Newsletter IP/IT

Mai 2025

Inhalt

Der Cyber Resilience Act: Auswirkungen auf die Entwicklung und Verwendung von Open Source Software

Der Cyber Resilience Act (CRA), genauer gesagt die Verordnung (EU) 2024/2847 vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen, die am 10. Dezember 2024 in Kraft getreten ist, wird EU-weit einheitliche, branchenübergreifende Vorgaben für die Cybersicherheit von vernetzten Hard- und Softwareprodukten machen. Die Vorgaben müssen schrittweise bis zum 11. Dezember 2027 umgesetzt werden. Auch in der Welt der Open Source Software (OSS) wird der CRA für beachtliche Veränderungen sorgen. Akteure entlang der OSS-Lieferkette müssen sich daher nun verstärkt mit den Vorgaben des CRA auseinandersetzen.

I. Entwicklung und Bereitstellung von Open Source Software

„Open Source“ bezeichnet solche Software, deren Quellcode offen geteilt wird und die grundsätzlich von jedem genutzt, geändert und weiterverbreitet werden kann. Nach den Erwägungsgründen des CRA sollten freie und quelloffene Softwarelösungen nur dann in den Anwendungsbereich der Verordnung fallen, wenn sie für kommerzielle Zwecke entwickelt und im Rahmen einer Geschäftstätigkeit vertrieben werden. Hierbei werden verschiedene Ausgestaltungen kommerzieller Aktivität eingeschlossen, wobei die Software nicht unmittelbar die Leistung sein muss, für die bezahlt wird. Zu berücksichtigen sind weitere Faktoren, wie z.B. die Regelmäßigkeit der Bereitstellung, Eigenschaften des Produkts und Absichten der Akteure. Nicht als Geschäftstätigkeit zu sehen ist z.B. die Annahme von Spenden ohne Gewinnerzielungsabsicht zur Deckung der tatsächlichen Kosten für die Konzeption, Entwicklung und Bereitstellung. Sofern jedoch die nicht kommerziell entwickelte OSS wiederum vermarktet wird, ist die Möglichkeit einer Geschäftstätigkeit eröffnet und der Pflichtenkatalog des CRA zu beachten.

Wie genau sich die Vorgaben des CRA auf Sicherheitspraktiken im Bereich Open Source Software auswirken werden, bleibt abzuwarten. Insbesondere sieht die Verordnung den Erlass von Leitlinien durch die EU-Kommission vor. Unter anderem sollen der Anwendungsbereich und die Auswirkung der Verordnung auf die Entwicklung freier und quelloffener Software weiter konkretisiert werden.

II. Integration von Open Source Software in Produkte mit digitalen Elementen

Hersteller von digitalen Produkten werden vor umfassenden Pflichten stehen, wenn sie OSS in diese digitalen Produkte integrieren. Das gilt explizit auch für die Integration solcher OSS, die nicht im Rahmen einer Geschäftstätigkeit auf dem Markt bereitgestellt wird und dadurch in der Entwicklungsphase nicht dem Regulierungsregime des CRA unterfällt.

Die Hersteller müssen sicherstellen, dass die Cybersicherheit ihrer Produkte durch die Integration von OSS nicht gefährdet wird. Sie müssen die gebotene Sorgfalt walten lassen, sodass das Gesamtprodukt gemäß den grundlegenden Cybersicherheitsanforderungen konzipiert, entwickelt und hergestellt wird. Darunter fallen unter anderem sichere Standardkonfigurationen, Sicherheitsaktualisierungen und Kontrollmechanismen zum Schutz gegen unberechtigten Zugriff. Zu diesem Zweck ist eine Bewertung der Cybersicherheitsrisiken durchzuführen. Deren Ergebnis muss während der gesamten Produktlebensdauer, angefangen bei der Planung und Entwicklung bis zur Lieferung und Wartung, berücksichtigt werden. So sollen Cybersicherheitsrisiken minimiert und Sicherheitsvorfälle verhindert werden. Entdeckte Sicherheitslücken und Schwachstellen müssen gemeldet und geschlossen werden.

Unternehmen, die sich bisher nicht intensiv mit Open Source-Compliance beschäftigt haben, werden nun umfangreiche Anpassungen vornehmen müssen. Die Einrichtung eines geeigneten Schwachstellen- und Risikomanagementsystems wird unerlässlich sein. Insbesondere der Umstand, dass Hersteller nicht nur für die Cybersicherheit ihres eigenen Produkts, sondern auch für die der verwendeten OSS-Komponenten verantwortlich sind, unterstreicht die Bedeutung vertraglicher Absicherungen mit Zulieferern und Dienstleistern. Nur durch die Bereitstellung weiterer Informationen über die OSS-Komponente kann überhaupt eine Bewertung der Cybersicherheitsrisiken durch den Hersteller durchgeführt und dokumentiert werden. Auch rechtliche Definitionen technischer Fachbegriffe, die Ausgestaltung der jeweiligen Pflichten, die regelmäßige und dauerhafte Bereitstellung von Informationen über etwaige Schwachstellen und Sicherheitslücken sollten vertraglich abgesichert werden.

III. Fazit und Ausblick

Ab Ende 2027 müssen Produkte mit digitalen Elementen, die neu auf den Markt gebracht werden, den Vorgaben des CRA gerecht werden. Der Implementierungsaufwand dieser Bestimmungen ist nicht zu unterschätzen. Unternehmen stehen nun vor dem entscheidenden Schritt zu identifizieren, inwiefern ihre Geschäftstätigkeit von der Verordnung betroffen ist und wie die Umsetzung der Anforderungen strategisch gelingen kann. Bei Nichteinhalten der Cybersicherheitsanforderungen drohen empfindliche Geldbußen, Haftungsfragen oder Korrekturmaßnahmen, wie z.B. Produktrückrufe durch die Marktüberwachungsbehörden. Daher empfiehlt es sich, bereits jetzt zu analysieren, welche Pflichten zu erfüllen sind und wie eine vertragliche Absicherung in der OSS-Lieferkette erfolgen kann.

Cybersecurity-Update: Wie geht es mit dem NIS2-Umsetzungsgesetz und dem KRITIS-Dachgesetz weiter?

Am 16. Januar 2023 sind zwei EU-Richtlinien für einen besseren Schutz kritischer Infrastrukturen in Kraft getreten. Mit den Richtlinien will die EU einen einheitlichen Schutz vor physischen Störungen und Cyberangriffen gewährleisten. So sind die erfassten Sektoren weitgehend identisch: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Öffentliche Verwaltung und Weltraum. Im Bereich der Cybersicherheit stellt die NIS2-Richtlinie (EU 2022/2555) einen wichtigen Schritt hin zu einem gemeinsamen Sicherheitsniveau aller EU-Mitgliedstaaten dar. Ziel der Richtlinie ist es, zunehmenden Cyberangriffen entgegenzuwirken, die immer mehr kritische Wirtschaftssektoren betreffen.

Die NIS2-Richtlinie ist nicht unmittelbar anwendbar, sondern verpflichtet die Mitgliedsstaaten der EU zur Umsetzung der Vorgaben in nationales Recht. Hierfür gab es eine Umsetzungsfrist, die bereits zum 17. Oktober 2024 abgelaufen ist. In Deutschland soll die NIS2-Richtlinie durch das Umsetzungsgesetz NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) umgesetzt werden. Hierfür wurde am 22. Juli 2024 ein Entwurf veröffentlicht, der nicht mehr verabschiedet wurde.

