# Verordnung zur Verwaltung der Netzwerkdatensicherheit

**中华人民共和国国务院令**

第 790 号

《网络数据安全管理条例》已经 2024 年 8 月 30 日国务院第 40 次常务会议通过，现予公布，自 2025 年 1 月 1 日起施行。

总理　李强
2024 年 9 月 24 日

**Erlass des Staatsrates der Volksrepublik China**

Nr. 709

Die „Verordnung zur Verwaltung der Netzwerkdatensicherheit“[1] ist am 30.8.2024 auf der 40. Ständigen Sitzung des Staatsrates verabschiedet worden, wird hiermit verkündet [und] wird vom 1.1.2025 an durchgeführt.

Li Qiang, Ministerpräsident
24.9.2024

**网络数据安全管理条例**

**第一章　总则**

**第一条**　为了规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律，制定本条例。

**Verordnung zur Verwaltung der Netzwerkdatensicherheit**

**1. Kapitel: Allgemeine Regeln**

**§ 1 [Verordnungszweck]** Um die Verarbeitung von Netzwerkdaten[2] zu regeln, die Netzwerkdatensicherheit zu gewährleisten, die vernünftige [und] effektive Nutzung von Netzwerkdaten nach dem Recht zu fördern, die legalen Rechte [und] Interessen von Einzelpersonen [und] Organisationen zu schützen, die staatliche Sicherheit und öffentliche Interessen aufrechtzuerhalten, wird aufgrund von Gesetzen wie dem[3] „Cybersicherheitsgesetz der Volksrepublik China“[4], dem „Gesetz der Volksrepublik China zur Datensicherheit“[5] [und] dem „Gesetz der Volksrepublik China zum Schutz persönlicher Daten“[6] diese Verordnung erlassen.

1 Quelle des chinesischen Textes: <https://www.gov.cn/zhengce/zhengceku/202409/content_6977767.htm>, chinesisch-englischer Text abrufbar unter <lawinfochina.com> (北大法律英文网)/<pkulaw.cn> (北大法宝), Indexnummer (法宝引证码) CLI.2.5232484(EN).

2 Eine Definition für „Netzwerkdaten“ findet sich in § 62 Nr. 1 und für „Verarbeitung von Netzwerkdaten“ in § 62 Nr. 2.

3 Die Verordnung schließt die Aufzählung der Rechtsgrundlagen mit dem Wort 等 ab. Dieses zeigt das Ende der Aufzählung an. Daraus lässt sich aber weder ableiten, dass die Aufzählung abschließend noch exemplarisch ist.

4 „Cybersicherheitsgesetz der Volksrepublik China“ (中华人民共和国网络安全法) vom 7.11.2016, chinesisch-deutsch in: ZChinR 2018, S. 213 ff. (im Folgenden als „CyberSichG“ abgekürzt).

5 „Gesetz der Volksrepublik China zur Datensicherheit“ (中华人民共和国数据安全法) vom 10.6.2021, chinesischer und englischer Text 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(EN) (im Folgenden als „DatenSichG“ abgekürzt).

6 „Gesetz der Volksrepublik China zum Schutz persönlicher Daten“ (中华人民共和国个人信息保护法) vom 20.8.2021, chinesisch-deutsch in: ZChinR 2021, S. 286 ff. (im Folgenden als „PersDatenSchG“ abgekürzt).

ZChinR 2025: S. 175–196
DOI: 10.71163/zchinr.2025.175-196

**第二条** 在中华人民共和国境内开展网络数据处理活动及其安全监督管理，适用本条例。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，符合《中华人民共和国个人信息保护法》第三条第二款规定情形的，也适用本条例。

在中华人民共和国境外开展网络数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

**§ 2 [Räumlicher Anwendungsbereich]** Diese Verordnung findet Anwendung auf die Entfaltung der Verarbeitung von Netzwerkdaten und Verwaltung von Sicherheit [und] Aufsicht innerhalb des Gebiets der Volksrepublik China.[7]

Diese Verordnung findet auch Anwendung auf die außerhalb des Gebiets der Volksrepublik China [stattfindende] Verarbeitung persönlicher Daten natürlicher Personen innerhalb des Gebiets der Volksrepublik China, wenn ein Umstand des § 3 Nr. 2 des „Gesetzes der Volksrepublik China zum Schutz persönlicher Daten" vorliegt.

Werden bei der Entfaltung der Verarbeitung von Netzwerkdaten außerhalb des Gebiets der Volksrepublik China die staatliche Sicherheit, öffentliche Interessen oder legale Rechte [und] Interessen von Bürgern [oder] Organisationen geschädigt, wird nach dem Recht die Haftung verfolgt.

**第三条** 网络数据安全管理工作坚持中国共产党的领导，贯彻总体国家安全观，统筹促进网络数据开发利用与保障网络数据安全。

**§ 3 [Grundsätze der Verwaltung von Netzwerkdaten]** Die Verwaltungsarbeit zur Netzwerkdatensicherheit unterliegt der Führung der Kommunistischen Partei Chinas [und] setzt das umfassende Konzept staatlicher Sicherheit[8] um, plant umfassend die Förderung der Entwicklung [und] Nutzung von Netzwerkdaten und die Gewährleistung der Netzwerkdatensicherheit.

**第四条** 国家鼓励网络数据在各行业、各领域的创新应用，加强网络数据安全防护能力建设，支持网络数据相关技术、产品、服务创新，开展网络数据安全宣传教育和人才培养，促进网络数据开发利用和产业发展。

**§ 4 [Staatliche Motivation]** Der Staat ermutigt innovative Anwendung von Netzwerkdaten in jeder Branche und auf jedem Gebiet, den Aufbau von Fähigkeiten zum Schutz von Netzwerkdaten zu stärken, Innovationen in Technologie, Waren [und] Dienste im Zusammenhang mit Netzwerkdaten zu unterstützen, Propaganda, Bildung und Talentbildung bei der Netzwerkdatensicherheit zu entfalten [und] Entwicklung, Nutzung und industrielle Entwicklung von Netzwerkdaten zu fördern.

**第五条** 国家根据网络数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对网络数据实行分类分级保护。

**§ 5 [Staatlicher Schutzmaßstab]** Der Staat nimmt einen klassifizierten und eingestuften Schutz von Netzwerkdaten aufgrund der Wichtigkeit von Netzwerkdaten für die sozioökonomische Entwicklung und des im Falle des Erleidens von Verfälschung, Zerstörung [oder] Weitergabe oder illegalen Erhaltens [oder] illegaler Nutzung für die staatliche Sicherheit, öffentliche Interessen oder legale Rechte [oder] Interessen von Einzelpersonen [oder] Organisationen entstehenden Gefahrenniveaus vor.

**第六条** 国家积极参与网络数据安全相关国际规则和标准的制定，促进国际交流与合作。

**§ 6 [Internationale Zusammenarbeit]** Der Staat nimmt aktiv an der Festlegung der internationalen Regeln und Standards teil, die in Zusammenhang mit der Netzwerkdatensicherheit stehen, [und] fördert internationalen Austausch und Kooperation.

7 Der Geltungsbereich dieser Verordnung schließt Hongkong, Macau und Taiwan nicht mit ein.

8 Das „umfassende Konzept staatlicher Sicherheit" wurde 2014 durch Xi Jinping auf der ersten Sitzung der Kommission für staatliche Sicherheit der KPCh verkündet. Es verbindet verschiedene Themen aus den Gebieten politischer, wirtschaftlicher, finanzieller und technologischer Sicherheit und Cybersicherheit. *Kerry Liu*, The economics of China's Holistic View of National Security: A preliminary assessment, in: Economic Affairs, abrufbar im Internet: <https://doi.org/10.1111/ecaf.12646> (Stand: 12.3.2025).

**第七条** 国家支持相关行业组织按照章程，制定网络数据安全行为规范，加强行业自律，指导会员加强网络数据安全保护，提高网络数据安全保护水平，促进行业健康发展。

**§ 7 [Staatliche Unterstützung von Branchenorganisationen]** Der Staat unterstützt betreffende Branchenorganisationen nach ihrer Satzung beim Erlass eines Verhaltenskodex für die Netzwerkdatensicherheit, bei der Stärkung der Selbstkontrolle, bei der Anleitung von Mitgliedern, die Netzwerkdatensicherheit zu schützen, bei der Anhebung des Schutzniveaus der Netzwerkdatensicherheit [und] bei der Förderung einer gesunden Entwicklung der Branche.[9]

## 第二章 一般规定

## 2. Kapitel: Allgemeine Bestimmungen

**第八条** 任何个人、组织不得利用网络数据从事非法活动，不得从事窃取或者以其他非法方式获取网络数据、非法出售或者非法向他人提供网络数据等非法网络数据处理活动。

**§ 8 [Verbot illegaler Verarbeitung von Netzwerkdaten, Verbot der Beihilfe]** Keine Einzelperson [oder] Organisation darf Netzwerkdaten für illegale Aktivitäten nutzen, darf Netzwerkdaten stehlen oder durch andere illegale Mittel erhalten [oder] Netzwerkdaten illegal verkaufen oder illegal einer anderen Person bereitstellen [oder sonst] Netzwerkdaten illegal verarbeiten.

任何个人、组织不得提供专门用于从事前款非法活动的程序、工具；明知他人从事前款非法活动的，不得为其提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助。

Keine Einzelperson [oder] Organisation darf Programme [und] Werkzeuge, die speziell für die Vornahme der im vorigen Absatz [genannten] illegalen Aktivitäten nutzbar sind, bereitstellen; wer weiß, dass ein anderer in den im vorigen Absatz [genannten] illegalen Aktivitäten tätig ist, darf [diesem] seinen Internetzugang, sein Server-Hosting, seinen Netzwerkspeicher, seinen Kommunikationstransport [oder andere] technische Unterstützung nicht bereitstellen oder Hilfe leisten [etwa] durch die Verbreitung von Werbung [oder] Zahlungsabwicklung.

**第九条** 网络数据处理者应当依照法律、行政法规的规定和国家标准的强制性要求，在网络安全等级保护的基础上，加强网络数据安全防护，建立健全网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用，处置网络数据安全事件，防范针对和利用网络数据实施的违法犯罪活动，并对所处理网络数据的安全承担主体责任。

**§ 9 [Allgemeine Pflichten der Verarbeiter von Netzwerkdaten]** Verarbeiter von Netzwerkdaten[10] müssen nach den Bestimmungen in Gesetzen, Verwaltungsrechtsnormen[11] und zwingenden Anforderungen staatlicher Standards auf Grundlage eines mehrstufigen Schutzes der Netzwerksicherheit den Schutz der Netzwerkdatensicherheit verstärken, ein starkes Verwaltungssystem für Netzwerkdatensicherheit errichten, technische Maßnahmen [wie etwa] Verschlüsselung, Datensicherung, Zugangskontrolle[12], Sicherheitszertifizierung und andere notwendige Maßnahmen ergreifen, Netzwerkdaten vor Verfälschung, Zerstörung, Weitergabe oder illegalem Erhalten [und] illegaler Nutzung schützen, Netzwerkdatensicherheitsvorfälle handhaben, rechtswidrigen kriminellen Aktivitäten vorbeugen, die gegen Netzwerkdaten gerichtet sind und diese ausnutzen, und für die Sicherheit der verarbeiteten Netzwerkdaten die Haftung als Subjekt tragen

9 Die Branchenorganisationen sind gemäß § 10 DatenSichG (Fn. 5) zu den genannten Aufgaben verpflichtet.

10 Eine Definition für „Verarbeiter von Netzwerkdaten“ findet sich in § 62 Nr. 3.

11 Die genannten „Verwaltungsrechtsnormen“ beziehen sich gemäß § 72 Gesetzgebungsgesetz der Volksrepublik China (中华人民共和国立法法) vom 15.3.2000 in der Fassung vom 13.3.2023 (chinesisch-deutsch in: ZChinR 2023, S. 87 ff.) ausschließlich auf Rechtsakte des Staatrates.

