Regional

China's Data Security Law Comes into Effect on 1 September 2021

Introduction

The Data Security Law of the People's Republic of China (中华人民共和国数据安全法) ("**Data Security Law**"), which was passed by the Standing Committee of the National People's Congress of the People's Republic of China on 10 June 2021, will come into effect from 1 September 2021.

The Data Security Law took less than one year, since its first public consultation in July 2020, to be passed into law in June 2021. The Data Security Law was one of the fastest laws to be passed in China's 2020 legislative programme.

The Data Security Law, together with the PRC Cybersecurity Law (中华人民共和国网络安全法, which came into effect on 1 June 2017) and the Personal Information Protection Law (中华人民共和国个人信息保护法, which will come into effect on 1 November 2021), make up China's three key "pillar" laws in terms of cybersecurity regulation and data protection.

The Data Security Law comprises 55 Articles spread across 7 Chapters, and deals with important issues such as Data Security and Development, Data Security Systems, Data Protection Obligations, and Security and Openness of Governmental Data. This update sets out some of the key highlights of the Data Security Law.

Key Highlights

Extraterritorial Effect

Article 2 of the Data Security Law states that it applies to data processing activities within China.[1] Further, legal responsibility would be pursued against data processing activities that take place outside China, if such activities would harm China's national security or public interests, or the lawful rights of its citizens and organisations. This gives the Data Security Law extraterritorial powers.

Article 26 further provides that where any nation or territory employs discriminatory prohibition,

[1] "Data", as used within the Data Security Law, refers to any record of information in electronic or other forms (Article 3).

restriction or other similar measures against China in terms of investment, trade and other aspects in relation to data and data exploitation technology, China may employ equal reciprocal measures against such nation or territory based on the actual circumstances. It is also noted that Article 43 of the Personal Information Protection Law contains a similar provision.

Work Coordination Mechanism

Article 5 provides that a National Data Security Work Coordination Mechanism ("**NDSWCM**") will be established to be responsible for major decision-making, deliberating and coordinating China's data security work; researching, drafting, and guiding the implementation of the national data security strategy and related major policy directives; planning and coordinating major matters and efforts in national data security, and establishing a coordination mechanism for national data security work.

Data Trading

Article 19 states that the State will establish a sound data trading management system to standardise data trading activities and develop a data trading market.

Article 33 further provides that intermediaries which are carrying out data trading should request the data providers to explain the source of their data, verify the identity of the parties involved in the data trading, and maintain records of the review and transaction process. Data intermediaries are therefore now delegated with the role of being frontline gatekeepers to ensure the legitimacy of the data source. However, merely obtaining contractual warranties from the data providers that the data source is legitimate may now be insufficient for the data intermediaries to be released from liabilities in the event that the data provided to them was illegally obtained. Data intermediaries therefore need to carry out adequate due diligence on the data providers and the data provided to them. However, the Data Security Law is silent on the standard of review required, and this may be the subject of further clarification in the future via the issuance of further subsidiary legislation.

Data Classification System

Article 21 provides that the State will establish a protection regime by classifying and categorising data based on their importance in economic and social development, as well as the extent of harm to national security, public interests, or the lawful rights of individuals or organisations if such data is altered, destroyed, leaked or accessed or used illegally.

The NDSWCM will be responsible for creating a catalogue of categories of important data to reinforce protection for important data. The regional and departmental authorities will identify a specific catalogue of important data for their own region or sector, as well as relevant industries and fields. It remains to be seen if a general catalogue will be promulgated at a national level to guide the regional and

departmental authorities so as to ensure coordination and consistency amongst the various state organs.

It is noteworthy that the final draft of the Data Security Law also introduced a category of "core national data", which did not appear in the previously-released drafts. Data that concerns national security, national economy, important aspects of people's livelihood or important public interests will belong to "core national data", and be subject to a more stringent management regime. It is foreseeable that the relevant authorities will develop implementation regulations for "core national data" to further strengthen the management of such data.

National Security Review

Article 24 provides that the State shall establish a data security review system to conduct national security reviews of data processing activities that affect or may affect national security. A security review decision made in accordance with the law shall be final.

This is consistent with the principle of national security review established under the new National Security Law of the People's Republic of China which came into effect on 1 July 2015, according to which the State shall establish the rules and mechanisms for national security review and supervision, and conduct national security review of foreign investment, particular materials and key technologies, and network information technology products and services that affect or may affect national security, construction projects that involve national security matters, and other major matters and activities to effectively prevent and resolve national security risks.

On 10 July 2021, the Cyberspace Administration of China released the amendment draft to the Cybersecurity Review Measures (for Public Comments) (网络安全审查办法(修订草案征求意见稿)). One of the key amendments is that operators with more than 1 million users' personal information must file a cybersecurity review with the Cyber Security Review Office when they go public abroad. Currently, such amendment has not come into effect. However, it shows that the regulators of China will take a stricter approach in implementing the Data Security Law and other relevant laws and regulations.

