Sino-German Cooperation on Industrie 4.0

Cross-border Industrial Data Transfer Regulations

Policy Briefing | June 2022

Cross-border industrial data transfer is crucial for supporting international value networks. In recent policy developments, the handling of industrial data has been further regulated. In the latest revised version of the Measures for Data Security Management in the Industry and Information Technology Sector (call for comments) (hereinafter called the Security Management Measures) published by the Ministry of Industry and Information Technology (MIIT), the 21st Article has stipulated to 1) cancel the prohibition of exporting core data and 2) allow the provision of industry and IT data to foreign companies under the approval of MIIT. In light of this new data security policy development, this policy briefing elaborates China's industrial data classification and outlines the recent regulatory changes on cross-border industrial data transfer.[1]

Industrial Data Definition and Classification

According to the Security Management Measures, industrial data refers to data obtained from research and development (R&D), production, business management, maintenance and industrial platform operations.

Industrial data is classified into three grades based on their risk estimations for each type of data on national security, public interest, individuals and organisational rights. According to the Security Management Measures, data meeting any of the following criteria will be characterised as:

1. **General data**

   In case of data breaches or leaks

   - negative impacts on public interests, individuals, organisational rights are small, and the negative social influence is moderate.
   - affected users and enterprises are few, the affected manufacturing or residential areas are small, and the impact duration is temporary.
   - negative impacts on the business and industrial development, technology progress as well as the industry ecosystem are strong.
   - none of the data belongs to the important and core data catalogues

2. **Critical data** (also known as important data):

   In case of data breaches or leaks

   - strong national threats are posed on politics, territory, military, economy, culture, society, technology, electromagnetic space, internet, ecology, natural resources, nuclear safety, and so on

[1] Disclaimer: The contents provided in this briefing are based on publicly available information and are not exhaustive. This document is for informational purpose only and should not be construed as business or legal advice on any specific facts or circumstances.

- crucial national security areas such as overseas interests, living things (eg humans, animals, plants) the space, polar region, deep sea, and Artificial Intelligence will be negatively influenced.
- there will be severe damage on development, production, operation, and economic interests of industries and information technologies.
- negative impacts on public interests, individuals, organisational rights are big, and the negative social influence is strong.
- a cascade effect is evident, affected industries and companies within the same industry are many, and the impact duration is long. Negative impacts on business and industrial development, technology progress as well as the industry ecosystem are strong.

Including any data that has been considered critical data following MIIT's assessment.

3. Core data

In case of data breaches or leaks

- significant national threats are posed on politics, territory, military, economy, culture, society, technology, electromagnetic space, internet, ecology, natural resources, nuclear safety, and so on. Severe negative influence on crucial national security areas such as overseas interests, living things, the space, polar region, deep sea, and Artificial Intelligence.
- there will be strong damage on system-relevant enterprises defined by MIIT, Critical Information Infrastructure (CII), and key national resources.
- there will be severe damage on manufacturing operations, telecommunication network (including internet) operation and service, and radio services. Large-scale operation termination, halting radio service, wide-scale internet and service paralysis, disabling big-scale business operations.

Including any data that has been considered core data following MIIT's assessment.

Furthermore, on 13th January 2022 the National Information Security Standardisation Technical Committee (TC260) published a Guideline for Identification of Critical Data calling for public comments. It shall set up a catalogue to support data operators as well as local and industry authorities to identify critical data.

Rules on Storing Industrial Data Domestically

As set out by the Security Management Measures, industrial data operators[2] are supposed to store their collected critical data and core data in China, including other industrial data as legally required. If industrial data needs to be transferred outside of China, MIIT's assessment and approval are required before any cross-border data transfers can proceed.

According to the Measures on Security Assessment of Cross-Border Data Transfer (call for comments) (hereinafter called Security Assessment Measures) published by the Cyberspace Administration of China (CAC), if any data meeting one of the following conditions needs to be transferred across borders, a security assessment by the national cybersecurity and information departments of MIIT are also required:

[2] According to the Article 3 of the Security Management Measures, industrial data operators include but not exclusive to enterprises, software and information technology service providers, telecommunications and radio service users who collect, store, use, manufacture, transfer, provide, and publicise the industrial data.

- Personal information and critical data are gathered by Critical Information Infrastructure Operators (CIIO)
- Any critical data is generated or collected
- Data covering more than 1.000.000 pieces of personal information is collected
- The accumulated amount of personal information transferred abroad exceeds the information of more than 100.000 people or the sensitive personal information of more than 10.000 people
- National cybersecurity and information departments have required to undergo cross-border data transfer security assessment

Security Assessment before Cross-border Data Transfer

The Security Assessment Measures describe the self-risk assessment as a legal obligation for all data processors and clearly regulate it as a prerequisite every time cross-border data transfer is conducted.

Only when the data transfer meets one of the regulated criteria, the security assessment conducted by national cybersecurity and information departments is required to be applied through local provincial-level departments.

Please find the detailed regulation criteria, assessment materials and processes in our project's previous policy update.

Outlook

Pilot areas

The free trade zones in Shanghai, Beijing, Zhejiang and Hainan released their own plans including practical trials for cross-border data transfer processing. Please find the background on the MOFCOM development plan for pilot areas and the cross-border data transfer pilots in different pilot zones in our project's previous policy updates: Innovative Development of Trade in Services in Pilot Areas and Cross-Border Data Transfer Piloting – focus on Hainan Free Trade Port.

Policy development

The Security Assessment Measures and the Security Management Measures are expected to be finalised after the final rounds of commenting. The specific dates have not been announced yet at the date of this publication. TC260 recently published the 2022 Cybersecurity National Standards' Requirement List, which includes standards for cross-border data transfer on "processing critical data", "CII evaluation" and "data exchange service". Further cross-border data transfer related regulations and standards within pilot zones or at national level are expected to be released by the end of this year.

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