Das neue chinesische Datenschutzrecht und die europäische DSGVO – Ein Rechtsvergleich

Rainer Burkardt / Jürgen Recha [1]

Abstract

Das Gesetz der Volksrepublik China zum Schutz persönlicher Daten (GSPD), welches am 1. November 2021 in Kraft trat, bildet zusammen mit dem Cybersicherheitsgesetz, dem Datensicherheitsgesetz und dem 4. Buch des Zivilgesetzbuches der Volksrepublik China die rechtliche Grundlage für den Datenschutz in China. Auch wenn das GSPD viele Ähnlichkeiten mit der EU-DSGVO aufweist, so enthält das GSPD auch eine Reihe von Abweichungen, die Verarbeiter persönlicher Daten, einschließlich ausländischer Unternehmen und deren Tochtergesellschaften in China, beachten müssen. Um die Konformität auch mit diesen abweichenden Anforderungen des GSPD sicherzustellen, müssen europäische Datenverarbeiter und deren Tochtergesellschaften in China ihre Datenschutzrichtlinien anpassen und entsprechende Maßnahmen ergreifen, denn eine bloße Übertragung der unternehmensinternen Richtlinien aus der EU nach China ist nicht ausreichend, um Compliance sicherzustellen. Der Artikel gibt einen Überblick über die wichtigsten Pflichten der Datenverarbeiter und stellt die wesentlichsten Unterschiede zwischen dem GSPD und der EU-DSGVO übersichtlich in einer Tabelle dar. Abschließend geben die Autoren Empfehlungen zur Überprüfung, ob und inwieweit Handlungsbedarf besteht, als auch zur Implementierung von technischen und organisatorischen Maßnahmen.

Am 1. November 2021 ist das „Gesetz der Volksrepublik China zum Schutz persönlicher Daten" (GSPD)[2] in Kraft getreten. Ähnlich wie die „EU-Datenschutzgrundverordnung" (DSGVO)[3] zielt das GSPD unter anderem darauf ab, persönliche Daten zu schützen und gesetzliche Standards für deren Verarbeitung festzulegen.

Dem Schutz von persönlichen Daten wurde in der Volksrepublik China („VR China" oder „China") lange Zeit keine Aufmerksamkeit zuteil und persönliche Daten wurden gesetzlich nur unzureichend geschützt, beispielsweise im Rahmen des Reputationsschutzes nach den „Allgemeinen Grundsätzen des Zivilrechts"[4] und des Privatrechtsschutzes nach dem „Delikthaftungsrecht der Volksrepublik China"[5]. Erst im „Cybersicherheitsgesetz der Volksrepublik China" (CybersichG)[6] (in Kraft seit dem 1. Juni 2017) wurde dem Schutz von persönlichen 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 Datenschutzgesetze erlassen und mit dem 4. Buch des „Zivilgesetzbuches der Volksrepublik China" (ZGB)[7] zum ersten Mal Persönlichkeitsrechte definiert.

Anders als Deutschland besitzt China kein vereinheitlichtes Gesetzeswerk für den Schutz von persönlichen 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 persönlicher Daten in China. Zusammen mit dem CybersichG, dem am 1. September 2021 in Kraft getretenen „Datensicherheitsgesetz der Volksrepublik China"[8] und dem am 1. Januar 2021 in Kraft getretenen 4. Buch des ZGB 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 innerhalb Chinas Waren oder Dienstleistungen anzubieten oder das Verhalten natürlicher Personen innerhalb Chinas zu analysieren oder zu bewerten.

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

[1] Rainer Burkardt, Head of Practice, Burkardt & Partner Rechtsanwälte in Shanghai; Jürgen Recha, Geschäftsführer, interev GmbH.

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

[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG vom 27.4.2016.

[4] 中华人民共和国民法通则 vom 12.4.1986 in der Fassung vom 27.8.2009; deutsche Übersetzung in: *Frank Münzel* (Hrsg.), Chinas Recht, 12.4.1986/1.

