Newsletter IP/IT

August 2024

Inhalt

Die KI-Verordnung ist (endlich) da – Auswirkungen, Anpassungsbedarf und Chancen

Die KI-Verordnung (KI-VO) ist am 1. August in Kraft getreten. Als europäische Verordnung muss sie nicht mehr in nationales Recht umgesetzt werden, sondern gilt ab sofort. Der europäische Gesetzgeber hat außerdem erstaunlich kurze Umsetzungsfristen festgelegt. Die ersten Verpflichtungen aus der KI-VO müssen bereits sechs Monate nach Inkrafttreten umgesetzt werden. Wir zeigen auf, was Unternehmen nun beachten müssen.

I. Der Weg zur KI-VO

Der Rat der 27 EU-Mitgliedstaaten hat am 21. Mai 2024 die KI-Verordnung (KI-VO) als einen einheitlichen Rahmen für den Einsatz von KI in der EU verabschiedet. Am 12. Juli 2024 wurde die KI-VO im EU-Amtsblatt veröffentlicht. Gemäß Art. 113 KI-VO tritt diese am zwanzigsten Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union in Kraft, also am 1. August 2024. Dabei erstrecken sich die Compliance-Umsetzungsfristen auf die nächsten 3 Jahre. Der deutschsprachige KI-VO-Text ist abrufbar unter: Verordnung - EU - 2024/1689 - EN - EUR-Lex (europa.eu).

II. Ziel der KI-VO

Der jetzige Verordnungstext verdeutlicht den Anspruch der EU, bei der Entwicklung sicherer, vertrauenswürdiger und ethisch vertretbarer KI-Anwendungen weltweit eine Führungsrolle einzunehmen. Die Kommission hat erkannt, welche Vorteile der Einsatz von KI für Gesellschaft und Umwelt hat und welche Wettbewerbsvorteile sich für europäische Unternehmen ergeben. Zugleich sieht der europäische Gesetzgeber die Risiken, die beim Einsatz von KI für die Gesellschaft entstehen können. Diese Risiken soll die KI-VO eindämmen, indem sie allen Akteuren in der Lieferkette eines KI-Systems Pflichten auferlegt. Was die KI-VO nicht regelt, sind Haftungsfragen rund um den Einsatz von KI. Diese sollen in zukünftigen Richtlinien der EU adressiert werden.

III. Anwendungsbereich

1. Sachlicher Anwendungsbereich: KI-Definition

Der europäische Gesetzgeber versucht sich in der KI-VO erstmalig an einer Definition für KI-Systeme. Die KI-VO definiert den Begriff „KI-System“ in Art. 3 Nr. 1 wie folgt:

*„KI-System“ ein maschinengestütztes **System**, das so konzipiert ist, dass es für einen in **unterschiedlichem Grade autonomen Betrieb** ausgelegt ist und das nach seiner Betriebsaufnahme **anpassungsfähig** sein kann und das aus den **erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden**, die physische oder virtuelle Umgebungen beeinflussen können.“*

Damit legt die KI-VO ein sehr weites Verständnis von KI-Systemen zugrunde, sodass erste Abgrenzungsschwierigkeiten zur herkömmlichen Software abzusehen sind. Während die herkömmliche Software ausschließlich auf und mit den von natürlichen Personen definierten Regeln funktioniert und Operationen automatisch ausführt, soll das KI-System mehr können. Vor allem soll es Eingaben oder Daten-Ergebnisse autonom ableiten können. Dabei nutzt ein KI-System in der Regel Machine Learning sowie andere von der Logik gestützte Konzepte, um mit verschiedenen Graden an Autonomie zu arbeiten.

2. Persönlicher Anwendungsbereich

Der persönliche Anwendungsbereich der Verordnung ist sehr weit. Sie richtet sich an nahezu alle Akteure in der KI-Wertschöpfungskette. Insbesondere wird sie „Anbieter“ und „Nutzer“ von KI-Systemen adressieren. Der Anwendungsbereich erstreckt sich auf zahlreiche Unternehmen am EU-Markt, die Softwarelösungen mit implementierten KI-Elementen einsetzen, zumal auch Nutzer unter Umständen Adressaten der Pflichten für Anbieter werden können. Darüber hinaus enthält die Verordnung Pflichten für „Einführer“ und „Händler“, also solche Akteure, die KI-Systeme aus dem Ausland in den europäischen Markt einführen oder die Systeme vertreiben.

IV. Wesentliche Regelungsinhalte

1. Regelungssystematik der KI-VO: Risikobasierter Ansatz

Die KI-VO verfolgt einen risikobasierten Ansatz. Das heißt, je höher die Risiken, die von einem KI-System für die Grundrechte von EU-Bürgern oder andere sensible Rechtsgüter ausgehen, desto strenger sind die regulatorischen Anforderungen. Die Verordnung sieht vier Risikoklassen vor.

a) Verbotene KI-Systeme

Zunächst führt die KI-VO eine Reihe von Praktiken auf, die im Bereich der künstlichen Intelligenz gänzlich verboten sein sollen. Grund dafür sind nicht hinnehmbare Risiken für die Grundrechte und Werte der Union. Dazu zählen die Entwicklung und Verwendung von KI-Systemen, die Personen manipulieren, sodass sie sich oder anderen Personen einen physischen oder psychischen Schaden zufügen können. Außerdem soll KI verboten sein, mittels derer die Schwäche oder Schutzbedürftigkeit gewisser (vulnerabler) Gruppen ausgenutzt wird und Personen in der Folge geschädigt werden können. Verboten werden zudem KI-Systeme, die zur Bewertung oder Klassifizierung der Vertrauenswürdigkeit von Personen benutzt werden sollen (Social-Scoring-Systeme). Zuletzt wird, bis auf wenige Ausnahmen, die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen durch Ermittlungsbehörden zum Zweck der Strafverfolgung untersagt. Diese Verbotsliste wird für die wenigsten Unternehmen eine praktische Bedeutung haben, da sie nur besonders kritische Systeme enthält. Im Unternehmensalltag werden diese gegenwärtig nicht eingesetzt.

b) Hochrisiko-KI-Systeme

Hochrisiko-KI umfasst solche Systeme, von denen eine besonders hohe Gefahr für die Gesundheit und Sicherheit oder die Grundrechte von EU-Bürgern befürchtet wird. Sie stellen den Hauptregelungsgegenstand der KI-VO dar, der Großteil der Anforderungen aus der Verordnung bezieht sich auf diese Risikogruppe. Viele Unternehmen nutzen – möglicherweise unbewusst – bereits jetzt Anwendungen, die zukünftig als Hochrisiko-KI eingestuft sein werden.

Wann eine KI mit hohem Risiko vorliegt, ist in der Verordnung (in Art. 6 und im Anhang III) geregelt. Danach soll ein KI-System zum einen dann mit einem hohen Risiko behaftet sein, wenn es selbst oder als Sicherheitsbauteil eines anderen Produktes aufgrund bereits bestehender EU-Harmonisierungsvorschriften einer Konformitätsbewertung unterzogen werden muss (sog. „embedded AI“). Vereinfacht gesagt, handelt es sich hier um bestimmte KI-Anwendungen, die in physischen Produkten verbaut sind.

Ferner wird zum anderen dann von einer Hochrisiko-KI ausgegangen, wenn das KI-System in bestimmten Bereichen

eingesetzt wird (z. B. Verwaltung, Personalmanagement oder Strafverfolgung) und einem der in Anhang III abschließend aufgeführten konkreten KI-Systeme aus diesen Bereichen entspricht (sog. „stand-alone AI“). Hochrisiko-KI-Systeme im HR-Bereich könnten beispielhaft solche KI-Systeme sein, die für die Einstellung und die Auswahl von (neuen) Mitarbeitern in Bewerbungsprozessen eingesetzt werden (vgl. Art. 6 Nr. 4 a) und b) KI-VO).

c) Geringes und minimales Risiko

Ferner beschreibt die KI-VO Systeme mit geringem und mit minimalem Risiko. KI-Systeme mit geringem Risiko sind solche, die für die Interaktion mit Menschen bestimmt sind und nicht unter die Gruppe der verbotenen KI oder der Hochrisiko-KI fallen. Von solchen Algorithmen sollen potenziell lediglich gewisse Manipulationsrisiken ausgehen. Darunter fallen beispielsweise Chatbots, die den Anschein menschlicher Kommunikation erwecken können. Daher müssen Unternehmen, die derartige Systeme entwickeln oder verwenden, vor allem gewisse Transparenzpflichten erfüllen. Die Nutzer von KI-Systemen sollen stets wissen, dass sie mit einer KI sprechen/schreiben oder KI-generierte Ergebnisse erhalten (gemeint sind vor allem Deepfakes). Nutzer von KI-Systemen mit minimalem Risiko sollen zudem Verhaltenskodizes (Code of Conduct) aufstellen, um einen verantwortungsbewussten Umgang mit KI-Systemen zu gewährleisten.

2. Wesentliche Pflichten aus der KI-VO

Die KI-VO enthält einen umfangreichen Katalog von Anforderungen und Verpflichtungen, die sich vor allem an Anbieter von KI richten. Doch auch für Nutzer bzw. Betreiber, wie diese nach der Terminologie der KI-VO genannt werden, Einführer und Händler enthält die Verordnung Pflichten.

Die Anbieter und Betreiber von KI-Systemen müssen Maßnahmen ergreifen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen (KI-Kompetenz, Art. 4 KI-VO). Dabei sollen ihre technischen Kenntnisse, ihre Erfahrung berücksichtigt werden, um eine bestmögliche Schulung zu ermöglichen. Die Etablierung einer KI-Kompetenz im Unternehmen soll bereits sechs Monate nach Inkrafttreten der KI-VO erfolgen. Unternehmen sollten deshalb jetzt schon planen, wie sie ihre Mitarbeiter schulen können (z.B. durch KI-Richtlinien, Mitarbeiterschulungen, etc.).

