CHINA 華牌 BRAND®

CYBERSECURITY UND DATENSCHUTZ IN CHINA

Neue Gesetze und Handlungsempfehlungen

Dr. Hans Joachim Fuchs, Mareike Seeßelberg, Zihao Liao

CHINABRAND IP CONSULTING GMBH

Grashofstrasse 3 ▪ 80995 München ▪ +49 89 32 12 12 800

info@chinabrand.de ▪ www.chinabrand.de

Grashofstraße 3, 80995 München

+49 89 321212800

www.chinabrand.de

Inhaltsverzeichnis

Übersicht neue Gesetze und Regularien

Die Volksrepublik China fühlt sich in ihrer nationalen Sicherheit bedroht. Der Grund liegt in den wachsenden Spannungen zwischen den USA und dem Reich der Mitte, die in der forcierten Entkoppelung der asiatischen Nation vom Westen – inklusive Europas – resultiert. China entkoppelt ebenso wie die USA nicht nur gezielt Lieferketten und Technologien, sondern auch grenzüberschreitende Datenflüsse, die Forschung, Standards und Personenfreizügigkeit.

Die politische Strategie zielt darauf, die chinesische Industrie zu nationalisieren und umfassend aufzuwerten, die Binnenwirtschaft (*Domestic Circle*) zu stärken und die Marktanteile ausländischer Unternehmen zu reduzieren oder sie ganz aus dem chinesischen Markt zu verdrängen. Der strategische Plan Made in China 2025, der zwar nicht mehr offensiv kommuniziert wird, ist weiterhin in Kraft und wird im Rahmen der neuen *Leitsätze zur Ausweitung von Investitionen in strategisch aufstrebende Industrien* durch verschiedene Behörden jetzt mit Nachdruck umgesetzt.

Digitale Technologien und Daten spielen in dieser Strategie eine herausragende Rolle. Die chinesische Regierung hat zahlreiche datenrelevante Stimulus-Maßnahmen in Hochtechnologie-Sektoren wie die 5G-Infrastruktur, Datenzentren, die Förderung digitaler Plattformen und einer Digitalwährung etabliert, die in den betroffenen Branchen als Markttreiber wirken.

Die stärkere politische Aktivität führt zu einer erhöhten regulatorischen Dynamik, die ausländische Unternehmen in China jetzt herausfordert. Sie sind zum einen gezwungen, die für ihr Geschäft relevanten wirtschaftspolitischen und regulatorischen Entwicklungen zeitnah zu beobachten und ihre Compliance-Aktivitäten anzupassen, müssen anderseits aber auch ihre Geschäftsmodelle und Strategien für den chinesischen Markt überdenken und ggf. anpassen.

In den Jahren seit dem in Kraft treten des *Cybersecurity Gesetzes* (CSL) in China am 1. Juni 2017, als grundlegendes Gesetz nicht nur für Cybersicherheit, sondern auch Datenschutz, hat die Gesetzgebungsaktivität in China zu diesen beiden Themenbereichen stetig zugenommen. Vor allem die Jahre 2019 und 2020 haben eine Flut an neuen Vorschriften und Standards gebracht. Nicht alle dieser Vorschriften fügen sich harmonisch zu einem Gesamtbild zusammen. Das liegt vor allem daran, dass es sich um eine bunte Mischung aus Vorschriften, Verordnungen und Standards von verschiedenen Ministerien und regionalen und nationalen Behörden handelt; für das Thema Cybersicherheit sind in China drei Ministerien gleichzeitig zuständig: die Cyberspace Administration of China (CAC), das Ministerium für Industrie und Informationstechnologie (MIIT) sowie das Ministerium für Öffentliche Sicherheit (MPS).

Die verstärkte politische und gesetzgeberische Aktivität in den Bereichen Cybersicherheit und Datenschutz ist nicht nur für ausländische Unternehmen, sondern auch für chinesische Unternehmen herausfordernd. Compliance mit den Vorschriften sollte nicht zuletzt wegen der hohen möglichen Bußgelder, einen hohen Stellenwert einnehmen.

Auch natürliche Personen haben inzwischen die Möglichkeit, zivilrechtlich gegen sie betreffende Datenschutzverletzungen vorzugehen. Grundlage hierfür ist das neue *Zivilgesetzbuch der VRC*, das am 1. Januar 2021 in Kraft trat. Für Unternehmen bedeutet das, dass sie bei Verstößen gegen den Datenschutz nicht mehr nur mit Bußgeldern, sondern auch mit Schadensersatzforderungen rechnen müssen.

Viele der oben bereits erwähnten Verordnungen enthalten Vorschriften, die zu einem konkreten Handlungsbedarf bei in China tätigen Unternehmen führen. Hier ist vor allem das *Multi-Level Protection Scheme 2.0 (MLPS 2.0)* zu erwähnen, auf das im Folgenden noch genauer eingegangen wird. Relevant sind aber beispielsweise auch Vorschriften zu Verschlüsselungstechnologien.

Auch die Implikationen des *Data Security Law (DSL)* und des *Personal Information Protection Law (PIPL)* sollten nicht missachtet werden. Das DSL ist am 1. September 2021 in Kraft getreten und das PIPL ist bereits verabschiedet und wird am 1. November 2021 in Kraft treten. Beide Gesetze, vor allem das *PIPL*, enthalten, neben der DSGVO sehr ähnlichen Regelungen zum Schutz von personenbezogenen Daten, Vorschriften, die beispielsweise den Transfer von Daten ins Ausland einschränken könnten.

Übersicht über die wichtigsten Gesetze, Verordnungen und Normen in der VR China:

Geltende Gesetze, Verordnungen und Standards			
Name	**Level**	**In Kraft seit**	**Relevante Artikel**
Criminal Law	Gesetz	1.3.2021	Artikel 253(1) [1]
Civil Code	Gesetz	1.1.2021	Artikel 111[2], 1034 ff.
State Security Law	Gesetz	1.7.2015	Artikel 25 [3]
Cybersecurity Law	Gesetz	1.6.2017	Komplett
Encryption Law	Gesetz	1.1.2020	Komplett
Personal Information Protection Law	Gesetz	1.11.2021	Komplett
Data Security Law	Gesetz	1.9.2021	Komplett
Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection	Gesetz	28.12.2012	Artikel 2, Artikel 3 [4]

[1] Article 253(1) When persons sell or provide personal information of citizens to others in violation of relevant national provisions, and the circumstances are serious, the sentence can be fixed-term imprisonment of no more than 3 years or criminal detention, in combination of fines, or the sentence can be fines alone; if the circumstances are particularly serious, the sentence shall be fixed-term imprisonment from 3 to 7 years, in combination of fines.

[2] Article 111 A natural person's personal information is protected by law. Any organization or individual that needs to access other's personal information must do so in accordance with law and guarantee the safety of such information, and may not illegally collect, use, process, or transmit other's personal information, or illegally trade, provide, or publicize such information. Article 1034 A natural person's personal information is protected by law. Personal information is the information recorded electronically or in other ways that can be used, by itself or in combination with other information, to identify a natural person, including the name, date of birth, identification number, biometric information, residential address, telephone number, email address, health information, whereabouts, and the like, of the person. The provisions on the right of privacy, or, in absence of which, the provisions on the protection of personal information, shall be applied to the private personal information.

[3] Article 25 The State shall develop network and information security assurance system, enhance network and information security assurance capabilities, strengthen innovative research and development and application of network and information technologies and realize the security and controllability of network and information core technologies, critical infrastructure and information systems and data in key areas; the State shall also enhance network management, prevent, deter and punish network criminal acts such as cyber-attacks, network intrusion, network theft and illegal spread of harmful information in order to safeguard the sovereignty, security and development interests of the state cyberspace.

