Zeitschrift für Datenschutz – ZD
www.zd-beck.de

ZD FOKUS

Axel Spies China veröffentlicht Standardvertragsklauseln für grenzüberschreitende Datentransfers

ZD-Aktuell 2022, 01262

RA Dr. Axel Spies, Mitherausgeber der ZD, berichtet im Beck-Blog, dass die chinesische Cyberspace-Verwaltung am 30.6.2022 ihre lang erwartete Vorlage für den Standardvertrag über den grenzüberschreitenden Datentransfer zur öffentlichen Konsultation freigegeben hat. Die Konsultationsfrist endet bereits am 29.7.2022.

Der Entwurf der chinesischen Standardvertragsklauseln (chinesischen SCCs) ergänzt und konkretisiert den Weg des „Standardvertrags" und wird sicherlich eine wichtige Orientierungshilfe für die Einhaltung des Datenschutzes durch multinationale Unternehmen in China. Die Entwürfe der chinesischen SCCs ähneln den SCCs der EU, spiegeln aber auch einige Besonderheiten und den Schwerpunkt der chinesischen Datenschutzaufsicht wider. Multinationale Unternehmen sollten ihre Arbeitsabläufe im Bereich des grenzüberschreitenden Datentransfers auf der Grundlage der Entwürfe überprüfen und die bestehenden Compliance-Maßnahmen entsprechend anpassen, wenn diese hauptsächlich in Übereinstimmung mit der DS-GVO eingeführt wurden.

1. Anwendungsbereich

Gemäß den Bestimmungen des Entwurfs sind die SCCs für China nur dann anwendbar, wenn alle der folgenden Bedingungen erfüllt sind:

- Der für die Verarbeitung personenbezogener Daten Verantwortliche (sog. PI-Handler) ist kein Betreiber einer kritischen Informationsinfrastruktur (CIIO).
- Der Umfang der vom PI-Handler verarbeiteten personenbezogenen Daten betrifft nicht mehr als 1 Mio. Personen.
- Die kumulative Zahl der Personen, deren personenbezogene Daten der PI-Handler seit dem 1. Januar des Vorjahres ins Ausland übermittelt hat, hat 100.000 nicht erreicht.
- Die kumulative Zahl der Personen, deren sensible personenbezogene Daten der PI-Verantwortliche seit dem 1. Januar des Vorjahres ins Ausland übermittelt hat, beträgt nicht mehr als 10.000.

Wird mindestens eine der o.g. Bedingungen nicht erfüllt, kommen die Maßnahmen zur Sicherheitsbewertung zur Anwendung, was bedeutet, dass die Übermittlung einer Sicherheitsbewertung durch die chinesische Regierung unterzogen wird. In diesem Fall können weder die SCC noch die Zertifizierung anstelle einer Sicherheitsüberprüfung verwendet werden.

Im Vergleich zu den SCCs der EU scheinen die SCCs des Entwurfs in China deshalb nur in relativ begrenzten Fällen anwendbar zu sein. Obwohl der Entwurf eine Begrenzung des Kumulierungszeitraums auf zwei Jahre vorsieht, erscheinen die Schwellenwerte von 1 Mio., 100.000 und 10.000 Personen für viele datenintensive Branchen (zB Einzelhandel, Transportwesen, Gesundheitswesen und Online-Dienste für Unternehmen), die mit Verbrauchern arbeiten, angesichts der Bevölkerungszahl Chinas recht niedrig, insbesondere wenn die Berechnung unabhängig von den Geschäftsszenarien auf Unternehmensebene durchgeführt wird.

