# Impact of the New China Data Security Law for International Investors and Businesses

July 26, 2021

## I. Introduction

Recent developments in the tech sector in China, including government directives concerning heightened regulatory scrutiny of tech companies listed or looking to list in the US or on exchanges in other overseas jurisdictions, highlight the elevated strategic importance of data security issues in China. This is the context in which the new Data Security Law (DSL) of the People's Republic of China[1] (PRC) will come into force on September 1, 2021.

The DSL represents the Chinese government's further efforts to protect data security and regulate cross-border data transfers, areas that have been a focus for policymakers since the launch of the Cybersecurity Law[2] (CSL) in 2016. The introduction of the DSL significantly bolsters the data security legal framework in China, but also leaves intact other data-related laws and regulations, such as the CSL and the PRC State Secrets Law[3] (SSL), which continue to apply in parallel. This means that businesses holding data classified as "state secrets", as well as data newly designated as "important data", will need to comply with the requirements of both the SSL and the DSL (as well as any other applicable rules and regulations).

Since the DSL is mostly principles-based legislation, it can be viewed as a framework to be fleshed out subsequently through implementing rules, guidance and national standards, as well as regulatory action and interpretations as and when authorities seek to enforce the law in practice. As with the CSL, the fleshing out of the DSL in this way will likely be an evolving process, with certain key measures expected to be introduced in the coming months but full implementation of all aspects of the law likely taking much longer.

In this update, we provide an overview of the DSL, including key considerations for international investors and businesses.

## II. Overview

The DSL was passed by the Standing Committee of the National People's Congress of the PRC on June 10, 2021. As the nation's first foundational law in the field of data security, the DSL regulates various aspects of data collection, processing and transfer

**Contact Information**

**If you have any questions concerning this alert, please contact:**

**Daniel L. Cohen**
Partner
daniel.cohen@akingump.com
Hong Kong
+852 3694.3032

**Tatman R. Savio**
Registered Foreign Lawyer
tatman.savio@akingump.com
Hong Kong
+852 3694.3015

**Sonia Lor**
Solicitor
sonia.lor@akingump.com
Hong Kong
+852 3694.3062

**Jingli Jiang**
Counsel
jjiang@akingump.com
Beijing
+86 10.8567.2229

**Natasha G. Kohne**
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

**Michelle A. Reed**
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

**Jenny Arlington**
Counsel
jarlington@akingump.com
London
+44 20.7012.9631

and identifies fundamental principles in connection with, among other things, data classification, data security obligations for data processors, cross-border data transfers and a national security review framework.

Of particular significance is the call for the establishment of a nationwide multidisciplinary data classification system, which will result in "data" being classified according to factors such as the degree of harm to national security or the public interest if the data in question is compromised. The DSL also refers to two special categories of data—"important data" and "national core data"—and specifically provides for stricter regulation of, as well as heavier penalties for breach incidents involving, these two categories of data.

The DSL applies to all data processing activities in China but will also have extraterritorial reach to the extent that data processing activities outside China harm or damage national security, the public interest or the rights and interests of any Chinese citizens or organizations. As such, and given the breadth of the term "data processing activities" (which include the collection and storage of data), it may turn out to be the case that a person or entity outside of China risks being in breach of the law and becoming the subject of enforcement action in a number of different circumstances. It remains to be seen, however, to what extent the extraterritorial provisions are interpreted and applied in practice—much will turn on implementing rules and the approach of policymakers.

For cross-border data transfers, the DSL overlaps to some extent with the CSL and the Export Control Law[4]. In addition, there is an important express general prohibition in the DSL on providing data stored in China to foreign law enforcement authorities without prior approval from relevant Chinese authorities.

## III. Key Features of the DSL

### 1. Scope and Territorial Reach

As discussed above, the DSL applies to data processing activities in China but has extraterritorial scope to the extent that data processing activities outside China harm or damage Chinese national security, the public interest or the lawful rights and interests of any Chinese citizens or organizations.

### 2. Regulation and Enforcement

The regulation of data security will not fall to a single authority. Instead, the DSL refers to the responsibilities of various government authorities, as follows:

| Authority | Responsibilities |
|---|---|
| 1. Central National Security Commission | • Implementation of national data security strategies and major policies.<br>• Establishment of a "national data security work coordination mechanism." |
| 2. Public security and national security authorities | • Supervision of data security. |

| Authority | Responsibilities |
|---|---|
| 3. Government departments across different sectors and levels | • Regulation of data security and processing in relevant sectors (e.g., telecommunications, transportation, finance, natural resources, public health, education, technology, and so on) and locations. |
| 4. Cyberspace Administration of China (CAC) | • Coordination and supervision of internet data security specifically. |

**3. Data Classification Protection System**

The DSL calls for the establishment of a data classification system to protect data based on:

I. The degree of importance of the data to the social and economic development of China.

II. The degree of harm to national security, the public interest or the rights and interests of individuals and organizations if the data is destroyed, leaked or used illegally.

