GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

July 2021

China Finalizes Data Security Law

On June 10, 2021, the final version of *Data Security Law* (***DSL***) of the People's Republic of China was published, and the *DSL* will take effect Sept. 1, 2021. Prior to the issuance of the final version, two drafts of the *DSL* were released to the public seeking comments, in July 2020 and April 2021, respectively. While the *DSL* provides for a three-level data classification system, the obligations for each classification level are described in vague and broad terms, making it likely that in the near future a regulation or official documents will be released that contain the precise compliance responsibilities.

Scope and Application of the *DSL*

The *DSL* applies broadly to both online and offline data processing activities. Article 3 of the *DSL* provides the definition of "data," "data processing," and "data security." Under the *DSL*, "data" refers to any record of information in electronic form or other form, "data processing" refers to the collection, storage, use, processing, transmission, provision, and disclosure of data.

The *DSL* not only regulates the domestic data processing activities but also has extraterritorial reach. Article 2 of the *DSL* provides that it applies to the data processing activities and data security regulation performed within the territory of the People's Republic of China, as well as the data processing activities performed outside of the territory of the People's Republic of China that threaten national security, public interests, or the legitimate rights and interests of the citizens or organizations of the People's Republic of China.

Data Classification Protection System

A data protection system with three classification levels will be implemented on a national scale. Classification will be determined based on the data's level of importance to economic and social development, and the scale of potential harm to national security, public interest, or the legitimate rights and interests of individuals or organizations in the event that the data are tampered with, destroyed, leaked, or illegally obtained or used. "National core data," defined in Article 21 of *DSL*, is the highest level of the three-level system and refers to the data "have a bearing on national security, the lifelines of national economy, people's key livelihood and major public interests." The national core data are subject to a stricter management system than that of the "important data," which is at the middle of the three-level classification system. However, the definition of "important data" is not provided in the *DSL*. Article 21 of the *DSL* only provides that (i) the national data security work coordination mechanism shall coordinate with the relevant departments/functions to formulate the catalogues for the important data and strengthen the protection of important data; and (ii) each region and department shall in accordance with the three-level classification data system, determine the specific catalogue for important data for the respective region and department, and of the relevant industries and sectors, and undertake special protection for the data included in such catalogue.

The definition of "important data" is otherwise provided in other legal documents (which can shed some light on such definition under the *DSL*, although these documents have only been published for public comment and are not finalized). In April 2017, the Cyberspace Administration of China issued a document for public comment – *Circular of the Cyberspace Administration of China on Seeking Public Comments on the Measures for Evaluating the Security of Transmitting Personal Information and Important Data Overseas (Draft for Comment)*, which defines "important data" as "the data closely related to national security, economic development and public interests, and the relevant national standards and guidelines for identification of important data shall apply mutatis mutandis to the specific scope of important data." Another document, *Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comment)*, published in August 2017 by the National Technical Committee on Information Security of Standardization Administration, provided a similar definition of "important data": "the data (including raw data and derived data) collected, generated in China by the relevant organizations, institution that are closely related to national security, economic development and public interests, but do not involve the national secrets."

Under the *DSL*, the listed responsibilities under the three-level data classification system are vague and broad, making it difficult to know their precise terms and obligations. Therefore, it seems likely that in the near future a regulation or official documents will be released that contain the precise compliance responsibilities. The issuance of *the Classification Guidance for Industrial Data (for Trial Implementation)* by the Ministry of Industry and Information Technology in February 2020 shows that classification of industrial data has taken place. With less than two months before the Sept. 1, 2021 effective date of the *DSL*, it is likely more data protection classification guidance or standards will be issued soon.

Data Security Mechanisms

In addition to the above data classification protection system, Chapter III - Data Security Systems of the *DSL* includes other data security mechanisms that must be established at the national level.

- **Mechanism for data security risk assessment, reporting, information sharing, supervision, and early warning**: Article 22 of the *DSL* stipulates that China shall establish a centralized, efficient, and authoritative mechanism for data security risk assessment, reporting,

information sharing, supervision, and early warning, and such mechanism involves the national data security work coordination mechanism for the coordination of the relevant authorities in their work of collection, analysis, determination, and early warning of the data security risk information.

- **Response mechanism to data security emergency**: Article 23 of the *DSL* stipulates that China shall establish a response mechanism to data security emergency, in which the relevant authority shall activate the contingency plan, adopt appropriate emergency response measures, prevent the expansion of harm, eliminate security risks, and promptly publish warning information related to the public.
- **National security review mechanism**: Article 24 of the *DSL* stipulates that China shall establish a data security review mechanism in which the data processing activities that affect or may have effect on national security will undergo the national security review, and such security review decisions issued in accordance with the law are final.
- **Export control mechanism**: Article 25 of the *DSL* stipulates that China shall implement export controls on the data which belong to the controlled-items categories in accordance with the law on data and those relevant to safeguarding national security and interests and fulfilling international obligations.
- **Anti-discrimination mechanism**: Article 26 of the *DSL* stipulates that China may adopt the equivalent measures (depending on the actual circumstances) against the country or region which adopts discriminatory prohibitions, limitations, or other similar measures in the investment, trade, and other areas against China, related to the data and data development and use technology.

Protection Responsibilities of Data Processors

Chapter IV of the *DSL* – Data Security Protection Responsibilities – includes the data protection responsibilities of data processors (including entities and individuals, public security organizations, and national security organizations and other competent authorities of China).

- **Establishment of data security management system**: The data processors shall establish a sound data security management system for the workflow of the data processing activities, organize and conduct data security education and training, and adopt corresponding technical measures and other necessary measures to safeguard data security. Those conducting data processing activities via the internet or other information networks shall perform the above data security protection obligations based on the multi-level protection scheme of cybersecurity (MLPS), which refers to the MLPS 2.0, a complex technology standard (updated in 2019) that requires companies as network operators to assess the current status of information and operations technology systems and the associated risks. The MLPS 2.0 requires network operators to classify their infrastructure and application systems into five separate protection levels and undertake the corresponding responsibilities. Those processing "important data" shall additionally specify the responsible person and management bodies for data security to implement the data security protection responsibilities.
- **Risk monitoring and control and report responsibilities**: Data processors shall strengthen risk monitoring and adopt remedial measures immediately once risks such as data security flaws and vulnerabilities are discovered, take immediate disposal measures once a data security incident occurs, and notify the users as required and report to the relevant authorities.
- **Regular risk assessment and report responsibilities**: The processors of "important data" shall regularly conduct risk assessments for data processing activities and submit to relevant authorities the risk assessment report, which must disclose the contents of the categories and quantities of the

important data processed, the implementation of the data processing activities, data security risks, and countermeasures.

- **Compliance with laws, social morals, and ethics**: (i) Data processing activities and research and development of new data technologies shall conform to social morals and ethics, and contribute to the advancement of economic and social development and the people's welfare; (ii) data collection conducted by any organization or individual shall adopt lawful and proper methods and shall not steal data or obtain them by other illegal means. Such collection shall comply with the legal provisions and administrative regulation related to the purpose or scope of data collection or use; (iii) data processing service providers shall obtain an administrative license if such license is required by the laws and administrative regulation for the data processing activities.
- **Review and record retention for data transaction responsibilities**: The data transaction intermediary service agency shall require data providers to explain the source of data, examine and verify the identity of the parties in such transaction, and retain the records of such review and transaction.
- **No abuse of data access right by public security organizations and national security organizations**: The public security organizations and national security organizations shall comply with strict approval procedures and relevant legal provisions, when such authorities need data access for to safeguard national security or investigate a crime.
- **Cross-border transfer of data**: (i) The provisions of the *Cybersecurity Law* of China shall apply to the outbound transfer of important data collected and generated during the operation of key information infrastructure in China; (ii) the outbound transfer of important data collected and generated in China by other data processers shall be applied to the administrative measures formulated by the national cyberspace administration authority jointly with the relevant departments of the State Council of China; (iii) any organization or individual in China, without the approval of the competent authority of China, must not provide any foreign judicial body or law enforcement body with any data stored in China; (iv) the competent authority of China shall handle the request(s) from any foreign judicial body or law enforcement body for providing any data in accordance with the relevant laws and the international treaty or agreement which China has concluded or acceded to, or under the principle of equality or mutual benefit.

Penalties for Violations of the *DSL*

The penalties imposed by the *DSL* in Chapter VI – Legal Liabilities for the violations of the *DSL* – include the issuance of an order to make a correction, and a warning, confiscation of illegal income (if any), imposition of fines to the organization and individual, or concurrently imposition of fines to the directly responsible person or person in charge (if any), issuance of an order to suspend the relevant business, or stop operation for rectification, or revocation of the relevant business permits or business license, or other sanctions in accordance with laws and regulations, and the relevant civil liabilities and/or criminal liabilities shall be imposed. Among the penalties for the various violations, the fines imposed for violation of the management system for national core data and causing harm to national sovereignty, security and development interests, are the most severe, ranging from Chinese yuan 2 million to 10 million.

In addition to the above penalties, the *DSL* includes one administrative measure: if the relevant competent authorities (in the course of performing their duties) discover any major security risk in data processing activities, they may make an appointment with the relevant organizations and individuals to discuss, and require such organizations and individuals to take corrective measures and eliminate hidden problems.

** This GT Alert is limited to non-U.S. matters and law.*

Authors

This GT Alert was prepared by:

- George Qi | +86 (0) 21.6391.6633 | qig@gtlaw.com
- Qianqian Li | +86 (0) 21.6391.6633 | liq@gtlaw.com