Darüber hinaus können multinationale Unternehmen mit großen Niederlassungen in China, die mehr als 10.000 Mitarbeiter beschäftigen, bei der grenzüberschreitenden Übermittlung personenbezogener Daten dieser Mitarbeiter möglicherweise nicht die SCC-Entwürfe für China verwenden, da die ins Ausland zu übermittelnden personenbezogenen Daten in der Regel sensible persönliche Daten enthalten. Daher ist es wahrscheinlich, dass viele Unternehmen in der Praxis nicht in der Lage sein werden, den SCC-Weg zu beschreiten und weiterhin den strengen Sicherheitsbewertungen für grenzüberschreitende Datenübertragungen unterworfen sein werden. Neben der Begrenzung des Datenvolumens sind die Parteien des Entwurfs der chinesischen SCC auch auf den Datenverantwortlichen und den Datenempfänger im Ausland beschränkt; es scheint jedoch so zu sein, dass in China ansässige beauftragte Parteien (die im Wesentlichen mit „Datenverarbeitern" gemäß der DS-GVO gleichzusetzen sind) nicht in der Lage sein werden, diesen Mechanismus zu nutzen.

Vor diesem Hintergrund gibt es einige Überschneidungen zwischen den SCC, der Sicherheitsbewertung und den bestehenden Zertifizierungswegen für grenz-

überschreitende Datenübermittlungen. Insbesondere verlangen die Maßnahmen zur Sicherheitsbewertung auch einen Vertrag zwischen dem Datenverarbeiter und dem Datenempfänger im Ausland als Teil der bei der Behörde einzureichenden Unterlagen. Die inhaltlichen Anforderungen an einen solchen Vertrag überschneiden sich weitgehend mit dem Entwurf der chinesischen SCCs. Daher können Unternehmen bei Datenübertragungen, die der Sicherheitsbewertung unterliegen, auch auf den Entwurf der chinesischen SCCs zurückgreifen, um den für die Sicherheitsbewertung erforderlichen Datenübertragungsvertrag zu formulieren. Die am 24.6.2022 herausgegebene Cyber Security Standard Practical Guidance – Security Certification Specification on Cross-border Transfer of Personal Information (Certification Specification) deutet ebenfalls darauf hin, dass eine verbindliche Vereinbarung für grenzüberschreitende Datenübertragungen erforderlich ist, um die Zertifizierung zum Schutz personenbezogener Daten zu erhalten.

2. Meldepflicht

China wendet für die SCC-Entwürfe eine Überwachungsmethode an, die eine „Kombination aus Zustimmung und Anmeldung" vorsieht. Eine vorherige Genehmigung ist für den Entwurf der chinesischen SCCs nicht erforderlich. Stattdessen muss der PI-Verantwortliche innerhalb von zehn Arbeitstagen nach Inkrafttreten der vorgeschriebenen Vereinbarung eine Mustervereinbarung bei der lokalen Niederlassung der Cyberspace Administration of China (CAC) auf Provinzebene einreichen.

In Anlehnung an das Gesetz zum Schutz personenbezogener Daten (Personal Information Protection Law – PIPL) wird in dem Entwurf bekräftigt, dass ein Bericht über die Folgenabschätzung für die Übermittlung personenbezogener Daten zusammen mit den unterzeichneten chinesischen SCCs ebenfalls bei der örtlichen CAC eingereicht werden muss. Im Gegensatz dazu verlangt die EU bekanntlich keine Einreichung von SCCs bei den DPAs.

Die Einreichung ist allerdings nicht gleichbedeutend mit einer Genehmigung, was bedeutet, dass die Zentrale Aufsichtsbehörde die SCC und den Bericht über die Folgenabschätzung für die Datenübermittlung nicht inhaltlich prüfen und die geplante Datenübermittlung ablehnen würde. Es bleibt jedoch genügend Raum für die Überwachung nach der Einreichung: Die örtliche Aufsichtsbehörde auf Provinzebene ist berechtigt, die Übermittlung personenbezogener Daten ins Ausland auszusetzen, wenn sie feststellt, dass die tatsächliche Übermittlung nicht den einschlägigen Vorschriften für die grenzüberschreitende Datenübermittlung entspricht. Wird ein Verstoß gegen die Aufbewahrungsvorschriften festgestellt, kann die Aufsichtsbehörde auch anordnen, dass die Daten innerhalb einer bestimmten Frist berichtigt werden müssen; sie kann Sanktionen verhängen, wenn sich der PI-Verantwortliche oder der Empfänger im Ausland weigert, die Daten zu berichtigen, oder wenn die mit den PI verbundenen Rechte und Interessen verletzt werden; oder sie kann strafrechtliche Schritte einleiten, wenn ein Verbrechen vorliegt.

