

## China Insight



# PRC Promulgated Data Security Law

Dear Sir or Madam,

On 10 June 2021, the Standing Committee of the National People's Congress adopted the *PRC Data Security Law* ("DSL"). It will take effect on 1 September 2021. The DSL is a fundamental piece of legislation on data security in China. It sets up a series of basic legal rules in the field of data, laying the foundation for Chinese data security management and protection, data circulation and application. Please find below an overview on the DSL.

Kind regards,

**CMS, China**

The Standing Committee of the National People's Congress on 10 June 2021 adopted the *PRC Data Security Law* ("DSL"). It will take effect on 1 September 2021.

## 1. Background

The DSL is a fundamental piece of legislation on data security in China. It sets up a series of basic legal rules in the field of data, laying the foundation for Chinese data security management and protection, data circulation and application. Together with the *PRC Cybersecurity Law* ("CSL") effective as of 1 June 2017 and the *PRC Personal Information Protection Law* ("PIPL"), of which the second draft is now under review by the Standing Committee of the National People's Congress, it will establish a complete legal system in the data and information field. The first draft of the DSL was published for comments on 3 July 2020 and the second draft of the DSL was published for comments on 29 April 2021. On 10 June 2021, the DSL was finally adopted.

## 2. Key Aspects in the DSL

The DSL covers the following key aspects:

- Application scope of the DSL;
- Classified and graded data protection system;
- Data security protection obligations;
- Restrictions on cross-border transmission of data; and
- Liabilities for violation of the DSL.

## 3. Application Scope of the DSL

### a) Definition of data and data handling

Before the promulgation of the DSL, there was no legislative definition of general data. The CSL only defines and regulates "network data", which refers to all kinds of electronic data collected, stored, transmitted, processed and generated through network, as well as "personal information", which refers to various information which is recorded in electronic or any other form and used alone or in combination with other information to recognize the identity of a natural person. As specific legislation regarding data security, the DSL aims to regulate all kinds of data and data handling activities. Article 2 of the DSL specifies that the DSL

shall apply to all data handling activities carried out within the territory of the People's Republic of China ("PRC") as well as the security regulation thereof. Further, Article 3 of the DSL provides that "data" under the DSL shall refer to any record of information in electronic or other forms, which means that non-electronic data are also subject to regulation under the DSL. Article 3 of the DSL further provides that "data handling" refers to the collection, storage, use, processing, transmission, provision, and disclosure of data, and, thus, covers the whole data life cycle.

b) Extraterritorial jurisdiction under the DSL

Article 2 of the DSL empowers the PRC with extraterritorial jurisdiction over data handling activities to some degree. It provides that data handling activities carried out outside the territory of the PRC will be subject to legal liabilities in accordance with the law, if they harm the national security, public interests, or the legitimate rights and interests of citizens or organizations of the PRC.

#### 4. Classified and Graded Data Protection System

a) Establishment of classified and graded data protection system

The concept of classified and graded data protection has already been incorporated in several regulations or industrial standards in specific areas previously. Examples are *JR/T 0158—2018 Data Classification Guidelines for Securities and Futures Industry* from 27 September 2018, and *Guidelines for Classification and Grading of Industrial Data (Trial)* from 27 February 2020, etc. With the promulgation of the DSL, for the first time, the classified and graded data protection system is established at the level of national law. Article 21 of the DSL stipulates that the State shall establish a classified and graded data protection system and carry out classified and graded data protection in accordance with the importance of data to economic and social development, and the damage to national security, public interests, or the legitimate rights and interests of individuals or organizations in the event that data are tampered with, destroyed, leaked, or illegally obtained or used.

b) Formulation of important data catalogues

In order to implement the classified and graded data protection system, the DSL also suggests formulating catalogues of important data as practical guidance.

At the national level, Article 21 of the DSL stipulates that the national data security coordination mechanism to be established by the National Security Commission shall make overall planning for and coordinate relevant departments in formulating the important data catalogues and strengthening the protection of important data. At the regional and sectoral level, it stipulates that each region and department shall further determine catalogues of specific important data in relevant industries and areas for the respective region and department, and undertake special protection for the data included in such catalogues.

