Thomas Weidlich, Dr. Yuan Shen

Netzwerksicherheit in China und grenzüberschreitender Datenaustausch

Rechtliche Herausforderungen und Handlungsempfehlungen

Durch die globale Vernetzung ist die Netzwerksicherheit weltweit von immenser Bedeutung. Besonders in Unternehmen spielt die Netzwerksicherheit aufgrund der zunehmenden Digitalisierung und Automatisierung eine immer größere Rolle. Die Infrastruktur von Unternehmen wird stetig komplizierter und die regulatorischen Anforderungen an die Netzwerksicherheit und den Datentransfer steigen. In Deutschland steht das Thema durch den Erlass des IT-Sicherheitsgesetzes, der EU-Richtlinie zur Netz- und Informationssicherheit (NIS-Direktive) und der EU-Datenschutzgrundverordnung (DSGVO) im Fokus einer breiten Öffentlichkeit. China reagierte mit dem Erlass eines umfassenden Netzwerksicherheitsgesetzes auf die wachsende Bedrohung, die von der Informationstechnik und dem Internet ausgeht und stellt damit in China tätige Unternehmen vor eine besondere Herausforderung.

Am 1. Juni 2017 trat das neue chinesische Netzwerksicherheitsgesetz (auch als „Cybersecurity Law“ bekannt, „CSL“) in Kraft. Zur Umsetzung des CSL hat China seitdem eine Vielzahl von Ausführungsbestimmungen und technischen Normen erlassen, darunter auch einen Entwurf über den grenzüberschreitenden Datentransfer („Measures for the security assessment of personal information and important data to be transmitted abroad“, „Measures for PI and ID Transfer“) und die technischen Normen „Personal Information Security Specification (GB/T 35273-2017)“ („Specification for PI Security“). Die im Mai 2018 erlassene Specification for PI Security dient als Ergänzung zum Datenschutz und regelt insbesondere die Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten. Zusammen mit anderen Ausführungsbestimmungen und technischen Normen ist die Umsetzung des CSL eine große Herausforderung für die IT-Infrastruktur und Compliance ausländischer Unternehmen mit Niederlassungen in China, deren tägliches Geschäft auf grenzüberschreitenden Datenverkehr angewiesen ist.

1. Rechtsentwicklung von Netzwerksicherheit und Datenschutz in China seit 2016

Die seit 2016 neu verabschiedeten über 40 Gesetze, Ausführungsbestimmungen und technischen Normen zeugen von der überragenden Bedeutung der Netzwerksicherheit für sämtliche Wirtschafts- und Lebensbereiche in China. Tabelle 1 fasst die wichtigsten bisher erlassenen Vorschriften und Entwürfe im Bereich Netzwerksicherheit und Datenschutz zusammen. Dabei gilt es zu beachten, dass technische Normen zwar lediglich eine Empfehlung darstellen und keine Gesetzesbindungskraft haben, in der Praxis aber dennoch bedeutsam sind. Denn bei fehlenden Ausführungsbestimmungen zum Netzwerksicherheitsgesetz können sich Unternehmen und Behörden an den technischen Normen als Leitfaden orientieren. Unternehmen können auf diese Weise bereits „Good Practice“ im Betrieb etablieren.

2. Anforderungen an Netzwerkbetreiber

Das relativ kompakte CSL ist ein klassisches chinesisches Rahmengesetz, das verschiedene Grundprinzipien formuliert, Grundbegriffe festlegt und an vielen Stellen auf Ausführungsbestimmungen der zuständigen staatlichen Organe verweist. Es ist damit zum einen die Grundlage für weitere Regulierungstätigkeit verschiedener Stellen, zum anderen stellt es die Klammer für einige bereits bestehende Regelungen dar, vor allem im Bereich der Informationssicherheits-Managementsysteme (ISMS).

