Geschäftsstelle Dresden:
Königsbrücker Landstraße 40
01109 Dresden
Tel: 0351 8881251

Niederlassung Böblingen:
Otto-Lilienthal-Straße 36
71034 Böblingen

mail@sodalitas-gmbh.de
www.sodalitas-gmbh.de
Fax: 0351 8881252

IT-Ticker 01/2024

Der IT-Ticker 01/2024 informiert Sie über folgende Themen:

- Künstliche Intelligenz
- Datenschutz
- Digital Decade der EU

Regeln der EU für den Einsatz künstlicher Intelligenz – Die KI Verordnung

Das EU-Parlament gibt grünes Licht für weltweit erste Regeln für künstliche Intelligenz (KI) in der Europäischen Union. Die Parlamentarier haben am Mittwoch in Straßburg mehrheitlich für ein entsprechendes Gesetz gestimmt. Die EU-KI-Verordnung (KI-VO) schafft einen einheitlichen rechtlichen Rahmen für KI in der EU, unabhängig von Branche oder Technologie. Durch ihre sofortige und einheitliche Anwendung in allen 26 EU-Mitgliedstaaten soll die Verordnung Rechtssicherheit in ganz Europa (und darüber hinaus) bieten.

Anwendungsbereich der KI-Verordnung

Die Verordnung regelt KI-Systeme, die sie definiert als maschinenbasierte Systeme, die autonom operieren. Dies bedeutet, dass sich solche KI-Systeme ohne dirigierenden menschlichen Einfluss selbst anpassen und entwickeln können. Die KI-Systeme können aus den Nutzereingaben selbständig Ergebnisse erzeugen.

Die KI-VO betrifft Anbieter, Bereitsteller, Importeure, Händler und Produkthersteller von KI-Systemen mit Sitz in der EU oder außerhalb. Entscheidend ist, dass sie die KI innerhalb der EU verwenden. Endverbraucher sind nicht direkt betroffen.

Risikobasierter Ansatz

Die KI-VO klassifiziert KI nach Risikogruppen. Verboten sind KI-Systeme mit unannehmbarem Risiko, während KI-Systeme mit hohem Risiko strengen Anforderungen unterliegen und nicht gänzlich verboten sind. KI-Systeme mit begrenztem oder minimalem Risiko haben spezifische Transparenzverpflichtungen. Eine General Purpose AI (GPAI), und ihre jeweiligen Grundmodelle, die die Grundlage für generative KI-Anwendungen wie ChatGPT bilden, unterliegen besonderen Regelungen.

Verbotene KI-Systeme

Die KI-VO verbietet den Einsatz bestimmter KI-Systeme, darunter manipulative Praktiken, biometrische Kategorisierung und Social Scoring. Arbeitgeber müssen den Einsatz der KI-Systeme am Arbeitsplatz sorgfältig prüfen und die Nutzung von KI für gezielte Werbung wird voraussichtlich eingeschränkt.

Hochriskante KI-Systeme

KI-Systeme mit erheblichem Risiko unterliegen ebenfalls strengen Vorgaben. Die KI-VO ermöglicht über einen gesetzlichen Filter Ausnahmen von diesen strengen Vorgaben, z.B. für KI-Systeme mit eng gefasster Verfahrensaufgabe. Dafür müssen sie aber in einer offiziellen EU-Datenbank registriert sein, bevor sie in der EU auf den Markt gebracht werden. GPAI-Modelle, die aufgrund der Menge durchgeführter Berechnungen besonders relevant („systemisch“) sind, haben zusätzliche Verpflichtungen, um systemrelevante Risiken zu mindern.

Anbieter hochriskanter KI-Systeme müssen ein Risiko- und Qualitätsmanagementsystem etablieren, und sicherstellen, dass das KI-System ein angemessenes Niveau an Robustheit, Genauigkeit und Cybersicherheit aufweist. Betreiber müssen eine menschliche Aufsicht gewährleisten und Risiken melden, sowie stets eine Folgenabschätzung für Grundrechte durchführen. Die Parallelen zur Datenschutzfolgenabschätzung der DSGVO und zur Registrierung von Medizinprodukten sind offensichtlich erkennbar und dürften bei der praktischen Umsetzung der KI-VO hilfreich sein. Die Verordnung betont insbesondere auch hohe Fairness-Anforderungen bei der Auswahl von Trainingsdaten, um verzerrte und unfaire Ergebnisse zu vermeiden.

General Purpose AI (GPAI)

Eine GPAI unterliegt speziellen Regelungen, mit umfangreichen Informations- und Dokumentationspflichten für Anbieter. Die Verwender dieser Systeme sollen die Fähigkeiten und Grenzen des KI-Modells im Sinne einer „explainable AI“ verstehen können. Systemische GPAI-Modelle müssen zusätzliche Sicherheitsmaßnahmen treffen und Verhaltenskodizes entwickeln. Einsatz von KI-Systemen gegenüber menschlichen Individuen

Transparenz ist für KI-Systeme, die direkt mit Menschen interagieren, erforderlich. Generative KI-Systeme müssen ihre Ausgabe als künstlich erzeugt kennzeichnen. Betreiber von KI-Systemen für biometrische Kategorisierung oder Emotionserkennung müssen die Endnutzer transparent informieren.

Kontrolle und Durchsetzung

Nationale Behörden überwachen die Einhaltung der KI-VO, wobei es bisher noch ungeklärt ist, welche Behörde auf deutscher Ebene mit dieser wichtigen Überwachungsaufgabe betraut sein wird. Das neu errichtete KI-Büro der EU-Kommission überwacht die GPAI-Modelle und -Systeme. Sanktionen für Verstöße können bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes betragen.

Zeitplan für den Übergangszeitraum

Die KI-VO tritt voraussichtlich im April oder Mai 2024 in Kraft. Unterschiedliche Fristen gelten für verbotene KI-Systeme, KI-Modelle, GPAI und KI-Systeme mit hohem Risiko. Verhaltenskodizes können nach 9 Monaten eingereicht werden, und Sanktionen werden nach 12 Monaten wirksam. Wir empfehlen zudem, die neuen Regeln für Produkthaftung und die Haftungsregeln der KI-Verordnung eng zu beobachten, da auch in diesem Bereich konkrete neue Regeln auf EU-Ebene in Arbeit sind.

Dr. Matthias Orthwein
Dr. Stefan Peintinger

"KI-Flash": Regulierung Künstlicher Intelligenz durch die EU - Was ist ein "KI System" nach dem EU AI Act?

Nachdem wir in unserem letzten KI-Flash über Mitbestimmungsrechte des Betriebsrats beim Einsatz von ChatGPT berichtet haben, möchten wir Ihnen auch weiterhin in regelmäßigen Abständen rechtliche Impulse mit auf den Weg geben.