[4] Article 2 Network service providers and other enterprises and public institutions that collect or use citizens' personal electronic information in the their business activities shall follow the principles of lawfulness, reasonableness and necessity, explicitly state the purpose, method and scope of collection and use of the information, obtain the consent of the one whose information is collected, and shall not collect or use information in a manner that violates the provisions of laws and regulations, or the agreement of the parties. Network information providers and other enterprises and public institutions that collect or use citizens' personal electronic information shall make in public their rules for the collection and use. Article 3 Network service providers and other enterprises, public institutions and their

Provisions on Protecting the Personal Information of Telecommunications and Internet Users	Verordnung	1.9.2013	Komplett
Provisions on the Cyber Protection of Children's Personal Information	Verordnung	1.10.2019	Komplett
Guidelines for Internet Personal Information Security Protection	Richtlinie	10.4.2019	Komplett
Information Security Technology—Guideline for Personal Information Protection within Information System for Public and Commercial Services (GB/Z 28828-2012)	Freiwilliger Standard	1.2.2013	Komplett
Information Security Technology—Personal Information Security Specification (GB/T 35273—2017)	Freiwilliger Standard	1.10.2020	Komplett
Information Security Technology—Baseline for Classified Protection of Cybersecurity (GB / T 22239-2019)	Freiwilliger Standard	1.12.2019	Komplett
Information Security Technology—Technical Requirements of Security Design for Classified Protection of Cybersecurity (GB / T 25070-2019)	Freiwilliger Standard	1.12.2019	Komplett
Information Security Technology—Evaluation Requirements for Classified Protection of Cybersecurity (GB / T 28448-2019)	Freiwilliger Standard	1.12.2019	Komplett
Entwürfe			
Name	**Level**	**Veröffentlichung**	**Relevante Artikel**
Measures for the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft for Comment)	Verordnung	11.4.2017	Komplett
Administrative Measures on Data Security (Draft for Comment)	Verordnung	28.5.2019	Komplett
Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment)	Verordnung	13.6.2019	Komplett
Regulations on the Multi-Level Protection Scheme for Cybersecurity (Draft for Comment)	Verordnung	27.6.2018	Komplett
Measures for Cybersecurity Review	Verordnung	21.5.2019	Komplett

employees must strictly keep confidential of citizens' personal electronic information collected during their business activities and may not disclose, falsify, damage, sell or illegally provide such information to others.

Implementation Opinions on Carrying out the Testing and certification Work of Commercial Cryptographic Products (Draft for Comment)	Verordnung	20.2.2020	Komplett
Information Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comment)	Standard	30.8.2017	Komplett
Information Security Technology - Security Impact Assessment Guide of Personal Information (Draft for Comment)	Standard	11.6.2018	Komplett
Information Security Technology - Guidelines for Personal Information Notices and Consent (Draft for Comment)	Standard	20.1.2020	Komplett

Im Folgenden wird auf die einzelnen relevanten Gesetze und Regelungen genauer eingegangen.

Ziel dieses White Paper ist es, Unternehmen die Beurteilung ihrer Betroffenheit durch die relevanten Gesetze im Bereich der Cybersecurity und des Datenschutzes zu ermöglichen und das weitere erforderliche Vorgehen zur Compliance zu skizzieren. Der Fokus liegt vor allem auf Vorschriften, die Unternehmen betreffen, die nicht Betreiber kritischer Infrastruktur sind.

Grundlage des White Papers sind die aktuell vorliegenden Gesetze und Verordnungen sowie noch nicht in Kraft getretene Gesetzesentwürfe und Verordnungsentwürfe im Zusammenhang mit Cybersecurity und Datenschutz.

Cyber Security Law (CSL)

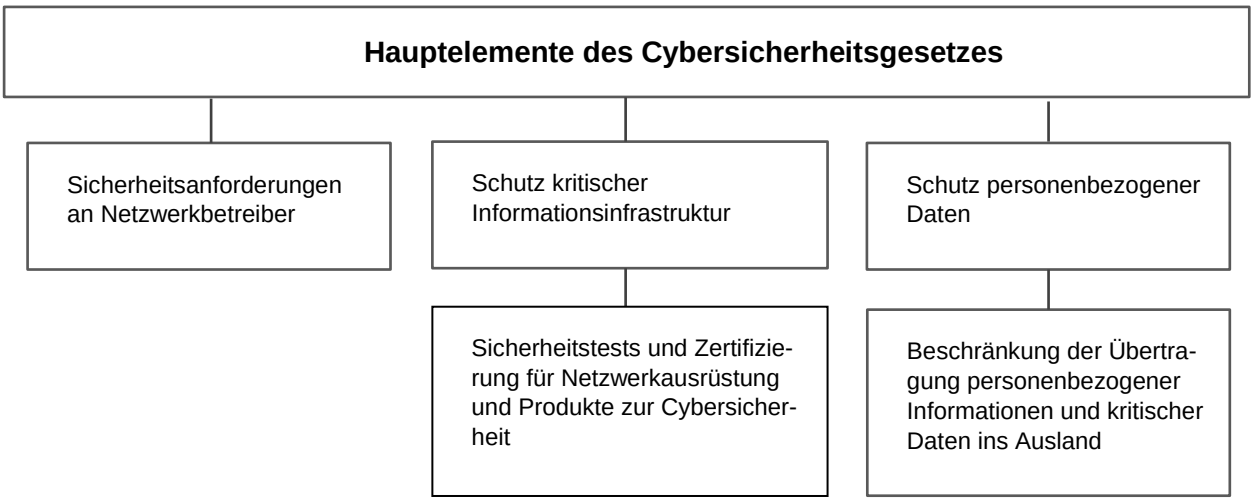
Das *Cybersicherheitsgesetz der Volksrepublik China* (CSL) ist Grundlage für Chinas heutige Gesetzgebung zu Netzwerksicherheit und Datenschutz.

Das Gesetz sieht strenge Regelungen und Haftung für sogenannte „Netzwerkbetreiber“ und noch strengere Regulierungen für diejenigen Organisationen, die so genannte „kritische Infrastruktur“ betreiben, vor. „Netzwerkbetreiber“ sind Inhaber, Betreiber und Nutzer eines Netzwerkes sowie Netzwerkdienstanbieter. Ein „Netzwerk“ wird als ein System definiert ist, das aus Computern oder anderen Informationsterminals und damit verbundener Ausrüstung besteht und nach bestimmten Regeln und Verfahren Informationen sammelt, speichert, überträgt, tauscht und verarbeitet. Das bedeutet, dass jedes Unternehmen in China, das ein Computernetzwerk oder aber auch nur eine Website betreibt, ein Netzwerkbetreiber im Sinne der oben genannten Definition ist.

Betreiber kritischer Informationsinfrastruktur sind nach dem *CSL* vor allem Organisationen im Transport-, Energie und Finanzsektor sowie in den Bereichen der öffentlichen Kommunikation und Information, des Wasserbaus und der E-Governance. Außerdem alle Unternehmen mit Informationssystemen, bei denen im Falle einer Störung mit schwerwiegenden Folgen für den Staat und die öffentliche Sicherheit zu rechnen ist. Die konkrete Bestimmung der einzelnen betroffenen Organisationen obliegt dem Staatsrat. Eine weitere Konkretisierung der Definition von CIIOs findet sich in den *Vorschriften zum Schutz der Sicherheit von kritischen Informationsinfrastrukturen (Entwurf)*. Alle oben genannten Definitionen müssen immer in Zusammenhang mit den weiteren relevanten Verordnungen zur Cybersicherheit und dem Datenschutz gesehen werden. In diesen finden sich häufig weitere Ausführungen zu den Definitionen.

Inhaltlich deckt das *CSL* unter anderem die Themenbereiche Schutz personenbezogener Daten, Netzwerksicherheit, Schutz von kritischer Informationsinfrastruktur, Datenlokalisierung und Risikobewertung bei Datentransfer ins Ausland sowie Sicherheitsüberprüfung von Netzwerkprodukten und Dienstleistungen ab.

Die Hauptelemente des Cybersicherheitsgesetzes können wie folgt dargestellt werden:



Das *CSL* ist das Grundgerüst für die darauffolgenden Vorschriften, die die recht allgemeinen Vorgaben des *CSL* konkretisieren und teilweise erst umsetzbar machen.

Für Unternehmen sind vor allem die Vorschriften zu

- Multi-Level Protection Scheme
- Schutz von personenbezogenen Daten
- Einsatz von Netzwerkprodukten und
- Verschlüsselungstechnologien

relevant. Grundsätzlich kann zwischen Vorschriften zum Datenschutz und Vorschriften zur Netzwerksicherheit im CSL differenziert werden.

