LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice

July 21, 2021 | Number 2882

China's New Data Security Law: What to Know

The Data Security Law will enhance an increasingly comprehensive legal framework for information and data security in the PRC.

Key Points:
Notably, the DSL:

- Applies to a wide range of data and data activities, with extraterritorial jurisdiction
- Refines regulations on "important data" and emphasizes protection of "core state data"
- Imposes a set of obligations combined with high fines and severe penalties on entities and individuals who conduct data activities

Background

On June 10, 2021, the Standing Committee of China's National People's Congress passed the Data Security Law (DSL), which will take effect on September 1, 2021. The primary purpose of the DSL is to regulate "data activities" (as defined below), safeguard data security, promote data development and usage, protect individuals and entities' legitimate rights and interests, and safeguard state sovereignty, state security, and development interests. 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).

Scope

Jurisdiction

The DSL provides broader extraterritorial jurisdiction than the Network Security Law. 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 citizens or entities"

Comparatively, the Network Security Law applies to limited network activities occurring outside of the PRC that attack, infringe, interfere with, or damage critical information infrastructure in the PRC and lead to severe consequences.

Regulated activities

The DSL broadly defines "data" as any record of information created in electronic or other forms.

The DSL's definition of "data activities" is also comprehensive and includes data collection, storage, usage, processing, transmission, provision, and disclosure of data. In particular, the DSL regulates the commercial "transaction" of data for the first time.

The DSL provides that data activities as part of statistical and archival works, as well as data activities involving personal information, must also comply with other applicable laws and regulations.

The DSL does not apply to:

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

Enforcement

The DSL lists multiple government authorities that will oversee data security matters:

- On the central government level, the Central National Security Leadership Organ[1] is responsible for issuing and overseeing national data security strategies and major policies, and is required to establish a national data security working and coordination mechanism (Mechanism). 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, the Cyberspace Administration of China is responsible for coordinating, overseeing, and supervising network data security.

The DSL requires industrial organizations to issue data security codes of conduct and organizational standards, and guide members to strengthen the protection of data security. In addition, the DSL entitles individuals and entities to report activities in violation of the DSL to related authorities, and requires the authorities to deal with the reports in a timely manner and maintain confidentiality of the reports and the reporters' information.

Data Development and Data Security

The DSL provides directions and guidelines to encourage data development and data security from a macro perspective. According to the DSL, the focus on data development and data security is expected to:

- Advance data security via data development and usage and industrial development, and safeguard data and industrial development via advanced data security
- Implement big data strategy and promote data infrastructure development
- Improve the intelligence of public services via data usage and development

- Support data development and usage and data security technology research
- Establish national standards of data development and usage and data security
- Promote the development of data security testing, assessment, and certification services
- Establish a comprehensive data transaction management system to regulate data transaction activities and cultivate the data transaction market
- Support education and trainings relating to data development and usage and data security

Data Security Framework

The DSL defines "data security" as the ability to ensure that data is effectively protected and lawfully used through adopting necessary measures, and remain continually in a secure state. The DSL sets out a 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, public interest, and individuals' and entities' legitimate rights and interests. Using the class-based system as a guide, the DSL requires the Mechanism to coordinate with related authorities to provide a list of "important data"[2] to strengthen the protection of the relevant data.

The DSL further introduces the concept of "core state data" and emphasizes that the state will implement a strengthened management system in relation to core state data involving national security, lifelines of the national economy, important people's livelihood and major public interests.

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.

Data security risk management system

The DSL requires that a unified, effective, and authoritative system is established to evaluate, report, share, and monitor data security risks but does not elaborate on the details, which are pending future regulations and/or national standards.

Emergency response system for data security incidents

The DSL requires that an emergency response system for data security incidents is established. Effectively, upon the occurrence of a data security incident, relevant authorities are required to carry out emergency plans to mitigate security risks, eliminate safety hazards, 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, and stipulates that the security review decision made via the system will be a "final decision."

Under the current legal framework, the 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 (CIIOs)[3] that may impact

national security. The DSL expands the scope of this these reviews 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 requires that export control measures are implemented for data to be transferred overseas and within the scope of controlled items as defined in related export control laws and regulations.

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 imposes various data security compliance obligations on entities and individuals.

General obligations

The DSL imposes general obligations on entities and individuals who carry out any data activities, 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
- Regularly conducting risk assessments of the data activities for processors of important data, and reporting results to related authorities

Non-compliant entities and individuals may face penalties including monetary fines of up to CNY2 million (~US$310,000) per case and/or revocation of business licenses or demands to close down businesses. Responsible personnel may be subject to fines of up to CNY200,000 (~US$31,000).