Weitere Anforderungen und Pflichten beziehen sich vor allem auf Hochrisiko-KI.

Anbieter von Hochrisiko-KI-Systemen trifft die Verpflichtung zur Etablierung und Umsetzung von Maßnahmen aus den Bereichen:

- Risikomanagementsysteme
- Data-Governance
- Dokumentationspflichten
- Aufzeichnungspflichten
- Transparenz- und Instruktionspflichten
- Menschliche Aufsicht
- Genauigkeit, Robustheit und Cybersicherheit
- Qualitätsmanagementsystem
- Konformitätsbewertungsverfahren

Betreiber von Hochrisiko-KI-Systemen trifft u.a. die Verpflichtung zur Etablierung und Umsetzung von Maßnahmen aus den Bereichen:

- Etablierung von geeigneten technischen und organisatorischen Maßnahmen zur Verwendung von KI-Systemen gemäß der den Systemen beigefügten Betriebsanleitungen
- Menschliche Aufsicht durch qualifiziertes Personal
- Überwachung des Betriebs des Hochrisiko-KI-Systems anhand der Betriebsanleitung
- Protokollaufbewahrungspflichten
- Durchführung von Datenschutz-Folgenabschätzungen
- Zusammenarbeit mit Aufsichtsbehörde

V. Verhältnis KI-VO und DSGVO

KI arbeitet in vielen Fällen mit enormen Datenmengen. Deshalb sind bei der Entwicklung, aber auch im Umgang mit KI-Systemen häufig datenschutzrechtliche Anforderungen zu beachten. Insbesondere im Rahmen des maschinellen Lernens (Machine Learning) werden KI-Algorithmen mit einer Vielzahl an Datensätzen trainiert. Beim Machine Learning lernt die Software autonom, indem sie auf Basis der Korrelation von alten und neuen Datenmustern, Arbeitsergebnisse produziert. Je nach Input und Anwendungsfeld kommt es dabei auch zur Verarbeitung von personenbezogenen Daten. Die KI-VO stellt mit Blick auf den Datenschutz in Art. 2 Abs. 7 klar, dass die Vorgaben der DSGVO vollumfänglich Anwendung finden und von den betroffenen Unternehmen parallel zu den Vorgaben aus der KI-VO einzuhalten sind (z.B. bei der Entwicklung und Nutzung von KI), demgemäß wird es gegebenenfalls zu „Doppelverpflichtungen“ aus den beiden Verordnungen kommen. Die beiden Regelungsmaterien liegen inhaltlich nah beieinander, zudem ähnelt sich die Natur der Verpflichtungen und Regelungsansätze aus KI-VO und

DSGVO an vielen Stellen. Bislang haben sich diverse Datenschutzaufsichtsbehörden zur Verarbeitung personenbezogener Daten in KI-Systemen (insbesondere beim Training von KI-Systemen) geäußert, z.B. zuletzt die Aufsichtsbehörde Hamburg. Unklar ist bislang, ob die Einhaltung der KI-VO in Deutschland durch die Datenschutzaufsichtsbehörden überwacht wird. Hierfür hat sich in einem am 16. Juli 2024 veröffentlichen Statement der Europäische Datenschutzausschuss ausgesprochen.

VI. Ausblick und Handlungsempfehlung

Die KI-VO umfasst eine Vielzahl von Anwendungen in unterschiedlichsten Bereichen. Smarte Vorsortierungen in der HR, Chatbots und generative KI im Marketing sowie optische Auswertungen in der Industrie und Medizin werden bereits seit Jahren zunehmend von Unternehmen genutzt. Die weite Definition der KI-VO könnte dazu führen, dass ein Großteil dieser Systeme zukünftig dem Anwendungsbereich der KI-VO unterfallen.

Bei Nichteinhaltung der Vorschriften der KI-VO drohen insbesondere Bußgelder von bis zu 7 % des jährlichen weltweiten Umsatzes des Unternehmens bzw. bis zu 35 Millionen Euro.

Unternehmen sollten zeitnah identifizieren, welche KI-Systeme oder KI-Modelle sie einsetzen bzw. auf dem Markt anbieten. Im nächsten Schritt sind Anwendungen entsprechend der Klassifizierung der KI-VO einzuordnen und die daraus resultierenden Verpflichtungen zu ermitteln und umzusetzen. Dies betrifft insbesondere die Informations- und Dokumentationspflichten aus der KI-VO sowie der DSGVO. Zur Umsetzung können Unternehmen beispielsweise KI-Richtlinien erarbeiten und intern kommunizieren, die eine einheitliche Umsetzung der Vorgaben aus der KI-VO gewährleisten.

Im Übrigen kann es je nach Umfang des Einsatzes oder der Entwicklung von KI-Anwendungen im Unternehmen empfehlenswert sein, ein interdisziplinäres KI-Gremium zu etablieren, welches die Umsetzung der KI-VO überwacht und KI-Einführungsprojekte begleitet. Alternativ kann auch ein AI Officer bzw. KI-Compliancebeauftragter benannt werden, welcher in die verschiedenen KI-Projekte eingebunden wird. Zwar schreibt die KI-VO solche Positionen nicht vor, aber innerhalb eines Unternehmens muss geklärt sein, wer für diese Themen verantwortlich ist. Eine entsprechende Governance- und Compliancestruktur muss etabliert werden.

Ziele und Herausforderungen bei der Gesundheitsdatennutzung in Deutschland und Europa

Die Digitalisierung im Gesundheitswesen bietet viele Chancen, die Versorgung für Patientinnen und Patienten zu verbessern und die Arbeit für die Ärzteschaft zu erleichtern. Zwei deutsche Gesetze und eine geplante EU-Verordnung sollen dies voranbringen: Das Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz - DigiG), das Gesetz zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz - GNDG) sowie die Verordnung über den europäischen Raum für Gesundheitsdaten (EHDS-VO).

I. Hintergrund

Alle drei Vorhaben dienen der Digitalisierung des Gesundheitswesens. Das Digital-Gesetz soll den Behandlungsalltag für Behandelnde und Patienten in Deutschland insbesondere durch die flächendeckende Einführung der elektronischen Patientenakte (ePA) vereinfachen. Das GDNG sieht beispielsweise vor, dass ePA-Daten in anonymisierter Form zu bestimmten Zwecken, insb. Forschungszwecken, verwendet werden können. Und der EHDS soll es Patienten und Datennutzenden ermöglichen, grenzüberschreitend auf Gesundheitsdaten zuzugreifen.

II. Gesetz zur verbesserten Nutzung von Gesundheitsdaten (GDNG)

Am 26. März 2024 ist das Gesetz zur verbesserten Nutzung von Gesundheitsdaten in Kraft getreten.

Mit dem GDNG sollen Gesundheitsdaten für die Forschung erschlossen werden. Kern des Gesetzes ist die erleichterte Nutzbarkeit von Gesundheitsdaten für gemeinwohlorientierte Zwecke. Dazu wird unter anderem eine dezentrale Gesundheitsdateninfrastruktur mit einer zentralen Datenzugangs- und Koordinierungsstelle geschaffen, die die Gesundheitsdaten für Kranken- und Pflegekassen sowie Forschungs- und andere Einrichtungen besser verfügbar und nutzbar macht. Gleichzeitig sollen bürokratische Hürden reduziert und der Gesundheitsdatenschutz gestärkt werden.

1. Für wen gilt das GDNG?

Der Kreis der Antragsberechtigten für den Zugang zu der Datenzugangs- und Koordinierungsstelle ist breit gefasst. Zur Weiterverarbeitung sind datenverarbeitende Gesundheitseinrichtungen berechtigt. Darunter versteht das GDNG u.a. solche Einrichtungen, in denen für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin Daten von oder unter der Verantwortung von Angehörigen eines Heilberufs verarbeitet werden, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert. Zudem haben gesetzliche Kranken- und Pflegekassen die Möglichkeit, datengestützte Auswertungen durchzuführen.

2. Was regelt das GDNG?

Ein zentraler Bestandteil des GDNG besteht in der Einrichtung einer Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten. Diese Stelle ist die Hauptanlaufstelle, wenn Personen oder Einrichtungen Zugang zu Gesundheitsdaten wünschen, die bei sog. datenhaltenden Stellen gespeichert sind. Hier werden erstmalig Gesundheitsdaten aus verschiedenen Datenquellen zu Forschungszwecken miteinander verknüpft werden. Die Datenhaltung erfolgt weiterhin dezentral, indem die Daten am bisherigen Ort gespeichert bleiben und lediglich spezifisch für den jeweiligen Forschungsantrag in einer sicheren Verarbeitungsumgebung zugänglich gemacht werden. Die Datenzugangs- und Koordinierungsstelle unterstützt den Antragsteller in erster Linie organisatorisch, leitet z.B. Anträge weiter und gibt Anweisungen zum Datenschutz. Das GDNG bietet auch neue rechtliche Möglichkeiten für die Weiterverarbeitung von Gesundheitsdaten, insbesondere zur Qualitätssicherung.