Datenschutz

Das *CSL* enthält eine Reihe von Vorschriften in Bezug auf das Sammeln, Speichern und Verarbeiten von personenbezogenen Informationen. Außerdem reguliert es die Übermittlung von kritischen Daten und personenbezogenen Informationen ins Ausland. Der Begriff „personenbezogene Daten" bezieht sich auf verschiedene Informationen, in elektronischer oder anderer Form, über eine natürliche Person, die allein oder in Kombination mit weiteren Informationen die Identifikation der Person ermöglichen, wie der Name, das Geburtsdatum, die ID Nummer, biometrische Informationen, die Adresse, Telefonnummern und E-Mail-Adressen.

Im geltenden freiwilligen Standard *Personal Information Security Specification* wird des Weiteren der Begriff „sensible personenbezogenen Daten" definiert als Informationen, die, wenn sie geleakt werden, die Sicherheit der Person gefährden, ihrer Reputation schaden oder zu diskriminierender Behandlung führen – beispielsweise ID Nummern, persönliche biometrische Informationen, Bank Accounts, Kommunikationsauszeichnungen, Eigentumsinformationen und Kreditinformationen.

Weitere relevante durch die *Specification* definierte Begriffe sind „Subjekt personenbezogener Daten", die natürliche Person, die durch die entsprechenden personenbezogenen Daten identifiziert werden kann, und „Daten Controller", die Organisation oder das Individuum, das die entsprechenden personenbezogenen Daten kontrolliert und den Zweck und die Art der Datenverarbeitung bestimmt.

Der Schutz von personenbezogenen Daten, wie im *CSL*, dem *Zivilgesetzbuch* und weiteren Vorschriften geregelt, unterliegt den folgenden Grundprinzipien, die der DSGVO in vielen Punkten ähneln:

- Integrität und Vertraulichkeit
- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit

Betroffene in China haben ähnlich wie in der DSGVO das Recht über die Datensammlung sowie die Art der Datenverarbeitung informiert zu werden, das Recht, die über sie gespeicherten Daten abzufragen, Fehler zu korrigieren, die Löschung der Daten zu fordern und das Recht, die Verarbeitung der Daten abzulehnen.

Bei Verstößen von Netzwerkbetreibern gegen die Datenschutzvorschriften können die verantwortlichen Behörden die Unternehmen auffordern Sicherheitslücken zu beheben, illegale Einnahmen konfiszieren und Bußgelder auferlegen.

Privatpersonen können auf dem zivilrechtlichen Weg gegen Datenschutzverletzungen vorgehen und Schadensersatz fordern. Auch strafrechtlich ist der Missbrauch oder illegale Verkauf von Daten relevant: seit der letzten Änderung des Strafgesetzes kann der aktive Verkauf oder das Anbieten gesammelter persönlicher Daten mit einer Freiheitsstrafe von bis zu sieben Jahren geahndet werden. Auch Unternehmen können Täter sein, die verantwortliche Person im Unternehmen haftet entsprechend.

Auch das Thema der Übertragung von Daten nach außerhalb von China wird im *CSL* aufgegriffen. Allerdings schränkt das *CSL* nur die Übertragung von bestimmten wichtigen und personenbezogenen Daten durch Betreiber von CIIOs ein. Betreiber kritischer Informationsinfrastruktur dürfen weder persönliche Informationen noch wichtige Daten, die in China gesammelt wurden, ohne eine vorherige Sicherheitskontrolle durch chinesische Behörden auf Server oder zu Empfängern im Ausland übertragen. Für die Definition von wichtigen Daten wird auf die *Richtlinie zur Identifikation wichtiger Daten* verwiesen, die sich im Anhang des Standard *Information Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comment)* befindet und, neben einer Definition, eine Liste mit Beispielen für wichtige Daten, sowie Hinweise darauf, wie wichtige Daten identifiziert werden können enthält. Laut diesem Standard sind wichtige Daten diejenigen Daten, die in China von Unternehmen, Organisationen oder Privatpersonen gesammelt oder erzeugt werden, die kein Staatsgeheimnis sind, aber einen engen Bezug zu der nationalen Sicherheit, der wirtschaftlichen Entwicklung und dem öffentlichen Interesse haben und die im Falle eines Leaks, dem Verlust, dem Missbrauch, der Verfälschung oder der Löschung, oder auch nach Kombination, Integration oder weiterer Analyse zu den unten aufgeführten Folgen führen können:

1. Gefährdung der nationalen Sicherheit, von Verteidigungsinteressen und internationaler Beziehungen;
2. Verletzung von Staatseigentum, öffentlichen Interessen und legale Interessen von Privatpersonen;
3. Auswirkung auf nationale Prävention und das Vorgehen gegen wirtschaftliche und militärische Spione, politische Einflussnahme und organisiertes Verbrechen;
4. Auswirkungen auf die legale Verfolgung von illegalem Verhalten durch Behörden;
5. Störung der legalen Durchführung von Überwachung, Management, Inspektion und Überprüfung durch Regierungsabteilungen und Behinderung von Regierungsabteilung bei ihrer Pflichterfüllung;
6. Gefährdung der Sicherheit von grundlegenden Infrastruktur, kritischer Informationsinfrastruktur oder Regierungsinformationssysteme;
7. Auswirkung auf oder Gefährdung der Wirtschaftsordnung oder finanzieller Sicherheit;
8. Möglichkeit der Auswertung und Analyse von Staatsgeheimnissen oder sensiblen Informationen;
9. Auswirkungen auf oder Gefährdung der nationalen Politik, des Territoriums, von Militärangelegenheiten, Wirtschaft, Kultur, Gesellschaft, Wissenschaft, Informationen, Ökonomie, Ressourcen, nukleare Anlagen, und andere Angelegenheiten der nationalen Sicherheit.

In den *Maßnahmen zum Sicherheits-Assessment des Cross-Border Transfers von personenbezogenen Daten und wichtigen Daten (Entwurf)* werden wichtige Daten ebenfalls definiert als: Daten mit engem Bezug zur nationalen Sicherheit, der wirtschaftlichen Entwicklung und den öffentlichen Interessen der Gesellschaft.

So würden beispielsweise Dokumente zu den Sicherheitssystemen eines Unternehmens in der Energieversorgung unter die Definition wichtiger Daten fallen. Aber auch die riesigen Mengen an Daten die Alibaba gesammelt hat, nicht alle davon personenbezogen, fallen in diese Kategorie. Allerdings ist keines der oben genannten Dokumente offiziell gültig. Sie dienen daher mehr als Orientierungshilfe, solange keine rechtlich wirksame Definition existiert.

Abhängig von weiteren Ausführungsbestimmungen zum *CSL*, bzw. weiterer Gesetzgebung, könnte die Einschränkung der Übermittlung von Daten ins Ausland in naher Zukunft auch für einfache Netzwerkbetreiber gültig werden. Derartige Einschränkungen würden für ausländische Unternehmen ein großes Hindernis darstellen, da eine Übermittlung von personenbezogenen Daten an das Hauptquartier der Firma in vielen Branchen Standard ist und der Transfer von Daten über Grenzen hinweg im alltäglichen Geschäftsverkehr nicht wegzudenken ist. Weitere Details zu den aktuellen Entwicklungen im Bereich Datentransfer finden Sie in den Kapiteln zum *DSL* und *PIPL*.

Im Moment gibt es keine einheitliche Behörde zur Überwachung der Umsetzung der Vorschriften des *CSL*. Involvierte Behörden sind unter anderen die Cyberspace Administration China (CAC), das Ministerium für Industrie und Informationstechnologie, sowie die Behörde für öffentliche Sicherheit.

Unternehmen sollten sich informieren, welche Vorschriften für sie gelten und ob ihr aktuelles Datenschutzsystem den gesetzlichen Anforderungen entspricht. Ist das nicht der Fall müssen die Systeme zeitnah angepasst werden.

Netzwerksicherheit

Das *CSL* beinhaltet grundlegende Vorschriften zur Netzwerksicherheit. Für die Betreiber von CIIOs und die Hersteller von cybersicherheitsrelevanten Produkten gibt es Vorschriften zum Vertrieb, bzw. Erwerb von Netzwerk Ausrüstung, Cybersicherheitsprodukten und -dienstleistungen.

Kritische Netzwerkausrüstung und Produkte mit Bezug zu Cybersicherheit müssen seit Inkrafttreten des Gesetzes vor dem Vertrieb durch qualifizierte Einrichtungen zertifiziert werden.

