Sino-German Cooperation on Industrie 4.0

Measures on Security Assessment of Cross-Border Data Transfer (Draft for comment)

Policy Update | November 2021

On October 29th, the Cyberspace Administration of China (CAC) released the draft version of the **"Measures on Security Assessment of Cross-Border Data Transfer" (hereinafter called the Measures)**. The Measures are open for public commenting until November 28th[1].

The measures are based on the "troika" of cybersecurity regulations – the **Cybersecurity Law** (in effect since 2017), the **Data Security Law** (in effect since September 1st, 2021), and the **Personal Information Protection Law** (in effect since November 1st,2021).

Legislative history

With the release of the new Measures, the legislative process shows a transformation in the regulatory approach towards cross-border data transfer. In 2017, CAC published the "Measures on Security Assessment of Personal Information and Important Data Cross-Border Transfer (draft for comment)". The attempt was to regulate the cross-border data transfer of personal information and important data together in one document. When the "Measures on Security Assessment of Personal Information Cross-Border Transfer (draft for comment)" where released in 2019 the approach seemed to be regulating Personal Information separately. With the Measures now published, the regulatory approach is again to regulate the cross-border transfer of all types of data under one umbrella.

Assessment models and process

Two step risk assessment:

1. Self-assessment

The Measures describe the **risk self-assessment** as a legal obligation for all **data processors**[2]. This mechanism has already been introduced in the Data Security Law (DSL) and the Personal Information Protection Law (PIPL). The Measures now clearly regulate it as a prerequisite **every time cross-border data transfer is conducted**. The data amount, scope and the transfer purpose are not restrictively regulated in the Measures. This open regulation means that a self-assessment needs to be conducted every time data is transferred across borders.

The **self-assessment** includes **three main areas**:

- the legality of the purpose, scope, methods of the data transfer and the data processed by recipients

[1] Publication notice from CAC and the original Chinese text: http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm English translation (unofficial): https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/

[2] "Data processing (or handling)" is defined as "actions include the collection, storage, use, processing, transmission, provision, disclosure, etc., of data" in the Data Security Law. A Policy Briefing on the Data Security Law can be found on the project website.

- the potential risks of the data transfer with regards to Chinese national security, public interest as well as lawful rights and interests of individuals and organisations
- whether the cross-border data transfer-related contract with the recipient fully regulates the data security protection responsibilities and duties

2. Security assessment

The **Security assessment** conducted by national cybersecurity and information departments is required to be applied through local provincial-level departments, **only when the data transfer meets one of the following criteria**:

- if personal information and important data is concerned or the data is collected or produced by **Critical Information Infrastructure Operators** (CIIO[3])
- cross-border data contains **important data**; *(Even though the DSL gives some direction on how to categorize data the clear definition/catalogue of "important data" is still outstanding.)*
- data transferred by the personal information processor, if the processer processes **personal information of over 1 million people**
- if the **accumulated amount** of personal information **transferred to abroad** exceeds the information of more than 100,000 people or the sensitive personal information of more than 10,000 people
- other situations, that are regulated by national cybersecurity and information departments. *(This seems to be a flexibility clause to give room for sectoral regulations or regulations scenarios that are not clearly defined here.)*

Assessment materials

The Measures describe the documents the data processor is required to deliver for the application:

1. **Application letter** *(Usually, relevant templates are made available at MIIT's or other responsible ministry's websites after a regulation becomes effective. Since the Measures are still in the commenting phase, a template has not been made available yet.)*
2. **Risk self-assessment report** *(same as 1. above)*
3. The **legal contract** or documents between the data processor and the foreign recipients (hereinafter called the contracts)
4. **Other materials**, which are required for security assessment *("Other materials" is not further clarified in the Measures.)*

The measures regulate that the contracts shall fully comprise the data security protection responsibilities and duties. The requirements of the contracts in the Measures might overlap or be a part of the so-called "standard contract", described in the Personal Information Protection Law [4].

---

[3] Critical Information Infrastructure (CII): network facilities and information systems that are indispensable to support the continuous and stable operation of Critical Business. In essence, it constitutes the digital infrastructure of Critical Business and provides support for it based on modern communication, network and database technology.
Reference from SAMR "Guide to security inspection and evaluation of critical information infrastructure":
http://std.samr.gov.cn/gb/search/gbDetailed?id=62550C53E443BA34E05397BE0A0AAB2B

[4] The "standard contract formulated by national cybersecurity and information departments" has been mentioned in article 38 of the PIPL. The original Chinese text can be found on the NPC website:
http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
English translation (unofficial): https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

According to the Measures, the assessment will mainly focus on a few key evaluation areas to avoid potential risks. One of the key points is to check the “cybersecurity environment” as well as the data security protection policies, laws, and regulations of the country or region that the recipient is located in. Specifically, whether the data protection level of the receiving country or region meet the requirements of the laws, administrative regulations, and mandatory national standards of China. Overall, this regulatory aspect is kept rather vague and poses further uncertainties for companies requiring international data transfer. Clarifications and further developments need to be monitored closely.

Assessment departments and processing time

According to the Measures the national cybersecurity and information departments will give written feedback whether they accept or reject the application within seven working days after they received the application. After accepting, the national departments will instruct the relevant industry departments, relevant State Council departments, provincial-level cybersecurity and information departments and specialised agencies to process the assessment within 45 workdays. For “complicated” situations or when more supplementary material is needed, the time can be extended but only to a maximum to 60 workdays. A more specific explanation of these situations is not given. If the main circumstances or legal environment of both sending and receiving countries have not changed, the assessment results is valid for two years.

We hope you have enjoyed reading this Policy Update and welcome your comments and suggestions. Your feedback to info@i40-china.org is highly appreciated. More policy products are available in our Download Area. More information about the Sino-German Industrie 4.0 Cooperation can be found on our Project Website www.industrie40-china.org.