Weitere wichtige Änderungen für gesetzliche Kranken- und Pflegekassen finden sich auch im SGB V. Diese Änderungen erlauben es ihnen, Gesundheitsdaten der Versicherten (z.B. Diagnosen und verordnete Medikamente) für gesetzlich definierte Zwecke auszuwerten und die Ergebnisse dieser Analysen den Versicherten mitzuteilen. Diese Zwecke umfassen beispielsweise die Erkennung von seltenen oder schwerwiegenden Krankheiten sowie die Erkennung von Impfindikationen für Schutzimpfungen. In der Praxis können Krankenkassen ihre Versicherten auf Basis der vorliegenden Daten über ein erhöhtes Krebsrisiko oder empfohlene Impfungen informieren. Die Kranken- und Pflegekassen haben in diesem Zusammenhang besondere Transparenzpflichten. Die Versicherten müssen vor der geplanten Auswertung ihrer Daten informiert werden und können der Auswertung widersprechen. Die Kranken- und Pflegekassen müssen auch eine Reihe von Informations-, Melde- und Anzeigepflichten beachten. Zudem wurde eine Ordnungswidrigkeit im Falle des Verstoßes eingeführt.

Die federführende Datenschutzaufsicht für länderübergreifende Forschungsvorhaben wird auf alle Gesundheitsdaten ausgeweitet. Die datenschutzrechtliche Aufsicht für länderübergreifende Forschungsvorhaben im Gesundheitswesen wird durch eine/n Landesdatenschutzbeauftragte/n koordiniert.

Das GDNG führt ein Forschungsgeheimnis für die Nutzung von Gesundheitsdaten ein. Das bedeutet, dass Forschende die Gesundheitsdaten nur in Übereinstimmung mit den gesetzlichen Bestimmungen nutzen und weitergeben dürfen und verpflichtet sind, die Daten geheim zu halten. Falls diese Geheimhaltungspflichten verletzt werden, wird es in Zukunft eine Strafnorm geben.

Das GDNG sieht bei der Freigabe von Daten aus der elektronischen Patientenakte (ePA) ein Opt-Out-Verfahren vor. Es ermöglicht eine bessere Nutzung von Behandlungsdaten für Forschungszwecke. Es werden ausschließlich zuverlässig pseudonymisierte Daten automatisiert übermittelt. Eine digitale Verwaltung der Widersprüche wird eingerichtet, damit Patienten entscheiden können, ob ihre Daten für die Forschung oder andere Zwecke freigegeben werden sollen. Die Versicherten können ihren Widerspruch auch bei den Ombudsstellen der Krankenkassen erklären, falls sie die ePA nicht nutzen oder ihren Widerspruch nicht digital erklären möchten.

III. Digital-Gesetz

Am 26. März 2024 ist das Digital-Gesetz in Kraft getreten.

Mit diesem Gesetz bezweckt der Gesetzgeber die Vereinfachung des Behandlungsalltags für Ärzte und Patienten durch digitale Lösungen. Ab Anfang des Jahres 2025 wird die elektronische Patientenakte (ePA) für alle gesetzlich Versicherten eingerichtet. Wer die ePA nicht nutzen möchte, kann dem widersprechen (Opt-Out). Private Krankenversicherungen können ihren Versicherten ebenfalls eine ePA auf Widerspruchsbasis anbieten. Die ePA ermöglicht den Versicherten eine vollständige digitale Medikationsübersicht, welche größtenteils automatisch erstellt wird. Durch enge Verknüpfung mit dem weiterentwickelten E-Rezept können somit unerwünschte Wechselwirkungen zwischen Medikamenten besser vermieden und Ärzte im Behandlungsprozess unterstützt werden. Die ePA-App soll als Zugangsweg zum E-Rezept fungieren, das weiterhin als verbindlicher Standard in der Arzneimittelversorgung etabliert werden soll.

Zudem sieht das DigiG vor, dass Digitale Gesundheitsanwendungen (DiGA) tiefer in die Versorgungsprozesse integriert werden und ihr Einsatz transparent gemacht wird. Durch die Erweiterung der DiGA auf digitale Medizinprodukte der Risikoklasse IIb können sie auch für komplexe Behandlungsprozesse wie das Telemonitoring genutzt werden.

Um die Telemedizin zu einem festen Bestandteil der Gesundheitsversorgung zu machen, werden die Mengenbegrenzungen aufgehoben. Mit assistierter Telemedizin wird auch ein niedrigschwelliger Zugang zur Versorgung angeboten. Die Erbringung telemedizinischer Leistungen durch Einrichtungen wie Hochschulambulanzen oder Psychiatrische Institutsambulanzen sowie psychotherapeutische Sprechstunden wird ermöglicht.

Ein Digitalbeirat, in dem Vertreter des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sowie des Bundesamts für Sicherheit in der Informationstechnik (BSI) vertreten sind und der in Zukunft unter Berücksichtigung ethischer und medizinischer Perspektiven besetzt werden soll, wird bei der Gematik GmbH eingerichtet. Der Digitalbeirat wird die Gematik GmbH in allen Angelegenheiten bezüglich Datenschutz, Datensicherheit, Datennutzung und Anwenderfreundlichkeit beraten.

IV. Europäischer Gesundheitsdatenraum (EHDS)

Der europäische Raum für Gesundheitsdaten (EHDS) ist einer der zentralen Bestandteile der europäischen Gesundheitsunion und stellt den ersten gemeinsamen EU-Datenraum in einem spezifischen Bereich dar, der aus der EU-Datenstrategie hervorgeht.

Der EHDS baut auf den Regelungen der DSGVO, dem Data Governace Act, dem Data Act und der NIS-2-Richtlinie auf. Als horizontale Rahmenregelungen enthalten diese Rechtsakte und Vorschläge Vorschriften (einschließlich Sicherheitsmaßnahmen), die auch für den Gesundheitssektor gelten. Der europäische Raum für Gesundheitsdaten wird jedoch zur Berücksichtigung der Sensibilität von Gesundheitsdaten zusätzliche, sektorspezifische Vorschriften enthalten.

1. Was regelt die Verordnung?

Durch die EHDS-VO soll EU-weit ein Rechtsanspruch auf schnellen und einfachen Zugang zu ihren eigenen elektronischen Gesundheitsdaten für Patientinnen und Patienten ermöglicht werden. Darüber hinaus sollen Angehörige der Gesundheitsberufe umfangreichen Zugriff auf Daten erhalten, die für die optimale Behandlung von Patientinnen und Patienten notwendig sind (z. B. Röntgenbilder, Impfungen usw.) – dies wird als Primärnutzung bezeichnet.

Im EHDS werden auch Bestimmungen für die Sekundärnutzung von Gesundheitsdaten festgelegt. Die EHDS-Verordnung regelt die Voraussetzungen für eine datenschutzkonforme Nutzung von Gesundheitsdaten für Patienten- und Produktsicherheit, Forschung, Innovation und Politikgestaltung. Zukünftig sollen Forscher, Innovatoren und öffentliche Institutionen einen Antrag auf Verwendung von de-identifizierten individuellen Gesundheitsdaten stellen können, indem sie einheitliche europaweite Verfahren nutzen, um diese für spezifisch gesetzlich festgelegte Zwecke zu verwenden.

Die elektronische Patientenakte (ePA) ist als zentraler Zugangspunkt für Patientinnen und Patienten sowie Leistungserbringer auch im Rahmen des EDHS relevant. Mitgliedsstaaten haben die Möglichkeit, spezifische Widerspruchsrechte in Bezug auf die Primärnutzung von Gesundheitsdaten zu schaffen, wodurch die im DigiG vorgesehenen Opt-out-Möglichkeiten erhalten bleiben können. Die Entscheidung über die Nutzung und Weitergabe von Daten im Rahmen der Versorgung wird unter den Vorgaben der EHDS-Verordnung weiterhin von den Patientinnen und Patienten getroffen.

Für die Sekundärnutzung sieht der EHDS ein verpflichtendes Widerspruchsrecht vor, damit Bürgerinnen und Bürgern die Möglichkeit haben, der Weitergabe ihrer personenbezogenen Gesundheitsdaten zu Forschungszwecken oder für andere Zwecke zu widersprechen. Unter bestimmten Bedingungen können Mitgliedsstaaten Ausnahmen von diesem Opt-Out machen. Das Recht auf Widerspruch gegen die Sekundärnutzung von Gesundheitsdaten ist bereits im GDNG für Daten aus der ePA festgelegt. Über die ePA können Gesundheitsdaten datenschutzkonform für die Sekundärnutzung bereitgestellt werden, wenn die Versicherten nicht vollständig oder für bestimmte Zwecke dagegen widersprechen.

2. Wie geht es weiter?

Nach dem Beschluss des EU-Parlaments am 14.03.2024 wird der Text derzeit noch redaktionell bereinigt, sprachjuristisch geprüft und übersetzt. Der finalisierte Text wird voraussichtlich im Herbst 2024 dem neuen Europäischen Parlament zur erneuten Abstimmung vorgelegt, bevor er dann dem Rat zur förmlichen Annahme übermittelt wird. Die EHDS-VO wird zwanzig Tage nach ihrer Veröffentlichung im Amtsblatt der EU in Kraft treten. Dies wird voraussichtlich im Herbst/Winter 2024 sein.

Anwendung finden die Vorschriften der EHDS-VO teilweise nach zwei Jahren, teilweise nach vier, sechs oder zehn Jahren nach Inkrafttreten.

Die Bundesregierung wird nun den rechtlichen Anpassungsbedarf für Deutschland ermitteln, damit Patientinnen und Patienten im Gesundheits- und Forschungsstandort Deutschland frühzeitig von einem gemeinsamen europäischen Gesundheitsdatenraum profitieren können.