Entities and individuals who violate the core state data management system or harm state sovereignty, national security, and development of interests may face penalties including monetary fines of up to CNY10 million (~US$1.5 million) per case and/or revocation of business licenses or demands to close down businesses, and bear criminal responsibilities (if applicable).

Specific obligations

Cross-border data transfer

The DSL stipulates that the cross-border transfer of "important data" collected and produced by CIIOs must comply with the Network Security Law. The cross-border transfer of important data collected and produced by other business operators must comply with related regulations issued by the Cyberspace Administrative Office and other authorities under the State Council.

Non-compliant entities may face penalties including monetary fines of up to CNY10 million (~US$1.5 million) and/or revocation of business licenses or demands to close down businesses. Responsible personnel may be subject to fines of up to CNY1 million (~US$150,000).

Data collection

The DSL prevents any organization or person from stealing data or obtaining data through illegal methods.

Data intermediaries

The DSL requires data intermediaries to request that data providers 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 (~US$150,000) if no illegal gains are derived, or 10 times the illegal gains. Responsible personnel may be subject to fines of up to CNY100,000 (~US$15,000).

Online data processing operators

The DSL requires providers of online data processing services to obtain administrative permits for their business operations.

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. Penalties for breach include monetary fines of up to CNY500,000 (~US$77,000) for entities. Responsible personnel may be subject to fines of up to CNY100,000 (~US$15,000).

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). Penalties for breach include monetary fines of up to CNY5 million (~US$770,000) for entities. Responsible personnel may be subject to fines of up to CNY500,000 (~US$77,000).

Penalties

Sanctions for breach of the DSL include demands for rectification, warnings, monetary fines, forfeiture of illegal gains, revocation of business licenses, and/or demands to close down 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 allows parties to recover damages through civil litigation in court.

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.

Administrative Data Security and Publication

The DSL, again for the first time, regulates the security and publication of government data at the legislation level. State organs must conduct data collection and usage in accordance with applicable laws, rules, and regulations, and must establish data security management system. Functionaries of state

organs must keep the confidentiality of personal privacy, personal information, and trade secrets obtained in performance of duties.

State organs must entrust others to build and maintain electronic administrative systems, as well as store and process administrative data. State organs should adhere to strict approval procedures, and should supervise the entrusted parties to fulfill their corresponding data security protection obligations.

The DSL further provides the establishment of a government data disclosure directory to set up a unified, safe, and controllable government data disclosure platform.

Conclusion

The DSL is understood to have a profound influence on China's data and information regulation. Given its broad coverage and expansive compliance obligations, it is advisable for individuals and entities engaging in data activities to closely monitor further legislative developments, and perform necessary self-evaluations to assess status of data compliance as early as possible.

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

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

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

You Might Also Be Interested In

China Issues Draft Data Security Law for Public Comment

Extensive Changes to Singapore's Data Protection Regime Take Effect

Transferring Data Between Japanese Companies and the UK Post-Brexit

Hong Kong Considers Sweeping Changes to Privacy Laws

Endnotes

[1] According to the PRC National Security Law, the Central National Security Leadership Organ is a central national organ responsible for the decision-making, discussions, and coordination of national security projects. The Central National Security Leadership Organ formulates, guides, and implements national security strategies and other related significant policies, as well as coordinates major national security matters, and promotes the construction and development of national security rule of law.

[2] The term "important data" was first introduced in the 2016 in the PRC Network Security Law, which 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. For example, in military sector, "important data" include information on the name, quantity, source and agent of purchased components, software, materials, industrial control equipment test instruments, and information on the internal name, geographical location, construction plans, security planning, secrecy level, plant drawings, storage volume, reserves of military research and production institutions; in petrochemicals sector, "important data" include main economic and technical indicators and major policy measures in annual, medium-term and long-term development plans of the national petroleum and petrochemical industries, and annual import plans for important production materials in petrochemical industry.

[3] According to the PRC Network Security Law, for critical information infrastructure (CII) 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 being damaged, disabled or with their data disclosed, may severely threaten the national security, national economy, people's livelihood and public interests, the State shall impose extra protection on the basis of cybersecurity multi-level protection system. The specific scope and security measures for critical information infrastructure shall be developed by the State Council.

According to the Guidance on Implementing the Cybersecurity Multi-level Protection System and Critical Information Infrastructure Security Protection System issued by the PRC Ministry of Public Security in 2020, competent authorities in important industries and sectors such as public communication and information services, energy, transportation, water conversancy, finance, public services, e-government, and defense technology industry shall formulate the identification guidance of CII in their industries and sectors, and timely notify the relevant operators of the identification results and report to the Ministry of Public Security.