Die EU-Verordnung über Künstliche Intelligenz („AI Act“) ist ihrem Inkrafttreten ein Stück näher gerückt. Nachdem sich das EU-Parlament und der Rat im Dezember 2023 politisch auf eine angepasste Fassung des AI Acts geeinigt haben, wurde diese Fassung schließlich Anfang Februar 2024 von den Mitgliedstaaten der EU einstimmig gebilligt. In diesem KI Flash befassen wir uns mit der Definition des „KI-Systems“ in der aktualisierten Fassung des AI Acts. Was versteht also der AI Act unter Künstlicher Intelligenz?

Inkrafttreten und Wirksamwerden des AI Acts

Nach der erfolgten politischen Einigung Anfang Februar 2024 müssen nun noch das Europäische Parlament und eine Ratsformation formell zustimmen, bevor die Verordnung im EU-Amtsblatt veröffentlich werden kann. Am 20. Tag nach der Veröffentlichung tritt der AI Act in Kraft.

2 Jahre nach Inkrafttreten wird die überwiegende Anzahl der Vorschriften des AI Acts tatsächlich anwendbar. Allerdings werden im AI Act vorgesehene Verbote (verbotene KI-Systeme) voraussichtlich bereits 6 Monaten nach Inkrafttreten wirksam, die Vorschriften zu KI-Modellen mit allgemeinem Verwendungszweck (GPAI) voraussichtlich nach 12 Monaten.

Was ist ein KI-System nach dem AI Act?

Der Begriff des KI-Systems wurde im Gesetzgebungsprozess heftig diskutiert. Nach der Kompromissfassung des AI Acts ist nach Art. 3(1) der englischen Sprachfassung ein KI-System

„a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

Die Definition wurde bewusst an eine Fassung der OECD angelehnt. Dadurch verspricht sich die EU mehr Akzeptanz und Kohärenz auf internationaler Ebene.

Als zentrales Merkmal zur Abgrenzung der „KI-Systeme" von traditioneller Software setzt ein KI-System nach der Definition voraus, dass es aus dem Input Schlussfolgerungen für den Output ableitet („infers, from the input it receives, how to generate outputs"). Dies soll die Fähigkeit von KI-Systemen hervorheben, aus eingegebenen Daten Modelle, und/oder Algorithmen abzuleiten. Systeme, die hingegen auf Regeln beruhen, die ausschließlich von natürlichen Personen festgelegt werden, um automatische Vorgänge auszuführen, wollte die EU damit vom Anwendungsbereich des AI Acts ausschließen. Die Fähigkeiten von KI-Systemen sollen definitorisch über grundlegende Datenverarbeitungsvorgänge hinausgehen und eher als Lernen, Schlussfolgern oder Modellieren zu begreifen sein.

Außerdem geht die Definition im AI Act davon aus, dass KI-Systeme mit unterschiedlichem Grad an Autonomie arbeiten („designed to operate with varying levels of autonomy"). Es muss demnach ein gewisses Maß an Unabhängigkeit des Handelns des Systems vom Menschen bestehen. Mit anderen Worten muss das System ohne menschliches Eingreifen operieren können.

In dem Merkmal der Anpassungsfähigkeit („adaptivness") soll die Fähigkeit eines KI-Systems zum Ausdruck kommen, selber (weiter) zu lernen und sich dadurch laufend zu verändern.

Gesetzliche Definitionen sind auslegungsfähig und oftmals auslegungsbedürftig. Dies gilt auch für die Definition der „KI-Systeme" im AI Act. Sprechen Sie uns gerne an. Wir helfen bei der Einordnung Ihrer Software als KI-System und der möglichen Konsequenzen, die sich aufgrund der EU Regulierung ergeben können.

Dr. Christoph Krück
Dr. Daniel Meßmer

„KI-Flash": Mitbestimmungsrechte des Betriebsrats beim Einsatz von ChatGPT?

Nachdem wir in unserem letzten KI-Flash über den Hinweis des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zu den Auswirkungen des SCHUFA-Urteils auf KI-Anwendungen berichtet haben, möchten wir Ihnen auch weiterhin in regelmäßigen Abständen rechtliche Impulse mit auf den Weg geben. Da Zeit in der heutigen Gesellschaft ein rares Gut ist, wollen wir mit unseren „KI-Flash" gleich auf den Punkt kommen und die rechtlichen Herausforderungen kurz und prägnant zusammenfassen:

Heutiges Thema: Mitbestimmungsrechte des Betriebsrats beim Einsatz von ChatGPT?

Immer mehr Unternehmen gestatten ihren Mitarbeiter*innen proaktiv die Nutzung generativer KI-Tools zur Unterstützung ihrer Arbeitstätigkeiten. Bei der Einführung von ChatGPT & Co. stellt sich allerdings die Frage, ob dem Betriebsrat hierfür ein Mitbestimmungsrecht zugutekommt. Nach einer aktuellen

Entscheidung des Arbeitsgerichts Hamburg vom 16.01.2024 (24 BV Ga 1/24)ist dies zu verneinen – allerdings war das konkrete Einsatzmodell des Unternehmens entscheidend.

Sachverhalt

In dem vom ArbG Hamburg zu entscheidenden Fall wollte ein Unternehmen seinen Mitarbeiter*innen die Nutzung gängiger KI-Anwendungen wie ChatGPT im Rahmen ihrer Arbeitstätigkeit ermöglichen. Dazu veröffentliche es im Intranet entsprechende Guidelines, Richtlinien und ein Handbuch, um seine Mitarbeiter*innen über Art und Umfang der Nutzung von KI zu sensibilisieren und zu informieren. Darin wurde auch darauf hingewiesen, dass die mittels KI erzielten Arbeitsergebnisse entsprechend gekennzeichnet werden müssten. Das Unternehmen entschied sich allerdings dafür, den Mitarbeiter*innen entsprechende KI-Anwendungen nicht selbst zur Verfügung zu stellen, sondern gestattete diesen lediglich die Nutzung privater Accounts zu dienstlichen Zwecken auf eigene Kosten der Mitarbeiter. Es wurden daher weder KI-Anwendungen auf den Systemen des Unternehmens installiert, noch gab es unternehmensseitige Accounts, welche den Mitarbeitern zur dienstlichen Nutzung überlassen wurden. Die Nutzung erfolgte nur über die browserbasierten Zugänge der Mitarbeiter*innen. Der Betriebsrat sah hierin seine Mitbestimmungsrechte verletzt und begehrte im Rahmen des einstweiligen Rechtsschutzes das Verbot des Einsatzes von entsprechenden KI-Anwendungen.

Entscheidung

Nach Auffassung des ArbG Hamburg ist im vorliegenden Fall ein Mitbestimmungsrecht des Betriebsrats nicht anzunehmen.