Des Weiteren müssen sich Betreiber kritischer Informationsinfrastruktur, die Netzwerkprodukte und -dienstleistungen kaufen, einer Sicherheitsuntersuchung unterziehen.

Vor allem die Zertifizierung von Cybersicherheitsprodukten und Dienstleistungen, aber auch die Sicherheitsüberprüfung, bereitet ausländischen Unternehmen Sorge. Es besteht die Sorge, dass hierbei beispielsweise Quellcode von Computerprogrammen herausgegeben werden muss, also IP-rechtlich geschütztes Material. Die Angst vor IP-Diebstahl ist deswegen groß.

Ob diese Angst begründet ist, bleibt abzuwarten. In jedem Fall ist Kooperation mit den chinesischen Behörden im Falle einer Sicherheitsuntersuchung wichtig, um negative Folgen für das Unternehmen zu vermeiden. Relevant in diesem Bereich ist auch das *Kryptographie Gesetz* auf das in einem späteren Kapitel eingegangen wird.

Seit Mitte 2018 werden vermehrt Unternehmen auf ihre Compliance zu Cybersicherheitsvorschriften überprüft und mit entsprechenden Bußgeldern belegt, meist nachdem Systeme gehackt und Daten geleakt wurden. In 2018 traten die *Vorschriften zur Cybersicherheits-Überwachung und -Untersuchung der Behörde für Öffentliche Sicherheit* in Kraft, die es den Public Security Bureaus (PSB) erlaubt Unternehmen zukünftig auf ihre Einhaltung des *CSL* überprüfen. Inspektionen können sowohl vor Ort als auch remote – also über das Internet – durchgeführt werden. Kontrolliert wird beispielsweise, ob ein Datenschutzbeauftragter ernannt wurde, geeignete technische Schutzmaßnahmen vorhanden sind oder ob Daten illegal weitergegeben werden, aber auch ob die IT Systeme sicher vor Angriffen sind. Das PSB erhält damit potentiellen Zugang zu einer Vielzahl hoch sensibler Unternehmensdaten. Die Anforderung, Informationen für Stichproben zu übermitteln, erhöht das Risiko einer Sicherheitsverletzung oder eines Informationsverlustes für Unternehmen deutlich.

Ein weiterer relevanter Teil der Vorschriften zur Netzwerksicherheit ist das Multi-Level Protection Scheme (MLPS). Hierbei handelt es sich nicht um ein separates Gesetz, sondern um einen Teil des *CSL*, der durch weitere Verordnungen konkretisiert und in den letzten Jahren verstärkt durchgesetzt wird. Im folgenden Kapitel finden Sie mehr Informationen zum MLPS.

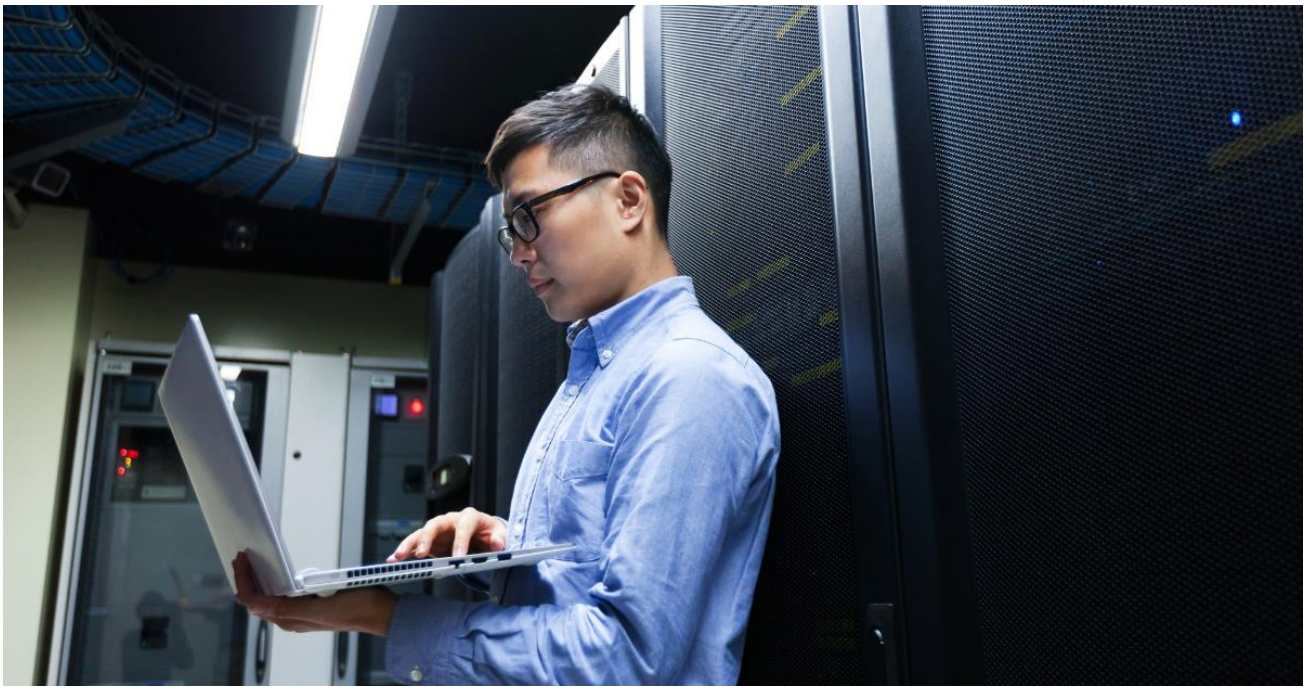
Multi-Level Protection Scheme (MLPS 2.0)

Das auf Art. 21 *CSL* beruhende Multi-Level Protection Scheme 2.0 (MLPS) wird seit dem Jahr 2019 forciert umgesetzt. Das Regulierungssystems für Daten- und Cybersicherheit schreibt vor, dass alle Unternehmen nach den Vorgaben eines mehrstufigen Schutzsystems sicherzustellen haben, dass ihr Netzwerk frei von Interferenzen, Schäden oder unbefugtem Zugang ist und dass keine Daten weitergegeben, gestohlen oder gefälscht werden können. Der Rahmen des obligatorischen MLPS 2.0 ist weit und umfasst ebenso wie das *CSL* praktisch alle in China tätigen Unternehmen.

In den Jahren 2019 und 2020 wurden nationalen Standards herausgegeben, um die Umsetzung des MLPS durch detailliertere technische Anforderungen zu fördern:

- *Informationssicherheitstechnologie - Leitfaden für den klassifizierten Schutz der Cybersicherheit (GB / T 22240-2020)*
- *Grundlegenden Anforderungen für den mehrstufigen Schutz der Cybersicherheit* (GB / T 22239-2019),
- *Informationssicherheitstechnologie - Technische Anforderungen an das Sicherheitsdesign für den klassifizierten Schutz der Cybersicherheit* (GB / T 25070-2019) und
- *Informationssicherheitstechnologie - Bewertungsanforderungen für den klassifizierten Schutz der Cybersicherheit* (GB / T 28448-2019).

Diese zentralen Standards definieren das MLPS und anhand dieser Standards können Unternehmen, bzw. Netzwerkbetreiber, Netzwerksicherheitsunternehmen und Netzwerksicherheitsdienstanbieter, alle Schritte des MLPS umsetzen. Das MLPS bewertet vor allem die technischen Aspekte der Netzwerksicherheit sowie das Sicherheitsmanagement, beispielsweise die Verwaltung des Sicherheitspersonals, interne Richtlinien und Verfahren sowie die Einrichtung und Wartung des Systems.



Das MLPS 2.0 unterscheidet 5 Sicherheitsstufen für IT-Systeme, von Risiko-Level 1, gering, bis Risiko-Level 5, sehr hoch. Unternehmen müssen auf Basis des festgelegten Anforderungskataloges in einem ersten Schritt eine ungefähre Einschätzung des Risiko-Levels ihrer genutzten IT Systeme durchführen. Diejenigen IT-Systeme eines Unternehmens, die in dieser Voreinschätzung eine Klassifizierung der Stufe 2 oder höher erreichen, müssen durch einen qualifizierten und zertifizierten Experten überprüft und das Risiko-Level verifiziert werden. Die Sicherheitsstufen der einzelnen IT-Systeme müssen dann bei der Behörde für öffentliche Sicherheit hinterlegt werden.

