Chinas Verordnung zum Sicherheitsmanagement von Netzwerkdaten durch Unternehmen – konkretisierte Datenschutz- und -sicherheitspflichten

Am 1. Januar 2025 ist in der Volksrepublik China („VR China“ oder „China“) die Verordnung zum Sicherheitsmanagement von Netzwerkdaten[1] („Verordnung“) in Kraft getreten.

Die Verordnung ist eine Durchführungsverordnung zum Cybersicherheitsgesetz der VR China („CSG“), dem Gesetz der VR China zum Schutz personenbezogener Daten („GSPD“) und dem Datensicherheitsgesetz der VR China („DSG“), welche den Rechtsrahmen für den Datenschutz in China bilden.

Der erste Entwurf der Verordnung wurde bereits am 14. November 2021, kurz nach dem Inkrafttreten des GSPD und des DSG, zur Kommentierung veröffentlicht und im Vergleich zum Wortlaut der nun erlassenen Verordnung umfassend revidiert.

Der nachstehende Text fasst die wichtigsten Neuerungen zum Thema Datenschutz und Datensicherheit aus der Verordnung zusammen.

I. Anwendungsbereich der Verordnung

Die Verordnung gilt für Verarbeiter von Netzwerkdaten, d. h. für alle Personen, welche elektronischen Daten in einem Netzwerk generieren und verarbeiten, einschließlich personenbezogener, nicht-personenbezogener und wichtiger Daten.

Ein „Netzwerk“ ist im CSG als ein System definiert, das sich aus Computern oder anderen Endgeräten und zugehöriger Ausrüstung zusammensetzt, und welches Informationen sammelt, speichert, überträgt, austauscht und Daten nach bestimmten Regeln und Verfahren verarbeitet.

Die Verordnung gilt auch extraterritorial für im chinesischen Ausland ansässige Personen, wenn diese Produkte oder Dienstleistungen natürlichen Personen in China anbieten oder deren Verhalten analysieren bzw. auswerten.

In der Praxis betrifft die Verordnung alle Unternehmen und Personen, die als Betreiber von Kommunikationsnetzwerken, als Anbieter von Online-Diensten und als Nutzer, Daten über das Internet oder LANs, wie z.B. beim Einsatz von SAP und CRM, verarbeiten.

II. Neuerungen im Bereich Datensicherheit

Allgemeine Datensicherheitspflichten: Die Verordnung konkretisiert die in den drei oben genannten Gesetzen vorgesehenen Datensicherheitspflichten. Gemäß der Verordnung sind Verarbeiter von Netzwerkdaten dafür verantwortlich, den Sicherheitsschutz von Netzwerkdaten zu verstärken, ein Netzwerkdatensicherheitsmanagementsystem einzurichten bzw. zu stärken,

[1] 《网络数据安全管理条例》

technische Sicherungsmaßnahmen wie Datenverschlüsselung und -backup, Zugangskontrolle, Sicherheitsauthentifizierung, Notfallpläne für den Umgang mit Datensicherheitsvorfällen einzurichten und andere notwendige Maßnahmen zu ergreifen, um Netzwerkdaten vor Veränderung, Zerstörung, Datenlecks oder illegalem Zugriff zu schützen.

Berichterstattungspflicht bei Sicherheitsvorfällen: Nach Art. 22 CSG müssen Anbieter von Netzprodukten und -dienstleistungen unverzüglich Abhilfemaßnahmen ergreifen, die Nutzer gemäß der Verordnung rechtzeitig informieren und den jeweils zuständigen Behörden Bericht erstatten, wenn sie Sicherheitsmängel, Lücken und andere Sicherheitsrisiken im Zusammenhang mit ihren Netzwerkprodukten und -dienstleistungen feststellen.

Die Verordnung legt nun in Art. 10 eine konkrete Frist von 24 Stunden für die Berichterstattung fest, soweit ein Sicherheitsrisiko eine Beeinträchtigung der nationalen Sicherheit oder des öffentlichen Interesses herbeiführt. In der Verordnung wird jedoch nicht spezifiziert, welche Sicherheitsmängel oder Risiken die nationale Sicherheit oder das öffentliche Interesse beeinträchtigen könnten. Hierfür sind auch keine Bewertungskriterien vorgesehen.

Datenschutzvereinbarung: Verarbeiter von Netzwerkdaten sind nach Art. 12 der Verordnung verpflichtet, mit jedem Dritten, an den sie personenbezogene oder wichtige Daten übermitteln, eine entsprechende Datenschutzvereinbarung abzuschließen. Die Datenschutzvereinbarung und die entsprechenden Verarbeitungsprotokolle müssen mindestens drei Jahre lang aufbewahrt werden.

