Newsletter IP/IT

August 2025

Inhalt

Positionspapier der Datenschutzkonferenz zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen

Der Zusammenschluss der deutschen Datenschutzaufsichtsbehörden, die Datenschutzkonferenz (DSK) hat kürzlich eine Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen veröffentlicht.

Die DSK formuliert darin umfassende Anforderungen, mit dem Ziel, datenschutzrechtliche Vorgaben, insbesondere die der Datenschutz-Grundverordnung (DSGVO), konsequent umzusetzen und somit die Rechte und Freiheiten natürlicher Personen zu schützen. Die Orientierungshilfe richtet sich primär an Hersteller und Entwickler von KI-Systemen, bietet jedoch auch Verantwortlichen, die solche Systeme einsetzen, wertvolle Hinweise.

Technische und organisatorische Anforderungen an KI-Systeme entlang des Lebenszyklus eines KI-Systems

Die DSK unterteilt den Lebenszyklus eines KI-Systems in folgende zentrale Phasen: Designphase, Entwicklungsphase, Einführungsphase sowie Betriebs- und Monitoringphase. Jede dieser Phasen erfordert spezifische technische und organisatorische Maßnahmen, um die datenschutzrechtlichen Anforderungen der DSGVO zu erfüllen.

Zur Einhaltung der Anforderungen orientiert sie sich an den Gewährleistungszielen Datenminimierung, Verfügbarkeit, Vertraulichkeit, Integrität, Intervenierbarkeit, Transparenz und Nichtverkettung (Art. 5 und 32 DSGVO). Im Folgenden werden ausgewählte Gewährleistungsziele anhand der Lebensphasen eines KI-Systems im Überblick dargestellt.

Designphase

In der Designphase werden grundlegende Entscheidungen über die Architektur des KI-Systems getroffen. Der Grundsatz „Data Protection by Design“ soll den Datenschutz von Anfang an berücksichtigen. Um der Datenminimierung gerecht zu werden, dürfen nur die für den Zweck des KI-Systems erforderlichen Daten erhoben werden. Da das Training einer KI eine Verarbeitung im Sinne der DSGVO darstellt, muss bei der Verarbeitung personenbezogener Daten eine einschlägige Rechtsgrundlage vorhanden sein. Zudem muss dokumentiert werden, wo Daten erhoben, gespeichert und verarbeitet werden. Bereits hier sollten Verschlüsselungstechniken sowie rollenbasierte Zugriffskontrollen als Sicherheitsmaßnahmen eingeplant werden, um unbefugten Zugriff auf sensible Daten zu verhindern. Bei der Auswahl der technischen Grundlage des KI-Modells ist zu beachten, dass dieses nach einer Löschanfrage entsprechend angepasst werden muss, um personenbezogene Daten zu entfernen. Hierfür sollen, sofern möglich, die personenbezogenen Daten im KI-Modell direkt identifiziert und entfernt werden. Alternativ können Techniken des Machine Unlearning oder des Fine-Tuning zum Einsatz kommen.

Entwicklungsphase

Die Rohdaten müssen in der Entwicklungsphase aufbereitet werden. Außerdem ist das KI-Modell zu trainieren und zu validieren. Die zuvor angedachten Schutzmechanismen sind umzusetzen. Personenbezogene Daten, die für das KI-Modell zwingend notwendig sind, sind zu anonymisieren oder zu pseudonymisieren. Der Verantwortliche hat zu dokumentieren, welche personenbezogenen Rohdaten er zu Trainingsdaten verarbeitet. Es sind Informationspflichten über Verarbeitungszwecke, Datenempfänger und Speicherfristen festzulegen, damit der Verantwortliche seine Transparenzpflicht erfüllen kann. Er muss die Integrität des trainierten KI-Modells und der Trainings-, Validierungs- und Testdaten sicherstellen. Darüber hinaus muss er die Qualität der Ausgaben prüfen und sicherstellen, dass keine Rückschlüsse auf personenbezogene Ergebnisse oder eine Identifizierung einer Person aus den zugrundeliegenden Daten möglich sind.

Einführungsphase

Die Einführungsphase umfasst die Verteilung der Software sowie deren Konfiguration für den Produktivbetrieb. Vor der Freigabe des Systems müssen datenschutzfreundliche Voreinstellungen implementiert werden - „Data Protection by Default“. Damit geht auch eine Dokumentation einher, die auch für Nicht-Entwickler verständlich sein soll. Dies betrifft insbesondere die Konfiguration von Zugriffsrechten und Protokollierungsmechanismen.

