

WHITEPAPER

Grenzüberschreitender Datenverkehr

© Copyright 2025 CHINABRAND IP CONSULTING GMBH



Herausforderungen, Umsetzung und Compliance-Strategien

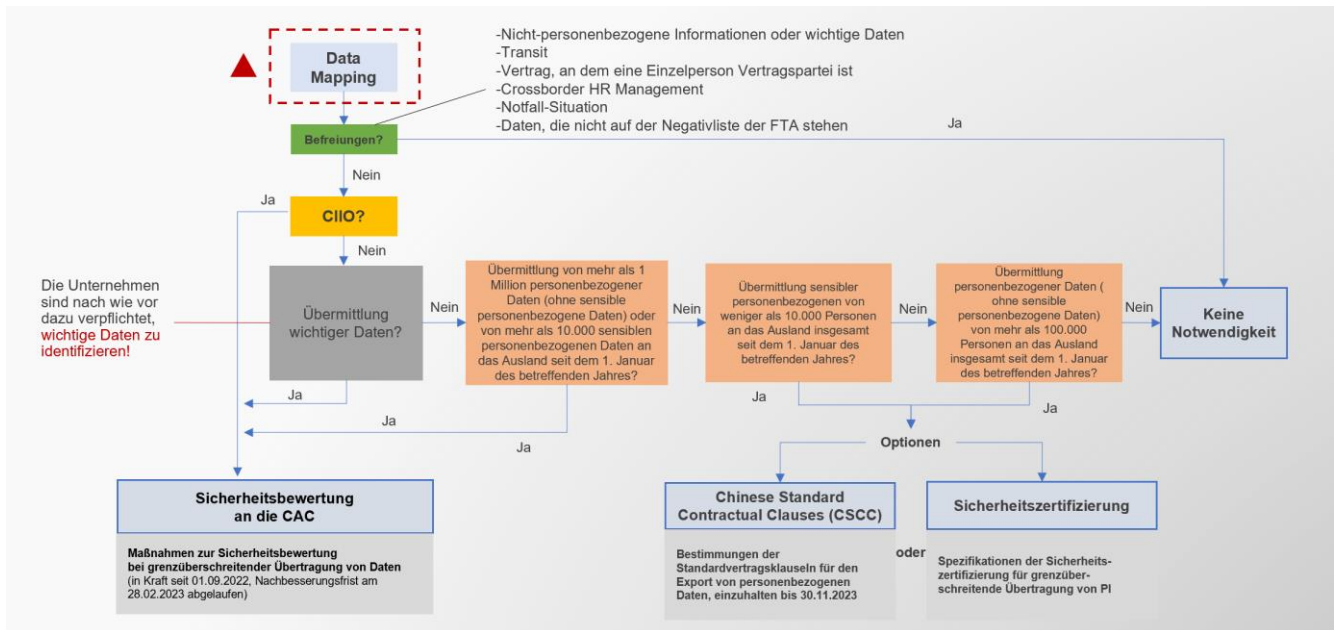
Der grenzüberschreitende Datenverkehr (*Cross-Border Data Transfer, CBDT*) in China ist durch eine Vielzahl regulatorischer Anforderungen geprägt, die Unternehmen vor komplexe Herausforderungen stellen. Mit der jüngsten Verordnung zur Anpassung der Compliance-Vorgaben hat die chinesische Regierung nunmehr klare Schwellenwerte definiert, die Unternehmen dabei helfen sollen, ihre Datenströme effizient und rechtssicher zu organisieren. Die Verordnung trägt zur Vereinfachung der Vorschriften bei, indem sie bestimmte Szenarien von zusätzlichen Prüfverfahren befreit, während sie gleichzeitig substanzielle Datenschutz- und Datensicherheitsanforderungen aufrechterhält.

Diese neuen Regularien haben weitreichende Konsequenzen für Unternehmen mit Niederlassungen oder Geschäftsaktivitäten in China. Die regulatorischen Hürden für den internationalen Datenaustausch sind weiterhin hoch, und Verstöße gegen die Vorschriften können empfindliche Strafen nach sich ziehen. Daher ist es für Unternehmen essenziell, ein belastbares Compliance-Framework zu entwickeln, das sowohl den neuen Anforderungen als auch bestehenden gesetzlichen Grundlagen wie dem *Personal Information Protection Law (PIPL)*, dem *Cyber Security Law (CSL)* und dem *Data Security Law (DSL)* entspricht.