12 „访问控制“ bedeutet wörtlich „Besuchskontrolle“.

**第十条** 网络数据处理者提供的网络产品、服务应当符合相关国家标准的强制性要求；发现网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告；涉及危害国家安全、公共利益的，网络数据处理者还应当在 24 小时内向有关主管部门报告。

**§ 10 [Pflichten der Verarbeiter von Netzwerkdaten in Bezug auf Netzwerkprodukte und -dienste]** Von Verarbeitern von Netzwerkdaten bereitgestellte Netzwerkprodukte [und] -dienste müssen den betreffenden zwingenden Anforderungen staatlicher Standards entsprechen; werden an den Netzwerkprodukten [oder] -diensten bestehende Sicherheitsmängel, -lücken [oder andere] Risiken entdeckt, müssen sofort Abhilfemaßnahmen ergriffen, nach den Bestimmungen unverzüglich die Nutzer benachrichtigt sowie der betreffenden zuständigen Abteilung Bericht erstattet werden; soweit die staatliche Sicherheit [oder] öffentliche Interessen gefährdet sind, muss der Verarbeiter von Netzwerkdaten auch innerhalb von 24 Stunden der betreffenden zuständigen Abteilung Bericht erstatten.

**第十一条** 网络数据处理者应当建立健全网络数据安全事件应急预案，发生网络数据安全事件时，应当立即启动预案，采取措施防止危害扩大，消除安全隐患，并按照规定向有关主管部门报告。

**§ 11 [Pflicht der Verarbeiter von Netzwerkdaten zum Aufstellen eines Notfallplans für Sicherheitsvorfälle; Benachrichtigungspflichten]** Verarbeiter von Netzwerkdaten müssen einen starken Notfallplan für Netzwerkdatensicherheitsvorfälle errichten; tritt ein Netzwerkdatensicherheitsvorfall ein, muss sofort der Plan ausgeführt, Maßnahmen zur Verhinderung der Ausweitung der Gefährdung ergriffen, latente Sicherheitsgefahren beseitigt sowie nach den Bestimmungen der betreffenden zuständigen Abteilung Bericht erstattet werden.

网络数据安全事件对个人、组织合法权益造成危害的，网络数据处理者应当及时将安全事件和风险情况、危害后果、已经采取的补救措施等，以电话、短信、即时通信工具、电子邮件或者公告等方式通知利害关系人；法律、行政法规规定可以不通知的，从其规定。网络数据处理者在处置网络数据安全事件过程中发现涉嫌违法犯罪线索的，应当按照规定向公安机关、国家安全机关报案，并配合开展侦查、调查和处置工作。

Entsteht durch den Netzwerkdatensicherheitsvorfall eine Gefahr für legale Rechte [und] Interessen von Einzelpersonen [oder] Organisationen, muss der Verarbeiter der Netzwerkdaten unverzüglich mittels Telefons, Kurznachricht, Instant-Messaging-Dienst, E-Mail oder öffentlicher Bekanntmachung [oder durch andere] Mittel Interessierten[13] über den Sicherheitsvorfall und die Risikosituation, die Konsequenzen der Gefährdung [und] die bereits ergriffenen Abhilfemaßnahmen benachrichtigen; bestimmen Gesetze [oder] Verwaltungsrechtsnormen, dass nicht benachrichtigt werden muss,[14] gelten diese Bestimmungen. Entdeckt der Verarbeiter von Netzwerkdaten im Verlauf der Handhabung von Netzwerkdatensicherheitsvorfällen verdächtige rechtswidrige kriminelle Spuren, muss er nach den Bestimmungen den Behörden für öffentliche Sicherheit [und] den staatlichen Sicherheitsbehörden[15] Anzeige erstatten sowie beim Entfalten von Ermittlungs-, Untersuchungs- und Handhabungsarbeiten kooperieren.

13 Wörtlich: „[dazu] in einer Beziehung von Nutzen und Schaden stehende Person".

14 Wörtlich: „bestimmen Gesetze [und] Verwaltungsrechtsnormen, dass es möglich ist, nicht zu benachrichtigen […]".

15 Sowohl die Behörden für öffentliche Sicherheit (公安机关) als auch die staatlichen Sicherheitsbehörden (国家安全机关) sind Verwaltungsbehörden, die für die Ermittlung unrechtmäßigen Verhaltens zuständig sind. Sie unterscheiden sich allerdings in ihren Aufgaben: Die Hauptaufgabe der staatlichen Sicherheitsbehörden ist die Wahrung der Staatssicherheit, etwa durch die Verhinderung von Straftaten wie der Spionage oder anderer schwerwiegender Aktivitäten. Die Behörden für öffentliche Sicherheit sind zuständig für die Verhinderung und Ermittlung bezüglich anderer, geringschwelligerer krimineller Aktivitäten. Siehe die betreffende Anmerkung zum CyberSichG (Fn. 4) in der Übersetzung von *Peter Leibküchler*, in: ZChinR 2018, S. 119 (dort: Fn. 21).

**第十二条** 网络数据处理者向其他网络数据处理者提供、委托处理个人信息和重要数据的，应当通过合同等与网络数据接收方约定处理目的、方式、范围以及安全保护义务等，并对网络数据接收方履行义务的情况进行监督。向其他网络数据处理者提供、委托处理个人信息和重要数据的处理情况记录，应当至少保存 3 年。

**§ 12 [Pflichten bei der Bereitstellung bestimmter Daten an andere Verarbeiter von Netzwerkdaten]** Wenn ein Verarbeiter von Netzwerkdaten anderen Verarbeitern von Netzwerkdaten persönliche Daten und wichtige Daten[16] bereitstellt [oder] sie mit [deren] Verarbeitung beauftragt[17], muss er etwa durch Vertrag mit der Empfängerseite [etwa] die Verarbeitungszwecke, -mittel, -bereiche sowie die Pflichten zum Schutz der Sicherheit vereinbaren sowie die Erfüllung der Pflichten durch die Empfängerseite der Netzwerkdaten beaufsichtigen. Die Aufzeichnungen über persönliche Daten und wichtige Daten, die anderen Verarbeitern von Netzwerkdaten bereitgestellt [oder] mit deren Verarbeitung andere [Verarbeiter von Netzwerkdaten] beauftragt werden, müssen mindestens drei Jahre aufbewahrt werden.

网络数据接收方应当履行网络数据安全保护义务，并按照约定的目的、方式、范围等处理个人信息和重要数据。

Die Empfängerseite von Netzwerkdaten muss ihre Pflichten zum Schutz der Netzwerkdatensicherheit erfüllen sowie die persönlichen Daten und wichtigen Daten nach den vereinbarten Zwecken, Mitteln und Bereichen verarbeiten.

两个以上的网络数据处理者共同决定个人信息和重要数据的处理目的和处理方式的，应当约定各自的权利和义务。

Entscheiden mehrere Verarbeiter von Netzwerkdaten gemeinsam die Verarbeitungszwecke und Verarbeitungsmittel persönlicher Daten und wichtiger Daten, müssen die jeweiligen Rechte und Pflichten vereinbart werden.

**第十三条** 网络数据处理者开展网络数据处理活动，影响或者可能影响国家安全的，应当按照国家有关规定进行国家安全审查。

**§ 13 [Pflicht der Verarbeiter von Netzwerkdaten zur Durchführung von Sicherheitstests]** Verarbeiter von Netzwerkdaten, die beim Entfalten der Verarbeitung von Netzwerkdaten die staatliche Sicherheit beeinflussen oder beeinflussen können, müssen nach den betreffenden staatlichen Bestimmungen einen staatlichen Sicherheitstest durchführen.

**第十四条** 网络数据处理者因合并、分立、解散、破产等原因需要转移网络数据的，网络数据接收方应当继续履行网络数据安全保护义务。

**§ 14 [Pflichten bei der Übermittlung von Netzwerkdaten]** Wenn für Verarbeiter von Netzwerkdaten wegen Vereinigung, Spaltung, Auflösung, Konkurs [oder anderer] Ursachen die Übermittlung von Netzwerkdaten notwendig ist, muss die Empfängerseite der Netzwerkdaten die Erfüllung der Pflichten zum Schutz der Netzwerkdatensicherheit fortführen.

**第十五条** 国家机关委托他人建设、运行、维护电子政务系统，存储、加工政务数据，应当按照国家有关规定经过严格的批准程序，明确受托方的网络数据处理权限、保护责任等，监督受托方履行网络数据安全保护义务。

**§ 15 [Pflichten staatlicher Behörden bei der Beauftragung anderer]** Beauftragen staatliche Behörden einen anderen mit dem Aufbau, Betrieb [oder] Schutz elektronischer Verwaltungssysteme[18] [oder] der Speicherung [oder] Bearbeitung von amtlichen Daten[19], müssen [die staatlichen Behörden] nach den betreffenden staatlichen Bestimmungen ein strenges Genehmigungsverfahren durchführen, [etwa] eindeutig benennen, welche Befugnisse [und] Verantwortungen zur Datenverarbeitung der Beauftragte hat, [und] überwachen, dass der Beauftragte die Pflichten zum Schutz der Netzwerkdatensicherheit erfüllt.

16 Eine Definition für „wichtige Daten“ findet sich in § 62 Nr. 4.

17 Eine Definition für „Beauftragung mit der Verarbeitung“ findet sich in § 62 Nr. 5.

18 „电子政务系统“ bedeutet wörtlich „Systeme elektronischer Regierungsangelegenheiten“. Gemeint sind hiermit elektronisch funktionierende Systeme der öffentlichen Verwaltung.

19 „政务数据“ bedeutet wörtlich „Daten zu Regierungsangelegenheiten“.

**第十六条** 网络数据处理者为国家机关、关键信息基础设施运营者提供服务，或者参与其他公共基础设施、公共服务系统建设、运行、维护的，应当依照法律、法规的规定和合同约定履行网络数据安全保护义务，提供安全、稳定、持续的服务。

**§ 16 [Pflichten von beauftragten Verarbeitern von Netzwerkdaten für den öffentlichen Sektor]** Wenn Verarbeiter von Netzwerkdaten für staatliche Behörden [oder] Betreiber wesentlicher Informationsinfrastrukturen Dienste anbieten oder beteiligt sind am Aufbau, Betrieb [oder] Schutz anderer öffentlicher Infrastruktur [oder] Systeme des öffentlichen Dienstes, müssen sie auf Grundlage von Gesetzen, Rechtsnormen und Vertragsvereinbarungen ihre Pflichten zum Schutz der Netzwerkdatensicherheit erfüllen [und] sichere, stabile [und] andauernde Dienste erbringen.

前款规定的网络数据处理者未经委托方同意，不得访问、获取、留存、使用、泄露或者向他人提供网络数据，不得对网络数据进行关联分析。

Die im vorherigen Absatz bestimmten Verarbeiter von Netzwerkdaten dürfen ohne Zustimmung des Auftraggebers die Netzwerkdaten nicht abrufen[20], herunterladen[21], speichern, nutzen, weitergeben oder anderen zur Verfügung stellen [und] dürfen nicht die Verbindung [zwischen] Netzwerkdaten analysieren.

**第十七条** 为国家机关提供服务的信息系统应当参照电子政务系统的管理要求加强网络数据安全管理，保障网络数据安全。

**§ 17 [Pflichten staatlichen Behörden Dienstleistungen anbietender Informationssysteme]** Ein Informationssystem, das für staatliche Behörden Dienste anbietet, muss entsprechend den Verwaltungsanforderungen des elektronischen Verwaltungssystems die Verwaltung der Netzwerkdatensicherheit stärken und die Netzwerkdatensicherheit gewährleisten.

**第十八条** 网络数据处理者使用自动化工具访问、收集网络数据，应当评估对网络服务带来的影响，不得非法侵入他人网络，不得干扰网络服务正常运行。

**§ 18 [Pflicht der Verarbeiter von Netzwerkdaten bei der Verwendung automatisierter Werkzeuge]** Verarbeiter von Netzwerkdaten, die automatisierte Werkzeuge zum Abrufen [oder] Sammeln von Netzwerkdaten verwenden, müssen den damit einhergehenden Einfluss auf Netzwerkdienste bewerten, dürfen nicht illegal in die Netzwerke anderer eindringen [und] dürfen nicht den ordnungsgemäßen Betrieb der Netzwerkdienste stören.

