LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice

August 14, 2020 | Number 2774

China Issues Draft Data Security Law for Public Comment

点击这里查看本客户通讯中文版。

The proposed Data Security Law has a broad jurisdictional scope and will expand the PRC's regulatory framework for information and data.

On July 3, 2020, the Standing Committee of China's National People's Congress issued the draft Data Security Law (DSL) for public comment. Once finalized, the DSL, together with the Network Security Law and the proposed Personal Information Protection Law, will form an increasingly comprehensive legal framework for information and data security in the People's Republic of China (PRC).

Notably, the DSL:

- Has a broader scope than the PRC Network Security Law, both in relation to extraterritorial jurisdiction as well as the types of data and data activities it regulates
- Categorizes data based on its importance to the state's economic development, national security, and public interest, while also providing additional safeguards for "important data"
- Imposes a set of obligations on entities and individuals who conduct data activities

Entities and individuals who fail to comply with the requirements of the DSL may face potential penalties and sanctions, including demands for rectification, warnings, forfeiture of illegal gains, and closure of businesses, as well as the revocation of business licenses and other applicable criminal, administrative, or civil liabilities.

Scope

The DSL's scope extends beyond the current PRC Network Security Law in multiple respects.

Jurisdictional scope

The DSL provides far broader extraterritorial jurisdiction than the PRC Network Security Law. The current legal framework only authorizes PRC authorities to monitor and take preventive/defensive actions against certain network activities that occur outside of the PRC in limited circumstances, (e.g., any foreign entities or individuals that attack, infringe, interfere with, or damage critical information infrastructure in the PRC).

According to Article 2, the DSL will apply to both:

- "Data activities" conducted within the territory of the PRC
- Data activities conducted outside of the PRC that may "harm the national security or public interests of the PRC, or the legitimate rights of Chinese individuals or entities"

The DSL does not specify criteria to determine what data activities would be deemed "harmful" pursuant to Article 2.

Regulated activities

The DSL broadly defines "data" as any record of information made in electronic or other forms. Conversely, the PRC Network Security Law mainly protects the electronic form of data collected, stored, transmitted, or processed on networks (i.e., "network data") and personal information while the PRC Criminal Law mainly protects data stored, processed, or transmitted through computer information systems.

The DSL's definition of "data activities" is also more comprehensive than that provided under the draft Data Security Management Measures, which was issued by the Cyberspace Administration of the PRC on May 28, 2019. In particular, the DSL would legally regulate the commercial "transaction" of data for the first time if enacted. Other activities referenced by the DSL include data collection, storage, processing, use, provision, and publication.

The DSL carves out:

- Data activities relating to state secrets, which shall comply with the Law on Guarding State Secrets
- Military data, for which measures shall be promulgated by the Central Military Commission

The DSL provides that data activities involving personal information shall also comply with other applicable laws and regulations governing personal information. The Standing Committee of the National People's Congress of the PRC recently announced a proposal for new laws on personal information protection, which will further develop the regulatory framework governing data and personal information.

Data Security Framework

The DSL sets out a new data security framework based on the following systems and measures.

Class-Based Data Protection System

The DSL proposes to classify and protect data based on its importance to the state's economic development, national security, and public interest. This approach is consistent with the class-based network protection mechanism under the PRC Network Security Law.

Using the class-based system as a guide, the DSL emphasizes the protection of "important data" without defining the term. The term "important data" was first introduced in the 2016 Network Security Law, which also did not provide a definition. Under the 2017 draft recommended national standard "Guidelines for Cross-Border Data Transfer Security Assessments" (the Draft Guidelines), "important data" refers to data collected or derived in the PRC that closely relates to national security, economic development, and public interests. Appendix A of the Draft Guidelines sets out a detailed list of important data in various industries.

The DSL empowers regional and industry authorities to formulate specific catalogs of important data and measures to protect such data, for their relevant regions and industries. The application of the DSL will therefore depend on central, regional, and industry-specific classifications of "important data" and associated data safeguards.

Data Security Risk Management System

The DSL calls for a unified mechanism to evaluate, report, share, and monitor data security risks. Details of the system are not elaborated in the DSL, and are pending future regulations or national standards.

Emergency Response System for Data Security Incidents

The DSL also calls for an emergency response mechanism. Upon the occurrence of a data security incident, relevant authorities shall carry out their emergency plans to mitigate security risks, control the impact of the incident, and notify the public in a timely manner.

Data Security Review System

The DSL proposes a national data security review system to identify data activities that may impact national security.

Under the current legal framework, the PRC Network Security Law provides that the Cyberspace Administrative Office is responsible for coordinating and conducting national security reviews of network products and services procured by critical information infrastructure operators that may impact national security. The DSL expands the scope of this national security review beyond critical information infrastructure operators, though it does not detail how the data security review system will be implemented.

Data Export Control System

The DSL proposes data export control measures for complying with international obligations and safeguarding national security.

Counter-Measure System Against Discriminatory International Measures

The DSL provides that if any foreign states or regions discriminate against the PRC with respect to investment and trade related to data or data-centric technologies, the PRC can adopt corresponding counter-measures.

Data Security Compliance Obligations

The DSL proposes various data security compliance obligations for both entities and individuals.