This is not the first time a data classification system has been proposed. Sector-specific rules already exist, such as the Guidelines for Data Classification and Grading for the Securities and Futures Industry[5]. However, the DSL classification system is an overarching statutory endorsement of the principle that all data ought to be classified and regulated taking into account national security and/or strategic development goals.

**4. Regulation of "Important Data" and "National Core Data"**

The DSL refers to two special categories of data—"important data" and "national core data"—and specifically provides for stricter regulation of, as well as heavier penalties for breach incidents involving, these two categories of data.

"Important data" is not defined but will be explicitly designated as such based on the two considerations set out in paragraph 3 above. There is expected to be a catalogue of "important data" designated at the national level, as well as designations at regional and/or sector-specific levels. The CAC, for example, has recently issued the draft Provisions on Automobile Data Security Management[6], which define the scope of "important data" in the automotive industry and designate certain categories of data as "important data" (e.g., traffic flow data in military control zones, mapping data that is more precise than that published by the government and statistics on the types and flows of vehicles).

The definition of "national core data" is vague and includes data concerning national security, the economic pillars, the livelihood of the Chinese people and significant public interest matters. The concept of "national core data" was introduced late in the day into the final version of the DSL, so there is limited market commentary currently on specific examples of "national core data" in practice or the significance of data being characterized as such. What can be said is that "national core data" is expected to be protected to a higher degree and more strictly regulated than "important data." It is likely that, as with "important data," "national core data" will also be designated as such by the relevant authorities.

**5. Data Processors and Their Data Security Obligations**

In broad terms, data processors are required by the DSL to:

I. Establish a data security management system aimed at safeguarding data security, including by way of identifying data security risks or breach incidents and providing notification of such risks or incidents.

II. Comply with the existing "multi-level protection scheme," which requires internet network operators to classify their systems in China based on the risks to national security, social order or economic interests if such systems are damaged or attacked.

III. With respect to "important data," appoint a data security officer and management body to be responsible for ensuring data security, carrying out regular risk assessments and filing assessment reports with the relevant regulatory bodies.

**6. Cross-border Transfers of Data**

There are three key themes in the DSL in relation to cross-border data transfers.

First, the DSL distinguishes between Critical Information Infrastructure (CII) operators and non-CII data processing entities and establishes different frameworks for cross-border transfers of "important data" by these two types of operator:

I. CII operators are engaged in important industries and sectors such as information services, finance and public services. They must follow the rules established under the CSL, which require storage in China of data gathered or produced in China, and a security assessment conducted by the relevant government authorities where cross-border transfers of the data are necessary for business purposes.

II. Non-CII data processing entities are other operators of data who must comply with separate rules that are to be published by CAC and other relevant government departments.

Second, individuals and organizations are expressly prohibited under the DSL from providing data stored in China to foreign law enforcement authorities, save with the prior approval of relevant Chinese authorities. This prohibition is very broad, so it is expected that there will be further detailed measures or guidelines to shed light on what constitutes data stored in China and how an applicant should apply for approval to make a relevant disclosure.

Third and finally, the DSL specifies that data relating to a controlled item under the relevant export control rules also constitutes a controlled item, meaning that a permit is required from the Ministry of Commerce or its local bureau to authorize a cross-border transfer of such data. This is consistent with the Export Control Law.

**7. National Security Review System**

The DSL establishes a data security review regime to identify data processing activities that impact or may impact national security. It is unclear which authority will be responsible for implementing such a system, what types of data processing activities will fall within the scope of the regime and what criteria will form the basis of the review. However, it is likely that once a clearer regulatory framework is established, national security data reviews will become as important as cybersecurity reviews and will need to be factored into routine corporate compliance activities.

### 8. Other Key Provisions and Sanctions

Other noteworthy provisions in the DSL include the specific reference to China's ability to adopt countermeasures if any foreign country or region takes discriminatory measures against Chinese investment or trade relating to data or data technologies, as well as the potential establishment of a data trading management system to regulate trading in data.

A breach of the DSL may give rise to administrative, civil and/or criminal liabilities and different penalties may be imposed depending on the type and severity of the violation and the type of data (e.g., noncompliance relating to "important data" or "national core data" will attract more severe penalties). Penalties that may be issued by the Chinese authorities include correction orders, warnings and fines as well as, in serious cases, confiscation of illegal income, revocation of business licenses and suspension of operations.

## IV. Key Implications for Foreign Investors and Businesses

The DSL will take effect at a time of tightening international regulation in the sphere of data security, so it does not exist in a vacuum. Other key markets have similarly sought to ensure robust measures are in place for controlling data collection, processing, handling and disclosures and so market participants, especially those that conduct cross-border investments and operations, are therefore well accustomed to data security requirements. In the context of the DSL, foreign investors and businesses will need to be attuned to these considerations in the Chinese market.

However, since the DSL is mostly principles-based, the real impact of the law remains to be seen and will depend on the content of expected implementing rules and other guidance and how the regime is implemented. In the meantime, overlaps between the DSL and other key data-related legislation in China (e.g., the CSL and the upcoming Personal Information Protection Law[7] (PIPL)), as well as the involvement of different authorities with responsibilities for different aspects of DSL oversight and enforcement, signal that DSL compliance may be tricky to navigate.