**第十九条** 提供生成式人工智能服务的网络数据处理者应当加强对训练数据和训练数据处理活动的安全管理，采取有效措施防范和处置网络数据安全风险。

**§ 19 [Pflichten von künstliche Intelligenz anbietenden Verarbeitern von Netzwerkdaten]** Verarbeiter von Netzwerkdaten, die Dienste generativer künstlicher Intelligenz anbieten, müssen die Sicherheit der Verwaltung im Hinblick auf die Trainingsdaten und die Verarbeitung der Trainingsdaten verstärken [und] wirksame Maßnahmen zur Vorbeugung und Handhabung von Risiken für die Netzwerkdatensicherheit ergreifen.

**第二十条** 面向社会提供产品、服务的网络数据处理者应当接受社会监督，建立便捷的网络数据安全投诉、举报渠道，公布投诉、举报方式等信息，及时受理并处理网络数据安全投诉、举报。

**§ 20 [Pflichten der Verarbeiter von Netzwerkdaten bei der Bereitstellung von Waren und Diensten für die Gesellschaft]** Verarbeiter von Netzwerkdaten, die für die Gesellschaft[22] Waren und Dienste bereitstellen, müssen sich der öffentlichen Aufsicht unterstellen, einen bequemen Kanal für Beschwerden und Anzeigen zur Netzwerkdatensicherheit errichten, Beschwerde- [und] Anzeigeformen [sowie ähnliche] Informationen öffentlich bekannt machen [und] Beschwerden [und] Anzeigen zur Netzwerkdatensicherheit unverzüglich annehmen und bearbeiten.[23]

20 „访问“ bedeutet wörtlich „besuchen“. Hier ist damit aber der Aufruf oder die Inaugenscheinnahme der Netzwerkdaten gemeint.

21 „获取“ bedeutet wörtlich „erhalten“.

22 Gemeint ist hier die öffentliche Gesellschaft.

23 „处理“ hier aufgrund des Kontextes und in Abgrenzung zur Verarbeitung von Netzwerkdaten als „bearbeiten“ übersetzt.

## 第三章　个人信息保护

**第二十一条**　网络数据处理者在处理个人信息前，通过制定个人信息处理规则的方式依法向个人告知的，个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容明确具体、清晰易懂，包括但不限于下列内容：

（一）网络数据处理者的名称或者姓名和联系方式；

（二）处理个人信息的目的、方式、种类，处理敏感个人信息的必要性以及对个人权益的影响；

（三）个人信息保存期限和到期后的处理方式，保存期限难以确定的，应当明确保存期限的确定方法；

（四）个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的方法和途径等。

网络数据处理者按照前款规定向个人告知收集和向其他网络数据处理者提供个人信息的目的、方式、种类以及网络数据接收方信息的，应当以清单等形式予以列明。网络数据处理者处理不满十四周岁未成年人个人信息的，还应当制定专门的个人信息处理规则。

**第二十二条**　网络数据处理者基于个人同意处理个人信息的，应当遵守下列规定：

（一）收集个人信息为提供产品或者服务所必需，不得超范围收集个人信息，不得通过误导、欺诈、胁迫等方式取得个人同意；

## 3. Kapitel: Schutz persönlicher Daten

**§ 21 [Anforderung an die Information über die Regeln für die Verarbeitung persönlicher Daten[24]]** Informieren Verarbeiter von Netzwerkdaten vor der Verarbeitung persönlicher Daten Einzelpersonen nach dem Recht im Wege festgelegter Regeln für die Verarbeitung persönlicher Daten, müssen die Regeln für die Verarbeitung persönlicher Daten zentral öffentlich vorgeführt, einfach abrufbar sowie an einer auffälligen Stelle platziert werden, einen deutlich benannten, konkreten, klaren [und] verständlichen Inhalt haben [und] folgende Inhalte umfassen, ohne darauf begrenzt zu sein:

1. die Bezeichnung oder der Name und die Kontaktmöglichkeiten[25] des Verarbeiters von Netzwerkdaten;

2. die Zwecke, Mittel [und] Arten der Verarbeitung persönlicher Daten, die Notwendigkeit der Verarbeitung sensibler persönlicher Daten und die Auswirkungen auf die Rechte [und] Interessen der Einzelperson;

3. die Speicherfrist von persönlichen Daten und die Formen der Verarbeitung nach Ablauf [der Speicherfrist]; falls die Speicherfrist schwierig zu bestimmen ist, muss deutlich benannt werden, nach welchen Methoden die Speicherfrist bestimmt wird;

4. die Methoden und Wege einer Einzelperson, [ihre] persönlichen Informationen einzusehen, zu kopieren, zu übermitteln, zu berichtigen, zu ergänzen, zu löschen [oder] die Verarbeitung einzuschränken sowie [ihr] Konto zu schließen [und] Einwilligungen zu widerrufen.

Informieren Verarbeiter von Netzwerkdaten Einzelpersonen nach den Bestimmungen des vorherigen Absatzes über Zwecke, Mittel und Arten von gesammelten und anderen Verarbeitern von Netzwerkdaten bereitgestellten persönlichen Daten und über die Informationen der Empfängerseite von Netzwerkdaten, müssen sie in Formen [wie etwa] einer Liste aufgeführt werden. Verarbeiten Verarbeiter von Netzwerkdaten persönliche Daten von Minderjährigen, die jünger als 14 Lebensjahre sind, müssen sie auch spezielle Regeln für die Verarbeitung [ihrer] persönlichen Daten festlegen.

**§ 22 [Pflichten der Verarbeiter von Netzwerkdaten bei der Verarbeitung persönlicher Daten auf Grundlage einer Einwilligung[26]]** Verarbeiten Verarbeiter von Netzwerkdaten auf Grundlage einer Einwilligung der [betroffenen] Person persönliche Daten, müssen sie folgende Bestimmungen einhalten:

1. Ist das Sammeln von persönlichen Daten für das Anbieten von Waren und Diensten notwendig, darf der Umfang[27] der gesammelten persönlichen Daten nicht überschritten werden [und] darf die Einwilligung der [betroffenen] Person

24 Die Informationspflicht ergibt sich für den Verarbeiter aus § 17 PersDatenSchG (Fn. 6).

25 „联系方式“ bedeutet wörtlich „Kontaktformen“.

26 Die Voraussetzungen für eine wirksame Einwilligung ergeben sich aus § 14 PersDatenSchG (Fn. 6).

27 Gemäß § 6 Abs. 2 PersDatenSchG (Fn. 6) dürfen persönliche Daten nur in dem für die Realisierung des Verwendungszweckes notwendigen Maß gesammelt werden.

nicht durch Mittel [wie etwa] Irreführung, Täuschung [oder] Drohung erlangt werden;

（二）处理生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息的，应当取得个人的单独同意；

2. werden sensible persönliche Daten [wie etwa] über biometrische Erkennungsverfahren, Religion [oder] Glauben, eine bestimmte Identität, medizinische Behandlung, Gesundheit, Finanzkonten, Aufenthaltsort [oder] Ortswechsel verarbeitet, muss eine separate Einwilligung[28] der [betroffenen] Einzelperson eingeholt werden;

（三）处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意；

3. werden persönliche Daten von Minderjährigen, die jünger als 14 Lebensjahre sind, verarbeitet, muss die Einwilligung der Eltern oder eines anderen Vormunds der Minderjährigen eingeholt werden;

（四）不得超出个人同意的个人信息处理目的、方式、种类、保存期限处理个人信息；

4. die Zwecke, Mittel, Arten und Speicherfrist der Verarbeitung persönlicher Daten dürfen nicht über die Einwilligung der [betroffenen] Einzelperson hinausgehen;

（五）不得在个人明确表示不同意处理其个人信息后，频繁征求同意；

5. nachdem die [betroffene] Person ausdrücklich erklärt, nicht in die Verarbeitung ihrer persönlichen Informationen einzuwilligen, darf die Einwilligung nicht wiederholt ersucht werden;

（六）个人信息的处理目的、方式、种类发生变更的，应当重新取得个人同意。

6. wenn sich die Zwecke, Mittel [oder] Arten der Verarbeitung persönlicher Daten ändern, muss erneut die Einwilligung der [betroffenen] Einzelperson eingeholt werden.

法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

Bestimmen Gesetze [oder] Verwaltungsrechtsnormen, dass für die Verarbeitung sensibler persönlicher Daten eine schriftliche Einwilligung eingeholt werden muss, gelten diese Bestimmungen.

**第二十三条** 个人请求查阅、复制、更正、补充、删除、限制处理其个人信息，或者个人注销账号、撤回同意的，网络数据处理者应当及时受理，并提供便捷的支持个人行使权利的方法和途径，不得设置不合理条件限制个人的合理请求。

**§ 23 [Pflichten der Verarbeiter von Netzwerkdaten im Umgang mit den Rechten von Einzelpersonen bei der Verarbeitung persönlicher Daten**[29]**]** Fordert eine Einzelperson Einsicht, Kopie, Berichtigung, Ergänzung, Löschung [oder] Beschränkung der Verarbeitung ihrer persönlichen Daten oder schließt [sie ihr] Konto [oder] widerruft [sie ihre] Einwilligung, muss der Verarbeiter von Netzwerkdaten [dies] unverzüglich annehmen und Einzelpersonen bequeme Unterstützung bei den Methoden und Wegen zur Ausübung [ihrer] Rechte bereitstellen [und] darf keine unvernünftigen Voraussetzungen stellen, die vernünftige Forderungen von Einzelpersonen beschränken.

**第二十四条** 因使用自动化采集技术等无法避免采集到非必要个人信息或者未依法取得个人同意的个人信息，以及个人注销账号的，网络数据处理者应当删除个人信息或者进行匿名化处理。法律、行政法规规定的保存期限未届满，或者删除、匿名化处理个人信息从技术上难以实现的，网络数据处理者应当停止除存储和采取必要的安全保护措施之外的处理。

**§ 24 [Pflichten der Verarbeiter von Netzwerkdaten bei Unmöglichkeit der rechtmäßigen Datenerhebung]** Kann wegen der Verwendung automatisierter Sammeltechnologien [oder aus anderen Gründen] nicht verhindert werden, dass nicht notwendige persönliche Daten gesammelt, Einwilligungen von Einzelpersonen nicht nach dem Recht eingeholt oder Konten von Einzelpersonen geschlossen werden, müssen Verarbeiter von Netzwerkdaten die persönlichen Daten löschen oder eine Anonymisierung durchführen. Ist die durch Gesetze [oder] Verwaltungsrechtsnormen bestimmte Speicherfrist nicht abgelaufen [oder] ist das Löschen [und] Anonymisieren

28 Definition für „separate Einwilligung“ in § 62 Rn. 7.

29 Die Rechte der betroffenen Einzelpersonen bei der Verarbeitung ihrer persönlichen Daten ergeben sich aus dem 4. Kapitel des PersDatenSchG (Fn. 6).

der persönlichen Daten technisch schwierig, müssen Verarbeiter von Netzwerkdaten die Verarbeitung, außer solche des Speicherns und des Ergreifens notwendiger Sicherheits- [und] Schutzmaßnahmen, einstellen.