Nationale Strategien (2)	National Strategy for Cyberspace Security
	Strategy for International Cooperation in Cyberspace
Gesetze und gerichtliche Auslegungen (4)	General Rules of the Civil Law
	Interpretation of Several Issues regarding Application of Law to Criminal Cases of Infringement of Citizen's Personal Information ("PI") Handled by the Supreme People's Court and the Supreme People's Procuratorate
	Cybersecurity Law
	E-Commerce Law
Ausführungsbestimmungen (14)	Regulations on Security Protection of Critical Information Infrastructure ("CII") *(draft)*
	Measures for the Security Assessment of PI and Important Data to be Transmitted Abroad *(draft)*
	Administrative Measures for Content Management Practitioners in Entities Offering Internet News Information Services
	Administrative Provisions on Evaluating the Safety of New Technologies and Applications for Internet News Information Services
	Implementing Rules for the Administration of the Licensing for Internet News Information Services
	Provisions on the Administrative Law Enforcement Procedures for Internet Information Content Management
	Measures for Examining the Security of Network Products and Services (for trial implementation)
	Catalog of Key Network Equipment and Specific Network Safety Products (Batch One)
Technische Normen (20)	Specification for PI Security
	Guidance on De-identification of PI *(draft)*
	Guidance on Examination and Assessment of the Security of CII *(draft)*
	Evaluation Index System for Security of CII *(draft)*
	General Requirements for the Security of Network Products and Services *(draft)*
	Guidance on Examination and Assessment Process of Graded Protection of Cybersecurity *(draft)*
	Requirements for Examination and Assessment of Graded Protection of Cybersecurity (for each part) *(draft)*
	Guidance on Security Assessment of Data to be Transmitted Abroad *(draft)*

Tabelle 1: Übersicht der wichtigsten Vorschriften und Entwürfe im Bereich Netzwerksicherheit und Datenschutz

Sicherheits- und Schutzpflichten	Prävention und Reaktion	Schutz personenbezogener Daten	Beschwerde- und Berichtssystem
• Einrichtung eines Informationssicherheits-Managementsystems • Ernennung von Internetsicherheits-Verantwortlichen • Überwachung und Aufzeichnung von Sicherheitsvorfällen und Vorbeugung gegen Sicherheitsvorfälle • Einstufung von Daten sowie Sicherung und Verschlüsselung wichtiger Daten • Datenspeicherung für mindestens 6 Monate	• Erstellen eines Notfallschutzplanes • Schnelle Reaktionen • Unverzügliche Auslösung des Notfallschutzplans • Berichterstattung	• Strenge Geheimhaltung • Einrichtung eines Nutzerinformationen-Schutzsystems • Gesetzeskonforme Datenerhebung und -verwendung mit Zustimmung von Nutzern • Verwirklichung von technischen Schutzmaßnahmen • Unverzügliche Abhilfemaßnahmen	• Einrichtung eines Beschwerde- und Berichtssystems • Veröffentlichung der Informationen • Zusammenwirkung mit zuständigen Behörden

Tabelle 2: Übersicht von durch das CSL vorgegebenen Maßnahmen zum Schutz von Netzwerken

Das CSL unterscheidet zwischen den „einfachen" Netzwerkbetreibern und den Betreibern kritischer Informations-Infrastruktur (KRITIS). Netzwerkbetreiber ist jedes Unternehmen oder jede Organisation, die einen Server betreibt, der mit dem Internet verbunden ist. Strenggenommen reicht schon ein einzelner Computer mit Internetzugang. Die Definition für Betreiber kritischer Informations-Infrastrukturen ähnelt der des deutschen IT-Sicherheitsgesetzes. Kritische Informationsinfrastrukturen umfassen Geltungsbereiche, wie z. B. Radio, Fernsehen, die Energie- und Finanzwirtschaft oder den Verkehrs- und Wasserschutz, aus denen bei einer möglichen Beschädigung der Netzwerksysteme ernsthafte Bedrohungen für die nationale Sicherheit des Landes, die nationale Wirtschaft oder die Lebensgrundlage der Bevölkerung resultieren können.

