

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

Artikel von Burkardt & Partner, 22. April 2024

I. Einführung

Mehr als zwei Jahre nach der Verabschiedung des *Gesetzes zum Schutz personenbezogener Daten* („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 *Bestimmungen zur Regulierung und Förderung des grenzüberschreitenden Datenverkehrs* („CAC-Bestimmungen“), welche am selben Tag in Kraft getreten sind, veröffentlicht.

Die CAC-Bestimmungen enthalten die seit langem erwarteten Ausnahmen für die grenzüberschreitende Übermittlung von personenbezogenen Daten ins chinesische Ausland und stellen, insbesondere für KMU, welche nur geringe Mengen personenbezogener Daten verarbeiten und ins chinesische Ausland übertragen, eine Lockerung des strengen Regimes nach dem GSPD dar.

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. Zum Abschluss stellen die Autoren die Herausforderungen für KMU bei der Erfüllung der gesetzlichen Anforderungen dar und geben Empfehlungen für deren Compliance-Praxis.

II. Ausnahme von den Drei Voraussetzungen für „Re-Exporte“ personenbezogener Daten nach Art. 4

Die CAC-Bestimmungen enthalten 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 Art. 38 GSPD erfüllen, d.h. es ist weder eine CAC-Sicherheitsbewertung noch eine Zertifizierung und auch kein CAC-Standardvertrag (im Folgenden gemeinsam die „Drei Voraussetzungen“) erforderlich.

Diese Ausnahme gilt 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 nach Art. 5

Eine der für KMU in China wichtigsten und, wie in unserem [Artikel zum Entwurf](#) kommentiert, auch kontroversesten Regelungen ist die Regelung in Art. 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) Erforderliche Übermittlung von personenbezogenen Daten ins Ausland, wenn dies für den **Abschluss oder die Erfüllung eines Vertrages** erforderlich ist, dessen Vertragspartei der Betroffene (natürliche Person, deren personenbezogenen Daten verarbeitet werden, Anm. d. Verf.) ist, wie z. B. bei Kaufverträgen, Postversand, Geldüberweisungen, Flug- und Hotelreservierungen, Visumanträge, Prüfungsdienste;

(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, Anm. d. Verf.) seit dem 1. Januar eines Jahres durch Datenverarbeiter, welche keine Betreiber kritischer Informationsinfrastrukturen (Critical Infrastructure Operator „CIIO“) sind.

Bei den Ausnahmen gemäß Art. 5 ist zu beachten, dass die Ausnahme für Vertragsschluss/-erfüllung unter Nr. (1) nur für Verträge gilt, dessen Vertragspartei der Betroffene ist. Dies legt den Schluss nahe, dass Art. 5 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 bspw. in Verträgen zwischen chinesischen Tochtergesellschaften und deren Muttergesellschaften in Europa enthalten sind, nicht unter diese Ausnahmen.

Weiter stellt sich bei der Ausnahme unter Nr. (2) die Frage, ob nur die ausdrücklich erwähnten Kollektivarbeitsverträge oder auch individuelle Arbeitsverträge unter die Ausnahme fallen.

Die Notfallausnahme unter Nr. (3) ist für die Übermittlung von personenbezogenen Daten im alltäglichen Betrieb von KMU von geringer praktischer Relevanz.

Darüber hinaus verlangen die Ausnahmen in Nr. (1) und Nr. (2), dass die Datenübertragung „erforderlich“ 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 Art. 8

Nach Art. 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 1 Million** Betroffenen (ausschließlich sensibler personenbezogener Daten, Anm. d. Verf.) 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.