Important data is not a new terminology. But until now, there was no definition of "important data" in any effective laws and regulations. The *Measures for Security Assessment of Outbound Transmission of Personal Information and Important Data* (a consultation draft issued on 11 April 2017, not effective yet, the "Draft Measures") defines that "important data" refers to the data closely related to national security, economic development, and social and public interests, and its specific scope shall be referred to relevant national standards and important data identification guidelines. Further, the national standard *Information Security Technology-Guidelines for Data Cross-Border Transfer Security Assessment* (a consultation draft issued on 25 August 2017, not effective yet, the "Guidelines") defines "important data" to be the data collected and generated in the PRC, not related to State secrets, but closely related to national security, economic development and public interest, including raw and derived data. The Guidelines specify the key industries which may involve important data, such as finance, food and drug, nuclear facilities, electricity, etc., and provide detailed reference for determination of important data in different industries. However, neither the Draft Measures nor the Guidelines have taken effect yet. With the formulation of important data catalogues at the national, regional and sectoral levels pursuant to the DSL, the definition and classification of important data will be ascertained and clarified in the future.

c) Introduction of core data of the State

In addition, Article 21 of the DSL introduces a new definition of "core data of the State", which has not been mentioned in the previous drafts of the DSL. Core data of the State are defined as data related to national security, the lifelines of national economy, people's key livelihood and major public interests. They shall be subject to stricter management system. The DSL does not elaborate on what items such stricter management system consists of. Thus, this remains to be determined in future legislation.

#### 5. Data Security Protection Obligations

a) General obligations for data handling

Article 27 of the DSL stipulates general obligations for conducting data handling activities. Those who conduct data handling activities shall establish and perfect a data security management system across the entire workflow, organize and conduct data security education and training, and adopt the corresponding technical measures and other necessary measures to ensure data security in accordance with laws and regulations. If the data handling activities are conducted via the internet or other information networks, the aforesaid data security protection obligations shall be performed based on the graded cybersecurity protection system as specified in the CSL. In addition, those who handle important data shall clearly specify responsible personnel and management institutes for data security and fully implement data security protection responsibilities.

Article 29 of the DSL requires those who conduct data handling activities to strengthen risk monitoring. When risks, such as data security flaws and vulnerabilities, are discovered, remedial measures shall be adopted immediately. In the event of data security incidents, those who conduct data handling activities shall immediately take remedial measures, notify users and report the incident to the relevant competent authorities timely in accordance with the law.

b) Risk assessment obligation for handling important data

The DSL stipulates risk assessment requirements for those who handle important data. According to Article 30 of the DSL, they shall periodically conduct risk assessment for their data handling activities and submit a risk assessment report to the relevant competent authorities. The risk assessment report shall include the categories and quantities of important data handled, how data are handled, and the data security risks faced and countermeasures to be taken.

c) Special obligations for data transaction intermediaries

The DSL stipulates special obligations for data transaction intermediaries. According to Article 33 of the DSL, intermediaries who engage in data transaction intermediary services shall require the data provider to explain the source of data, examine and verify the identity of both parties to the transaction, and retain the records of verification and transaction process.

d) Obligation of cooperation upon data access requests from public security organs and national security organs

Pursuant to Article 35 of the DSL, in addition to the above affirmative obligations to be undertaken by those who conduct data handling activities, relevant individuals and organizations shall cooperate upon request, if public security organs and national security organs need to access relevant data in order to safeguard national security or investigate a crime in accordance with the law. Although the provision grants the public security organs and national security organs power to access the data of individuals and organizations, it also provides that such request for accessing data shall go through strict approval procedures and be in accordance with relevant laws.

## 6. Restrictions on Cross-border Transmission of Data

According to Article 11 of the DSL, the State shall actively engage in international exchange and cooperation in such areas as data security governance and data development and use, participate in the formulation of international rules and standards related to data security, and promote the secure and free flow of data across borders. In spite of the aforesaid State's positive attitudes towards cross-border transmission of data, the DSL provides a number of restrictions on cross-border transmission of data under the following circumstances.

a) Restrictions on cross-border transmission of important data

In accordance with the strengthened protection for important data pursuant to Article 21 of the DSL, Article 31 of the DSL provides that cross-border transmission of important data collected and generated by critical information infrastructure operators ("CIIO") in China shall be subject to the provisions of the CSL, while cross-border transmission of important data collected and generated by other data handlers shall be subject to administrative measures to be formulated by the national cyberspace and administration authority in collaboration with relevant departments of the State Council.

By reference to Article 37 of the CSL, where it is necessary for CIIO to transfer the personal information and important data overseas due to business demands, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace and administration authority in collaboration with relevant departments of the State Council. Therefore, the DSL reiterates that the security assessment should be the prerequisite for cross-border transmission of important data collected and generated by CIIO in China.

According to Article 2 of the Draft Measures, the security assessment requirement is proposed to be applicable to all kinds of network operators for cross-border transmission of important data. However, the Draft Measures have not been promulgated yet and do not apply to other important data handlers who handle data not via network. Therefore, specific measures regarding cross-border transmission of important data by data handlers other than CIIO still need to be promulgated by the national cyberspace and administration authority in collaboration with relevant departments of the state council in furtherance of the DSL.

b) Export control on specific data

According to Article 2 of the *PRC Export Control Law* ("ECL"), dual-use items, military products, nuclear materials and other goods, technologies, services and items that are related to the protection of national security and interests or the fulfillment of nonproliferation or other international obligations are referred to as controlled items and subject to export control. Controlled items shall include any technical materials or other data related to such items. Export control means that prohibitive or restrictive measures shall be taken by the State on the transfer of controlled items from the territory of PRC to overseas, and on the provision of controlled items by any PRC citizen or incorporated or non-incorporated organization to any foreign organization or individuals.

