Checklist
Data Security Law of China

Are you on track for compliance with the Data Security Law of China?

On 10 June 2021, the Data Security Law (the "DSL") was passed in the Standing Committee of the National People's Congress and will take effect on 1 Sep 2021. The DSL serves as a fundamental legislation in the field of data security and compliance. Various obligations are imposed on entities that process any amount of data in and outside China. There is also expected to be a series of implementation rules to clarify the relevant obligations in the future.

How can multinational corporations prepare for compliance at this stage? We have listed the following the DSL Checklist to help companies grasp the important points and understand what they are suggested to do next to adapt to these rules more smoothly.

You also should be aware of the consequences in case of a violation. The legal liabilities may include warning, correction order, fine, suspension of business, and revocation of business license. This Checklist can serve as a quick-reference guide. On top of this, you are suggested to pay close attention to relevant updates. And it is highly recommended to ask professional law firms for help so that you can build reliable company policies and systems.

The DSL Compliance Checklist is as follows.

Category	Action(s) / Deliverable(s)	Article of DSL
1. Scope of Application and Extraterritorial Reach		
(1) Application Scope and Extraterritorial Reach	☐ Asse ss whether your organization is processing any data in China. • *Note: "**data**" under the DSL refers to any record of information in electronic or non-electronic form.* • *Note: "**data processing**" include activities such as the collection, storage, use, refinery, transfer, provision, or public disclosure of the data.*	2
	☐ Assess whether your organization is processing any data outside China, which may have an impact on the national security, public interests, or the lawful rights and interests of citizens or organizations in China. • *Note: this clause provides a broad scope of extraterritorial reach and the DSL does not give typical examples of such cases. Generally, processing data collected or generated from business operation in China will be caught by this clause.*	2
2. General Considerations for Data Processing		
2.1. Data Governance		
(2) Policy Framework	☐ Introduce external facing terms of services, policies, guidelines, and/or directions ("**Policies and Guidelines**") or review your existing Policies and Guidelines and make amendments to ensure compliance of relevant requirements under the DSL.	27
	☐ Introduce internal data security governance model and relevant operation guidelines or review existing internal Policies and Guidelines and make adjustments to ensure compliance of relevant requirements.	27
	☐ Implement policies on technical measures such as data encryption, data back-up and access control to ensure security.	27
	☐ If your organization is engaging in providing intermediary services for data transaction, such as a data broker, establish a policy to check the identity of the data provider and the data recipient.	33
(3) Incident Response	☐ Establish a response policy for data security incidents.	29
	☐ Establish a mechanism to deal with notification to users and authorities about data security incidents.	29
(4) Trainings and Education	☐ Provide education and training programs on data security to employees with a role in data processing, security, or compliance.	27

2.2. Data Security Measures and Obligations		
(5) Data Operation	☐ Check if your data is from legal and proper sources, for example, by: • clarifying the scope, purpose, method, and security measures of data collected in each business scenario if the data is directly collected by yourself; • ensuring that there are measures to verify or commitments as to the lawfulness of data sources if the data is collected and provided by others and keep relevant records. ☐ Ensure to obtain an administrative license when processing the data that requires the license according to laws or administration regulations. ☐ Conduct risk monitoring and adopt remedial measures immediately when your organization identifies risks such as data security defects or breaches.	32 34 29
(6) Multi-Level Protection Scheme (MLPS) of Cybersecurity	☐ Check if an MLPS assessment is properly conducted. ☐ Perform data security obligations imposed by the DSL based on requirements of the corresponding security level (1 to 5) under the MLPS.	27 27
(7) Classification and Categorization of Data	☐ Monitor updates issued by sectoral authorities and local authorities on catalogues of Important Data and National Core Data and ensure that they are implemented in your classification and categorization of data. • *Note:* **Important Data** *refers to "data that is closely related to national security, economic development and societal and public interests".* • *Note:* **National Core Data** *refers to "data related to national security, the lifeblood of the national economy, people's wellbeing, and public interests, which is subject to a stricter management system".*	21
(8) Provide E-gov Vendor Services to State Agencies	☐ Obtain relevant approval and fulfill corresponding data security protection obligations in accordance with the laws and regulations and contractual agreements. Do not retain, use, disclose or provide government affairs data to others without authorization.	40
2.3. Export Control over Data		
(9) Export Control	☐ Monitor the updates related to China's Export Control Law, check the control list to determine whether it is applicable to any of your data and, if applicable, • keep updated of regulations and enforcement activities by the enforcement bodies including the ministry of commerce, the ministry of industry and information technology and the central military commission; • isolate the data of controlled items from other data and implementing differentiated access control for the data of controlled items between Chinese employees and non-Chinese employees. ☐ Check license application procedures for controlled items.	25 /

2.4. Data Security Review		
(10) Data Security Review	☐ Establish an internal review procedure prior to the launch of new projects involving Important/National Core Data and new data processing activities that may have an impact on national security of China. ☐ Monitor the updates related to the Cybersecurity Review Measures and its enforcement activities. • *Note: the Cybersecurity Review Measures issued in June 2020 is under the speedy process of amendments since the Didi was under this kind of investigation early July. In its revised draft for public comment, the procedures and key considerations of the national security review under the DSL are provided.*	24 24
2.5. Access to Data by Authority		
(11) Data Assess by Chinese authorities	☐ Cooperate with the Chinese public security agency and national security agency when they need to access data for legitimate reasons and procedures such as safeguarding national security or investigating crimes. ☐ Confirm whether the authority can provide the official approval of data assess.	35 35
(12) Restrictions on Data Transfer to Foreign Authorities	☐ Report to the competent authorities of China and seek approval when the foreign judicial or law enforcement agencies make requests to access data.	36
3. Additional Considerations for Processing Important Data		
(13) Personnel	☐ Designate specific personnel and department to manage data security matters and set out clear functions, roles, responsibilities, and reporting lines for such personnel, if your organization is processing any Important Data.	27
(14) Risk Assessment	☐ Carry out risk assessments on processing activities related to Important / National Core Data on a regular basis. ☐ Communicate proactively with competent authorities on risk assessment and submit reports upon requests or according to regulations.	30 30
(15) Cross-border Data Transfer	☐ Assess whether your organization may be considered as a critical information infrastructure operator ("**CIIO**"). ☐ Localize all the Important Data collected and generated from business operation in China by your organization if it is a CIIO, and where it is necessary to export data, a security assessment procedure implemented by the authority shall be passed. ☐ As a best practice, also localize all the Important Data collected and generated from business operation in China even though your organization is not a CIIO.	31 31 31

CSBrand-67745-Data Security Law of China - Checklist — 02/09/2021