3. Voraussetzung für die Übermittlung von Daten ins Ausland: PIPIA

In den Art. 55 und 56 PIPL wird das Konzept der chinesischen Datenschutz-Folgenabschätzung (PIPIA) erwähnt, das einer Datenschutz-Folgenabschätzung (DPIA) gemäß der DS-GVO ähnelt. Es werden folgende gemeinsame Punkte festgelegt, die in jedem PIPIA-Szenario bewertet werden:

- die Rechtmäßigkeit, Legitimität und Notwendigkeit des Zwecks, des Umfangs und der Methode der Verarbeitung personenbezogener Daten (PI);
- die Risiken, die der PI-Export für die mit PI verbundenen Rechte und Interessen mit sich bringen kann; und
- die Rechtmäßigkeit und Wirksamkeit der Schutzmaßnahmen, und ob sie dem Risikoniveau entsprechen.

In Anlehnung an die PIPL werden in den Entwürfen zusätzliche Punkte genannt, die in einer PIPIA im Szenario eines grenzüberschreitenden Datentransfers zu bewerten sind:

- die Verantwortlichkeiten und Verpflichtungen, zu denen sich der Empfänger im Ausland verpflichtet, sowie die Frage, ob sein Management und seine technischen Maßnahmen und Fähigkeiten zur Erfüllung der Verantwortlichkeiten und Verpflichtungen die Sicherheit der zu exportierenden PI gewährleisten können;
- die Risiken von Datenlecks, Schäden, Manipulationen und Missbrauch usw. nach der grenzüberschreitenden Übermittlung; und
- die Auswirkungen der PI-Schutzpolitik und -vorschriften des Landes oder der Region, in dem/der der Empfänger im Ausland ansässig ist, auf die Erfüllung der SCC-Entwürfe für China (sozusagen ein umgekehrtes „Schrems II").

Nach dem Entwurf der Bestimmungen soll die PIPIA immer durchgeführt werden, bevor personenbezogene Daten ins Ausland übermittelt werden. Unabhängig davon, welchen Weg der Datenexporteur für die grenzüberschreitende Datenübermittlung wählt (zB Sicherheitsbewertung, Zertifizierung, SCC), sollte eine PIPIA eine Vorbedingung sein.

4. Onward Transfer (Weiterübermittlung) der Daten

Interessant ist, dass die Entwürfe der chinesischen SCC die Weiterübermittlung von Daten an Dritte außerhalb Chinas beschränken, es sei denn, alle folgenden Bedingungen sind erfüllt:

- es besteht ein tatsächlicher geschäftlicher Bedarf;
- die betroffene Person wird informiert und es wird eine gesonderte Einwilligung eingeholt;
- der Empfänger in Übersee schließt einen Vertrag mit dem Dritten ab, und der Dritte erfüllt den Standard eines gleichwertigen Schutzes und würde die Mithaftung übernehmen; und
- dem Verantwortlichen wird eine Kopie der Vereinbarung mit dem Dritten vorgelegt.

Darüber hinaus verlangt der Entwurf der chinesischen SCCs die Identifizierung eines solchen ausländischen Dritten. Dies kann jedoch auf erhebliche praktische Hindernisse stoßen, da der ausländische Empfänger mitunter nicht in der Lage ist, den Bedarf für die Weiterübermittlung zu prognostizieren, geschweige denn die Identität der weiteren Empfänger zu kennen.

- Vgl. hierzu auch Johannes ZD-Aktuell 2021, 05455; Johannes ZD 2022, 90; Johannes ZD-Aktuell 2021, 05456; ZD-Aktuell 2021, 05319; Johannes ZD-Aktuell 2021, 05219; Richter ZD 2021, 233; Kipker ZD 2021, 397; Delval ZD-Aktuell 2019, 04373; Wagner ZD 2020, 140; Köstner/Nonn MMR 2020, 591 und Binding ZD 2014, 327.

Dr. Axel Spies
ist Rechtsanwalt in der Kanzlei Morgan Lewis & Bockius in Washington DC und Mitherausgeber der ZD.