Kurze Beiträge

CAC-Bestimmungen zur Förderung und Regulierung des grenzüberschreitenden Datenverkehrs – Echte Erleichterungen des strengen Datenschutzregimes für KMU in China?

Rainer Burkardt / Ondřej Zapletal [1]

Abstract

Die „Bestimmungen zur Förderung und Regulierung des grenzüberschreitenden Datenverkehrs“[2] („CAC-Bestimmungen“) enthalten die seit Langem erwarteten Ausnahmen für die grenzüberschreitende Übermittlung von personenbezogenen Daten ins chinesische Ausland.

Dieser Artikel fasst nachstehend die CAC-Bestimmungen zusammen, erläutert deren praktische Auswirkungen auf KMU in China und zeigt auf, unter welchen Voraussetzungen KMU von den in den CAC-Bestimmungen enthaltenen Ausnahmen bei grenzüberschreitenden Datentransfers ins chinesische Ausland Gebrauch machen können.

Darüber hinaus zieht der Artikel einen Vergleich zu dem Entwurf der CAC-Bestimmungen vom 28. September 2023[3] („Entwurf“) und stellt dar, ob und welche der im Entwurf enthaltenen offenen Punkte in den CAC-Bestimmungen adressiert wurden. Zum Abschluss werden Herausforderungen von KMU bei der Erfüllung der gesetzlichen Anforderungen dargestellt und Empfehlungen gegeben.

I. Einführung

Mehr als zwei Jahre nach der Verabschiedung des „Gesetzes der Volksrepublik China zum Schutz personenbezogener Daten“[4] („GSPD“), welches strenge Voraussetzungen für die Übermittlung personenbezogener Daten ins chinesische Ausland vorsieht, hat die Cyberspace Administration of China („CAC“) am 22. März 2024 die CAC-Bestimmungen erlassen, welche am selben Tag in Kraft getreten sind.

Die CAC-Bestimmungen stellen für Unternehmen in China, welche nur geringe Mengen personenbezogener Daten verarbeiten und ins chinesische Ausland übertragen, eine Lockerung des strengen Regimes nach dem GSPD dar.

Eine der für KMU wichtigsten und am meisten diskutierten Regelungen ist § 5 der CAC-Bestimmungen. Dieser sieht vier Ausnahmetatbestände vor, bei deren Vorliegen die drei Voraussetzungen für grenzüberschreitende Übermittlung von personenbezogenen Daten nach dem GSPD keine Anwendung finden. Wie nachstehend dargestellt, sind die Erleichterungen der grenzüberschreitenden Datenübermittlung nach den CAC-Bestimmungen jedoch nicht so umfassend, wie es auf den ersten Blick erscheinen mag.

II. Ausnahme von den „Drei Voraussetzungen“ für „Re-Exporte“ personenbezogener Daten

Die CAC-Bestimmungen enthalten in § 4 eine Ausnahme bzw. Klarstellung für den „Re-Export“, d. h. den grenzüberschreitenden Transfer von personenbezogenen Daten, die außerhalb von China erhoben oder generiert wurden.

Diese Ausnahme betrifft personenbezogene Daten, die z. B. in der Muttergesellschaft in der EU gesammelt, dann an die Tochtergesellschaft in China bereitgestellt und schließlich von dieser zurück in die EU übermittelt werden. In diesem Fall muss die chinesische Tochtergesellschaft bei der (Rück-)Übermittlung der personenbezogenen Daten in die EU keine der drei Voraussetzungen nach § 38 GSPD erfüllen, d. h., es ist weder das Bestehen der von der CAC organisierten Sicherheitsbewertung[5] („CAC-Sicherheitsbewertung“) noch das Bestehen der von einer qualifizierten Institution durchgeführten Zertifizierung zum Schutz von PD („Zertifizierung“) noch der Abschluss eines

[1] Rainer Burkardt ist Gründer und Geschäftsführer der chinesischen Anwaltskanzlei Burkardt & Partner in Shanghai. Ondřej Zapletal ist Rechtsberater bei Burkardt & Partner in Shanghai.

