Zunehmend schwieriger: Grenzüberschreitender Datenaustausch und VPN-Nutzung

Seit dem Inkrafttreten des chinesischen Netzwerksicherheitsgesetzes („Cybersecurity Law“ bzw. „CSL“) im Juni 2017 hat China eine Vielzahl von Ausführungsbestimmungen und technischen Normen erlassen. Dieser Regelungskomplex und die damit verbundenen Verpflichtungen stellen eine besondere Herausforderung für in China tätige ausländische Unternehmen bei Erhebung, Speicherung, Verarbeitung sowie Übertragung von Daten dar. Hinzu kommt, dass die Nutzung von VPN seit Anfang dieses Jahres strenger kontrolliert wird und die ersten Strafen gegen private Nutzer verhängt wurden.

Ausländischen Unternehmen wird empfohlen, bei grenzüberschreitendem Datenaustausch ein besonderes Augenmerk auf „personenbezogene Informationen“ und „wichtige Daten“ zu legen, da diese speziellen gesetzlichen Vorgaben unterliegen.

Datenlokalisierung und grenzüberschreitender Datenaustausch

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. Zu den personenbezogenen Informationen zählen Name, Geburtstag, Personalausweisnummer, Adresse, Telefonnummer, Korrespondenzprotokolle und -inhalte, Vermögens- und Transaktionsinformationen usw. „Wichtige Daten“ sind nach dem im April 2017 erlassenen Entwurf der „Measures for the security assessment of personal information and important data to be transmitted abroad“ („Measures for PI and ID Transfer“) solche Daten, die Auswirkungen auf die nationale Sicherheit und die wirtschaftliche Entwicklung haben könnten oder von besonderem gesellschaftlichen und öffentlichen Interesse sind.

Schon seit einigen Jahren müssen personenbezogene Informationen, die der Betreiber erhebt oder verarbeitet, in China gespeichert werden und dürfen nur mit Zustimmung der betroffenen Person ins Ausland exportiert werden. Für Betreiber kritischer Informations-Infrastruktur (KRITIS) gilt darüber hinaus, dass personenbezogene Informationen und wichtige Daten in China gespeichert werden dürfen, auch wenn die betroffenen Personen oder Geschäftspartner nicht 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 überprüft werden muss.

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

Eine Sicherheitsüberprüfung durch die Branchenaufsicht oder Regulierungsbehörde ist durchzuführen:

- wenn personenbezogene Informationen von mehr als 500.000 Personen transferiert werden
- wenn die Menge der Daten 1.000 GB überschreitet
- bei sensiblen Daten wie Informationen über kerntechnische, chemische und biologische Anlagen, die nationale Verteidigungsindustrie oder den Gesundheitszustand der Bevölkerung
- 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 wird
- wenn die sozialen und öffentlichen Interessen beeinträchtigt werden könnten
- wenn die Daten von den Behörden als nicht übertragbar eingestuft wurden.

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 bisher noch nicht zwingend durchgeführt werden. Allerdings ist zu erwarten, dass die Kontrolle des grenzüberschreitenden Datentransfers künftig ausgeweitet wird. Deswegen sollten Unternehmen, die geschäftlich auf personenbezogene Daten in China angewiesen sind, präventiv mehr Wert auf den Schutz der Daten legen, damit diese für die künftige Sicherheitsüberprüfung bereits die entsprechenden Vorausset-

zungen schaffen. Alternativ könnten diese auch Vorkehrungen dahingehend treffen, dass die Daten nicht zwingend ins Ausland übermittelt werden, sondern direkt auf Datenservern in China gespeichert und verarbeitet werden.

Great Firewall: Vorgehen gegen illegale VPN-Nutzung

Wer in China nach bestimmten Begriffen oder Webseiten sucht, gelangt in der Regel auf eine leere Seite oder erhält eine Fehlermeldung. Einige ausländische Suchmaschinen wie Google und die meisten westlichen sozialen Netzwerke, Videoportale und Kurznachrichtendienste wie Facebook, YouTube und WhatsApp sind komplett gesperrt. Wer in China geschäftlich oder privat unterwegs ist, nutzt daher meist einen VPN-Account, um die „Great Firewall“ zu überwinden und auf blockierte Internetseiten und -dienste zugreifen zu können. Ein VPN-Account baut eine verschlüsselte Verbindung zu einem VPN-Server im Ausland auf, sodass die Daten sicher durch sogenannte VPN-Tunnel übertragen werden. Bislang war dies eine gängige Methode sowohl für ausländische Geschäftsleute und Touristen als auch für inländische Nutzer ausländischer Webseiten.