In consistency with the ECL, Article 25 of the DSL emphasizes that the State shall implement export control on data which belong to controlled items and are relevant to safeguard national security and interests and fulfill international obligations in accordance with the law. Therefore, if the data to be transferred overseas fall into the scope of controlled items under the ECL, the data handlers need to seek approval from the state export control authorities in accordance with the ECL.

c) Restriction on provision of data to foreign judicial organs and law enforcement organs

With regard to provision of domestic data to foreign judicial organ and law enforcement organ upon request, Article 36 of the DSL provides that the competent PRC authority shall handle the request from a foreign judicial body and law enforcement body for providing any data in accordance with relevant laws and international treaties or agreements which the PRC has concluded or acceded to, or under the principle of equality and reciprocity. However, without such specific approval from the competent PRC authority, any organization or individuals within the territory of the PRC shall not provide any foreign judicial organs and law enforcement organs with any data stored within the territory of PRC.

## 7. Liabilities for Violation of the DSL

The DSL stipulates respective liabilities for violation of specific provisions. Compared with the first draft of the DSL, the general trend in the promulgated DSL is to strengthen administrative penalties for violation of the DSL. In the event of violation of the aforesaid obligations, the following liability will be imposed on the corresponding individuals or organizations.

a) Liability for violation of data security obligations

According to Article 45 of the DSL, those who fail to fulfill the data security obligations stipulated in Article 27 (please refer to above item 5. a)), Article 29 (please refer to above item 5. a)), and Article 30 (please refer to above item 5. b)) shall be ordered to make correction, given warnings, and may also be imposed with a fine of no less than RMB 50,000 but no more than RMB 500,000 by relevant competent authorities. In addition, the persons directly in charge and other directly responsible persons may be imposed with a fine of no less than RMB 10,000 but no more than RMB 100,000. Those who refuse to make correction or cause major data leakages or other serious consequences shall be imposed with a fine of no less than RMB 500,000 but no more than RMB 2 million, and may also be ordered to suspend relevant business or stop operation for rectification, or be subject to revocation of relevant business permission or business license. Under serious circumstances, the persons directly in charge and other directly responsible persons shall be imposed with a fine of no less than RMB 50,000 but no more than RMB 200,000.

Further, according to Article 47 of the DSL, any data transaction intermediary who fails to perform the obligations as stipulated in Article 33 (please refer to above item 5. c)) shall be ordered to make correction, subject to confiscation of any illegal income, and shall be imposed with a fine of no less than one but no more than ten times the illegal income. If there is no illegal income or the illegal income is less than RMB 100,000, a fine of no less than RMB 100,000 but no more than RMB 1 million shall be imposed. The intermediary may also be ordered to suspend relevant business or stop operation for rectification, or be subject to revocation of relevant business permission or business license. The persons directly in charge and other directly responsible persons shall be imposed with a fine of no less than RMB 10,000 but no more than RMB 100,000.

In addition, according to Article 48 of the DSL, those who refuse to cooperate with the public organs or national security organs regarding data access requests as stipulated in Article 35 (please refer to above item 5. d)) shall be ordered to make correction and given warnings, and may be imposed with a fine of no less than RMB 50,000 but no more than RMB 500,000 concurrently by relevant competent authorities. The persons directly in charge and other directly responsible persons shall be imposed with a fine of no less than RMB 10,000 but no more than RMB 100,000.

b) Liability for violation of the management system for the core data of the state

According to Article 45 of the DSL, those who violate the management system for the core data of the State and cause harm to national sovereignty, security and development interests shall be imposed with a fine of no less than RMB 2 million but no more than RMB 10 million by the relevant competent authorities, and shall be ordered to suspend relevant business or stop operation for rectification, or be subject to revocation of relevant business permission or business license, as appropriate. Further, if the violation constitutes a crime under PRC laws, the corresponding individuals or organizations shall be held criminally liable in accordance with the law. Although the management system for the core data of the state has not been elaborated yet, the corresponding liability implies the strict regulation on handling core data of the State in the future.

c) Liability for violation of restrictions on cross-border transmission of data

According to Article 46 of the DSL, those who provide important data overseas in violation of Article 31 of the DSL (please refer to above item 6. a)) shall be ordered to make correction, given warnings, and may also be imposed with a fine of no less than RMB 100,000 but no more than RMB 1 million by relevant competent authorities. The persons directly in charge and other directly responsible persons may be imposed with a fine of no less than RMB 10,000 but no more than RMB 100,000. In case of serious circumstances, the individuals or organizations shall be imposed with a fine of no less than RMB 1 million but no more than RMB 10 million, and concurrently may be ordered to suspend relevant business or stop operation for rectification, or be subject to revocation of relevant business permission or business license. Under serious circumstances, the persons directly in charge and other directly responsible persons shall be imposed with a fine of no less than RMB 100,000 but no more than RMB 1 million.