V. Handlungsempfehlung

Die umfassenden Neuerungen des GDNG können für viele Unternehmen und Institutionen aus dem Gesundheits- und Forschungssektor relevant sein und bieten große Chancen für eine effiziente Nutzung von Gesundheitsdaten, was gesellschaftliche und wirtschaftliche Vorteile bringt. Deshalb sollten Unternehmen und Institutionen aus diesem Bereich sorgfältig prüfen, ob und in welchem Rahmen sie berechtigt sind, bestimmte Gesundheitsdaten zu erhalten und zu verarbeiten.

Neue Regeln für Online-Plattformen: Der Digital Services Act und Digitale-Dienste-Gesetz

Mit dem Digital Services Act (DSA) schafft die EU einen einheitlichen Rechtsrahmen für Online-Angebote. Der DSA ist seit dem 16. November 2022 in Kraft und gilt seit dem 17. Februar 2024 für alle betroffenen Unternehmen. Er adressiert Risiken und Herausforderungen, die aus der digitalen Transformation und dem damit verbundenen Entstehen neuer digitaler Geschäftsmodelle hervorgegangen sind.

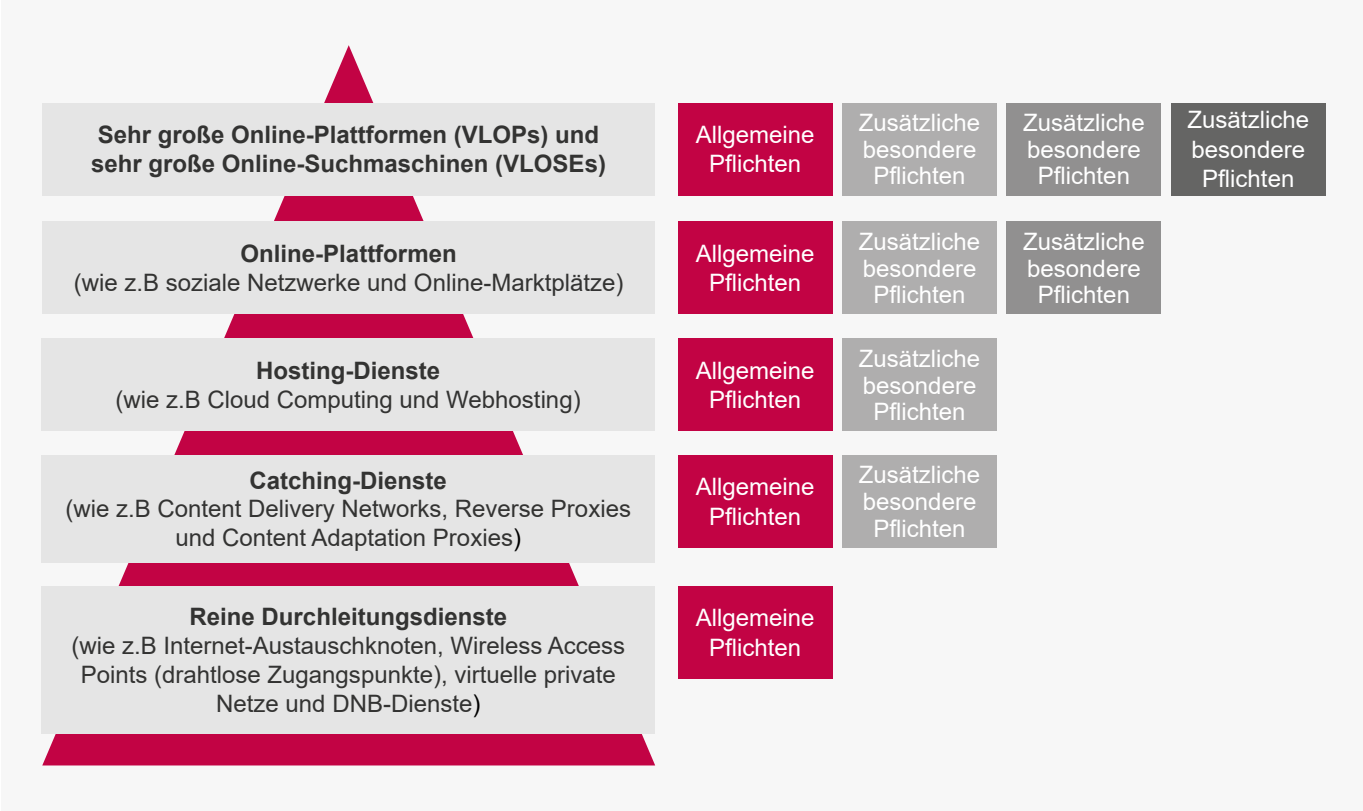
I. Für welche Anbieter gilt der DSA?

Der DSA richtet sich an B2B- und B2C-Anbieter von digitalen Vermittlungsdiensten (Intermediäre), die Nutzern in der EU Zugang zu Waren, Dienstleistungen und Inhalten verschaffen. Dazu gehören Anbieter von folgenden Diensten:

- Reine Durchleitungsdienste, wie z.B. Internet-Austauschknoten, Wireless Access Points (drahtlose Zugangspunkte), virtuelle private Netze und DNS-Dienste.
- Caching-Dienste, wie z.B. Content Delivery Networks, Reverse Proxies und Content Adaptation Proxies.
- Hosting-Dienste, wie z.B. Cloud Computing und Webhosting.
- Online-Plattformen, wie z.B. soziale Netzwerke und Online-Marktplätze.
- Online-Suchmaschinen.

Die Terminologie und der Anwendungsbereich der Klassifizierungen des DSA weisen keine randscharfen Konturen auf, sodass ein digitaler Dienst auch mehrere Dienste oder Funktionalitäten kombinieren kann, und damit den unterschiedlichen Klassifizierungen und unterschiedlichen Regeln des DSA unterliegen kann. Hierdurch verbleibt Interpretationsspielraum und es können Unsicherheiten entstehen.

Kleine Unternehmen und Kleinstunternehmen (mit weniger als 50 Beschäftigten und einem Jahresumsatz von weniger als 10 Millionen Euro) sind von der Einhaltung einiger Pflichten des DSA befreit.



II. Welche Pflichten treffen die Anbieter?

Der DSA folgt in erster Linie einem abgestuften Regulierungssystem, das bedeutet, dass die Pflichten der einzelnen Online-Unternehmen je nach Rolle, Größe und Auswirkung im Online-Umfeld variieren.

Auf Grundlage dessen gelten für alle Vermittlungsdienste allgemeine Pflichten, die dann je nach Art und Klassifizierung des jeweiligen Vermittlungsdienstes durch weitere spezielle Pflichten ergänzt werden. Sehr große Online Plattformen (engl.: Very large online platforms - VLOPs) und sehr große Online Suchmaschinen (engl.: Very large online search engines – VLOSEs) sind solche mit mehr als 45 Millionen durchschnittlich monatlich aktiven Nutzern in der EU.

Unter den umfangreichen Vorschriften des DSA sind die folgenden besonders erwähnenswert:

a) Umgang mit rechtswidrigen Inhalten

Ein zentraler Aspekt des DSA ist, dass Diensteanbieter rechtswidrige Inhalte schnell und effizient entfernen müssen. Anbieter von Hosting-Diensten müssen vordefinierte Melde- und Abhilfeverfahren für die Meldung mutmaßlich rechtswidriger Inhalte bereitstellen und solchen Meldungen nachgehen und die erforderlichen Maßnahmen ergreifen. Ob ein Inhalt als rechtswidrig einzustufen ist oder nicht, wird nicht durch den DSA selbst, sondern durch das geltende Recht des betroffenen EU-Mitgliedstaates bestimmt. Die Haftungsprivilegien der E-Commerce-Richtlinie wurden in den DSA übernommen. Daher bleibt das ursprünglich im Rahmen der E-Commerce-Richtlinie eingeführte und entwickelte Konzept des Melde- und Abhilfeverfahrens (sog. „notice and take-down“) weitgehend erhalten. Diensteanbieter müssen die Rechtmäßigkeit der Inhalte nicht proaktiv überprüfen.

b) Zentrale Kontaktstelle

Anbieter von Vermittlungsdiensten müssen eine zentrale Kontaktstelle benennen, die als direkter Ansprechpartner für Behörden der EU-Mitgliedstaaten, die Europäische Kommission und Nutzer fungiert.

c) Transparenzberichtspflichten

Je nach Klassifizierung des betroffenen Diensteanbieters gibt es verschiedene abgestufte Transparenzpflichten, die regelmäßige Berichte über die Moderation von Inhalten und andere Maßnahmen vorsehen.

d) Internes Beschwerdemanagementsystem

Anbieter von Online-Plattformen müssen ein internes Beschwerdemanagementsystem einrichten, das Nutzern z.B. ermöglicht, die angeblich unberechtigte Entfernung von Inhalten, die Sperrung von Nutzerkonten und andere Maßnahmen mit nachteiligen Auswirkungen zu beanstanden. Die Entscheidung über eine Beschwerde muss eine Begründung des Anbieters der Online-Plattform enthalten und darf nicht rein automatisiert erfolgen.

e) Online-Werbung und Transparenz

Neben der allgemeinen Anforderung, Online-Werbung eindeutig als solche zu kennzeichnen, treffen Anbieter von Online-Plattformen weitere Transparenzpflichten im Zusammenhang mit Online-Werbung.

f) Teilweises Verbot von auf Profiling basierender Online-Werbung

Anbietern von Online-Plattformen ist es untersagt, auf Profiling basierte Online-Werbung zu betreiben, soweit dies auf Grundlage von sensiblen Daten (z.B. Gesundheitsdaten) erfolgt oder an Minderjährige gerichtet ist.

g) Ansprüche und Rechtsbehelfe von Nutzern

Nutzer haben das Recht, bei Verstößen gegen den DSA Ansprüche gegen die Diensteanbieter geltend zu machen, einschließlich Schadensersatzansprüchen nach dem Recht der EU und der EU-Mitgliedstaaten.

h) Sehr große Online-Plattformen und sehr große Online-Suchmaschinen (VLOPs und VLOSEs)

Der DSA schreibt vor, dass Anbieter von VLOPs und VLOSEs regelmäßig eine Bewertung ihrer systemischen Risiken vornehmen müssen. Auf Grundlage der daraus hervorgehenden Ergebnisse müssen Maßnahmen zur Risikominderung ergriffen werden. Darüber hinaus müssen Anbieter von VLOPs und VLOSEs regelmäßig unabhängige Compliance-Prüfungen durchführen und eine qualifizierte Compliance-Abteilung einrichten, die von den operativen Funktionen unabhängig ist.

