Int. Cybersecur. Law Rev. (2021) 2:209–221
https://doi.org/10.1365/s43439-021-00038-3

Understanding the Chinese Data Security Law

Jihong Chen · Jiabin Sun

Received: 9 September 2021 / Accepted: 12 September 2021 / Published online: 12 October 2021

Abstract On 10 June 2021, the *Data Security Law of the People's Republic of China* (hereinafter the "DSL") was adopted at the 29th session of the Standing Committee of the 13th National People's Congress, effective as of 1 September 2021. The DSL is the fundamental law in the data security sphere and, together with the *Cybersecurity Law* (hereinafter the "CSL") and the *Personal Information Protection Law* (hereinafter the "PIPL"), outlines the data regulatory framework in China. The DSL contains seven chapters and 55 articles that widely cover data security mechanisms, obligations and liabilities at both State administration and data handler levels. In this article, the key contents of the DSL together with the intensively promulgated supplemental laws and regulations will be analyzed to provide a comprehensive grasp of data security supervision in China. Specifically, section one explains the basic concepts of the DSL, section two highlights the key data security protection mechanisms such as the Important Data protection and data cross-border transfer and section three will summarize the main compliance obligations for companies to effectively put laws into actions.

Keywords Data security administration · Important data · Data cross-border transfer · Data security review · Data security obligations

Jihong Chen · Jiabin Sun (✉)
Zhong Lun Law Firm, Beijing, China
E-Mail: sunjiabin@zhonglun.com

Jihong Chen
E-Mail: chenjihong@zhonglun.com

1 Basic concepts of the *Data Security Law*

1.1 Applicable scope

This law applies to data handling activities conducted within the territory of China and the security supervision and administration over such activities. The Data Security Law of the People's Republic of China (hereinafter the "DSL") also has certain extra-territorial application since it states that "data handling activities conducted outside the territory of China, harming national security, public interests or legitimate rights and interests of citizens and organizations shall be legally liable in accordance with laws".[1] Foreign companies with targeted businesses in China or whose data handling activities may exert substantial impact on China shall be mindful of the DSL.

1.2 Regulatory bodies

The DSL expressly outlines the data security regulatory framework. It specifies the head role of the central leading institution for national security especially in coordinating the data security work at the State level via the coordination mechanism (Fig. 1). The DSL clarifies the respective data supervision responsibilities of various national public departments (for example, the State Cyberspace Administrative Departments, the public security organs and the national security organs) and industrial competent authorities, in avoidance of ambiguous and repetitive administration.[2]

2 Key administration roadmap under the *Data Security Law*

2.1 Underlying cornerstone: the hierarchical data classification mechanism

The DSL, following the governance logic of the cybersecurity multi-level protection scheme ("MLPS") under the CSL, regulates data handling activities and data security thereof through the hierarchical data classification mechanism. The DSL Article 21 stipulates that the State shall establish a hierarchical data classification mechanism. Data under the mechanism is matrixed in accordance with its importance in economic and social development and degree of harm to national security, public interests or legitimate rights and interests of individuals and organizations once tampered, destroyed, leaked or illegally obtained or utilized. Article 21 specifies that Important Data shall require prioritized protection and Core Data shall be administrated at a more stringent level. Both Important Data and Core Data are proper nouns under the Chinese law. Important Data was first mentioned in the CSL. An official definition of Important Data has not yet been given; reference can be made to the *Administrative Measures for Data Security (Draft for Comment)* promulgated by the Cyberspace Administration of China ("CAC") in 2019, where

[1] Data Security Law of the People's Republic of China, Article 2.

[2] Data Security Law of the People's Republic of China, Article 5, Article 6.