[2] 促进和规范数据跨境流动规定 (wörtlich: Bestimmungen zur Förderung und Normierung des grenzüberschreitenden Umlaufs von Daten) vom 22.3.2024, chinesisch-deutsch in diesem Heft, S. 159 ff.

[3] 规范和促进数据跨境流动规定（征求意见稿） vom 28.9.2023, chinesischer Text abrufbar auf der Webseite der Cyberspace Administration of China unter <http://www.cac.gov.cn> (<https://perma.cc/T9TX-USSW>).

[4] 中华人民共和国个人信息保护法 vom 20.8.2021, chinesisch-deutsche Fassung in: ZChinR 2021, S. 286 f.

[5] *Rainer Burkardt / Ondřej Zapletal,* Sicherheitsbewertung für grenzüberschreitende Datentransfers aus China, ChinaContact 5/6 2022, abrufbar unter <https://www.bktlegal.com> (<https://perma.cc/A4KY-ANS7>).

Vertrags mit dem Datenempfänger im Ausland gemäß dem von der CAC formulierten Standardvertrag („CAC-Standardvertrag") erforderlich. Die CAC-Sicherheitsbewertung, die Zertifizierung und der CAC-Standardvertrag werden im Folgenden gemeinsam als die „Drei Voraussetzungen" bezeichnet.[6]

Diese Ausnahme gilt gemäß § 4 CAC-Bestimmungen jedoch nur dann, wenn die zu „re-exportierenden" personenbezogenen Daten keine neuen in China generierten personenbezogenen Daten bzw. wichtigen Daten enthalten.

III. Vier Ausnahmen von den „Drei Voraussetzungen"

Eine der für KMU in China wichtigsten und, wie im Artikel zum Entwurf[7] kommentiert, auch kontroversesten Regelungen ist die Regelung in § 5 der CAC-Bestimmungen, welche die vier folgenden Ausnahmetatbestände vorsieht, bei deren Vorliegen die „Drei Voraussetzungen" für grenzüberschreitende Übermittlung von personenbezogenen Daten nach dem GSPD keine Anwendung finden:

1. Übermittlung von personenbezogenen Daten ins Ausland, wenn dies für den Abschluss oder die Erfüllung eines Vertrags erforderlich ist, dessen Vertragspartei der Betroffene (die natürliche Person, deren personenbezogenen Daten verarbeitet werden) ist, wie z. B. bei Kaufverträgen, Postversand, Geldüberweisungen, Flug- und Hotelreservierungen, Visumanträgen, Prüfungsdiensten;

2. erforderliche Übermittlung von personenbezogenen Daten von Arbeitnehmern zwecks Personalverwaltung in Übereinstimmung mit rechtmäßigen unternehmensinternen Arbeitsregelungen und Kollektivverträgen;

3. Übermittlung von personenbezogenen Daten in Notfällen zum Schutz von Leben, Gesundheit und Eigentum natürlicher Personen;

4. Übermittlung von weniger als 100.000 personenbezogener Daten (ausschließlich sensibler personenbezogener Daten) seit dem 1. Januar eines Jahres durch Datenverarbeiter, welche keine Betreiber kritischer Informationsinfrastrukturen (Critical Infrastructure Operator, „CIIO") sind.

Bei den Ausnahmen gemäß § 5 Nr. 1 CAC-Bestimmungen ist zu beachten, dass die Ausnahme für Vertragsschluss/-erfüllung nur für Verträge gilt, deren Vertragspartei der Betroffene ist. Dies legt den Schluss nahe, dass § 5 Nr. 1 CAC-Bestimmungen nur für Verträge mit Endverbrauchern (B2C-Verträge), nicht jedoch für Verträge mit anderen Unternehmen (B2B-Verträge) gilt. Dadurch fällt die grenzüberschreitende Übermittlung von personenbezogenen Daten, die beispielsweise in Verträgen zwischen chinesischen Tochtergesellschaften und deren Muttergesellschaften in Europa enthalten sind, nicht unter diese Ausnahmen.