Ein Mitbestimmungsrecht nach § 87 Abs. 1 S. 1 Nr. 1 BetrVG (Fragen der Ordnung des Betriebs oder des Verhaltens der Arbeitnehmer im Betrieb) bestehe nicht, da der Einsatz dieser KI-Tools unter das mitbestimmungsfreie Arbeitsverhalten falle. Auch die Zurverfügungstellung von KI-Richtlinien, Guidelines oder Handreichungen sind Anordnungen, die die mitbestimmungsfreie Art und Weise der Arbeitserbringung betreffen.

Ferner besteht gemäß § 87 Abs. 1 S. 1 Nr. 6 BetrVG (Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen) nach Ansicht des ArbG Hamburg kein Mitbestimmungsrecht. Zum einen seien ChatGPT und Co. nicht auf den Systemen des Unternehmens installiert, zum anderen werde die Einwahl und Nutzung des Tools über den Browser zwar regelmäßig aufgezeichnet, dies stelle jedoch keine Besonderheit von ChatGPT dar, sondern sei schlicht auf die Funktionsmöglichkeit des Webbrowsers zurückzuführen. Hinsichtlich der Nutzung des Webbrowsers selbst bestehe also an sich ein Mitbestimmungsrecht. Zur Nutzung von Browsern existierte aber bereits eine Konzernbetriebsvereinbarung, sodass der Betriebsrat insoweit sein Mitbestimmungsrecht aus § 87 Abs. 1 S. 1 BetrVG schon ausgeübt hatte. Auch die im konkreten Fall geforderte Kennzeichnung der mithilfe von KI erzeugten Arbeitsergebnisse löst kein Mitbestimmungsrecht aus. Denn die Kennzeichnung und die damit verbundene Kontrollmöglichkeit des Unternehmens erfolgt durch den Mitarbeitenden selbst und nicht das Tool.

Ausblick und Praxishinweise

Die Entscheidung des Arbeitsgerichts Hamburg verdeutlicht, dass es für die Frage nach dem Bestehen eines Mitbestimmungsrechts des Betriebsrats für Tools wie ChatGPT stets auf das konkrete Anwendungsszenario ankommt. In diesem speziellen Fall gestattete das Unternehmen lediglich die Nutzung browserbasierter KI-Anwendungen privater Accounts. Außerdem ist zu beachten, dass in dem vorliegenden Fall eine Konzernbetriebsvereinbarung zur Verwendung von Browsern durch Mitarbeiter bereits vorlag. Fehlt eine solche Vereinbarung, ist jedenfalls dieser Einsatz grundsätzlich eine mitbestimmungspflichtige Maßnahme – unabhängig von deren Nutzung für KI-Tools.

Viele Unternehmen werden jedoch ein Interesse daran haben, die tätigkeitsbezogene Nutzung entsprechender Tools systemseitig zu steuern und zu verwalten und den Mitarbeiter*innen solche Anwendungen selbst unternehmensseitig zur Verfügung zu stellen. Dies gilt insbesondere vor dem Hintergrund, dass sich bei der Nutzung von KI wie ChatGPT weitere rechtliche Folgefragen stellen, die von Unternehmen zu beachten sind (dazu haben wir etwa hier und hier berichtet).

Soweit ein Unternehmen seinen Mitarbeitern die KI-Nutzung über einen Unternehmensaccount gewährt oder auf eine „Enterprise“-Lösung mit zugehörigen Mitarbeiteraccounts zurückgreift, kann die Rechtslage daher anders zu bewerten sein. Ähnliches gilt, wenn maßgeschneiderte KI-Lösungen zum Einsatz kommen sollen, die für spezielle Anwendungsfälle im Unternehmen angepasst werden können. Auch solche Anwendungen werden in der Regel in der eigenen IT-Umgebung des Unternehmens bereitgestellt, sodass ihr Einsatz in der Regel zu einem Mitbestimmungsrecht des Betriebsrats nach § 87 Absatz 1 Nr. 6 BetrVG führen wird. Der Arbeitgeber muss jedoch den Betriebsrat beim Einsatz von KI-Tools zwingend unterrichten, § 90 Abs. 1 Nr. 3 BetrVG.

Ferdinand Schwarz
Tamara Ulm

"KI-Flash": Hinweis des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zu den Auswirkungen des SCHUFA-Urteils auf KI-Anwendungen

Nachdem wir in unserem letzten KI-Flash über den aktuellen Stand zur Europäischen KI-Verordnung (Stand: 19. Dezember 2024) berichtet haben, möchten wir Ihnen auch weiterhin in regelmäßigen Abständen rechtliche Impulse mit auf den Weg geben. Da Zeit in der heutigen Gesellschaft ein rares Gut ist, wollen wir mit unseren „KI-Flash“ gleich auf den Punkt kommen und die rechtlichen Herausforderungen kurz und prägnant zusammenfassen:

Heutiges Thema: Hinweis des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit („HmbBfDI“) zu den Auswirkungen des SCHUFA-Urteils (Az. C-634/21) auf KI-Anwendungen.

Mit Urteil vom 07. Dezember 2023 (Az. C-634/21) entschied der EuGH, dass die Verwendung des sog. SCHUFA-Scores eine „ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung“ nach Art. 22 DS-GVO darstelle, sofern Dritte ausschließlich auf Grundlage des Scores über den Abschluss von Verträgen mit Betroffenen entscheiden.
Noch am selben Tag der Entscheidung erfolgte ein Hinweis des HmbBfDI, dass dieses Urteil weitereichende Folgen auch für viele KI-Anwendungen habe, da diese - ähnlich wie beim Scoring - Entscheidungen mithilfe von Algorithmen vorbereiten. Analog wie Auskunfteien, setzen nämlich Unternehmen vermehrt KI-Systeme ein, um bestimmte Entscheidungsprozesse (etwa im Bewerberprozess) vorzubereiten. Sofern die von der KI vorgeschlagenen Ergebnisse auf Basis kaum nachvollziehbarer und von der KI eigenständig entwickelter Kriterien entstanden sind, könne das Urteil des EuGHs auf diese Fälle entsprechend angewendet werden.

Auf Grundlage des Urteils müssten solche KI-basierten Bewertungen daher mit einer menschlichen Beurteilung verknüpft werden. Konsequenz sei folglich, dass die letztentscheidende Person die Sachkunde und daneben genug Zeit benötige, um die maschinelle Vorentscheidung hinterfragen zu können. Hierfür sei wiederum erforderlich, dass KI Entwickler die Entscheidungswege der KI in transparenter Form abbilden. Anwender hingegen seien verpflichtet, sich mit der Funktionsweise der KI auseinanderzusetzen und diese regelmäßig zu überprüfen.