Ergänzend, zum Schutz der physischen Widerstandsfähigkeit kritischer Infrastrukturen, zielt die CER-Richtlinie (EU 2022/2557) auf die Stärkung der physischen Resilienz kritischer Einrichtungen gegenüber Bedrohungen wie Naturkatastrophen, Terroranschlägen und Sabotage ab. Zur nationalen Umsetzung der CER-Richtlinie wurde in Deutschland der Entwurf für das KRITIS-Dachgesetz am 6. November 2024 verabschiedet. Verkündet wurde das Gesetz jedoch unter der alten Bundesregierung nicht mehr, sodass auch dieses Gesetz in der alten Legislaturperiode nicht mehr zustande gekommen ist.

I. Folgen des gescheiterten Gesetzgebungsverfahrens

Der Diskontinuitätsgrundsatz im deutschen Verfassungsrecht besagt, dass alle Gesetzesvorhaben und anderen parlamentarischen Vorlagen, die innerhalb einer Legislaturperiode nicht abgeschlossen wurden, nach Ablauf dieser Periode als erledigt gelten. Dies bedeutet, dass die Entwürfe für das NIS2UmsuCG und das KRITIS-Dachgesetz in der neuen Legislaturperiode neu eingebracht und verhandelt werden müssen. Insoweit bleibt abzuwarten, ob die neue die aktuellen Umsetzungsentwürfe wieder aufgreifen oder mit komplett neuen Umsetzungsentwürfen ins Gesetzgebungsverfahren gehen wird. In jedem Fall müssen die Entwürfe aber in den neu konstituierten Bundestag erneut eingebracht, beraten und sodann verabschiedet werden.

Zudem führt die verspätete Umsetzung der NIS2-Richtlinie in nationales Recht nicht dazu, dass die Verpflichtungen aus der NIS2-Richtlinie nach Ablauf der Umsetzungsfrist unmittelbar von den betroffenen Unternehmen zu beachten sind. Jedoch hat die Europäische Kommission aufgrund der verspäteten Umsetzung der NIS2-Richtlinie in nationales Recht nunmehr gegen Deutschland und 22 weitere Mitgliedstaaten ein Vertragsverletzungsverfahren eingeleitet.

Die Umsetzungsfrist für die CER-Richtlinie läuft hingegen noch bis zum 17. Juli 2026.

II. Fazit und Ausblick

Unternehmen sollten die „gewonnene Zeit“ sinnvoll nutzen, um sich gezielt auf die kommenden Anforderungen vorzubereiten. Es gilt weiterhin zu prüfen, ob sie unter die Geltungsbereiche der NIS2- und CER-Richtlinien fallen und – sofern zutreffend – welche spezifischen Anforderungen sie zu erfüllen haben. Besonders im Fokus steht dabei die Umsetzung technischer und organisatorischer Maßnahmen zur Erhöhung der IT-Sicherheit. Es ist empfehlenswert, sich bereits jetzt sowohl an den europäischen Vorgaben der genannten Richtlinien als auch an den aktuellen nationalen Umsetzungsentwürfen zu orientieren.

Die Erforderlichkeit eines KI-Sachverständigen für den Betriebsrat

Mit dem Betriebsrätemodernisierungsgesetz von 2021 hat der Gesetzgeber das BetrVG erstmals um Bestimmungen zu Künstlicher Intelligenz (KI) ergänzt. Diese Anpassungen spiegeln die wachsende Bedeutung von KI in Betrieben wider. Eine zentrale Neuerung stellt die Erweiterung des § 80 Abs. 3 BetrVG um einen zweiten Satz dar, der es dem Betriebsrat ermöglicht, in Angelegenheiten der KI leichter einen Sachverständigen hinzuziehen zu können.

I. Die Erforderlichkeitsfiktion: Vereinfachter Zugriff auf außerbetrieblichen Sachverstand

Die zentrale Neuerung von § 80 Abs. 3 Satz 2 BetrVG besteht darin, dass die Erforderlichkeit eines Sachverständigen für den Betriebsrat unwiderlegbar vermutet wird, wenn er die Einführung oder Anwendung von KI im Betrieb beurteilen muss. Damit darf der Betriebsrat verlangen, dass der Arbeitgeber der Hinzuziehung eines Sachverständigen zustimmt. Anders als bisher muss der Betriebsrat nicht mehr darlegen, warum er das Fachwissen eines externen Sachverständigen benötigt, wenn ein spezifischer Bezug zur KI gegeben ist. Selbst ein sachkundiger Betriebsrat darf danach einen Sachverständigen verlangen.

1. Anforderungen und Reichweite der Fiktion

a) Aufgabenbezug

Die Fiktion gilt jedoch nur unter bestimmten Bedingungen. Der Betriebsrat muss darlegen, dass durch die Einführung oder Anwendung von KI ein Bezug zu seinen Aufgaben hergestellt ist, d.h. beispielsweise das Mitbestimmungsrecht bei der Einführung technischer Einrichtungen gem. § 87 Abs. 1 Nr. 6 BetrVG oder sonst die im BetrVG geregelten Beteiligungsrechte. Aufgaben des Betriebsrates können sich sowohl aus der Anbahnungs-, der Durchführungs- wie auch der Beendigungsphase von Arbeitsverhältnissen ergeben.

b) Hinreichender Bezug zur KI

Zentrale Voraussetzung ist, dass das der Betriebsrat zur Durchführung seiner Aufgaben die Einführung oder Anwendung von KI beurteilen muss. Es müssen daher einerseits überhaupt Bezugspunkte zu Elementen der KI bestehen. Andererseits greift die Fiktion nicht, wenn der Einsatz der KI nur einen marginalen Bezug zur Arbeit des Betriebsrats hat. Es dürfte daher nicht ausreichen, wenn eine Maßnahme nur „irgendwie“ mit KI zusammenhängt – der Zusammenhang muss konkret und relevant sein.

Man denke hierbei etwa an KI-gestützte Systeme, die das Verhalten oder die Leistung von Arbeitnehmern analysieren, z. B. Fahrdatenanalyse in Dienstfahrzeugen oder Algorithmen, die Personalauswahl oder Leistungsbeurteilung beeinflussen.

Enthält ein System sowohl KI-gestützte als auch nicht KI-gestützte Elemente, muss die konkret zu untersuchende Verhaltenskontrolle im Einzelfall danach beurteilt werden, inwiefern diese einen maßgeblichen KI-Bezug aufweist.

c) Herausforderung der KI-Definition

Eine Definition von „Künstlicher Intelligenz“ fehlt im Gesetz. Auch gibt es kein allgemeingültiges Verständnis von KI. Damit besteht für den Rechtsanwender die Schwierigkeit, den Begriff im spezifischen Kontext erst auslegen zu müssen, wenn es um die Beurteilung geht, ob der Aufgabenbereich des Betriebsrates eine hinreichende Verknüpfung zu KI-Sachverhalten aufweist. In der arbeitsrechtlichen Praxis wird KI häufig als nicht-deterministisches System verstanden, dass Ergebnisse erzeugt, die nicht vollständig vorhersehbar sind sowie Komponenten der Selbstoptimierung, des Selbstlernens oder der selbstständigen Aufgabenerledigung beinhaltet. Begriffe wie maschinelles Lernen, „Deep Learning“, Robotik oder virtuelle Realität sind heutzutage prägend für das Begriffsverständnis von KI, wobei unser Verständnis von KI einem stetigen Wandel unterliegt.