**第二十五条** 对符合下列条件的个人信息转移请求，网络数据处理者应当为个人指定的其他网络数据处理者访问、获取有关个人信息提供途径:

**§ 25 [Voraussetzungen für das Fordern der Übertragung persönlicher Daten,[30] Gebühren]** Wird entsprechend den folgenden Voraussetzungen gefordert, persönliche Daten zu übertragen, müssen Verarbeiter von Netzwerkdaten einem anderen Verarbeiter von Netzwerkdaten, der durch die [betroffene] Einzelperson bestimmt wurde, Wege zum Abrufen [und] Herunterladen der betreffenden persönlichen Daten bereitstellen:

(一)能够验证请求人的真实身份;

1. Die wahre Identität des Fordernden kann bestätigt werden;

(二) 请求转移的是本人同意提供的或者基于合同收集的个人信息;

2. die geforderten persönlichen Daten werden aufgrund eigener Einwilligung bereitgestellt oder auf Grundlage eines Vertrags gesammelt;

(三) 转移个人信息具备技术可行性;

3. die Übertragung der persönlichen Daten ist technisch möglich;

(四) 转移个人信息不损害他人合法权益。

4. die Übertragung der persönlichen Daten schädigt nicht die legalen Rechte [oder] Interessen anderer.

请求转移个人信息次数等明显超出合理范围的, 网络数据处理者可以根据转移个人信息的成本收取必要费用。

Übersteigt die Häufigkeit an Forderungen zur Übertragung persönlicher Daten offensichtlich einen vernünftigen Umfang, können Verarbeiter von Netzwerkdaten notwendige Ausgaben entsprechend den Kosten für die Übertragung persönlicher Daten einziehen.

**第二十六条** 中华人民共和国境外网络数据处理者处理境内自然人个人信息, 依照《中华人民共和国个人信息保护法》第五十三条规定在境内设立专门机构或者指定代表的，应当将有关机构的名称或者代表的姓名、联系方式等报送所在地设区的市级网信部门；网信部门应当及时通报同级有关主管部门。

**§ 26 [Pflichten ausländischer Verarbeiter von Netzwerkdaten]** Verarbeiter von Netzwerkdaten außerhalb des Gebiets der Volksrepublik China, die persönliche Daten von natürlichen Einzelpersonen innerhalb des [chinesischen] Gebiets verarbeiten [und] nach den Bestimmungen des § 53 des „Gesetzes der Volksrepublik China zum Schutz persönlicher Daten“ innerhalb des [chinesischen] Gebiets ein spezielles Organ errichten oder einen Repräsentanten bestimmen, müssen die Bezeichnung des betreffenden Organs oder den Namen, die Kontaktmöglichkeiten und andere [Informationen] des Repräsentanten den örtlichen Abteilungen für Netzwerke [und] Informationen auf der Ebene der in Bezirke aufgeteilten Städte melden; die Abteilungen für Netzwerke [und] Informationen müssen unverzüglich den betreffenden zuständigen Abteilungen derselben Ebene Bericht erstatten.

**第二十七条** 网络数据处理者应当定期自行或者委托专业机构对其处理个人信息遵守法律、行政法规的情况进行合规审计。

**§ 27 [Pflichten der Verarbeiter von Netzwerkdaten zur Vornahme periodischer Compliance Audits]** Verarbeiter von Netzwerkdaten müssen selbst oder [durch] Beauftragung eines Fachorgans im Hinblick auf die Umstände, wie sie bei ihrer Verarbeitung persönlicher Daten die Gesetze [und] Verwaltungsrechtsnormen einhalten, periodisch Compliance Audits vornehmen.

30 Das Recht der betroffenen Einzelperson, die Übertragung persönlicher Daten zu fordern, ergibt sich aus § 45 Abs. 3 PersDatenSchG (Fn. 6).

**第二十八条** 网络数据处理者处理1000万人以上个人信息的，还应当遵守本条例第三十条、第三十二条对处理重要数据的网络数据处理者（以下简称重要数据的处理者）作出的规定。

**§ 28 [Pflichten der Verarbeiter von Netzwerkdaten einer Vielzahl von Personen]** Verarbeiter von Netzwerkdaten, die persönliche Daten von 10 Millionen oder mehr Personen verarbeiten, müssen auch die Bestimmungen der §§ 30 [und] 32 dieser Verordnung für Verarbeiter von Netzwerkdaten, die wichtige Daten verarbeiten (nachfolgend abgekürzt: Verarbeiter wichtiger Daten), einhalten.

## 第四章 重要数据安全

## 4. Kapitel: Sicherheit wichtiger Daten

**第二十九条** 国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、的重要数据具体目录，对列入目录的网络数据进行重点保护。

**§ 29 [Katalog wichtiger Daten, Pflichten der Verarbeiter von Netzwerkdaten zur Identifizierung und Meldung]** Der Koordinationsmechanismus zur Arbeit der staatlichen Datensicherheit[31] plant umfassend die Koordination betreffender Abteilungen, Kataloge wichtiger Daten festzulegen, [und] verstärkt den Schutz wichtiger Daten. Alle Regionen [und] alle Abteilungen müssen nach dem klassifizierten und eingestuften Schutzsystem von Netzwerkdaten[32] Kataloge wichtiger Daten für ihre Region, ihre Abteilung sowie für betreffende Branchen [und] Gebiete deutlich benennen [und] die im Katalog enthaltenen Netzwerkdaten schwerpunktmäßig schützen.

网络数据处理者应当按照国家有关规定识别、申报重要数据。对确认为重要数据的，相关地区、部门应当及时向网络数据处理者告知或者公开发布。网络数据处理者应当履行网络数据安全保护责任。

Verarbeiter von Netzwerkdaten müssen nach den betreffenden staatlichen Bestimmungen wichtige Daten identifizieren[33] [und] melden. Werden sie als wichtige Daten bestätigt, müssen betreffende Regionen [oder] Abteilungen unverzüglich den Verarbeiter von Netzwerkdaten benachrichtigen oder [die Bestätigung] öffentlich bekannt machen. Verarbeiter von Netzwerkdaten müssen ihre Verantwortung zum Schutz von Netzwerkdaten erfüllen.

国家鼓励网络数据处理者使用数据标签标识等技术和产品，提高重要数据安全管理水平。

Der Staat ermutigt Verarbeiter von Netzwerkdaten zur Nutzung von Identifikation mit Labeln [oder ähnlichen] Technologien und Waren, [um] das Niveau der Verwaltung der Sicherheit wichtiger Daten zu erhöhen.

**第三十条** 重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。网络数据安全管理机构应当履行下列网络数据安全保护责任：

**§ 30 [Verantwortlicher und Verwaltungsapparat für die Netzwerkdatensicherheit, Befugnis direkter Berichterstattung, Sicherheitsüberprüfung]** Verarbeiter wichtiger Daten müssen eindeutig Verantwortliche für die Netzwerkdatensicherheit und Verwaltungsorgane für die Netzwerkdatensicherheit benennen. Das Verwaltungsorgan für die Netzwerkdatensicherheit muss folgende Pflichten[34] zum Schutz von Netzwerkdaten erfüllen:

（一）制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案；

1. ein Verwaltungssystem für die Netzwerkdatensicherheit, Betriebsbestimmungen und einen Notfallplan für Netzwerkdatensicherheitsvorfälle festlegen und umsetzen;

（二）定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件；

2. eine periodische Entfaltung von Risikoüberwachung, Risikobewertung, Notfallübung, Propaganda, Bildung, Schulung [und] anderer Aktivitäten zur Netzwerkdatensicherheit organisieren [und] Netzwerkdatensicherheitsrisiken und [Netzwerkdatensicherheits-]Vorfälle unverzüglich handhaben;

31 Dieser Mechanismus wurde auf Grundlage von § 5 DatenSichG (Fn. 5) durch das zentrale Führungsorgan der zentralen staatlichen Sicherheit, ein Gremium unter der Führung der KPCh, errichtet.

32 Vgl. im Hinblick auf das hier erwähnte klassifizierte und eingestufte Schutzsystem von Netzwerkdaten § 5.

33 „识别“ bedeutet wörtlich „unterscheiden“.

34 Hier wird „责任“ (sonst „Verantwortung“ oder „Haftung“) abweichend als „Pflichten“ übersetzt.

（三）受理并处理网络数据安全投诉、举报。

网络数据安全负责人应当具备网络数据安全专业知识和相关管理工作经历，由网络数据处理者管理层成员担任，有权直接向有关主管部门报告网络数据安全情况。

掌握有关主管部门规定的特定种类、规模的重要数据的网络数据处理者，应当对网络数据安全负责人和关键岗位的人员进行安全背景审查，加强相关人员培训。审查时，可以申请公安机关、国家安全机关协助。

**第三十一条** 重要数据的处理者提供、委托处理、共同处理重要数据前，应当进行风险评估，但是属于履行法定职责或者法定义务的除外。

风险评估应当重点评估下列内容：

（一）提供、委托处理、共同处理网络数据，以及网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要；

（二）提供、委托处理、共同处理的网络数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利益或者个人、组织合法权益带来的风险；

（三）网络数据接收方的诚信、守法等情况；

（四）与网络数据接收方订立或者拟订立的相关合同中关于网络数据安全的要求能否有效约束网络数据接收方履行网络数据安全保护义务；

3. Beschwerden [und] Anzeigen zur Netzwerkdatensicherheit annehmen und bearbeiten.

Der Verantwortliche für die Netzwerkdatensicherheit muss spezielle Kenntnisse zur Netzwerkdatensicherheit und Verwaltungsarbeit betreffende Erfahrung besitzen; der Verarbeiter von Netzwerkdaten ist wegen des Fungierens als Mitglied der Verwaltungsebene berechtigt, der betreffenden zuständigen Abteilung direkt Bericht über die Situation der Netzwerkdatensicherheit zu erstatten.

Verarbeiter von Netzwerkdaten, welche wichtige Daten besonderer Arten [und] Ausmaße, die von der betreffenden zuständigen Abteilung bestimmt wurden, beherrschen, müssen eine Überprüfung des sicherheitsrelevanten Hintergrunds[35] der Verantwortlichen für die Netzwerkdatensicherheit und des Personals auf Schlüsselpositionen durchführen [und] die Schulung betreffenden Personals verstärken. Für die Zeit der Überprüfung können sie die Hilfe der Behörden für öffentliche Sicherheit [und] der staatlichen Sicherheitsbehörden beantragen.

**§ 31 [Pflicht der Verarbeiter wichtiger Daten zur Risikobewertung bei Übertragung wichtiger Daten]** Verarbeiter wichtiger Daten müssen vor der Bereitstellung, Beauftragung mit der Verarbeitung [oder] gemeinsamen Verarbeitung[36] von wichtigen Daten eine Risikobewertung durchführen, es sei denn, dies gehört zur Erfüllung gesetzlich bestimmter Amtspflichten oder gesetzlich bestimmter Pflichten.

Die Risikobewertung muss schwerpunktmäßig folgende Inhalte bewerten:

1. ob die Bereitstellung, Beauftragung mit der Verarbeitung [oder] gemeinsame Verarbeitung von Netzwerkdaten sowie die Zwecke, Mittel [und] Bereiche der Verarbeitung der Netzwerkdaten durch die Empfängerseite der Netzwerkdaten legal, gerechtfertigt [und] notwendig sind;

2. Risiken der Bereitstellung, Beauftragung mit der Verarbeitung [oder] gemeinsamen Verarbeitung von Netzwerkdaten für Verfälschung, Zerstörung, Weitergabe oder illegalen Erhalt [und] illegale Nutzung sowie damit einhergehende Risiken für die staatliche Sicherheit, öffentliche Interessen oder die legalen Rechte [und] Interessen von Einzelpersonen [und] Organisationen;

3. Redlichkeit[37], Rechtstreue [und andere] Umstände der Empfängerseite von Netzwerkdaten;

4. ob die Anforderungen, welche die Netzwerkdatensicherheit betreffen, im mit der Empfängerseite von Netzwerkdaten abgeschlossenen oder abzuschließen geplanten Vertrag die Empfängerseite von Netzwerkdaten wirksam an die Erfüllung der Pflichten zum Schutz der Netzwerkdatensicherheit binden;

35 „安全背景“ bedeutet wörtlich „Sicherheitshintergrund“.

