datenschutz-berater.de

45. Jahrgang DSB 12/2021

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Stichwort des Monats

Datenschutz im Fokus

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Rainer Burkardt und Jürgen Recha

Das neue chinesische Datenschutzrecht und die europäische DSGVO im Rechtsvergleich

Am 1.9.2021 ist das Gesetz zum Schutz personenbezogener Daten der Volksrepublik China („GSPD") in Kraft getreten. Ähnlich wie die DSGVO, zielt das GSPD u. a. darauf ab, personenbezogene Daten und Personen, auf die sich diese beziehen, zu schützen und gesetzliche Standards für Verarbeitungen personenbezogener Daten festzulegen. Dieser Beitrag gibt einen Überblick zu den Regelungen in der Volksrepublik China („VR China" oder „China") und erläutert ausgewählte Gemeinsamkeiten und Unterschiede im Vergleich zur DSGVO.

Dem Schutz von personenbezogenen Daten wurde in der VR China lange Zeit keine Aufmerksamkeit zuteil und personenbezogene Daten wurden gesetzlich nur unzureichend geschützt, bspw. im Rahmen des Reputationsschutzes nach den Allgemeinen Grundsätzen des Zivilrechts und des Privatrechtsschutzes nach dem Delikthaftungsrecht. Erst im Cybersicherheitsgesetz (in Kraft seit dem 1.6.2017) wurde dem Schutz von Daten mehr Aufmerksamkeit geschenkt. Da elektronische Daten und deren Kontrolle in modernen Geschäftsmodellen eine immer größere Rolle spielen, hat die VR China die Gesetzeslage den wirtschaftlichen, aber vor allem den staatlichen Erfordernissen schnell angepasst und innerhalb nur eines Jahres zwei neue Datenschutzgesetzte erlassen und mit dem 4. Buch des Zivilgesetzbuches zum ersten Mal Persönlichkeitsrechte definiert.

Anders als Deutschland besitzt China kein vereinheitlichtes Gesetzeswerk für das Recht auf Schutz von personenbezogenen Daten. Auch nach dem Inkrafttreten des GSPD sind datenschutzrechtliche Normen in mehreren sich überschneidenden Gesetzen enthalten. Das GSPD ist jedoch die wichtigste und umfassendste Vorschrift für den Schutz personenbezogener Daten in China. Zusammen mit dem Cybersicherheitsgesetz, dem am 1.9.2021 in Kraft getretenen Datensicherheitsgesetz und dem am 1.1.2021 in Kraft getretenen 4. Buch des Zivilgesetzbuches bildet das GSPD ein umfassendes Regelungswerk zum Schutz von Daten in China.

Das GSPD gilt grundsätzlich für alle Datenverarbeiter (Individuen und Organisationen, einschließlich der ausländisch investierten Unternehmen) in der VR China. Aufgrund der grenzüberschreitenden Wirkung können dem GSPD auch Unternehmen außerhalb Chinas unterliegen, die persönliche Daten von natürlichen Personen innerhalb Chinas mit dem Zweck verarbeiten, natürlichen Personen in China Produkte oder Dienstleistungen anzubieten oder das Verhalten natürlicher Personen in China zu analysieren oder zu bewerten. Das entspricht der Regelung aus Art. 3 Abs. 2 DSGVO.

Obwohl das GSPD in vielerlei Hinsicht der DSGVO ähnelt, reicht es für ein gesetzmäßiges Handeln nicht aus, die für die Einhaltung der DSGVO im deutschen Unternehmen getroffenen Maßnahmen einfach auf die chinesische Tochtergesellschaft zu übertragen. Darum ist es erforderlich, dass Unternehmen, die Geschäfte in oder mit China betreiben, deren Datenschutzmaßnahmen anpassen, um den Datenschutzanforderungen des GSPD nachzukommen.