2. Darlegungslast

Der Betriebsrat muss aufzeigen, dass durch die geplante Maßnahme des Arbeitgebers tatsächlich seine Aufgaben berührt werden. Außerdem entlastet die Regelung des § 80 Abs. 3 Satz 2 BetrVG den Betriebsrat nicht von der Darlegungspflicht, dass die von ihm wahrzunehmende Aufgabe im hinreichenden Zusammenhang mit KI steht. Eine Schwierigkeit besteht darin, überhaupt zu definieren, wann die erforderliche Schwelle eines hinreichenden KI-Bezugs gegeben ist. Gelingt es dem Betriebsrat nicht, einen solchen Aufgabenbezug zur KI darzulegen, kann er sich nicht auf § 80 Abs. 3 Satz 2 BetrVG stützen. In diesen Fällen muss er sich ggf. unternehmensinterner Informationsquellen bedienen, um die Voraussetzungen der Fiktion darzulegen.

3. Vereinbarung mit dem Arbeitgeber

Liegen die Voraussetzungen der Fiktion vor, darf der Betriebsrat nicht eigenständig und ohne Rücksprache mit dem Arbeitgeber einen Sachverständigen beauftragen. Stattdessen hat er eine Vereinbarung mit dem Arbeitgeber über die Hinzuziehung des Sachverständigen zu treffen. Diese soll die Festlegung der Person, die Aufgabenstellung und die Vergütung des Sachverständigen festlegen.

Dies hat auch in dringenden Fällen zu erfolgen. Bestehen Meinungsverschiedenheiten zwischen den Betriebsparteien muss der Betriebsrat die Zustimmung des Arbeitgebers notfalls im Wege eines einstweiligen Verfügungsverfahrens ersetzen lassen. Gem. § 80 Abs. 3 Satz 3 BetrVG können sich die Betriebsparteien in Angelegenheiten des § 80 Abs. 3 Satz 2 BetrVG auch auf einen ständigen Sachverständigen einigen.

II. Fazit und Ausblick

Für den Arbeitgeber stellt die Neuregelung einen nicht zu vernachlässigenden Kostenfaktor dar. Darüber hinaus birgt das unscharfe Begriffsverständnis von KI Konfliktpotential. Zieht man das Kriterium der „selbstständigen Aufgabenerledigung“ heran, stellt man schnell fest, dass bereits jetzt ein großer Teil der vorhanden Tools auf Elemente von KI zurückgreifen. Je nach Auslegung könnten daher bereits Übersetzungsprogramme oder einfache Analysewerkzeuge als KI gelten. Für den Arbeitgeber ist es mit zunehmendem Einsatz von KI-Tools umso entscheidender für Transparenz zu sorgen und mit dem Betriebsrat klare Abgrenzungen zu regeln, um Konfliktsituationen zu vermeiden und frühzeitig Akzeptanz zu schaffen.

Oberlandesgericht Schleswig-Holstein erklärt eine Ende-zu-Ende-Verschlüsselung beim Rechnungsversand per E-Mail im B2C-Bereich für erforderlich

Mit Urteil vom 18. Dezember 2024 (Az.: 12 U 9/24) hat das Schleswig-Holsteinische Oberlandesgericht zu der Frage Stellung genommen, welche Anforderungen an die Verschlüsselung von E-Mails zu stellen sind, wenn mit diesen eine Rechnung im B2C-Bereich versandt wird. Das Urteil setzt neue Maßstäbe für die datenschutzrechtlichen Anforderungen an den digitalen Geschäftsverkehr und könnte erhebliche praktische Konsequenzen für Unternehmen nach sich ziehen.

I. Der Sachverhalt

Die Klägerin, eine Bauunternehmerin, installierte für eine private Auftraggeberin, die Beklagte, eine Heizung. Anschließend übersandte sie der Beklagten per E-Mail eine Werklohnrechnung in Höhe von 15.000 Euro. Zur Sicherheit verschlüsselte die Klägerin die E-Mail mittels einer Transportverschlüsselung. Während des Übertragungsprozesses gelang es einem Dritten, die E-Mail abzufangen und die in der Rechnung angegebene Kontonummer zu manipulieren. Die Beklagte beglich daraufhin die Rechnung, allerdings nicht auf das Konto der Klägerin, sondern auf das manipulierte Konto der Betrüger. Als die Klägerin daraufhin die erneute Zahlung forderte, verweigerte die Beklagte diese mit der Begründung, dass die ungesicherte Übermittlung der Rechnung per E-Mail fahrlässig gewesen sei und sie dadurch einen Schaden erlitten habe.

II. Das Urteil

Das Landgericht Kiel hatte zunächst zugunsten des Unternehmens entschieden. Das OLG Schleswig-Holstein kassiert jedoch die Entscheidung und stellte fest, dass der Beklagten ein Schadensersatzanspruch aus Art. 82 Abs. 1 DSGVO zusteht, der der Werklohnforderung (in selber Höhe) entgegengehalten werden kann. Durch den Versand der E-Mail mittels Transportverschlüsselung habe die Klägerin gegen die Grundsätze der DSGVO, namentlich Art. 5, 24 und 32 DSGVO verstoßen. Art. 5 Abs. 2 i. V. m. Art. 24 DSGVO enthält den Grundsatz der Rechenschaftspflicht. Hiernach muss die Klägerin darlegen und beweisen, dass die Transportverschlüsselung geeignet war, die in der E-Mail enthaltenen personenbezogenen Daten entsprechend dem von der DSGVO verlangten Sicherheitsniveau vor dem Zugriff Unbefugter zu schützen. Zwar enthält die DSGVO keine spezifischen Vorschriften zur

E-Mail-Verschlüsselung. Art. 32 DSGVO sieht jedoch vor, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen ergreifen muss, um ein angemessenes Sicherheitsniveau zu gewährleisten. Hierzu zählen auch Maßnahmen wie die Pseudonymisierung und die Verschlüsselung personenbezogener Daten. Das Gericht nahm an, dass dieses Schutzniveau im vorliegenden Fall nur durch die Versendung mittels Ende-zu-Ende-Verschlüsselung hätte erreicht werden können.

III. Transportverschlüsselung vs. Ende-zu-Ende-Verschlüsselung

Bei der Transportverschlüsselung (z. B. mittels TLS) wird die E-Mail während der Übertragung zwischen den Mailservern verschlüsselt, liegt jedoch auf den Servern der Anbieter und auf den Endgeräten der Kommunikationspartner unverschlüsselt vor. Demgegenüber stellt die Ende-zu-Ende-Verschlüsselung sicher, dass nur der Absender und der vorgesehene Empfänger Zugriff auf den Klartext der Nachricht haben; selbst die beteiligten Mailserver können den Inhalt nicht einsehen.

IV. Was gilt für den B2B-Bereich?

In einem vergleichbaren Fall kam das OLG Karlsruhe zu einer anderen Entscheidung (Urteil vom 27. Juli 2023 – Az.: 19 U 83/22). Die Parteien – beide juristische Personen – stritten um die Zahlung einer Kaufpreisforderung. Die Klägerin übersandte die Rechnung per E-Mail, ohne besondere Verschlüsselung. Auch hier wurde die Rechnung beim Übermittlungsvorgang so manipuliert, dass die Beklagte das Geld auf ein falsches Konto überwies. Das Gericht entschied, dass die Klägerin weiterhin Zahlung des Kaufpreises verlangen könne. Die Beklagte könne der Klägerin keinen Schadensersatzanspruch gemäß § 280 Abs. 1, § 241 Abs. 2 BGB entgegenhalten. Durch das Versenden der E-Mail ohne besondere Verschlüsselung habe die Klägerin keine Nebenpflichtverletzung begangen. Im B2B-Bereich gibt es ebenfalls keine konkreten gesetzlichen Vorgaben zu Sicherheitsvorkehrungen beim Versand von E-Mails. Die oben verletzten Grundsätze der DSGVO finden im Verhältnis B2B jedoch keine Anwendung, da der sachliche Anwendungsbereich der DSGVO nicht eröffnet ist. Die DSGVO umfasst nur die Verarbeitung von Daten, die sich auf natürliche Personen beziehen (vgl. Art. 2 Abs. 1, Art. 4 Nr. 1 DSGVO).