Sollte dies nicht möglich sein, so dürfen automatische Entscheidungen einer KI nur in folgenden Fällen übernommen werden:

- Die betroffene Person hat ausdrücklich eingewilligt, oder
- die automatisierte Entscheidung ist im Ausnahmefall für die Erfüllung eines Vertrags erforderlich, da beispielsweise in einer Online-Anwendung die sofortige verbindliche Rückmeldung notwendig ist.

Betroffene haben in diesen Fällen jedoch stets die Möglichkeit, die Nachprüfung der Entscheidung durch einen Menschen zu verlangen.

Der EuGH hat somit – auch nach Auffassung des HmbBfDI – insbesondere die Spielregeln für den Einsatz von KI konkretisiert und damit ein wegweisendes Urteil für KI-basierte Entscheidungen geschaffen. Für Unternehmen bedeutet dies in der Folge, dass die eingesetzten (oder auch eigenständig entwickelten) KI Anwendungen genauestens zu prüfen sind. Dies gilt insbesondere für

die Frage, ob und inwieweit der Anwendungsbereich des Art. 22 DS-GVO im Einzelfall eröffnet ist, bzw. eröffnet sein kann.

In unserem nächsten KI-Flash werden wir auf die finalen Regelungen der europäischen KI-Verordnung eingehen und insoweit einen etwas umfassenderen Überblick zu den künftigen Anforderungen aufzeigen.

Marius Drabiniok
Marwah Kamal
Franziska Ladiges

Fällt der EU-Kommission nun der Europäische Datenschutz auf die Füße?

Der Europäische Datenschutzbeauftragte (EDSB) hat am 8. März 2024 festgestellt, dass die Europäische Kommission bei der Nutzung von Microsoft 365 gegen EU-Datenschutzrichtlinien verstößt und ihr Abhilfemaßnahmen auferlegt.

Die Frage, ob der Einsatz von Microsoft 365 datenschutzkonform ist, wird bereits seit längerer Zeit kontrovers diskutiert. Der Europäische Datenschutzbeauftragte EDSB hat hierauf nun eine klare Antwort gegeben und in einer Pressemitteilung das Ergebnis seiner im Mai 2021 gestarteten Untersuchung zum Einsatz von Microsoft 365 durch die EU-Kommission verkündet: Die EU-Kommission habe danach gegen mehrere Bestimmungen der Verordnung (EU) 2018/1725, die den Datenschutz für die Organe der EU regelt, verstoßen. Es sei im Vertrag zwischen der Kommission und Microsoft nicht ausreichend festgelegt und spezifiziert, welche Arten von personenbezogenen Daten zu welchen expliziten Zwecken bei der Nutzung von Microsoft 365 erhoben und verarbeitet werden sowie welche Daten an welche Empfänger zu welchen Zwecken weitergegeben werden dürfen. Zudem habe die Kommission insbesondere in der Vergangenheit vor Inkrafttreten des Angemessenheitsbeschlusses mit der USA versäumt, angemessene Garantien dafür zu schaffen, dass personenbezogene Daten, die an Drittländer übermittelt werden, ein angemessenes Schutzniveau erhalten.

Der EDSB hat die Kommission daher angewiesen, spätestens bis zum 9. Dezember 2024 alle Datenströme auszusetzen, die sich aus der Nutzung von Microsoft 365 an Microsoft und an seine verbundenen Unternehmen und Unterauftragsverarbeiter in Drittländer ergeben. Ausnahmen gelten lediglich für Drittstaaten, die ein mit der EU vergleichbares Datenschutzniveau haben. Durch Inkrafttreten des EU-U.S. Data Privacy Frameworks im Juli 2023 zählt die USA derzeit zu den Ländern, in denen ein solches Datenschutzniveau besteht. Darüber hinaus muss die Kommission bis zum genannten Stichtag ihre Datenverarbeitung unter Verwendung von Microsoft 365 in Einklang mit den Vorgaben der Verordnung (EU) 2018/1725 bringen und die entsprechende Datenschutz-Compliance nachweisen. Die Liste der zu ergreifenden Maßnahmen ist umfassend: So gibt der EDSB der Kommission auf, (i) ein Data-Transfer-Mapping zu erstellen, um festzustellen an welche Empfänger welche Daten in welche Drittländer zu welchen Zwecken und mit welchen Schutzmaßnahmen gelangen, (ii) sicherzustellen, dass Daten im Rahmen der Auftragsverarbeitung nur auf Weisung der Kommission verarbeitet werden sowie (iii) vertragliche Grundlagen zu schaffen zur Einhaltung der Gebote der Zweckbindung sowie Datenminimierung, der Gewährleistung interner Transparenz über die Datenverarbeitung sowie die Verhinderung der Offenlegung personenbezogener Daten an staatliche Stellen außerhalb des EWR.

Diese Anordnung des EDSB bedeutet nicht, dass der Einsatz von Microsoft 365 generell nicht rechtskonform möglich wäre. Auch findet die Verordnung (EU) 2018/1725, auf die sich die Entscheidung stützt, keine Anwendung auf private Unternehmen. Die für diese geltende DSGVO enthält jedoch identische Anforderungen an die Einbindung von Clouddienstleistern. Damit unterstreicht und bestätigt diese Entscheidung des EDSB die bereits von der Datenschutzkonferenz (DSK) und verschiedenen Aufsichtsbehörden veröffentlichte Auffassung, dass verantwortliche Stellen, die Microsoft 365 einsetzen, gehalten sind, eindeutig in den Auftragsverarbeitungsverträgen mit Microsoft zu bestimmen, welche personenbezogenen Daten zu welchen Zwecken über die Cloudanwendung verarbeitet werden und sich interne Transparenz hinsichtlich der Verarbeitung in Drittländern zu verschaffen, um dort geeignete Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus zu implementieren. Unternehmen, die Microsoft 365 einsetzen, sollten daher eine datenschutzrechtliche Überprüfung durchführen, wie genau im Einsatz des Tools personenbezogene

Daten durch wen (einschließlich etwaiger Unterauftragnehmer) verarbeitet werden, inwieweit Microsoft Daten möglicherweise gar zu eigenen Zwecken verarbeitet, wie das Weisungsrecht gegenüber Microsoft vertraglich ausgestaltet wird, welche Regelungen zur Datenlöschung erforderlich sind, wie genau die technischen und organisatorischen Maßnahmen (TOMs) auszugestalten sind und welche weitere Risiko-Assessments einschließlich einer etwaigen Datenschutzfolgenabschätzung (DSFA) erforderlich sind.

Jan-Dierk Schaal

EuGH-Urteil zu Real Time Bidding: Was Werbetreibende jetzt beachten müssen

Der EuGH hat am 7. März 2024 sein Urteil in der Rechtssache C-604/22 veröffentlicht.

Das Vorlagenverfahren betrifft grundlegende Fragen zum Datenschutz in digitalen Werbe-Ökosystemen. Das gezielte Ausspielen von (digitaler) Werbung für einen Nutzer gehört seit Jahren zum Werkzeugkasten jedes Werbetreibenden. Die Entscheidung wird daher aller Voraussicht nach weitreichende praktische Konsequenzen haben.