Als nächster Schritt ist es notwendig die Kataloge der Anforderungen an die Sicherheit von IT-Systemen in bestimmten Risiko-Leveln durchzugehen und zu identifizieren, ob die IT-Systeme dem geforderten Sicherheitsniveau bereits entsprechen oder ob Anpassungen vorgenommen werden müssen. Allein in den *Grundlegenden Anforderungen für den mehrstufigen Schutz der Cybersicherheit* werden für Systeme der Stufe 2 ca. 200 Anforderungen, für Systeme der Stufe 3 ca. 310 und für Systeme der Stufe 4 ca. 340 Anforderungen aufgelistet.

8.1.4.8	Requirements: GB / T 22239-2019	Evaluation: GB / T 28448-2019
8.1.4.8.a	应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据，重要业务数据和重要个人信息等 Cryptographic techniques should be used to ensure the confidentiality of important data during transmission, including but not limited to identification data, important business data and important personal information.	测评对象:业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 测评实施包括以下内容: 1) 应核查系统设计文档,鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性 2) 应通过嗅探等方式抓取传输过程中的数据包,鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理 Object of evaluation: business applications, database management systems, middleware and system management software and system design documentation Evaluation implentation include: 1) Verification of system design documents, identification of data, important business data and important personal information, and whether cryptography is used to ensure confidentiality during transmission 2) Capturing packets in transit by sniffing and other methods to identify whether data, important business data and important personal information are encrypted in transit
8.1.4.8.b	应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据，重要业务数据和重要个人信息等 Cryptographic techniques should be used to ensure the confidentiality of important data during storage, including but not limited to identification data, important business data and important personal information.	测评对象:业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备中的重要配置数据 测评实施包括以下内容: 1) 应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 应核查是否采用技术措施(如数据安全保护系统等)保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 3) 应测试验证是否对指定的数据进行加密处理 Object of evaluation: business applications, database management systems, middleware and system management software and system design documentation, data security protection system, operating systems in devices such as terminals and servers, critical configuration data in network devices and security appliances Evaluation implementation include: 1) It shall be verified whether cryptography is used to ensure confidentiality of identification data, important business data and important personal information during storage 2) It should be verified that technical measures (such as data security protection systems) are used to ensure the confidentiality of identification data, important business data and important personal information during storage 3) It should be tested to verify whether the specified data are encrypted

Beispiel für Anforderungen und Bewertungen

Nach der Anpassung der Systeme wird überprüft, ob die Sicherheit des Systems nun gegeben ist. Dies geschieht durch externe, staatlich zertifizierte Dienstleister. In einem letzten Schritt wird eine behördliche Inspektion durchgeführt. Die Behörde für öffentliche Sicherheit kann grundsätzlich jederzeit Inspektionen durchführen, wird aber zumindest einmal, bevor sie bestätigt, dass die IT-Systeme sicher sind, eine Überprüfung der Systeme vornehmen, bei der sie Zugang zu den Netzwerken der Unternehmen benötigt und potentiell Zugriff auf vertrauliche Daten und Informationen erlangen könnte.

Je nach Risiko Level der IT-Systeme ist eine derartige Inspektion nicht nur einmalig, sondern regelmäßig notwendig.

5 Schritte der Umsetzung des MLPS

Wir empfehlen allen in China tätigen Unternehmen dringend, die Umsetzung des MLPS 2.0 zügig anzugehen – auch wenn sie einen erheblichen Aufwand an Zeit, Geld und Personalressourcen erfordert. Die Durchsetzung des Systems durch die chinesische Regierung nimmt Fahrt auf. Wer die Vorgaben des MLPS nicht erfüllt, dem drohen empfindliche Strafen. Dazu gehören nicht nur hohe Geldbußen, sondern auch eine Schwarzlistung im *Corporate Social Credit System*.

Exkurs: Internationale Kooperation

Der chinesische Staat wird die Cyber-Kriminalität und den Diebstahl von Geschäftsgeheimnissen über das Internet zukünftig auch verstärkt in Kooperation mit anderen Ländern verfolgen. Dazu hat das Ministerium für öffentliche Sicherheit im Juli 2019 eine Operation namens Cloud Sword ins Leben gerufen, die sich auf die internationale Zusammenarbeit bei der Bekämpfung der transnationalen Cyberkriminalität konzentriert.

Das neue Programm zeigte schnell Ergebnisse. Im Dezember 2019 hat die nepalesische Polizei 122 chinesische Bürger verhaftet, die im Verdacht stehen, am grenzüberschreitenden Cyber-Betrug beteiligt zu sein. An diesem Fall war neben der chinesischen auch die Polizei in Nigeria beteiligt. Schon im Oktober 2019 verhaftete die mongolischen Strafverfolgungsbehörden in vier Hotels in Ulaanbaatar 790 chinesische Bürger, die des Betrugs an Telekommunikationsnetzen verdächtigt wurden, und beschlagnahmten gleichzeitig fast 1.000 Computer, Tausende von Mobiltelefonen und andere Hilfsmittel. 759 Verdächtige wurden nach China zurückgeschickt. I

In Europa hat das chinesische Ministerium für öffentliche Sicherheit in Zusammenarbeit mit der spanischen Polizei 229 chinesische Personen, die des Telekommunikationsbetrugs verdächtig sind, verhaften und nach China zurückführen lassen. Auf der Agenda des Ministeriums ganz oben steht auch die internationale Verfolgung des Diebstahls von Geschäftsgeheimnissen (Trade Secrets) durch Cyberspionage. Im Visier der Angreifer stehen nicht nur technische Daten, sondern auch geschäftliche Listen von Kunden und Zulieferern. Das Programm zeigt, dass sich China auch in der Strafverfolgung entkoppelt und eigene Wege geht.

Encryption Law

Seit dem 1. Januar 2021 ist das chinesische *Kryptographie Gesetz (KG)* in Kraft. Es soll die Nutzung und Verwaltung von Verschlüsselungstechnologien regeln und die Entwicklung der Kryptographie Branche erleichtern. Zum Gesetz gehört eine Liste an kommerziellen Verschlüsselungstechnologien, für die besondere Vorschriften beim Import oder Export nach/aus China gelten, die ebenfalls seit dem 1. Januar 2021 gültig ist.

Das Gesetz unterscheidet zwischen Kern-, Standard- und kommerzieller Kryptographie. Da Kern- und Standard-Kryptographie zum Schutz von Staatsgeheimnissen verwendet werden, sind sie für die meisten ausländischen Unternehmen in China nicht relevant. Die kommerzielle Kryptographie kann von Bürgern, juristischen Personen und Organisationen genutzt werden, um ihre Daten und Systeme zu schützen.

Neu ist, dass das *KG* die Verwendung ausländischer Verschlüsselungstechnologien in China für den kommerziellen Gebrauch nicht ausdrücklich verbietet. Bereits 2017 hat die chinesische Regierung beschlossen, einige Einschränkungen, denen ausländische Unternehmen im Bereich Verschlüsselungstechnologie unterliegen, abzuschaffen. So beispielsweise die Notwendigkeit für ausländisch investierte Unternehmen, Genehmigungen einzuholen, wenn außerhalb Chinas produzierte Verschlüsselungstechnologie oder Ausrüstung, die Verschlüsselungstechnologie enthält, in China eingesetzt wird. Dies Beschlüsse wurden auf Gesetzesebene mit dem *KG* umgesetzt.

Ende 2019 wurde des Weiteren das bis dahin bestehende Zertifizierungssystem für Verschlüsselungstechnologien gelockert, d.h. es müssen nur noch kommerzielle Verschlüsselungsprodukte zertifiziert werden, die auf der Liste kritischer Netzwerkausrüstung und dezidierter Cybersicherheitsprodukte stehen.

Kommerzielle kryptographische Produkte oder Technologien, die von ausländischen Unternehmen entwickelt, verwendet, verkauft, importiert oder exportiert werden, werden jetzt genauso behandelt wie einheimische Produkte oder Technologien. Für den Import von Kryptographie-Produkten, es sei denn es handelt sich um öffentlich zugängliche Konsumprodukte, ist jedoch nach wie vor eine Importlizenz notwendig, bei der genau angegeben werden muss, wer das Produkt benutzen wird und zu welchem Zweck.