(1) Verpflichtungen der „einfachen" Netzwerkbetreiber

Das CSL verpflichtet sämtliche Netzwerkbetreiber zur Anpassung ihrer Netzwerksysteme, um diese vor Beschädigungen, Störungen, Datendiebstählen oder Hackerangriffen zu schützen. Die Netzwerkbetreiber sind fortan gehalten, bestimmte durch das CSL vorgegebene Maßnahmen zu ergreifen, um den Schutz ihrer Netzwerke zu gewährleisten. Eine Übersicht dieser Maßnahmen ist in Tabelle 2 abgebildet.

(2) Striktere Anforderungen an KRITIS-Betreiber

Das CSL stellt an die KRITIS-Betreiber weitaus striktere Anforderungen als an die „einfachen" Betreiber. Beispielsweise sind erstere nunmehr verpflichtet, eine Abteilung zur Internetsicherheit einzurichten, während der „einfache" Betreiber seiner Verpflichtung bereits durch Stellung eines Internetsicherheits-Verantwortlichen nachkommt. Mit Sicht auf die Angestellten im IT-Bereich in führenden und kritischen Positionen ist der KRITIS-Betreiber gehalten, regelmäßig Sicherheitsüberprüfungen des Hintergrundes der Angestellten durchzuführen sowie regelmäßig Internetsicherheitsausbildungen und technische Trainings durchführen zu lassen. Zudem unterliegen die Betreiber der Verpflichtung, jährlich eine Sicherheitsüberprüfung durchzuführen. Diese können sie entweder selbst oder durch zertifizierte Unternehmen für Cyber-Sicherheitsdienste durchführen lassen. Die Ergebnisse und Verbesserungsmaßnahmen sind sodann an die zuständige Aufsichtsbehörde zu übermitteln.

(3) Das Sicherheitsstufenkonzept zur Einordnung der Betreiber

In Zusammenarbeit mit dem Ministerium für die öffentliche Sicherheit (MPS) hat die Cyberspace Administration of the People's Republic of China (CAC) ein Sicherheitsstufenkonzept zur Einordnung von Netzwerkbetreibern verabschiedet. Danach werden die Betreiber durch eine lizenzierte Bewertungsinstitution in fünf aufsteigende Sicherheitsstufen eingeordnet, abhängig davon, welche Risiken bei einer Störung oder einem Ausfall des jeweiligen Betreibernetzwerks für außenstehende Netzwerknutzer oder die Allgemeinheit bestehen können. Eine Einordnung in Stufe 1 oder 2 erfolgt, wenn Störungen oder Schädigungen des Systems zwar den gesetzlichen Rechten und Interessen von Bürgern, juristischen Personen oder anderen Organisationen schaden können, die nationale Sicherheit jedoch nicht betroffen ist. Eine Einordnung in Stufe 3 oder eine höhere Stufe erfolgt, wenn die nationale Sicherheit bzw. die öffentliche Ordnung beeinträchtigt werden kann. Erfolgt eine Einordnung in Stufe 3 oder eine höhere Stufe, ist in der Regel davon auszugehen, dass man als KRITIS-Betreiber den besonderen Verpflichtungen des CSL unterliegt. Die Zuweisung zu einer Sicherheitsstufe entscheidet letztlich darüber, welche Anforderungen der Netzwerkbetreiber zur Gewährleistung des CSL zu erfüllen hat und welchem Niveau der Überwachung der Netzwerkbetreiber durch die zuständigen Regierungsbehörden unterliegt.

3. Datenschutz und grenzüberschreitender Datenaustausch

Für in China tätige ausländische Unternehmen gilt es, ein besonderes Augenmerk auf die Regularien zur Erhebung, Speicherung, Verarbeitung sowie Übertragung von Daten zu legen. In diesem Kontext kommt vor allem den Begriffen der „personenbezogenen Information" und der „wichtigen Daten" eine besondere Bedeutung zu.

