A Close Reading Of China's Data Security Law, In Effect Sept. 1, 2021

China's Data Security Law contains provisions that cover the usage, collection, and protection of data in the PRC. Violations will trigger penalty fines and even suspension of business and revocation of license or permits. The person directly in charge of implementing compliance at the company will be exposed to penalty risks – hence businesses are advised to closely read the Data Security Law and track upcoming legislative developments. This is more important as the Data Security Law currently does not provide details on obtaining the approval of the relevant competent authority, or which authorities will have the right to approve cross-border data sharing. Similarly, the Law as it stands does not specify how intermediary service providers will be examined and whether the non-compliance of the data provider will be passed onto the intermediary service provider. Finally, the Data Security Law introduces ethics and social morality as new compliance considerations for companies dealing in data processing activities and the research and development of new data technologies.

On June 10, 2021, the Data Security Law of the People's Republic of China ("**Data Security Law**" or this "**Law**") was officially passed during the 29th session of the Standing Committee of the 13th National People's Congress. This Law has been reviewed three times since June 2020 and will come into force on **September 1, 2021**.

Aiming to further strengthen the current protection regime for the country's fast-growing digital economy, the law stipulates how data is used, collected, developed, and protected in China. It emphasizes on top-down coordination of data security implementation among local governments and differentiated fines based on severity of violations.

Data has been deemed as a basic and strategic resource of the country. According to Xinhua, the law will play an important role in implementing data security and safeguard the core interests of China.

Highlights of the Data Security Law

Although the law doesn't provide any detailed guidance, it highlights some key issues that businesses should pay attention to in daily operations.

Cross-border data transfer requirements

For multinational companies headquartered in China or with branches in China, cross-border data transfer might be inevitable when engaging with overseas companies or investors.

The Data Security Law has strengthened the management of cross-border data transfer, which is embodied in Article 31 and Article 36.

According to **Article 31** of the Data Security Law, the cross-border transfer of important data collected and generated by critical information infrastructure operators within China shall be governed by the Cybersecurity Law, under which data collected and generated by critical information infrastructure operators are bound to be stored within the territory of China by principle. Whenever such data needs to be transferred overseas, a security assessment has to be performed.

China · Germany · Hong Kong · India · Italy · Singapore · United States · Vietnam
Dezan Shira Asian Alliance: Indonesia · Malaysia · Thailand · The Philippines

www.dezshira.com

Important data refers to those defined in Article 21 of the Data Security Law and will be provided in the data classification and hierarchical protection catalogue developed by respective regions and departments and for relevant industries and field.

Critical information infrastructures refer to infrastructure in important industries and sectors, such as public communications, information service, energy, transport, water conservancy, finance, public service, and e-government, and other critical information infrastructure that – once damaged, disabled, or data disclosed – may severely threaten the national security, national economy, people's livelihood, and public interests (according to Article 37 of the Cybersecurity Law).

For the cross-border transfer of important data collected and produced during operation by general data processors within the territory of the People's Republic of China, Article 31 of the Data Security Law stipulates that security review measures shall be formulated by the state cyberspace administration in concert with the relevant departments under the State Council. That is to say, for the moment, there are no specific rules on general data processor for transferring important data abroad.

Data processors who violate Article 31 of the Data Security Law and illegally transfer important data to overseas will be ordered by the relevant competent authority to make rectifications and given a warning and may be concurrently fined not less than RMB 100,000 (US$15,460) but not more than RMB 1 million (US$154,600). If the circumstances are serious, they will be fined not less than RMB 1 million (US$154,600) but not more than RMB 10 million (US$1.55 million), and may be ordered to suspend the relevant business, stop the business for rectification, and their relevant business permit or business license will be revoked. The person directly in charge and other directly liable persons will be fined will be fined between RMB 100,000(US$15,460) and RMB 1 million (US$154,600).

Conducting a cyber security audit is growing more important for companies as China is tightening its cybersecurity practices and regulation thereof. Businesses are well advised to carefully evaluate if they fall into the scope of critical information infrastructures operators before transferring their data to overseas parties and must keep a close eye on future legislative developments to avoid compliance risks and potential penalties.

Article 36 of the Data Security Law stipulates requirements on providing data to judicial or law enforcement authorities outside China.