Hintergründe

Hintergründe zum Real Time Bidding-Verfahren

Für das gezielte Ausspielen von digitaler Werbung an einen bestimmten Webseitennutzer oder einen Nutzer einer Anwendung („App“) wird in der Praxis häufig das sog. Real Time Bidding-Verfahren genutzt.

Wenn ein Nutzer eine Webseite oder eine App mit einem Werbeplatz aufruft, können Werbeunternehmen, insbesondere Data Broker und Werbeplattformen, die Tausende von Werbetreibenden vertreten, anonym in Echtzeit Gebote abgeben, um über ein automatisiertes Versteigerungssystem („Bidding“) unter Verwendung von Algorithmen diesen Werbeplatz zu erhalten und dort gezielt Werbung anzuzeigen, die spezifisch auf das Profil eines solchen Nutzers abgestimmt ist.

Der Vorteil für einen Werbetreibenden ist u. a., dass er seinen Streuverlust bei der Schaltung von Werbung reduzieren kann. Der Werbetreibende zahlt für möglichst gezielte Werbung an bestimmte Nutzer.

Für Webseitenbetreiber liegt der Vorteil in der „mehrfachen“ Verkaufsmöglichkeit von digitalen Werbeflächen. Zwei Nutzer, die zeitgleich eine bestimmte Webseite aufrufen, sehen (mit an Sicherheit grenzender Wahrscheinlichkeit) unterschiedliche Werbungen, basierend auf unterschiedlichen Profilen. Der Webseitenbetreiber verdient doppelt.

Hintergründe zur Nutzung des Real Time Bidding-Verfahrens auf der Grundlage des Transparency & Consent Framework des IAB Europe

Das Interactive Advertising Bureau („IAB Europe“) ist ein Verband, welcher die digitale Werbe- und Marketingindustrie auf europäischer Ebene vertritt. Zu den Mitgliedern von IAB Europe gehören u. a. Unternehmen, die durch den Verkauf von Werbeplätzen auf Webseiten oder in Apps hohe Einnahmen erzielen.

IAB Europe hat das „Transparency & Consent Framework“ („TCF“) entwickelt. Dies stellt einen Regelungsrahmen dar, der aus Richtlinien, Anweisungen, technischen Spezifikationen, Protokollen und vertraglichen Verpflichtungen besteht, die es sowohl dem Anbieter einer Webseite oder App als auch Datenbrokern oder Werbeplattformen ermöglichen, personenbezogene Daten („pbD“) eines Nutzers rechtmäßig zu verarbeiten.

Das Ziel des TCF besteht insbesondere darin, die Einhaltung der DSGVO zu erleichtern, wenn Unternehmen das Real Time Bidding nutzen. Bevor jedoch eine solche gezielte Werbung angezeigt wird, muss die vorherige Einwilligung des Nutzers eingeholt werden.

Dafür wird eine „Consent Management Platform“ („CMP“) genutzt, welche es dem Nutzer ermöglicht, zum einen dem Anbieter der Webseite bzw. App seine Einwilligung zur Erhebung und Verarbeitung seiner pbD für vorher festgelegte Zwecke, wie u. a. Marketing oder Werbung, oder zum Austausch dieser Daten mit bestimmten Anbietern zu geben, und zum anderen verschiedenen Arten der Datenverarbeitung oder dem Austausch von Daten aufgrund der von den Anbietern geltend gemachten berechtigten Interessen im Sinne von Artikel 6 Abs. 1 lit. f) DSGVO („berechtigtes Interesse“) zu widersprechen. Diese pbD betreffen insbesondere den Standort des Nutzers, sein Alter, den Verlauf seiner Suchanfragen und seine zuletzt getätigten Einkäufe.

Das TCF bietet einen Rahmen für die umfangreiche Verarbeitung pbD und erleichtert die Erfassung der Nutzerpräferenzen mittels der CMP.

Diese Präferenzen werden anschließend in einem String kodiert und gespeichert, der aus einer Kombination von Buchstaben und Zeichen besteht und von IAB Europe als Transparency and Consent String („TC-String“) bezeichnet wird. Der jeweilige TC-String wird mit den an Real Time Bidding-Verfahren beteiligten Brokern für pbD und Werbeplattformen geteilt. Diese können damit feststellen, worin der Nutzer eingewilligt und/oder wogegen er Widerspruch eingelegt hat.

Die CMP speichert auch ein Cookie (Euconsent-v2) auf dem jeweiligen genutzten Gerät des Nutzers.

Miteinander kombiniert, können der jeweilige TC-String und das jeweilige Cookie der genutzten IP-Adresse eines konkreten Nutzers zugeordnet werden.

Rechtliche Fragestellungen

TC-String kann ein personenbezogenes Datum darstellen.

Zunächst musste der EuGH die Frage klären, ob ein TC-String, im vorgelegten Sachverhalt, als pbD anzusehen ist. Dabei geht der EuGH zunächst davon aus, dass ein TC-String ein pbD sein kann, auch wenn ein solcher TC-String selbst keine unmittelbar identifizierbaren Informationen enthält.

Aufgrund der weiten Definition des Begriffs „Personenbezug“ in Artikel 4 Nr. 1 DSGVO ist auch eine Personenbeziehbarkeit ausreichend, wenn wie hier eine Zuordnung zu einer bestimmten natürlichen Person möglich ist. Der EuGH hat IAB Europe daher als Verantwortlichen im Sinne der DSGVO eingestuft (vgl. Artikel 4 Nr. 7 DSGVO).

Selbst die Tatsache, dass IAB Europe nicht selbst und unmittelbar über die Mittel einer Identifizierung verfügt, ist nach Ansicht des EuGH und seiner bisherigen Rechtsprechung kein Grund, den Personenbezug aus Sicht der IAB Europe zu verneinen. Aufgrund der Aktenlage geht der EuGH davon aus, dass Mitglieder von IAB Europe (= z. B. Werbetreibende; Data Broker) verpflichtet sind, dem IAB Europe auf Anfrage alle Informationen zu übermitteln, die es ihm ermöglichen, die Nutzer zu identifizieren, deren Daten Gegenstand eines TC-Strings sind.

Damit verfüge der IAB Europe grundsätzlich über Mittel, die es ihm nach allgemeinem Ermessen ermöglichen, eine bestimmte natürliche Person anhand der Informationen zu identifizieren, die ihm seine Mitglieder und andere am TCF teilnehmende Organisationen zur Verfügung stellen müssen (vgl. Erwägungsgrund Nr. 26 S. 3 und S. 4 DSGVO).

Ein TC-String ist daher, aus der Perspektive des IAB Europe, als pbD anzusehen.