Kryptographische Produkte, die in China verkauft und verwendet werden, müssen einem strengen Normenwerk entsprechen, das durch weitere Vorschriften näher definiert werden wird. Auch für den Export von kryptographischen Produkten muss momentan noch eine Lizenz beantragt werden. Das soll jedoch bald durch ein umfassendes Import-Lizenz- und Export-Kontrollen-System nach internationaler Praxis ersetzt werden.

Alle Unternehmen, die kommerzielle Kryptographie zum Schutz ihrer Daten einsetzen, unterliegen der Überwachung und Bewertung durch die *State Cryptography Administration (SCA)*, die das Recht hat zu prüfen, ob Kryptographie-Produkte und -Technologien gesetzeskonform eingesetzt werden. Das *KG* bezieht sich jedoch in Art. 26 auch direkt auf das *CSL*: Die Sicherheitstests und die Zertifizierung von kommerzieller Verschlüsselungs-Technologie unterliegen den Vorschriften des *CSL* und sollen nach den Vorgaben des MLPS ausgerichtet werden, um wiederholte Tests und Überprüfungen zu vermeiden.

Data Security Law (DSL)

Der nationale Volkskongress hat im Juli 2020 den Entwurf für das neue *Data Security Law* (DSL) vorgestellt. Inzwischen ist das Gesetz bereits seit dem 1. September 2021 in Kraft. Ziel des Gesetzes ist nicht allein der Schutz von Daten, sondern vor allem die Förderung von Dateninfrastruktur und innovativer Nutzung von Daten durch die Industrie, sowie die Entwicklung der digitalen Wirtschaft. Die Regierungen der Provinzen werden angehalten Pläne für die Weiterentwicklung der digitalen Wirtschaft zu formulieren. Grundlage für eine funktionierende, sichere digitale Wirtschaft ist sowohl Cybersicherheit, als auch Datensicherheit.

Das Gesetz stellt ein System zur Klassifizierung von Daten vor: bewertet wird, wie relevant diese Daten für die Wirtschaft und die gesellschaftliche Entwicklung sind, und wie groß der Schaden wäre, wenn diese Daten missbraucht würden. Die Kompetenz zu entscheiden, was sogenannte „wichtige Daten" sind, wird an regionale Regierungen und für bestimmte Industrien verantwortliche Gremien abgegeben, die entsprechende Kataloge veröffentlichen sollen. Das bedeutet, dass Unternehmen in Zukunft möglicherweise auf regionaler Basis überprüfen müssen, ob die in der jeweiligen Region verarbeiteten Daten der dort gültigen Definition von „wichtigen Daten" entsprechen.

Das Gesetz spricht immer wieder von zentralisierten Mechanismen, Systemen und zertifizierten Dienstleistungen für Datensicherheitsbewertungen, Datentransaktionsmanagement, Datensicherheitsnotfall-Management, deren Einrichtung dem Staat obliegt. Die Details zu derartigen Systemen sind momentan noch nicht klar, und werden sich jetzt – nach dem in Kraft treten des Gesetzes - in weiteren Verordnungen und Standards herauskristallisieren.

Das *DSL* sieht vor, dass datenverarbeitende Unternehmen verpflichtet sind ein Datensicherheits-Managementsystem einzurichten und regelmäßig an die geltenden Vorschriften anzupassen. Dieses System soll technische und operative Maßnahmen beinhalten, um die Datensicherheit zu gewährleisten. Unternehmen, die sogenannte „wichtige Daten" verarbeiten, sollen verpflichtet werden einen Datenschutzverantwortlichen zu ernennen und regelmäßige Datenschutz-Folgeabschätzungen der Verarbeitungsaktivitäten durchzuführen, deren Ergebnis an die verantwortliche Behörde gemeldet werden muss.

Grundsätzlich soll jede Art der Datensammlung oder Datenverarbeitung legal und mit legalen Methoden erfolgen. Alle Gesetze und Vorschriften, die Regelungen zu Zweck und Umfang von Datensammlung und -verarbeitung enthalten, müssen beachtet werden. Organisationen oder Unternehmen, die Datensätze verkaufen, sollen verpflichtet werden zu verifizieren, woher die Daten kommen und müssen die Überprüfung, sowie alle Transaktionen dokumentieren. Anbieter von online Datenverarbeitung sollen eine spezielle Gewerbeerlaubnis beantragen müssen.

Bemerkenswert ist, dass laut auch Organisationen und Personen außerhalb Chinas rechtliche Verpflichtungen haben, sobald sie an China-bezogenen Datenaktivitäten beteiligt sind, sollten diese die nationale Sicherheit, das öffentliche Interesse oder andere legale Interessen chinesischer Bürger oder Organisationen verletzen. Ein Standort außerhalb Chinas bedeutet dementsprechend nicht unbedingt Sicherheit vor dem langen Arm des chinesischen *DSL*.

Im Gesetz werden einige Prinzipien zum Cross-Border Transfer von Daten formuliert. In Art. 11 *DSL* heißt es: „Der Staat führt aktiv internationalen Austausch und Zusammenarbeit im Bereich Daten

durch, beteiligt sich an der Formulierung internationaler Regeln und Standards für die Datensicherheit und fördert den sicheren und freien grenzüberschreitenden Datenfluss“. Dennoch beinhaltet das Gesetz auch Regelungen, die den freien Datenfluss unter bestimmten Umständen einschränken, so beispielsweise, wenn es sich um Daten handelt, die sich auf kontrollierte Gegenstände beziehen, die mit der Erfüllung internationaler Verpflichtungen und der Wahrung der nationalen Sicherheit zusammenhängen. Eine konkrete Liste dieser Daten-Typen gibt es bisher jedoch nicht. Hier liegt auch ein Hinweis auf das neue Exportkontrollgesetz (*Export Control Law),* das nicht nur auf Produkte und Dienstleistungen, sondern auch auf in ihnen enthaltene Daten und auf Know-how zielt.

Weitere Vorschriften zur Datenübertragung nach außerhalb Chinas finden sich in den *Administrative Measures on Data Security (Draft for Comment)*, den *Measures for the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft for Comment)* und *Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment).*

Während in dem Entwurf der *Administrative Measures on Data Security (Draft for Comment)* vorgesehen ist, dass Netzwerkbetreiber, bevor sie „wichtige Daten“ ins Ausland übertragen, eine Risikobewertung durchführen, diese der verantwortlichen Behörde vorlegen und dann eine Genehmigung erhalten muss, regeln die *Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment),* dass Netzwerkbetreiber auch bei der Übermittlung von personenbezogenen Daten erst eine Sicherheitsüberprüfung und Genehmigung durch die Cyberspace Behörde durchlaufen müssen, bevor die Daten übertragen werden dürfen.

Weitere Voraussetzungen für den Transfer soll beispielsweise ein Vertrag mit dem Empfänger der Daten sein, der ein gleich hohes Datenschutzniveau beim Empfänger vorschreibt und die Verantwortlichkeit für die Datensicherheit festlegt. Jährliche Berichte an die verantwortliche Behörde durch den Netzwerkbetreiber sollen den Behörden ermöglichen, einen Überblick über „exportierte“ Daten zu behalten. Des Weiteren sollen ausländische Organisationen, die in China Daten sammeln, in China einen rechtlichen Vertreter benennen müssen, der für die Einhaltung der Datenschutzvorschriften in China zuständig ist.

Die *Measures for the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft for Comment)* gibt weitere Details zu der Durchführung von Sicherheitsbewertungen vor dem Transfer von Daten ins Ausland und beinhaltet gleichzeitig die Liste von Beispielen „wichtiger Daten“ (siehe Kapitel zu *CSL* Datenschutz) in verschiedenen Industrien.

Relevanter als das *DSL* in Hinsicht auf Vorschriften zum Schutz von personenbezogenen Daten ist der das *Gesetzes zum Schutz personenbezogener Daten*, auf das im folgenden Kapitel eingegangen wird.

Exkurs: Unlauterer Wettbewerb mit Datenrechten

In China wurde jüngst die erste Entscheidung zum *unlauteren Wettbewerb mit Datenrechten* an Internet-Plattformen veröffentlicht. Der Hintergrund: Tencent, der König der sozialen Medien, verfügt über die Daten und eingeschränkte Datenrechte der täglich rund 900 Millionen Nutzern der App

WeChat. Es ist bekannt, daß Tencent einen Großteil dieser Daten mit der chinesischen Regierung teilt. Dennoch hat der Konzern gegen zwei kooperierende chinesische Technologieunternehmen wegen unlauteren Wettbewerbs geklagt.