Dabei sind insbesondere die nachstehend beschriebenen Unterschiede zwischen GSPD und DSGVO zu beachten:

	GSPD	DSGVO
Rechtsgrundlagen für die Verarbeitung personenbezogener Daten	Art. 13 GSPD sieht folgende Rechtsgrundlagen für die Datenverarbeitung vor: • Aktive Zustimmung der/s Betroffenen • Vertragliche Verpflichtung • Gesetzliche Verpflichtung • Abwehr von Gefahren für die öffentliche Gesundheit und im Notfall zum Schutz von Leben, Gesundheit oder Eigentum • Öffentliches Interesse • Verarbeitung von freiwillig öffentlich bekannt gegebenen personenbezogenen Daten in angemessenem Umfang	Art. 6 DSGVO sieht folgende Rechtsgrundlagen für die Datenverarbeitung vor: • Einwilligung der/s Betroffenen • Vertragliche Verpflichtung oder vorvertragliche Maßnahme • Gesetzliche Verpflichtung • Schutz von lebensnotwendigen Interessen • Öffentliches Interesse • Berechtigtes Interesse

	GSPD	DSGVO
Rechte der/des Betroffenen	Rechte nach Art. 44 ff. GSPD (Auszug): • Auskunft • Zugang und Kopieren • Widerruf der Einwilligung • Berichtigung • Datenübertragung • Einschränkung • Ablehnung • Löschung	Rechte nach Art. 12 ff. DSGVO (Auszug): • Auskunft • Widerruf der Einwilligung • Berichtigung • Datenübertragung • Widerspruchsrecht • Einschränkung • Löschung
Sensible Daten nach dem GSPD und besondere Kategorien personenbezogener Daten nach der DSGVO	Art. 28 GSPD Daten, die im Falle einer Offenlegung oder einer illegalen Verwendung zu Diskriminierung, Sicherheitsbedrohung des Einzelnen oder Beschädigung des Eigentums führen können, wie: • Religiöse Überzeugungen • Medizinische Daten • Biometrische Daten • Bestimmte Identitäten • Finanzkonten • Daten über den Aufenthaltsort • Personenbezogene Daten von Jugendlichen unter 14 Jahren • Andere personenbezogenen Daten. Das GSPD stellt strengere Anforderungen an den Schutz von sensiblen Daten.	Art. 9 DSGVO Daten, die ein hohes Risiko für die Person bedeuten können, wie: • Rassische und ethnische Herkunft • Politische Meinungen • Religiöse und philosophische Überzeugung • Gewerkschaftszugehörigkeit • Gesundheit • Sexualleben • Genetische und biometrische Angaben Die Verarbeitung personenbezogener Daten aus besonderen Kategorien ist nur in den von der DSGVO vorgesehenen Fällen erlaubt.
Separate Einwilligung	Art. 23, 25, 29, 39 GSPD Separate Einwilligung ist erforderlich für: • Bereitstellung von Daten an Dritte • Veröffentlichung von Daten • Verarbeitung von sensiblen Daten • Bereitstellung von Daten im Ausland	Art. 7 DSGVO • Separate Einwilligung muss für verschiedene Verarbeitungszwecke und -vorgänge abgegeben werden
Voraussetzungen für die Benennung einer für den Datenschutz verantwortlichen Person/einer/s „Datenschutz-beauftragten“	Art. 52 GSPD Datenverarbeiter müssen eine für den Datenschutz verantwortliche Person (“data protection officer“) benennen, wenn die Menge der verarbeiteten personenbezogenen Daten einen von der der Cyberspace Administration of China („CAC“) festgelegten Schwellenwert überschreitet.	Art. 37 DSGVO Datenverarbeiter müssen eine/n Datenschutzbeauftragte/n benennen, wenn die Kerntätigkeit der/s Verantwortlichen oder der Auftragsverarbeiter • In der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder • In der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten besteht.
Compliance Audits	Art. 54 GSPD Datenverarbeiter haben die Rechtsmäßigkeit der Datenverarbeitung regelmäßig zu prüfen.	Art. 32 Abs. 1 lit. d) DSGVO Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen Verantwortliche und Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, z. B.: d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