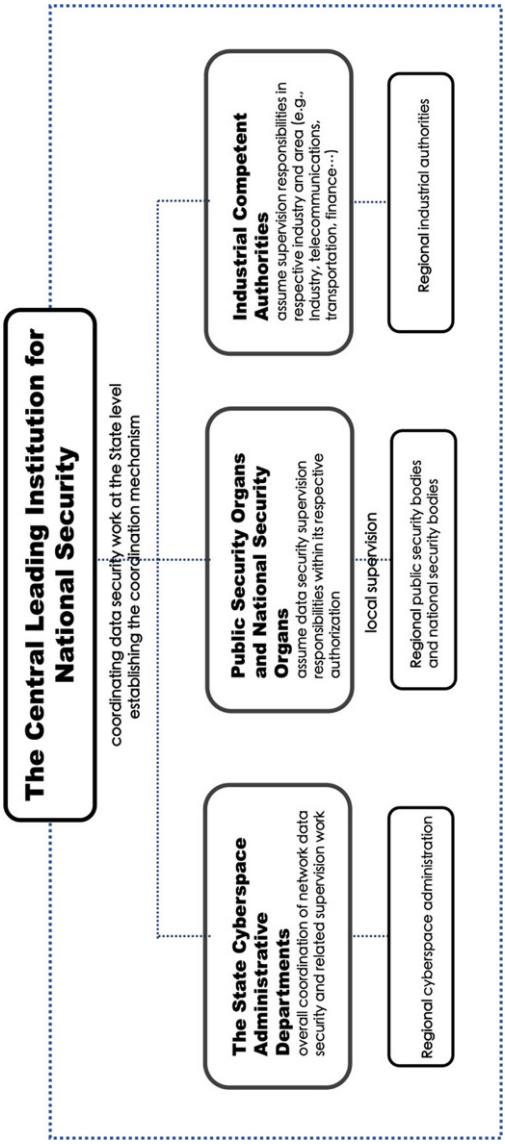

Fig. 1 Data security regulatory bodies

Important Data is referred as the kind of data that, if divulged, may directly affect national security, economic security, social stability and public health and security, such as undisclosed government information, large-area population, genetic health, geography and mineral resources. Core Data is first proposed in the DSL (second draft for deliberation), which refers to data in relation to the national security, the lifeline of the national economy, important parts of people's livelihood and major public interests.[3] It can be understood that Core Data is part of Important Data that merits more stringent supervision and protection due to its nature.

[3] Data Security Law of the People's Republic of China, Article 21.

The DSL sets a top-down administration path to the establishment of the hierarchical data classification mechanism at the State level. In addition, sectorial legislative attempts regarding the formulation of the hierarchical data classification mechanism have long existed, including but not limited to the *Data Classification Guidelines for Securities and Futures Industry*[4], the *Guidelines for the Classification and Grading of Industrial Data (Trial)* published by the MIIT in 2020, the *Financial Data Security—Guidelines for Data Security Classification*.[5]

Companies following the national administrative mechanism and fully considering the sectorial regulatory requirements, shall conduct their own internal data classification work or perform self-examination and correction to their existing mechanisms. A truly effective full-lifecycle data security scheme can only be established on such a data classification basis, mapping various security measures to different categories of data at storage, utilization, sharing stage, etc. accordingly.

2.2 Deep dive: stringent supervision of important data

Important Data supervision lies at the heart of the State data security administration under the DSL. On the one hand, such administration is achieved through the formulation of an Important Data Catalogue. The catalogue formulation also features the top-down design throughout the DSL. Article 21 clarifies that relevant departments under the coordination mechanism by the central leading institution for national security shall formulate the catalogue at the State level and then each region and sector shall develop its specific catalogue. DSL Article 6 might shed some light on key sectors that will require specific Important Data Catalogues of their own. Article 6 states that competent authorities in industry, telecommunications, transportation, finance, natural resources, health, education and technology are responsible for data security supervision in their respective industries and fields. Booming sectors with great public concerns are also the regulatory focus; for example, China has accelerated its promulgation of laws in the automotive sector in the last few months, in particular, the *Several Provisions on Automotive Data Security Management (for Trial Implementation)* (hereinafter the "Provisions") released by the CAC together with the NDRC, MIIT, MPS and the Ministry of Transport on 16 August 2021, effective as of 1 October 2021. The provisions, as the first ever binding law regarding data security in the automotive sector, enumerate in Article 3 the scope of

[4] JR/T 0158—2018, published by the China Securities Regulation Commission ("CSRC"), effective as of 27 September 2018.