Branchenverbände, wie IAB Europe, können als Joint Controller angesehen werden.

Der EuGH musste anschließend die Fragen klären, ob der IAB Europe nicht nur als Verantwortlicher im datenschutzrechtlichen Sinne anzusehen ist, sondern für das TCF sogar eine gemeinsame Verantwortlichkeit gegeben sein kann im Sinne von Artikel 26 DSGVO. Eine gemeinsame Verantwortlichkeit führt zu weiteren datenschutzrechtlichen Anforderungen, auch im Rahmen von Webseiten- und/oder App-Datenschutzhinweisen.

Der IAB Europe, als Branchenorganisation, hat seinen Mitgliedern einen von dem IAB Europe aufgestellten Regelungsrahmen in Bezug auf die Einwilligung im Bereich der Verarbeitung

personenbezogener Daten angeboten, der nicht nur verbindliche technische Vorschriften enthält, sondern auch Vorschriften, die detailliert festlegen, wie pbD, die diese Einwilligung betreffen, gespeichert und verbreitet werden müssen. Dabei war auch fraglich, ob sich die Einschätzung daran richtet, ob der IAB Europe selbst unmittelbaren Zugang zu den pbD hat, die von seinen Mitgliedern innerhalb dieses Regelungsrahmens verarbeitet werden.

Zudem musste der EuGH klären, ob eine gemeinsame Verantwortung (vgl. Artikel 26 DSGVO) anzunehmen ist, wenn eine solche Branchenorganisation auf die Weiterverarbeitung personenbezogener Daten durch Dritte, wie beispielsweise Mitgliedern des IAB Europe, Einfluss hat, z. B. in Bezug auf Nutzerpräferenzen für gezielte Online-Werbung.

1. Branchenverband kann Verantwortlicher sein.
   Zunächst hat der EuGH unter Verweis auf ältere EuGH-Entscheidungen entschieden, dass eine natürliche oder juristische Person, die aus Eigeninteresse auf die Verarbeitung pbD Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt, als Verantwortlicher im Sinne von Artikel 4 Nr. 7 DSGVO angesehen werden kann.

2. Branchenverband kann Gemeinsamer Verantwortlicher sein.
   Die Mitwirkung an der Entscheidung über die Zwecke und Mittel der Verarbeitung kann verschiedene Formen annehmen und sich sowohl aus einer gemeinsamen Entscheidung von zwei oder mehr Einrichtungen als auch aus übereinstimmenden Entscheidungen solcher Einrichtungen ergeben.

   Daher kann auch eine Branchenorganisation wie der IAB Europe als Gemeinsamer Verantwortlicher im Sinne von Artikel 4 Nr. 7 und Artikel 26 Abs. 1 DSGVO angesehen werden. Nach der Rechtsprechung des EuGH setzt die gemeinsame Verantwortlichkeit mehrerer Akteure für dieselbe Verarbeitung nach der DSGVO nicht voraus, dass jeder der Akteure Zugang zu den betreffenden pbD hat (vgl. entsprechende EuGH-Entscheidung vom 10. Juli 2018, C-25/17, Zeugen Jehovas).

   Im Einzelfall ist daher zu prüfen, ob eine solche Branchenorganisation unter Berücksichtigung der besonderen Umstände des vorliegenden Falles aus Eigeninteresse auf die Verarbeitung pbD, wie des TC-Strings, Einfluss nimmt und gemeinsam mit anderen die Zwecke der und die Mittel zur fraglichen Verarbeitung festlegt. Der IAB Europe wäre dann nicht lediglich eine Organisation zur Standardisierung von Prozessen (hier: der Verarbeitung von pbD in einem bestimmten Kontext), sondern möglicherweise gemeinsam, mit anderen Verantwortlichen, als Gemeinsamer Verantwortlicher im Sinne von Artikel 4 Nr. 7 und Artikel 26 Abs. 1 DSGVO abzusehen.

   Was erstens die Zwecke einer solchen Verarbeitung pbD betrifft, ergibt sich für den EuGH – vorbehaltlich der vom vorlegenden Gericht vorzunehmenden Prüfungen –, dass das von IAB Europe eingerichtete TCF einen Regelungsrahmen darstellt, der sicherstellen soll, dass die Verarbeitung pbD eines Nutzers einer Webseite oder App durch bestimmte Wirtschaftsteilnehmer, die an der Online-Versteigerung von Werbeflächen teilnehmen, mit der DSGVO in Einklang steht.

   Unter diesen Umständen soll das TCF im Wesentlichen den Verkauf und den Kauf von Werbeflächen im Internet durch diese Wirtschaftsteilnehmer fördern und ermöglichen.

   Vorbehaltlich der Prüfung des nationalen Gerichts im Einzelfall kann daher davon ausgegangen werden, dass IAB Europe aus Eigeninteresse auf die hier relevanten Verarbeitungen pbD Einfluss nimmt und damit gemeinsam mit seinen Mitgliedern die Zwecke solcher Verarbeitungsvorgänge festlegt.

Ausblick

Die Entscheidung des EuGH überrascht wenig. Der EuGH führt seine Rechtsprechung fort. Daher ist es weiterhin wichtig festzuhalten, dass der EuGH keine klare Entscheidung in Richtung „absoluter Personenbezug“ oder „relativer Personenbezug“ trifft. Dies war hier wohl auch nicht nötig, weil Mitglieder des IAB Europe verpflichtet sind, Informationen zu Nutzern zur Verfügung zu stellen und diese Nutzer dann jedenfalls identifizierbar sind.

Die Argumentation in Richtung einer Gemeinsamen Verantwortlichkeit überrascht ebenfalls wenig.

Aus praktischer Sicht sind die Anforderungen an Datenschutzhinweise und datenschutzrechtliche Marketingeinwilligungen im Rahmen des Real Time Bidding-Verfahrens (weiterhin) hoch. Werbetreibende stehen vor hohen Herausforderungen. Zum einen ist es eine Herausforderung, die transparente Darstellung aller Player in einem digitalen und dynamischen Werbe-Ökosystem, in welchem Real Time Bidding genutzt wird, zu erreichen. Zum anderen ist die transparente Vorformulierung für eine entsprechende datenschutzrechtliche Marketingeinwilligung eine Herausforderung.

Ob der IAB Europe sein TCF (es gibt verschiedene Versionen) weiterentwickelt und den Ansatzpunkten des EuGH den Boden entzieht bzw. entziehen kann, bleibt abzuwarten. Für die digitale Werbeindustrie wäre es jedenfalls den Versuch wert. Zudem werden auch andere Anbieter für digitale Werbe-Ökosysteme prüfen müssen, inwieweit diese EuGH-Entscheidung auf ihre Konstruktionen anwendbar ist.

Dr. Elisabeth von Finckenstein
Dr. Stefan Peintinger

EuGH - Ängste und Sorgen ausreichend für immateriellen Schadensersatz!