Betriebs- und Monitoringphase

In dieser Phase wird das KI-System in seiner Produktivumgebung aktiv genutzt und ist kontinuierlich zu überwachen. Alle relevanten Aktivitäten im System sollten protokolliert werden, um die Nachvollziehbarkeit zu gewährleisten. Regelmäßige Prüfungen sind notwendig, um sicherzustellen, dass das System den definierten Standards weiterhin entspricht. Für Systeme mit hohem Risiko müssen Mechanismen zur Risikobewertung implementiert sein. Es ist auch darauf zu achten, dass nur relevante personenbezogene Daten herausgegeben werden.

Besondere Bedeutung kommt hier der Intervenierbarkeit zu. Bei entscheidungsunterstützenden KI-Systemen sind Einwirkungsmechanismen zu implementieren, die eine fundierte menschliche Entscheidung ermöglichen. Darüber hinaus sind die Betroffenenrechte nach Art. 15, 16, 17 und 18 DSGVO zu wahren. Es muss möglich sein, unrichtige personenbezogene Trainingsdaten auf Verlangen eines Betroffenen zu berichtigen. Ein Löschungsanspruch eines Betroffenen muss mithilfe der in der Designphase implementierten technischen Lösungen umgesetzt werden, wobei der Erfolg nachgewiesen werden muss. Ein Ausgabefilter stellt keine Löschung dar.

Fazit und Handlungsempfehlung

Angesichts der meist sehr großen Datenmengen, die sowohl für die Entwicklung als auch für das laufende Training und die Aktualisierung von KI-Systemen erforderlich sind, ist es für Unternehmen unerlässlich, von Anfang an die Vorgaben des Datenschutzrechts konsequent zu beachten und „mitzudenken“. Nur so lassen sich die Rechte und Freiheiten betroffener Personen wirksam schützen und haftungsrechtliche Risiken verringern. Die Ausführungen der DSK können dabei eine wertvolle Orientierung bieten und sollten bei der Planung und Entwicklung von KI-Systemen berücksichtigt werden.

Europäischer Datenschutzausschuss konkretisiert Anforderungen an Unternehmen beim Einsatz von Auftragsverarbeitern und Unterauftragsverarbeitern

Der Europäische Datenschutzausschuss (EDSA) veröffentlichte Ende 2024 eine richtungsweisende Stellungnahme zu den Pflichten von Verantwortlichen beim Einsatz von Auftragsverarbeitern und Unterauftragsverarbeitern. Die Stellungnahme konkretisiert zentrale Auslegungsfragen zu Art. 28 Datenschutz-Grundverordnung (DSGVO) und enthält praxisrelevante Empfehlungen zur Anpassung unternehmensinterner Datenschutzprozesse.

Bisher besteht häufig Unsicherheit über die Reichweite des datenschutzrechtlichen Verantwortlichen bei der (Unter-)Auftragsverarbeitung. In der Praxis verarbeitet der Verantwortliche die personenbezogenen Daten im Rahmen seiner Geschäftstätigkeit häufig nicht ausschließlich allein, sondern beauftragt hierfür externe Dienstleister (sog. „Kettenverarbeitung“). Mit dieser hat sich der Ausschuss nun befasst und dabei erörtert, inwiefern der Verantwortliche hierbei weiterhin verantwortlich bleibt. Darüber hinaus hat sich der Ausschuss mit der Identifizierung der (Unter-)Auftragsverarbeitern, den Prüfungs- und Kontrollpflichten sowie der Drittlandübermittlung befasst.

Überblick (Unter-)Auftragsverarbeitung

Art. 28 DSGVO regelt die rechtlichen Beziehungen zwischen dem Verantwortlichen, dem Auftragsverarbeiter und etwaigen Unterauftragsverarbeitern. Eine Auftragsverarbeitung liegt vor, wenn ein Verantwortlicher – etwa ein Unternehmen – einen externen Dienstleister (Auftragsverarbeiter) mit der Verarbeitung personenbezogener Daten ausschließlich auf Grundlage seiner Weisungen betraut. Typische Anwendungsfälle sind IT-Dienstleister, Cloud-Anbieter oder externe Lohnbuchhaltungen, die im Auftrag und unter Kontrolle des Verantwortlichen tätig werden. Der Auftragsverarbeiter ist verpflichtet, die Daten ausschließlich weisungsgebunden zu verarbeiten und darf sie nicht für eigene Zwecke nutzen.