[5] JR/T 0197—2020, published by the People's Bank of China, effective as of 23 September 2020.

Important Data in a non-exhaustive manner.[6] Such a sectorial definition unites both the gist of the DSL and characteristics of the automotive industry; it also states that personal information of more than 100,000 data subjects belongs to Important Data, clarifying the long-standing controversy that Important Data excludes personal information. The State, on the other hand, sets several data protection obligations for the handlers of Important Data, that is, Important Data handlers shall specify the responsible person and the management body for data security to implement and fulfil data security protection obligations.[7] Handlers of Important Data shall regularly conduct risk assessments and submit the risk assessment reports to competent authorities.[8] The cross-border transfer of Important Data shall be regulated by the security assessment by the State Cyberspace Administrative Departments or related measures to be enacted by the State Cyberspace Administrative Departments together with relevant departments of the State Council.[9]

The two-tier scheme of the Important Data Catalogue answers the long-standing debate over determination of Important Data and reflects great coordination between the State and specific regions and departments. The catalogue at the State level would ensure a unified determination criterion of Important Data and when setting specific catalogue, each region and sector is well enabled to consider actual situations of various fields and regions. Companies shall cautiously conduct an internal data inventory on such a basis. Once any data falls within the scope of Important Data, companies shall strictly abide by the compliance obligations mentioned above. For companies violating Important Data protection obligations, relevant competent authorities could order the suspension or termination of the business at issue for rectification and revoke business licenses or permits. Companies can be fined 10 million yuan and the directly responsible person in charge can be fined 1 million yuan at most.[10]

2.3 Challenge I: cross-border transfer of data

The DSL in general sets the basic tone of promotion of data cross-border transfer in a safe and free manner.[11] The DSL Article 31, in convergence with the CSL

[6] For the purpose of the Provision, Important Data refers to the data that may endanger national security, public interests or the legitimate rights and interests of individuals or organizations once tampered, damaged, leaked, illegally obtained or illegally used, including: (a) geographic information, passenger flow, vehicle flow and other data of important sensitive areas such as military administrative zones, entities of science, technology and industry for national defense, and CPC and government organs at the county level or above; (b) data reflecting economic operations such as vehicle flow, logistics, etc.; (c) operational data of the automobile charging network; (d) video and image data outside the vehicles that contain face information, license plate information, etc.; (e) the personal information of more than 100,000 persons as the subject of personal information is involved; (f) other data that may endanger national security, public interests or the legitimate rights and interests of individuals or organizations as determined by the relevant authorities including the CAC, NDRC, MIIT, MPS and the Ministry of Transport.

[7] Data Security Law of the People's Republic of China, Article 27.

[8] Data Security Law of the People's Republic of China, Article 30.

[9] Data Security Law of the People's Republic of China, Article 31.

[10] Data Security Law of the People's Republic of China, Article 45, 46.

[11] Data Security Law of the People's Republic of China, Article 11.

Article 37, provides the specific rule for cross-border transfer of Important Data, that is, Important Data collected or generated by Critical Information Infrastructure Operators (CIIOs) shall be stored within the territory of China and shall pass the security assessment by the State Cyberspace Administrative Departments when truly necessary to be transferred outside the territory of China, and the cross-border transfer of Important Data of non-CIIOs shall be regulated by measures to be enacted by the State Cyberspace Administrative Departments together with relevant departments of the State Council. The DSL, as opposed to the CSL, includes non-CIIOs in the regulatory scope relating to the cross-border transfer of Important Data and therefore fills the regulatory gap. From the latest legislation and law enforcements, it can be seen that supervision of cross-border transfer of data is getting ever tighter. Again, the newly released *Several Provisions on Automotive Data Security Management (for Trial Implementation)* stipulate in Article 11 that Important Data of all automotive data handlers[12], whether CIIO or not, shall be stored within the territory of China and shall pass the security assessment by the State Cyberspace Administrative Departments when truly necessary to be transferred outside the territory of China. That is to say, companies, especially MNCs with global systems, can no longer transfer the regulated data under localization requirements to their servers overseas directly. The needs to localize their IT infrastructure are becoming unavoidable. In addition, remote access of the parent company to data centers of its subsidiaries located within the territory of China also falls into the regulatory scope of cross-border transfer.