Nachdem der Europäische Gerichtshof im Mai diesen Jahres noch im Sinne der Wirtschaft geurteilt hat, dass der bloße Datenschutzverstoß nicht ausreichend für einen Anspruch auf Schadensersatz ist (siehe unseren Beitrag), musste er nun konkreter werden und urteilen, was als immaterieller Schaden anerkannt werden kann (Urteil vom 14. Dezember 2023, Rs. C-340/21).

Ausgangsfall

Im Jahr 2019 wurde eine bulgarische Behörde Opfer eines Cyberangriffs, bei welchem die unbekannten Angreifer sich Zugang zu Steuer- und Sozialversicherungsdaten von Millionen von Personen verschafft haben. Die Daten sollen anschließend laut Medienberichten im Internet veröffentlich worden sein. Daraufhin klagten mehrere hundert betroffene Personen auf Ersatz des immateriellen Schadens, der sich aus der Offenlegung der personenbezogenen Daten ergeben haben soll. Die Klägerin im Ausgangsverfahren machte geltend, dass ihr immaterieller Schaden in der Befürchtung besteht, dass ihre personenbezogenen Daten künftig missbräuchlich verwendet würden oder dass sie selbst erpresst, angegriffen oder sogar entführt werde.

Der EuGH wurde durch das bulgarische Berufungsgericht angerufen, um unter anderem folgende Fragen zu klären:

1. Stellt allein die Tatsache, dass Angreifer Daten ausspähen konnten, ein Datenschutzverstoß dar?
2. Besteht ein ersatzfähiger immaterieller Schaden bereits in Sorgen, Ängsten und Befürchtungen über einen möglichen zukünftigen Missbrauch?

Entscheidung

Während der EuGH die erste Frage im Ergebnis verneint hat, wurde ein Schadensersatzanspruch bereits bei Ängsten und Befürchtungen nicht kategorisch ausgeschlossen.

1. *Kein Datenschutzverstoß, wenn der Verantwortliche ausreichende Sicherungsmaßnahmen getroffen hat*
   Der EuGH betont erneut, dass Voraussetzung für einen Schadensersatzanspruch zunächst ein Datenschutzverstoß sei. Ein solcher liege nicht automatisch vor, wenn Dritte sich unbefugt Zugang zu personenbezogenen Daten verschafft haben. Die DS-GVO verlange vom Verantwortlichen lediglich, dass dieser ausreichende technische und organisatorische Maßnahmen träfe, die darauf gerichtet sind, jede Verletzung des Schutzes personenbezogener Daten so weit wie möglich zu verhindern. Nationale Gerichte müssten im Einzelfall durch geeignete Beweiserhebungen prüfen, ob der Verantwortliche ausreichende Maßnahmen ergriffen hat, die speziell mit der betreffenden Verarbeitung sowie den davon ausgehenden Risiken verbunden sind. Die Beweislast liege insofern beim Verantwortlichen.

Damit wird Unternehmen schon auf der ersten Stufe der Prüfung die Möglichkeit eröffnet, einen Schadensersatzanspruch abzuwehren. Dies erfordert jedoch, dass die ergriffenen Maßnahmen ausreichend dokumentiert und begründet sind.

2. *Befürchtungen grundsätzlich als immaterieller Schaden anerkannt*
   Nach der für Unternehmen positiven Beantwortung der ersten Vorlagefragen, wird der EuGH allerdings wieder verbraucherfreundlicher. Unter Auslegung des Wortlauts des DS-GVO hat der EuGH entschieden, dass Sorgen, Ängste oder Befürchtungen eines zukünftigen Missbrauchs einen immateriellen Schaden darstellen können.

   Diese Entscheidung ist von hoher praktischer Relevanz, da Ängste und Befürchtungen in der Regel die erste Reaktion von betroffenen Personen sein dürften, wenn Sie vom Verlust ihrer Daten durch einen Cyberangriff erfahren, unabhängig davon, ob es später tatsächlich zu einem Missbrauch kommt. Schon heute werden in jedem Schadensersatzprozess aufgrund eines Datenschutzverstoßes Ängste und Sorgen der betroffenen Person erwähnt. Deutsche Gerichte standen dieser Argumentation bislang eher abweisend gegenüber.

Wichtig ist es jedoch, dass auch der EuGH einschränkend darauf hinweist:

„[…] dass eine Person, die von einem Verstoß gegen die DSGVO betroffen ist, der für sie negative Folgen gehabt hat, nachweisen muss, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 DSGVO darstellen (vgl. in diesem Sinne Urteil vom 4. Mai 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, EU:C:2023:370, Rn. 50).

Insbesondere muss das angerufene nationale Gericht, wenn sich eine Person, die auf dieser Grundlage Schadenersatz fordert, auf die Befürchtung beruft, dass ihre personenbezogenen Daten in Zukunft aufgrund eines solchen Verstoßes missbräuchlich verwendet werden, prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann.“ (Hervorhebungen nicht im Original)

Betroffene Personen müssen somit ihre Ängste, Sorgen und Befürchtungen auch beweisen können. Eine pauschale Behauptung – wie in Masseverfahren üblich – ist für die Darlegung nicht ausreichend. Insbesondere bei hohen Schadensersatzforderungen liegt häufig der Verdacht nahe, dass es die Kläger vor allem finanzielle Interessen und keinen erlittenen Schaden haben.

<u>Praxishinweis</u>

Das Urteil des EuGH vom 14. Dezember 2023 bringt mehr Klarheit und gibt auch deutschen Gerichte klarere Hinweise für die Entscheidung. Es sind allerdings noch weitere Fragen mit Bezug zum Schadensersatz nach Art. 82 DS-GVO offen, insbesondere zur Höhe des Schadensersatzes oder weitere „gefühlte“ Beeinträchtigungen. Wir werden die ausstehenden Entscheidungen des EuGH insofern weiter eng beobachten und Sie informiert halten.

Aufgrund des vorliegenden Urteils sollten Unternehmen prüfen, ob ihre ergriffenen technischen und organisatorischen Maßnahmen ausreichend dokumentiert und auch begründet sind. Zur Abwehr von Schadensersatzansprüchen müssen Unternehmen darlegen können, warum sie die ergriffenen Maßnahmen für ausreichend erachtet haben. Gerne beraten und unterstützen wir Sie dabei mit unseren Spezialisten.

Zudem werden auf Massenverfahren spezialisierte Anwaltskanzleien dieses Urteil aufgreifen, um nach größeren Cyberangriffen Schadensersatzansprüche für betroffene Personen geltend zu machen. Unternehmen sind hier gut beraten, ebenfalls frühzeitig Kontakt zu auf Massenverfahren spezialisierte Wirtschaftskanzleien aufzunehmen, um sich gegen diese Ansprüche erfolgreich zur Wehr zu setzen. Unser Team aus spezialisierten Anwälten und LegalTech-Experten berät und unterstütz Sie gerne.

