Schränkt China den grenzüberschreitenden Datenverkehr ein?

Author : Jan Michael Hähnel

Globale Infrastruktur von Unternehmen versus Datenlokalisierung: Wie wirkt sich das chinesische Netzwerksicherheitsgesetz auf deutsche Unternehmen und ihre Tochtergesellschaften in China mit weltweit vernetzten Produktionen und Personalverwaltungen aus?

Das Netzwerksicherheitsgesetz (NSG) oder Cybersecurity Law hat mit seinen vagen Formulierungen und scharfen Strafen schon vor seinem Inkrafttreten im Juli 2017 hohe Wellen geschlagen.

Viele weitere Gesetzes- und Verordnungsentwürfe, die sich auf das NSG beziehen, haben zusätzlich zur Verwirrung von Unternehmensvertretern in China beigetragen.

Dem NSG nähert man sich vorzugsweise über dessen Zweckbestimmung, nämlich den Schutz von Netzwerken und insbesondere sogenannter „kritischer Informationsinfrastruktur“ (KII). Vorschriften zur Datenlokalisierung, mit denen sich dieser Artikel befasst, sind nur Ausfluss dieses Zweckes.

So wundert es nicht, dass das NSG nur eine einzige Regelung zum Thema Datenlokalisierung enthält. Es gibt zwar weitere Regelungen außerhalb des NSG, diese betreffen jedoch Spezialgebiete wie etwa Banken, Kliniken oder geografische Daten und sollen daher hier unberücksichtigt bleiben.

Pflicht zur lokalen Datenspeicherung

Die oben genannte Regelung im NSG besagt, dass „persönliche Informationen“ und „wichtige Daten“, die von KII „gesammelt“ werden, in China gespeichert werden müssen (Pflicht zur lokalen Datenspeicherung). Dort, wo es aufgrund von „Geschäftserfordernissen notwendig ist“, solche Daten ins Ausland zu übertragen, muss eine Sicherheitsprüfung durchgeführt werden.

Die Pflicht zur lokalen Datenspeicherung wirft jedoch mehrere Fragen auf.

Zuvorderst stellt sich die Frage, wer Adressat dieser Pflicht, also „KII-Betreiber“ ist.

Das NSG enthält keine Definition von KII, sondern nur Beispiele wie Infrastrukturen zur Energieversorgung oder solche, welche die nationale Sicherheit betreffen. Interpretationsspielraum bietet die Nennung von Netzwerken, die im Falle von Zwischenfällen das „öffentliche Leben“ und das „öffentliche Interesse“ gefährden.

KII lässt sich jedoch über eine Richtlinie für Behörden zur nationalen Sicherheitsprüfung konkretisieren. Diese enthält eine Tabelle, welche die Identifikation von KII in bestimmten Industrien und Industriesektoren erleichtert.

Globale Infrastruktur von Unternehmen versus Datenlokalisierung: Wie wirkt sich das chinesische Netzwerksicherheitsgesetz auf deutsche Unternehmen und ihre Tochtergesellschaften in China mit weltweit vernetzten Produktionen und Personalverwaltungen aus?

So werden im Rahmen der industriellen Produktion „intelligente Produktionssysteme“ als möglicher Industriesektor für KII aufgezählt. Eine intelligente Produktion wird unter anderem dann als KII klassifiziert, wenn ein „Ereignis“ fünf Tote oder mehr als 50 Schwerverletzte verursachen kann.

Hierbei ist zu bedenken, dass sich KII nicht auf Unternehmen, sondern auf Netzwerke bezieht. KII kann daher einzelne Unternehmsteile oder aber ganze Unternehmensgruppen umfassen.

Die Konsequenz für KII-Betreiber ist aber immer die gleiche: Sie müssen „persönliche Informationen“ oder „wichtige Daten“ in China speichern.

© Copyright - GoingPublic Media AG

Was sind persönliche Informationen?

Persönliche Informationen sind im NSG definiert als Daten, die entweder alleine oder in Kombination mit anderen Daten genutzt werden können, um eine natürliche Person zu identifizieren.

Diese Definition erlaubt zwar bei offensichtlich persönlichen Daten wie zum Beispiel dem Namen oder der Ausweisnummer eine klare Abgrenzung. In Zweifelsfällen hilft sie jedoch nicht weiter. So stellt sich beispielsweise die Frage, ob Unternehmenskontaktdaten, bei denen der Name und die Position des Mitarbeiters angegeben werden, als „persönliche Informationen“ gelten. Denn auch diese Daten können genutzt werden, um eine Person zu identifizieren. Diese und ähnliche Fragen sind derzeit noch nicht abschließend geklärt. Im Zweifel sollten aber alle Daten, die genutzt werden können, um eine Person zu identifizieren, als persönliche Informationen im Sinne des NSG behandelt werden.

Zu wichtigen Daten enthält das NSG keine Definition. Hierauf lassen nur Gesetzesentwürfe Rückschlüsse zu.

Gemäß diesen Entwürfen handelt es sich bei „wichtigen Daten“ um Daten, die eng mit der nationalen Sicherheit, der wirtschaftlichen Entwicklung und dem möglichen gesellschaftlichen und öffentlichen Interesse Chinas in Verbindung stehen.

Auch diese Beschreibung ist jedoch so vage, dass die Behörden grundsätzlich alle Daten, die sie für wichtig erachten, als „wichtige Daten“ erfassen können.