Weiter stellt sich bei der Ausnahme nach § 5 Nr. 2 CAC-Bestimmungen die Frage, ob sie nur für personenbezogene Daten gilt, die in Übereinstimmung mit den ausdrücklich erwähnten Kollektivarbeitsverträgen unter die Ausnahme fallen, oder ob die Ausnahme auch für Daten gilt, deren Übermittlung in Übereinstimmung mit individuellen Arbeitsverträgen zwecks Personalverwaltung erforderlich ist.

Die Notfallausnahme gemäß § 5 Nr. 3 CAC-Bestimmungen ist für die Übermittlung von personenbezogenen Daten im alltäglichen Betrieb von KMU von geringer praktischer Relevanz.

Darüber hinaus verlangen die Ausnahmen in § 5 Nr. 1 und Nr. 2 CAC-Bestimmungen, dass die Datenübertragung „erforderlich"[8] sein muss. Dies bedeutet, dass der Datenverarbeiter im Zweifelsfall nachweisen muss, dass der grenzüberschreitende Datentransfer erforderlich war. In den CAC-Bestimmungen wird der Begriff „Erforderlichkeit" jedoch nicht definiert und die Erforderlichkeit des Datentransfers muss daher im Einzelfall geprüft werden.

IV. Ausnahmen von der CAC-Sicherheitsbewertung

Nach § 8 der CAC-Bestimmungen ist in den folgenden Fällen zwar keine CAC-Sicherheitsbewertung erforderlich, aber der Datenverarbeiter muss entweder die Zertifizierung erhalten oder einen CAC-Standardvertrag mit dem Datenempfänger im Ausland abgeschlossen haben:

1. grenzüberschreitende Übermittlung personenbezogener Daten von insgesamt mehr als 100.000, aber weniger als einer Million Betroffenen (ausschließlich sensible personenbezogener Daten) seit dem 1. Januar eines Jahres;

2. grenzüberschreitende Übermittlung von sensiblen personenbezogenen Daten von weniger als 10.000 Betroffenen seit dem 1. Januar eines Jahres.

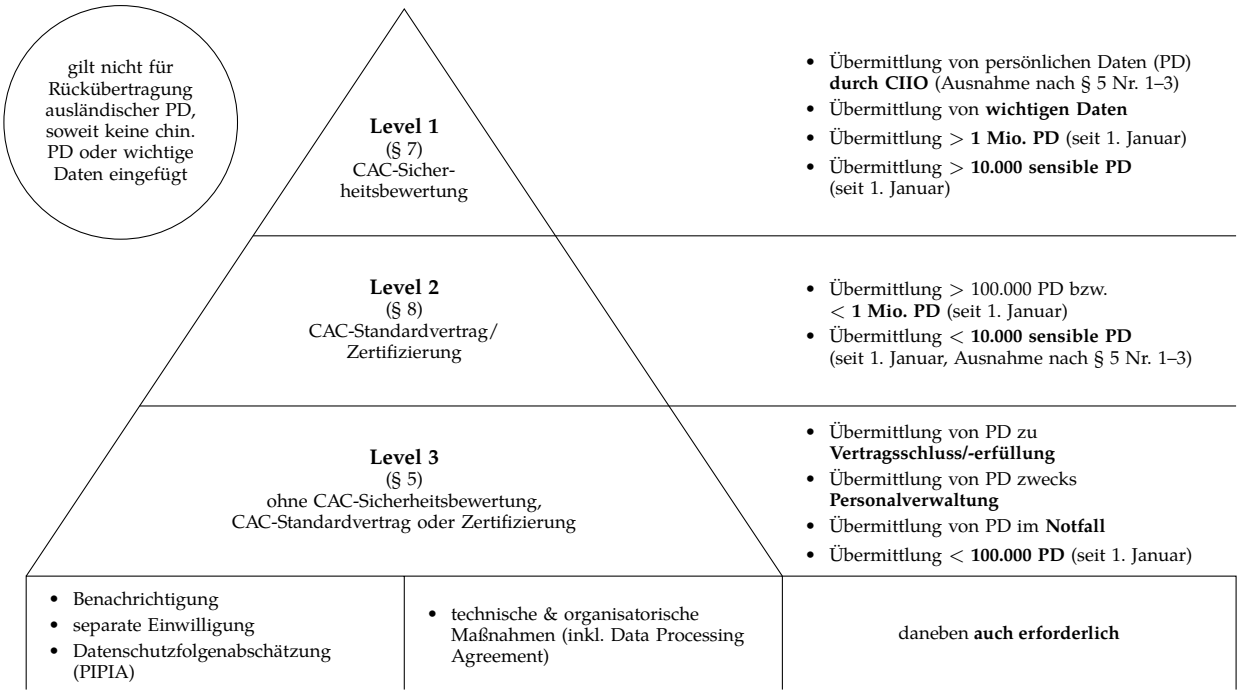
Hierbei ist zu beachten, dass die oben genannten Ausnahmen gemäß § 7 CAC-Bestimmungen unter folgenden Umständen (Rückausnahmen) nicht gelten und damit eine CAC-Sicherheitsbewertung durchlaufen werden muss:

