Daniel Albrecht

Umdenken bei Netzbetreibern

Neue Anfroderungen durch aktuelles Datenschutzgesetz der VR China

In den vergangenen Jahren waren Datenerpressung, -diebstahl, -offenlegung und andere Vorfälle in China an der Tagesordnung. Datensicherheitsprobleme sind auf ein beispielloses Niveau gestiegen und haben direkte Auswirkungen auf die Informationssicherheit des Landes, der Industrie, der Unternehmen und der Einzelpersonen. Vor diesem Hintergrund wurde das Datenschutzgesetz (DSL) der Volksrepublik China vom Ständigen Ausschuss des 13. Nationalen Volkskongresses am 10. Juni 2021 verabschiedet und am 1. September 2021 offiziell umgesetzt.

Die Etablierung von Datenklassifizierungen und hierarchischen Schutzsystemen ist die Grundlage und Hauptarbeit des gesamten Datensicherheitssystems in China. Die Daten werden nach unterschiedlicher Bedeutung für die wirtschaftliche und soziale Entwicklung klassifiziert. Dabei sind auch die Höhe des Schadens für die nationale Sicherheit, öffentliche Interessen und die legitimen Rechte und Interessen von Einzelpersonen und Organisationen durch Datenmanipulation, Korruption, Datenlecks und unbefugten Zugriff und unbefugte Nutzung zu berücksichtigen. Die nationalen Kerndaten unterliegen einem strengeren Managementsystem.

Der Staat richtet ein System zur Überprüfung der Datensicherheit ein, um nationale Sicherheitsüberprüfungen von Datenverarbeitungsaktivitäten durchzuführen, die die nationale Sicherheit beeinträchtigen oder beeinträchtigen können. Eine in Übereinstimmung mit dem Gesetz getroffene Sicherheitsüberprüfungsentscheidung ist endgültig.Bei der Datenverarbeitung muss gemäß den

Bestimmungen ein prozessübergreifendes Datensicherheitsmanagementsystem aufgebaut und verbessert werden, Datensicherheitsschulungen sind zu organisieren und entsprechende technische und andere erforderliche Maßnahmen zum Schutz der Daten sind zu ergreifen. Bei der Verarbeitung von Daten unter Verwendung des Internets oder eines anderen Informationsnetzes werden die oben genannten Datenschutzverpflichtungen auf der Grundlage des hierarchischen Cybersicherheitsschutzsystems erfüllt. Ein Verarbeiter wichtiger Daten benennt einen Datenschutzbeauftragten und ein Datenschutzorgan.

Sicherheitsbewertung für die grenzüberschreitende Übermittlung personenbezogener Daten

Die Maßnahmen zur Sicherheitsbewertung für die grenzüberschreitende Übermittlung personenbezogener Daten wurden am 13. Juni 2019 von der Cyberspace Administration of China (CAC) als Entwurf herausgegeben. Dieser weist erhebliche Unterschiede zu den Maßnahmen zur Sicherheitsbewertung der grenzüberschreitenden Übermittlung personenbezogener Daten und wichtiger Daten aus dem Jahr 2017 auf. Die Maßnahmen gelten nur für den grenzüberschreitenden Verkehr personenbezogener Daten und nicht mehr für wichtige Daten. Der grenzüberschreitende Verkehr wichtiger Daten wird jetzt durch die Verwaltungsmaßnahmen zur Datensicherheit geregelt. Auch die Notwendigkeit einer lokalen Datenspeicherung wird nicht mehr erwähnt. Schließlich richten sich die Maßnahmen zur Sicherheitsbewertung für die grenzüberschreitende Übermittlung personenbezogener Daten auch an ausländische Unternehmen, alos auch an Unternehmen, die nicht in China ansässig sind.