V. Ausblick und Kritik

Das Urteil des Schleswig-Holsteinischen Oberlandesgerichts kann große Auswirkungen auf den Umgang mit sensiblen Informationen in der digitalen Kommunikation haben. Es bleibt aber abzuwarten, ob dieses Urteil über die nächste Instanz Bestand haben wird (die Revision ist zugelassen) oder andere Gerichte von der Rechtsauffassung abweichen. Diese Entwicklung wird jedenfalls strengstens beobachtet werden, denn die Entscheidung wird in der juristischen Literatur stark kritisiert. Zum einen wird entgegen der Feststellung des Gerichts nicht angenommen, dass die Ende-zu-Ende Verschlüsselung im B2C-Bereich Standard wäre, da die meisten Verbraucher als E-Mail-Empfänger nicht über die geeigneten technischen Mittel oder Erfahrungen verfügen würden, die E-Mails zu öffnen. Zum anderen wird das unzureichende Schutzniveau der Transportverschlüsselung anders bewertet. Unter Berücksichtigung des risikobasierten Ansatzes der DSGVO, seien Unternehmen verpflichtet, angemessene Schutzmaßnahmen basierend auf einer Risikoanalyse zu implementieren. Eine pauschale Verpflichtung zur Ende-zu-Ende-Verschlüsselung bei Rechnungs-E-Mails würde diesem flexiblen Ansatz widersprechen und die unternehmerische Freiheit bei der Wahl geeigneter Sicherheitsmaßnahmen einschränken.

Der Europäische Datenschutzausschuss (EDSA) konkretisiert den Begriff der Pseudonymisierung

Die Pseudonymisierung von Daten spielt eine entscheidende Rolle im Datenschutzrecht und ist ein wichtiges Instrument zur Erfüllung der Anforderungen der Datenschutz-Grundverordnung (DSGVO). Der Europäische Datenschutzausschuss (EDSA) hat am 16. Januar 2025 den Begriff der Pseudonymisierung personenbezogener Daten weiter definiert und damit praxisrelevante Klarstellungen getroffen.

I. Hintergrund

Im Rahmen einer öffentlichen Konsultation hat der EDSA einen Vorschlag für Leitlinien zur Pseudonymisierung von personenbezogenen Daten veröffentlicht, zu denen die Öffentlichkeit in diesem Verfahren nun Stellung nehmen kann. Die öffentliche Konsultation basiert insbesondere auf Art. 70 DSGVO, der die Aufgaben des EDSA festlegt. Dazu gehört die Förderung einer einheitlichen Anwendung der DSGVO in der EU durch Leitlinien und Empfehlungen. Nach der Konsultationsphase bewertet der EDSA die Rückmeldungen und überarbeitet gegebenenfalls die Vorschläge, bevor sie final verabschiedet werden.

II. Zielsetzung der Leitlinien

In diesen Leitlinien wird der Begriff der Pseudonymisierung umfassend definiert und es werden Hinweise auf die praktische Anwendung von Pseudonymisierung gegeben. Die Leitlinien sollen Unternehmen und anderen Organisationen dabei helfen, ihren Verpflichtungen im Datenschutz nachzukommen. Besonderes Augenmerk legt der Ausschuss dabei auch auf die Vorteile von pseudonymisierten Daten und die (technische) Umsetzung dieser Pseudonymisierung.

III. Der Begriff der Pseudonymisierung

Unter Pseudonymisierung versteht die DSGVO in Art. 4 Abs. 5 eine Verarbeitung personenbezogener Daten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Die Identität der betroffenen Personen soll denjenigen verborgen bleiben, die keinen Zugang zu solchen zusätzlichen Informationen haben.

Im Gegensatz dazu ermöglichen anonymisierte Daten abschließend keine Zuordnung mehr zu der dahinterstehenden natürlichen Person. Pseudonymisierte Daten fallen daher anders als anonymisierte Daten unter den Anwendungsbereich und damit auch unter das Haftungsregime der DSGVO. Unternehmen bleiben daher verpflichtet, die Betroffenenrechte – insbesondere das Recht auf Auskunft, Berichtigung und Löschung – zu gewährleisten.

IV. Vorteile der Pseudonymisierung

Die Leitlinien betonen, dass nach der DSGVO keine generelle Pflicht zur Pseudonymisierung besteht. Dafür werden aber die Vorteile der Pseudonymisierung hervorgehoben.

Die Pseudonymisierung kann Risiken reduzieren und die Nutzung berechtigter Interessen als Rechtsgrundlage erleichtern (Art. 6 Abs. 1 lit. f DSGVO), sofern alle anderen Anforderungen der DSGVO erfüllt sind. Ebenso kann die Pseudonymisierung dazu beitragen, die Vereinbarkeit mit dem ursprünglichen Zweck zu gewährleisten (Art. 6 Abs. 4 DSGVO). In den Leitlinien wird erläutert, wie die Pseudonymisierung Organisationen dabei helfen kann, ihren Verpflichtungen in Bezug auf die Umsetzung der Datenschutzgrundsätze (Art. 5 DSGVO), den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) und der Sicherheit (Art. 32 DSGVO) nachzukommen.

V. Praktische Umsetzung der Pseudonymisierung

Die Pseudonymisierung erfolgt in zwei Schritten: Zunächst werden die Daten pseudonymisiert, und dann wird sichergestellt, dass sie geschützt bleiben. Die Verantwortlichen müssen die mit der Pseudonymisierung verbundenen Risiken definieren und die Pseudonymisierungsumgebung festlegen, um die Identifizierung von Personen auszuschließen. Direkte Identifikatoren müssen entfernt oder durch Pseudonyme ersetzt werden. Die Pseudonymisierung erfolgt durch Verwendung geheimer Informationen (sog. Pseudonymisierungsgeheimnisse), die vertraulich behandelt werden müssen. Es gibt zwei übliche Methoden, um Pseudonymisierungsgeheimnisse sicher aufzubewahren: kryptographische Algorithmen und Zuordnungstabellen, die die Leitlinien darstellen. Die Auswahl hängt von der Unumkehrbarkeit der Pseudonymisierung und den Risiken kryptoanalytischer Angriffe ab.

Abschließend sind geeignete technische und organisatorische Maßnahmen (TOMs) zu implementieren, die eine unbefugte Re-Identifikation zu verhindern. Dazu gehören unter anderem der Einsatz von Zugangsbeschränkungen, die Speicherung von Pseudonymisierungsgeheimnissen an unterschiedlichen Orten und die Zufallsgenerierung von Pseudonymen.