Companies in violation of the DSL Article 31 relating to cross-border transfer of Important Data can be ordered to suspend or terminate the business at issue for rectification, get their business licenses or permits revoked and be fined at most 10 million yuan at the company level and 1 million yuan for the directly responsible person in charge.

2.3.1 Full landscape

As personal information is also part of data[13] under the DSL, combining the cross-border transfer rules under the PIPL promulgated by the Standing Committee of the 13th National People's Congress on 20 August 2021, effective as of 1 November 2021, hereby the full landscape of data cross-border transfer rules in China is provided. The PIPL states that data handlers shall conduct an impact assessment prior to any cross-border transfer of personal information (equivalent to the Data Protection Impact Assessment ["DPIA"] under the General Data Protection Regulation

[12] Several Provisions on Automotive Data Security Management (for Trial Implementation) Article 3, Automotive data processors refer to organizations carrying out automotive data handling activities, including automobile manufacturers, parts and software suppliers, distributors, maintenance agencies and travel service providers, etc.

[13] Data Security Law of the People's Republic of China, Article 3, for the purpose of this law, the term "data" refers to any recording of information by electronic or other means.

["GDPR"]) and obtain separate consent from data subjects.[14] PIPL Article 40 specifies that CIIOs and data handlers reaching the threshold of the amount of personal information under processing prescribed by the State Cyberspace Administrative Departments shall store their personal information generated and collected in China within the territory of China and shall pass the security assessment by the State Cyberspace Administrative Departments when the data truly necessarily needs to be transferred outside the territory of China. PIPL Article 38 states that besides as provided in Article 40, data handlers shall either enter into contracts with the overseas recipient in accordance with the standard contract to be formulated by the State Cyberspace Administration Departments or conduct personal information protection certification by designated institutions unless otherwise prescribed by laws or administrative regulations or by the State Cyberspace Administrative Departments (Fig. 2).

2.3.2 Identification of CIIO

CIIOs bear great data protection obligations, especially those of data localization requirements as illustrated above—therefore the identification of CIIO becomes critical. On July 30, 2021, the *Security Protection Regulations for Critical Information Infrastructure* (hereinafter the "Regulations") were promulgated in the form of Decree No. 745 of the State Council, effective as of September 1, 2021. In accordance with the Regulations, CII refers to the important network facilities and information systems in important industries and fields such as public telecommunication and information services, energy, transportation, water conservancy, finance, public services, e-government and national defense science, technology and industry, as well as other important network facilities and information systems which, in the case of destruction, loss of function or leak of data, may result in serious damage to national security, the national economy and people's livelihood and public interests.[15] Relevant authorities in light of the actual conditions of respective industries and fields shall develop specific rules for the identification of CII and shall file such rules with the public security departments under the State Council for records. The following factors shall be taken into account while developing the identification rules with regard to the network facility, information system etc. at issue, that is, its importance to core business of the industry and field concerned; the degree of harm it may cause in the event of any destruction, loss of function or leak of data and its relevance to other industries and fields.[16] Companies playing critical parts in the sector should keep a close eye on any legislative developments of CII identification, conduct internal assessments of information systems when necessary, raise compli-

[14] Personal Information Protection Law of the People's Republic of China, Article 39, Article 55. As regard the obtainment of separate consent under cross-border transfer of PI, currently one interpretation is that separate consent is only required where such handling is conducted on the basis of consent, as Art. 13 para. 2 specifies that where other legal bases suffice, consent is not required. Another interpretation is that separate consent herein prevails other legal bases. Further clarification may need to be provided.

[15] Security Protection Regulations for Critical Information Infrastructure, Article 2.

[16] Security Protection Regulations for Critical Information Infrastructure, Article 9.