	GSPD	DSGVO
Voraussetzungen für die Durchführung der Datenschutzfolge-abschätzung	Art. 55 GSPD Die Durchführung der Datenschutz-Folgenabschätzung ist verpflichtend für: • Verarbeitung sensibler personenbezogener Daten • Verwendung personenbezogener Daten für automatisierte Entscheidungen • Beauftragung anderer mit der Verarbeitung personenbezogener Daten • Weitergabe personenbezogener Daten an andere Datenverarbeiter • Veröffentlichung personenbezogener Daten • Bereitstellung personenbezogener Daten im Ausland und • Sonstige Verarbeitungen personenbezogener Daten, die einen wesentlichen Einfluss auf die Rechte und Interessen von Personen haben.	Art. 35 Abs. 1 DSGVO Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Eine Datenschutz-Folgenabschätzung ist u. a. in folgenden Fällen erforderlich: • Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen; • Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.
Voraussetzungen für die Bereitstellung von personenbezogenen Daten im Ausland	Art. 38, 39 GSPD Für die Bereitstellung von personenbezogenen Daten im Ausland müssen folgende Bedingungen kumulativ erfüllt werden: • Erfüllung der Informationspflicht gegenüber dem Betroffenen (Informationen über Namen und Kontaktdaten des Datenempfängers, Zwecke und Methoden der Verarbeitung, Arten der personenbezogenen Daten, Methode und Verfahren für die Ausübung der Rechte des Betroffenen gegenüber dem Datenempfänger, usw.); • Erhalt einer separaten Zustimmung des Betroffenen; • Ergreifen von erforderlichen Maßnahmen, um sicherzustellen, dass die Tätigkeiten der Datenverarbeitung durch die Empfänger im Ausland den im GSPI festgelegten Datenschutzstandards entsprechen; und darüber hinaus eine der folgenden Bedingungen: • Bestehen der von der CAC organisierten Sicherheitsbewertung; • Erhalt einer Zertifizierung zum Schutz personenbezogener Daten, die von einer professionellen Institution nach den Bestimmungen der CAC durchgeführt wird, oder • Unterzeichnung des von der CAC formulierten Standardvertrags mit den Empfängern im Ausland	Art. 44 ff. DSGVO Personenbezogene Daten dürfen in ein Drittland übermittelt werden, wenn: • Die EU-Kommission die Angemessenheit des Datenschutzniveaus im Drittland festgestellt hat; • Verantwortliche oder der Auftragsverarbeiter geeignete Garantien für den Datenschutz vorgesehen haben (Formulierung von verbindlichen internen Datenschutzvorschriften, Verwendung von durch die EU-kommission formulierten Standarddatenschutzklauseln, Einhaltung der durch die Aufsichtsbehörde genehmigten Verhaltensregeln, die für den Verantwortlichen oder den Auftragsverarbeiter rechtsverbindlich und durchsetzbar sind, usw.) • Eine der in der DSGVO vorgesehen Ausnahmen vorliegt (Einwilligung des Betroffenen, Erforderlichkeit zur Vertragserfüllung, Verfolgung von Rechtsansprüchen, Wahrung von Interessen natürlicher Personen usw.)
Strafen	Art. 66 ff. GSPD • Bußgeld von bis zu RMB 50 Mio. (ca. EUR 6,8 Mio.) oder 5 % des Jahresumsatzes (unklar, ob weltweiter oder in China erzielter Umsatz) • Beschlagnahme der illegal erzielten Gewinne • Widerruf der Geschäftslizenz • Eintrag in der Corporate Social Credit System Datenbank	Art. 83 ff. DSGVO • Bußgeld von bis zu EUR 10 Mio. oder von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes • Bußgeld von bis zu EUR 20 Mio. oder von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes

	GSPD	DSGVO
Haftung von natürlichen Personen	Art. 66 GSPD Neben dem Datenverarbeiter kann auch die verantwortliche Person ("Datenschutzbeauftragter") mit einem Bußgeld von bis zu RMB 1 Mio. (ca. EUR 137.000,-) bestraft werden. Art. 66 GSPD spricht nicht ausdrücklich von einer/m „Datenschutzbeauftragten" ("data protection officer"), sondern von der „verantwortlichen Person" ("person in charge") und von „anderen unmittelbar Verantwortlichen" ("other personnel subject to direct liabilities"). Der Datenschutzbeauftragte kann u. a. zu den „verantwortlichen Personen" oder zu den „anderen unmittelbar Verantwortlichen" des Unternehmens gehören.	Art. 82 DSGVO Nach der DSGVO können für Datenschutzverstöße sowohl juristische als auch natürliche Personen als Verantwortliche oder als Auftragsverarbeiter haften. Verwaltungsrechtliche Haftung des Datenschutzbeauftragten ist in der DSGVO nicht vorgesehen. Auf der zivilrechtlichen Ebene kann ein Datenschutzbeauftragter gegenüber dem Verantwortlichen für schlechte Beratungsleistungen haften.

Die Compliance-Pflichten der Datenverarbeiter nach dem GSPD

Datenverarbeiter müssen sicherstellen und nachweisen können, dass deren Datenverarbeitung im Einklang mit den Datenschutzprinzipien und aufgrund einer der im Art. 13 GSPD genannten Rechtsgrundlagen erfolgt.