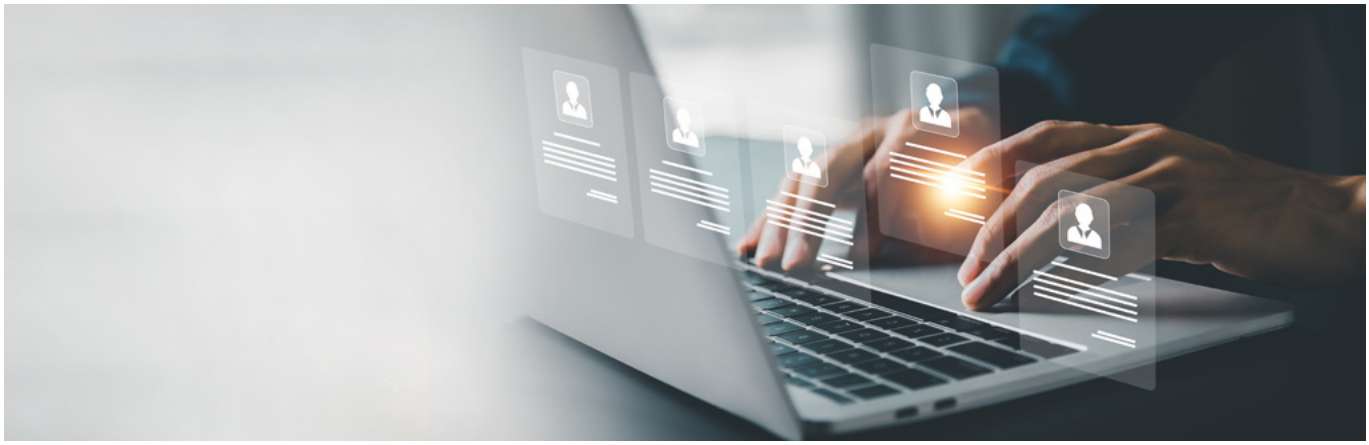
VI. Fazit und Ausblick

Die Pseudonymisierung stellt ein effektives Mittel zur Erhöhung der Datensicherheit dar und ermöglicht Unternehmen die Durchführung wertvoller Datenanalysen, während gleichzeitig die datenschutzrechtlichen Anforderungen eingehalten werden. Die EDSA-Leitlinien bieten hierbei eine wertvolle Grundlage, die zum einen die technischen und organisatorischen Maßnahmen detailliert beschreibt und zum anderen rechtliche Gesichtspunkte hervorhebt.

Zwar haben die Leitlinien des EDSA keinen bindenden Charakter, sie bieten Unternehmen jedoch konkrete Handlungsmöglichkeiten und Lösungsansätze, um einen Ausgleich zwischen Nutzung von personenbezogenen Daten und Schutz dieser Daten gewährleisten zu können. Dies geschieht insbesondere auch durch die Sammlung an Praxisbeispielen, die Teil des Anhangs der Leitlinien sind. Es ist daher ratsam für Unternehmen, die Empfehlungen des EDSA konsequent umzusetzen und ihre internen Prozesse regelmäßig zu überprüfen, um den aktuellen datenschutzrechtlichen Anforderungen zu entsprechen.

Betriebsvereinbarungen als Rechtsgrundlage für die Datenverarbeitung: Das Urteil des Europäischen Gerichtshofs vom 19. Dezember 2024 (Az.: C-65/23)

Gemäß Art. 88 der Datenschutz-Grundverordnung (DSGVO) haben die Mitgliedsstaaten die Möglichkeit, durch nationale Vorschriften oder Kollektivvereinbarungen spezielle Regelungen für die Verarbeitung personenbezogener Daten im Beschäftigungskontext festzulegen. In Deutschland hat das Bundesdatenschutzgesetz (BDSG) von diesem Spielraum Gebrauch gemacht und in § 26 Abs. 4 BDSG festgelegt, dass Mitarbeiterdaten auf Basis von Kollektivvereinbarungen verarbeitet werden dürfen. Doch welche Anforderungen müssen an solch eine nationale Rechtsvorschrift oder darauf beruhende Betriebsvereinbarungen gestellt werden?



Der Europäische Gerichtshof (EuGH) hat in seinem Urteil vom 19. Dezember 2024 (Az.: C-65/23) die Auslegung von Art. 88 Abs. 1 und 2 der DSGVO behandelt und dabei zwei entscheidende Fragen zur Verarbeitung personenbezogener Daten im Beschäftigungskontext auf Grundlage einer Kollektivvereinbarung geklärt.

I. Hintergrund

Bislang ungeklärt waren die Fragen, ob sich die Datenschutzkonformität von Vereinbarungen im Beschäftigungskontext ausschließlich an den Anforderungen des Art. 88 Abs. 2 DSGVO oder zusätzlich an den übrigen Vorgaben der DSGVO, insbesondere Art. 5, Art. 6 Abs. 1 und Art. 9 Abs. 1 und 2 DSGVO, messen lassen müssen und inwiefern nationale Gerichte eine Überprüfungskompetenz hinsichtlich der Betriebsvereinbarungen haben. Der Entscheidung des EuGH ist ein Vorabentscheidungsersuchen des Bundesarbeitsgericht (BAG) nach Art. 267 AEUV vorausgegangen. Dieses ermöglicht es nationalen Gerichten, dem EuGH Fragen zur Auslegung und Gültigkeit des Unionsrechts vorzulegen.

II. Der Sachverhalt

Im vorliegenden Fall verarbeitete die Beklagte K-GmbH anfänglich personenbezogene Daten ihrer Beschäftigten für Abrechnungszwecke mithilfe einer SAP-Software. Dies wurde durch mehrere Betriebsvereinbarungen mit dem Betriebsrat geregelt. Im Jahr 2017 führte der D-Konzern, zu dem die K-GmbH gehörte, konzernweit die cloudbasierte Software “Workday” als einheitliches Personal-Informationsmanagementsystem ein, um die zentrale Verarbeitung von Mitarbeiterdaten zu ermöglichen. Im Zuge dieser Umstellung übertrug die K-GmbH verschiedene personenbezogene Daten ihrer Beschäftigten von der vorherigen SAP-Software auf einen Server der Muttergesellschaft in den USA.

Um die Verwendung der neuen Software zu standardisieren, wurde eine “Duldungs-Betriebsvereinbarung” unterzeichnet, die festlegte, welche Datenkategorien für das Befüllen der Software verwendet werden durften.

Ein Mitarbeiter der K-GmbH reichte daraufhin Klage ein, um auf spezifische Informationen zuzugreifen, seine persönlichen Daten zu löschen und Schadensersatz beim Arbeitsgericht und später beim Landgericht zu fordern. Er argumentierte unter anderem, dass die K-GmbH persönliche Daten von ihm auf den Server der Muttergesellschaft übertragen hatte, von denen einige in der Duldungs-Betriebsvereinbarung nicht genannt waren, insbesondere seine privaten Kontaktdaten, Vertrags- und Vergütungsdetails, Sozialversicherungsnummer, Steueridentifikationsnummer, Staatsangehörigkeit und Familienstand. Dies sei ohne rechtliche Grundlage erfolgt und stelle somit eine Verletzung der DSGVO dar.

Nachdem der Kläger Berufung eingelegt hatte, musste sich das BAG mit der Klage befassen und legte dem EuGH die Rechtsfragen zur Vorabentscheidung vor.