2. Aufsicht und Durchsetzung

Jeder EU-Mitgliedstaat muss bis zum 17. Februar 2024 einen Koordinator für digitale Dienste (DSC) als zuständige Behörde zur Überwachung und Durchsetzung der Einhaltung des DSA ernennen (in Deutschland die Bundesnetzagentur). Die zuständige Behörde für VLOPs und VLOSEs ist in erster Linie die Europäische Kommission selbst.

Die Behörden und die Europäische Kommission (soweit zuständig) haben weitreichende Rechte auf Zugang, Einholung von Informationen, Inspektion, Anordnung und Sanktionierung von Diensteanbietern.

Verstöße gegen den DSA können mit Geldbußen von bis zu 6 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden. Bei Verstößen gegen eine Informationspflicht des DSA ist die Geldbuße auf maximal 1 % des Vorjahreseinkommens oder des weltweiten Vorjahresumsatzes begrenzt.

III. Nationale Umsetzung des DSA durch das Digitale Dienste Gesetz

Das Digitale-Dienste-Gesetz (DDG) ist am 14. Mai 2024 in Kraft getreten und schafft die notwendigen nationalen Voraussetzungen für die effektive Umsetzung des DSA in Deutschland. Dies beinhaltet Anpassungen der Zuständigkeiten, die Ernennung der Bundesnetzagentur als Digital Services Coordinator (DSC) und Informationspflichten.

Mit Inkrafttreten des DDG verliert das Telemediengesetz (TMG) seine Wirkung und geht im DSA und DDG auf. Zudem wird das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) in Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) umbenannt. Die bisherigen Regelungen des TMG zur Verantwortlichkeit entfallen weitgehend und sind nunmehr ohne wesentliche inhaltliche Änderungen vom DSA erfasst. Weitere Änderungen betreffen unter anderem das Netzwerkdurchsetzungsgesetz, das Jugendschutzgesetz und das Urheberrechts-Diensteanbieter-Gesetz.

Das DDG ergänzt den DSA um weitere Bußgeldvorschriften für verschiedene Ordnungswidrigkeiten. Diese betreffen hauptsächlich Verstöße gegen gesetzlich vorgeschriebene Informations-, Auskunfts-, Prüfungs- und Zugangsverpflichtungen nach dem DDG und dem DSA sowie gegen die P2B-VO. Die Geldstrafen variieren je nach Schwere des Verstoßes, wobei einige bis zu 300.000 Euro reichen können. In schwereren Fällen, insbesondere bei juristischen Personen oder Personenvereinigungen mit einem hohen Jahresumsatz, können die Strafen sogar bis zu 6 Prozent des Jahresumsatzes betragen.

IV. Unsere Checkliste für die erforderlichen Anpassungen nach dem DDG

Die Gesetzesänderungen betreffen auf nationaler Ebene alle Unternehmen zur Umbenennung von „Telemedien“ zu „Digitale Dienste“. Es entstehen somit vor allem redaktionelle Änderungserfordernisse:

- Anpassungsbedarf auf der Webseite
  - Änderung der Begrifflichkeit „Telemedien“ zu „Digitale Dienste“, sowie die Überprüfung, ob weitere Anpassungen notwendig sind.
  - Innerhalb des Impressums ergeben sich die „Allgemeinen Informationspflichten“ aus § 5 DDG (zuvor § 5 TMG). Die „Besonderen Pflichten bei kommerziellen Kommunikationen“ ergibt sich nun aus § 6 DDG (zuvor § 6 TMG).
  - Sofern in der CMP/Cookie-Banner Bezug auf § 25 TTDSG genommen wurde, ist dieser Bezug auf § 25 TDDDG abzuändern. Auch hier ist der Begriff „Telemedien“ durch „Digitale Dienste“ zu ersetzen.
  - Die Datenschutzinformationen auf der Webseite sind ebenfalls von TMG zu DDG und von TTDSG zu TDDDG abzuändern.
  - Sofern andere bzw. eigene Erklärungen auf der Webseite vorgenommen wurden, sind diese auf die Formulierungen „Telemedien“ sowie die alten Gesetzesbezeichnungen zu kontrollieren.
- Anpassungsbedarf in den Datenschutzerklärungen gem. Art. 13 und 14 DSGVO
  - Sämtliche Datenschutzerklärungen (z. B. für Kunden, Lieferanten, Bewerberinnen und Bewerber, Mitarbeiterinnen und Mitarbeiter etc.) sind auf Verweise auf das TMG und TTDSG hin zu überprüfen. „Telemedien“ ist durch „Digitale Dienste“ zu ersetzen.
  - Solche Verweise können im Rahmen der Rechtsgrundlage abzuändern sein.
  - Eine Informierung der Betroffenen aufgrund der abgeänderten Datenschutzerklärungen ist nicht erforderlich.
- Anpassungsbedarf bei Verpflichtungserklärungen zum Datenschutz für Mitarbeiterinnen und Mitarbeiter
  - Überprüfung und Anpassung aller datenschutzrechtlichen Verpflichtungserklärungen auf Verweise zum TMG und TTDSG. Hier kommen insbesondere Verweise auf das Fernmeldegeheimnis (zuvor § 3 TTDSG oder § 88 TKG) gem. § 3 TDDDG infrage. Zudem ist die Formulierung „Telemedien“ zu „Digitale Dienste“ abzuändern.
  - Eine Abänderung der bereits unterschriebenen Verpflichtungserklärungen mit Mitarbeitern und Mitarbeiterinnen ist nicht erforderlich.

Update IT-Sicherheitsrecht – Neue europäische Anforderungen im Cybersicherheitsrecht – die NIS-2-Richtlinie, der Digital Operations Act und der Cyber Resilience Act im Überblick

Cybersicherheitsbedrohungen sind oft grenzüberschreitend. Um diesen Bedrohungen zu begegnen, hat die Europäische Kommission beschlossen, eine neue Cybersicherheitsstrategie für die EU zu erarbeiten. Die Strategie soll die Sicherheit wesentlicher Dienstleistungen wie Krankenhäuser, Energienetze und Eisenbahnen, sowie die Sicherheit der ständig wachsenden Anzahl von vernetzten Objekten in Privathaushalten schützen. Diese Strategie ist die Grundlage mehrerer Gesetzgebungsvorhaben auf dem Gebiet der Cybersicherheit, die wir im Folgenden überblicksartig darstellen wollen.

I. Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS-2-Richtlinie) und das NIS-2-UmsuCG

Die NIS-2-Richtlinie sieht rechtliche Maßnahmen vor, um das Gesamtniveau der Cybersicherheit in der EU zu erhöhen. Die Richtlinie trat am 16. Januar 2023 in Kraft. Die Mitgliedstaaten haben bis zum 18. Oktober 2024 Zeit, um die Bestimmungen in nationales Recht umzusetzen. Am 24. Juli 2024 wurde zur Umsetzung der Richtlinie der Regierungsentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS-2-UmsuCG) verabschiedet.

1. Wen betreffen die Regelungen?

Die NIS-2-Richtlinie erweitert den Anwendungsbereich gegenüber ihrem Vorgänger der NIS-1-Richtlinie, indem neue Sektoren auf der Grundlage ihres Digitalisierungsgrads und ihrer Vernetzung und ihrer Bedeutung für Wirtschaft und Gesellschaft hinzugefügt werden. Es gibt eine klare Größenschwellenregel, was bedeutet, dass alle mittleren und großen Unternehmen in ausgewählten Sektoren in den Anwendungsbereich einbezogen werden. Mittlere Unternehmen sind solche die 50-249 Beschäftigte haben oder 10-50 Mio. Euro Jahresumsatz oder mehr als 43 Mio. Euro Jahresbilanz haben. Große Unternehmen sind solche, die mindestens 250 Mitarbeitende oder mindestens 50 Mio. EUR Jahresumsatz haben. Zu den nun betroffenen Unternehmen gehören solche aus den folgenden Sektoren:

- Anhang I regelt die Sektoren besonders wichtiger und wichtiger Einrichtungen: Energie, Verkehr, Bank- und Finanzwesen, Gesundheitswesen, Wasserversorgung, Digitale Infrastruktur, IKT-Dienste, Weltraum;
- Anhang II umfasst weitere Sektoren wichtiger Einrichtungen: Post- und Kurierdienste, Abfallwirtschaft, Chemie, Ernährung, Herstellung von Waren, Digitale Dienste und Forschung.