Regulatorische Rahmenbedingungen und Anforderungen

Die neuen Vorgaben stellen insbesondere klar, unter welchen Bedingungen Unternehmen ihre Daten ohne zusätzliche Genehmigungen ins Ausland übertragen dürfen und wann zusätzliche Sicherheitsbewertungen erforderlich sind. Die Einstufung erfolgt anhand von drei wesentlichen Kriterien:

1. **Datenvolumen und Sensibilität:** Unternehmen, die jährlich mehr als eine Million personenbezogene Daten oder mehr als 10.000 sensible personenbezogene Daten ins Ausland transferieren, müssen eine behördliche Sicherheitsbewertung durchführen lassen. Liegt der Transfer zwischen 100.000 und einer Million personenbezogener Daten, ist ein Standardvertrag (SCC) oder eine Zertifizierung erforderlich. Für Unternehmen mit weniger als 100.000 personenbezogenen Datentransfers entfallen zusätzliche Melde- und Vertragsverpflichtungen.
2. **Branchenabhängigkeit und kritische Infrastruktur:** Betreiber kritischer Informationsinfrastruktur (CIIO) unterliegen weiterhin den strengsten Regularien und müssen jegliche Datenexporte einer Sicherheitsprüfung unterziehen.
3. **Definition wichtiger Daten:** Die Verantwortung zur Identifikation und Meldung wichtiger Daten liegt nun nicht mehr ausschließlich bei Unternehmen, sondern auch bei den Behörden, die offizielle Verzeichnisse für verschiedene Branchen veröffentlichen. Unternehmen müssen ihre eigenen Datenbestände regelmäßig mit diesen Verzeichnissen abgleichen.



Einige spezifische Szenarien sind nun von zusätzlichen Compliance-Maßnahmen befreit. Dazu gehören internationale Geschäftstransaktionen wie grenzüberschreitende Zahlungen, Vertragsabschlüsse, HR-Datenübertragungen für globale Personalverwaltung sowie Notfalldatenübertragungen zum Schutz von Leben und Eigentum.

Typ des Datenverarbeiters	Typ der Daten	Exportpfad (Statistische Basis: Kumulative Bereitstellung von Daten ins Ausland seit dem 1. Januar)		
		Sicherheitsbewertung	Standardvertrag oder Zertifizierung	Ausnahmen
Betreiber kritischer Informationsinfrastrukturen	Wichtige Daten	✓	X	✓ Artikel 5 und Artikel 6 der 'Neuen Regelungen zur Grenzüberschreitung'
	Persönliche Informationen	✓	X	
Allgemeine Datenverarbeiter	Wichtige Daten	✓	X	✓ Weniger als 100.000 Personeninformationen; und keine sensiblen persönlichen Informationen oder ✓ Andere in Artikel 5 und Artikel 6 der 'Neuen Regelungen zur Grenzüberschreitung' festgelegte Fälle
	Persönliche Informationen	✓ Mehr als 1 Million Personeninformationen (ohne sensible persönliche Informationen) Oder ✓ Mehr als 10.000 sensible persönliche Informationen	✓ Mehr als 100.000 Personen, aber weniger als 1 Million Personeninformationen (ohne sensible persönliche Informationen) oder ✓ Weniger als 10.000 sensible persönliche Informationen	

Anpassung der Schwellenwerte

Herausforderungen für Unternehmen

Trotz dieser Erleichterungen bleibt der grenzüberschreitende Datenverkehr in China eine komplexe Angelegenheit. Unternehmen müssen sicherstellen, dass sie alle relevanten Regularien einhalten und ihre Prozesse kontinuierlich anpassen, um regulatorischen Risiken vorzubeugen. Die wesentlichen Herausforderungen umfassen:

- **Datenklassifizierung und -mapping:** Die Identifikation und Einstufung von Daten nach chinesischen Standards unterscheidet sich von den europäischen Anforderungen. Während die DSGVO primär personenbezogene Daten schützt, umfasst das chinesische Recht auch Kategorien wie „wichtige Daten“ und „Kerndaten“, die eng mit wirtschaftlichen und nationalen Sicherheitsinteressen verknüpft sind.
- **Rechtliche Unsicherheiten:** Die Interpretation der Verordnung kann je nach Branche und Region unterschiedlich ausfallen. Lokale Behörden haben einen gewissen Ermessensspielraum, was die Umsetzung und Durchsetzung der Vorgaben erschwert.
- **Technische und organisatorische Anforderungen:** Unternehmen müssen nicht nur geeignete IT-Sicherheitsmaßnahmen implementieren, sondern auch strenge Compliance-Prozesse etablieren, um Audit-Anforderungen zu erfüllen.
- **Risikomanagement bei externen Dienstleistern:** Unternehmen, die Cloud-Dienste oder IT-Dienstleister in China nutzen, müssen sicherstellen, dass ihre Partner ebenfalls den gesetzlichen Anforderungen entsprechen.