General Obligations

The DSL imposes general obligations on entities and individuals who carry out any data activities (as defined above), including:

- Establishing comprehensive data security management systems, organizing data security trainings, and implementing necessary measures to ensure data security
- Strengthening risk monitoring, taking remedial actions when data security defects or loopholes are detected, and notifying users and authorities of security incidents

- For processors of important data, appointing data management teams and data security officers, and regularly conducting and reporting on risk assessments of their data activities

Non-compliant entities and individuals may face penalties including monetary fines of up to CNY1 million. Responsible personnel may be subject to fines of up to CNY100,000. Entities and individuals may also be required to remediate data use that may result in serious security risks.

Specific Obligations

Online Data Processing Operators

The DSL requires providers of online data processing services to obtain business permits or complete filings for their business operations. Failure to comply with such requirements may lead to penalties including demands to close down businesses and/or monetary fines of up to 10 times the illegal gains or up to CNY1 million if no illegal gains are derived. Responsible personnel may be subject to fines of up to CNY100,000.

The DSL itself does not detail which kind of online operators need to obtain permits or complete filings, but designates the Ministry of Industry and Information Technology (MIIT) to promulgate detailed measures regulating online data processing operators. Under the PRC's current laws, a company needs to obtain an electronic data interchange license (EDI license) issued by MIIT, before providing online data processing services. The relationship between the DSL's requirements for online data processing operators and the EDI license requirements are not yet clear.

Data Intermediaries

For the first time, data transactions will be regulated by law. The DSL requires data intermediaries to request data providers to explain the sources of data, verify the identities of the parties, and retain verification and transaction records. Non-compliant intermediaries may face penalties including revocation of business licenses and/or monetary fines of up to CNY1 million if no illegal gains are derived or 10 times the illegal gains. Responsible personnel may be subject to fines of up to CNY100,000.

Data Collection

The DSL prevents any organization or person from stealing data or obtaining data through other illegal methods. Penalties for breach include monetary fines of up to CNY1 million. Responsible personnel may be subject to fines of up to CNY100,000.

Investigation Assistance

The DSL imposes obligations on individuals and entities when responding to requests for information from public and national security authorities, and requires the authorities to follow applicable approvals processes for data collection.

Individuals or entities receiving requests from overseas law enforcement authorities for data stored in the PRC must report the request to the competent regulatory authorities, and obtain prior approval for the disclosure of that data (unless otherwise provided for under international treaties or agreements in which the PRC participates). These requirements supplement the existing practices under the Network Security Law and the Draft Guidelines.

Enforcement and Penalties

The DSL lists multiple government authorities that will oversee data security matters. On the central government level, the National Security Commission is responsible for coordinating with other

government authorities to issue and oversee state data security strategies and major policies. National security and public security bureaus are responsible for data security supervision and management within their respective remits. On the regional and departmental levels, local governments and regulatory authorities are responsible for data security in their respective regions and industries.

In parallel, cyberspace administrative offices are responsible for coordinating, overseeing, and supervising network data security.

Sanctions for breach of the DSL include demands for rectification, warnings, penalties, forfeiture of illegal gains, revocation of business licenses, and/or demands for closing down of businesses. Non-compliance with the DSL that rises to the level of a criminal or administrative offense may also be prosecuted criminally under the PRC Criminal Law or be subject to administrative penalties. The DSL also allows a party to recover damages through civil litigation in court.

Compared to the PRC Network Security Law, the DSL imposes a higher maximum penalty of CNY1 million for non-compliance with general data security obligations. For example, failure to establish cybersecurity management systems may subject network operators to a maximum penalty of CNY100,000 under the PRC Network Security Law, while failure to establish data security management systems as required by the DSL may subject entities and individuals to a maximum penalty of up to CNY1 million.

With regard to state organs and functionaries of state organs, disciplinary action may be taken against those who fail to perform data security protection responsibilities under the DSL or those who neglect their duties, abuse powers, or commit malpractice for personal gains.

Comparison to Other Jurisdictions

The DSL appears to have a broader scope than similar regulations in other jurisdictions, such as the European General Data Protection Regulation. The definition of “data” extends beyond data that is personal to individuals. Foreign data processing activities (even those that do not involve the data of individuals or entities in the PRC) will be impacted if they could be perceived to harm China’s national security or public interests. Moreover, the DSL empowers PRC authorities to reactively respond to discriminatory data regulation in other jurisdictions that may be adverse to PRC companies.

Conclusion

The DSL will significantly expand China’s legal framework around information and data security. It is drafted in broad terms and imposes a range of obligations on individuals and entities using data. In light of the extensive and complex issues addressed by the DSL, the implications for organizations could be significant.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Hui Xu
hui.xu@lw.com
+86.10.5965.7006
Beijing

Gail E. Crawford
gail.crawford@lw.com
+44.20.7710.300
London

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Kieran Donovan
kieran.donovan@lw.com
+852.2912.2701
Hong Kong

Aster Y. Lin
aster.lin@lw.com
+852.2912.2705
Hong Kong

This *Client Alert* was prepared with the assistance of Esther Zheng and Jasmine Hu in the Shanghai office of Latham & Watkins.

You Might Also Be Interested In

China Introduces Legislation that Enhances Personal Information Rights

China Issues DSL Measures to Restrict the Overseas Transmission of Personal Data

EDPB Guidelines — What Is the Territorial Reach of the GDPR?

Data Protection in Investigations

https://www.sites.lwcommunicate.com/5/178/forms-english/subscribe.asp to subscribe to the firm's global client mailings program.