1. grenzüberschreitende Übermittlung von personenbezogenen Daten durch CIIOs (außer in den Fällen des § 5 Abs. 1 Nr. 1 bis 3 CAC-Bestimmungen);

[6] Ausführlicher zu diesen „Drei Voraussetzungen" siehe *Rainer Burkardt / Ondřej Zapletal*, How to Transfer Your Data Out of China, in German Chamber Ticker Winter 2022, abrufbar unter <https://www.bktlegal.com> (<https://perma.cc/EY3L-DHQG>).

[7] *Rainer Burkardt/Ondřej Zapletal*, Anmerkungen zum Entwurf der CAC-Bestimmungen zur Regulierung und Förderung des grenzüberschreitenden Datenverkehrs: Kommen die erhofften Ausnahmen von den bestehenden strengen GSPD-Regelungen? ZChinR 1/2024, S. 49 f.

[8] Chinesisch: 确需, wörtlich: wirklich notwendig.



Grafik 1: CAC-Bestimmungen zur Regulierung und Förderung des grenzüberschreitenden Datenverkehrs vom 22. März 2024

2. grenzüberschreitende Übermittlung von wichtigen Daten;

3. grenzüberschreitende Übermittlung von personenbezogenen Daten von mehr als einer Million Betroffenen (ausschließlich sensibler personenbezogener Daten) oder von sensiblen personenbezogenen Daten von mehr als 10.000 Betroffenen seit dem 1. Januar eines Jahres.

Die oben stehende Grafik fasst die Anforderungen für die grenzüberschreitende Datenübermittlung nach den CAC-Bestimmungen zusammen.

V. Ausnahme für Pilot-Freihandelszonen

Nach § 6 Abs. 1 der CAC-Bestimmungen dürfen Pilot-Freihandelszonen in China in Übereinstimmung mit den einschlägigen Bestimmungen zum nationalen Sicherheitsmanagement für grenzüberschreitende Datenexporte eigene Listen von Daten erstellen, deren grenzüberschreitende Übermittlung den „Drei Voraussetzungen" unterliegt (Negativlisten).

Solche Negativlisten bedürfen der vorherigen Genehmigung durch die Provinzkommission für Netzsicherheit und Informatisierung und müssen bei der CAC auf nationaler Ebene eingereicht werden.

Datenverarbeiter in einer Pilot-Freihandelszone, die Daten aus China ins Ausland übermitteln, welche nicht in den Negativlisten aufgeführt sind, sind gemäß § 6 Abs. 2 CAC-Bestimmungen von den „Drei Voraussetzungen" befreit und müssen bei der Übermittlung dieser Daten ins Ausland weder die CAC-Sicherheitsbewertung beantragen noch die Zertifizierung bestehen und auch keinen CAC-Standardvertrag abschließen.