36 Eine Definition von „gemeinsam verarbeiten“ findet sich in § 62 Nr. 6.

37 Normalerweise steht der Ausdruck „诚信“ abgekürzt für „Treu und Glauben“.

（五）采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险；

（六）有关主管部门规定的其他评估内容。

5. ob ergriffene oder zu ergreifen geplante technische oder verwaltende Maßnahmen wirksam der Verfälschung, Zerstörung, Weitergabe oder dem illegalen Erhalt, der illegaler Nutzung [oder anderen] Risiken vorbeugen;

6. andere Bewertungsinhalte, welche die betreffende zuständige Abteilung bestimmt.

**第三十二条** 重要数据的处理者因合并、分立、解散、破产等可能影响重要数据安全的，应当采取措施保障网络数据安全，并向省级以上有关主管部门报告重要数据处置方案、接收方的名称或者姓名和联系方式等；主管部门不明确的，应当向省级以上数据安全工作协调机制报告。

**§ 32 [Pflichten der Verarbeiter wichtiger Daten im Falle von Vereinigung, Spaltung, Auflösung, Konkurs und ähnlicher Umstände]** Verarbeiter wichtiger Daten müssen, wenn sie wegen Vereinigung, Spaltung, Auflösung, Konkurs [oder anderen] Ursachen die Netzwerkdatensicherheit beeinflussen können, Maßnahmen zur Gewährleistung der Netzwerkdatensicherheit ergreifen und der betreffenden zuständigen Abteilung auf Provinzebene [oder einer] höheren [Ebene] Bericht erstatten über das Konzept zur Handhabung wichtiger Daten [und] die Bezeichnung oder den Namen und die Kontaktmöglichkeiten der Empfängerseite; ist die zuständige Abteilung unklar,[38] muss dem Koordinationsmechanismus zur Arbeit der staatlichen Datensicherheit auf Provinzebene [oder einer] höheren [Ebene] Bericht erstattet werden.

**第三十三条** 重要数据的处理者应当每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告，有关主管部门应当及时通报同级网信部门、公安机关。

**§ 33 [Pflicht der Verarbeiter wichtiger Daten zur jährlichen Risikobewertung ihrer Verarbeitung von Netzwerkdaten]** Verarbeiter wichtiger Daten müssen jedes Jahr eine Risikobewertung ihrer Verarbeitung von Netzwerkdaten entfalten sowie der betreffenden zuständigen Abteilung auf Provinzebene [oder einer] höheren [Ebene] einen Risikobewertungsbericht melden; die betreffende zuständige Abteilung muss unverzüglich den Abteilungen für Netzwerke [und] Informationen und der Behörde für öffentliche Sicherheit Bericht erstatten.

风险评估报告应当包括下列内容：

Der Risikobewertungsbericht muss folgende Inhalte umfassen:

（一）网络数据处理者基本信息、网络数据安全管理机构信息、网络数据安全负责人姓名和联系方式等；

1. grundlegende Informationen des Verarbeiters von Netzwerkdaten, Informationen zum Verwaltungsorgan für die Netzwerkdatensicherheit, Name und Kontaktmöglichkeiten des Verantwortlichen für die Netzwerkdatensicherheit;

（二）处理重要数据的目的、种类、数量、方式、范围、存储期限、存储地点等，开展网络数据处理活动的情况，不包括网络数据内容本身；

2. Zwecke, Arten, Mengen, Mittel, Bereiche, Speicherfristen [und] Speicherorte der verarbeiteten wichtigen Netzwerkdaten [und] Umstände der Entfaltung der Verarbeitung von Netzwerkdaten, was nicht den Inhalt der verarbeiteten Netzwerkdaten selbst umfasst;

（三）网络数据安全管理制度及实施情况，加密、备份、标签标识、访问控制、安全认证等技术措施和其他必要措施及其有效性；

3. das Verwaltungssystem für die Netzwerkdatensicherheit und dessen Umsetzungssituation, die Verschlüsselung, Datensicherung, Identifizierung mit Labels, Zugangskontrolle, Sicherheitszertifizierung [und sonstige] technische Maßnahmen und andere notwendige Maßnahmen sowie deren Wirksamkeit;

（四）发现的网络数据安全风险，发生的网络数据安全事件及处置情况；

4. entdeckte Risiken für die Netzwerkdatensicherheit, eingetretene Sicherheitsvorfälle sowie die Handhabung der Situation;

（五）提供、委托处理、共同处理重要数据的风险评估情况；

5. die Situation der Bewertung von Risiken bei Bereitstellung, Beauftragung mit der Verarbeitung [oder] gemeinsamer Verarbeitung wichtiger Daten;

38 Gemeint ist die Unklarheit über die Zuständigkeit.

（六）网络数据出境情况；

（七）有关主管部门规定的其他报告内容。

处理重要数据的大型网络平台服务提供者报送的风险评估报告，除包括前款规定的内容外，还应当充分说明关键业务和供应链网络数据安全等情况。

重要数据的处理者存在可能危害国家安全的重要数据处理活动的，省级以上有关主管部门应当责令其采取整改或者停止处理重要数据等措施。重要数据的处理者应当按照有关要求立即采取措施。

6. die Situation der ausgehenden Netzwerkdaten;

7. andere Berichtinhalte, welche die betreffende zuständige Abteilung bestimmt.

Die gemeldeten Risikobewertungsberichte großer Netzwerkplattformendiensteanbieter[39], die wichtige Daten verarbeiten, müssen außer den von den Bestimmungen des vorigen Absatzes umfassten Inhalten auch vollständig die Netzwerkdatensicherheit in ihrer wesentlichen Geschäftstätigkeit und Lieferkette [und anderen] Situationen erklären.

Gibt es bei Verarbeitern wichtiger Daten die Verarbeitung wichtiger Daten, welche die staatliche Sicherheit gefährden können, muss die betreffende zuständige Abteilung auf Provinzebene [oder einer] höheren [Ebene] anordnen, dass diese Maßnahmen [wie etwa] die Korrektur oder die Beendigung der Verarbeitung wichtiger Daten ergreifen müssen. Die Verarbeiter wichtiger Daten müssen nach den betreffenden Anforderungen sofort Maßnahmen ergreifen.

## 第五章　网络数据跨境安全管理

## 5. Kapitel: Die Sicherheit der Verwaltung grenzüberschreitender Netzwerkdaten

**第三十四条**　国家网信部门统筹协调有关部门建立国家数据出境安全管理专项工作机制，研究制定国家网络数据出境安全管理相关政策，协调处理网络数据出境安全重大事项。

**§ 34 [Staatlicher Arbeitsmechanismus zur Verwaltung ausgehender Daten, Erlass von Politnormen]** Die staatlichen Abteilungen für Netzwerke [und] Informationen[40] planen umfassend die Koordination betreffender Abteilungen bei der Errichtung eines speziellen Arbeitsmechanismus, der die Sicherheit ausgehender Daten verwaltet, [die staatlichen Abteilungen für Netzwerke und Informationen] erforschen Politnormen[41], welche die Sicherheit der Verwaltung ausgehender Netzwerkdaten betreffen [und] legen solche fest [und] koordinieren wichtige Angelegenheiten der Sicherheit der Verwaltung ausgehender Netzwerkdaten.

**第三十五条**　符合下列条件之一的，网络数据处理者可以向境外提供个人信息：

（一）通过国家网信部门组织的数据出境安全评估；

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

（三）符合国家网信部门制定的关于个人信息出境标准合同的规定；

**§ 35 [Voraussetzungen für die Bereitstellung persönlicher Daten außerhalb des Gebiets der VR China]** Liegt eine der folgenden Voraussetzungen vor, können Verarbeiter von Netzwerkdaten persönliche Daten außerhalb des Gebiets [der VR China] bereitstellen:

1. [Sie] haben eine durch die staatlichen Abteilungen für Netzwerke [und] Informationen organisierte Sicherheitsbewertung für ausgehende Daten bestanden;

2. nach den Bestimmungen der staatlichen Abteilungen für Netzwerke [und] Informationen hat ein Fachorgan den Schutz persönlicher Daten zertifiziert;

3. [die Bereitstellung] entspricht den Bestimmungen der Standardverträge der staatlichen Abteilungen für Netzwerke [und] Informationen bezüglich ausgehender persönlicher Daten;

39 Das Wort „groß“ bezieht sich nur auf die Netzwerkplattformen selbst; eine Definition für „große Netzwerkplattformen“ findet sich in § 62 Nr. 8.

40 „国家网信部门“ schließt nicht nur die sog. „Cyberspace Administration of China“ (CAC, 中华人民共和国国家互联网信息办公室), die identisch mit dem sog. „Office of the Central Cyberspace Affairs Commission“(中共中央网络安全和信息化委员会办公室) ist, sondern auch staatliche Abteilungen für Netzwerke und Informationen aller Stufen ein. Siehe die betreffende Anmerkung zum CyberSichG (Fn. 4) in der Übersetzung von *Peter Leibküchler*, in: ZChinR 2018, S. 115 (dort: Fn. 8).

41 Politnormen sind Normen eines mehrstufigen Systems von Parteinormen, die durch die Kommunistische Partei Chinas oder Untergliederungen dieser erlassen werden. Siehe hierzu ausführlich *Harro von Senger*, Einführung in das chinesische Recht, 1994, S. 300.

（四）为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息；

4. es ist für Abschluss [oder] Erfüllung eines Vertrags, bei dem eine Einzelperson eine Vertragspartei ist, wirklich notwendig, außerhalb des Gebiets [der VR China] persönliche Daten bereitzustellen;

（五）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息；

5. es ist nach Arbeitsregelsystemen, die nach dem Recht festgelegt wurden, und Kollektivverträgen, die nach dem Recht geschlossen [und] unterzeichnet wurden, für die Umsetzung grenzüberschreitenden Personalmanagements wirklich notwendig, außerhalb des Gebiets [der VR China] persönliche Daten von Mitarbeitern bereitzustellen;

（六）为履行法定职责或者法定义务，确需向境外提供个人信息；

6. es ist zur Erfüllung gesetzlich bestimmter Amtspflichten oder gesetzlich bestimmter Pflichten wirklich notwendig, außerhalb des Gebiets [der VR China] persönliche Daten bereitzustellen;

（七）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息；

7. es ist aufgrund dringender Umstände zum Schutz des Lebens, der Gesundheit und der Sicherheit von Vermögen natürlicher Personen wirklich notwendig, außerhalb des Gebiets [der VR China] persönliche Daten bereitzustellen;

（八）法律、行政法规或者国家网信部门规定的其他条件。

8. andere durch Gesetze, Verwaltungsrechtsnormen [oder] von den staatlichen Abteilungen für Netzwerke [und] Informationen bestimmte Voraussetzungen [liegen vor].

**第三十六条** 中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

**§ 36 [Weitere mögliche Voraussetzungen völkerrechtlicher Verträge oder Abkommen]** Enthalten internationale Verträge [oder] Abkommen, welche die Volksrepublik China geschlossen hat oder an denen [sie] sich beteiligt, Bestimmungen [wie etwa] über Voraussetzungen für die Bereitstellung persönlicher Daten an [einen anderen] außerhalb des Gebiets der Volksrepublik China, kann nach diesen Bestimmungen verfahren werden.

**第三十七条** 网络数据处理者在中华人民共和国境内运营中收集和产生的重要数据确需向境外提供的，应当通过国家网信部门组织的数据出境安全评估。网络数据处理者按照国家有关规定识别、申报重要数据，但未被相关地区、部门告知或者公开发布为重要数据的，不需要将其作为重要数据申报数据出境安全评估。

**§ 37 [Voraussetzungen für und Pflichten bei Bereitstellung wichtiger Daten ins Ausland]** Ist es für Verarbeiter von Netzwerkdaten wirklich notwendig, wichtige Daten, die während des Betriebs innerhalb der Volksrepublik China gesammelt und produziert wurden, außerhalb des Gebiets [der VR China] bereitzustellen, müssen sie eine durch die staatlichen Abteilungen für Netzwerke [und] Informationen organisierte Sicherheitsbewertung für ausgehende Daten bestehen. Verarbeiter von Netzwerkdaten müssen wichtige Daten nach den betreffenden staatlichen Bestimmungen identifizieren und melden, aber [sie] müssen keine Sicherheitsbewertung grenzüberschreitender Daten als wichtige Daten melden, wenn [die Daten] von den betreffenden Abteilungen [oder] Regionen nicht als wichtige Daten gemeldet oder öffentlich bekannt gemacht worden sind.