Zur Kategorisierung sieht die NIS-2-Richtlinie Schwellenwerte vor:

- Wichtige Einrichtungen: Mittlere Unternehmen (mehr als 50 Mitarbeiter oder mehr als 10 Mio. EUR Jahresumsatz oder mehr als 10 Mio. EUR Jahresbilanz)
- Besonders wichtige Einrichtungen: Großunternehmen (mehr als 250 Mitarbeiter oder mehr als 50 Mio. EUR Jahresumsatz und mehr als 43 Mio. EUR Jahresbilanz)
- Betreiber kritischer Anlagen: werden nach ihrer Versorgungsrelevanz bestimmt (anlagenspezifische Schwellenwerte)

Dadurch wird der Anwendungsbereich in Deutschland enorm ausgeweitet. Insgesamt von den Regelungen betroffen werden damit ca. 21.600 Unternehmen sein als wichtige Einrichtungen, ca. 8.250 als besonders wichtige Einrichtungen und ca. 2.000 als Betreiber kritischer Anlagen.

2. Welche Pflichten sehen die NIS-2-Richtlinie und das NIS-2-UmsuCG-E vor?

Um ein dem beschriebenen Risiko angemessenes Schutzniveau herbeiführen zu können sieht die NIS-2-Richtlinie als eine wesentliche Pflicht die Umsetzung von Risikomanagement-Maßnahmen zur Ergreifung geeigneter und verhältnismäßiger technischer, operativer und organisatorischer Maßnahmen nach dem Stand der Technik vor.

Die Richtlinie stärkt und rationalisiert die Sicherheits- und Berichtspflichten für Unternehmen, indem sie einen Risikomanagementansatz vorschreibt, der einen Katalog an mindestens zu ergreifenden Maßnahmen enthält. Dieser Katalog umfasst Maßnahmen zur Risikoanalyse, Bewältigung von Sicherheitsvorfällen, Krisenmanagement, Sicherheit in der Lieferkette und Cybersicherheitsschulungen. Außerdem werden genauere Bestimmungen über das Verfahren für die Meldung von Vorfällen, den Inhalt der Berichte und die Fristen eingeführt.

Um eine wirkliche Rechenschaftspflicht für die Cybersicherheitsmaßnahmen auf organisatorischer Ebene zu gewährleisten, führt die Richtlinie Bestimmungen über die Haftung natürlicher Personen ein, die Führungspositionen in den in den Anwendungsbereich der neuen Richtlinie fallenden Unternehmen innehaben.

Darüber hinaus befasst sich die Richtlinie mit der Sicherheit von Lieferketten und Lieferantenbeziehungen, indem einzelne Unternehmen aufgefordert werden, Cybersicherheitsrisiken in den Lieferketten und Lieferantenbeziehungen anzugehen.

3. Überwachung und Durchsetzung der Regelungen

Um die Durchsetzung wirksam zu gestalten, wird mit der neuen Richtlinie ein kohärenter Rahmen für Sanktionen in der gesamten Union geschaffen. Sie legt daher eine Mindestliste verwaltungsrechtlicher Sanktionen für Verstöße gegen die in der NIS-2-Richtlinie festgelegten Verpflichtungen für das Cybersicherheitsrisikomanagement und die Berichterstattung fest. Diese Sanktionen umfassen verbindliche Anordnungen, beispielsweise zur Umsetzung eines Sicherheitsaudits oder die Sicherheitsmaßnahmen mit den NIS-Anforderungen in Einklang zu bringen, und Verwaltungsbußgelder.

In Bezug auf Geldbußen unterscheidet die NIS-2-Richtlinie zwischen wesentlichen und wichtigen Stellen. In Bezug auf wesentliche Einrichtungen sind die Mitgliedstaaten verpflichtet, eine bestimmte Höhe von Geldbußen vorzusehen, insbesondere einen Höchstbetrag von mindestens 10.000.000 EUR oder 2 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Wert höher ist. In Bezug auf wichtige Einrichtungen schreibt NIS-2 vor, dass die Mitgliedstaaten eine Geldbuße von höchstens 7.000.000 EUR oder mindestens 1,4 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres vorsehen, je nachdem, welcher Wert höher ist.

II. Digital Operational Resilience Act (DORA)

Mit dem Digital Operational Resilience Act (DORA) schafft die Europäische Kommission einen einheitlichen Rahmen für ein effektives und umfassendes Management von Cybersicherheits- und IKT(Informations- und Kommunikationstechnologien)-Risiken auf den Finanzmärkten. Die Hauptziele der Verordnung sind die Stärkung der operationalen Widerstandsfähigkeit von Finanzunternehmen gegenüber Störungen, Cyberangriffen und anderen Risiken zu erhöhen, die Sicherstellung der Geschäftskontinuität durch Festlegung von Maßnahmen, um die Kontinuität der Geschäftsabläufe sicherzustellen und Ausfallzeiten zu minimieren, sowie den Schutz von Verbrauchern und Investoren durch Stärkung des Vertrauens in das Finanzsystem, indem Risiken für Verbraucher und Investoren reduziert werden.

1. Anwendungsbereich

Die Regelungen des DORA gelten für alle Finanzinstitute in der EU. Das umfasst traditionelle Finanzunternehmen wie Banken, Investmentfirmen und Kreditinstitute sowie nicht-traditionelle Entitäten wie Krypto-Asset-Serviceanbieter und Crowdfunding-Plattformen. Die Vorschrift listet 21 Tätigkeitsbereiche im Finanzsektor auf. Zudem gelten die Regelungen mittelbar für Anbieter von IKT-Drittdienstleistungen.

2. Regelungsinhalte

Der DORA regelt einen ganzheitlichen Rahmen für ein effektives Risikomanagement, das die betroffenen Finanzunternehmen umzusetzen haben. Hierfür sieht DORA das Aufsetzen eines internen Governance- und Kontrollrahmens zur Gewährleistung des IKT-Risikomanagements vor. Außerdem sind die Einrichtung und Pflege belastbarer IKT-Systeme und -Werkzeuge umzusetzen, die die Auswirkungen von IKT-Risiken minimieren, sowie die kontinuierliche Überwachung aller Quellen von IKT-Risiken, um Schutz- und Präventionsmaßnahmen einzurichten. Dazu kommt die Einführung spezieller und umfassender Business-Continuity-Richtlinien sowie Notfall- und Wiederherstellungspläne, einschließlich jährlicher Tests der Pläne, die alle unterstützenden Funktionen abdecken und die Einrichtung von Mechanismen, um sowohl aus externen Ereignissen als auch aus eigenen IKT-Vorfällen zu lernen und sich weiterzuentwickeln. Die Verantwortung der Umsetzung des IKT-Risikomanagementrahmens liegt bei dem Leitungsorgan des Finanzunternehmens.

Des Weiteren trifft die Finanzunternehmen die Pflicht zur Klassifizierung und Behandlung von IKT-bezogenen Vorfällen. Sie müssen ein IKT-Vorfallmanagementprozess zur Aufzeichnung, Überwachung und Behebung von Vorfällen und eine Meldepflicht bei schwerwiegenden Vorfällen etablieren. Daneben sind Tests der operationalen Resilienz durch Einführung eines umfassenden Programms für digitale operationale Resilienz-Tests entsprechend eines risikobasierten Ansatzes durchzuführen.

Eine weitere wesentliche Pflicht betrifft das IKT-Drittparteienrisikomanagement. Der DORA sieht die Überwachung von IKT-Drittdienstleistern während des gesamten Lebenszyklus innerhalb des IKT-Risikorahmens vor, insbesondere durch detaillierte Vorgaben an vertragliche Vereinbarungen, sowie behördliche Überwachung kritischer IKT-Drittdienstleister.

3. Überwachung und Durchsetzung

Die Überwachung der Einhaltung des DORA erfolgt durch verschiedene Mechanismen. Die Finanzinstitute unterliegen der Aufsicht durch nationale und europäische Aufsichtsbehörden wie der Europäischen Zentralbank (EZB) oder der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in Deutschland. Die Aufsichtsbehörden führen Prüfungen und Inspektionen durch, um die Einhaltung von DORA zu überwachen. Sie können unangekündigte Besuche vor Ort durchführen und Dokumente, Prozesse und Systeme prüfen. Daneben müssen die Finanzunternehmen regelmäßig Selbstbewertungen durchführen, um ihre eigene operationale Resilienz zu überprüfen und sicherzustellen, dass sie den Anforderungen von DORA entsprechen. Zudem müssen sie Vorfälle, die ihre operationale Resilienz beeinträchtigen könnten, an die Aufsichtsbehörden melden. Diese Meldungen werden analysiert, um mögliche Verstöße zu identifizieren.

Der DORA legt für Finanzunternehmen, die gegen die dargestellten Vorgaben verstoßen, die folgenden Sanktionen fest. Zunächst können die Finanzunternehmen mit Geldbußen von bis zu 10 Millionen Euro oder 5 % ihres jährlichen Gesamtumsatzes belegt werden, je nach Schwere des Verstoßes. Daneben ermöglicht der DORA den Aufsichtsbehörden, öffentliche Rügen auszusprechen, um auf Verstöße hinzuweisen, sowie bei schwerwiegenden Verstößen vorübergehende oder dauerhafte Untersagungen für bestimmte Aktivitäten oder Dienstleistungen. Für kritische IKT-Drittdienstleister sieht der DORA Geldbußen bis 1% des durchschnittlichen weltweiten Tagesumsatzes vor.

4. Ausblick

Für die Implementierung des DORA, der seit dem 17. Januar 2023 in Kraft ist, gilt eine Umsetzungsfrist von zwei Jahren. Im Laufe des Jahres 2024 sind zur Umsetzung der Vorgaben die Veröffentlichungen Technische Regulierungsstandards (RTS) und Technische Durchführungsstandards (IST) geplant, die die Aufsichtsbehörden erarbeiten, um die Inhalte des DORA zu konkretisieren.

III. Cyber Resilience Act (CRA)

Die Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyber Resilience Act – CRA) wurde ebenfalls in der EU-Cybersicherheitsstrategie 2020 angekündigt und ergänzt die vorgenannten Rechtsvorschriften.