VI. Verbesserungen in den CAC-Bestimmungen im Vergleich zum Entwurf

Obwohl die CAC-Bestimmungen immer noch einige Fragen aufwerfen, sind die neuen CAC-Bestimmungen im Vergleich zum Entwurf juristisch präziser formuliert, verweisen explizit auf die höherrangigen Gesetze, schließen stellenweise im Entwurf enthaltene Gesetzeslücken und klären einige der im Artikel zum Entwurf[9] aufgeworfenen Fragen. Folgende Verbesserungen sind erwähnenswert:

1. Expliziter Verweis auf die drei höherrangigen Gesetze

Obwohl die Frage der Zuständigkeit von CAC und der Konflikt des nachrangigen § 5 der CAC-Bestimmungen mit dem höherrangigen § 38 GSPD nicht gelöst wurde, verweisen die CAC-Bestimmungen in § 1 nun explizit auf das Cybersicherheitsgesetz[10], das Datensicherheitsgesetz[11] und das GSPD, was darauf schließen lässt, dass diese im Konfliktfall vorgehen.

2. Angleichung der Schwellenwerte für die CAC-Sicherheitsbewertung

Die Schwellenwerte für die CAC-Sicherheitsbewertung wurden an die in den „Maßnahmen zur Si-

[9] *Rainer Burkardt / Ondřej Zapletal* (Fn. 7), S. 49 f.

[10] 中华人民共和国网络安全法 vom 7.11.2016, chinesisch-deutsch abgedruckt in: ZChinR 2018, S. 113 ff.

[11] 中华人民共和国数据安全法 vom 10.6.2021, chinesisch-englisch abrufbar unter <lawinfochina.com> (北大法律英文网)/<pkulaw.cn> (北大法宝), Indexnummer (法宝引证码) CLI.1.5015167.

cherheitsbewertung der grenzüberschreitenden Datenübermittlung“[12] („Maßnahmen zur CAC-Sicherheitsbewertung“) angeglichen und folglich von 10.000 auf 100.000 erhöht.

3. Abgrenzung von personenbezogenen Daten und sensiblen personenbezogenen Daten

Die CAC-Bestimmungen unterscheiden nun explizit zwischen personenbezogenen Daten und sensiblen personenbezogenen Daten und sehen in § 5 Nr. 4, § 7 Nr. 2 und § 8 Abs. 1 nun vor, dass sensible personenbezogene Daten bei der Berechnung der personenbezogenen Daten nicht einzuziehen sind.

4. Neue Schwellenwerte für sensible personenbezogene Daten

In den §§ 7 und 8 legen die CAC-Bestimmungen sensible personenbezogene Daten von 10.000 Personen neu als Schwellenwert für sensible personenbezogene Daten fest.

5. Klarstellung der vorrangigen Anwendung von Ausnahmen und Schwellenwerten

Die CAC-Bestimmungen lösen durch die neuen Regelungen in § 7 Abs. 2 und § 8 Abs. 2 die sich aus dem Entwurf ergebende Frage, ob die Ausnahmen in § 5 Abs. 1 Nr. 1 bis 3 Anwendungsvorrang vor den jeweiligen Schwellenwerten haben und somit unabhängig von der Anzahl der ins Ausland übermittelten personenbezogenen Daten gelten. Die CAC-Bestimmungen regeln nun explizit, dass die Ausnahmen in § 5 sowie die Tatbestände nach den §§ 3, 4, 5 und 6 vorrangig vor den Ausnahmen bzw. Schwellenwerten in den §§ 7 und 8 anzuwenden sind. Dies hat unter anderem zur Folge, dass beispielsweise ein Unternehmen die Anzahl der Mitarbeiter, die unter die Ausnahmen des § 5 Abs. 1 Nr. 2 CAC-Bestimmungen fallen, nicht in die Gesamtzahl der Personen einbeziehen muss, deren personenbezogene Daten von dem Unternehmen ins Ausland übermittelt werden sollen.

VII. Offene Fragen und Herausforderungen

1. Fehlende Definition von CIIO und wichtigen Daten

Trotz der vorstehend dargestellten Verbesserungen in den neuen CAC-Bestimmungen bleiben weiterhin einige Fragen offen. Die CAC-Bestimmungen verwenden, definieren aber einige wichtige Begriffe nicht, einschließlich „CIIO“ oder „wichtige Daten“, was die Anwendung der Ausnahmen in der unternehmerischen Praxis erschwert.