Allerdings hat im Dezember 2018 die Behörde für öffentliche Sicherheit in der Provinz Guangdong die erste Geldstrafe gegen eine chinesische Privatperson wegen illegaler VPN-Nutzung verhängt. Der Betroffene hatte über eine VPN-App rund 500 illegale Internetverbindungen innerhalb einer Woche aufgerufen. Im Januar 2019 wurde eine andere Privatperson in Chongqing ebenfalls wegen Einrichtung beziehungsweise Nutzung illegaler Kanäle für internationale Netzwerkverbindungen von der lokalen Behörde für öffentliche Sicherheit zur politischen Ermittlung geladen. Diese beiden Fälle haben einige Unruhe unter den ausländischen VPN-Nutzern in China verursacht, denn bisher waren die behördlichen Maßnahmen lediglich an VPN-Software-Entwickler oder kommerzielle Händler gerichtet und fanden vor dem Hintergrund einer Kampagne des Ministeriums für Industrie und Informationstechnolgie (MIIT) statt. Im Rahmen des Erlasses “Cleaning Up and Regulating the Internet Access Service Market” wurden zwischen Januar 2017 und März 2018 Bußgelder in Höhe von bis zu 500.000 Yuan verhängt und Freiheitsstrafen von maximal 5,5 Jahren verhängt. Offenbar wurden auch die drei staatlichen Telekommunikationsanbieter (China Telecom, China Mobile und China Unicom) angewiesen, die Nutzung von VPN-Diensten einzuschränken beziehungsweise zu erschweren.

Diese tendenzielle Richtungsänderung im Vorgehen gegen illegale VPN-Nutzung ist nicht auf Gesetzesänderungen zurückzuführen, sondern auf eine verschärfte Durchsetzung der bereits seit 1996 bestehenden Vorschriften (Interim Regulations on Administration of Computer Information Network International Connectivity – “Interim Regulations”). Demnach muss jede direkte internationale Verbindung eines Computerinformationsnetzes über den internationalen Internet-Austauschkanal erfolgen, der vom staatlichen öffentlichen Telekommunikationsnetz des Ministeriums für Post und Telekommunikation (jetzt MIIT) eingerichtet wurde. Bisher haben jedoch nur die drei staatlichen Telekommunikationsanbieter die entsprechende MIIT-Lizenz bekommen. Es dürfen keine anderen Kanäle für die internationale Netzwerkverbindung eingerichtet oder genutzt werden. Dazu zählt – streng genommen – auch ein Internetzugang über einen firmeninternen VPN. Bei Verstößen gegen die „Interim Regulations“ kann die Behörde für die öffentliche Sicherheit die Netzwerkverbindung aussetzen, eine Abmahnung aussprechen und eine Geldstrafe von bis zu 15.000 Yuan verhängen. Dennoch ist die Einrichtung und Nutzung eines firmeninternen VPN zum internen Datenaustausch nicht per se illegal, das MIIT ist jedoch darüber zu informieren.

Vorbeugende Maßnahmen ergreifen

Chinesische Tochtergesellschaften deutscher Unternehmen nutzen in der Regel einen grenzüberschreitenden Internetkanal von einem der drei chinesischen staatlichen Telekommunikationsanbieter, entweder über einen Service-Vertrag von der deutschen Muttergesellschaft oder über einen direkten Vertrag mit einem der chinesischen Telekommunikationsanbieter. Die Einrichtung eines VPN zum firmeninternen Datenaustausch erfolgt auch über diese Anbieter und ist legal, sofern es ein geschlossenes Netz bleibt. Problematisch ist dagegen, wenn Mitarbeiter in China durch das firmeninterne VPN auch Zugriff auf das öffentliche Internetnetzwerk im Ausland erhalten. Dies würde dann nicht mehr den Anforderungen der Ziffer 6 der Interim Regulations entsprechen.

Bisher ist kein Fall bekannt, bei dem chinesische Behörden gegen eine internationale Internetnutzung mittels eines firmeninternen VPN vorgegangen sind. Aufgrund der weit verbreiteten Praxis wird dies voraussichtlich weiterhin geduldet, sofern die VPN-Nutzung im normalen Umfang und Ausmaß erfolgt. Angesichts der aktuellen Entwicklung hin zu einer verschärften Durchsetzung der bestehenden Vorschriften ist es für ausländische Unternehmen trotzdem ratsam, vorbeugende Maßnahmen zu ergreifen. Im Zusammenhang mit einer VPN-Einrichtung wäre beispielsweise die Einführung einer Sperrliste mit kritischen Webseiten und Begriffen oder ein eingeschränkter Zugang für ausschließlich geschäftlich relevante Webseiten für Mitarbeiter in China denkbar. Auch sollten im Mitarbeiter-Handbuch Regelungen für die Internet-Nutzung mit dem Firmencomputer oder -handy festgelegt werden. Mitarbeiter sollten zudem durch regelmäßige Schulungen für das Thema sensibilisiert werden.

Zusammenfassend lässt sich sagen, dass sich der grenzüberschreitende Datenaustausch für ausländische Unternehmen zunehmend schwieriger gestaltet und auch der Zugriff auf Informationen und Webseiten im Ausland über einen VPN-Account weiter eingeschränkt wird. Deutsche Unternehmen in China sollten sich daher frühzeitig damit auseinandersetzen, welche Auswirkungen das CSL und die zahlreichen bestehenden und noch zu erwartenden Ausführungsbestimmungen auf ihr Unternehmen haben werden und entsprechende Vorkehrmaßnahmen treffen.

Thomas Weidlich
ist Rechtsanwalt und Partner bei Luther Rechtsanwaltsgesellschaft mbH in Köln.
Thomas.Weidlich@luther-lawfirm.com

Dr. Yuan Shen
ist Legal Consultant und Senior Associate bei Luther Rechtsanwaltsgesellschaft mbH in Köln.
Yuan.Shen@luther-lawfirm.com