[5] 中华人民共和国侵权责任法 vom 26.12.2009, chinesisch-deutsche Übersetzung in ZChinR 2010, S. 41 ff.

[6] 中华人民共和国网络安全法 vom 7.11.2016, chinesisch-deutsche Übersetzung in ZChinR 2018, S. 113 ff.

[7] 中华人民共和国民法典 vom 28.5.2020, chinesisch-deutsche Übersetzung in ZChinR 2020, S. 207 ff.

[8] 中华人民共和国数据安全法 vom 10.6.2021.

chinesische Tochtergesellschaft zu übertragen. Darum ist es erforderlich, dass Unternehmen, die Geschäfte in oder mit China betreiben, ihre Datenschutzmaßnahmen anpassen, um den Datenschutzanforderungen des GSPD nachzukommen.

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

	GSPD	**DSGVO**
Die wichtigsten Begrifflichkeitsunterschiede	• Verarbeiter persönlicher Daten • Verantwortliche für den Datenschutz	• Verantwortliche • Datenschutzbeauftragte
Rechtsgrundlagen für die Verarbeitung persönlicher Daten	§ 13 GSPD sieht folgende Rechtsgrundlagen für die Datenverarbeitung vor: • Aktive Einwilligung der betroffenen Person • Abschluss oder Erfüllung eines Vertrags • Gesetzliche Verpflichtung • Behandlung der Notfälle im Bereich der öffentlichen Gesundheit oder unter dringenden Umständen zum Schutz des Lebens, der Gesundheit oder der Sicherheit des Vermögens natürlicher Personen • Öffentliches Interesse • Verarbeitung von durch die betroffene Person oder anders rechtmäßig offengelegten persönlichen Daten in angemessenem Umfang	Art. 6 DSGVO sieht folgende Rechtsgrundlagen für die Datenverarbeitung vor: • Aktive Einwilligung der betroffenen Person • Erfüllung eines Vertrags oder Durchführung vorvertraglicher Maßnahmen • Gesetzliche Verpflichtung • Schutz von lebensnotwendigen Interessen • Öffentliches Interesse • Berechtigtes Interesse des Verantwortlichen oder eines Dritten
Rechte der betroffenen Person	Rechte der betroffenen Person nach dem GSPD (Auszug): • Auskunft (§ 44) • Einsichtnahme und Kopieren (§ 45) • Widerruf der Einwilligung (§ 46) • Berichtigung (§ 46) • Datenübertragbarkeit (§ 45) • Einschränkung (§ 44) • Verweigerung (§ 44) • Löschung (§ 47)	Rechte der betroffenen Person nach der DSGVO (Auszug): • Auskunft (Art. 15) • Widerruf der Einwilligung (Art. 7 Abs. 3) • Berichtigung (Art. 16) • Datenübertragbarkeit (Art. 20) • Widerspruchsrecht (Art. 21) • Einschränkung (Art. 18) • Löschung (Art. 27)
Sensible persönliche Daten nach dem GSPD und besondere Kategorien personenbezogener Daten nach der DSGVO	§ 28 GSPD – Daten, die im Falle einer Weitergabe oder einer illegalen Verwendung zur Verletzung der Würde der Persönlichkeit natürlicher Personen oder zur Gefährdung der Sicherheit einer Person oder des Vermögens führen können, wie: • Religion oder Glaube • Medizinische Daten • Biometrische Daten • Bestimmte Identitäten • Finanzkonten • Daten über den Aufenthaltsort • Persönliche Daten von Minderjährigen unter 14 Jahren • Andere persönliche Daten Das GSPD stellt strengere Anforderungen an den Schutz von sensiblen persönlichen Daten.	Art. 9 DSGVO – Daten, die ein hohes Risiko für die Person bedeuten können, wie: • Rassische und ethnische Herkunft • Politische Meinungen • Religiöse und weltanschauliche Überzeugungen • Gewerkschaftszugehörigkeit • Gesundheit • Sexualleben und sexuelle Orientierung • Genetische und biometrische Angaben Die Verarbeitung personenbezogener Daten aus besonderen Kategorien ist nur in den von der DSGVO vorgesehenen Fällen erlaubt.
Separate Einwilligung der betroffenen Person	Separate Einwilligung der betroffenen Person ist nach dem GSPD erforderlich für: • Bereitstellung von persönlichen Daten an Dritte (§ 23) • Veröffentlichung von persönlichen Daten (§ 25) • Verarbeitung von sensiblen persönlichen Daten (§ 29) • Grenzüberschreitende Bereitstellung von persönlichen Daten (§ 39)	Separate Einwilligung nach Art. 6 DSGVO • Separate Einwilligung der betroffenen Person muss für verschiedene Verarbeitungszwecke und -vorgänge abgegeben werden.