Nach § 2 der „Verordnung für den Schutz kritischer Informationsinfrastrukturen“[13] („CIIO-Verordnung“) bezieht sich der Begriff „CIIO“ auf „wichtige Branchen und Bereiche wie etwa die öffentlichen Kommunikations- und Informationsdienste, die Energie-, Transport- und Wasserwirtschaft, das Finanzwesen, den öffentlichen Dienst, die elektronischen Behördendienste, die Landesverteidigung und die Wissenschafts- und Technologieindustrie sowie andere wichtige Einrichtungen wie etwa Netzwerkeinrichtungen und Informationssysteme, die bei Schädigung, Funktions- oder Datenverlust die nationale Sicherheit, Volkswirtschaft und den Lebensunterhalt der Bevölkerung oder die öffentlichen Interessen ernsthaft gefährden können“.

Obwohl die Abgrenzung der CIIO von anderen Unternehmen nach der vorstehenden Definition unklar ist, spielt die fehlende bzw. unklare Definition in der Praxis eine nur untergeordnete Rolle. Wie von der CIIO-Verordnung vorgesehen, informieren die für die Kategorisierung eines Unternehmens als CIIO zuständigen Behörden ein Unternehmen, wenn dies nach der CIIO-Verordnung als CIIO einzustufen ist. Soweit ein Unternehmen daher nicht von den Behörden als CIIO eingestuft und entsprechend informiert wurde, können Unternehmen bis auf Weiteres davon ausgehen, dass sie keine CIIO sind.

Praxisrelevanter für KMU ist die Abgrenzung von wichtigen und sonstigen Daten, denn bei der Übermittlung von wichtigen Daten ins Ausland gelten die Ausnahmen der CAC-Bestimmungen nicht, § 5 Abs. 2 und § 7 CAC-Bestimmungen. Eine wenn auch sehr allgemeine Definition von wichtigen Daten befindet sich in § 19 der Maßnahmen zur CAC-Sicherheitsbewertung. Nach dieser Definition sind wichtige Daten „Daten, die nach ihrer Manipulation, Zerstörung, Weitergabe, unrechtmäßigen Erlangung oder unrechtmäßigen Verwendung die nationale Sicherheit, die Wirtschaft, die soziale Stabilität, die öffentliche Gesundheit und Sicherheit usw. gefährden können“.

Das Fehlen einer konkreten Definition von wichtigen Daten wird zukünftig dadurch ausgeglichen, dass die dafür zuständigen Behörden wichtige Daten als solche öffentlich bekannt gegeben müssen, § 2 Satz 2 CAC-Bestimmungen. Diese Pflicht zur Bestimmung von wichtigen Daten steht im Einklang mit § 21 Abs. 1 Satz 2 Datensicherheitsgesetz, nach dem die Behörden Kataloge wichtiger Daten für bestimmte Sektoren erlassen. Zum Datum der Veröffentlichung dieses Beitrags waren den Verfassern jedoch noch keine Kataloge von wichtigen Daten bekannt. Am 15. März 2024 hat die CAC die ersten nationalen Standards zur Datenklassifizierung (GB/T 43697-2024) erlassen, welche die Grundsätze und die Methoden für die Identifizierung der Klassifizierung von wichtigen und anderen Daten

[12] § 4 Nr. 3 Maßnahmen zur Sicherheitsbewertung der grenzüberschreitenden Datenübermittlung (数据出境安全评估办法) vom 7.7.2022, Webseite der Cyberspace Administration of China, chinesischer Text abrufbar unter <http://www.cac.gov.cn> (<https://perma.cc/K6JG-7B2V>).

[13] § 2 Verordnung für den Schutz kritischer Informationsinfrastrukturen (关键信息基础设施安全保护条例) vom 30.7.2021, Webseite der Regierung der Volksrepublik China, chinesischer Text abrufbar unter <https://www.gov.cn> (<https://perma.cc/QC26-55XG>).

enthalten.[14] Es ist daher davon auszugehen, dass die Behörden zeitnah Kataloge mit wichtigen Daten veröffentlichen werden.

2. Klassifizierung und Berechnung von (sensiblen) personenbezogenen Daten

Eine weitere praktische Herausforderung für KMU ist die Klassifizierung und Berechnung von personenbezogenen und sensiblen personenbezogenen Daten.