**第三十八条** 通过数据出境安全评估后，网络数据处理者向境外提供个人信息和重要数据的，不得超出评估时明确的数据出境目的、方式、范围和种类、规模等。

**§ 38 [Bindung der Verarbeiter von Netzwerkdaten an die in der Sicherheitsbewertung benannten Umstände]** Stellt ein Verarbeiter von Netzwerkdaten persönliche Daten und wichtige Daten außerhalb des Gebiets [der VR China] zur Verfügung, nachdem er die Sicherheitsbewertung für ausgehende Daten bestanden hat, darf er die Zwecke, Mittel, Bereiche und Arten, Ausmaße [und sonstigen Umstände] der ausgehenden Netzwerkdaten, die im Zeitpunkt der Bewertung deutlich benannt wurden, nicht überschreiten.

**第三十九条** 国家采取措施，防范、处置网络数据跨境安全风险和威胁。任何个人、组织不得提供专门用于破坏、避开技术措施的程序、工具等；明知他人从事破坏、避开技术措施等活动的，不得为其提供技术支持或者帮助。

**§ 39 [Staatlicher Schutzauftrag, Verbot der Bereitstellung gefährlicher Mittel gegen technische Maßnahmen, Verbot der Beihilfe]** Der Staat ergreift Maßnahmen zur Vorbeugung und Handhabung von Risiken und Bedrohungen für die Sicherheit grenzüberschreitender Netzwerkdaten. Keine Einzelperson [oder] Organisation darf Programme, Werkzeuge [oder] Ähnliches bereitstellen, die speziell zum Zerstören [oder] Umgehen technischer Maßnahmen nutzbar sind; wer weiß, dass ein anderer in der Zerstörung [oder] Umgehung technischer Maßnahmen [oder] ähnlicher Aktivitäten tätig ist, darf diesem keine technische Unterstützung oder Hilfe bereitstellen.

## 第六章 网络平台服务提供者义务

## 6. Kapitel: Pflichten von Netzwerkplattformendiensteanbietern

**第四十条** 网络平台服务提供者应当通过平台规则或者合同等明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务，督促第三方产品和服务提供者加强网络数据安全管理。

**§ 40 [Benennung von Pflichten zur Netzwerkdatensicherheit, Haftung, Versicherung von Schäden]** Netzwerkplattformendiensteanbieter müssen durch Plattformregeln oder Vertrag [oder Ähnliches] Pflichten zum Schutz der Netzwerkdatensicherheit für Drittanbieter von Waren und Diensten, die ihre Plattformen betreten, deutlich benennen [und] Drittanbieter von Waren und Dienstleistungen zur Verstärkung der Sicherheit der Verwaltung von Netzwerkdaten anhalten.

预装应用程序的智能终端等设备生产者，适用前款规定。

Auf Produzenten von smarten Endgeräten[42], auf denen Anwendungsprogramme vorinstalliert sind, [und] anderer Anlagen finden die Bestimmungen des vorigen Absatzes Anwendung.

第三方产品和服务提供者违反法律、行政法规的规定或者平台规则、合同约定开展网络数据处理活动，对用户造成损害的，网络平台服务提供者、第三方产品和服务提供者、预装应用程序的智能终端等设备生产者应当依法承担相应责任。

Verstoßen Drittanbieter von Waren und Diensten bei der Entfaltung der Verarbeitung von Netzwerkdaten gegen Bestimmungen aus Gesetzen oder Verwaltungsrechtsnormen oder Plattformregeln [oder] Vertragsvereinbarungen [und] entsteht für Nutzer ein Schaden, müssen Netzwerkplattformendiensteanbieter, Drittanbieter von Waren und Diensten [und] Produzenten von smarten Endgeräten, auf denen Anwendungsprogramme vorinstalliert sind, [und] anderer Anlagen nach dem Recht entsprechend die Haftung tragen.

国家鼓励保险公司开发网络数据损害赔偿责任险种，鼓励网络平台服务提供者、预装应用程序的智能终端等设备生产者投保。

Der Staat ermutigt Versicherungsgesellschaften, eine Versicherungsart für die Haftung auf Schadensersatz bei der Verletzung von Netzwerkdaten zu entwickeln, [und] motiviert Netzwerkplattformendiensteanbieter [und] Produzenten vorinstallierter Anwendungsprogramme auf smarten Endgeräten [und] andere Anlagen, eine Versicherung abzuschließen.

**第四十一条** 提供应用程序分发服务的网络平台服务提供者，应当建立应用程序核验规则并开展网络数据安全相关核验。发现待分发或者已分发的应用程序不符合法律、行政法规的规定或者国家标准的强制性要求的，应当采取警示、不予分发、暂停分发或者终止分发等措施。

**§ 41 [App-Verteilungsdienste]** Netzwerkplattformendiensteanbieter, die Verbreitungsdienste für Anwendungsprogramme[43] bereitstellen, müssen Überprüfungsregeln für Anwendungsprogramme errichten und betreffende Überprüfungen der Netzwerkdatensicherheit entfalten. Wird entdeckt, dass zu verbreitende oder bereits verbreitete Anwendungsprogramme Gesetzen, Verwaltungsrechtsnormen oder zwingenden Anforderungen staatlicher Standards nicht entsprechen, müssen Maßnahmen [wie etwa] Warnung, Nichtgewährung

42 Mit dem Begriff der „smarten Endgeräte“ dürften Geräte wie Smartphones, Tablets, Smart-TVs oder Smartwatches gemeint sein.

43 Gemeint sein dürften hier Dienste, die der Verbreitung von Software an Endnutzer dienen, also App-Verteilungsdienste wie etwa „Google Play Store“ oder „Apple App Store“.

der Verbreitung, vorläufige Einstellung der Verbreitung oder Beendigung der Verbreitung ergriffen werden.

**第四十二条** 网络平台服务提供者通过自动化决策方式向个人进行信息推送的，应当设置易于理解、便于访问和操作的个性化推荐关闭选项，为用户提供拒绝接收推送信息、删除针对其个人特征的用户标签等功能。

**§ 42 [Nutzung automatisierter Entscheidungsfindung für Push-Benachrichtigungen]** Netzwerkplattformendiensteanbieter, die durch Mittel automatisierter Entscheidungsfindung Push-Benachrichtigungen gegenüber Einzelpersonen durchführen, müssen einfach verständliche, bequem abrufbare und durchführbare Optionen zum Ablehnen[44] personalisierter Empfehlungen einrichten [und] den Nutzern Funktionen [wie etwa] zum Ablehnen des Empfangs von Push-Benachrichtigungen [und] zum Löschen von Nutzer-Tags, die auf ihre persönlichen Merkmale ausgerichtet sind, bereitstellen.

**第四十三条** 国家推进网络身份认证公共服务建设，按照政府引导、用户自愿原则进行推广应用。

**§ 43 [Öffentliche Dienste zur Zertifizierung von Internet-Identitäten]** Der Staat treibt den Aufbau öffentlicher Dienste zur Zertifizierung von Internet-Identitäten voran [und] bewirbt deren Anwendung nach der Führung der Regierung [und] dem Grundsatz der Freiwilligkeit der Nutzer.

鼓励网络平台服务提供者支持用户使用国家网络身份认证公共服务登记、核验真实身份信息。

[Der Staat] motiviert Netzwerkplattformendiensteanbieter dazu, Nutzer zu unterstützen, öffentliche Dienste zur Zertifizierung von Internet-Identitäten zu benutzen, [um] wahre Identitätsinformationen einzutragen und zu überprüfen.

**第四十四条** 大型网络平台服务提供者应当每年度发布个人信息保护社会责任报告，报告内容包括但不限于个人信息保护措施和成效、个人行使权利的申请受理情况、主要由外部成员组成的个人信息保护监督机构履行职责情况等。

**§ 44 [Jährlicher Datenschutzbericht großer Netzwerkplattformendiensteanbieter]** Große Netzwerkplattformendiensteanbieter müssen jedes Jahr einen Bericht über [ihre] gesellschaftliche Verantwortung zum Schutz persönlicher Daten bekannt machen; der Berichtsinhalt muss Maßnahmen zum Schutz persönlicher Daten und [deren] Effekte, die Situation der beantragten und bearbeiteten Rechte, die von Einzelpersonen ausgeübt worden sind, [und] die Situation der Erfüllung von Amtspflichten durch die Organe zur Überprüfung des Schutzes persönlicher Daten, die hauptsächlich aus externen Mitgliedern bestehen,[45] umfassen, ohne darauf begrenzt zu sein.

**第四十五条** 大型网络平台服务提供者跨境提供网络数据，应当遵守国家数据跨境安全管理要求，健全相关技术和管理措施，防范网络数据跨境安全风险。

**§ 45 [Pflichten bei grenzüberschreitendem Datenverkehr großer Netzwerkplattformendiensteanbieter]** Stellen große Netzwerkplattformendiensteanbieter grenzüberschreitend Netzwerkdaten bereit, müssen sie die staatlichen Anforderungen an die Sicherheit der Verwaltung grenzüberschreitender Daten einhalten, betreffende technische und verwaltende Maßnahmen stärken [und] Sicherheitsrisiken grenzüberschreitender Netzwerkdaten vorbeugen.

**第四十六条** 大型网络平台服务提供者不得利用网络数据、算法以及平台规则等从事下列活动：

**§ 46 [Verbot bestimmter Aktivitäten für große Netzwerkplattformendiensteanbieter]** Große Netzwerkplattformendiensteanbieter dürfen Netzwerkdaten, Algorithmen sowie Plattformregeln nicht nutzen, um folgende Aktivitäten auszuüben:

（一）通过误导、欺诈、胁迫等方式处理用户在平台上产生的网络数据；

1. Daten, die Nutzer auf der Plattform produziert haben, durch Mittel [wie etwa] Irreführung, Täuschung [oder] Drohung verarbeiten;

（二）无正当理由限制用户访问、使用其在平台上产生的网络数据；

2. Nutzer ohne rechtfertigenden Grund einschränken, ihre auf der Plattform produzierten Daten abzurufen [und] zu nutzen;

44 „关闭“ bedeutet wörtlich „schließen“.

45 Die Pflicht zur Gründung solcher Organe ergibt sich aus § 58 Nr. 1 PersDatenSchG (Fn. 6).

（三）对用户实施不合理的差别待遇，损害用户合法权益；

3. gegenüber Nutzern unvernünftige Ungleichbehandlungen umsetzen [oder] legale Rechte [oder] Interessen der Nutzer schädigen;

（四）法律、行政法规禁止的其他活动。

4. andere Aktivitäten, die durch Gesetze [oder] Verwaltungsrechtsnormen verboten sind.

## 第七章　监督管理

## 7. Kapitel: Aufsicht [und] Verwaltung

**第四十七条**　国家网信部门负责统筹协调网络数据安全和相关监督管理工作。

**§ 47 [Zuständige Abteilungen, Amtspflichten]** Die staatlichen Abteilungen für Netzwerke [und] Informationen sind verantwortlich für die umfassende Planung der Koordination der Netzwerkdatensicherheit und betreffender Aufsichts- [und] Verwaltungsarbeiten.

公安机关、国家安全机关依照有关法律、行政法规和本条例的规定，在各自职责范围内承担网络数据安全监督管理职责，依法防范和打击危害网络数据安全的违法犯罪活动。

Die Behörden für öffentliche Sicherheit [und] die staatlichen Sicherheitsbehörden tragen nach betreffenden Bestimmungen in Gesetzen, Verwaltungsrechtsnormen und dieser Verordnung im Bereich der jeweiligen Amtspflichten die Amtspflichten zur Aufsicht [und] Verwaltung der Netzwerkdatensicherheit [und] beugen nach dem Recht rechtswidrigen kriminellen Aktivitäten, welche die Netzwerkdatensicherheit gefährden, vor und bekämpfen [diese].