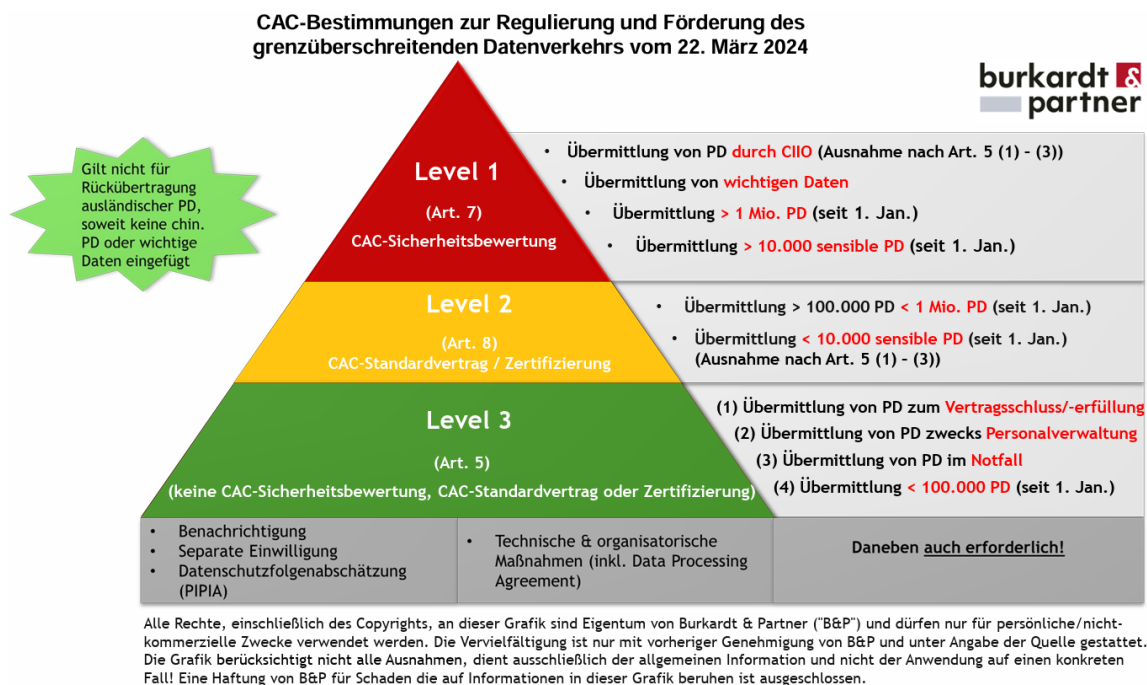
Hierbei ist zu beachten, dass die oben genannten Ausnahmen unter folgenden Umständen (Rückausnahmen) nicht gelten und damit eine CAC-Sicherheitsbewertung durchlaufen werden muss:

(1) Grenzüberschreitende Übermittlung von personenbezogenen Daten durch CIIOs (außer in den Fällen des Art. 5 Abs. I. Nr. (1) bis (3));

(2) Grenzüberschreitende Übermittlung von wichtigen Daten;

(3) Grenzüberschreitende Übermittlung von personenbezogenen Daten **von mehr als 1 Million Betroffenen** (ausschl. sensibler personenbezogener Daten, Anm. d. Verf.) oder **von sensiblen personenbezogenen Daten von mehr als 10.000 Betroffenen** seit dem 1. Januar eines Jahres.

Die nachstehende Grafik fasst die Anforderungen für die grenzüberschreitende Datenübermittlung nach den CAC-Bestimmungen zusammen:



V. Offene Fragen und Herausforderungen

1) Fehlende Definition von CIIO und wichtigen Daten

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 in unserem [Artikel zum Entwurf](#) aufgeworfenen Fragen. Trotz der Verbesserungen in den neuen CAC-Bestimmungen bleiben weiterhin einige Fragen offen.

Die CAC-Bestimmungen verwenden, definieren aber nicht einige wichtige Begriffe, einschl. „CIIO“ oder „wichtige Daten“, was die Anwendung der Ausnahmen in der unternehmerischen Praxis erschwert.