	GSPD	**DSGVO**
Voraussetzungen für die Benennung eines Verantwortlichen/ Datenschutzbeauftragten für den Schutz persönlicher Daten	§ 52 GSPD – Datenverarbeiter müssen einen für den Datenschutz Verantwortlichen benennen, wenn die Menge der verarbeiteten persönlichen Daten einen von der Abteilung für Netzwerke und Informationen (Cyberspace Administration of China – „CAC“) festgelegten Schwellenwert überschreitet.	Art. 37 DSGVO – Datenverarbeiter müssen einen Datenschutzbeauftragten 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.
Einrichtung einer Stelle oder Benennung eines Vertreters in der VR China/EU	§ 53 GSPD – Die dem GSPD unterliegenden Datenverarbeiter außerhalb Chinas sollen eine spezielle Stelle einrichten oder einen Vertreter innerhalb Chinas benennen, die/ der für den Schutz persönlicher Daten verantwortlich ist und der zuständigen Behörde den Namen, die Kontaktdaten usw. des speziellen Organs oder des Vertreters mitteilt.	Art. 27 DSGVO – Die nicht in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeiter nach Art. 3 Abs. 2 DSGVO sollen in der EU schriftlich einen Vertreter in der EU benennen, es sei denn: • die Datenverarbeitung erfolgt nur gelegentlich, • besondere Kategorien personenbezogener Daten werden nicht im großen Umfang verarbeitet, und • die Datenverarbeitung voraussichtlich führt nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.
Compliance Audits	§ 54 GSPD – Datenverarbeiter haben im Hinblick auf die Umstände, wie sie bei der Verarbeitung persönlicher Daten die Gesetze und Verwaltungsvorschriften einhalten, periodisch Compliance Audits vorzunehmen.	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.: 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 Datenschutzfolgenabschätzung	§ 55 GSPD – Die Durchführung der Datenschutzfolgenabschätzung ist verpflichtend für: • Verarbeitung sensibler persönlicher Daten • Verwendung persönlicher Daten für automatisierte Entscheidungen • Beauftragung anderer mit der Verarbeitung persönlicher Daten • Bereitstellung persönlicher Daten an andere Datenverarbeiter • Offenlegung persönlicher Daten • Grenzüberschreitende Bereitstellung persönlicher Daten und • sonstige Verarbeitungen persönlicher Daten, die schwerwiegende Auswirkungen auf die Rechte und Interessen der betroffenen 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 Datenschutzfolgenabschätzung 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
Bedingungen für die Bereitstellung von persönlichen Daten im Ausland	Für die grenzüberschreitende Bereitstellung von persönlichen Daten müssen folgende Bedingungen kumulativ erfüllt werden: • Erfüllung der Informationspflicht gegenüber der betroffenen Person (Informationen über die Identität und Kontaktdaten des Datenverarbeiters, den Zweck und die Mittel der Datenverarbeitung, die Speicherfrist, die Rechte der betroffenen Person und die Methoden und Verfahren für deren Ausübung, usw. (§ 39) • Erhalt einer separaten Einwilligung der betroffenen Person (Art. 39) • Ergreifen von notwendigen Maßnahmen, um zu gewährleisten, dass die Datenverarbeitung durch den Empfänger im Ausland die im GSPD festgelegten Datenschutzstandards erreicht (§ 38 Abs. 3) • Durchführung einer Datenschutzfolgenabschätzung (§ 55) und darüber hinaus eine der folgenden Bedingungen (§ 38 Abs. 1): • Bestehen der von der CAC organisierten Sicherheitsbewertung • Erhalt einer Zertifizierung zum Schutz persönlicher Daten, die von einem Fachorgan nach den Bestimmungen der CAC durchgeführt wird, oder • Abschluss des von der CAC formulierten Standardvertrags mit dem Empfänger im Ausland	Nach der DSGVO dürfen personenbezogene Daten in ein Drittland übermittelt werden, wenn: • die EU-Kommission die Angemessenheit des Datenschutzniveaus im Drittland festgestellt hat (Art. 45) • 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 verbindlichen internen Datenschutzvorschriften, die für den Verantwortlichen oder den Auftragsverarbeiter rechtsverbindlich und durchsetzbar sind, usw.) (Art. 46 ff.) • eine der in der DSGVO vorgesehenen Ausnahmen vorliegt (Einwilligung der betroffenen Person, Erforderlichkeit zur Vertragserfüllung, Verfolgung von Rechtsansprüchen, Wahrung von Interessen natürlicher Personen usw.) (Art. 49)