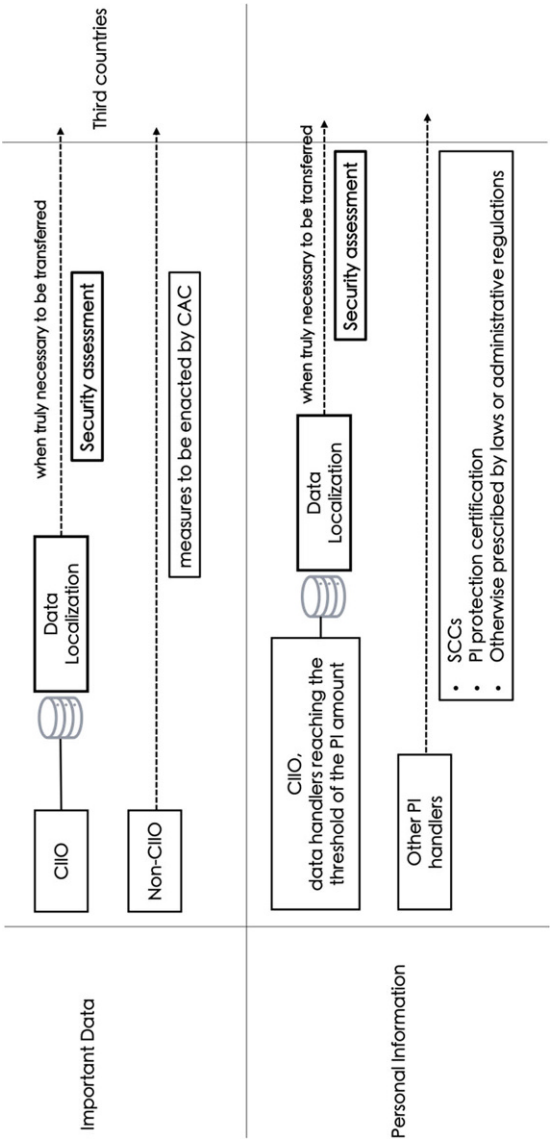

Fig. 2 Data cross-border transfer rules. *CIIO* Critical information infrastructure operator, *CAC* the Cyberspace Administration of China, *PI* Personal information, *SCCs* Standard contractual clauses

ance awareness and take preventive measures especially with regard to data cross-border transfer restrictions and cybersecurity review obligations.

2.3.3 Export control

The DSL in line with the *Export Control Law* specifies that the State exercises export control over the data relating to the safeguarding of national security and interests and the fulfilment of international obligations which also falls under the controlled

items.[17] Controlled items here mean dual-use items, military products, nuclear and other goods, technologies, services and items that relate to the safeguarding of national security and interests.[18] Article 2 of the *Export Control Law* states that data such as any technical information on controlled items shall be deemed to also be part of the controlled items. The DSL confirms the applicability of export control to data handling activities. Once any data falls into the export control list, it may only be transferred outside the territory of China with a license granted by competent authorities. For MNCs, when investing or conducting related businesses, for example communication technology or aviation technology, it shall be kept in mind that certain technologies and related data may be subject to export control.

2.4 Challenge II: data security review

The DSL, in convergence with the *National Security Law*, stipulates that data handling activities that affect or may affect national security shall be subject to national security review.[19] On 10 July 2021, the *Cybersecurity Review Measures (Draft Revision for Comment)* (hereinafter the "Measures") were issued for public comments by the CAC, which is set to be an essential supplemental measure for the data security review mechanism under the DSL. The Measures on the one hand proactively respond to the data security concerns incurred by the recent listing of domestic companies overseas; on the other hand they incorporate the data security review mechanism into the existing cybersecurity review mechanism, promoting the implementation of such a mechanism. The Measures prescribe that both data handling activities that affect or may affect national security and overseas listings of operators with personal information of more than 1 million users would trigger a cybersecurity review.[20] The risk of Core Data, Important Data or large-scale personal information being stolen, leaked, destroyed, illegally utilized or transferred outside the territory of China is listed as one of the main assessment focuses of the cybersecurity review.[21] It can be suggested to companies to conduct an internal data inventory and self-assessment in advance, pay attention to any business lines with more than 1 million users or involving Core Data and Important Data. Companies should proactively implement the requirements under the DSL and keep a close eye on any legislative and enforcement developments especially with regard to the protection of Core Data and Important Data and data cross-border transfer.