Personenbezogene Daten sind nach § 4 Abs. 1 GSPD alle Arten von Informationen in Bezug auf identifizierte oder identifizierbare natürliche Personen, die elektronisch oder anderweitig aufgezeichnet sind. § 28 Abs. 1 GSPD definiert sensible personenbezogene Daten als Daten, die im Falle einer Offenlegung oder einer illegalen Verwendung zu Diskriminierung[15], Sicherheitsbedrohung des Betroffenen oder Beschädigung des Eigentums[16] führen können.

Sensible personenbezogene Daten sind z. B. medizinische Daten, biometrische Daten, Finanzkonten, Daten über den Aufenthaltsort und andere personenbezogenen Daten. Beachtenswert ist, dass chinesische Personalausweise als sensible personenbezogene Daten betrachtet werden, einschließlich der Ausweisnummer, welche das Geburtsdatum und verschlüsselt den Geburtsort enthält. Der vom Nationalen technischen Ausschuss für die Normung der Netzsicherheit herausgegebene Standard „Informationssicherheitstechnik: Normung der Sicherheit persönlicher Daten (GB/T 35273-2020)“[17] bietet genauere Anleitungen zur Identifizierung (sensibler) personenbezogener Daten.

Was den Zeitraum für die Berechnung der Anzahl der ins Ausland übermittelten personenbezogenen Daten anbelangt, so bestimmen die CAC-Bestimmungen den 1. Januar eines Jahres als Anfangszeitpunkt für den Berechnungszeitraum, ohne jedoch dessen Ende zu spezifizieren. Im Rahmen der Pressekonferenz zum Anlass der Bekanntmachung der CAC-Bestimmungen hat die CAC angekündigt, dass sich der einschlägige Zeitraum vom 1. Januar eines Jahres bis zum Datum der Anmeldung zur CAC-Sicherheitsbewertung erstreckt.[18] Dem Wortlaut der CAC-Bestimmungen kann man entnehmen, dass der Berechnungszeitraum spätestens am 31. Dezember des laufenden Jahres endet und die Zahlen der ins Ausland übermittelten Daten folglich mit Beginn des folgenden Jahres neu zu berechnen sind.

Darüber hinaus ist zu beachten, dass sich die CAC-Bestimmungen auf die Anzahl der Betroffenen und nicht auf die Anzahl der personenbezogenen Daten als Grundlage für die Berechnung der Anzahl der personenbezogenen Daten beziehen. Für die Berechnung ist deshalb die Anzahl der Dateninhaber, deren personenbezogene Daten ins Ausland übermittelt werden, maßgeblich und nicht die Anzahl der in den einzelnen Datensätzen enthaltenen personenbezogenen Daten.

VIII. Fazit und Empfehlungen

Die CAC-Bestimmungen beseitigen einige Unklarheiten und lockern die aktuell strengen Voraussetzungen beim grenzüberschreitenden Datentransfer. Für die meisten KMU beschränken sich die Lockerungen jedoch hauptsächlich auf die in § 5 CAC-Bestimmungen genannten Ausnahmen und sind daher nicht so umfangreich, wie es auf den ersten Blick erscheint und in den Medien dargestellt wurde.

Von Vorteil ist, dass nach der Erfahrung der Autoren die meisten KMU unter dem Schwellenwert des § 5 Abs. 1 Nr. 4 CAC-Bestimmungen liegen, da diese in der Regel in einem Kalenderjahr personenbezogene Daten von weniger als 100.000 Personen ins Ausland übermitteln.

Für den Fall, dass sensible personenbezogene Daten ins Ausland übertragen werden sollen, müssen die KMU als Datenverarbeiter grundsätzlich weiterhin vor der grenzüberschreitenden Datenübermittlung eine der zwei Voraussetzungen (Zertifizierung / CAC-Standardvertrag) nach § 8 CAC-Bestimmungen erfüllen. In diesem Fall ist für KMU regelmäßig der CAC-Standardvertrag wegen geringerer Kosten und klareren Regelung die bessere Option.