	GSPD	DSGVO
Sanktionen	Sanktionen nach dem GSPD (Auszug): • Bußgeld von bis zu RMB 50 Mio. (ca. EUR 6,9 Mio.) oder 5 % des Jahresumsatzes (unklar, ob weltweiter oder in China erzielter Umsatz) (§ 66 Abs. 2) • Einziehung der illegal erzielten Gewinne • Widerruf der Geschäftslizenz (§ 66 Abs. 2) • Aufzeichnung in der Corporate Social Credit System-Datenbank (§ 67)	Sanktionen nach der DSGVO (Auszug): • (2) Bußgeld von bis zu EUR 10 Mio. oder von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes (Art. 83 Abs. 4) • (5) Bußgeld von bis zu EUR 20 Mio. oder von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes (Art. 83 Abs. 5)
Haftung von Verantwortlichen/ Datenschutzbeauftragten und anderen natürlichen Personen	§ 66 GSPD – Neben dem Datenverarbeiter können auch verantwortliche natürliche Personen mit einem Bußgeld von bis zu RMB 1 Mio. (ca. EUR 139.000) bestraft werden. § 66 GSPD spricht nicht ausdrücklich von einem Verantwortlichen, sondern von der „unmittelbar verantwortlichen Person" und von „anderen unmittelbar verantwortlichen Personen". Der Verantwortliche für den Schutz persönlicher Daten 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 § 13 GSPD genannten Rechtsgrundlagen erfolgt.

Soll die Verarbeitung persönlicher Daten aufgrund der Einwilligung der betroffenen Person erfolgen, muss die Einwilligung die im GSPD geregelten Form- und Inhaltsanforderungen erfüllen. Die Einwilligung muss von der betroffenen Person in vollständiger Kenntnis, freiwillig und ausdrücklich gegeben werden. Die bewilligte Datenverarbeitung darf nicht den Rahmen der Einwilligung überschreiten. Obwohl das GSPD keine Formerfordernisse für die Einwilligung zur Verarbeitung von nichtsensiblen persönlichen Daten vorschreibt,[9] sollen Datenverarbeiter entsprechende Maßnahmen ergreifen, um das Vorliegen der Einwilligung nachweisen zu können. Für die Verarbeitung persönlicher Daten von Minderjährigen unter 14 Jahren ist die Einwilligung der Eltern einzuholen und es sind besondere Regeln für die Verarbeitung dieser Daten zu formulieren.