2.5 International response: blocking provisions and countermeasures

The DSL imposes control on requests of data by foreign judicial or law enforcement agencies. DSL Article 36 stipulates that no organization or individual within the territory of China can provide foreign judicial or law enforcement authorities

[17] Data Security Law of the People's Republic of China, Article 25.

[18] Export Control Law of the People's Republic of China, Article 2.

[19] Data Security Law of the People's Republic of China, Article 24.

[20] Cybersecurity Review Measures (Draft Revision for Comment) Article 2, Article 6.

[21] Cybersecurity Review Measures (Draft Revision for Comment) Article 10.

with data stored within the territory of China without the approval of competent authorities. The DSL sets substantial liabilities for violating this provision: companies can be ordered to suspend or terminate the business at issue for rectification, get their business licenses or permits revoked and be fined at most 5 million yuan at company level and 500,000 yuan for the directly responsible person in charge.[22] When confronted with unreasonable requests from foreign judicial or law enforcement agencies, companies can resort to this provision as a legal basis. Therefore, the approval mechanism under Article 36 is seen as an important system to protect data sovereignty and the legitimate rights and interests of companies and individuals. Yet it is worth noticing that such provisions may affect domestic companies or MNCs involved in evidence disclosure and information gathering requests for foreign criminal proceedings, civil proceedings and administrative investigations. The specific approval procedures are to be further specified. At the same time, the DSL echoing the current international situation, states that China may adopt equivalent countermeasures against any prohibitive or restrictive measure imposed by any country or region in terms of data related to investment or trade.[23]

2.6 A closed loop: full lifecycle data security protection

As the fundamental law in data security regards, the DSL aims to set full lifecycle data security measures. The DSL specifies that the State establishes a centralized, unified, efficient and authoritative data security risk assessment, reporting, information sharing, monitoring and early warning mechanism, as well as a data security emergency response mechanism.[24] The DSL also regulates data transactions with intermediaries and prohibits unfair competitive conducts by stealing or otherwise illegally obtaining data and carrying out data handling activities to eliminate or restrict market competition.[25]

3 Comprehensive data security protection obligations

Data security refers to the status of effective protection and lawful utilization of data as well as the capability to guarantee continuous security of data through the adoption of necessary measures.[26] The DSL places a raft of data security protection obligations on data handlers in the entire Chapter IV. It shall be noted that the DSL itself merely provides the scaffold and would require supplemental regulations, national standards and guidance for further implementation in practice. Companies shall keep a close eye on any legislative developments for compliance purposes. Related obligations under the DSL mainly comprise:

[22] Data Security Law of the People's Republic of China, Article 48.

[23] Data Security Law of the People's Republic of China, Article 26.

[24] Data Security Law of the People's Republic of China, Article 22, Article 23.

[25] Data Security Law of the People's Republic of China, Article 19, Article 51.

[26] Data Security Law of the People's Republic of China, Article 3.