(1) Personenbezogene Informationen und wichtige Daten

Nach dem CSL sind „personenbezogene Informationen" alle Informationen, die in elektronischer oder anderer Form festgehalten sind und dafür genutzt werden können – alleine oder zusammen mit anderen Informationen – die Identität einer natürlichen Person zu bestimmen. Personenbezogene Informationen sind Name, Geburtstag,

Personalausweisnummer, Adresse, Telefonnummer, Korrespondenzprotokoll und -inhalt, Vermögens- und Transaktionsinformationen usw. „Wichtige Daten“ sind nach dem Entwurf der Measures for PI and ID Transfer solche Daten, die einen Bezug zur nationalen Sicherheit, zur wirtschaftlichen Entwicklung und zum sozialen und öffentlichen Interesse haben.

(2) Schutz personenbezogener Informationen

Hinsichtlich des Schutzes personenbezogener Daten wird das CSL durch die technischen Normen der Specification for PI Security ergänzt und konkretisiert. Die Specification for PI Security gilt allerdings nicht nur für Netzwerkbetreiber, auf die das CSL anwendbar ist, sondern auch für Organisationen und Individuen, die bei Offline-Geschäftstätigkeiten personenbezogene Daten erheben und verarbeiten.

Die Specification for PI Security stellt klar, dass der gesetzliche Vertreter für den Datenschutz die umfassende Verantwortung trägt und die erforderlichen Finanzmittel, Personal und Ressourcen sicherzustellen hat. In der Specification for PI Security wird zwischen personenbezogenen Daten und personenbezogenen sensiblen Daten unterschieden. In den Anlagen werden dafür Beispiele aufgeführt. Name, Adresse, Geburtsdatum, gehören z. B. zu den personenbezogenen Daten, während Passwörter, Fingerabdruck oder Personalausweis als personenbezogene sensible Daten einzustufen sind. Bei Letzteren gelten strengere Schutzpflichten, z. B. bei der Einwilligung, bei der Verschlüsselung und Übertragung sowie bei der Kontrolle der Zugangsbefugnisse. Zudem enthält die Specification for PI Security Musterklauseln für Datenschutzerklärungen, die die Anforderungen an Klarheit, Richtigkeit und Vollständigkeit erfüllen.

(3) Datenlokalisierung

Schon seit einigen Jahren besteht die Verpflichtung, dass personenbezogene Informationen, die der Betreiber erhebt oder verarbeitet, in China gespeichert werden müssen und nur mit Zustimmung der betroffenen Person ins Ausland exportiert werden dürfen. Für KRITIS-Betreiber gilt darüber hinaus, dass personenbezogene Informationen und wichtige Daten nur in China gespeichert werden dürfen, unabhängig davon, ob die betroffenen Personen oder Geschäftspartner eingewilligt haben. Der Entwurf der Measures for PI and ID Transfer will diese Pflicht teilweise auch auf Nicht-KRITIS-Betreiber ausdehnen. Allerdings soll es von diesem Grundsatz Ausnahmen geben, wenn der Transfer ins Ausland „geschäftlich begründet" ist und die Sicherheit der Datenübertragung ins Ausland zuvor überprüft worden ist.

(4) Grenzüberschreitender Datentransfer und Sicherheitsüberprüfung

Bei Übertragung von personenbezogenen Informationen und wichtigen Daten ins Ausland müssen nach dem Entwurf der Measures for PI and ID Transfer der betroffenen Person der Zweck, Umfang, Inhalt, Empfänger und das Zielland übermittelt und ihre Einwilligung eingeholt werden. Zudem muss der Netzwerkbetreiber vor der Datenübertragung eine eigene Sicherheitsüberprüfung durchführen. Überprüft werden unter anderem die Notwendigkeit der Datenübertragung, die Menge, der Umfang, der Typ und die Sensibilität der Daten, das Sicherheitsniveau des Empfängers sowie das Risiko von Vorfällen nach der Übertragung.