Die wichtigsten Aspekte der Verordnung sind:

- Bei der grenzüberschreitenden Übertragung wichtiger Daten sind die Netzbetreiber nur unter besonderen Umständen verpflichtet, die ausgehenden Daten der Branchenaufsicht oder der Regulierungsbehörde für die Sicherheitsbewertung zu melden, und zwar dann wenn sie personenbezogene Daten von mehr als 500.000 Personen erhalten oder ansammeln und das Datenvolumen 1.000 GB überschreitet. Die Netzbetreiber müssen vor jeder grenzüberschreitenden Datenübertragung bei den Landesbehörden für den Cyberspace an ihrem Standort eine Sicherheitsprüfung beantragen, was die Situation der Sicherheitsprüfung personenbezogener Daten mit Auslandsbezug erheblich erweitert.
- Die Forderung der lokalen Datenspeicherung, die nach dem Cybersicherheitsgesetz nur für Betreiber kritischer Informationsinfrastruktur gilt, wurde in früheren Entwürfen auf alle Netzbetreiber ausgeweitet. Diese Anforderung wurde in den neuen Maßnahmen zur Sicherheitsbewertung für die grenzüberschreitende Übermittlung personenbezogener Daten vollständig gestrichen. Es sei darauf hingewiesen, dass diese Maßnahme gemäß dem Cybersicherheitsgesetz der VR China formuliert ist und ihr rechtlicher Rang viel niedriger als das Gesetz zum Schutz personenbezogener Daten ist, so dass Artikel 37 des Cybersicherheitsgesetzes und Artikel 40 des Gesetzes zum Schutz personenbezogener Daten (PIPL) einzuhalten sind. Offensichtlich sollten im derzeit geltenden Rechtstext nur die personenbezogenen Daten erfasst werden, bei deren Verarbeitung die von der nationalen Cyberspace-Verwaltung festgelegten Schwellenwerte erreicht werden. Dies kann dazu führen, dass nach internationaler Kritik auf die Vorgabe einer lokalen Speicherung für alle Netzbetreiber verzichtet wird. Hier bleibt die weitere Entwicklung abzuwarten. Gegebenenfalls wird das Erfordernis in einer anderen Bestimmung wieder aufgegriffen. Experten bezweifeln, dass die zuständigen Behörden über ausreichende Kapazitäten verfügen, um diesen Verpflichtungen nachzukommen. Dennoch wird eine strikte Datenlokalisierung als wichtiges Mittel gesehen, um die Souveränität des Cyberspace und die Netzwerksicherheit zu erreichen.
- Ausländische Institute, die im Rahmen ihrer Geschäftstätigkeit personenbezogene Daten von inländischen Nutzern in China über das Internet erheben, müssen die in den Maßnahmen zur Sicherheitsbewertung für die grenzüberschreitende Übermittlung personenbezogener Daten geregelten Anforderungen an Netzbetreiber erfüllen. Die Erfüllung der Aufgaben erfolgt durch Vertreter oder Organisationen in China.

Verordnung zum Schutz der Sicherheit kritischer Informationsinfrastrukturen

Am 17. August 2021 hat der Staatsrat die Verordnung zum Schutz der Sicherheit kritischer Informationsinfrastrukturen

(CII-Sicherheitsverordnung) veröffentlicht. In Übereinstimmung mit dem chinesischen Cybersicherheitsgesetz (CSL) definiert die CII-Sicherheitsverordnung CII als „wichtige Netzeinrichtungen, Informationssysteme uns so weiter in wichtigen Industrien und Bereichen wie öffentliche Kommunikations- und Informationsdienste, Energie, Verkehr, Wasser, Finanzen, öffentliche Dienste, E-Government-Angelegenheiten und Verteidigungstechnologien, die im Schadensfall, bei Funktionsverlust oder Verlust von Daten die nationale Sicherheit, die Volkswirtschaft und die Lebensgrundlagen der Menschen oder das öffentliche Interesse ernsthaft gefährden können". Die Schutzbehörden identifizieren und benachrichtigen Betreiber in ihren Branchen, die als CII bezeichnet werden, und geben damit den Betreibern Klarheit darüber, ob sie die für CII geltenden Anforderungen erfüllen müssen.