Data Security Obligation

Article 27 provides that when carrying out data processing activities, comprehensive data security management protocols should be established, data security education and training should be organised and conducted, and corresponding technical measures and other necessary measures should be implemented to safeguard data security. When carrying out data processing activities using the Internet and other information networks, the foregoing measures should be conducted under the existing network security classification protection regimes. In addition, organisations that are processing important data shall clearly designate persons responsible for data security and data security

management bodies to ensure accountability for data security and protection.

Value Guidance

Article 28 provides that the conduct of data processing activities and research and development of new data technology shall be conducive to promoting economic development, improve the welfare of the people, and comply with social mores and ethics.

Cross Border Transfer of Data

Article 31 clarifies that the cross border transfer of important data collected by critical information infrastructure operators during their operations will be governed by the Cybersecurity Law, while the cross border transfer of important data collected and generated by all other data processors in China will be subject to rules to be drafted by the Cyberspace Administration of China in conjunction with relevant departments of the State Council. On 11 April 2017, the Cyberspace Administration of China released the draft Measures on Security Assessment of Cross-border Transfer of Personal Information and Important Data (for Public Comments) (个人信息和重要数据出境安全评估办法(征求意见稿)). However, these draft measures are still in a draft form and have not been passed.

Article 46 further provides that those who violate Article 31 may be punished with a fine between RMB 100,000 and RMB 1,000,000, and managers and other personnel who are directly responsible may be punished with a fine between RMB 10,000 and RMB 50,000. If the circumstances are serious, a fine of between RMB 1,000,000 and RMB 10,000,000 may be imposed instead, and the managers and other personnel who are directly responsible may also be punished with an increased fine of between RMB 100,000 and RMB 1,000,000. In addition, they may be ordered to suspend relevant operations or even have their business permits or licenses revoked.

Access to Data by Chinese Security Departments

Article 35 provides that the public security bureaus and national security agencies shall follow the strict approval procedures in accordance with the law when requesting data for national security and criminal investigations, and relevant organisations and individuals should comply with such requests. Those who refuse to comply may be punished with a fine between RMB 100,000 and RMB 1,000,000.

Responding to Requests for Data by Foreign Justice or Law Enforcement Agencies

Article 36 provides that (a) all requests for the provision of data by foreign justice or law enforcement bodies are to be handled by the competent State organs, based on relevant laws and international treaties and agreements concluded or participated in by China, or in accordance with the principle of reciprocity, and (b) domestic organisations and individuals are not allowed to provide data stored within

China to foreign justice or law enforcement bodies without the approval of the competent State organs. A similar provision may be found under the Personal Information Protection Law as well, under Article 42.

Article 48 further provides that those who violate Article 36 may be punished with a fine between RMB 100,000 and RMB 1,000,000. In addition, they may be ordered to suspend relevant operations or even have their business permits or licences revoked.

Conclusion

The entry into force of the Data Security Law ushers in a new era of regulation of data activities in China. With the promulgation of a series of laws and regulations in the cybersecurity and data protection sector this year, the Data Security Law, together with the Cybersecurity Law and the Personal Information Protection Law, now establishes the core tenets of cybersecurity regulation and data protection in China.

The Data Security Law brings about important ramifications for companies operating in China in terms of their compliance obligations, in particular, their ability to transfer data out of China and their ability to comply with requests for data by foreign justice or law enforcement agencies. At the same time, given the broad and expansive nature of the provisions of the Data Security Law, it is also expected that further regulations will be introduced to provide clarity in the near future.

In light of the recent legislative changes, businesses carrying out data processing activities in China should ensure that they establish and adopt robust data protection frameworks internally to ensure compliance with the new laws. In particular, businesses should (i) ensure that they establish and implement adequate data handling and protection policies to provide employees with adequate guidance on how to handle and use data in compliance with the laws; (ii) adopt a security-by-design approach in their data processing activities; (iii) conduct regular internal and external audits to ensure existing systems and processes are sufficiently robust to fulfil the legal requirements; and (iv) regularly conduct training for employees to ensure they keep updated with the best practices. Our data protection teams can most certainly assist with the above.

Disclaimer: *Rajah & Tann Singapore LLP Shanghai Representative Office is a foreign law firm licenced by the Ministry of Justice of the People's Republic of China (the "**PRC**"). As a foreign law firm, we may not issue opinions on matters of PRC law. Any views we express in relation to PRC laws and regulations for this matter are based on our knowledge and understanding gained from our handling of PRC-related matters and through our own research, and also from our consultations with PRC lawyers. Therefore, such views do not constitute (and should not be taken as) opinion or advice on PRC laws and regulations.*

Contacts

Benjamin Cheong
Partner
Rajah & Tann Singapore LLP

T +65 6232 0738

benjamin.cheong@rajahtann.com

Chen Xi
Partner (Foreign Lawyer)
Rajah & Tann Singapore LLP

T +65 6232 0158

chen.xi@rajahtann.com

Linda Qiao
Senior International Counsel
Rajah & Tann Shanghai Representative Office

T +86 21 6120 8818

linda.qiao@rajahtann.com

Chia Lee Fong
Partner (Foreign Lawyer)
Rajah & Tann Singapore LLP

T +65 6232 0734

lee.fong.chia@rajahtann.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

Our Regional Contacts

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*
R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence