DS NEWSLETTER savoir, faire
NEWSLETTER – LEGAL INFORMATIONS
PROPOSED BY DS AVOCATS

Seek a quick path to know the new PRC Data Security Law? Check the FAQs!

ASIE

Facing the increasingly complicated international economic and political climate, and the domestic data issues (leakage of data, etc.), *PRC Data Security Law (DSL)* is in urgent need in the PRC. As the first fundamental data law, it took almost 3 years to formulate *DSL*. It was approved on June 10th, 2021 and will become effective on September 1st, 2021. Obviously, *DSL* will affect almost all industries, who only have a few months to be ready. Because *DSL* is concise, vague and technical to some extent, to help enterprises better understand it, we present the following frequently asked question (FAQs) with brief answers for your reference.

WHAT IS THE RELATIONSHIP BETWEEN *CYBER SECURITY LAW (CSL)*, *DSL* AND THE UPCOMING *PERSONAL INFORMATION PROTECTION LAW DRAFT [PIPL (DRAFT)]*?

CSL was released in 2016 and became effective on June 1st, 2017. It applies to the construction, operation, maintenance and use of the network as well as the supervision and administration of the cybersecurity within the PRC. *CSL* requires network operators to fulfill several basic obligations of "cyber data" (which refers to all kinds of electronic data collected, saved, transmitted, processed and generated through the network.). However, *CSL* does not define "data" in a general way or set forth detailed regulatory regime concerning data.

PIPL (Draft) applies to activities of processing personal information of natural persons within and outside (conditionally) the PRC. Hence, personal information is part of data to be specially regulated by the upcoming *PIPL*.

The regulatory scope of *DSL* is more general than *PIPL (Draft)*. Except data concerning state secrets (governed by *the Law of the PRC on Protecting State Secrets*) and military data (governed by measures formulated by central government), general data shall be governed by DSL. As for personal information, *DSL* and *PIPL (Draft)* shall be applicable at the same time, and the latter would be the special law with its priority in application.

WHAT IS THE TERRITORIAL SCOPE OF *DSL*?

DSL is to regulate the data processing activities carried out within the territory of the PRC and ensure data security.

Meanwhile, it also mentions that legal liabilities shall be investigated where data processing activities carried out outside the territory of the PRC harms the national security, public interests, or the legitimate rights and interests of citizens or organizations of the PRC. *DSL* is the first law to clarify the long-arm jurisdiction of data outside the PRC. It is possible that some counteracting discriminatory measures will be used as the punishment in this scenario.

WHAT TYPE OF DATA WILL BE REGULATED BY *DSL*?

Per *DSL*, data shall refer to any record of information in electronic or other form. In other words, here data not only refers to content saved under electronic devices but also content showed in traditionally ways (i.e. in writing). It is necessary because it becomes easier nowadays to change the carrier of data than before. For example, wechat mobile application already has the function to extract information from hardcopies, not to mention other professional applications to transfer files into different formats.

WHAT ARE THE MAIN PRINCIPLES OF *DSL*?

DSL lists the following principles.

- Data classification protection system;

Data should be managed and graded per its importance and the damage it may cause.

※ important data protection system;

Industries and authorities should formulate the catalogue of important data and put important data under strict regulation.

※ national core data protection system;

For data matters national security, national economy and livehood, public interests, etc., it shall be considered as national core data and subject to stricter regulation.

- Data security risk early warning and emergency response mechanism;

Authorities will share data security information, jointly analyze risks, decide on disposal measures and issue alerts. Besides the existing requirements for enterprises under *CSL*, *DSL* sets forth how authorities will manage data accidents.

- Data national security review mechanism;

Authorities shall have the right to conduct security assessment of data processing activities which affects or may affect national security.

- Data export control system; and,

Authorities will formulate other regulations to regulate the export of important data processed by non-CIIOs (see paragraph 7 below).

- Counter-acting discriminatory measures.

For any discriminatory measures taken by any country or region against the PRC in terms of the investment and/trade of data and/or use of data, Chinese authority may adopt the equivalent measures against such country or region.

WHAT ARE THE MAIN OBLIGATIONS OF ENTERPRISES PER *DSL*?

- Obtaining data in a lawful and proper way;
- To establish and improve the whole process of data security management system, organize and carry out data security education and training, and take corresponding technical measures and other necessary measures to ensure data security. When using the Internet and other information networks to carry out data processing activities, the above-mentioned data security protection obligations shall be fulfilled on the basis of the Multi-level Protection Scheme required by *CSL*;
- Risk monitoring shall be strengthened for data processing activities. When risks such as data security defects and loopholes are found, remedial measures shall be taken immediately. When data security incidents occur, disposal measures shall be taken immediately, and users shall be informed in time according to regulations and reported to relevant competent departments; and,
- For institutions engaged in data transaction intermediary services, data providers should be required to explain the data sources, verify the identities of both parties, and keep audit and transaction records.

WHAT IS THE COMPETENT AUTHORITY IN CHARGE OF DATA SECURITY MATTERS IN THE PRC?

The Cybersecurity Administration of China (CAC) and its branches at all levels are responsible for the comprehensive coordination of online data security and related supervision. In practice, other authorities may also participate in the regulatory activities, such as Public Security Bureaus, national security authorities, relevant competent authorities of industries.

WHAT IS NEW ABOUT *DSL* IN CROSS-BORDER DATA TRANSFER?

CSL sets forth the requirements on cross-border data transfer for critical information infrastructure operators (CIIOs). So, what about the requirements for cross-border data transfer for non-CIIOs? In fact, *DSL* does not answer the question directly and only points out that the relevant measures will be formulated by the authorities. So this issue remains to be solved by the upcoming law and regulations which stay draft version yet.

HOW ABOUT DATA USED IN FOREIGN JURISDICTION OR LAW ENFORCEMENT AUTHORITIES?

The State will handle requests for data from foreign judicial or law enforcement authorities in accordance with international treaties, agreements or the principle of equality and reciprocity. Without the approval of the competent authorities of the PRC, domestic organizations (including enterprises) and individuals shall not provide data stored in the PRC to foreign judicial or law enforcement authorities. Violation of this requirement will bring a fine up to RMB 5 million for the legal entity and RMB 500,000 for the person in charge, plus revocation of business license in worst case.

WHAT IS THE CONSEQUENCE FOR VIOLATION OF *DSL*?

Situations (non- exhaustive list)	Punishment (non- exhaustive list)
Violation of the obligation of data security protection	• The maximum fine for a legal entity is RMB 2 million, and such legal person can be ordered to suspend relevant business, suspend business for rectification, and revoke its business approval or business license. • The maximum fine for the person in charge and other persons directly responsible is RMB 200, 000.
Violation of the national core data management system, which endangers national sovereignty, security and development interests	• a fine of no less than RMB 2 million but no more than RMB 10 million; • order to suspend relevant business or stop operation for rectification, or be subject to revocation of relevant business permits or business license; • where a crime is constituted, they shall be held criminally liable in accordance with the law.
provide important data to overseas countries in violation of the provisions of the *DSL*	• a fine of no less than RMB 100,000 but no more than RMB 10 million; • order to suspend relevant business or stop operation for rectification, or be subject to revocation of relevant business permits or business license; • The maximum fine for the person in charge and other persons directly responsible is RMB 1 million.

***

Data is already key for digital enterprises and more enterprises are racing to become digitalized. In this context, data compliance is not an additional request but a mandatory and fundamental compliance task faced by enterprises. Though we believe the authorities will allow enterprises some time to take a breath and get prepared, it is advised to seriously take into account data compliance and bring it into agenda. At least, it cannot be done overnight.

For any additional information please contact:

ZHANG Beibe
Associate- Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer- Shanghai Office
doyon@dsavocats.com