Der Wortlaut des Art. 12 der Verordnung lässt sich so interpretieren, dass die Pflicht zum Abschluss einer Datenschutzvereinbarung sowohl für Übertragungen von einem „Verarbeiter an einen anderen Verarbeiter“ als auch für Übertragungen von einem „Verarbeiter an einen Auftragsverarbeiter“ gilt. Bis zum 1. Januar 2025 galt diese Pflicht nur bei der Übermittlung personenbezogener Daten, nicht jedoch für wichtige Daten.

Besondere Pflichten bei der Verarbeitung von wichtigen Daten:

- **Pflicht zur Benennung eines „Beauftragten für die Netzwerkdatensicherheit“:** Nach dem DSG sind Verarbeiter von wichtigen Daten verpflichtet, einen Beauftragten für den Schutz von wichtigen Daten zu benennen und eine für das Sicherheitsmanagement zuständige Abteilung einzurichten. Art. 30 der Verordnung etabliert nun dieselbe Pflicht bei der Verarbeitung von wichtigen Netzwerkdaten und konkretisiert die Kompetenzanforderungen an den Beauftragten für die Netzwerkdatensicherheit sowie die Pflichten der Abteilung für das Sicherheitsmanagement.

  Mit der Pflicht zur Benennung eines Beauftragten für die Netzwerkdatensicherheit schafft die Verordnung neben dem Datenschutzbeauftragten, Datensicherheitsbeauftragten und dem Cybersicherheitsbeauftragten eine zusätzliche vierte Funktion. Die einschlägigen Gesetze lassen offen, ob die vier oben genannten Funktionen von einer einzigen Person übernommen werden dürfen oder ob mehrere (entsprechend qualifizierte) Personen erforderlich sind.

- **Pflicht zur Risikobewertung vor Übertragung von wichtigen Daten an Dritte:** Nach dem DSG müssen Verarbeiter wichtiger Daten regelmäßig eine Risikobewertung in Bezug auf alle

Datenverarbeitungsaktivitäten vornehmen und den Datenschutzbehörden entsprechend Bericht erstatten. In Art. 31 stellt die Verordnung spezielle Anforderungen an die Weitergabe von wichtigen Daten an Dritte, an eine Verarbeitungsbeauftragung oder an eine gemeinsame Datenverarbeitung mit Dritten. Die speziellen Anforderungen entfallen, wenn die Datenübermittlung zwingend gesetzlich vorgeschrieben ist.

Die Risikobewertung muss unter anderem eine Bewertung der Datenschutzfähigkeiten des Empfängers der wichtigen Daten sowie die Wirksamkeit des mit dem Datenempfänger abgeschlossenen Vertrags zur Einhaltung der einschlägigen Datenschutzverpflichtungen umfassen. Somit scheint die Risikobewertung nach Art. 31 der Verordnung dem Konzept der Datenschutzfolgenabschätzung nach dem GSPD zu folgen.

- **Pflicht zur jährlichen Risikobewertung und Berichterstattung:** Außer der Risikobewertung und Berichterstattung nach Art. 31 sind Verarbeiter von wichtigen Daten nach Art. 33 der Verordnung verpflichtet, eine jährliche Risikobewertung der Verarbeitungsaktivitäten durchzuführen und darüber an die Behörden auf Provinzebene oder höher zu berichten.

Weiterhin fehlende Definition von wichtigen Daten: Nach Art. 29 Abs. 2 der Verordnung sind Datenverarbeiter für die Identifizierung und die behördliche Anmeldung wichtiger Daten verantwortlich. Die Verordnung enthält jedoch keine Definition von wichtigen Daten, die über die bereits bestehende allgemeine Beschreibung hinausgehen würde. Nach der Verordnung sollen für unterschiedliche Regionen und Branchen spezifische Kataloge wichtiger Daten festgelegt werden. Zum Zeitpunkt der Veröffentlichung dieses Beitrages war noch kein Katalog veröffentlicht.

III. Neuerungen im Bereich Datenschutz

Die Verordnung konkretisiert auch die in den oben genannten drei Gesetzen vorgesehenen Datenschutzbestimmungen und sieht neue Rechte und Pflichten für Verarbeiter personenbezogener Daten vor.

Datenübertragbarkeit: Das GSPD gibt, auch wenn derzeit in China von diesem Recht kaum Gebrauch gemacht wird, den betroffenen Personen das Recht, deren personenbezogenen Daten auf einen anderen Verarbeiter zu übertragen. Die Verordnung legt erstmals die Voraussetzungen für die Ausübung dieses Rechts vor.

Ferner stellt die Verordnung nun klar, dass, wenn die Anzahl der Ersuchen um die Datenübertragung einen angemessenen Rahmen erheblich überschreitet, der Datenverarbeiter die notwendigen Kosten für die Umsetzung des Ersuchens dem Datensubjekt/Ersuchenden in Rechnung stellen darf.

