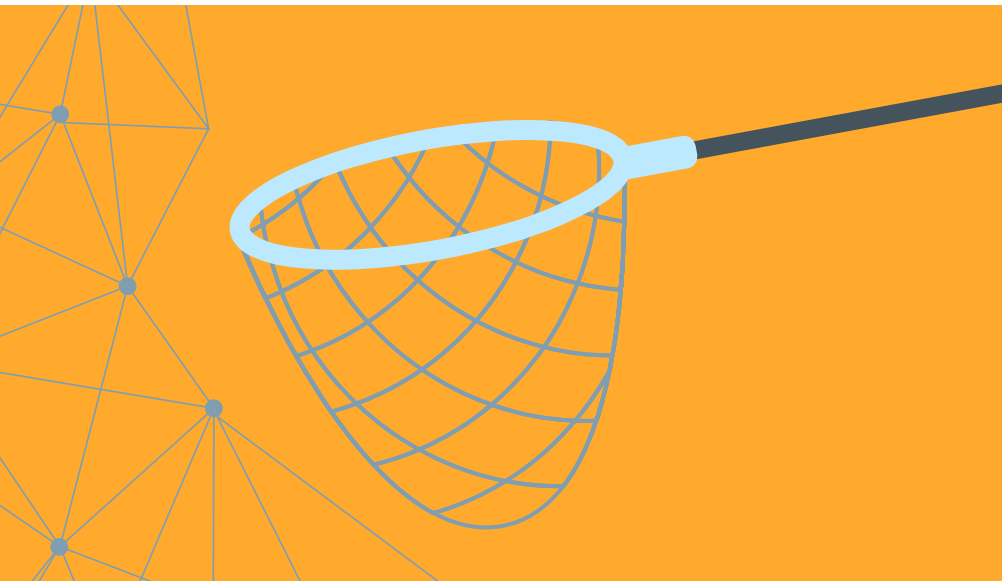

Privacy Policies generativer KI-Plattformen

DeepSeek wird als technisch bahnbrechend gefeiert, doch wirft es Bedenken hinsichtlich des Datenschutzes auf. Aber unterscheiden sich DeepSeeks Datenschutzbestimmungen überhaupt von OpenAI oder Mistral? Ein Überblick.

Von Christina Kiefer

Als das chinesische Start-up Hangzhou DeepSeek Artificial Intelligence Co., Ltd. im Januar 2025 das Reasoning-Modell DeepSeek-R1 vorstellte, sprach man weltweit von einem „chinesischen Sputnik-Moment“. Doch schon kurz darauf schränkten erste Aufsichtsbehörden in der EU den Zugang ein. DeepSeek hat zwar seinen Sitz in China, dennoch ist die EU-Datenschutz-Grundverordnung (DSGVO) anwendbar. Sie gilt nämlich unabhängig vom Unternehmenssitz, wenn personenbezogene Daten Betroffener verarbeitet werden, die sich in der EU aufhalten. Entscheidend ist, dass sich ein Angebot an den EU-Markt richtet, was im Hinblick auf den englischsprachigen Webauftritt von DeepSeek, der die Bezahlung in Euro erlaubt, eindeutig der Fall ist. Werden personenbezogene Daten von Nutzern aus der EU verarbeitet, muss DeepSeek also die Vorgaben der DSGVO einhalten.

Acht Tage nach der Vorstellung von DeepSeek verbot Italien den Zugang zu diesem Modell, die Datenschutzaufsichtsbehörden aus Polen, Griechenland und Luxemburg rieten zur Vorsicht bei der Nutzung. In Deutschland und Irland prüfen die Datenschutzaufsichtsbehörden noch. Beteiligt sind die Landesdatenschutzaufsichtsbehörden von Rheinland-Pfalz, Baden-Württemberg, Thüringen, Sachsen-Anhalt, Hessen, Bremen und Berlin. „Die beteiligten Behörden stimmen sich zu ihrem Vorgehen auf nationaler und europäischer Ebene ab“, heißt es in der Stellungnahme des hessischen Datenschutzbeauftragten.

Doch DeepSeek ist bekanntlich nicht das erste große KI-Sprachmodell. Andere Beispiele sind ChatGPT von OpenAI, Claude von Anthropic oder die Modelle von Mistral. Der Einsatz solcher KI-Werkzeuge birgt – unabhängig von der konkreten Anwendung – datenschutzrechtliche Herausforderungen.