Die Regelungen des CRA stellen harmonisierte Vorschriften für das Inverkehrbringen von Produkten oder Software mit einer digitalen Komponente dar. Sie gilt für alle Produkte, die direkt oder indirekt mit einem anderen Gerät oder Netzwerk verbunden sind, mit Ausnahme bestimmter Ausschlüsse wie Open-Source-Software oder Dienste, die bereits unter bestehende Vorschriften fallen, wie beispielsweise Medizinprodukte oder Autos. Die Vorschriften sehen einen Rahmen von Cybersicherheitsanforderungen für die Planung, Gestaltung, Entwicklung und Wartung solcher Produkte mit Verpflichtungen, die in jeder Phase der Wertschöpfungskette zu erfüllen sind, vor. Diese Sorgfaltspflicht besteht für die Unternehmen für den gesamten Lebenszyklus solcher Produkte.

Mit Inkrafttreten der Verordnung müssen Software und Produkte, die mit dem Internet verbunden sind, die CE-Kennzeichnung tragen, um anzuzeigen, dass sie den neuen Normen entsprechen.

Die Verordnung ist seit dem 12. März 2024 in Kraft getreten. Die Hersteller müssen die Vorschriften 36 Monate nach ihrem Inkrafttreten anwenden. Die Kommission wird das Gesetz dann regelmäßig überprüfen und über dessen Funktionsweise berichten.

IV. Abschließende Handlungsempfehlung

Obwohl sowohl die NIS-2-Richtlinie als auch der DORA und CRA derzeit noch nicht anwendbar sind, ist es für Unternehmen wichtig, sich zeitnah mit den Vorgaben auseinander zu setzen, um frühzeitig zu erkennen, ob und inwiefern sie von den Anwendungsbereich der Regelungen betroffen sein werden. Im Anschluss ist eine Gap-Analyse durchzuführen, die eine abgleichende Prüfung der umzusetzenden Maßnahmen mit den bereits ergriffenen Maßnahmen umfasst. Denn die Planung und Umsetzung der identifizierten Gaps und den entsprechenden Maßnahmen kann mit Herausforderungen verbunden sein. Zur Umsetzung können die Umsetzungshilfen der Aufsichtsbehörde (technische Regulierungs- (RTS) und Implementierungsstandards (ITS) genutzt werden. Jedenfalls müssen die Vorgaben bis Oktober 2024 (NIS-2-Richtlinie) bzw. bis Januar 2025 (DORA) umgesetzt sein.

Update zur EuGH-Rechtsprechung zum Schadensersatz nach Art. 82 DSGVO

Die DSGVO soll datenverarbeitende Verantwortliche dazu anhalten, die personenbezogenen Daten von Betroffenen angemessen zu schützen. Um die Einhaltung der datenschutzrechtlichen Vorschriften sicherzustellen, wurden mit der DSGVO wirksame Betroffenenrechte sowie abschreckende Sanktionsmechanismen, wie die Bußgeldbefugnis der Aufsichtsbehörden, implementiert. Neben den Rechten etwa auf Auskunft, Berichtigung oder Löschung kann Betroffenen ein Anspruch auf Schadensersatz nach Art. 82 DSGVO zustehen. Die Anforderungen an einen solchen Anspruch sind streitig.

Gemäß Art. 82 Abs. 1 DSGVO hat insofern

„*Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, […] Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.*“

In Anbetracht des offen gehaltenen Wortlauts kamen schnell Fragen zum Tatbestand auf. Daher war es seit Inkrafttreten der DSGVO Aufgabe der Rechtsprechung, die Kriterien und Grenzen des DSGVO-Schadensersatzanspruchs sinnvoll zu definieren und angemessen auszulegen. Nachfolgend soll aufgezeigt werden, welche Tatbestandsvoraussetzungen die Rechtsprechung für den Schadensersatzanspruch nach DSGVO aufgestellt hat.

I. Anspruchsvoraussetzungen des Art. 82 DSGVO

Zu den Anspruchsvoraussetzungen hat sich der Europäische Gerichtshof (EuGH) bereits in einigen Entscheidungen, unter anderem zuletzt mit Urteilen vom 11.04.2024, vom 25.01.2024 und vom 14.12.2023 geäußert und beispielsweise der Annahme einer Erheblichkeitsschwelle, wie sie einige Gerichte forderten, eine Absage erteilt. Darüber hinaus hat der EuGH entschieden, dass nicht jeder Verstoß gegen eine Vorschrift der DSGVO automatisch einen nach Art. 82 DSGVO ersatzfähigen Schaden darstellt. Vielmehr müsse ein auf dem DSGVO-Verstoß kausal beruhender materieller oder immaterieller Schaden nachgewiesen und festgestellt werden.

1. Verstoß gegen die DSGVO Vorschriften

Zunächst setzt ein DSGVO-Schadenersatzanspruch gemäß Art. 82 Abs. 1 DSGVO den Verstoß gegen eine DSGVO-Vorschrift voraus. Der Verantwortliche, gegen den der Ersatzanspruch gerichtet wird, muss sich also in irgendeiner Weise datenschutzwidrig verhalten haben. Art. 82 Abs. 1 DSGVO schränkt den Kreis ersatzfähiger Datenschutzverstöße nicht ein, sodass grundsätzliche jede Zuwiderhandlung gegen eine DSGVO-Norm ausreichend sein kann. In Betracht kommen vor allem:

- die Verarbeitung von personenbezogenen Daten ohne entsprechende oder ohne hinreichende Rechtsgrundlage im Sinne von Art. 6 DSGVO (auch die Berufung auf eine falsche, nicht einschlägige Rechtsgrundlage),
- der Verstoß gegen Betroffenenrechte nach Art. 15 ff. DSGVO, insbesondere die verspätete oder unzureichende Bearbeitung und Umsetzung von Betroffenenbegehren,
- der Verstoß gegen Datensicherheitsvorgaben nach Art. 32 ff. DSGVO (insbesondere die fehlende oder unzureichende Einrichtung technischer und organisatorischer Maßnahmen),
- der Verstoß gegen die Voraussetzungen einer Auftragsverarbeitung nach Art. 28 DSGVO,
- der Verstoß gegen die Vorschriften einer gemeinsamen Verantwortlichkeit gemäß Art. 26 DSGVO (insbesondere das Fehlen eines hinreichenden „Vertrages über die gemeinsame Verantwortlichkeit“).

2. Verschulden

Zweitens ist erforderlich, dass der Verantwortliche oder der Auftragsverarbeiter, gegen den der Ersatzanspruch gerichtet wird, den Datenschutzverstoß auch verschuldet hat. Ein solches Verschulden liegt dann vor, wenn der DSGVO-Verstoß durch ein Verhalten des Anspruchsgegners vorsätzlich oder fahrlässig verursacht worden ist.

Das Verschulden nach Art. 82 Abs. 3 DSGVO wird hierbei grundsätzlich vermutet. Der Verantwortliche oder Auftragsbearbeiter muss für seine haftungsrechtliche Entlastung also aktiv nachweisen, für das schadensauslösende Ereignis nicht verantwortlich gewesen zu sein. Eine originäre Nachweispflicht des Betroffenen für ein Verschulden des Anspruchsgegners ist gerade nicht vorgesehen.

Eine Entlastung des Verantwortlichen ist vor allem im Bereich von Datenlecks möglich, die sich durch Hacking- oder Phishing-Angriffe auch dann ereignen können, wenn alles Zumutbare getan wurde, um solchen Angriffen vorzubeugen. Ereignet sich daher eine Datenpanne, wenn diese von Dritten durch rechtswidrige Überwindung hinreichend etablierter technischer und organisatorischer Maßnahmen verursacht wurde, kann eine Exkulpation des Verantwortlichen mangels Verschuldens gelingen. Unter Bezugnahme auf ein kurz zuvor ergangenes Urteil des EuGH vom 14.12.2023 (Az: C-340/21), verwies der Gerichtshof darauf, dass die genannten Normen keine absolute Sicherheit gegen Verstöße erforderten, sondern angemessene Maßnahmen, um die Sicherheit zu gewährleisten. Erst wenn ein Organisationsversagen vorliege und die irrtümliche Weitergabe von Dokumenten deren Folge sei, könne ein Verstoß gegen Art. 24 und Art. 32 DSGVO bejaht werden (EuGH, Urt. v. 25.01.2024 , Az: C-687/21).

In der Entscheidung vom 11.04.2024 hat der EuGH, wie bereits in vorherigen Entscheidungen, erneut bestätigt, dass eine Haftungsexkulpation des Verantwortlichen nach Art. 82 Abs. 3 DSGVO nur gelingt, wenn dieser nachweist, in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich zu sein. Der einfache Verweis auf das weisungswidrige Verhalten eines Mitarbeiters nach Art. 29 DSGVO erfüllt dieses Kriterium nicht, denn nach Art. 32 Abs. 4 DSGVO muss der Verantwortliche sicherstellen und kontrollieren, dass der Unterstellte weisungsgetreu handelt. Sonst würde die praktische Wirksamkeit des Anspruchs nach Art. 82 Abs. 1 DSGVO von unternehmerischer Seite leicht ausgehebelt werden können (EuGH, Urt. v. 11.04.2024, Az.: C-741/21).

Für deutsche Unternehmen ergibt sich aus diesen Ausführungen nichts Neues, denn grundsätzlich gilt auch nach deutschem Recht im Hinblick auf eine mögliche Haftungsexkulpation wegen Verschuldens einer unterstellten Person immer, dass der einfache Verweis auf weisungswidriges Handeln nicht ausreicht. Stattdessen muss stets bewiesen werden, dass die stetigen Aufsichts- und Kontrollpflichten als Weisungsgeber nicht missachtet worden sind.