国家数据管理部门在具体承担数据管理工作中履行相应的网络数据安全职责。

Während staatliche Abteilungen für Netzwerkdatenverwaltung konkrete Datenverwaltungsarbeiten übernehmen, erfüllen sie die Amtspflichten der Netzwerkdatensicherheit.

各地区、各部门对本地区、本部门工作中收集和产生的网络数据及网络数据安全负责。

Alle Regionen [und] alle Abteilungen sind verantwortlich für die während der Arbeit ihrer Region [oder] ihrer Abteilung gesammelten und produzierten Netzwerkdaten und die Netzwerkdatensicherheit.

**第四十八条**　各有关主管部门承担本行业、本领域网络数据安全监督管理职责，应当明确本行业、本领域网络数据安全保护工作机构，统筹制定并组织实施本行业、本领域网络数据安全事件应急预案，定期组织开展本行业、本领域网络数据安全风险评估，对网络数据处理者履行网络数据安全保护义务情况进行监督检查，指导督促网络数据处理者及时对存在的风险隐患进行整改。

**§ 48 [Amtspflichten betreffender zuständiger Abteilungen]** Alle betreffenden zuständigen Abteilungen tragen die Amtspflichten für die Aufsicht [und] Verwaltung der Netzwerkdatensicherheit ihrer Branchen [und] ihrer Gebiete [und] müssen deutlich Organe für die Arbeit [und] den Schutz der Netzwerkdatensicherheit ihrer Branchen [und] ihrer Gebiete benennen, umfassend Notfallpläne für Netzwerkdatensicherheitsvorfälle ihrer Branchen [und] ihrer Gebiete planen, festlegen und deren Durchführung organisieren, die periodische Entfaltung von Risikobewertungen der Netzwerkdatensicherheit ihrer Branchen [und] ihrer Gebiete organisieren, Aufsicht [und] die Untersuchung der Situation der Erfüllung der Pflichten von Netzwerkdatenverarbeitern zum Schutz von Netzwerkdaten durchführen [und] Netzwerkdatenverarbeiter bei der unverzüglichen Durchführung von Korrekturen bestehender Risiken [und] latenter Gefahren anleiten [und] anhalten.

**第四十九条**　国家网信部门统筹协调有关主管部门及时汇总、研判、共享、发布网络数据安全风险相关信息，加强网络数据安全信息共享、网络数据安全风险和威胁监测预警以及网络数据安全事件应急处置工作。

**§ 49 [Koordination betreffender zuständiger Abteilungen]** Die staatlichen Abteilungen für Netzwerke [und] Informationen planen umfassend die Koordination betreffender zuständiger Abteilungen beim unverzüglichen Zusammentragen, Untersuchen, Beurteilen, Austauschen [und] Bekanntmachen von Netzwerkdatensicherheitsrisiken betreffende Informationen, verstärken den Informationsaustausch zur Netzwerkdatensicherheit, die Überwachung und Frühwarnung von Netzwerkdatensicherheitsrisiken und -bedrohungen sowie die Arbeit zur Handhabung von Netzwerkdatensicherheitsvorfällen [und] -notfällen.

**第五十条** 有关主管部门可以采取下列措施对网络数据安全进行监督检查：

（一）要求网络数据处理者及其相关人员就监督检查事项作出说明；

（二）查阅、复制与网络数据安全有关的文件、记录；

（三）检查网络数据安全措施运行情况；

（四）检查与网络数据处理活动有关的设备、物品；

（五）法律、行政法规规定的其他必要措施。

网络数据处理者应当对有关主管部门依法开展的网络数据安全监督检查予以配合。

**§ 50 [Befugnisse betreffender zuständiger Abteilungen]** Betreffende zuständige Abteilungen können folgende Maßnahmen zur Durchführung von Aufsicht [und] Untersuchung der Netzwerkdatensicherheit ergreifen:

1. [Sie können] von Netzwerkdatenverarbeitern und ihrem betreffenden Personal verlangen, eine Erklärung zu Angelegenheiten der Aufsicht [und] Untersuchung abzugeben;

2. [sie können] Schriftstücke [und] Aufzeichnungen, welche die Netzwerkdatensicherheit betreffen, einsehen [und] kopieren;

3. [sie können] die Betriebssituation[46] von Netzwerkdatensicherheitsmaßnahmen untersuchen;

4. [sie können] Anlagen und Gegenstände, welche die Verarbeitung von Netzwerkdaten betreffen, untersuchen;

5. andere notwendige Maßnahmen, die durch Gesetze [und] Verwaltungsrechtsnormen bestimmt sind.

Verarbeiter von Netzwerkdaten müssen bei der Entfaltung von Aufsicht [und] Untersuchung nach dem Recht durch betreffende zuständige Abteilungen kooperieren.

**第五十一条** 有关主管部门开展网络数据安全监督检查，应当客观公正，不得向被检查单位收取费用。

有关主管部门在网络数据安全监督检查中不得访问、收集与网络数据安全无关的业务信息，获取的信息只能用于维护网络数据安全的需要，不得用于其他用途。

有关主管部门发现网络数据处理者的网络数据处理活动存在较大安全风险的，可以按照规定的权限和程序要求网络数据处理者暂停相关服务、修改平台规则、完善技术措施等，消除网络数据安全隐患。

**§ 51 [Anforderungen an die Ausübung der Befugnisse, zusätzliche Befugnisse bei verhältnismäßig großen Sicherheitsrisiken]** Betreffende zuständige Abteilungen entfalten die Aufsicht [und] die Untersuchung der Netzwerkdatensicherheit, müssen objektiv [und] unparteiisch [sein und] dürfen von den untersuchten Einheiten keine Gebühren einziehen.

Betreffende zuständige Abteilungen dürfen bei der Aufsicht [und] der Untersuchung der Netzwerkdatensicherheit keine geschäftlichen Informationen abrufen [oder] sammeln, die in keinem Zusammenhang zur Netzwerkdatensicherheit stehen; [sie] dürfen erhaltene Informationen nur zum Schutz von Erfordernissen der Netzwerkdatensicherheit verwenden [und] dürfen [diese] nicht für andere Anwendungsbereiche verwenden.

Entdecken betreffende zuständige Abteilungen, dass bei der Verarbeitung von Netzwerkdaten von Verarbeitern von Netzwerkdaten verhältnismäßig große Sicherheitsrisken bestehen, können [sie] nach den bestimmten Befugnissen und Verfahren von Verarbeitern von Netzwerkdaten verlangen, betreffende Dienste vorläufig einzustellen, Plattformregeln anzupassen [oder] technische Maßnahmen zu vervollständigen [und] latente Netzwerkdatensicherheitsgefahren zu beseitigen.

**第五十二条** 有关主管部门在开展网络数据安全监督检查时，应当加强协同配合、信息沟通，合理确定检查频次和检查方式，避免不必要的检查和交叉重复检查。

**§ 52 [Vermeidung unnötiger Aufsicht und Überwachung]** Während betreffende zuständige Abteilungen die Aufsicht [und] die Überwachung der Netzwerkdatensicherheit entfalten, müssen sie die Koordination, die Kooperation [und] den Informationsaustausch verstärken, vernünftige Aufsichtsfrequenzen und Aufsichtsmittel festlegen [und] nicht notwendige Aufsicht und sich überschneidende [und] wiederholende Aufsicht vermeiden.

46 Gemeint ist hier wohl die Situation der Implementierung.

个人信息保护合规审计、重要数据风险评估、重要数据出境安全评估等应当加强衔接，避免重复评估、审计。重要数据风险评估和网络安全等级测评的内容重合的，相关结果可以互相采信。

Compliance Audits zum Schutz persönlicher Daten, Risikobewertungen wichtiger Daten [und] Sicherheitsbewertungen wichtiger ausgehender Daten müssen stärker verbunden [und] wiederholte Bewertungen [und] Audits vermieden werden. Überschneiden sich die Inhalte der Risikobewertungen wichtiger Daten mit [denen] der Einstufung und Bewertung der Netzwerksicherheit,[47] können betreffende Ergebnisse gegenseitig akzeptiert werden.

**第五十三条** 有关主管部门及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等网络数据应当依法予以保密，不得泄露或者非法向他人提供。

**§ 53 [Geheimhaltungspflicht betreffender zuständiger Abteilungen]** Betreffende zuständige Abteilungen und ihr Personal müssen die während der Erfüllung von Amtspflichten zur Kenntnis gelangten persönlichen privaten Angelegenheiten,[48] persönlichen Daten, Geschäftsgeheimnisse, geheim gehaltene Geschäftsinformation [und] andere Netzwerkdaten nach dem Recht geheim halten [und] dürfen [diese] nicht weitergeben oder illegal anderen bereitstellen.

**第五十四条** 境外的组织、个人从事危害中华人民共和国国家安全、公共利益，或者侵害中华人民共和国公民的个人信息权益的网络数据处理活动的，国家网信部门会同有关主管部门可以依法采取相应的必要措施。

**§ 54 [Befugnisse bei staatsgefährdenden Aktivitäten außerhalb des Gebiets der VR China]** Betreiben Organisationen [und] Einzelpersonen außerhalb des Gebiets [der VR China] Verarbeitung von Netzwerkdaten, welche die staatliche Sicherheit [oder] öffentliche Interessen der Volksrepublik China gefährden oder Rechte [und] Interessen persönlicher Daten von Bürgern der Volksrepublik China verletzen, können die staatlichen Abteilungen für Netzwerke [und] Informationen zusammen mit den betreffenden zuständigen Abteilungen nach dem Recht notwendige Maßnahmen ergreifen.

## 第八章 法律责任

## 8. Kapitel: Rechtliche Haftung

**第五十五条** 违反本条例第十二条、第十六条至第二十条、第二十二条、第四十条第一款和第二款、第四十一条、第四十二条规定的，由网信、电信、公安等主管部门依据各自职责责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处 100 万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员可以处 1 万元以上 10 万元以下罚款。

**§ 55 [Sanktionen bei Verstößen gegen Pflichten bei besonderen Arten der Verarbeitung]** Wird gegen die Bestimmungen der §§ 12, 16 bis 20, 22, 40 Abs. 1 und Abs. 2, 41 [oder] 42 dieser Verordnung verstoßen, ordnen zuständige Abteilungen [wie etwa] die für Netzwerke [und] Informationen, Telekommunikation [oder] öffentliche Sicherheit gemäß den jeweiligen Amtspflichten Korrekturen an, verwarnen [und] nehmen rechtswidrige Einkünfte in Beschlag; wird die Korrektur verweigert oder liegen erschwerende Umstände vor, wird eine Geldstrafe in Höhe von bis zu 1.000.000 Yuan verhängt und es kann die vorübergehende Einstellung betreffender Geschäftstätigkeiten, die Betriebsstilllegung zur Korrektur, die Annullierung betreffender betrieblicher Genehmigungen oder die Annullierung der Gewerbeerlaubnis angeordnet werden [und] gegenüber direkt verantwortlichem zuständigem Personal und anderem direkt verantwortlichem Personal eine Geldstrafe in Höhe von 10.000 Yuan bis 100.000 Yuan verhängt werden.

47 Grundlage ist das in § 21 CyberSichG (Fn. 4) durch den Staat implementierte mehrstufige Schutzsystem der Netzwerksicherheit.

48 An anderer Stelle wird „隐私“ als „Privatsphäre“ übersetzt; vgl. etwa § 1032 „Zivilgesetzbuch der Volksrepublik China“ (中华人民共和国民法典) vom 28.5.2020, chinesisch-deutsch in: ZChinR 2020, S. 207 ff.