CII-Betreiber müssen zusätzlich zu den in der CSL festgelegten Sicherheitsverpflichtungen ihre kritische Infrastruktur gemäß der CII-Verordnung planen, nutzen und für Sicherheitsmaßnahmen sorgen. Vorgeschrieben ist eine spezielle Einrichtung für das Sicherheitsmanagement und Sicherheitsüberprüfungen sind durchzuführen. Außerdem müssen ein Notfallplan erstellt und regelmäßige Notfallübungen organisiert werden. Zudem sind relevante Cyber-Sicherheitsvorfälle und andere wichtige Angelegenheiten den Behörden zu melden.

Mindestens einmal jährlich müssen Cyber-Sicherheitstests und Risikobewertungen durchgeführt werden. Die aufgedeckten Sicherheitsprobleme sind zu beheben und Meldungen sind entsprechend den Vorgaben der Schutzbehörden zu erstellen. Könnte die nationale Sicherheit durch die Beschaffung von Netzprodukten oder -diensten durch den CII-Betreiber gefährdet sein, muss vor dem Einsatz eine Sicherheitsüberprüfung erfolgen. Bei einer Verschmelzung, Spaltung oder Auflösung des Betreibers kritischer Infrastruktur sind die Schutzbehörden zu benachrichtigen und die Infrastruktur ist entsprechend den Anforderungen der Schutzbehörden anzupassen.

CII-Betreiber können bei Nichteinhaltung der Sicherheitsverpflichtungen mit verschiedenen Strafen belegt werden, einschließlich Anordnungen zur Berichtigung, Verwarnungen, Verwaltungsstrafen von bis zu einer Million Yuan oder dem zehnfachen des Preises des von ihm beschafften Produkts oder der Dienstleistung. Der Verantwortliche und andere direkt verantwortliche Personen können auch persönlich haften. Die von der CII-Sicherheitsverordnung vorgeschriebenen Strafen gelten zusätzlich zu denen, die in anderen Gesetzen wie der CSL oder dem Strafrecht festgelegt sind.

Facit

Insgesamt stellen die administrativen Maßnahmen zur Datensicherheit und die Maßnahmen zur Sicherheitsbewertung für die grenzüberschreitende Übermittlung personenbezogener Daten und die neue Spezifikation zur Sicherheit personenbezogener Daten weitreichende neue Anforderungen an die Netzbetreiber. Aus praktischer Sicht sollten daher ausländische Investoren, die chinesische Investitionsziele im Auge haben, die Notwendigkeit sehen, die Datenschutz- und Sicherheitssysteme dieser Ziele sorgfältig zu prüfen. Relevante Überlegungen zur Datensicherheit können auf nationaler, regionaler, lokaler und/oder sektorspezifischer Ebene notwendig sein, sodass eine umfassende Betrachtung in Verbindung mit einem lokalen Berater in China mit geeigneter Expertise erfolgen sollte. Zudem bringt die aktuelle komplexe Compliance-Landschaft größere Herausforderungen mit sich, wie Unternehmen die Risiken des Schutzes personenbezogener Daten effektiv managen können, insbesondere wie der Schutz personenbezogener Daten im Prozess der digitalen Transformation und der Anwendung neuer Technologien wie Big Data berücksichtigt wird.

Leider klären die neuen Regelungen die wichtige Frage der lokalen Datenspeicherung noch nicht. Die Vervielfältigung von Inhalten, die administrativen Maßnahmen zur Datensicherheit und die Spezifikation zur Sicherheit personenbezogener Daten sorgen letztendlich für zusätzliche Irritationen. Die CII-Sicherheitsverordnung bestätigt den ungeschriebenen Ansatz der chinesischen Behörden in Bezug auf CII. Dies sollte Unternehmen, die in China Geschäfte tätigen, mehr Sicherheit geben, sodass sie erkennen können, welche Sicherheitsanforderungen gelten, und Bedenken hinsichtlich einer Sanktionierung wegen Verstößen gegen die CII-Sicherheitsverpflichtungen ausräumen, ohne zu wissen, dass diese anwendbar sind. ○

Daniel Albrecht
ist Managing Counsel und Rechtsanwalt der Starke (Beijing) Intellectual Property Co. Ltd.
law@starke-ip.com