

WHITEPAPER

Cross-Border Data Transfer

© Copyright 2025 CHINABRAND IP CONSULTING GMBH



Challenges, Implementation, and Compliance Strategies

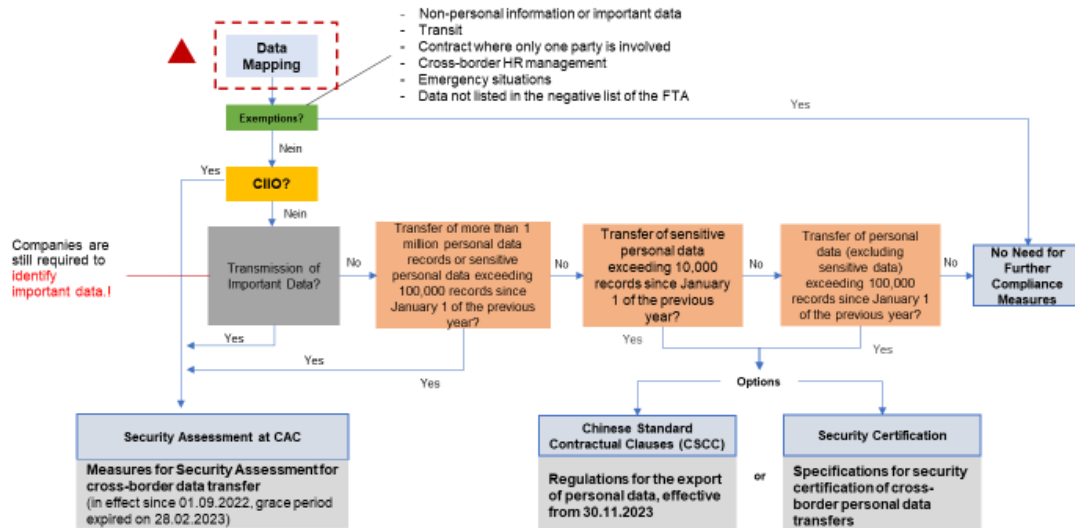
Cross-border data transfer (CBDT) in China is governed by a multitude of regulatory requirements, presenting companies with complex challenges. With the latest regulation adjusting compliance requirements, the Chinese government has now defined clear thresholds to help businesses efficiently and legally organize their data flows. The regulation simplifies certain aspects by exempting specific scenarios from additional review procedures while maintaining substantial data protection and security requirements.

These new regulations have far-reaching consequences for companies with subsidiaries or business activities in China. The regulatory hurdles for international data exchange remain high, and violations of the regulations can result in significant penalties. Therefore, it is essential for companies to develop a robust compliance framework that aligns with the new requirements as well as existing legal frameworks such as the Personal Information Protection Law (PIPL), the Cyber Security Law (CSL), and the Data Security Law (DSL).

Regulatory Framework and Requirements

The new provisions clarify under which conditions companies can transfer their data abroad without additional approvals and when additional security assessments are required. The classification is based on three key criteria:

1. **Data Volume and Sensitivity:** Companies transferring more than one million personal data records or over 10,000 sensitive personal data records annually must undergo a government security assessment. Transfers between 100,000 and one million personal data records require a Standard Contract (SCC) or certification. Companies transferring fewer than 100,000 personal data records are exempt from additional reporting and contract obligations.
2. **Industry Dependence and Critical Infrastructure:** Operators of critical information infrastructure (CII) remain subject to the strictest regulations and must conduct a security review for all data exports.
3. **Definition of Important Data:** The responsibility for identifying and reporting important data no longer lies solely with companies; authorities now publish official lists for various industries. Companies must regularly compare their data inventories with these lists.



© 2024 CHINABRAND IP CONSULTING GMBH

15

Some specific scenarios are now exempt from additional compliance measures. These include international business transactions such as cross-border payments, contract conclusions, HR data transfers for global personnel management, and emergency data transfers to protect life and property.

Type of Data Processor	Type of Data	Export Path (Statistical Basis: Cumulative provision of data abroad since January 1)		
		Security Assessment	Standard Contract or Certification	Exceptions
Critical Information Infrastructure Operator	Important Data	✓	X	✓ Articles 5 and 6 of the "New Rules on Cross-border Transfer"
	Personal Information	✓	X	
General Data Processor	Important Data	✓	X	✓ Less than 100,000 personal data items and no sensitive personal information
	Personal Information	✓ More than 1 million items of personal information (without sensitive personal information) Or ✓ More than 10,000 items of sensitive personal information	✓ More than 100,000 but less than 1 million items of personal information (without sensitive personal information) Or ✓ Less than 10,000 items of sensitive personal information	Or ✓ Other cases stipulated in Articles 5 and 6 of the "New Rules on Cross-border Transfer"

Challenges for Companies

Despite these simplifications, cross-border data transfer in China remains a complex issue. Companies must ensure that they comply with all relevant regulations and continuously adjust their processes to mitigate regulatory risks. The key challenges include:

- **Data Classification and Mapping:** Identifying and categorizing data according to Chinese standards differs from European requirements. While the GDPR primarily protects personal data, Chinese law includes categories such as 'important data' and 'core data,' which are closely linked to economic and national security interests.
- **Legal Uncertainties:** The interpretation of regulations can vary depending on industry and region. Local authorities have some discretion, making implementation and enforcement more complex.
- **Technical and Organizational Requirements:** Companies must not only implement appropriate IT security measures but also establish strict compliance processes to meet audit requirements.
- **Risk Management with External Service Providers:** Companies using cloud services or IT providers in China must ensure their partners also comply with legal requirements.

Solutions and Our Consulting Services

To address these challenges, we support companies with a structured approach to legally compliant cross-border data transfer. Our consulting services include:

1. Conducting a Comprehensive Data Mapping

A key part of a compliance strategy is a detailed inventory of all data processed within and outside China. This includes not only personal data but also the identification of critical business and corporate data. We help companies analyze their data flows, classify sensitive data, and detect compliance risks early on.

2. Gap Analysis and Development of a Compliance Framework

Each company has unique requirements for cross-border data transfer. We analyze existing data protection policies and IT infrastructures to identify compliance gaps. We then develop tailored recommendations to minimize risks and meet regulatory requirements.

3. Support with Government Approval Processes

Companies subject to a government security review must provide extensive documentation and technical evidence. We assist in this process, prepare the necessary compliance documents, and support communication with Chinese authorities.

4. Implementation of Technical Protection Measures

In addition to organizational requirements, companies must ensure that their IT infrastructure complies with legal provisions. This includes measures such as data encryption, access controls, security monitoring, and the implementation of Security Information and Event

Management (SIEM) systems. Our team assists with selecting and implementing appropriate technical solutions.

5. Employee Training and Awareness Programs

Many data protection violations result from human error or a lack of awareness of regulatory requirements. We offer practical training to prepare employees for the specific risks and regulations of Chinese data protection laws. This includes raising awareness of compliance processes, secure data transfer practices, and the proper handling of sensitive information.

For Further Informations

For more Informations about our services, please visit:

www.chinabrand.de

Contakt und Feedback

info@chinabrand.de

Blog | LinkedIn

© Copyright 2025 CHINABRAND IP CONSULTING GMBH. All rights reserved.

Grashofstraße 3, 80995 München - +49 89 321212800 - www.chinabrand.de