Vor Beginn der Datenverarbeitung haben Datenverarbeiter umfassenden Informationspflichten (in Form einer Datenschutzerklärung) ggü. der betroffenen Person nachzukommen. Die Datenschutzerklärung soll wahrheitsgemäß, präzise, vollständig und in einer klaren und verständlichen Sprache formuliert und der betroffenen Person in auffälliger Weise zur Kenntnis gebracht werden. Die Datenschutzerklärung soll mindestens die Identität und Kontaktdaten des Datenverarbeiters, den Zweck und die Mittel der Datenverarbeitung, die Speicherfrist, die Rechte der betroffenen Person und die Methoden und Verfahren für deren Ausübung enthalten (§ 17 GSPD).

Datenverarbeiter sind nach dem GSPD an eine Verschwiegenheitspflicht gebunden. Ohne vorherige separate Einwilligung der betroffenen Person dürfen persönliche Daten nicht offengelegt oder an Dritte bereitgestellt werden (§§ 23, 25 GSPD).

Je nach Zweck und Art der Verarbeitung persönlicher Daten, den Kategorien persönlicher Daten, der Auswirkung auf die Rechte und Interessen der betroffenen Person, potenzieller Sicherheitsrisiken usw. sollen Datenverarbeiter folgende Maßnahmen ergreifen, um die Rechtmäßigkeit der Datenverarbeitung zu gewährleisten und unbefugten Zugriff, Leckage, Verfälschung oder Verlust von persönlichen Daten zu verhindern (§§ 51, 52 GSPD):

- Formulierung interner Unternehmensrichtlinien und Betriebsprozesse;
- Klassifizierte Verwaltung persönlicher Daten;
- Ergreifung von entsprechenden technischen Sicherheitsmaßnahmen wie Verschlüsselung und De-Identifizierung;
- Festlegung von betriebsinternen Befugnissen für die Verarbeitung persönlicher Daten;
- Durchführung von regelmäßigen Audits;
- Durchführung von regelmäßigen Sicherheitsschulungen und -trainings für Mitarbeiter;
- Festlegung und Umsetzung eines Notfallplans für Sicherheitsvorfälle usw.

[9] Für die Verarbeitung von sensiblen persönlichen Daten muss nach § 29 GSPD eine separate Einwilligung eingeholt werden. Die Einwilligung zur Verarbeitung von sensiblen persönlichen Daten soll in schriftlicher Form erfolgen, sofern dies durch andere Gesetze oder Verwaltungsvorschriften vorgesehen ist.

Obwohl sich die Pflichten zur Datenschutzfolgenabschätzung 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 Datenschutzfolgenabschätzung durchführt: grenzüberschreitende Bereitstellung persönlicher Daten, Beauftragung eines externen Datenverarbeiters, Bereitstellung persönlicher Daten an andere Datenverarbeiter und Offenlegung persönlicher Daten (§ 55 GSPD).

Die Datenschutzfolgenabschätzung ist ex ante durchzuführen und in deren Rahmen soll bewertet werden, ob die Zwecke und Mittel der Verarbeitung persönlicher Daten rechtmäßig, gerechtfertigt und notwendig sind, was die Auswirkungen auf die Rechte und Interessen der betroffenen Personen und die Sicherheitsrisiken sind und ob die getroffenen Schutzmaßnahmen rechtmäßig und wirksam sind und dem Risikoniveau entsprechen (§ 56 GSPD). Im Vergleich zur DSGVO sieht das GSPD keine Pflicht zur Konsultation einer Aufsichtsbehörde vor, wenn die Datenschutzfolgenabschätzung ergibt, dass bestimmte Risiken nicht beseitigt werden können.

