国家机关委托他人建设、维护电子政务系统， 存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应

undergo strict approval procedures, and shall supervise the entrusted party to fulfill corresponding data security protection obligations. The entrusted party shall perform its data security protection obligations in accordance with the laws and regulations and contractual agreements, and shall not retain, use, disclose or provide government affairs data to others without authorization.	的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。
Article 41 State agencies shall be fair and impartial. They shall provide convenient services to citizens, publishing government data accurately in a timely manner in accordance with regulations, except where the law prohibits such public disclosure.	**第四十一条** 国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。
Article 42 The State stipulates government data openness catalogs; builds a uniform and standardized, interconnected and interactive, secure and controllable government data public platform; and promotes the public use of government data.	**第四十二条** 国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。
Article 43 Organizations that have duties to manage public affairs as authorized by laws and regulations shall comply with requirements under this Chapter, when they carry out data processing activities to fulfill their legal obligations.	**第四十三条** 法律、法规授权的具有管理公共事务职能的组织为履行法定职责开展数据处理活动，适用本章规定。
Chapter VI Legal Liability	**第六章 法律责任**
Article 44 When departments performing data security duties, in the course of performing their duties, discover relatively high risk exists resulting from data processing activities, they may interview relevant organizations and	**第四十四条** 有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈。并要求有关组

individuals. They shall ask the relevant organizations and individuals to adopt measures in accordance with the requirements to correct and eliminate the risk.	织、个人采取措施进行整改，消除隐患。
Article 45 For organizations and individuals carrying out data processing activities that do not perform data security protection obligations as required by Articles 27, 29, and 30 of this Law, departments performing data security duties may order corrections, issue warning, and may also impose a fine of more than 50,000 yuan and less than 500,000 yuan; the direct responsible person in charge and other directly responsible persons shall be subject to a fine of more than 10,000 yuan and less than 100,000 yuan; those who refuse to make corrections or create serious consequences such as the leakage of large amount of data are subject to a fine of more than 500,000 yuan and less than 2,000,000 yuan, and may be ordered to suspend relevant businesses, close businesses and take corrective actions, as well as revoke relevant business licenses or business licenses; under this circumstance, the directly responsible person in charge and other person directly responsible shall be subject to a fine of more than 50,000 yuan and less than 200,000 yuan. Where an individual or organization violates the national core data management system and endangers national sovereignty, security and development interests, they may be subject to a fine of more than 2,000,000 yuan and less than 10,000,000 yuan, and can be ordered to suspend related businesses, suspend business for rectification, and revoke relevant business permits or business licenses; if a crime is constituted, criminal liability shall be pursued in accordance with the law.	**第四十五条** 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。 违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

Article 46 Where individuals or organizations violate the provisions of Article 31 of this Law and provide important data abroad, they will be ordered to make corrections by departments responsible for data security duties, be warned, and may be subject to a fine of more than 100,000 yuan and less than 1,000,000 yuan. Direct responsible person in charge and other directly responsible person may be subject to a fine of more than 10,000 yuan and less than 100,000 yuan; if the circumstances are serious, they can be fined 1,000,000 yuan to 10,000,000 yuan, and can be ordered to suspend related businesses, suspend business for rectification, and revoke relevant business permits or business licenses, and the directly responsible person in charge and other directly responsible persons shall be fined 100,000 yuan up to 1,000,000 yuan.	**第四十六条** 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。
Article 47 For data trading intermediary agencies that fail to fulfill obligations under Article 33 of this Law, departments performing data security duties may order corrections, confiscate any illegal gains, and impose a fine of more than 1 time and less than 10 times the amount of the illegal gains; in case there is no illegal gains or the illegal gains are less than 100,000 yuan, intermediary agencies are subject to a fine of more than 100,000 yuan and less than 1,000,000 yuan, and may be ordered to suspend relevant businesses, close businesses and take corrective actions, as well as revoke relevant business permits or business licenses. The direct responsible person in charge and other directly responsible person are subject to a fine of more than 10,000 yuan and less than 100,000 yuan.	**第四十七条** 从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款， 没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。
Article 48 Where individuals or organizations violate any requirements under Article 35 of	**第四十八条** 违反本法第三十五条规定，拒不配合数据调取的，由有

this Law and do not assist with the request for data, they will be ordered to make corrections by departments responsible for data security duties, be warned, and may be subject to a fine of more than 50,000 yuan and less than 500,000 yuan. Direct responsible person in charge and other directly responsible person may be subject to a fine of more than 10,000 yuan and less than 100,000 yuan. Where individuals or organizations violate requirements under Article 36 of this Law and provide data to foreign judicial or law enforcement organs without obtaining approval from competent authorities, departments performing data security duties may issue warnings and may impose a fine of more than 100,000 yuan and less than 1,000,000 yuan; directly responsible person in charge and other directly responsible person may be subject to a fine of more than 10,000 yuan and less than 100,000 yuan; if the circumstances are serious, they can be fined more than 10,000 yuan and less than 100,000 yuan and can be ordered to suspend related businesses, suspend business for rectification, and revoke relevant business permits or business licenses, and the directly responsible person in charge and other directly responsible persons shall be fined more than 50,000 yuan and less than 500,000 yuan.	关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款。 违反本法第三十六条规定，未经主管机关批准向境外的司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。
Article 49 If State agencies do not fulfill data security protection obligations under this Law, responsible person in charge and other directly responsible person will be punished according to law.	**第四十九条** 国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。
Article 50 If officers at departments performing data security duties neglect their duty, abuse their power, or abuse their position for private gain,	**第五十条** 履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。

they shall be punished in accordance with the law.	
Article 51 Stealing or obtaining data in other illegal ways, entities that exclude or restrict competitions, or harm the lawful rights and interests of individuals or organizations by carrying out data processing activities shall be punished in accordance with relevant laws and administrative regulations.	**第五十一条** 窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。
Article 50 Entities violating requirements under this Law and harming other individuals shall assume civil liability in accordance with law. If the violation of this Law constitutes a violation of public security administrative rules, entities shall be penalized according to public security administrative rules. If the violation constitutes a crime, entities shall assume the criminal liability in accordance with law.	**第五十二条** 违反本法规定，给他人造成损害的，依法承担民事责任。 违反本法规定，构成违反治安管理处罚行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。
Chapter VII Supplementary Provisions	**第七章 附则**
Article 53 Where carrying out data processing activities involving state secrets, laws and administrative regulations such as the "Law of the People's Republic of China on Guarding State Secrets" are applicable. Those carrying out data activities involving personal information and data processing activities in statistics and archival work, shall abide by personal information protection laws and administrative regulations.	**第五十三条** 开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。 在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，应当遵守个人信息保护法律、行政法规的规定。

Article 54 Measures for protecting military data are drafted separately by the Central Military Commission in accordance with this Law.	**第五十四条** 军事数据安全保护的办法，由中央军事委员会依据本法另行制定。
Article 55 This Law shall be effective since September 1, 2021.	**第五十五条** 本法自 2021 年 9 月 1 日起施行。