Nikolaus Bertermann
Dr. Oliver Hornung
Franziska Ladiges

Kann ein Verstoß gegen die DS-GVO zu einem Bußgeld gegen eine juristische Person führen?

Lange erwartet und nunmehr geurteilt. Der Europäische Gerichtshof (EuGH) hat in der Rechtssache „Deutsche Wohnen“ (Az. C-807/21) die Voraussetzungen konkretisiert, unter welchen eine nationale Aufsichtsbehörde ein Bußgeld aufgrund eines Verstoßes gegen datenschutzrechtliche Bestimmungen gegenüber einer juristischen Person verhängen darf. Hintergrund der Entscheidung war ein im Jahr 2019 von der Berliner Datenschutzaufsichtsbehörde gegen die Immobiliengesellschaft Deutsche Wohnen verhängtes Bußgeld in Höhe von ca. 14 Mio. Euro. Behauptet wurden insoweit verschiedene Verstöße gegen die DS-GVO im Zusammenhang mit Mieterdaten. Dreh- und Angelpunkt der Entscheidung war sodann die Frage, ob ein entsprechendes Bußgeld – wie dies im deutschen Ordnungswidrigkeitengesetz (OWiG) in § 30 festgehalten ist – das Verschulden einer Leitungsperson voraussetzen.

Was sind die Kernaussagen des EuGH?

- Im Falle des Verstoßes gegen die DS-GVO kann ein Bußgeld unmittelbar gegenüber der verantwortlichen Stelle (auch im Falle einer juristischen Person) verhängt werden.
- Nur schuldhafte (also vorsätzliche oder fahrlässige) Verstöße gegen die DS-GVO können mit einem Bußgeld sanktioniert werden.
- Für die Klärung der Verschuldensfrage kommt es weder auf das Handeln noch auf die Kenntnis einer Leitungsperson an. Dies bedeutet, dass das Fehlverhalten etwa aller Beschäftigten von Relevanz sein kann.

Was bedeutet dies für die Praxis?

Aus wirtschaftlicher Sicht erfreulich ist zunächst die Tatsache, dass die DS-GVO keine verschuldensunabhängige Verhängung eines Bußgeldes vorsieht. Es muss stets im jeweiligen Einzelfall nachgewiesen werden, dass ein schuldhafter Verstoß gegen die DS-GVO begangen wurde.

Dies darf jedoch nicht zu der Fehlannahme führen, in Zukunft sei mit insgesamt weniger Bußgeldverfahren wegen Verstößen gegen die DS-GVO zu rechnen. Da letztlich sämtliche natürlichen Personen im Unternehmen schuldhaft (also vorsätzlich oder auch nur fahrlässig) gegen datenschutzrechtliche Bestimmungen verstoßen können, bleibt eine solide Datenschutz-Compliance stets das effektivste Mittel gegenüber lästigen Auseinandersetzungen mit den Aufsichtsbehörden. Auch ist es aus rechtlicher Sicht nicht abschließend geklärt, welche Anforderungen an einen entsprechenden Verschuldensnachweis zu stellen sind und wie Verstöße bei einem Auftragsverarbeiter behandelt werden müssen.

Die Entscheidung des EuGH sollte daher jedenfalls als Anlass genommen werden, die internen Regelungen zum Datenschutz nochmal auf den Prüfstand zu stellen. Liegt bspw. ein (aktuell gehaltenes) Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DS-GVO vor, mittels welchen die Grundsätze aus Art. 5 Abs. 1 DS-VO geprüft und entsprechend nachgewiesen werden können? Werden Beschäftigte im Unternehmen regelmäßig zum Datenschutz geschult?

Man kann sicherlich viel und lange zu den dogmatischen Fragen um das Sanktionsregime der DS-GVO diskutieren. Hierbei sollte jedoch der vielleicht wichtigste Schritt nicht vergessen werden: Die Sicherstellung einer soliden Datenschutz-Compliance. Häufig sind es die einfachen Maßnahmen im Unternehmen, die viel Ärger vermeiden können.

Marius Drabiniok
Dr. Oliver Hornung
Franziska Ladiges

Die Uhr tickt – der EU Data Act ist in Kraft

Der EU Data Act (VERORDNUNG (EU) 2023/2854) ist am 11.01.2024 in Kraft getreten. Insbesondere für Hersteller vernetzter Produkte und Anbieter verbundener Dienste läuft damit die Frist zur Umsetzung der neuen Vorgaben zum fairen Datenzugang und zur fairen Datennutzung.

Der Data Act wird mit Ablauf von 20 Monaten, also im September 2025 verbindlich. Für einzelne Anforderungen gilt eine etwas längere Umsetzungsfrist von 32 Monaten. Der Data Act gilt als Verordnung unmittelbar in allen EU-Mitgliedsstaaten. Eine Umsetzung in nationales Recht ist also nicht erforderlich.

Mit dem Data Act sollen gesetzliche, wirtschaftliche und technische Hemmnisse für die Data Economy möglichst beseitigt werden.

Dazu schafft der Data Act etwa einen Anspruch auf Datenzugang: Danach muss Nutzern vernetzter Produkte und verbundener Dienste Zugang zu den Daten gewährt werden, die bei ihrer Verwendung des Produkts oder Dienstes generiert werden. Dies betrifft sowohl vernetzte Verbraucherprodukte, wie etwa Wearables oder Smart-Home-Devices, aber auch rein gewerblich genutzte Produkte oder und Dienste, von der vernetzten Landwirtschaftsmaschine bis zur IoT-Industrieanlage. Der Anspruch auf Datenzugang richtet sich gegen den „Dateninhaber“, also den Hersteller des vernetzten Produkts beziehungsweise Anbieter des verbundenen Dienstes.

Zudem führt der Data Act ein Recht der Nutzer auf Datenportabilität ein, verpflichtet Produkthersteller und Diensteanbieter zur Information über die bei Nutzung der Produkte und Dienste jeweils generierten Daten und enthält inhaltliche Vorgaben für Verträge zur Datenlizenzierung, vergleichbar dem AGB-Recht. Details zum Data Act haben wir als Überblick hier zusammengefasst.

Der Data Act selbst unterscheidet für die datenbezogenen Ansprüche und Pflichten zunächst nicht zwischen personenbezogenen und nicht-personenbezogenen Daten. Für Herausgabe und Nutzung personenbezogener Daten gelten jedoch zusätzlich die Vorgaben der DSGVO. Zudem sind etwa Geschäftsgeheimnisse der Hersteller und Anbieter vom Anspruch der Nutzer auf Datenzugang ausgenommen.

Dr. Daniel Meßmer
Dr. Stefan Peintinger