Ähnlich wie die DSGVO regelt auch das GSPD die Pflicht zur Aufzeichnung der Verarbeitungstätigkeit. Im Unterschied zur DSGVO sind Datenverarbeiter nach dem GSPD zur Aufzeichnung der Verarbeitungstätigkeiten immer dann verpflichtet, wenn eine der Bedingungen zur Durchführung einer Datenschutzfolgenabschätzung vorliegt. Berichte über eine Datenschutzfolgenabschätzung und die Aufzeichnungen der Verarbeitungstätigkeit müssen mindestens drei Jahre aufbewahrt werden (§ 55 GSPD).

Bei Verarbeitung persönlicher Daten, deren Menge den von der CAC („Cyberspace Administration of China") festgelegten Schwellenwert überschreitet, ist nach § 52 GSPD ein für den Datenschutz Verantwortlicher zu benennen. Zum Datum der Veröffentlichung dieses Artikels war von der CAC diesbezüglich keine Regelung erlassen und nähere Voraussetzungen für die Benennung des Verantwortlichen bleiben daher abzuwarten.

Datenverarbeiter außerhalb Chinas, auf die das GSPD Anwendung findet, sollen eine spezielle Stelle einrichten oder einen lokalen Vertreter innerhalb Chinas benennen, die/der für den Datenschutz zuständig ist, und zwar unabhängig von der Menge der verarbeiteten persönlichen Daten. Anders als die DSGVO sieht das GSPD keine Ausnahmen von dieser Pflicht vor und ausländische Datenverarbeiter sollen der Pflicht zur Einrichtung einer speziellen Stelle oder Benennung eines lokalen Vertreters innerhalb Chinas nachkommen, ungeachtet der Kategorien der verarbeiteten Daten, der Häufigkeit der Datenverarbeitung oder der Risiken der Datenverarbeitung für Rechte und Freiheiten der betroffenen Person (§ 53 GSPD).

Datenverarbeiter sind verpflichtet, die persönlichen Daten von sich aus oder auf Antrag der betroffenen Person zu löschen, wenn: der mit der Datenverarbeitung angestrebte Zweck erreicht ist oder nicht erreicht werden kann, die persönlichen Daten für die Realisierung des Verarbeitungszwecks nicht mehr erforderlich sind, die betroffene Person die Einwilligung widerrufen hat, die persönlichen Daten rechtswidrig verarbeitet werden usw. Ist die durch Rechts- oder Verwaltungsvorschriften vorgeschriebene Aufbewahrungsfrist noch nicht abgelaufen odr ist die Löschung persönlicher Daten technisch schwierig zu realisieren, müssen persönliche 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 sowohl Abhilfemaßnahmen ergreifen als auch die für den Schutz persönlicher Daten zuständige Behörde und die betroffene Person benachrichtigen. In der Benachrichtigung sind folgende Informationen anzuführen: die Kategorien der persönlichen Daten, die durchgesickert sind, verfälscht oder verloren wurden oder werden könnten, die Ursachen dafür und die Gefahren, die dadurch verursacht wurden bzw. verursacht werden könnten; Abhilfemaßnahmen des Datenverarbeiters persönlicher 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 (§ 57 GSPD).

Grenzüberschreitende Bereitstellung persönlicher Daten

Besondere Pflichten gelten für Datenverarbeiter, die persönliche Daten ins Ausland übermitteln. Die grenzüberschreitende Datenübermittlung betrifft vor allem multinationale Unternehmen, die persönliche Daten im Rahmen der Unternehmensgruppe teilen, 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 persönliche Daten ihrer Mitarbeiter (z. B. Name und E-Mail-Adresse) in China oder von Geschäftspartnern in China deren Muttergesellschaft in Deutschland zur Verfügung stellen. In diesen Situationen finden die Regelungen bezüglich grenzüberschreitender Bereitstellung persönlicher Daten entsprechende Anwendung.