- *Data Collection and Handling.* Data handling activities shall conform to social morals and ethics.[27] Data collection shall be legitimate and fair.[28] The collection and use of data shall be limited to the prescribed purposes and scope by laws and administrative regulations.[29]
- *Data Security Management System.* Companies shall establish and complete a life-cycle data security management system, take corresponding technical and other necessary measures to ensure data security and conduct relevant data security education and training.[30]
- *Multi-Level Protection Scheme (MLPS).* By stating "data security protection obligations shall be fulfilled on the basis of MLPS when conducting data handling activities via Internet and other information networks", the DSL sets out the fundamental role of MLPS in data security protection.[31]
- *Important Data Handling and Cross-Border Transfer.* As illustrated above, Important Data handlers shall specify the responsible person and the administrative body to implement and fulfil data security protection obligations, conduct regular risk assessments and submit the risk assessment reports to competent authorities,[32] and abide by the cross-border transfer rules.
- *Security Risk Monitoring and Incident Response Obligations.*[33] Data handlers shall enhance risk monitoring and take immediate remedies for any security bugs or vulnerabilities. Data handlers shall respond quickly to any data breach and inform users and report to competent departments in a timely manner.
- *Enforcement Cooperation.* Domestically, companies shall cooperate with the legitimate request for data retrieval by public security organs and national security organs.[34] Internationally, companies or individuals shall not provide data stored within the territory of China to foreign judicial or law enforcement agencies as requested, unless approved by competent authorities.[35]
- *Data Transaction and License Requirement.* Companies conducting data handling activities shall obtain a relevant license qualification as prescribed by laws (for example, ICP, IDC and EDI license under value-added telecommunication services).[36] Data transaction intermediaries shall review the identity of parties involved in the transaction, obtain data source description and create the related documentation.[37]

[27] Data Security Law of the People's Republic of China, Article 28.
[28] Data Security Law of the People's Republic of China, Article 32.
[29] Data Security Law of the People's Republic of China, Article 32.
[30] Data Security Law of the People's Republic of China, Article 27.
[31] Data Security Law of the People's Republic of China, Article 27.
[32] Data Security Law of the People's Republic of China, Article 30.
[33] Data Security Law of the People's Republic of China, Article 29.
[34] Data Security Law of the People's Republic of China, Article 35.
[35] Data Security Law of the People's Republic of China, Article 36.
[36] Data Security Law of the People's Republic of China, Article 34.
[37] Data Security Law of the People's Republic of China, Article 33.

Table 1 Compliance checklist of the DSL

Compliance obligation		Compliance guidance	
1	Baseline data security protection obligations Article 27	1	Establish data security management systems in companies
		2	Organize and carry out data security education and training
		3	Take relevant technical measures and other necessary measures
2	Hierarchical Data Classification Article 21	4	Companies should carry out internal data classification and hierarchical management, considering features of the company and its sector. Companies should correspondingly establish management systems and adopt technical measures in terms of data of various types and hierarchy
		5	The hierarchical data classification should closely link to measures in relation to the use, retention, desensitization and access of data, to achieve systematic management
3	Important Data identification and management Article 21, 27, 30	6	Companies should adjust their existing Important Data list based on the Important Data Catalogue (competent authorities will formulate and release an Important Data identification guideline and list)
		7	Designate responsible person(s) and management department for data security in respect of handling of Important Data
		8	Formulate regular assessments and reporting system in respect of handling of Important Data
4	Data security risk monitoring and incident response Article 29	9	Companies should develop a data security risk monitoring system and implement relevant responsibilities
		10	When spotting any risks of data security, bugs or vulnerabilities, companies should immediately take remedies
		11	If any data security incident occurs, companies should initiate an emergency plan, take incident response measures and report to users and competent authorities in a timely manner
5	Cross-border transfer of Important Data Article 31	12	For CIIOs, cross-border transfer of Important Data is subject to CSL Article 37 (data localization + security assessment by the State Cyberspace Administration Departments)
		13	For non-CIIOs, cross-border transfer of Important Data is subject to measures to be enacted otherwise
6	Data national security review Article 24	14	Cautiously assess the triggering condition with regard to data security review and cooperate with any review initiated by competent authorities
7	Cooperation with data retrieval requests by domestic law enforcement authorities Article 35	15	Companies could require relevant law enforcement departments to present the approval and shall cooperate with the provision of data
8	Requirements in responding to data disclosure requests by foreign judicial and law enforcement agencies Article 36	16	Companies shall report and obtain approval from competent authorities when facing data disclosure requests from foreign judicial and law enforcement agencies
9	Lawfulness and fairness in data collection Article 32	17	Companies should develop data collection specifications, especially focusing on the application of data scraping technology

In a nutshell, it is recommended for companies to follow the compliance checklist as below and conduct internal review proactively (see Table 1).

Jihong Chen Partner

Jiabin Sun Associate