Von einer Ketten- oder Unterauftragsverarbeitung spricht man, wenn der ursprünglich beauftragte Auftragsverarbeiter seinerseits weitere Dienstleister zur Erfüllung einzelner Verarbeitungsschritte hinzuzieht – beispielsweise wenn ein IT-Dienstleister wiederum die Cloud-Services eines Dritten verwendet. Die DSGVO gestattet den Einsatz von (Unter-) Auftragsverarbeitern nur dann, wenn diese hinreichende Garantien für die Einhaltung angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten bieten (Art. 28 Abs. 4 DSGVO).

Zentrale Anforderungen laut EDSA

Transparenz in der Verarbeitungskette: Wer muss identifiziert werden?

Verantwortliche müssen jederzeit Kenntnis über die Identität aller eingesetzten Auftragsverarbeiter und Unterauftragsverarbeiter entlang der gesamten Verarbeitungskette haben, und zwar nicht nur über die erste Ebene. Dazu gehören Name, Anschrift, Ansprechpartner und eine Beschreibung der jeweiligen Verarbeitungstätigkeit. Dies gilt unabhängig von dem mit der Verarbeitungstätigkeit verbundenen Risiko.

Bereits bei Vertragsschluss sollte eine vollständige Liste aller genehmigten (Unter-)Auftragsverarbeiter vorliegen, die regelmäßig aktualisiert wird. Diese Transparenz ist auch für die Erfüllung von Auskunftsersuchen und im Fall von Datenschutzverletzungen essenziell.

Überprüfungspflicht: Wie tief muss geprüft werden?

Der Verantwortliche ist gemäß Art. 5 Abs. 1 DSGVO für die Einhaltung der Datenschutzgrundsätze verantwortlich und muss deren Einhaltung nachweisen können (Grundsatz der Rechenschaftspflicht). Das gilt auch, wenn er Auftragsverarbeiter oder Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten in seinem Namen betraut, und zwar für die gesamte Verarbeitungskette.

Nach Ansicht des EDSA müssen Verantwortliche prüfen und dokumentieren, ob alle (Unter-)Auftragsverarbeiter „hinreichende Garantien“ für die Einhaltung der DSGVO bieten. Die Prüfungspflicht besteht unabhängig vom mit der jeweiligen Verarbeitung verbundenen Risiko. Dagegen kann jedoch der Umfang der Prüfung je nach Risikoeinschätzung variieren. Bei geringem Risiko genügt eine weniger eingehende Prüfung, während bei hohem Risiko eine vertiefte Prüfung bis hin zur Einsicht in Unterauftragsverträge erforderlich sein kann. Grundsätzlich darf sich der Verantwortliche dabei auf die Informationen verlassen, die er vom „ersten“ Auftragsverarbeiter in der Verarbeitungskette erhält. Eine systematische Einsichtnahme in sämtliche Unterauftragsvereinbarungen ist nicht zwingend erforderlich, es sei denn, es bestehen Zweifel an der Einhaltung datenschutzrechtlicher Vorgaben oder eine Aufsichtsbehörde verlangt dies.

Drittlandübermittlungen: Besondere Anforderungen bei internationalen Datenflüssen

Werden personenbezogene Daten durch einen (Unter-)Auftragsverarbeiter in ein Drittland übermittelt, verbleibt der Verantwortliche für das Schutzniveau verantwortlich. Es gelten sowohl die Pflichten aus Art. 44 ff. DSGVO als auch aus Art. 28 Abs. 1 DSGVO. Durch die Übermittlung darf der durch die DSGVO garantierte Schutz personenbezogener Daten nicht untergraben werden.