Entsprechend dem Prinzip der Datenlokalisierung sind Daten grundsätzlich innerhalb Chinas zu speichern. Persönliche Daten dürfen nur unter kumulativer Erfüllung der folgenden Bedingungen im Ausland bereitgestellt werden:

- Erfüllung der Informationspflicht gegenüber der betroffenen Person. Der Datenverarbeiter soll die betroffene Person über Namen und Kontaktdaten des Datenempfängers, Zwecke und Mittel der

Verarbeitung, Kategorien der persönlichen Daten, Methode und Verfahren für die Ausübung der Rechte der betroffenen Person gegenüber dem Datenempfänger usw. informieren (§ 39 GSPD);

- Erhalt einer separaten Einwilligung der betroffenen Person (§ 39 GSPD);
- Ergreifen von notwendigen Maßnahmen, um zu gewährleisten, dass die Datenverarbeitung durch die Empfänger im Ausland den im GSPD festgelegten Datenschutzstandard erreicht (§ 38 Abs. 3 GSPD);
- Durchführung einer Datenschutzfolgenabschätzung (§ 55 GSPD).

Darüber hinaus muss eine der folgenden Bedingungen erfüllt werden (§ 38 Abs. 1 GSPD):

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

Im Vergleich zur DSGVO enthält das GSPD keine Ausnahmen für die Bereitstellung von persönlichen Daten im Ausland. Keine der in § 38 GSPD geregelten Bedingungen darf durch die Einwilligung der betroffenen Person ersetzt werden. Am 29. Oktober 2021 veröffentlichte die CAC den „Entwurf der Maßnahmen zur Sicherheitsbewertung des grenzüberschreitenden Datentransfers“[10] 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.

[10] 数据出境安全评估办法，征求意见稿 vom 29.10.2021.

Unsere Empfehlungen

1. Überprüfung und Klassifizierung der zu verarbeitenden persönlichen 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 persönlicher Daten.
3. Bewertung der Datenschutzrisiken nach Eintrittswahrscheinlichkeit und Schadenshöhe.
4. Analyse des Datenflusses: Überprüfung, wo, wie und für wie lange die zu verarbeitenden persönlichen Daten gesichert werden und ob sie an Dritte und/ oder in einem Drittland bereitgestellt werden. Unternehmen sollen den sog. Informationsfluss prüfen und ein Datenmapping durchführen, um festzustellen, wo persönliche 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 (TOMs) durch:
   - Bewertung, ob ein Verantwortlicher/ Datenschutzbeauftragter eingesetzt werden muss
   - Ergreifen von technischen Sicherheitsmaßnahmen (z. B. Anonymisierung oder Verschlüsselung persönlicher Daten)
   - Einführung eines Verfahrens für die Bearbeitung von Anfragen der betroffenen Personen
   - Formulierung eines Notfallplans für den Fall eines Sicherheitsvorfalles und Durchführung von regelmäßigen Audits
   - Erlass von Regelungen, Anweisungen usw.

* * *

The New Chinese Data Protection Law and the European GDPR – A Legal Comparison

Together with the Cybersecurity Law, the Data Security Law, and the 4th Part of the Civil Code, the Personal Data Protection Law of the People's Republic of China (GSPD), which took effect on November 1, 2021, provides the legal basis for data protection in China. Although the GSPD shares many similarities with the EU's GDPR, it contains a range of differences that personal data processors, including foreign companies and their subsidiaries in China, must take into consideration. Particularly with the GSPD's differences, data processors in Europe and their subsidiaries in China need to adapt their data protection programs and take appropriate measures to ensure compliance, as merely transplanting their data protection programs from the EU to China will not suffice to ensure compliance. The article gives an overview of data processors' main obligations and provides a table clearly outlining the chief differences between the GSPD and the EU's GDPR. Finally, the authors recommend ways to ascertain how much action is required as well as how to implement technical and organizational measures.