Nach der Verordnung für den Schutz kritischer Informationsinfrastrukturen („CIIO-Verordnung“) bezieht sich der Begriff „CIIO“ auf *“Unternehmen in wichtigen Industrien, die bei Schädigung, Funktions- oder Datenverlust die nationale Sicherheit, Volkswirtschaft und 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 weiteren davon ausgehen, dass diese 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. Eine wenn auch sehr allgemeine Definition von wichtigen Daten befindet sich in den 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 bekanntgegeben müssen. Diese Pflicht zur Bestimmung von wichtigen Daten steht im Einklang mit Art. 21 Datensicherheitsgesetz, nach dem die Behörden Kataloge wichtiger Daten für bestimmte Sektoren erlassen sollen. 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 von Klassifizierung von wichtigen und anderen Daten enthalten. 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 dem GSPD alle Arten von Informationen in Bezug auf identifizierte oder identifizierbare natürliche Personen, die elektronisch oder anderweitig aufgezeichnet sind. Das GSPD definiert sensible personenbezogene Daten als Daten, die im Falle einer Offenlegung oder einer illegalen Verwendung zu Diskriminierung, Sicherheitsbedrohung des Betroffenen oder Beschädigung des Eigentums 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. Die *Information Security Technology - Personal Information*

Security Specification (GB/T 35273-2020), 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 Veröffentlichung 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.¹ 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-Bestimmung 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 Datensätze enthaltenen personenbezogenen Daten.

VI. Fazit & 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 Art. 5 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 Art. 5 Abs. 1 Nr. (4) 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 jedoch weiterhin vor der grenzüberschreitenden Datenübermittlung eine der zwei Voraussetzungen (Zertifizierung/CAC-Standardvertrag) nach Art. 8 erfüllen, da der grenzüberschreitende Transfer von sensiblen personenbezogenen Daten nicht unter die Ausnahmetatbestände des Art. 5 Abs. 1 Nr. (1) bis (3) fallen. In diesem Fall ist für KMU regelmäßig der CAC-Standardvertrag wegen geringerer Kosten und klarerer 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 Art. 10 und Art. 11 der CAC-Bestimmungen klargestellt. Danach müssen Datenverarbeiter vor der Übermittlung personenbezogener Daten ins Ausland u.a.:

- Deren Benachrichtigungspflichten ggü. dem Betroffenen erfüllen,
- Eine qualifizierte Einwilligung des Betroffenen einholen,
- Eine Datenschutzfolgenabschätzung (Personal Information Impact Assessment – PIPIA) durchführen, und
- Technische organisatorische Maßnahmen (TOMs), inkl. des Abschlusses einer Datenverarbeitungsvereinbarung 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.

¹ https://www.cac.gov.cn/2024-03/22/c_1712776611649184.htm

Um zu ermitteln, ob und welche der vorstehenden Pflichten erfüllt werden müssen, sollten Unternehmen zunächst ein sog. „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 ausgelöst werden. Burkardt & Partner hat eine effiziente Methode entwickelt, welche im Rahmen des Datenmapping eine zuverlässige Datenklassifizierung und Quantifizierung ohne Zugriff auf Unternehmensdaten ermöglicht.

Sollten Sie bei der Durchführung Ihres Datenmappings, der Durchführung Ihrer Datenschutzfolgenabschätzung, der Erstellung einer Datenschutzerklärung (Privacy Policy) für Ihre Website, dem Entwerfen einer Einwilligungserklärung und einer Datenverarbeitungsvereinbarung sowie anderen datenschutzrechtlichen Belangen in China Unterstützung benötigen, so steht Ihnen Burkardt & Partner mit Rat und Tat zur Seite.

Kontaktieren Sie uns gerne unter info@BKTlegal.com für unverbindliches Gespräch!

Mehr Informationen über unsere Kanzlei und unsere Expertise im chinesischen Datenschutzrecht finden Sie auf unserer Webseite unter www.bktlegal.com.



BURKARDT & PARTNER RECHTSANWÄLTE

Suite 1706, Five Corporate Avenue, No. 150 Hubin Road, Shanghai 200021, P.R. China
中国上海湖滨路150号企业天地5号楼1706室, 邮编: 200021

WEBSITE www.BKTlegal.com
OFFICE +86 (21) 6321 0088

CONNECT WITH US ON [LinkedIn](#)

Dieser Beitrag ist die gekürzte Fassung unseres in der [Zeitschrift für Chinesisches Recht](#) veröffentlichten Artikels.