III. Das Urteil

Der EuGH stellt in seinem Urteil klar, dass Rechtsvorschriften und Kollektivvereinbarungen nach Art. 88 Abs. 1 und 2 DSGVO neben den Anforderungen aus Art. 88 Abs. 2 DSGVO auch diejenigen aus Art. 5, Art. 6 Abs. 1 sowie Art. 9 Abs. 1 und 2 DSGVO erfüllen müssen. Zur Begründung führt er zunächst aus, dass Bestimmungen des Unionsrechts aufgrund des Vollharmonisierungsgrundsatzes in der gesamten Union einheitlich auszulegen seien. Obwohl Art. 88 DSGVO eine Öffnungsklausel zum Erlass spezifischer Rechtsvorschriften und Kollektivvereinbarungen enthalte, dürfe die Auslegung von Art. 88 DSGVO nach Auffassung des Gerichts nicht dazu führen, das andere Bestimmungen der DSGVO umgangen werden. Hierfür spreche insbesondere die Systematik der DSGVO. Die im Kapitel II („Grundsätze“) der DSGVO stehenden Art. 5, 6 und 9 hätten allgemeine Tragweite. Zudem verweise Art. 6 DSGVO in seinen Absätzen 2 und 3 ausdrücklich auf die Bestimmungen des Kapitel IX, mithin auf den darin enthaltenen Art. 88 DSGVO. Ergänzend beruft sich der EuGH auf Erwägungsgrund 8, 10 und 155 der DSGVO und sein Urteil vom 30. März 2023 (Az.: C-34/21).

Ferner stellt der EuGH klar, dass nationale Gerichte, unabhängig von dem Inhalt einer Rechtsvorschrift oder Kollektivvereinbarung nach Art. 88 Abs. 1 DSGVO, eine uneingeschränkte Kontrolle ausüben. Die gerichtliche Kontrolle umfasse daher auch den Spielraum der Parteien von Kollektivvereinbarungen bei der Bestimmung der „Erforderlichkeit“ einer Verarbeitung personenbezogener Daten im Sinne von Art. 5, 6 Abs. 1 sowie Art. 9 Abs. 1 und 2 DSGVO. Zur Begründung führt der EuGH insbesondere aus, dass die Beurteilungsbefugnis der Parteien einer Kollektivvereinbarung nicht dazu führen dürfe, dass die Parteien aus Gründen der Wirtschaftlichkeit oder Einfachheit Kompromisse schließen, die das Ziel der DSGVO, einen umfassenden Schutz personenbezogener Daten zu gewährleisten, in unzulässiger Weise beeinträchtigen könnten. Gleichwohl wird in der Entscheidung auch betont, dass die Parteien einer Kollektivvereinbarung im Allgemeinen über gute Grundlagen für die Beurteilung verfügen, ob eine Datenverarbeitung in einem konkreten beruflichen Kontext erforderlich ist. Trotzdem sei die Annahme einer eingeschränkten gerichtlichen Kontrolle nicht mit den Grundsätzen der DSGVO vereinbar.

IV. Fazit und Ausblick

Das Urteil verdeutlicht, dass hiervon auch im Beschäftigungskontext keine Ausnahme von der bisherigen Rechtsprechung des EuGHs im Hinblick auf die Gewährung eines hohen Schutzniveaus für die Rechte und Freiheiten der von einer Datenverarbeitung betroffenen Person zu machen ist. Der durch Art. 88 DSGVO gewährte Beurteilungsspielraum darf nicht zur Umgehung der allgemeinen Grundsätze der DSGVO zweckentfremdet werden.

Für Unternehmen steht angesichts des Urteils im Vordergrund, dass die Inhalte einer Betriebsvereinbarung gerichtlich voll überprüfbar und Unterschreitungen des Schutzstandards der DSGVO unzulässig sind. Insofern können auch datenschutzrechtliche Verstöße im Rahmen von Betriebsvereinbarungen u.a. einen Anspruch auf Schadensersatz sowie die Verhängung von empfindlichen Geldbußen zur Folge haben. Insbesondere deshalb sollten Unternehmen kontinuierlich umfassende Rechtmäßigkeitskontrollen aller Verarbeitungsvorgänge von personenbezogenen Beschäftigtendaten vornehmen.

Der datenschutzrechtliche Mitarbeiterexzess

Regelmäßig haben Mitarbeitende von Unternehmen und Behörden Zugriff auf sensible personenbezogene Daten und verarbeiten diese im Rahmen ihrer Tätigkeit. Aus rechtlicher Sicht ist eine solche Verarbeitung grundsätzlich von Art. 29 DSGVO gedeckt. Hiernach dürfen Auftragsverarbeiter und diesen unterstellte Personen ausschließlich auf Weisung des Verantwortlichen personenbezogene Daten verarbeiten, außer sie sind zu der Verarbeitung nach Unionsrecht oder dem Recht der Mitgliedstaaten verpflichtet. Doch was sind die Konsequenzen eines Überschreitens dieser Weisungen? Sowohl die Rechtsprechung als auch die Datenschutzaufsichtsbehörden befassen sich vermehrt mit diesen Fällen und den einhergehenden Folgen der Haftung nach Art. 82 DSGVO, einer Geldbuße nach Art. 83 DSGVO sowie des Auskunftsanspruch nach Art. 15 DSGVO.

I. Verantwortlichkeit für Handeln von Beschäftigten

Die DSGVO kennt einen weiten Spielraum bei der Zurechnung des Mitarbeiterverhaltens auf das Unternehmen, für das die Mitarbeiter tätig sind. Die datenschutzrechtliche Verantwortlichkeit liegt grundsätzlich beim Unternehmen. Die einzelnen Beschäftigten sind im Grundsatz nicht als Verantwortliche nach Art. 4 Nr. 7 DSGVO anzusehen und tragen daher keine Verantwortung für die Einhaltung der Bestimmungen der DSGVO. Vielmehr ist es die Pflicht der Unternehmensleitungen, durch Weisungen nach Art. 29 DSGVO und entsprechende technische Beschränkungen dafür zu sorgen, dass Beschäftigte personenbezogene Daten nur im Rahmen ihrer betrieblich veranlassten Tätigkeit verarbeiten.

Davon ausgenommen sind jedoch Konstellationen, in denen Beschäftigte im Exzess handeln, indem sie sich selbst zum Verantwortlichen aufschwingen. Einen solchen Mitarbeiterexzess definiert die Datenschutzkonferenz (DSK) in einer Entschließung vom 3. April 2019 als Handlung von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden kann. Sie nimmt also eine objektive Betrachtungsweise ein. Es kommt nicht primär darauf an, ob die Beschäftigten subjektiv eigene Interessen verfolgen, sondern ob die objektive Zweckbestimmung den ihnen zugewiesenen Aufgaben entspricht. Verfolgt ein Beschäftigter eigene Zwecke, wird er dadurch zum Verantwortlichen im Sinne des Art. 4 Nr. 7 DSGVO.

Nur in Ausnahmefällen, beispielsweise wenn das Unternehmen das Verhalten des Mitarbeiters billigt oder Kenntnis davon hat und nicht eingreift, kann eine gemeinsame Verantwortlichkeit (Art. 26 DSGVO) bestehen.

II. Aufsichtsbehördliche Stellungnahmen zum datenschutzrechtlichen Mitarbeiterexzess

Einige Datenschutzaufsichtsbehörden berichten vermehrt über Fälle von Mitarbeiterexzessen in ihrem letzten Tätigkeitsberichten. So auch die Landesdatenschutzbeauftragten aus Rheinland-Pfalz, Mecklenburg-Vorpommern und Brandenburg.