Darüber hinaus ist zu beachten, dass eine Befreiung von den „Drei Voraussetzungen“ keine Befreiung von den weiteren Pflichten nach dem GSPD darstellt. Diese grundlegenden Pflichten werden in den §§ 10 und 11 der CAC-Bestimmungen klargestellt. Danach müssen Datenverarbeiter vor der Übermittlung personenbezogener Daten ins Ausland u. a.:

- ihre Benachrichtigungspflichten gegenüber dem Betroffenen, z. B. im Rahmen einer Datenschutzerklärung (Privacy Policy), erfüllen,
- eine qualifizierte Einwilligung des Betroffenen einholen,
- eine Datenschutzfolgenabschätzung (Personal Information Impact Assessment – PIPIA) durchführen und
- technische organisatorische Maßnahmen (TOMs) inklusive des Abschlusses einer Datenverarbei-

[14] Information Security Technology – Rules for data classification and grading (GB/T 43697-2024) (数据安全技术：数据分类分级规则) vom 21.3.2024, Webseite des Nationalen Technischen Ausschusses für die Normung der Netzsicherheit (SAC/TC260), chinesisch abrufbar unter <https://www.tc260.org.cn> (<https://perma.cc/7KF5-XSGW>).

[15] Chinesisch: 人格尊严受到侵害, wörtlich: Verletzung der Würde der Persönlichkeit.

[16] Chinesisch: 人身、财产安全受到危害, wörtlich: Gefährdung der Sicherheit einer Person oder des Vermögens.

[17] Information Security Technology – Personal Information Security Specification (GB/T 35273-2020) (信息安全技术：个人信息安全规范) vom 6.3.2020, Webseite des Nationalen Technischen Ausschusses für die Normung der Netzsicherheit (SAC/TC260), englische Übersetzung abrufbar unter <https://www.tc260.org.cn> (<https://perma.cc/AW8V-JLMJ>).

[18] Fragen und Antworten zu den CAC-Bestimmungen (《促进和规范数据跨境流动规定》答记者问) vom 22.3.2024, Webseite des CAC, Cyberspace Administration of China, chinesischer Text abrufbar unter <https://www.cac.gov.cn> (<https://perma.cc/6YPA-VS4B>).

tungsvereinbarung zwischen dem Datenverarbeiter und dem Datenempfänger im Ausland ergreifen.

Die Möglichkeit, bei der Übermittlung personenbezogener Daten ins Ausland auf den CAC-Standardvertrag zu verzichten, stellt somit nur eine kleine Erleichterung des mit dem grenzüberschreitenden Datentransfer verbundenen Gesamtarbeitsaufwands dar.

Um zu ermitteln, ob und welche der vorstehenden Pflichten erfüllt werden müssen, sollten Unternehmen zunächst ein sogenanntes „Datenmapping" vornehmen. Dieses versetzt einen Datenverarbeiter in die Lage, analysieren zu können, wie viele und welche Daten an welchem Ort gespeichert sowie welche Daten ins Ausland übermittelt werden.

Aufgrund der Komplexität empfiehlt es sich, dieses in Zusammenarbeit und mit Unterstützung von Experten durchzuführen. Im Idealfall haben die externen Experten im Rahmen des Datenmapping keinen Zugriff auf die Daten des Unternehmens, damit keine „Weitergabe von personenbezogenen Daten" vorliegt und die damit verbundenen Pflichten nicht ausgelöst werden.

* * *

Do the CAC's Provisions on Promoting and Regulating Cross-border Data Flows relieve SMEs from China's strict data-protection regime?

The Cyberspace Administration of China's Provisions on Promoting and Regulating Cross-border Data Flows (the "CAC Provisions") contain long-awaited exceptions for the cross-border transfer of personal data out of China.

This article summarizes the CAC Provisions, explains their practical implications for SMEs in China, and highlights the conditions under which SMEs can make use of the exceptions in the CAC Provisions to effect outbound data transfers.

It also compares the final CAC Provisions with the draft of September 28, 2023, showing which of the issues left unresolved in the draft are addressed in the final version of the Provisions. Finally, the article discusses and provides recommendations on the challenges SMEs face in complying with the legal requirements.