In folgenden Fällen ist eine Sicherheitsüberprüfung durch die Branchenaufsicht oder Regulierungsbehörde durchzuführen:

- wenn personenbezogene Informationen von über 500.000 Personen transferiert werden,
- wenn die Menge der Daten 1.000 Gigabyte überschreitet,
- bei sensiblen Daten, z. B. über kerntechnische Anlagen, chemische und biologische Anlagen, die nationale Verteidigungsindustrie oder den Gesundheitszustand der Bevölkerung usw.,
- wenn die Daten Netzsicherheitsinformationen über KRITIS enthalten,
- bei Datenübertragung durch KRITIS-Betreiber.

Eine Datenübertragung ins Ausland ist verboten:

- wenn die betroffene Person nicht in die Übertragung der personenbezogenen Informationen einwilligt oder

die Gefahr besteht, dass deren Interessen beeinträchtigt werden,

- wenn die sozialen und öffentlichen Interessen geschädigt werden könnten,
- wenn die Daten von den Behörden als nicht übertragbar eingestuft wurden.

4. Durchsetzung nach dem CSL

Das CSL sieht vor allem verwaltungsrechtliche Konsequenzen vor, wenn die Netzwerkbetreiber ihre Pflichten verletzen. Die zuständige Behörde wird bei rechtswidrigem Verhalten eine Frist zur Korrektur setzen und kann ein Bußgeld verhängen, sofern das rechtswidrige Verhalten nicht korrigiert wird oder zu schwerwiegenden Folgen führt. Verletzt der Netzwerkbetreiber z. B. seine Sicherheits- und Schutzpflichten, kann ein Bußgeld von bis zu 500.000 Renminbi für das Unternehmen und 100.000 Renminbi für den direkt Verantwortlichen auferlegt werden. Liegt eine Verletzung von Datenschutzrechten beim Netzwerkbetreiber vor, kann ein Bußgeld von bis zum Zehnfachen der illegalen Einnahmen oder bis zu einer Million Renminbi verhängt werden. Darüber hinaus kann die zuständige Behörde die Schließung der Website oder die Aufhebung der Geschäftslizenz anordnen. Die rechtswidrigen Verhaltensweisen können auch im chinesischen „Credit System“ aufgenommen und bekanntgemacht werden. Meist werden die Behörden aufmerksam, wenn Datenlecks aufgrund von Lücken im Netzwerksicherheitssystem oder Hackereingriffen aufgefallen sind. So wurde einer Bibliothek in der Provinz Henan wegen mangelnder Durchsetzung des Schutzsystems für die Netzwerksicherheit eine Geldstrafe von 20.000 Renminbi und dem Verantwortlichen eine Geldstrafe von 5.000 Renminbi sowie eine Verwarnung auferlegt.

5. Handlungsempfehlungen

Unternehmen mit operativem Geschäft in China sind gehalten, den besonderen Verpflichtungen des CSL rasch nachzukommen, um die Risiken von Verstößen bzw. deren Sanktionen zu vermeiden. Die Personen, die für die Internetsicherheit und den Datenschutz verantwortlich sind, sollten von der Managementebene schnellstmöglich benannt werden. Dies beinhaltet zum einen die Ernennung mindestens einer zuständigen Person für den Netzwerkbetrieb oder, soweit es sich um KRITIS-Betreiber handelt, das Einrichten einer Abteilung, die für die Netzwerksicherheit

zuständig ist. Es gilt, die Mitarbeiter für die Einhaltung des CSL zu sensibilisieren. Maßnahmen können unter anderem die Einführung von Schulungen zur Einhaltung der IT-Sicherheit und des Datenschutzes oder das Aktualisieren von Mitarbeiter-Handbüchern sein.