Any organizations and individuals in China must obtain the approval of the competent authority when dealing with cross-border data submission requests made by foreign judicial or law enforcement authorities.

And it is stipulated that the competent authority shall deal with the application in accordance with the relevant laws and the international treaties and agreements concluded or acceded to by the People's Republic of China or on the principle of equality and mutual benefit.

Those who provide data to foreign judicial or law enforcement agencies without the approval of the competent authorities may face a fine ranging from RMB 100,000 (US$15,460) to RMB 5 million (US$773,000). At the same time, the incompliant companies could be ordered by the competent authorities to suspend relevant businesses or suspend whole operations for rectification, its relevant business permit or business license will be revoked, and the person directly in charge and other directly

liable persons will be fined between RMB 50,000(US$7,730) and RMB 500,000 (US$77,300).

For the moment, the Data Security Law does not provide details about how to obtain the approval of the competent authority, or which authorities have the right to approve. Businesses are suggested to keep a close eye on the future developments of the implementation measures.

Compliance requirements on data intermediary services providers

With the ability to gather, analyze, and use data being improved, the demand for market-oriented data trading keeps expanding.

Many data trading platforms have emerged, such as Tianyancha, Qichacha, Tianyuan Data, Jingdong Cloud, Guiyang Big Data Exchange, and Shanghai Data Exchange Center, etc.

In fact, such data trading platforms act as an intermediary service provider, providing a trading platform for data suppliers and data demanders. In other words, it is like an online shopping platform, such as Alibaba, eBay, Amazon, etc., except that the commodities on this platform are data, and because of this, the transaction process, objects, and so on are very different. We give one simple illustration here for easier understanding:

Previously, there was no exact laws or regulations to monitor and control the data trading process. The interests of the parties involved in data transactions were sometimes negatively impacted by the lack of standards on intermediary service providers.

Now, for the first time, the Data Security Law puts forwards some formal requirements on the data trading process. This serves as a starting point in fostering a healthy data trading market.

To be more specific, Article 33 of the Data Security Law imposes the below requirements for institutions engaged in data transaction intermediary services:

- The institution engaged in data transaction intermediary services shall **require the data provider to explain the data source**. The data should have no ownership defect, meaning that the data is not acquired by theft or other illegal means, and the data is not among those prohibited by Chinese laws and regulations.
- The institution engaged in data transaction intermediary services shall **check the identity of both parties to the transaction.** Both parties should be legal organizations or natural persons. For certain data trading activities that require relevant parties to obtain certain licenses before engaging in the transactions, the intermediate institution should check if the party has the

required licenses.
- The institution engaged in data transaction intermediary services shall **retain the examination and transaction records**.

Data intermediary service providers who fail to fulfill the obligations mentioned above could be subjected to multiple penalties. The illegal gains will be confiscated and a fine ranging from one to 10 times of the illegal gains will be imposed. If there are no illegal gains or the illegal gains are less than RMB 100,000 (US$15,460), the data intermediary service provider failing to fulfill the obligations will be fined not less than RMB 100,000 (US$15,460) but not more than RMB 1 million (US$154,600). Also, it could be required to stop relevant businesses, stop the whole operation for rectification, or its relevant business permit or business license could be revoked. At the same time, the person directly in charge and other directly liable persons will be fined between RMB 10,000 (US$1,546) and RMB 100,000 (US$15,460).

Currently, the Data Security Law does not specify the details on how the intermediary service providers will be examined and whether the incompliance responsibility of the data provider will be passed to the intermediary service provider. Relevant parties are suggested to keep a close eye on the future implementation measures.

Protection of public interests

In addition to the aforementioned compliance requirements and obligations that must be met, the Data Security Law also embodies certain human concerns and strives to ensure that people can equally enjoy the convenience brought by the digital economy.

Care for special groups

In recent years, China has made big improvements in the efficient delivery of public services thanks to the data revolution. On the other hand, certain groups like the elderly and the disabled have suffered a lot of difficulties in using digital technologies.

In practice, there have been many cases in which the sellers or service providers refuse to accept cash while the elderly do not know how to use Alipay or WeChat Pay. Also, since the outbreak of COVID-19, it has been reported that in certain cities, people were denied to access public transportation or services because they failed to obtain the digital health code, implemented as part of the epidemic prevention measures.