In addition, according to Article 48 of the DSL, those who provide any data to any foreign judicial organ or law enforcement organ without approval of the competent PRC authority in violation of Article 36 (please refer to above item 6. c)), shall be given warnings, and may also be imposed with a fine of no less than RMB 100,000 but no more than RMB 1 million by relevant competent authorities. In addition, the persons directly in charge and other directly responsible persons may be imposed with a fine of no less than RMB 10,000 but no more than RMB 100,000. In case of serious consequences caused, the individuals or organizations shall be imposed with a fine of no less than RMB 1 million but no more than RMB 5 million, and may be ordered to suspend relevant business or stop operation for rectification, or be subject to revocation of relevant business permission or business license. Under serious circumstances, the persons directly in charge and other directly responsible persons shall be imposed a fine of no less than RMB 50,000 but no more than RMB 500,000.

## 8. Conclusion

Overall, in the DSL, there are many policy-based and principle-based provisions, and fewer specific and enforceable obligatory provisions. Many new data management systems are introduced to be detailed and implemented by the relevant competent authorities in the subsequent issuance of supporting regulations and national standards. We also anticipate that the PIPL will be promulgated soon and form part of the fundamental system for cyberspace supervision and data protection together with the promulgated CSL and DSL. In the face of the strengthened regulations on data handling activities, we recommend that enterprises shall keep close eyes on relevant legislations and review internal policies on data handling regularly in order to be compliant with relevant PRC laws.

---

In case you have questions or for further information, please contact the authors of this newsletter:



**Panpan Tang**

Associate  
CMS, China

T +86 21 6289 6363  
E panpan.tang@cmslegal.cn



**Spring Zhu**

Junior Associate  
CMS, China

T +86 21 6289 6363  
E spring.zhu@cmslegal.cn

# About CMS, China

## 关于 CMS, 中国

CMS is one of the top 10 global law firms. With more than 4,800 professional legal and tax advisors in over 70 offices in more than 40 countries, we advise clients on both global and local matters and provide pragmatic and commercial advice.

CMS, China has been advising clients on doing business in China for several decades. As one of the top international law firms in China, we are able to support international companies and Chinese enterprises on all their legal needs through our full service offering. We advise in the areas of M&A, corporate restructuring, FDI, distribution and commercial, competition, compliance, employment, banking and finance, insurance, real estate and construction, technology licenses, IP registration and enforcement, dispute resolution as well as tax and customs.


Our team of legal experts are from China, Germany and the UK, and have an in - depth knowledge and understanding in many industrial sectors such as automotive, manufacturing, machinery and equipment, life sciences and healthcare, energy, banking & finance and TMC. We focus on serving the needs of our clients and on providing them with solution driven and business-oriented advice.

作为全球最大的法律与税务服务机构之一，CMS 通过旗下遍布于 40 多个国家超过 70 个办公室的 4,800 多名律师，提供覆盖全球及本土化的商业可行性解决方案。

如今，CMS 在中国服务客户已有数十年的历史。作为中国最大的外资律所代表处之一，CMS, 中国专注于并购、公司重组、外商直接投资、分销和商法、竞争法、合规、劳动法、银行和金融、保险、房地产和建筑、技术许可、知识产权注册与执行、争议解决及税务和海关等各个领域，为国际与中国公司提供全方位的法律咨询服务。


我们的顾问团队由来自中国、德国和英国的专家组成，对汽车、制造、机械设备、生命科学和医疗保健、能源、银行金融以及技术、传媒与通讯等行业领域有着全面深入的了解。我们注重为客户提供实际有效的咨询和解决方案，以帮助客户达到既定商业目标。

 3108 Plaza 66, Tower 2, 1266 Nanjing Road West, Shanghai 200040 P.R.China  
上海市南京西路 1266 号恒隆广场 2 期 3108 室

 Phone/ 电话: + 86 21 6289 6363

Fax/ 传真: + 86 21 6289 0731

 Web/ 网址: <https://cms.law/en/chn/>

 Email/ 电邮: [info@cmslegal.cn](mailto:info@cmslegal.cn)



Welcome to follow our WeChat account where you will find the updated legal insights and news.

欢迎扫码关注我们的微信公众号，在这里您可以获取最新的法律资讯和新闻。