### 1. Foreign Investors

The DSL has very clear national security objectives (among others). The same is true of legal and regulatory developments in other areas in China, including tightened regulation of the FinTech sector, the introduction of national security review in the context of inbound foreign investments, as well as very recent policy statements regarding more stringent regulation of Chinese businesses seeking overseas listings. All of these developments have prompted or been prompted by rather dramatic regulatory activity in China that has impacted large businesses, entire sectors and markets more generally. Against this backdrop, data security in China is no longer a minor compliance matter. It has become a policy and enforcement tool for achieving key national policy objectives of China in the context of broader geopolitical risks.

From a practical perspective, therefore, foreign investors considering Chinese investment targets should consider the need to carefully diligence the data protection and security systems of those targets. Relevant data security considerations could arise at the national, regional, local and/or sector-specific levels, meaning that a broad scoping of these considerations should be undertaken in conjunction with local counsel in China with suitable expertise.

While it may not be possible to eliminate risks in this area, not least because of the evolving nature of the applicable legal framework, investors should at a minimum seek to obtain comfort on a target group's ability to respond to and accommodate regulatory requirements and/or actions in the data security space and appropriately factor in any such risks in the structuring and pricing of relevant investments. Investors may also wish to require targets to rectify data compliance issues before closing a deal and/or ensure suitable downside protection and remedies are in place when, for example, a listing cannot be achieved within an agreed timeframe.

Although the extent to which foreign persons may be the subject of enforcement activity under the DSL remains to be seen, potential recipients of data from Chinese parties may, depending on the context, wish to exercise more caution. For example, it may be prudent to diligence the disclosing party's data protection, security and compliance systems and, where appropriate, agree to suitable contractual protections, such as an indemnity for breach of data protection laws, to help de-risk DSL noncompliance where there could be extraterritorial consequences.

**2. Businesses**

Corporate culture in much of the world has already adapted to the changing international body of data protection laws and regulations. In order to comply with increasingly complex data-related laws and regulations, businesses have grown more cautious and strategic about how systems involving data are established and operated as they seek to manage compliance risks at an early stage. It is, for example, increasingly common for businesses to:

I. Conduct a holistic review of their data systems to understand precisely what data is collected, where that happens and where the data is transferred, as well as system weaknesses and controls.

II. Proactively consult with regulators with respect to sector-specific data, to the extent practicable.

III. Adopt a flexible framework of controls based on core data privacy and security principles, which is adaptable as the law and regulatory environment evolves.

IV. Prepare relevant manuals and training programs to educate employees about key risks and developments.

The DSL will require such activities from a Chinese law perspective and may, if such steps are not already a feature of a corporate compliance program (for the purpose of identifying state secrets information, for example), require a company to undertake a comprehensive ongoing data collection, identification and categorization exercise involving the data generated by the business. This may be the only way to manage appropriately the compliance risks associated with collecting or generating "important data" and "national core data."

Businesses will also need to be mindful of the prohibition on the provision of data stored in China (without consent) to foreign agencies. It is currently unclear how this prohibition — which applies to all data — will be applied in practice, but we may see it narrowed in scope to ensure that businesses with an international footprint, in particular, are able to comply with it in practice. In the past, significant tensions have resulted from overseas listed Chinese companies being required by applicable foreign law and regulation to disclose information for audit and other purposes that is

considered sensitive from a Chinese perspective. The DSL may mean such tensions arise more regularly and in more contexts for Chinese businesses.

## V. Outlook for Data Security Development in the PRC

Data security is a key focus for policymakers in China and is a strong theme in the evolving legal landscape, now reinforced by the DSL as a framework for the articulation of detailed measures and regulations in the coming months and years. These will give life to critically important matters such as the cataloguing of "important data" and "national core data," the data national security review process and the approvals procedure for cross-border data transfers.

The DSL does not displace, but instead supplements other laws that already regulate different aspects of data security. In addition to existing regulations and data cataloguing requirements at local or sector-specific levels, the DSL follows on the coattails of the CSL and is expected to be followed by the PIPL, which will be aimed at protecting personal information under a more structured framework, similar to the General Data Protection Regulation in the EU. The SSL also remains in place and applies to all state secrets information. Careful scrutiny and monitoring of data security issues is now therefore more important and complex than ever – for both businesses focused on data security compliance and investors who wish to ensure that investee companies and targets subject to the DSL are well positioned to meet the new requirements and address further regulatory developments in this area.

[1] 《中华人民共和国数据安全法》

[2] 《中华人民共和国网络安全法》

[3] 《中华人民共和国保守国家秘密法》

[4] 《中华人民共和国出口管制法》.

[5] 《证券期货业数据分类分级指引》

[6] 《汽车数据安全管理若干规定（征求意见稿）》

[7] 《中华人民共和国个人信息保护法》

akingump.com