In Ausnahmefällen dürfen persönliche Informationen oder wichtige Daten exportiert werden, etwa wenn dies zu Geschäftszwecken notwendig ist und eine Sicherheitsprüfung durchgeführt wird.

Was als „zu Geschäftszwecken notwendig“ gilt, liegt im freien Ermessen der Behörden.

Auch wie die Sicherheitsprüfung genau aussehen soll, ergibt sich nicht aus dem NSG. Jedoch gibt es auch hier Gesetzesentwürfe, die Rückschlüsse zulassen.

Globale Infrastruktur von Unternehmen versus Datenlokalisierung: Wie wirkt sich das chinesische Netzwerksicherheitsgesetz auf deutsche Unternehmen und ihre Tochtergesellschaften in China mit weltweit vernetzten Produktionen und Personalverwaltungen aus?

Diese Entwürfe sehen unter anderem vor, dass bestimmte Daten nicht exportiert werden dürfen, so beispielsweise persönliche Informationen ohne die Zustimmung des Dateninhabers.

Diese Regelung könnte insbesondere solchen Unternehmen Probleme bereiten, die Lieferanten-, Kunden- oder Personaldaten aus China ins unternehmenseigene ERP-System im Ausland übertragen möchten. Denn hierfür müsste die Zustimmung aller Dateninhaber vorliegen.

Des Weiteren verweisen die Entwürfe darauf, dass die Sicherheitsprüfung grundsätzlich als Selbstprüfung, die den Behörden vorgelegt werden muss, ausgestaltet werden soll.

Schwellenwerte sind nicht klar definiert

Eine Prüfung durch die Behörden soll nur dann notwendig sein, wenn bestimmte Datenmengen beziehungsweise eine bestimmte Anzahl von Personen überschritten werden. Wo diese Schwellenwerte liegen, ist derzeit noch unklar. Auch wird der Export von sicherheitsrelevanten Daten oder Informationen über Sicherheitslücken in Netzwerken möglicherweise einer behördlichen Prüfung bedürfen. Eine solche Prüfung muss entweder vor jeder einzelnen Datenübertragung oder, bei dauerhafter Datensynchronisation, zumindest jährlich durchgeführt werden.

Die Handhabung persönlicher Informationen wird mittlerweile in einem freiwilligen Standard geklärt. Auch wenn diese Standards unverbindlich sind, werden sie in der Praxis von chinesischen Behörden als Richtlinien angelegt.

Es gibt in einigen Entwürfen Hinweise darauf, dass die Datenlokalisierungspflicht in Zukunft auch andere Netzwerkbetreiber erfassen könnte. Netzwerkbetreiber ist jeder, der zwei Geräte oder mehr vernetzt hat. Ob und

© Copyright - GoingPublic Media AG

wieweit die Pflicht zur Datenlokalisierung Netzwerkbetreiber tatsächlich erfassen wird, ist derzeit noch unklar. Unseres Erachtens ist es jedoch wahrscheinlich, dass Netzwerkbetreiber künftig entweder auch der Datenlokalisierungspflicht oder einer ähnlichen Pflicht unterliegen werden. Dies ergibt sich aus dem Schutzzweck des NSG, denn KII-Daten können auch bei anderen Netzwerkbetreibern lagern, die keine KII sind. Würde nun eine Übertragung von KII-Daten ins Ausland nicht auch für Netzwerkbetreiber eingeschränkt, so wäre dies eine Sicherheitslücke für KII. Auch kann es nicht gewollt sein, dass persönliche Informationen nur im Rahmen von KII geschützt werden sollen.

Fazit

Es erscheint also im Ergebnis nicht so, dass es, wie vielfach befürchtet, Unternehmen bald unmöglich gemacht werden soll, ihre Daten aus China heraus zu transferieren.

Der Staat möchte sich aber ein Mitspracherecht bei Sicherheitsfragen und den persönlichen Daten der Bürger einräumen. Deswegen sind auch in Zukunft neue Standards und Definitionen zu erwarten, die einen Datentransfer zu wirtschaftlichen Zwecken regeln.

Allerdings wird der Staat vom KII-Betreiber erwarten, dass dieser über Transfer und Inhalt von Daten jederzeit Auskunft geben kann und die Sicherheit der Daten gewährleistet wird.

Ziel von Unternehmen sollte deswegen sein, sich schon jetzt möglichst umfassend auf Informationspflichten gegenüber dem Staat vorzubereiten sowie sicherzustellen, dass die Erlaubnis der Dateninhaber zum Transfer der Daten gegeben ist.

Zu den Personen

Rainer Burkardt arbeitet und lebt bereits seit 21 Jahren in China und berät vornehmlich Unternehmen aus dem deutschsprachigen Raum bei deren Geschäften in China.

Jan Michael Hähnel arbeitet und lebt seit fünf Jahren in China und unterstützt Mandanten unter anderem im IT- und Datenschutzrecht.

Burkardt & Partner ist eine Rechtsanwaltskanzlei, die vorwiegend mittelständische Unternehmen, aber auch Unternehmensgruppen und internationale Industriekonzerne aus Deutschland, der Schweiz und Österreich bei ihren Investitionen in der Volksrepublik China berät.

© Copyright - GoingPublic Media AG

www.bktlegal.com.

© Copyright - GoingPublic Media AG