Der rheinland-pfälzische Datenschutzbeauftragte schildert den Fall, in dem ein Bankmitarbeiter, der privat eine Wohnung vermietet, die Möglichkeit einer Bonitätsabfrage nutzt um die Bonität eines möglichen Mieters abzufragen. Für diese Handlungen sei nicht mehr der Arbeitgeber verantwortlich, sondern der Beschäftigte wird selbst zum Verantwortlichen und Adressat aufsichtsbehördlicher Maßnahmen. Zudem gewährt der Datenschutzbeauftragte einen Einblick in die Praxis bei der Verhängung von Sanktionen bei einem Mitarbeiterexzess. Entscheidend sei dabei für ihn auch, welche arbeitsrechtlichen Maßnahmen der Arbeitgeber bereits getroffen habe.

Der Datenschutzbeauftragte aus Mecklenburg-Vorpommern unterstreicht im Rahmen seines Tätigkeitsberichts zudem die Wichtigkeit der Weisungen und Maßnahmen durch den Arbeitgeber. Fehlt es an geeigneten Weisungen und technischen Vorkehrungen durch den Arbeitgeber, kann dieser auch bei einem Mitarbeiterexzess Verantwortlicher sein.

Die Datenschutzbeauftragte aus Brandenburg befasst sich in ihrem Tätigkeitsbericht mit Fällen der unbefugte Datenabfragen in Krankenhäusern. In verschiedenen Krankenhäusern wurde durch einzelne Krankenhausmitarbeiter ohne dienstlichen Grund Einsicht in die elektronische Patientenakte einer Kollegin genommen, die in dem jeweiligen Krankenhaus zugleich selbst Patientin war. Von dieser Einsichtnahme waren u. a. Arztbriefe, Laborergebnisse sowie Berichte über Behandlungen und Operationen umfasst. Diese beinhalten besonderen Kategorien von personenbezogenen Daten im Sinne des Art. 9 Abs. 1 DSGVO, die durch die DSGVO besonders geschützt sind. Für die Rechtmäßigkeit der Verarbeitung müssen insoweit neben einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO auch die besonderen Anforderungen aus Art. 9 Abs. 2 DSGVO erfüllt sein. Insofern stellte die LDA Brandenburg als Ergebnis der Überprüfung fest, dass eine Rechtsgrundlage für die fragliche Verarbeitung nicht vorliege, weil die Personen beim Abruf der Patientenakte weder mit der Behandlung noch mit der Abrechnung betraut seien. Vielmehr sei die Datenabfrage aus privaten Gründen bzw. Neugier über den Krankheitsverlauf der Kollegin und ohne dienstlichen Anlass erfolgt. Folglich liege ein Mitarbeiterexzess vor, sodass das Bußgeld für die Rechtsverstöße unmittelbar gegen die jeweiligen Krankenhausmitarbeiter festgesetzt wurde.

III. Aktuelle Rechtsprechung zum datenschutzrechtlichen Mitarbeiterexzess

Das OLG Stuttgart hat in seiner Entscheidung vom 25. Februar 2025 (Az.: 2 ORbs 16 Ss 336/24) festgestellt, dass die nicht dienstlich veranlasste Datenbankabfrage durch einen Polizeibeamten eine eigene Verantwortlichkeit nach der DSGVO begründet. Im konkreten Fall verurteilte das AG Stuttgart den Polizeibeamten wegen der rechtswidrigen Verarbeitung personenbezogener Daten zu einer Geldbuße von 1.500 Euro. Der Beamte hatte ohne dienstlichen Anlass das polizeiliche Auskunftssystem POLAS genutzt, um Daten über einen damaligen Kollegen abzurufen. Das AG Stuttgart hatte den Beamten als Verantwortlichen nach Art. 4 Nr. 7 DSGVO angesehen.

Das OLG Stuttgart bestätigte die Entscheidung der Vorinstanz und wies die Berufung als unbegründet zurück. Das OLG folgte in seiner Entscheidung der Entschließung der DSK, wonach ein Beschäftigter, der Daten für eigene Zwecke verarbeitet, als Verantwortlicher anzusehen ist. Beschäftigte, die personenbezogene Daten für Zwecke außerhalb ihrer dienstlichen Tätigkeit abrufen, entziehen sich der Aufsicht und Leitung ihrer Vorgesetzten und treffen eigene Entscheidungen über die Zwecke und Mittel der Datenverarbeitung. Es handelt sich um einen Mitarbeiterexzess, da nicht weisungswidrig, sondern überhaupt nicht dienstlich gehandelt wird. Hat der Arbeitgeber alle erforderlichen Maßnahmen ergriffen, um einen solchen Mitarbeiterexzess zu verhindern, kommt eine Haftungsbefreiung in Betracht. Notwendige Grundlage hierfür ist ein enges Weisungskonzept und technische Schutzmaßnahmen zur Verhinderung von Datenschutzverstößen.

IV. Konsequenzen für Unternehmen

Für Unternehmen ergibt sich insbesondere die Notwendigkeit konkrete Weisungen erteilen und Schutzmaßnahmen ergreifen, um eine Mitverantwortlichkeit zu vermeiden. Dies gilt insbesondere deshalb, da sich auch bei einem Mitarbeiterexzess eine gesamtschuldnerische Haftung gemäß Art. 82 Abs. 2 DSGVO ergeben kann und somit auch das Unternehmen haf-

ten könnte. Dringend erforderlich ist daher die Ausarbeitung und Dokumentation eines umfangreichen Datenschutzkonzeptes, das insbesondere klare Richtlinien und Verfahren für den Zugriff auf und die Verarbeitung von personenbezogenen Daten, sowie regelmäßige interne Kontrollen und Audits vorsieht, um so die Möglichkeit einer Exkulpation zu schaffen. Arbeitgeber sollten ihre Mitarbeiter regelmäßig über die datenschutzrechtlichen Bestimmungen und die Konsequenzen von Verstößen informieren, insbesondere auch über die ernsthaften arbeitsrechtlichen und disziplinarischen Konsequenzen.

Ebenfalls zu beachten ist, dass ein Mitarbeiterexzess ein Datenschutzverstoß nach Art. 33 und 34 DSGVO darstellen kann, sodass regelmäßig die Aufsichtsbehörden und gegebenenfalls auch die Betroffenen hierüber zu informieren sind. Dies gilt auch dann, wenn dem Unternehmen kein datenschutzrechtliches Fehlverhalten zugerechnet werden kann.

Der Entwurf der Financial Data Access Regulation: Ein Meilenstein für den digitalen Finanzmarkt der Zukunft

Am 28. Juni 2023 veröffentlichte die Europäische Kommission den Entwurf der Financial Data Access Regulation (FIDA-E), die den Datenaustausch im Finanzsektor erleichtern soll. Ein Austausch von Finanzdaten über Schnittstellen soll für Finanzunternehmen Chancen hinsichtlich neuer Finanzprodukte, innovative Geschäftsmodelle und personalisierte Services eröffnen.

I. Hintergrund des FIDA-E

Derzeit haben Personen, die Finanzprodukte und -dienstleistungen in Anspruch nehmen (sog. Kunden, vgl. Art. 3 Nr. 2 FIDA-E), keine wirksame Kontrolle über den Zugang zu ihren Daten und deren Austausch im EU-Finanzsektor über Zahlungskonten hinaus. In Ermangelung eines Regelwerks stehen Kunden dem Austausch ihrer Daten daher häufig ablehnend gegenüber. Unternehmen, die auf Kundendaten zugreifen möchten, um innovative Dienstleistungen anbieten zu können (sog. Datennutzer, vgl. Art. 3 Nr. 6 FIDA-E), haben Schwierigkeiten, auf Daten zuzugreifen, die sich im Besitz der Finanzinstitute befinden, die diese Kundendaten erheben, speichern und verarbeiten (sog. Dateninhaber, vgl. Art. 3 Nr. 5 FIDA-E). Die Gründe für die genannten Schwierigkeiten sind in den erheblichen Unterschieden zwischen den Daten und der technischen Infrastruktur zu finden, die insbesondere auf eine mangelnde Standardisierung zurückzuführen sind.