Für die Nutzung braucht es eine gültige Rechtsgrundlage, also eine Ermächtigung, die die Verarbeitung im Einzelfall stützt. Bei komplexen KI-Modellen ist es aber beispielsweise schwierig, das Recht auf Auskunft und das Recht auf Datenberichtigung sicherzustellen. Auch das oft beschriebene Halluzinieren kann den Datenschutz verletzen, da es personenbezogene Daten falsch wiedergibt. In Form von „Privacy by Design“ müsste der Datenschutz schon bei der Technikgestaltung berücksichtigt werden. Setzt ein Unternehmen eine KI-Anwendung ein, liegt außerdem regelmäßig eine Auftragsverarbeitung vor, was entsprechende vertragliche Vereinbarungen erforderlich macht. All diese Aspekte prüfen europäische und deutsche Datenschutzaufsichtsbehörden also gerade, und zwar mit Blick auf das gesamte Anbieterfeld.

Welche Daten erhebt DeepSeek?

Es bietet sich an, zu untersuchen, wie sich DeepSeek im Hinblick auf den Datenschutz von seinen Wettbewerbern – OpenAIs ChatGPT und Mistral – unterscheidet. Grundlage der Bewertung ist die aktualisierte DeepSeek Privacy Policy vom 14. Februar 2025. Sie enthält zusätzliche Regelungen für die Nutzung der DeepSeek-Dienste im Europäischen Wirtschaftsraum (EWR), in der Schweiz und Großbritannien.

DeepSeek verarbeitet verschiedene personenbezogene Daten aus unterschiedlichen Quellen. Die Daten sind dabei mit den verarbeiteten Daten bei ChatGPT oder Mistral Le Chat vergleich-

iX-TRACT

- Das KI-Modell DeepSeek-R1 geriet wegen des angeblich mangelhaften Datenschutzes schnell ins mediale Kreuzfeuer. Im Vergleich mit den Datenschutzbestimmungen von ChatGPT und Mistrals Le Chat zeigt sich aber: Es gibt kaum Unterschiede.
- DeepSeek hat sich den Auflagen der DSGVO angenähert, stellt aber im Unterschied zu OpenAI und Mistral keinen Vertreter als Ansprechpartner in der EU.
- Privatnutzer gelten nach DSGVO nicht als „Verantwortliche“, die ihre Daten in ein Drittland wie China übermitteln.
- In konkreten Einzelfällen und mit vertraglichen Vereinbarungen ist ein DSGVO-konformer Einsatz von DeepSeek möglich.

bar, wie in der Tabelle „Welche personenbezogenen Daten sind betroffen?“ zu sehen. Auch die Zwecke ihrer Verarbeitung ähneln denen, die Mistral und OpenAI in ihren Datenschutzbestimmungen aufrufen, wie die Tabelle „Zu welchen Zwecken werden personenbezogene Daten verarbeitet?“ zeigt.

Welche personenbezogenen Daten sind betroffen?

Herkunft der Daten	ChatGPT	DeepSeek-R1	Mistral Le Chat
Daten, die der Nutzer direkt bereitstellt	Kontodaten, Nutzerinhalte, Kommunikationsinhalte, sonstige vom Nutzer bereitgestellte Informationen	Kontodaten, Nutzerinhalte, Kommunikationsinhalte	Kontodaten, Identitäts- und Kontaktdaten, Zahlungs- und Rechnungsinformationen
nutzungsgenerierte Daten	Protokolldaten, Geräteinformationen, Standortdaten, Cookies und ähnliche Techniken, Nutzungsdaten	Protokolldaten, Geräte- und Netzwerkinformationen, Standortdaten, Cookies und ähnliche Techniken, Zahlungsinformationen	Sicherheitsprotokolle, Geräte- und Netzwerkinformationen, Zahlungsinformationen, Ausgaben
Informationen aus anderen Quellen	öffentlich im Internet verfügbare Informationen, Daten, die Sicherheitspartner und Marketinganbieter bereitstellen	öffentlich im Internet verfügbare Informationen, Login-Informationen, Anmeldedaten oder verknüpfte Dienste, Sicherheitsinformationen	öffentlich im Internet verfügbare Informationen, Daten, die Dritte bereitstellen, z. B. Hugging Face

hervorgehend aus den Privacy Policies der einzelnen Anbieter; Wortlaut angeglichen