To protect these special groups and ensure they can equally access public services, Article 15 of the Data Security Law emphasizes any organization or individual should take full consideration of the needs of the elderly and the disabled when designing and developing the application for public services.

This can be divided into two aspects.

On the one hand, the elderly and the disabled cannot be forced to use the so called intelligent products. For example, in addition to ordering food by scanning QR Code and paying the bill by digital payments, the restaurants must provide traditional order and payment methods as alternatives.

On the other hand, the developers should take the characteristics of the elderly and the disabled into consideration when they design and develop relevant products, for example, adding an audible function

for people with visual impairment designers, enabling large font for elderly users, etc.

Stick to the bottom line on ethics

Data has brought great convenience to people's daily lives. On the other hand, however, it has been observed that users' personal data and privacy are becoming highly vulnerable and easy to infringe upon. For example, there used to be an online car-hailing platform where the driver could directly check the personal information (e.g. gender, age, job, etc.) registered by the passenger without any consent. Moreover, the driver could get the passenger's fixed route through the platform, and comment on the passenger's appearance, voice, figure, etc. publicly, which provided criminal opportunities for some offenders.

All these lead to the question: What is the bottom line when it comes to data processing activities and researching and development of new data technologies?

Article 28 stipulates that any organizations or individuals that carry out data processing activities and the research and development of new data technologies shall be conducive to promoting economic and social development, enhancing the well-being of the people, and complying with social morality and ethics.

It can be seen that the Data Security Law puts forward requirements on data processing activities and the research and development of new data technologies from the moral level. In the past, the relevant regulatory authorities have focused more on legal and compliance issues when reviewing data processing activities and the research and development of new data technologies.

Given this, companies that engage in data trading, information matching, software development, and other related activities, shall conduct social morality and ethics review on data analysis and product designed by themselves in advance, so as to avoid the violation of social morality and ethics after entering the market, which may affect the business reputation and daily operation.

How the Data Security Law works with existing data and information security laws

At present, there are three laws related to data and information protection in China:

- The Cybersecurity Law of the People's Republic of China ("**Cybersecurity Law**"), implemented on June 1, 2017.
- The Personal Information Protection Law of the People's Republic of China (Second Revision of the Draft) ("**The Draft PIPL**"), issued on April 29, 2021, which is still under review.
- The Data Security Law, to be implemented from September 1, 2021.

While the common goal of these three laws is to build a comprehensive legal framework to regulate the information and data security regime in China, their priorities are different. Comparisons between them are presented in the following table.

Comparison of the Three Major Data and Information Security Laws			
	Cybersecurity Law	Draft PIPL	Data Security Law
Purpose	Ensure cybersecurity, secure cyberspace sovereignty, national security, and public interests.	Protect the rights and interests of personal information, regulate personal information processing activities, and promote the rational use of personal information.	Ensure data security and focus on data processing activities, data development, and data utilization.
Priority	Security of the cyberspace	Protection of personal information	Security of the data itself, data processing activities, and safety supervision
Scope of application	Network construction, operation, and maintenance in China	Personal information processing of natural persons within China and personal information processing of natural persons outside China under certain conditions	Data processing activities carried out within or outside China
Definition of data	Various electronic data are collected, stored, transmitted, processed, and generated through the network	No definition of data	Any recording of information by electronic or other means
Who are regulated	Network operators	Any organization or individual that processes personal information	Any organization or individual that process data
Extraterritorial jurisdiction	Not applicable	Applicable under certain conditions	Applicable under certain conditions
Cross-Border data transfer	Security review shall be carried out in accordance with relevant measures	Safety assessment might be required by the Cyberspace Administration of the State	Relevant administrative measures formulated by the Cyberspace Administration of the State and the relevant departments under the State Council shall be followed

Graphic© Asia Briefing Ltd.

With the release of the Data Security Law, the policy requirements of data security protection in China have been strengthened and clarified. However, the Law is more of an outline for data security supervision and protection that links to different aspects.

The specific rules for implementation are expected to be clarified in other supporting laws and regulations in the future, and to be explored and observed in practice.

This article was first published by China Briefing, which is produced by Dezan Shira & Associates. The firm assists foreign investors throughout Asia from offices across the world, including in China, Hong Kong, Vietnam, Singapore, India, and Russia. Readers may write to info@dezshira.com for more support.