Zum anderen sollte der Status quo in allen Unternehmensbereichen, z. B. IT, Personal, Einkauf, Marketing, mittels einer Bestandsaufnahme ermittelt werden. Dabei sollte überprüft werden, ob und welche internen Richtlinien und Maßnahmen zu Internetsicherheit und Datenschutz vorliegen bzw. befolgt werden. Darüber hinaus sollte unter anderem geprüft werden, welche Daten vom Unternehmen gesammelt, gespeichert und verarbeitet werden sowie ob die personenbezogenen und wichtigen Daten verschlüsselt werden. Auf Basis der Bestandsaufnahme sollte ein Soll-Ist-Vergleich durchgeführt werden, um Handlungsbedarfe zu identifizieren sowie Verbesserungsmaßnahmen aufzuarbeiten. Häufig müssen die Datenschutzerklärungen auf der Firmenwebsite gesetzeskonform angepasst und die Arbeitsverträge der Mitarbeiter, insbesondere aus der Personal- und IT-Abteilung, aktualisiert werden oder es muss eine Zusatzvereinbarung mit den Mitarbeitern geschlossen werden. Auch Verträge mit IT-Dienstleistern und Kunden sollten überprüft und gegebenenfalls überarbeitet werden.

Beim Datentransfer aus China gilt es insbesondere Folgendes zu beachten: Da die Measures for PI and ID Transfer noch nicht in Kraft sind, ist zurzeit die grenzüberschreitende Übermittlung von personenbezogenen Daten seitens Nicht-KRITIS-Betreibern grundsätzlich möglich, soweit die Einwilligung der betroffenen Person eingeholt wird. Eine Sicherheitsüberprüfung muss noch nicht zwingend durchgeführt werden. Allerdings ist zu erwarten, dass die Kontrolle über den grenzüberschreitenden Datentransfer in der Zukunft ausgeweitet wird. Deswegen sollten diejenigen Unternehmen, die geschäftlich auf personenbezogene Daten in China angewiesen sind, präventiv mehr Wert auf den Schutz der Daten legen, und so für die zukünftige Sicherheitsüberprüfung bereits die geeigneten Voraussetzungen schaffen. Alternativ könnten auch Vorkehrungen dahingehend getroffen werden, dass die Daten nicht zwingend ins Ausland übermittelt werden, sondern direkt in China gespeichert und verarbeitet werden. Dies kann durch die Einrichtung von Datenservern in China erreicht werden.

Es empfiehlt sich zudem, die aktuelle Entwicklung in China zu verfolgen. Das CSL wird regelmäßig durch Richtlinien von staatlichen Einrichtungen konkretisiert. Um die internen Prozesse entsprechend anpassen zu können, sollte das Unternehmen auf dem aktuellsten Wissensstand sein. ■

Thomas Weidlich, LL.M.
Rechtsanwalt, Partner

Thomas Weidlich ist Rechtsanwalt und Partner sowie Leiter des China-Desk der Luther Rechtsanwaltsgesellschaft mbH. Er gehört der Kanzlei seit 1996 an. Zwischen 2000 und 2005 hat er das Büro der Kanzlei in Singapur geleitet. Seit 2005 leitet er ein Corporate-M&A-Team im Kölner Büro und ist der verantwortliche Partner für die rechtliche Beratung im gesamten Asien-Pazifik-Raum mit Schwerpunkt auf China und Indien.

Tel.: +49 221 9937 16280
E-Mail: thomas.weidlich@luther-lawfirm.com

Dr. Yuan Shen, LL.M.
Attorney-at-Law (China),
Senior Associate

Dr. Yuan Shen studierte Rechtswissenschaften in Chongqing, Peking und Köln. Sie ist seit 2010 im Kölner Büro/China-Desk von Luther tätig und spezialisiert auf Gesellschaftsrecht, Arbeitsrecht und Börsengänge (IPO). Sie konzentriert sich auf die Unterstützung deutscher und europäischer Mandanten in den Bereichen Unternehmensgründung, Joint Ventures sowie Arbeitsrecht in China. Ein weiterer Schwerpunkt ist die Betreuung von chinesischen Unternehmen bei ihren Investitionen in Deutschland und anderen europäischen Ländern.

Tel.: +49 221 9937 25075
E-Mail: yuan.shen@luther-lawfirm.com

Luther Rechtsanwaltsgesellschaft mbH

Anna-Schneider-Steig 22 (Rheinauhafen), 50678 Köln

Fax: +49 221 9937 110
Internet: www.luther-lawfirm.com