Die beklagten Unternehmen bieten eine Social Media Management Software an, die mit den Funktionen der App WeChat interagiert. Nutzer können mit dieser Software ursprüngliche WeChat Funktionen wie Beiträge „liken“ oder „teilen“ individuell automatisieren und verbessern. Auch erweiternde Zusatzfunktionen wie etwa das Löschen von Spam-Anfragen oder unechte Accounts sind mit dieser Software möglich. Da die Software die Konto- und Nutzerinformationen sowie soziale Beziehungen erfasst und überwacht und diese auf dem Server eines der beklagten Unternehmen speichert, gilt die Software als rechtsverletzend. Das Internet-Gericht in Hangzhou hat in erster Instanz zugunsten des WeChat-Eigentümers Tencent entschieden. Die beklagten Unternehmen müssen Schadensersatz in Höhe von CNY 2.6 Millionen (ca. 319.000 EUR) bezahlen und Maßnahme treffen, die den entstandenen Schäden entgegenwirken. Dieser Fall ist ein klares Beispiel dafür, daß der Schutz vor unlauterem Wettbewerb in China auch in Bezug auf Daten relevant ist.

Personal Information Protection Law (PIPL)

Am 21. Oktober 2020 wurde der erste Entwurf des *Personal Information Protection Law* (PIPL) veröffentlicht. Nun wird es am 1. November 2021 in Kraft treten. Das Gesetz soll den Schutz personenbezogener Daten zusammen mit dem *CSL* und dem *DSL* stärken.

Ausländische Unternehmen müssen besonders die extraterritorialen Auswirkungen dieses Gesetzes und die Regelungen zum grenzüberschreitenden Transfer personenbezogener Daten beachten. Genau wie das Niederlassungskriterium und das Zielgebietskriterium der europäischen Datenschutz Grundverordnung (DSGVO) soll das *PIPL* nach in Kraft treten nicht nur für den Umgang mit personenbezogenen Daten innerhalb Chinas, sondern auch für Aktivitäten außerhalb das Landes gelten, wenn ein Unternehmen personenbezogene Daten zum Zweck der Bereitstellung von Produkten oder Dienstleistungen für Personen in China oder zur Analyse und Bewertung der Aktivitäten von Personen in China verarbeitet. Ein weiteres Risiko stellt Art. 42 *PIPL* dar: ausländische Unternehmen, deren Verarbeitung von personenbezogenen Daten außerhalb von China tatsächlich oder vermeintlich die Interessen von chinesischen Bürgern verletzt oder sogar die nationale Sicherheit Chinas gefährdet, können auf eine schwarze Liste gesetzt werden – mit der Konsequenz, dass die Bereitstellung von Daten an diese Unternehmen eingeschränkt oder komplett verboten wird.

Das Gesetz beinhaltet grundsätzliche Prinzipien der Verarbeitung von personenbezogenen Daten. So dürfen Daten nur mit legalen Methoden verarbeitet werden. Sie dürfen nur in dem Maße gesammelt werden, wie es für den Zweck der Verarbeitung notwendig ist, und die Verarbeitung muss offen und transparent sein. Das Datensubjekt muss über die Art und den Umfang der Datenverarbeitung informiert sein und ebenfalls darüber, wer die Daten zu welchem Zweck verarbeitet. Die verarbeiteten personenbezogenen Daten sollen richtig sein und wenn notwendig zeitnah aktualisiert werden. Der Daten-Verarbeiter trägt die Verantwortung für die Verarbeitung und soll entsprechende Sicherheitsmaßnahmen zum Schutz der Daten ergreifen. Nach Erfüllung des Zwecks, für den die personenbezogenen Daten gesammelt wurden, müssen sie zeitnah gelöscht werden. Mit wenigen Ausnahmen muss die Grundlage für die Verarbeitung von personenbezogenen Daten das informierte und freiwillige Einverständnis des Datensubjekts sein. Vielen Vorschriften der Sammlung und der Verarbeitung personenbezogener Daten ähneln stark den Vorgaben der Datenschutz-Grundverordnung (DSGVO), beispielsweise zu den Themen Datenspeicherung und Datenauftragsverarbeitung.

Ähnlich wie die DSGVO unterscheidet auch das *PIPL* zwischen personenbezogenen Daten und sensiblen personenbezogenen Daten. Diese dürfen nach dem *PIPL* nur für bestimmte Zwecke und nur wenn es notwendig ist verarbeitet werden. Die Definition sensibler personenbezogener Daten wird im *PIPL* im Vergleich zur *Personal Information Security Specification* etwas erweitert. Aufgezählt werden nun beispielsweise auch Rasse, Ethnie und Glaubensrichtung. Für die Verarbeitung sensibler personenbezogener Daten ist eine separate Einverständniserklärung des Betroffenen notwendig.

Das *PIPL* sieht außerdem standardmäßig Datenlokalisierungsanforderungen für Betreiber kritischer Informationsinfrastruktur vor sowie für Verarbeiter personenbezogener Daten, wenn die Menge der von ihnen verarbeiteten Daten einen bestimmten von der Cyberspace Administration festgelegten Schwellenwert überschreitet. Wenn die Notwendigkeit besteht, diese Daten ausländischen Organi-

sationen zur Verfügung zu stellen, ist es notwendig das ausdrückliche Einverständnis des Datensubjekts einzuholen und zuvor eine Sicherheitsüberprüfung durch die Cyberspace Verwaltung durchführen zu lassen.

Überschreitet die Menge der verarbeiteten Daten eines Unternehmens nicht die vorgegebene Grenze, so ist es dennoch vorgesehen, dass vor der Bereitstellung im Ausland eine Datenschutz-Folgenabschätzung durchgeführt und die folgende Verarbeitung der Daten dokumentiert werden muss. Die Folgenabschätzung muss eine Überprüfung der Legitimität, Berechtigung und Notwendigkeit des Zwecks und der Methoden der Datenverarbeitung beinhalten. Außerdem muss das Risiko einer Datenschutzverletzung, sowie die Angemessenheit der ergriffenen Schutzmaßnahmen bewertet werden. Es soll außerdem eine Zertifizierung für den Schutz von personenbezogenen Daten durch spezialisierte Organisationen durchgeführt werden oder ein Auftragsverarbeitungsvertrag mit der Partei, der die Daten bereitgestellt werden, geschlossen werden, der ein entsprechendes Datenschutzniveau beim Datenempfänger garantieren soll.

Nach in Kraft treten des *PIPL* wird es für alle Unternehmen verpflichtend sein, vor dem Bereitstellen von „wichtigen“ oder personenbezogenen Daten im Ausland in China entweder eine Selbstprüfung durchzuführen, eine Überprüfung durch die Behörden zu durchlaufen oder sogar eine behördliche Genehmigung zu beantragen.

Exkurs: National Security Law

Auch das im Juni 2020 in Kraft getretene Gesetz zur Gewährleistung der nationalen Sicherheit in der Sonderverwaltungszone Hongkong *(National Security Law, NSL)* hat Auswirkungen auf in Hongkong tätige Unternehmen bezüglich Technologie und Daten. So müssen Internetanbieter den Behörden jetzt Zugang zu Nutzerdaten gewähren und ihre grenzüberschreitenden Datenflüsse überprüfen. Technologieunternehmen müssen ihre Geschäftstätigkeit neu strukturieren, wenn bei sensiblen Technologien westliche Exportverbote greifen.

Mit der Aussetzung des United States – Hongkong Policy Act entfällt die Vorzugsbehandlung der USA bei Lizenzen, dem Export und dem Transfer sensibler Technologieprodukte. Infolge der Aussetzung werden nun alle Exporte, Reexporte und Transfers solcher Produkte nach Hongkong als für die VR China bestimmte Güter behandelt, und US-Unternehmen dürfen keine sensiblen Technologieprodukte nach Hongkong verkaufen. Die EU wird ähnlich reagieren, ein erstes Dokument zur Einführung von Beschränkungen wurde bereits veröffentlicht.