Rechtsgrundlagen

Die DSGVO enthält ein Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass jede Verarbeitung einer Rechtsgrundlage bedarf. Solche finden sich in der DSGVO in Artikel 6 und – für besondere Kategorien personenbezogener Daten, wie Gesundheitsdaten – zusätzlich in Artikel 9. Darüber hinaus können auch andere europarechtliche oder nationale Gesetze weitere Rechtsgrundlagen für bestimmte Fälle wie den medizinischen Bereich vorsehen. Die Verarbeitung personenbezogener Daten lässt sich im Kontext von KI-Anwendungen grob in zwei Schritte unterteilen: zum einen in die Verarbeitung von Trainingsdaten zur Entwicklung und zum andern in die Verarbeitung bei der konkreten Nutzung der Anwendung.

In den Supplemental Terms der DeepSeek Privacy Policy zum europäischen Wirtschaftsraum listet DeepSeek die Verarbeitungszwecke mit den jeweiligen verarbeiteten Daten sowie den einschlägigen Rechtsgrundlagen auf: Sie benennen die Vertragserfüllung, die Einwilligung und die Wahrung berechtigter Interessen, aber auch die Erfüllung rechtlicher Pflichten, das allerdings an anderer Stelle. Ob die Voraussetzungen der genannten Rechtsgrundlagen vorliegen, ist im Einzelfall zu prüfen.

Speicherdauer

DeepSeek speichert Informationen so lange, wie es für die Bereitstellung der Dienste und für andere in der Datenschutzrichtlinie genannte Zwecke erforderlich ist. Das schließt die Erfüllung vertraglicher und gesetzlicher Verpflichtungen ein, wenn DeepSeek ein geschäftliches Interesse daran hat – hierunter fällt die Verbesserung und Weiterentwicklung seiner Dienste und die Erhöhung ihrer Sicherheit und Stabilität.

Die Aufbewahrungsfristen hängen von verschiedenen Faktoren ab, wie der Menge, der Art und der Sensibilität der Daten, den Zwecken, für die DeepSeek die Daten verwendet, sowie von den gesetzlichen Bestimmungen. Wenn beispielsweise Informationen verarbeitet werden, um die vereinbarten Dienste zu erbringen, dann werden diese Informationen so lange aufbewahrt, wie das Nutzerkonto besteht. Danach werden sie entsprechend den gesetzlichen Vorschriften gelöscht oder anonymisiert, wobei bereits die Anonymisierung selbst schon einen Verarbeitungsvorgang darstellt, der der DSGVO entsprechen muss. Laut Datenschutzbestimmungen entspricht die Aufbewahrungsdauer bei DeepSeek im Wesentlichen der von OpenAI und Mistral.

Zu welchen Zwecken werden personenbezogene Daten verarbeitet?

ChatGPT	DeepSeek-R1	Mistral Le Chat
Bereitstellung, Analyse und Wartung der Dienste	Bereitstellung, Verwaltung und Wartung der Dienste	Bereitstellung, Verwaltung und Wartung der Dienste
Verbesserung und Weiterentwicklung der Dienste	Verbesserung und Weiterentwicklung der Dienste; schließt Überwachung der Interaktionen und der Nutzung auf den Geräten sowie die Analyse der Usernutzung mit ein	Verbesserung und Weiterentwicklung der Dienste
Nutzerkommunikation	Nutzerkommunikation	Nutzerkommunikation
Verhinderung von Betrug, illegalen Aktivitäten oder Missbrauch der Dienste	Förderung der Sicherheit und Stabilität der Plattform	Sicherheit der Dienste
Erfüllung gesetzlicher Verpflichtungen; zum Schutz der Rechte, der Privatsphäre, der Sicherheit oder des Eigentums der Nutzer, von OpenAI oder von Dritten	Erfüllung gesetzlicher Verpflichtungen; Bereitstellung von Informationen für Strafverfolgungsbehörden oder Notfalldienste in dringenden Situationen zum Schutz von Gesundheit oder Leben	Erfüllung gesetzlicher Verpflichtungen; Beantwortung von Anfragen der Betroffenen zu personenbezogenen Daten, Beilegung von Streitigkeiten
		Verwaltung und Durchsetzung der Lizenzvereinbarung
		Entwicklung und Training der Modelle; Opt-out-Option erst in der Pro-Variante
		Marketingaktivitäten; Newsletter, Identifizierung und Förderung potenzieller Geschäftsmöglichkeiten und Veranstaltungseinladungen

hervorgehend aus den Privacy Policies der einzelnen Anbieter; Wortlaut angeglichen

