Sino-German Cooperation on Industrie 4.0

Data Security Law (draft for comments)

Policy Briefing | July 2020

On 1 July, the draft Data Security Law was released by the National People's Congress Standing Committee with **a call for comments by 16 August 2020.**[1] An English translation of the full text could be found here. This policy briefing selects the key points from the draft, incorporating second-source analysis as well as the project's assessments.

What's the connection to the Cybersecurity Law?

- The Data Security Law has the same legal status as the Cybersecurity Law. Together with the Personal Information Protection Law (in the making process), they will constitute the **legal foundation of China's cyber and data regulation**.
- Based on the Cybersecurity Law, the Cyberspace Administration of China (CAC) released a draft version of **Data Security Management Measures** on 5 May 2019. This management measures, focusing on protecting personal information and important data in cyberspace on the network operator level, **has not taken effect**.

What are the most relevant contents and implications?

1. The draft Law provides a **definition of data, data activities and data security**. Particularly, data refers to recording information in both electronic and non-electronic forms; data security emphasises the capability of **"continuously staying secure."** (Article 3)
2. Regarding **cross-border data transfer**, the draft Law stipulates that "China should actively pursue international cooperation, participate in establishing international rules and standards and **promote the secure and free cross-border data transfer**." (Article 10)

   → Security requirements on cross-border data transfer (such as data localisation for critical information infrastructure operators) are not specified in the draft Law, possibly as a result of avoiding duplication with the Cybersecurity Law. Some commentary[2] also interprets this provision as a statement for China's opening up stance.
3. **Data classification and categorisation** is a key management mechanism in the draft law. Each region and department shall classify the data and formulate an "**important data**" protection catalogue. (Article 19)

   → This provision signals passing down more executive power to the local government and state departments of different industries.

[1] Comments could be submitted online via visiting this website or via mail to the NPC Standing Committee Legal Work Committee, Qianmen Xidajie 1, Xicheng District, Beijing, 100805 with an indication of "data security law draft for comments" on the envelop.
[2] Commented by lawyers from Beijing Zhonglun Law Firm in this article.

→ Even though the definition of data is clear, important data and implementation mechanism are not yet clarified. In the field of industrial data, MIIT published an "Industrial Data Categorisation and Classification Guide (Trial Version)" in February 2020, which classifies industrial data into three security levels and serves as a guide for enterprises.

→ It is noticed that local governments are responsible for determining "important data categories." Some analysis [3] comments that this might lead to discoordination and over-definition of important data and suggests that the central government should take this responsibility.

4. Regarding **"important data"**, specific personnel and departments should be established to take responsibility for the security of important data; risk assessments should be conducted regularly and be reported to relevant supervision bodies. (Article 25, 28)

   → This indicates how the enterprises shall carry out the regulations if they are categorised as processors of "important data".

5. In addition to data security, the draft Law also emphasises the **development of the data industry** such as **implementing national "big data strategy"** as well as encouraging local governments to formulate digital economic development plans. (Article 13)

   → These demonstrate China's strong focus on developing the digital economy.

6. **A national security review mechanism** will be established for data activities that could **impact national security**. The results of the security review will serve as the **"final decisions."** (Article 22)

   The State implements **export controls on data of controlled categories[4]** related to fulfilling international obligations and safeguarding national security. (Article 23)

   If other **countries or regions take discriminatory measures** in data-technology-related **trade and investment** against the PRC, the PRC could take **corresponding measures**. (Article 24)

   → The above three provisions further underline the State's strict approach with regards to national security and trade, as data security has increasingly come into focus of national security in recent years.

   → How these provisions will be implemented in coordination with the existing requirements in the Cybersecurity Law is unclear yet.

7. **Extraterritorial jurisdiction:** in addition to applying to data activities within the territory of the People's Republic of China (PRC), the draft Law also stipulates that data activities outside the territory of PRC, when harming national security, public interest or legal rights of individuals and organizations, should incur legal liability. (Article 2)

   → Some analysis[5] commented that this demonstrates only a "moderate" extraterritorial jurisdiction compared with regulations in the EU and US because it only applies when harm occurs. However, the definition of "national security" is unclear.

8. **Legal liabilities** such as fines are specified in the draft Law. (Article 41-48)

---

[3] Ibid.
[4] These categories concern military and nuclear non-proliferation items and are regulated according to the Export Control Law (Second Draft for Comments).
[5] Commented by Xu Ke, the Executive Director of Digital Economy and Legal Innovation Research Center of University of International Business and Economics, in this article.

Summary of the draft Law:

The draft Law has 7 chapters:

1. General Provisions

   Chapter 1 defines the scope of application including extraterritorial jurisdiction (Article 2) and provides a definition of data, data activities and data security (Article 3). The respective responsibility is clarified for different regulatory authorities including central, local and sectoral departments, public security bodies, the Cyberspace Administration of China, etc. (Article 7). Additionally, the State expresses the initiative of engaging in international cooperation and international standard-setting (Article 10).

2. Data Security and Development

   Chapter 2 emphasises on promoting data use and development. The promoting measures include formulating digital economy development plans (Article 13), strengthening basic research in relevant fields (Article 14), advancing data security standard systems (Article 15), etc.

3. Data Security Systems

   Chapter 3 begins with the classification and categorisation system for data protection. Each region and department shall classify the data, formulate a key data protection catalogue and undertake protective measures based on the classification (Article 19). It is also generally mentioned that the State shall establish the data security risk assessment mechanism (Article 20), the emergency management mechanism (Article 21) and the review mechanism (Article 22).

4. Data Security Protection Obligations

   Chapter 4 outlines the legal obligations of major stakeholders in the data industry:

   - Processors of important data shall regularly submit risk assessment reports to competent authorities. This report should include the kinds and quantity of important data and the situation of collecting, storing, processing and using data (Article 28).
   - Institutions engaged in data transaction intermediary services shall demand the data provider to clarify the data source (Article 30).
   - Operators specialising in providing services like online data processing shall obtain relevant state business licensing or registration records (Article 31).

5. Government Data Security and Openness

   Chapter 5 sketches the plan of the State to advance the construction of e-governance and manage the government data. The State shall build an open platform to promote the public use of government data (Article 39).

6. Legal Liability

   Chapter 6 specifies non-compliance penalties for organisations and individuals conducting data activities (Article 42), data transaction intermediary organisations (Article 43) and other businesses (Article 44). Punishment for State organs (Article 45) and government employees (Article 46) is also included in this Chapter.

7. Supplemental Provisions

   Chapter 7 specifies the exceptions of application in three areas: data activities concerning national secrets, personal information and military data security.