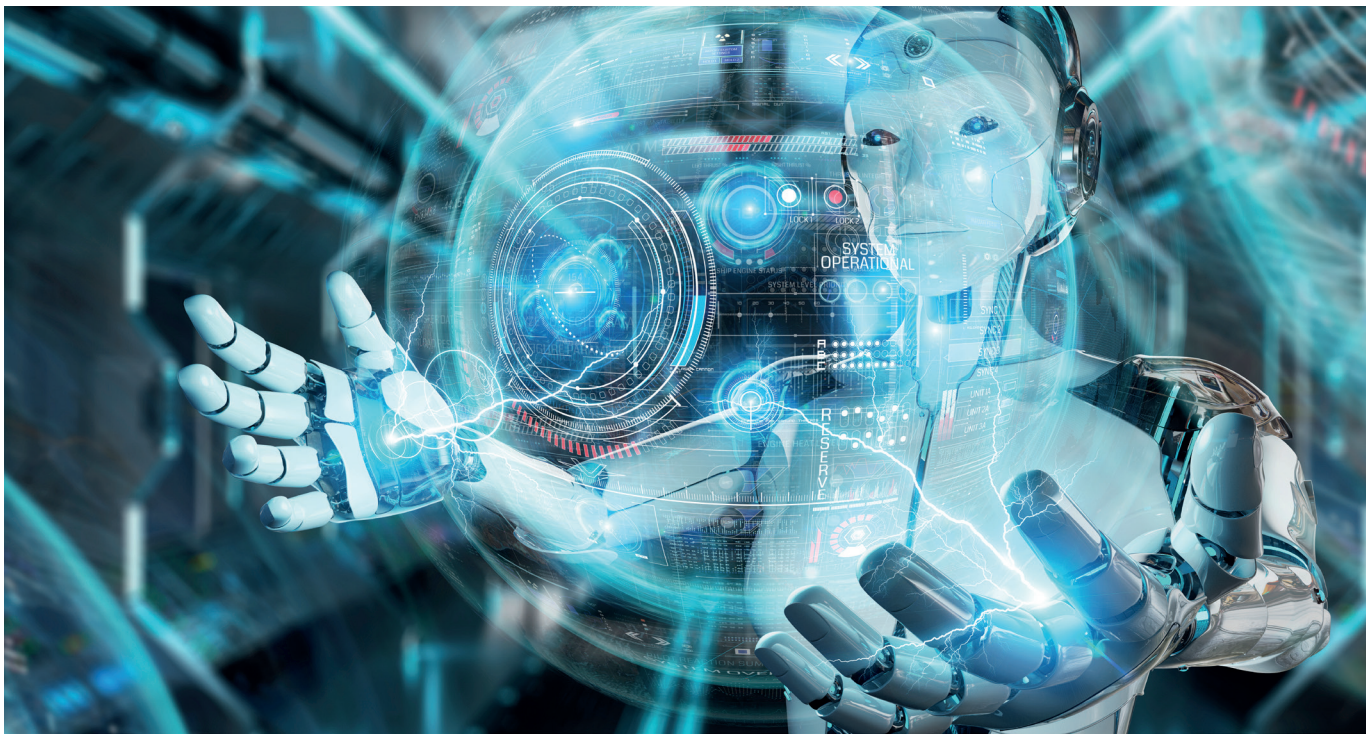
Praktische Schwierigkeiten bei der Kontrolle der Einstellung von Unterauftragsverarbeitern durch den Auftragsverarbeiter (insbes. bei Drittlandübermittlung) entbinden den Verantwortlichen nicht von seinen Pflichten zur Sicherstellung eines angemessenen Datenschutzniveaus. Die Übermittlung ist zu dokumentieren und einer Prüfung durch den Verantwortlichen zu unterziehen. Der EDSA empfiehlt hierzu ein zweistufiges Vorgehen. Unabhängig vom Übermittlungsgrund sollte der Verantwortliche in einem ersten Schritt volle Kenntnis von allen beabsichtigten Übermittlungen haben (sog. „Know your Transfers“). Hierzu sollte er sicherstellen, dass eine Übermittlungskartierung durch den (Unter-)Auftragsverarbeiter vorgenommen wird. Aus dieser muss hervorgehen, welche personenbezogenen Daten übermittelt werden, wohin und für welchen Zweck. Im zweiten Schritt ist zu prüfen, auf welcher Rechtsgrundlage eine Übermittlung erfolgt und ob im Drittland hinreichende Garantien für den Datenschutz bestehen.

Fazit und Handlungsempfehlungen für Unternehmen

Die EDSA-Stellungnahme verschärft die Anforderungen an Transparenz, Kontrolle und Dokumentation beim Einsatz von (Unter-)Auftragsverarbeitern erheblich. Letztlich bleibt der Verantwortliche für jeden Verstoß im Zusammenhang mit dem Einsatz von (Unter-)Auftragsverarbeiter verantwortlich und kann dafür haftbar gemacht werden. Eine stets aktuelle Liste aller eingesetzten (Unter-)Auftragsverarbeiter sowie eine fortlaufende Überprüfung der hinreichenden Garantien – angepasst an das jeweilige Risiko – ist unerlässlich. Vertragliche Prüf- und Einsichtsrechte in Unterauftragsvereinbarungen ermöglichen es, diesen Pflichten nachzukommen.