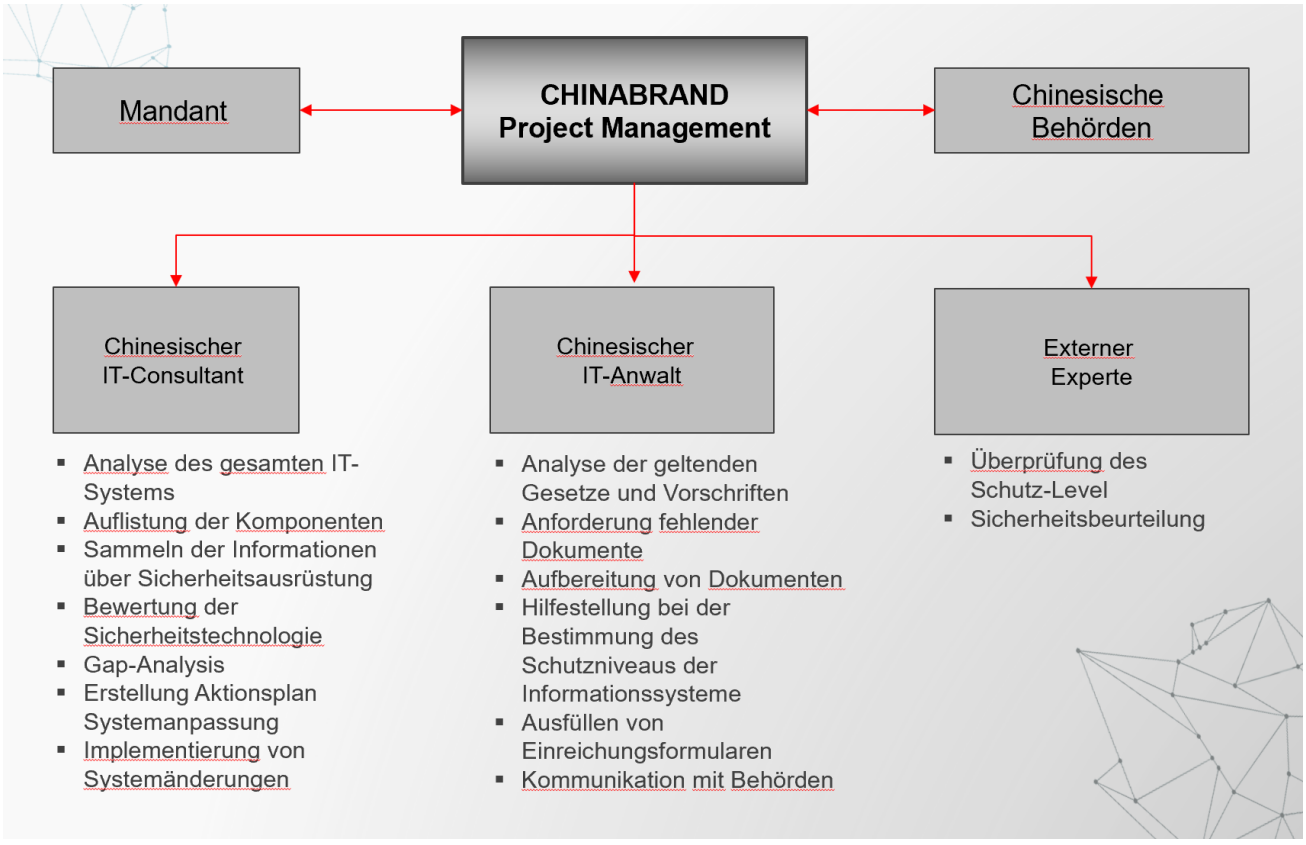
Die verschärften Exportbeschränkungen haben Auswirkungen auf Unternehmen, die sensible und hochtechnologische Produkte nicht mehr nach Hongkong versenden oder dort empfangen können. Dementsprechend sollten Lieferverträge und Compliance-Richtlinien überprüft und angepaßt sowie Kooperationen mit chinesischen Technologieanbietern und alternative Technologien in Betracht gezogen werden.

Handlungsempfehlungen

Die fortlaufende Verabschiedung neuer Gesetze zeigt die Entschlossenheit Chinas, den Schutz von Daten und die Cybersicherheit im Allgemeinen zu verstärken. Das bringt für die in China tätigen ausländischen Unternehmen zusätzliche Herausforderungen mit sich. Durch ständig neue Vorschriften werden sie gezwungen, die chinesische Gesetzgebung ständig zu überwachen und ihre Compliance-Strategien anzupassen.

Konkret sollten Unternehmen jetzt die folgenden Maßnahmen ergreifen:

CSL/ MLPS: Das *Multi-Level-Protection-Scheme* wird in China mit Nachdruck durchgesetzt. Jedes Unternehmen sollte überprüfen, welche IT-Systeme beurteilt und registriert werden müssen. Hierbei sollten erfahrene Berater hinzugezogen werden, um Fehler zu vermeiden. Nachdem festgestellt wurde, welche der IT-Systeme geprüft und registriert werden müssen, sollte zeitnah beurteilt werden, welches Risiko-Level diese Systeme haben. Nachdem der Risiko-Level bestätigt und beim regionalen Büro für öffentliche Sicherheit hinterlegt wurde, müssen die gesetzlichen Anforderung an IT-Systeme der ermittelten Risikostufen gesammelt, mit den vorhandenen Sicherheitsmaßnahmen abgeglichen und die Systeme dem entsprechend an die gesetzlichen Vorgaben angepasst werden.



CSL, DSL und PIPL: Westliche Unternehmen, die in und mit China wirtschaften, sollten ihre aktuelle Situation und die künftig zu erwartenden Anforderungen des CSL, DSL und des PIPL genau analysieren. Die der europäischen DSGVO ähnlichen Anforderungen umfassen unter anderem die Ernennung einer für die Sicherheit verantwortlichen Abteilung, die Risikoüberwachung, Analysen der Datenauswirkung sowie die Berichtserstattung bei den Behörden.

Unternehmen, die bereits Bemühungen für die Umsetzung von Konzepten gemäß der DSGVO getroffen haben, sind hier im Vorteil, wobei die Anforderungen des chinesischen DSL teilweise von denen der DSGVO abweichen, weswegen eine genaue Überprüfung der Vorschriften dennoch notwendig ist. Neben der Prüfung und Einhaltung der Standards sollten weitere strategische Entscheidungen zu den Datenaktivitäten in und mit China gefällt werden.

Des Weiteren sollten westliche Unternehmen die weiteren Entwicklungen der Anforderungen zu Datenlokalisierung und Datentransfer beobachten und frühzeitig beginnen zu prüfen, ob die Compliance mit den Vorschriften möglich ist oder ob Compliance-Systeme und Datenflüsse angepasst werden müssen.

NSL: In Hongkong tätige Unternehmen sollten ihre Situation evaluieren und einen Handlungsplan aufstellen, der für den Fall einer Überprüfung den Umgang mit den Behörden regelt. Wir empfehlen darüber hinaus, die eigene Lieferketten nach neuen Risiken im Zusammenhang mit dem NSL zu bewerten und den Datenaustausch ggf. vom globalen Netzwerk abzukoppeln. Das gilt auch für bilaterale Abkommen Hongkongs, die bisher den freien grenzüberschreitenden Datenfluss zwischen den Vertragspartnern zugelassen haben. Hier sollten die Risiken neu bewertet und bestehende Geschäftsverträge überprüft und angepaßt werden.

Weitere Informationen

Die Autoren dieses Whitepaper:

Dr. Hans Joachim Fuchs
Geschäftsführer
CHINABRAND IP CONSULTING GMBH
+49 89 321 212 8016
drhjfuchs@chinabrand.de

Mareike Seeßelberg, LL.M.
Senior Consultant
CHINABRAND IP CONSULTING GMBH
+49 89 321 212 8015
mseesselberg@chinabrand.de

Zihao Liao, LL.M.
Consultant
CHINABRAND IP CONSULTING GMBH
+49 89 321 212 8013
zliao@chinabrand.de

Weitere Informationen über unsere Dienstleistungen finden Sie hier:

www.chinabrand.de

Kontakt und Feedback

Blog | LinkedIn | XING

CHINABRAND IP CONSULTING GMBH
Mareike Seeßelberg
Grashofstraße 3, 80995 München
info@chinabrand.de
www.chinabrand.de
+49 89 321 212 800