Betroffenenrechte

Die DSGVO gewährt den von der Verarbeitung betroffenen Personen zahlreiche Rechte, die im KI-Kontext regelmäßig schwer umzusetzen sind. Wer als Verantwortlicher personenbezogene Daten verarbeitet, ist zum Beispiel dazu verpflichtet, die Datenverarbeitung für die betroffenen Personen transparent zu machen und sie entsprechend zu informieren. Das gilt, wenn personenbezogene Daten beim Betroffenen selbst (Art. 13 DSGVO), aber auch dann, wenn sie bei Dritten erhoben werden (Art. 14 DSGVO). Die Information muss dabei transparent und verständlich sein und in einer klaren und einfachen Sprache erfolgen.

Bei KI-Werkzeugen ist das aus mehreren Gründen erschwert: Zum einen ist der Einsatz von KI technisch anspruchsvoll und eine transparente und leicht verständliche Information schon aus diesem Grund eine Herausforderung. Zum andern müssen grundsätzlich alle Betroffenen informiert werden, deren personenbezogene Daten verarbeitet werden. Eine Ausnahme besteht nur dann, wenn das Informieren des Betroffenen unmöglich ist. Ein zentrales Recht der Betroffenen ist das Auskunftsrecht nach Art. 15 DSGVO. Es ist das Instrument, mit dem Betroffene überprüfen können, ob und welche personenbezogenen Daten in welchem Umfang verarbeitet werden. Sind die Daten überdies unrichtig oder werden sie nicht mehr benötigt, bestehen

An welche Empfänger werden personenbezogene Daten weitergegeben?

ChatGPT	DeepSeek-R1	Mistral Le Chat
Lieferanten und Dienstleister	Dienstleister	Dienstleister (Black Forest Labs, Lago und Ory sowie die US-amerikanischen Anbieter Azure, Brave Software, Inc., Cerebras, Cloudflare, GCP, E2B, Intercom, Kong, Mailjet und Stripe)
verbundene Unternehmen	Unternehmensgruppe	Mistrals Teammitglieder
staatliche Behörden, Branchenvertreter oder andere Dritte, wenn dies erforderlich ist, um einer gesetzlichen Verpflichtung nachzukommen	Strafverfolgungsbehörden, öffentliche Behörden, Urheberrechtsinhaber oder andere Dritte, wenn dies erforderlich ist, um einer gesetzlichen Verpflichtung nachzukommen	zuständige Gerichte, Mediatoren, Buchhalter, Wirtschaftsprüfer, Anwälte, Gerichtsvollzieher und Inkassobüros, Regulierungsbehörden wie CNIL
Bei strategischen Transaktionen, Restrukturierungen, Insolvenz [...] können personenbezogene Daten im Rahmen des Prüfprozesses an Beteiligte weitergegeben werden.	Bei Unternehmenstransaktionen wie einer Fusion, einem Verkauf von Vermögenswerten oder Aktien oder einer Umstrukturierung können personenbezogene Daten an Beteiligte weitergegeben werden.	Finanzinstitute
Administratoren von Geschäftskonten		
andere Nutzer und Dritte, mit denen interagiert wird oder Informationen ausgetauscht werden		

hervorgehend aus den Privacy Policies der einzelnen Anbieter; Wortlaut angeglichen

zudem weitere Rechte auf Berichtigung, Löschung oder gegebenenfalls die Einschränkung der Verarbeitung. Diese Betroffenenrechte bildet DeepSeek zumindest in seiner Privacy Policy ausreichend ab – vergleichbar mit den Privacy Policies von OpenAI und Mistral.