3. Schaden

Elementarer Kern eines begründeten Schadensersatzanspruches nach Art. 82 DSGVO ist nach ständiger Rechtsprechung der Eintritt eines konkreten Schadens. Eine zentrale Einschränkung für den Ersatzanspruch besteht nach weitgehend einhelliger Auffassung der Gerichte dahingehend, dass ein Schadenseintritt durch die Verletzung vom Anspruchsteller, also dem Betroffenen, aktiv dargetan werden muss und dabei von einem bloßen Datenschutzverstoß nicht automatisch auf einen Schadenseintritt geschlossen werden kann. Der EuGH argumentiert dafür mit dem Wortlaut des Art. 81 Abs.1 DSGVO,

der gerade beide Tatbestandsmerkmale, die Verletzung und den Schaden voraussetzt (vgl. zuletzt EuGH, Urt. v. 11.04.2024, Az.: C-741/21).

Daraus folgt, dass der Betroffene für einen Ersatzanspruch substantiiert darlegen muss, dass es durch einen Datenschutzverstoß des Verantwortlichen auch zu einem Schaden gekommen ist. Der Schadensbegriff ist nach Erwägungsgrund 146 der DSGVO dabei möglichst weit auszulegen.

Je nachdem, welche Art von Schaden behauptet wird, ergeben sich hierfür nach der Rechtsprechung unterschiedliche Voraussetzungen.

a) Materielle Schäden

Ersatzfähig sind nach Art. 82 Abs. 1 DSGVO zunächst materielle Schäden, die finanziell als Verlustpositionen konkret beziffert werden können. Die gängigste Fallkonstellation ist hier diejenige von Identitätsdiebstählen oder -betrügen, denen ein Betroffener aufgrund eines Datenschutzverstoßes zum Opfer fallen kann. Schadenspositionen können hierbei vor allem Vermögensverluste durch Nutzung fremder Zahlungsdaten sein. Materielle Schäden lassen sich in der Regel gut darlegen und beziffern.

b) Immaterielle Schäden

Schwieriger ist die Durchsetzung eines DSGVO-Schadensersatzes auf Basis von immateriellen Schäden, deren Niederschlag nicht in einer konkreten Vermögensminderung, sondern in der Beeinträchtigung gesetzlicher Rechte oder Rechtspositionen liegt.

Insbesondere die Auslegung des Begriffs des immateriellen Schadens war bereits Gegenstand vieler Entscheidungen.

Im Sinne einer engen Auslegung des Schadensbegriffes nahmen Gerichte teilweise einen immateriellen Schaden erst dann an, wenn eine Verletzung des Datenschutzrechts im Einzelfall zu einer konkreten, nicht bloß unbedeutenden oder empfundenen Verletzung von Persönlichkeitsrechten geführt hat. Zahlreiche deutsche Gerichte haben einen immateriellen Schaden wegen bloßen Bagatellverstößen, die die Belange des Betroffenen nicht ernsthaft beeinträchtigt und über das Niveau einer bloß individuell empfundenen Unannehmlichkeit nicht hinausgeht, abgelehnt. Nach Ansicht der Gerichte sei nachzuweisen, dass dem Betroffenen ein spürbarer Nachteil entstanden ist, der aus einer objektiv nachvollziehbaren, mit gewissem Gewicht erfolgten Beeinträchtigung von persönlichkeitsbezogenen Belangen resultiere. Es seien daher grundsätzlich nur erlittene, objektiv nachvollziehbare, erhebliche und spürbare gesellschaftliche oder persönliche Nachteile, etwa in Form einer öffentlichen Bloßstellung, ersatzfähig (vgl. beispielsweise OLG Düsseldorf, Urt. v. 09.03.2023, Az: 16 U 154/21, OLG Koblenz, Urt. v. 23.01.2023 Az: 12 U 2194/21).

Dem hat der EuGH unter anderem mit den Urteilen vom 04.05.2023 und 14.12.2023 eine Absage erteilt (EuGH, Urt. v. 04.05.2014, Az: C-300/21; EuGH, Urt. v. 14.12.2023, Az: C-340/21); und dies zuletzt erneut in einer Entscheidung vom 11.04.2024 bestätigt und ausgeführt, dass es auf die Schwere des Schadens nicht ankomme.

Der EuGH vertritt demnach eine weite Auslegung des Schadensbegriffs. Die Befürchtung des Missbrauchs personenbezogener Daten kann ein ersatzfähiger immaterieller Schaden sein. Im Falle der Befürchtung des Datenmissbrauchs durch Dritte als Schaden, muss die betroffene Person nachweisen, dass diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die eigene Person als begründet angesehen werden kann (EuGH, Urt. 25.01.2024 - Az: C-687/21). Gleichwohl bezieht sich der EuGH in seiner Entscheidung vom 11.04.2024 konkret auf den 85. Erwägungsgrund der DSGVO, der ausdrücklich den „Verlust der Kontrolle“ über eigene Daten als Schaden zählt, der durch die DSGVO-Verletzung verursacht werden kann – so geringfügig und kurzfristig er auch sein mag. (EuGH, Urt. v. 11.04.2024 - Az.: C-741/21).

II. Höhe des Schadensersatzes

Durch zahlreiche Entscheidungen der Gerichte in den letzten Jahren zu DSGVO Schadensersatzforderungen haben sich langsam allgemeine Maßstäbe etabliert für die Bemessung der Betragshöhe. Dennoch können die zugesprochenen Summen einzelfallabhängig, je nach Gericht, stark variieren. Die Gerichte sprechen Schadensersatz in Höhe von 50 Euro bis 500 Euro wegen Datenscraping aufgrund eines Datenlecks auf einer Social Media Plattform zu, für unbefugte Datenabflüsse und -weitergaben zwischen 1.500 Euro und 4.000 Euro. Für nicht erfüllte Auskunftsansprüche und nicht erfüllte Löschpflichten sind es hingegen zwischen 250 Euro und 10.000 Euro.

Denn die Höhe des konkreten Schadens ist zwingend nach den Umständen des konkreten Einzelfalls zu bemessen.

Kriterien, die für die Abwägung und Beurteilung von Bedeutung sind, sind insbesondere

- die Finanzkraft des Schädigers,
- die Bedeutung des verletzten Rechts bzw. des beeinträchtigten Belangs,
- die Schwere der Rechtsverletzung,
- die Schwere der Schuld des Verantwortlichen am Schadenseintritt.

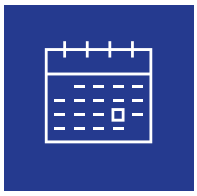
Bezüglich der Höhe des immateriellen Schadensersatzanspruchs betont der EuGH immer wieder die Ausgleichsfunktion des Anspruchs, die im Gegensatz zu der Straffunktion etwaiger Bußgeldvorschriften besteht. Die Ausgleichsfunktion des Art. 82 Abs. 1 DSGVO führt dazu, dass zwar der konkret erlittene Schaden in vollem Umfang zu ersetzen ist – allerdings nicht darüber hinaus. Dies hat er zuletzt bestätigt und entschieden, dass bei der Bemessung des Anspruchs auf immateriellen Schadensersatz der Geldbußen betreffende Art. 83 DSGVO nicht analog anzuwenden ist. Auch sei die Anzahl der Verletzungen kein relevantes Kriterium bei der Bemessung des Schadensersatzes (EuGH, Urt. v. 11.04.2024 - Az.: C-741/21).

III. Unser Fazit

Mit den dargestellten Entscheidungen konkretisiert der EuGH den Schadensersatzanspruch des Art. 82 DSGVO durch die folgenden wesentlichsten Erwägungen:

- Nicht jeder Verstoß gegen die Vorschriften der DSGVO löst automatisch einen Schadensersatzanspruch nach Art. 82 DSGVO aus. Der betroffenen Person muss ein materieller oder immaterieller Schaden entstanden sein, den diese nachzuweisen hat.
- Der Begriff des Schadens ist weit auszulegen. Der Anspruch auf Ersatz immaterieller Schäden setzt keinen spürbaren Nachteil voraus.
- Art. 82 DSGVO weist keine Erheblichkeitsschwelle oder Bagatellgrenze auf, die durch den Schaden überschritten sein müsste.
- Die Befürchtung des Missbrauchs personenbezogener Daten kann ein ersatzfähiger immaterieller Schaden sein. Im Falle der Befürchtung des Datenmissbrauchs durch Dritte als Schaden, muss die betroffene Person nachweisen, dass diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die eigene Person als begründet angesehen werden kann.
- Eine Haftungsbefreiung nach Art. 82 Abs. 3 DSGVO ist nur in engen Grenzen möglich.
- Die DSGVO enthält keine Regelungen zur Bemessung der Höhe des als Schadensersatz zu leistenden Betrags, sodass die nationalen Gerichte unter Beachtung der unionsrechtlichen Äquivalenz- und Effektivitätsgrundsätze die innerstaatlichen Vorschriften der einzelnen Mitgliedstaaten anwenden. Zur Bemessung der Höhe einer zu leistenden Entschädigung verlangt Art. 82 DSGVO nicht, dass dabei der Grad des Verschuldens oder die Anzahl der DSGVO-Verstöße des Verantwortlichen gegenüber dem Betroffenen berücksichtigt werden.
- Art. 82 DSGVO kommt eine Ausgleichs- und keine Abschreckungs- oder Straffunktion zu.

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, Singapur, Stuttgart, Yangon

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

unyer GLOBAL ADVISORS