Soll die Verarbeitung personenbezogener Daten aufgrund der Einwilligung des Betroffenen erfolgen, muss die Einwilligung die im GSPD geregelten Form- und Inhaltsanforderungen erfüllen. Die Einwilligung des informierten Einzelnen muss freiwillig und eindeutig sein. Die bewilligte Datenverarbeitung darf nicht den Rahmen der Einwilligung überschreiten, und Datenverarbeiter müssen Maßnahmen ergreifen, um das Vorliegen der erforderlichen Einwilligung nachweisen zu können. Für die Verarbeitung von personenbezogenen Daten von Jugendlichen unter 14 Jahren ist die Zustimmung der Eltern einzuholen und es sind besondere Regeln für die Verarbeitung dieser Daten zu formulieren.

Vor Beginn der Datenverarbeitung haben Datenverarbeiter umfassende Informationspflichten (in Form einer Datenschutzerklärung) ggü. dem Betroffenen nachzukommen. Die Datenschutzerklärung soll wahrheitsgemäß, genau und in einer klaren und einfachen Sprache formuliert werden und soll mindestens die Identität und Kontaktdaten des Datenverarbeiters, den Zweck und Methoden der Datenverarbeitung und die Rechte des Betroffenen enthalten (Art. 17 GSPD).

Datenverarbeiter sind nach dem GSPD an eine Verschwiegenheitspflicht gebunden. Ohne vorherige Zustimmung des Einzelnen dürfen personenbezogene Daten nicht veröffentlicht oder an Dritte weitergegeben werden (Art. 23 GSPD).

Je nach Zweck und Art der Verarbeitung der personenbezogenen Daten, der Art der personenbezogenen Daten, der Auswirkung auf die Rechte und Interessen der Personen, möglicher Sicherheitsrisiken usw. sollen Datenverarbeiter folgende Maßnahmen ergreifen, um die Rechtsmäßigkeit der Datenverarbeitung sicherzustellen, und unbefugten Zugriff, Leckage, Verfälschung oder Verlust von personenbezogenen Daten zu verhindern (Art. 51 GSPD):

- Formulierung interner Unternehmensrichtlinien und Betriebsprozesse;
- Klassifizierung personenbezogener Daten;
- Ergreifung von technischen Sicherheitsmaßnahmen wie Verschlüsselung und Anonymisierung;
- Festlegung der unternehmensinternen Befugnisse für die Verarbeitung personenbezogener Daten;
- Durchführung von regelmäßigen Audits;
- Durchführung von regelmäßigen Sicherheitsschulungen und -trainings für Mitarbeiter;
- Formulierung und Bereithaltung eines Notfallplans für Sicherheitsvorfälle usw.

Obwohl sich die Pflichten zur Datenschutz-Folgenabschätzung nach dem GSPD und der DSGVO ähneln, sind die Verarbeitungstätigkeiten, die eine solche Pflicht auslösen, unterschiedlich. Das GSPD verlangt, im Gegensatz zur DSGVO, dass der Datenverarbeiter auch in den folgenden Fällen eine Datenschutz-Folgenabschätzung durchführt: Grenzüberschreitende Übermittlung personenbezogener Daten, Beauftragung eines externen Datenverarbeiters, Übermittlung personenbezogener Daten an einen Dritten und öffentliche Bereitstellung personenbezogener Daten.

Im Rahmen einer Datenschutz-Folgenabschätzung nach dem GSPD soll bewertet werden, ob die Zwecke und Methoden der Verarbeitung personenbezogener Daten rechtmäßig, ordnungsgemäß und notwendig sind, was die Auswirkungen auf die Rechte und Interessen der Personen und die Sicherheitsrisiken sind, und ob die getroffenen Schutzmaßnahmen rechtmäßig und wirksam sind und dem Grad der Risiken entsprechen (Art. 56 GSPD). Im Vergleich zur DSGVO sieht das GSPD keine Pflicht zur Konsultation einer Aufsichtsbehörde vor, wenn die Daten-

schutz-Folgenabschätzung ergibt, dass bestimmte Risiken nicht beseitigt werden können.

Datenverarbeiter außerhalb Chinas sollen eine spezielle Stelle einrichten oder einen lokalen Vertreter innerhalb Chinas benennen, die für den Datenschutz zuständig sind. Bei Verarbeitung von Daten, deren Menge den von der CAC („Cyberspace Administration of China") festgelegten Schwellenwert überschreitet, ist eine für den Datenschutz verantwortliche Person ("data protection officer") zu benennen.