Vertreter in der EU

Ein Hauptkritikpunkt der Datenschutzaufsichtsbehörden an DeepSeek bleibt aber, dass nach Art. 27 Abs. 1 DSGVO jeder Verantwortliche, der Dienstleistungen für Betroffene in der EU anbietet, ohne dort niedergelassen zu sein, einen Vertreter in der EU benennen muss. Er dient den Betroffenen und der Aufsichtsbehörde als Ansprechpartner und muss das Recht haben, im Namen des Verantwortlichen oder des Auftragsverarbeiters zu handeln. Liegt ein Datenschutzverstoß vor, wird auch gegen den Vertreter ein Verfahren eingeleitet. DeepSeek hat aber, anders als beispielsweise OpenAI, noch keinen in der EU niedergelassenen Vertreter benannt. Da aber DeepSeek seine Privacy Policy bereits an die Vorgaben der DSGVO angepasst hat, bleibt abzuwarten, ob und wann das Unternehmen auch einen Vertreter benennen wird.

Drittlandübermittlungen?

DeepSeek listet in der Privacy Policy eine Reihe von möglichen Empfängern personenbezogener Daten auf, im Vergleich mit ChatGPT und Le Chat in der Tabelle „An welche Empfänger werden personenbezogene Daten weitergegeben?“ zu sehen.

DeepSeek verarbeitet alle Daten in China. Aus datenschutzrechtlicher Sicht muss man hier zwischen Privatnutzern und gewerblichen Nutzern der DeepSeek-Dienste unterscheiden: Für private Nutzer greift regelmäßig die Haushaltsausnahme nach Art. 2 Abs. 2 DSGVO. Danach findet die DSGVO keine Anwendung, sofern eine Person personenbezogene Daten rein für persönliche oder familiäre Zwecke verarbeitet. Die Haushaltsausnahme hat jedoch ihre Grenzen und greift nicht mehr, wenn der rein private Bereich verlassen wird. Das ist immer dann der Fall, wenn man ein KI-System zu beruflichen oder wirtschaftlichen Zwecken einsetzt.

Die personenbezogenen Daten, auch die von Dritten, die ein Privatnutzer in der EU an DeepSeek weitergibt, verarbeitet DeepSeek als Verantwortlicher also in China – und damit in einem Land außerhalb der EU, einem Drittland. In diesem Fall liegt entsprechend den Richtlinien 05/2021 des Europäischen Datenschutzausschusses aber überhaupt keine Drittlandübermittlung vor. Es fehlt in dieser Konstellation nämlich an einer Datenübertragung von einem Verantwortlichen oder Auftragsverarbeiter an einen anderen. Da die DSGVO für den Privatnutzer regelmäßig nicht anwendbar ist, kann er nicht als Verantwortlicher gelten. Stattdessen findet eine Verarbeitung durch einen Verantwortlichen in einem Drittland statt. Ohne dass eine Drittlandübermittlung vorliegt, greifen auch nicht die strengen entsprechenden Anforderungen nach Art. 44 ff. DSGVO.

Das bedeutet jedoch nicht, dass DeepSeek bezüglich der Verarbeitung in China keinerlei Vorgaben erfüllen muss – vielmehr unterliegt DeepSeek als Verantwortlicher den allgemeinen Anforderungen der DSGVO und hat neben einer Rechtsgrundlage für die Verarbeitung oder die Betroffenenrechte auch eine hinreichende Datensicherheit nach Art. 32 DSGVO sicherzustellen. In seiner Privacy Policy garantiert DeepSeek, angemessene technische, administrative und physische Sicherheitsmaßnahmen zu unterhalten, die dazu dienen, die Daten vor unbefugtem Zugriff, Diebstahl, Offenlegung, Änderung oder Verlust zu schützen. Eine Liste der technischen und organisatorischen Maßnahmen ist bislang aber nicht frei verfügbar, sodass die Nutzer auf die Informationen von DeepSeek vertrauen müssen.

Liegt keine Privatnutzung vor, setzt also ein Unternehmen DeepSeek ein, handelt das Unternehmen als datenschutzrechtlich Verantwortlicher. In dieser Konstellation liegt dann auch eine Übermittlung in ein Drittland vor und die Anforderungen der Art. 44 ff. DSGVO sind zu beachten. Eine Übermittlung in ein Drittland ist demnach nur zulässig, wenn für das betreffende Drittland ein Angemessenheitsbeschluss der EU-Kommission vorliegt, ein angemessenes Schutzniveau durch geeignete Garantien wie Standardvertragsklauseln (Standard Contractual Clauses, SCC) gewährleistet ist oder ein Ausnahmetatbestand nach Art. 49 DSGVO greift. Für China gibt es so einen Angemessenheitsbeschluss der EU-Kommission nicht. Die Gewährleistung eines angemessenen Schutzniveaus im Sinne von Art. 46 der DSGVO sichert DeepSeek nicht ausdrücklich zu.