Dies hat zur Folge, dass Kundinnen und Kunden, selbst wenn sie dies wünschen, keinen umfassenden Zugang zu datenbasierten Finanzdienstleistungen und -produkten haben. Der FIDA-E adressiert diese Herausforderungen und zielt darauf ab, sowohl Verbraucherinnen und Verbrauchern als auch Unternehmen eine gesteigerte Kontrolle über den Zugang zu Finanzdaten zu ermöglichen. Hierdurch sollen die Datennutzer maßgeschneiderter Finanzprodukte und -dienstleistungen entwickeln können, die den individuellen Bedürfnissen der Nutzer entsprechen.

II. Wesentliche Regelungsinhalte

Die Kundendaten stellen das zentrale Element des FIDA-E dar. Für die Verwaltung, die Nutzung und den Austausch dieser Daten sind drei zentrale Akteure von Bedeutung: der Kunde, der Datennutzer und der Dateninhaber.

1. Anwendungsbereich

Der sachliche Anwendungsbereich des FIDA-E erstreckt sich ausschließlich auf Kundendaten bestimmter Kategorien, die in Art. 2 Abs. 1 FIDA-E aufgeführt sind (z. B. Hypothekarkreditverträge). Die Definition von Kundendaten erfolgt gemäß Art. 3 Nr. 3 FIDA-E. Der persönliche Anwendungsbereich wird in Art. 2 Abs. 2 FIDA-E für bestimmte Stellen in deren Eigenschaft als Dateninhaber oder Datennutzer festgelegt. Klassische Finanzinstitute, wie z. B. Kredit- oder Zahlungsinstitute fallen insoweit unter diese Regelung. Eine wesentliche Neuerung des FIDA-E besteht darin, dass er den persönlichen Anwendungsbereich für Finanzinformationsdienstleister öffnet, wie in Art. 2 Abs. 2 lit. o) FIDA-E dargelegt. Dies ist nach Art. 3 Nr. 7 FIDA-E ein Datennutzer, der zum Zwecke der Erbringung von Finanzinformationsdienstleistungen gemäß Art. 14 FIDA-E berechtigt ist, auf die in Art. 2 Abs. 1 FIDA-E aufgeführten Kundendaten zuzugreifen. Die Voraussetzungen für die Zulassung als Finanzinformationsdienstleister sind in den Art. 12 ff. FIDA-E definiert.

2. Pflichtenkatalog

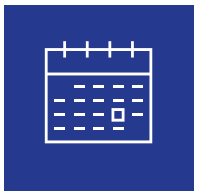
Der FIDA-E adressiert insbesondere den Dateninhaber, welchem bestimmte Pflichten im Verhältnis zum Kunden und zum Datennutzer obliegen. Auf Antrag des Kunden ist der Dateninhaber verpflichtet, die Kundendaten unverzüglich, unentgeltlich, kontinuierlich und in Echtzeit zur Verfügung zu stellen, vgl. Art. 4 FIDA-E. Zudem kann der Kunde dem Datennutzer eine Zugriffsberechtigung auf seine Daten erteilen. Zur Überwachung und Verwaltung der durch den Kunden erteilten Zugriffsberechtigungen ist der Dateninhaber verpflichtet, ein Dashboard einzurichten, welches den Voraussetzungen der Art. 7 lit. f. FIDA-E entspricht. Dem Kunden muss im Dashboard u. a. ein Überblick über alle aktiven Zugangsberechtigungen gegeben werden. Dieses muss leicht auffindbar und die Informationen klar, richtig und leicht verständlich sein. Erteilt der Kunde dem Datennutzer eine Zugriffsberechtigung auf seine Daten, ist der Dateninhaber nach Art. 5 Abs. 1 FIDA-E dazu verpflichtet, dem Datennutzer die Kundendaten unverzüglich, kontinuierlich und in Echtzeit zur Verfügung zu stellen. Für die Bereitstellung der Kundendaten kann der Dateninhaber gemäß Art. 5 Abs. 2 FIDA-E ein Entgelt verlangen, sofern die Kundendaten nach den Regeln und Modalitäten eines Systems für den Austausch von Finanzdaten bereitgestellt werden. Gemäß Art. 9 Abs. 1 FIDA-E sind die Dateninhaber und -nutzer verpflichtet, einem solchen System innerhalb von 18 Monaten nach Inkrafttreten der Verordnung beizutreten, wobei das System die Voraussetzungen des Art. 10 FIDA-E erfüllen muss. Gemäß Art. 9 Abs. 2 FIDA-E steht es den Dateninhabern und -nutzern frei, auch Mitglied mehrerer solcher Systeme zu werden.

III. Fazit und Ausblick

Der FIDA-E stärkt die Kontrolle der Verbraucher über ihre Finanzdaten und erleichtert Unternehmen den Zugang zu relevanten Informationen, um innovative Finanzprodukte zu entwickeln. Die Verpflichtung der Finanzinstitute, Daten in Echtzeit bereitzustellen, sowie die Möglichkeit für Kunden, den Zugang zu steuern, tragen zur Förderung des Vertrauens im Finanzsektor bei. Langfristig könnte der FIDA-E den Wettbewerb durch die Bereitstellung maßgeschneiderter Produkte und Dienstleistungen anregen und zu mehr Transparenz am Finanzmarkt beitragen. Die Realisierung dieses Potenzials ist jedoch maßgeblich von der Entwicklung und Implementierung einer geeigneten technischen Infrastruktur sowie der Akzeptanz der Verbraucherinnen und Verbraucher abhängig.

Die genaue Ausgestaltung der FIDA wird sich erst nach Abschluss des Trilog-Verfahrens, das seit dem 1. April 2025 läuft, zeigen. Finanzinstitute sollten sich aber rechtzeitig mit den Anforderungen an eine erfolgreiche Umsetzung auseinandersetzen, um die Chancen von FIDA optimal nutzen zu können.

Veranstaltungen, Veröffentlichungen und Blog



Eine Übersicht mit unseren Veranstaltungen finden Sie hier.

Eine Liste unserer aktuellen Veröffentlichungen finden Sie hier.

Unseren Blog finden Sie hier.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Michael Rath, Partner
Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 25795
michael.rath@luther-lawfirm.com

Haftungsausschluss

Obgleich dieser Newsletter sorgfältig erstellt wurde, wird keine Haftung für Fehler oder Auslassungen übernommen. Die Informationen dieses Newsletters stellen keinen anwaltlichen oder steuerlichen Rechtsrat dar und ersetzen keine auf den Einzelfall bezogene anwaltliche oder steuerliche Beratung. Hierfür stehen unsere Ansprechpartner an den einzelnen Standorten zur Verfügung.

Luther.

Bangkok, Berlin, Brüssel, Delhi-Gurugram, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Ho-Chi-Minh-Stadt, Jakarta, Köln, Kuala Lumpur, Leipzig, London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Weitere Informationen finden Sie unter
www.luther-lawfirm.com
www.luther-services.com

unyer GLOBAL ADVISORS