Ähnlich wie die DSGVO regelt auch das GSPD die Pflicht zur Aufnahme der Verarbeitungstätigkeit. Im Unterschied zur DSGVO sind Datenverarbeiter nach dem GSPD zur Aufnahme der Verarbeitungstätigkeiten immer dann verpflichtet, wenn eine der Bedingungen zur Durchführung einer Datenschutzfolgeabschätzung vorliegt. Berichte über eine Datenschutz-Folgeabschätzung und die Verzeichnisse der Verarbeitungstätigkeit müssen mindestens drei Jahre aufbewahrt werden (Art. 55 GSPD).

Datenverarbeiter sind verpflichtet die personenbezogenen Daten auf Antrag des Betroffenen zu löschen oder sobald der mit der Datenverarbeitung angestrebte Zweck erreicht ist. Ist die durch Rechts- oder Verwaltungsvorschriften vorgeschriebene Aufbewahrungsfrist noch nicht abgelaufen oder ist die Löschung personenbezogener Daten technisch schwierig zu realisieren, müssen personenbezogene Daten nicht gelöscht werden. In diesem Ausnahmefall sind die Verarbeitungsaktivitäten jedoch auf die Speicherung und Ergreifung erforderlicher Sicherheitsmaßnahmen einzuschränken. Andere Verarbeitungsaktivitäten sind nicht erlaubt.

Im Falle eines Datenschutzvorfalles sollen Datenverarbeiter Abhilfemaßnahmen ergreifen als auch die für den Schutz personenbezogener Daten zuständige Behörde und den Betroffenen informieren. In der Meldung sind folgende Informationen anzuführen: Die Art der personenbezogenen Daten, die durchgesickert sind, manipuliert oder verloren wurden oder werden könnten, die Gründe dafür und der Schaden, der dadurch verursacht wurde oder verursacht werden könnte; Abhilfemaßnahmen des Datenverarbeiters personenbezogener Daten und Maßnahmen, die die betroffenen Personen zur Schadensmilderung ergreifen können; sowie Kontaktdaten des Datenverarbeiters. Die in der DSGVO vorgesehene Anmeldungsfrist von 72 Stunden ist im GSPD nicht geregelt. Datenschutzvorfälle müssen unverzüglich angemeldet werden.

Grenzüberschreitende Datenübermittlung

Besondere Pflichten gelten für Datenverarbeiter, die personenbezogene Daten ins Ausland übermitteln. Die grenzüberschreitende Datenübermittlung betrifft vor allem multinationale Unternehmen, die personenbezogene Daten im Rahmen der Unternehmensgruppe teilen. Hierzu zählen z. B. Unternehmen, die eine universelle Datenverarbeitungsplattform verwenden, die auch durch die Tochtergesellschaften in China verwendet wird und die in der Unternehmenszentrale im Ausland gehostet wird oder chinesische Tochterunternehmen, die personenbezogene Daten ihrer Mitarbeiter (z. B. Name und E-Mail-Adresse) in China oder Geschäftspartner in China deren Muttergesellschaft in Deutschland zur Verfügung stellen. In diesen Situationen finden die Regelungen bezüglich grenzüberschreitender Datenübertragung entsprechend Anwendung.

Entsprechend dem Prinzip der Datenlokalisierung sind Daten grundsätzlich innerhalb Chinas zu speichern. Personenbezogene Daten dürfen nur unter Erfüllung der folgenden Voraussetzungen im Ausland bereitgestellt werden (Art. 39 GSPD):

- Erfüllung der Informationspflicht gegenüber dem Betroffenen. Der Datenverarbeiter soll den Betroffenen über Namen und Kontaktdaten des Datenempfängers, Zwecke und Methoden der Verarbeitung, Arten der personenbezogenen Daten, Methode und Verfahren für die Ausübung der Rechte des Betroffenen gegenüber dem Datenempfänger, usw. informieren;
- Erhalt einer separaten Zustimmung des Betroffenen;
- Ergreifen von erforderlichen Maßnahmen, um sicherzustellen, dass die Datenverarbeitung durch die Empfänger im Ausland den im GSPD festgelegten Datenschutzstandards entsprechen;
- Durchführung einer Datenschutz-Folgenabschätzung.