**第五十六条** 违反本条例第十三条规定的，由网信、电信、公安、国家安全等主管部门依据各自职责责令改正，给予警告，可以并处 10 万元以上 100 万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处 1 万元以上 10 万元以下罚款；拒不改正或者情节严重的，处 100 万元以上 1000 万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处 10 万元以上 100 万元以下罚款。

**§ 56 [Sanktionen bei Verstößen gegen die Pflicht zur Durchführung eines Sicherheitstests gemäß § 13]** Wird gegen die Bestimmungen des § 13 dieser Verordnung verstoßen, ordnen zuständige Abteilungen [wie etwa] die für Netzwerke [und] Informationen, Telekommunikation, öffentliche Sicherheit [oder] staatliche Sicherheit gemäß den jeweiligen Amtspflichten Korrekturen an [und] verwarnen, können eine Geldstrafe in Höhe von 100.000 Yuan bis 1.000.000 Yuan verhängen [und] können gegenüber direkt verantwortlichem zuständigem Personal und anderem direkt verantwortlichem Personal eine Geldstrafe in Höhe von 10.000 Yuan bis 100.000 Yuan verhängen; wird die Korrektur verweigert oder liegen erschwerende Umstände vor, wird eine Geldstrafe in Höhe von 1.000.000 Yuan bis 10.000.000 Yuan verhängt und es kann die vorübergehende Einstellung betreffender Geschäftstätigkeiten, die Betriebsstillegung zur Korrektur, die Annullierung betreffender betrieblichen Genehmigungen oder die Annullierung der Gewerbeerlaubnis angeordnet werden [und] gegenüber direkt verantwortlichem zuständigem Personal und anderem direkt verantwortlichem Personal eine Geldstrafe in Höhe von 100.000 Yuan bis 1.000.000 Yuan verhängt werden.

**第五十七条** 违反本条例第二十九条第二款、第三十条第二款和第三款、第三十一条、第三十二条规定的，由网信、电信、公安等主管部门依据各自职责责令改正，给予警告，可以并处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处 1 万元以上 10 万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处 50 万元以上 200 万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处 5 万元以上 20 万元以下罚款。

**§ 57 [Sanktionen bei Verstößen gegen Pflichten zum Schutz der Sicherheit wichtiger Daten]** Wird gegen die Bestimmungen der §§ 29 Abs. 2, 30 Abs. 2 und 3, 31 [oder] 32 dieser Verordnung verstoßen, ordnen zuständige Abteilungen [wie etwa] die für Netzwerke [und] Informationen, Telekommunikation [oder] öffentliche Sicherheit gemäß den jeweiligen Amtspflichten Korrekturen an, verwarnen [und] können eine Geldstrafe in Höhe von 50.000 Yuan bis 500.000 Yuan verhängen [und] können gegenüber direkt verantwortlichem zuständigem Personal und anderem direkt verantwortlichem Personal eine Geldstrafe in Höhe von 10.000 Yuan bis 100.000 Yuan verhängen; wird die Korrektur verweigert oder kommt es zur Weitergabe großer Mengen an Daten [oder] anderen schwerwiegenden Konsequenzen, wird eine Geldstrafe in Höhe von 500.000 Yuan bis 2.000.000 Yuan verhängt und es kann die vorübergehende Einstellung betreffender Geschäftstätigkeiten, die Betriebsstilllegung zur Korrektur, die Annullierung betreffender betrieblicher Genehmigungen oder die Annullierung der Gewerbeerlaubnis angeordnet werden [und] gegenüber direkt verantwortlichem zuständigem Personal und anderem direkt verantwortlichem Personal eine Geldstrafe in Höhe von 50.000 Yuan bis 200.000 Yuan verhängt werden.

**第五十八条** 违反本条例其他有关规定的，由有关主管部门依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律的有关规定追究法律责任。

**§ 58 [Haftungsverfolgung nach anderen Gesetzen bei Verstoß gegen andere Bestimmungen]** Wird gegen andere betreffende Bestimmungen dieser Verordnung verstoßen, verfolgen betreffende zuständige Abteilungen nach den betreffenden Bestimmungen des „Cybersicherheitsgesetzes der Volksrepublik China“, des „Datensicherheitsgesetzes der Volksrepublik China“, des „Gesetzes der Volksrepublik China zum Schutz persönlicher Daten“ [und] anderer Gesetze die gesetzliche Haftung.

**第五十九条** 网络数据处理者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依照《中华人民共和国行政处罚法》的规定从轻、减轻或者不予行政处罚。

**§ 59 [Milderung, Minderung oder Absehen von Sanktionen]** Bestehen bei dem Verarbeiter von Netzwerkdaten Umstände, dass die gefährlichen Konsequenzen rechtswidrigen Verhaltens von sich aus beseitigt oder gemindert wurden, das rechtswidrige Verhalten leicht und unverzüglich zu korrigieren ist und keine gefährlichen Konsequenzen eingetreten sind oder dass das erste Mal gegen Gesetze verstoßen wurde und die gefährlichen Konsequenzen leicht und unverzüglich zu korrigieren sind, wird nach den Bestimmungen des „Verwaltungsstrafgesetzes der Volksrepublik China“[49] die Verwaltungsstrafe gemildert, gemindert oder von ihr abgesehen werden.

**第六十条** 国家机关不履行本条例规定的网络数据安全保护义务的，由其上级机关或者有关主管部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

**§ 60 [Korrektur bei behördlichem Fehlverhalten]** Erfüllen staatliche Behörden ihre durch diese Verordnung bestimmten Pflichten zum Schutz der Netzwerkdatensicherheit nicht, ordnen die ihnen übergeordnete Behörden oder betreffende zuständige Behörden Korrekturen an; gegenüber direkt verantwortlichem zuständigem Personal und anderem direkt verantwortlichem Personal werden nach dem Recht Disziplinarmaßnahmen verhängt.

**第六十一条** 违反本条例规定，给他人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

**§ 61 [Zivilrechtliche, verwaltungsrechtliche und strafrechtliche Haftung]** Entsteht durch einen Verstoß gegen die Bestimmungen dieser Verordnung einem anderen ein Schaden, wird nach dem Recht die zivilrechtliche Haftung getragen; bildet [der Verstoß] eine Handlung gegen die Verwaltung öffentlicher Sicherheit, wird nach dem Recht eine Sanktion zur Sicherheitsverwaltung verhängt;[50] bildet [der Verstoß] eine Straftat, wird nach dem Recht die strafrechtliche Haftung verfolgt.

## 第九章 附则

## 9. Kapitel: Ergänzende Regeln

**第六十二条** 本条例下列用语的含义：

（一）网络数据，是指通过网络处理和产生的各种电子数据。

（二）网络数据处理活动，是指网络数据的收集、存储、使用、加工、传输、提供、公开、删除等活动。

（三）网络数据处理者，是指在网络数据处理活动中自主决定处理目的和处理方式的个人、组织。

**§ 62 [Definitionen]** Die Bedeutung folgender Begriffe in dieser Verordnung ist:

1. „Netzwerkdaten“ bezeichnet alle elektronischen Daten, welche durch Netzwerke verarbeitet oder produziert werden.

2. „Verarbeitung von Netzwerkdaten“ bezeichnet Aktivitäten [wie etwa] Sammeln, Speichern, Nutzen, Bearbeiten, Transportieren, Bereitstellen, Veröffentlichen [oder] Löschen von Netzwerkdaten.

3. „Verarbeiter von Netzwerkdaten“ bezeichnet Einzelpersonen oder Organisationen, welche selbstständig über die Verarbeitungszwecke und Verarbeitungsmittel der Verarbeitung von Netzwerkdaten entscheiden.

49 „Verwaltungsstrafgesetz der Volksrepublik China“ (中华人民共和国行政处罚法) vom 27.8.2009 in der Fassung vom 22.1.2021, deutsch in der Fassung vom 17.3.1996, in: *Robert Heuser*, „Sozialistischer Rechtsstaat“ und Verwaltungsrecht in der VR China (1982–2002), Hamburg 2003, S. 406 ff.

50 Nach dem „Gesetz der Volksrepublik China über die Strafen zur Regelung der öffentlichen Sicherheit“ (中华人民共和国治安管理处罚法) vom 28.8.2005 in der Fassung vom 26.10.2012, abgedruckt in der Fassung vom 26.10.2012 in: Amtsblatt des Ständigen Ausschusses des Nationalen Volkskongresses (中华人民共和国全国人民代表大会常务委员会公报) 2012, Nr. 6, S. 693 ff.

（四）重要数据，是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

（五）委托处理，是指网络数据处理者委托个人、组织按照约定的目的和方式开展的网络数据处理活动。

（六）共同处理，是指两个以上的网络数据处理者共同决定网络数据的处理目的和处理方式的网络数据处理活动。

（七）单独同意，是指个人针对其个人信息进行特定处理而专门作出具体、明确的同意。

（八）大型网络平台，是指注册用户 5000 万以上或者月活跃用户 1000 万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台。

**第六十三条** 开展核心数据的网络数据处理活动，按照国家有关规定执行。

自然人因个人或者家庭事务处理个人信息的，不适用本条例。

开展涉及国家秘密、工作秘密的网络数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

**第六十四条** 本条例自 2025 年 1 月 1 日起施行。

4. „Wichtige Daten“ bezeichnet Daten bestimmter Gebiete, bestimmter Gruppen, bestimmter Regionen oder [solche], die eine bestimmte Genauigkeit und Ausmaße erreichen, die im Falle der Verfälschung, Zerstörung, Weitergabe oder illegalen Erhalts [oder] illegaler Nutzung die staatliche Sicherheit, den Wirtschaftsbetrieb, die gesellschaftliche Stabilität [oder] die öffentliche Gesundheit und Sicherheit direkt gefährden.

5. „Beauftragung mit der Verarbeitung“ bezeichnet die Beauftragung von Einzelpersonen oder Organisationen durch Verarbeiter von Netzwerkdaten mit der Entfaltung der Verarbeitung von Netzwerkdaten nach vereinbarten Zwecken und Mitteln.

6. „Gemeinsame Verarbeitung“ bezeichnet die Verarbeitung von Netzwerkdaten, bei der zwei oder mehr Verarbeiter von Netzwerkdaten gemeinsam über die Verarbeitungszwecke und Verarbeitungsmittel der Verarbeitung von Netzwerkdaten entscheiden.

7. „Separate Einwilligung“ bezeichnet die speziell abgegebene spezifische [und] deutliche Einwilligung einer Einzelperson, welche auf die Durchführung bestimmter Verarbeitungen ihrer persönlichen Daten gerichtet ist.

8. „Große Netzwerkplattformen“ bezeichnen Netzwerkplattformen mit 50.000.000 oder mehr registrierten Nutzern oder 10.000.000 oder mehr monatlich aktiven Nutzern, mit komplizierten Geschäftstypen [oder solche], die auf die staatliche Sicherheit, den Wirtschaftsbetrieb [oder] die Lebenshaltung der Bevölkerung einen wichtigen Einfluss haben.

**§ 63 [Kerndaten, Haushaltsprivileg, Staats- und Arbeitsgeheimnisse]** Die Entfaltung der Verarbeitung von Netzwerkdaten von Kerndaten[51] erfolgt nach den betreffenden staatlichen Bestimmungen.

Auf die Verarbeitung persönlicher Daten, die eine natürliche Person wegen persönlicher oder familiärer Angelegenheiten vornimmt, findet diese Verordnung keine Anwendung.

Auf die Entfaltung der Verarbeitung von Netzwerkdaten, welche Staatsgeheimnisse [oder] Arbeitsgeheimnisse betrifft, finden die Bestimmungen des „Gesetzes der Volksrepublik China zum Schutz von Staatsgeheimnissen“ [und] weitere Gesetze [und] Verwaltungsrechtsnormen Anwendung.

**§ 64 [Inkrafttreten]** Diese Verordnung wird vom 1. Januar 2025 an durchgeführt.

Übersetzung, Paragrafenüberschriften in eckigen Klammern und Anmerkungen von Jack J. Zipke, Halle (Saale)

51 Zu Kerndaten gehören gemäß § 21 Abs. 2 DatenSichG (Fn. 5) solche mit Bezug etwa zur staatlichen Sicherheit, der Lebensader der Volkswirtschaft oder wichtigen öffentlichen Interessen.