Lösungsansätze und unsere Beratungsleistungen

Um diesen Herausforderungen zu begegnen, unterstützen wir Unternehmen mit einer strukturierten Herangehensweise an den gesetzeskonformen grenzüberschreitenden Datenverkehr. Unsere Beratungsleistungen umfassen:

1. **Durchführung eines umfassenden Data Mapping** Ein wesentlicher Bestandteil der Compliance-Strategie ist eine detaillierte Bestandsaufnahme aller Daten, die innerhalb und außerhalb Chinas verarbeitet werden. Dabei geht es nicht nur um personenbezogene Daten, sondern auch um die Identifikation kritischer Geschäfts- und Unternehmensdaten. Wir helfen Unternehmen, ihre Datenflüsse zu analysieren, sensible Daten zu klassifizieren und Compliance-Risiken frühzeitig zu erkennen.
2. **Gap-Analyse und Erstellung eines Compliance-Frameworks** Jedes Unternehmen hat individuelle Anforderungen an den grenzüberschreitenden Datenverkehr. Wir analysieren bestehende Datenschutzrichtlinien und IT-Infrastrukturen, um Lücken in der Compliance zu identifizieren. Anschließend entwickeln wir maßgeschneiderte Handlungsempfehlungen zur Risikominimierung und Erfüllung regulatorischer Anforderungen.
3. **Unterstützung bei behördlichen Genehmigungsprozessen** Unternehmen, die einer behördlichen Sicherheitsbewertung unterliegen, müssen umfangreiche Dokumentationen und technische Nachweise erbringen. Wir begleiten diesen Prozess, erstellen notwendige

Compliance-Dokumente und unterstützen die Kommunikation mit den chinesischen Behörden.

4. **Implementierung technischer Schutzmaßnahmen** Neben organisatorischen Anforderungen müssen Unternehmen sicherstellen, dass ihre IT-Infrastruktur den gesetzlichen Vorgaben entspricht. Dazu gehören Maßnahmen wie Datenverschlüsselung, Zugriffskontrollen, Sicherheitsüberwachung und Implementierung von Security Information and Event Management (SIEM)-Systemen. Unser Team unterstützt bei der Auswahl und Implementierung geeigneter technischer Lösungen.
5. **Schulungen und Sensibilisierung der Mitarbeiter** Viele Verstöße gegen Datenschutzvorgaben entstehen durch menschliche Fehler oder mangelndes Bewusstsein für regulatorische Anforderungen. Wir bieten praxisnahe Schulungen an, um Mitarbeiter auf die spezifischen Risiken und Vorschriften des chinesischen Datenschutzrechts vorzubereiten. Dies umfasst die Sensibilisierung für Compliance-Prozesse, sichere Datenübertragungspraktiken und den richtigen Umgang mit sensiblen Informationen.

Die neuen Regelungen zum grenzüberschreitenden Datenverkehr in China bieten einerseits Erleichterungen für Unternehmen, die sich an die Compliance-Vorgaben halten, verschärfen jedoch gleichzeitig die Anforderungen an Transparenz und Nachweisbarkeit. Die effektive Umsetzung dieser Vorgaben erfordert eine strategische Herangehensweise, technologische Anpassungen und kontinuierliches Risikomanagement.

Durch unsere langjährige Erfahrung im Bereich Datenschutz-Compliance in China unterstützen wir Unternehmen dabei, rechtliche Risiken zu minimieren, behördliche Anforderungen zu erfüllen und gleichzeitig einen reibungslosen internationalen Datentransfer sicherzustellen. Mit gezielten Audit-Strategien, datenbasierten Compliance-Lösungen und maßgeschneiderten Beratungsansätzen sorgen wir dafür, dass Unternehmen auch in einem anspruchsvollen regulatorischen Umfeld handlungsfähig bleiben und nachhaltige Datenschutzstrategien etablieren.

Weitere Informationen

Weitere Informationen über unsere Dienstleistungen finden Sie hier:

www.chinabrand.de

Kontakt 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