Darüber hinaus muss eine der folgenden Voraussetzungen erfüllt werden (Art. 38 GSPD):

- Bestehen der von der CAC organisierten Sicherheitsbewertung. Die Sicherheitsbewertung ist obligatorisch für CIIOs und Unternehmen, die personenbezogene Daten verarbeiten, die einen von der CAC noch festzulegenden Schwellenwert überschreiten;
- Erhalt einer Zertifizierung zum Schutz personenbezogener Daten, die von einer professionellen Institution nach den Bestimmungen der CAC durchgeführt wird; oder
- Unterzeichnung des von der CAC noch zu formulierenden Standardvertrags mit den Empfängern im Ausland.

Im Vergleich zur DSGVO enthält das GSPD keine Ausnahmen für die Bereitstellung von personenbezogenen Daten im Ausland. Keine der in Art. 38 GSPD geregelten Bedingungen darf durch die Einwilligung des Einzelnen ersetzt werden. Am 29.10.2021 veröffentlichte die CAC den Entwurf der Maßnahmen zur Sicherheitsbewertung des grenzüberschreitenden Datentransfers (chinesisch 数据出境安全评估办法, 征求意见稿) zur öffentlichen Kommentierung. Dieser definiert den Mechanismus der Sicherheitsbewertung und den Mindestinhalt der Standardverträge.

Die im Juni 2021 von der Europäischen Kommission veröffentlichten Standardvertragsklauseln regeln in vier Modulen den Datenaustausch zwischen der Europäischen Union und einem Drittland. Im direkten Vergleich zwischen den Regelungen der EU- Standardvertragsklauseln und den restriktiven Vorgaben der VR China zur grenzüberschreitenden Datenübermittlung scheint eine Harmonisierung nur schwer möglich zu sein. Inwieweit ein chinesisches Unternehmen die von einem deutschen Unternehmen vorgelegten EU- Standardvertragsklauseln unterzeichnen wird, ist ebenfalls fraglich. Hier wäre eine Anpassung der Vorgaben auf chinesischer Seite wünschenswert.

Unsere Empfehlungen

1. Überprüfung und Klassifizierung der zu verarbeitenden Daten. Im ersten Schritt ist es für Unternehmen wichtig zu verstehen, ob die zu verarbeitenden Daten überhaupt dem GSPD unterliegen. Unternehmen sollten daher alle Daten identifizieren und klassifizieren.
2. Überprüfung der Rechtsgrundlage für die Datenverarbeitung. Da die Verarbeitung von Daten immer auf einer der oben genannten Rechtsgrundlagen beruhen muss, ist es notwendig, für jede Verarbeitungsaktivität eine entsprechende Rechtsgrundlage zu identifizieren. Ein „berechtigtes Interesse“ gilt nach dem GSPD nicht als Rechtsgrundlage für die Verarbeitung personenbezogener Daten.
3. Bewertung der Datenschutzrisiken nach Eintrittswahrscheinlichkeit und Schadenshöhe.
4. Analyse des Datenflusses. Überprüfung, wo, wie und für wie lange die zu verarbeitende Daten gesichert werden, und ob sie an Dritte und/oder in ein Drittland bereitgestellt werden. Unternehmen sollen den sog. Informationsfluss prüfen und ein Datenmapping durchzuführen, um festzustellen, wo personenbezogene Daten verarbeitet (erhoben, gespeichert, abgerufen usw.) werden und zu welchem Zweck.
5. Überprüfung/Formulierung der Datenschutzerklärung, die die im GSPD vorgesehenen Form- und Inhaltsanforderungen erfüllen muss.
6. Implementierung von technischen und organisatorischen Maßnahmen durch:
   - Bewertung, ob eine verantwortliche Person/Datenschutzbeauftragter eingesetzt werden muss
   - Ergreifen von technischen Sicherheitsmaßnahmen (z. B. Anonymisierung oder Verschlüsselung personenbezogener Daten)
   - Einführung eines Verfahrens für die Bearbeitung von Anfragen der Betroffenen
   - Formulierung eines Notfallplans für den Fall eines Sicherheitsvorfalls und Durchführung von regelmäßigen Audits
   - Erlass von Regelungen, Anweisungen usw.

Autoren: **Rainer Burkardt ist Head of Practice/ Executive Counsel bei Burkardt & Partner in Shanghai und spezialisiert auf die Umsetzung des Datenschutzrechtes deutschsprachiger Unternehmen in China.**

Jürgen Recha ist Geschäftsführer der interev GmbH in Hannover/Langenhagen und spezialisiert auf die Umsetzung des Datenschutzes in mittelständischen deutschen Unternehmen.