protiviti®
Face the Future with Confidence

National People's Congress of China Publishes Draft of New Data Security Law

July 30, 2020

On July 3, 2020, China's top lawmaking body, the National People's Congress of China (NPC), published the draft of China's Data Security Law (DSL) for public comment. If passed, this law will establish a regulatory framework for data security in China, with a focus on governing data that, if leaked, could impact the country's national or economic security, social stability, or public health and security.

The reach of the law goes beyond China's borders, however. Article 2 states that the draft law applies not only to data activities within the country, but also to foreign organisations and persons that conduct any data activities which could harm China's natural security, public interests or the rights of Chinese citizens. Companies with operations in China may be required to disclose information about the security of their networks outside of China or to have their cyber security programs reviewed and certified by Chinese officials.

Overview of the Draft DSL

The draft DSL is composed of 51 articles across 7 chapters. Major legal compliance requirements can be found in Chapter 3 through Chapter 5, while legal prosecution and punishment are prescribed in Chapter 6. The summary of those compliance requirements includes:

- Data security administrative regulation (Chapter 3)
- Data security obligations (Chapter 4)
- Data services permission (Chapter 4)
- Data security regulation for administrative agency (Chapter 5)

The draft also defines various punishments, such as administrative fines, revocation of permits and business licenses, and administrative custody, as well as criminal prosecution where applicable, in accordance with relevant laws and administrative regulations. Multiple laws and regulatory rules can also be referenced for legal enforcement, including Public

Security Administration Punishment Law, Criminal Law and National Security Law of China.

Compliance Requirements of the Draft DSL

The draft DSL prescribes multiple compliance requirements and obligations for companies to control and process data. The law considers data as assets that have strategic significance and implications for geopolitical competition. It is intended to establish new international rules under the control of China, from which the Chinese government expects to gain advantages from economic and security perspectives. Meanwhile, the law is developed to increase the controls on information transmission for avoiding negative impacts to China.

Major compliance requirements in the DSL include the following:

ARTICLE	LEGAL REQUIREMENTS
Data Security Obligations	
Article 25	The processor of important data must: • Establish specific position and organisation for data security and protection • Comply with legal regulations and national standards • Establish a data security and protection policy • Organise training and awareness for data security and protection • Conduct technical controls for data security and protection in data lifecycle
Article 26*	The data research and development must: • Benefit economic and social development • Improve the welfare of people • Conform to social morality and ethics
Article 27	The legal entity in the data lifecycle must: • Enhance data risk monitoring • Remediate and mitigate detected vulnerabilities • Report security incidents to customers and regulatory agencies
Article 28	The processor of important data must: • Conduct a regular risk assessment and file risk reports to regulatory agencies
Article 29	Legal entities must not: • Collect data in any illegal method or beyond necessary scope or limitation
Article 32*	Legal entities must: • Cooperate with the data request from public and national security agencies

Article 33	Legal entities must: • Provide data requested by foreign legal enforcement after obtaining permission from the regulatory agency
Data Services Permission	
Article 30	The agency for data trade must: • Review the identities of both parties in trading and maintain records
Article 31*	Data processing services must: • Obtain industrial permission or registration according to industrial regulatory rules
Data Security Administrative Regulation	
Article 19	The state implements data classification for protection, and catalogues will be developed by administrative and industrial regulatory agencies for important data protection
Article 20	The state will establish data security risk assessment, reporting, information sharing, monitoring and alarming mechanism
Article 21	The state will establish an emergency response mechanism to handle a data breach and release associated information for the public
Article 22*	The state will establish a data security inspection and review mechanism
Article 23	The state will implement export controls on data in catalogues
Article 24	The state will take similar actions against discrimination on investment and trade for data research and development

Note: This list is not exhaustive.

* Due to vague provisions and sweeping definitions, this article involves potential risks of direct data ownership threats as well as legal prosecutions.

Compliance Implications

Sensitive Data Protection in Critical Industries

The draft DSL empowers legal enforcement agencies to inspect and review data security. Meanwhile, companies are required to cooperate with security agencies for investigations on suspected violations. Moreover, under Article 31, online data processing services will be controlled by industry regulatory agencies. These legal requirements might expose sensitive data to scrutiny or inspection, or even external access. Such exposure might lead to legal dispute, reputation damage and intellectual property loss. Such exposure of sensitive information in certain industries could raise concern to the multinational companies in those industries. Some examples are:

- Innovative Information Technology: cloud computing, big data, IoT, artificial intelligence, etc.

- High-Tech Equipment and Intelligent Manufacturing: aerospace, marine engineering, integrated circuit, etc.
- Biological Industry: biomedicine, biotechnology, genetic data, stem cell research, etc.
- New Energy: new power generation, energy-saving technology, etc.
- Environment Protection: pollution prevention and solution, resource recycling, waste disposal, etc.
- Material Industry: high-strength low-alloy steel, superalloy, high-temperature plastic materials, etc.
- Digital Innovation: virtual reality, augmented reality, digital interaction and design, etc.
- New-Energy Automobile: new-energy battery, connected drive, energy storage, energy conversion, etc.

Compliance Risk on Data Access Request

The draft DSL claims legal obligations and administrative controls over all personnel in related companies (or local subsidiaries of multinational companies), including third-party service providers. This means that law enforcement forces or industry regulatory agencies can directly request data from anyone in the companies. Declining the request for data may put the requested person at risk of administrative and criminal punishment. However, complying with the data request may require the person to make decisions for disclosing personal and confidential information. Subsequently, this may put the companies (or other subsidiaries or the headquarters of the multinational companies) at risk for legal sanctions from another sovereign state, business or civil litigation, or reputation damage, as well as significant revenue loss.

Compliance Risk on Third-Party Services

The draft DSL requires extra licenses for online data processing service providers – on top of the current Secondary Telecommunication Services (B21) and Electronic Data Interchange (EDI) licenses.

This requires further effort from companies and service providers. Companies will need to review the license of existing service providers. If the service providers do not have the extra license, companies might need to change to a new service provider, which may lead to unexpected investment and effort.

Technical Feasibility and Consistency

The draft DSL has granted authority to multiple ministries and commissions, as well as industry regulatory agencies. This will require legal entities to comply with legal requirements at different levels: central government, provinces, cities and industries. These requirements may be not consistent with each other since each administrative bodies might have their own interest to reflect. Furthermore, as most enterprises have their own security policies and architecture designs, the DSL requirements may not be consistent with the policies and designs of the companies.

Next Steps

In response to the increased data important to economic development and geopolitical competition, China's Data Security Law, if passed, will mean enterprises will likely face more security compliance obligations, placing further demands on already over-burdened IT divisions. Companies should be continue to monitor developments related to the law and should keep the management team informed as they begin to proactively devise their approach for complying with the new standards, should they become law.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

How Can Protiviti Help?

Protiviti can assist companies with preparing for this major change in data management in a variety of ways. Our professionals can:

- Assess organisational privacy risks, using best-of-breed privacy frameworks.
- Define long-term privacy objectives and the strategic plans to implement and operationalise privacy practices.
- Elaborate personal data inventories and processing activities; document data flows and Records of Processing Activities.
- Evaluate vendor risk programs and safeguards.
- Collaborate with Internal Audit departments to facilitate Privacy Program maturity assessments and organisational compliance with privacy laws and regulations.
- Identify and design process and technical solutions to remediate compliance gaps and enhance privacy operations.

protiviti®