Klärung der Zuständigkeit der Behörde für die Anmeldung des Datenschutzvertreters eines ausländischen Datenverarbeiters: Nach dem GSPD sind ausländische Datenverarbeiter verpflichtet, eine spezielle Stelle einzurichten oder einen Vertreter innerhalb Chinas zu ernennen. Nach Art. 26 der Verordnung müssen ausländische Datenverarbeiter Namen und Kontaktdaten der speziellen Stelle bzw. des Vertreters an die Cybersicherheitsbehörde (CAC) auf der Kommunalebene, in dessen Verwaltungsbezirk die spezielle Stelle oder der Vertreter registriert ist, melden.

Zusätzliche Pflichten für Verarbeiter von großen Mengen personenbezogener Daten: Für Verarbeiter von personenbezogenen Daten von mehr als 10 Millionen Personen gelten zusätzliche Pflichten, einschließlich der Pflicht zur Benennung eines Beauftragten für die Netzwerkdatensicherheit und Etablierung einer entsprechenden Abteilung im Unternehmen sowie Berichterstattung an Behörden im Falle von Verschmelzung, Liquidation, Insolvenz, usw.

IV. Grenzüberschreitende Datenübermittlung

In Bezug auf die grenzüberschreitende Übermittlung von personenbezogenen Daten sieht die Verordnung eine Ausnahme von den drei im GSPD vorgesehenen Voraussetzungen – CAC-Sicherheitsbewertung, Zertifizierung und CAC-Standardvertrag – für eine Übertragung von personenbezogenen Daten ins Ausland vor.[2] Die Ausnahme, welche bei der „Übermittlung personenbezogener Daten ins Ausland zur Erfüllung gesetzlicher Aufgaben oder Verpflichtungen“ greift, wird in der Unternehmenspraxis jedoch eine eher untergeordnete Rolle spielen. Es bleibt jedoch abzuwarten, wie die zuständigen Behörden die Begrifflichkeiten „Erfüllung der gesetzlichen Aufgaben oder Pflichten“ definieren werden.

V. Fazit

Die Verordnung enthält und konkretisiert vor allem bereits in anderen Vorschriften zu Cybersicherheit, Datensicherheit und Datenschutz enthaltene Pflichten.

Die Verordnung ist damit ein Beispiel einer sogenannten „kaskadierenden Gesetzgebung“, d.h. neue Gesetze wiederholen einerseits Regeln, welche in schon bestehenden Gesetzen aufgestellt wurden, fügen diesen aber andererseits neue Regelungen hinzu.

Der Verordnung werden weitere detaillierte Durchführungsverordnungen und andere Vorschriften im Bereich Datenschutz und Datensicherheit folgen, um einen umfassenden Rechtsrahmen zu schaffen und damit die Verarbeitung von Daten umfassend zu regulieren.

Angesichts der zunehmenden Anzahl von behördlichen und gerichtlichen Strafgeldern bei Verstößen gegen Datenschutz- und Datensicherheitspflichten sowie der Möglichkeit einer Sanktionsminderung bzw. Sanktionsaussetzung im Falle einer proaktiven Umsetzung von Datenschutz- und Datensicherheitsmaßnahmen, sollten Unternehmen entsprechende datensicherheits- und datenschutzbezogene Compliance-Maßnahmen ergreifen, nicht nur um die Anforderungen der Verordnung zu erfüllen, sondern insbesondere um das Risiko hoher Bußgelder, zivilrechtlicher oder gar strafrechtlicher Haftung zu minimieren.

Hierzu sollten unter anderem Daten-Mappings vorgenommen werden, um personenbezogene und wichtige Daten zu identifizieren, dann zu klassifizieren und abschließend eine Risikobewertungen durchzuführen, die erforderlichenfalls eine Anpassung der unternehmensinternen Datenschutzrichtlinien oder Vorschriften für die Verarbeitung personenbezogener Daten nach sich zieht. Gerne unterstützen wir Sie hierbei mit unserem Expertenteam!

---

[2] Mehr Informationen zu den drei Voraussetzungen sowie den anderen Ausnahmen finden Sie in unserem Artikel *“CAC-Bestimmungen zur Regulierung und Förderung des grenzüberschreitenden Datenverkehrs – Echte Erleichterungen des strengen Datenschutzregimes für KMU in China?“*

Sollten Sie zu diesem oder einem anderen Rechtsthema mit China-Bezug Fragen haben, so zögern Sie nicht, uns jederzeit zu kontaktieren!

Ihr Burkardt & Partner Team

BURKARDT & PARTNER RECHTSANWÄLTE
Suite 1706, Five Corporate Avenue, No. 150 Hubin Road, Shanghai 200021, P.R. China

E-MAIL info@bktlegal.com
WEBSITE www.BKTlegal.com
OFFICE +86 (21) 6321 0088

Connect with us on LinkedIn