So verweist DeepSeek im Gegensatz zu OpenAI nicht auf die Standardvertragsklauseln der EU-Kommission. Standardvertragsklauseln gibt es aber auch im chinesischen Datenschutzrecht. Sie sind am 1. Juni 2023 in Kraft getreten, weisen große Ähnlichkeiten mit dem europäischen Pendant auf und orientieren sich erkennbar daran. Zudem ist China kein datenschutzrechtliches Vakuum: Mit dem Personal Information Protection Law (PIPL) ist seit 2021 ein Datenschutzgesetz in Kraft. Das PIPL ähnelt in vielen Aspekten der DSGVO und enthält teilweise sogar strengere Anforderungen. Eine datenschutzkonforme Nutzung ist daher grundsätzlich möglich, sofern

Unternehmen das erforderliche Schutzniveau prüfen und zum Beispiel eine Vereinbarung mit SCC sicherstellen.

Fazit

DeepSeek gewährleistet – zumindest nach der Privacy Policy – das Einhalten der datenschutzrechtlichen Pflichten auf einem vergleichbaren Niveau wie seine Mitbewerber OpenAI oder Mistral. Dabei fallen einige Gemeinsamkeiten auf. Die Beschreibung der Rechtsgrundlagen unterscheidet sich eher in ihrer sprachlichen Natur. Gleiches gilt für die verarbeiteten Daten, die Verarbeitungszwecke und die Speicherdauer.

Der größte Unterschied liegt in der fehlenden Benennung eines Vertreters von DeepSeek in der EU und der Datenverarbeitung in China. In diesem Zusammenhang ist aber zu berücksichtigen, dass selbst europäische Lösungen nicht immer eine Verarbeitung in der EU garantieren können. Auch die europäischen Alternativen können personenbezogene Daten in Drittländer exportieren. In Mistrals Privacy Policy heißt es dazu: „[...] in exceptional cases, we may opt for non-EU providers that meet our high standards of data security and Personal Data protection." Die Server von OpenAI stehen bekanntlich in den USA, was im Hinblick auf die aktuellen politischen Entwicklungen eine gewisse Unsicherheit mit sich bringt.

Aber auch allgemein stößt die Nutzung von ChatGPT oder Mistral Le Chat aus datenschutzrechtlicher Sicht im beruflichen Kontext auf Probleme. Ein Beispiel ist die Vereinbarung eines Auftragsverarbeitungsvertrags, den OpenAI erst bei Nutzung der kostenpflichtigen Variante zur Verfügung stellt. Ein weiteres Beispiel: die Verarbeitung von Daten für Trainingszwecke. Mistral Le Chat verwendet die Nutzereingaben in der kostenfreien Variante zum Training der KI. Eine Opt-out-Option besteht erst in der Pro-Version. Bei ChatGPT ist erst in der kostenpflichtigen Variante voreingestellt, dass es Gespräche nicht zur Modellverbesserung verwendet. Daher bestehen auch hier datenschutzrechtliche Risiken.

Ganz unabhängig vom Anbieter birgt der Einsatz von KI generell datenschutzrechtliche Herausforderungen. Sei es die Gewährleistung der Transparenz, die Sicherstellung der Betroffenenrechte oder eine mögliche Datenschutzverletzung aufgrund fehlerhaft generierter Inhalte. Die Datensicherheit – gleich, ob die Verarbeitung im EU-Inland oder im EU-Ausland erfolgt – ist stets sicherzustellen. Mit entsprechenden vertraglichen Vereinbarungen und Zusagen im konkreten Einzelfall ist ein datenschutzkonformer Einsatz von KI-Werkzeugen, auch von DeepSeek, jedoch nicht unmöglich. (kki@ix.de)

Quellen

[1] Christian Winkler; DeepSeek-R1: Günstiges Reasoning für alle; iX 3/2025, S. 42

[2] Die Quellen zu den erwähnten Umständen und Rechtsmitteln sind unter ix.de/zet3 zu finden.

CHRISTINA KIEFER

ist Rechtsanwältin und Associate in der Digital Business Unit bei reuschlaw.