Handreichung HmbBfDI zum Data Act und Überblick über die Vorgaben des Data Acts für SaaS-Verträge und andere Cloud-Verträge

Am 12. September 2025 treten die wesentlichen Regelungen der Verordnung (EU) 2023/2854 (Data Act) in Kraft. Der Data Act regelt den Zugang zu und die Nutzung von Daten innerhalb der EU. Ziel des Data Act ist es, bestehende Datenmonopole aufzubrechen, den Zugang zu Daten für verschiedene Wirtschaftsteilnehmer zu erleichtern und damit einen fairen, sicheren und innovationsfreundlichen europäischen Datenbinnenmarkt zu schaffen.



Die Verordnung bringt zahlreiche Änderungen mit sich und betrifft, durch die fortschreitende Digitalisierung, nahezu alle Lebensbereiche und Produkte. Im Folgenden wollen wir anhand der kürzlich veröffentlichten Handreichung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) einen Überblick über die wesentlichen Regelungen des Data Acts geben und anschließend dessen Auswirkungen auf SaaS- und Cloud-Verträge darstellen.

Die Handreichung des HmbBfDI

Anwendungsbereich

Vom Anwendungsbereich sind insbesondere Hersteller, Dateninhaber und Nutzer vernetzter Produkte oder verbundener Dienste (Art. 1 Abs. 3 Data Act) betroffen. Erfasst sind alle „smarten“ Produkte – von Fitnessuhren und Smartphones bis hin zu landwirtschaftlichen Maschinen mit Sensorik –, sofern diese Umgebungs- oder Nutzungsdaten an den Hersteller oder Dritte übermitteln (Art. 2 Nr. 5 Data Act). Diese Umgebungs- und Nutzungsdaten werden mithilfe sogenannter verbundener Dienste dazu genutzt, das vernetzte Produkt zu betreiben und zu optimieren (Art. 2 Nr. 6 Data Act). Zu den verbundenen Diensten zählen beispielsweise Betriebssysteme, Steuerungssoftware oder Navigationsdienste.

Neu ist die ausdrückliche Einbeziehung nicht-personenbezogener Daten als Gegenstück zu den personenbezogenen Daten der DSGVO. Beide gelten als „Daten” im Sinne des Art. 2 Abs. 1 Data Act. Der Anwendungsbereich ist daher weit gefasst.

Zentrale Rechtspflichten

Eine der zentralen Pflichten des Data Acts ist die Zugänglichmachung der bei der Nutzung von vernetzten Produkten oder verbundenen Diensten erzeugten Daten („Access by Design", Art. 3 Abs. 1 Data Act). Vernetzte Produkte und die damit verbundenen Dienste müssen so gestaltet sein, dass die dabei entstehenden Daten – einschließlich relevanter Metadaten – für Nutzer standardmäßig leicht, sicher, kostenlos und in einem gängigen, maschinenlesbaren Format zugänglich sind.

Darüber hinaus verpflichtet der Data Act die Anbieter dazu, vor Vertragsabschluss, beispielsweise beim Kauf, der Miete oder dem Leasing eines Internet-of-Things-Produkts, bestimmte Informationen bereitzustellen (Art. 3 Abs. 2 Data Act). Dazu zählen unter anderem Angaben zur Art, zum Format und zum geschätzten Umfang der erzeugten Daten sowie zur Fähigkeit des Produkts, Daten kontinuierlich und in Echtzeit zu generieren. Diese Informationen müssen klar und verständlich formuliert sein.

Eine weitere wesentliche Regelung ist das Recht der Nutzer und Dateninhaber auf Zugang zu den Produktdaten und den Daten verbundenen Dienste sowie das Recht auf deren Nutzung (Art. 4 Data Act). Dieses Recht soll für mehr Transparenz sorgen und gleichzeitig den fairen Wettbewerb wahren, etwa durch den Schutz von Geschäftsgeheimnissen oder innovationsbezogenen Informationen.

Zu beachten ist auch, dass Dateninhaber sogenannte „ohne Weiteres verfügbare Daten", sofern sie nicht-personenbezogen sind, nur auf Grundlage einer vertraglichen Vereinbarung mit dem Nutzer verwenden dürfen (Art. 4 Abs. 13 Data Act). „Ohne Weiteres verfügbare Daten" sind Daten, die ohne unverhältnismäßigen Aufwand aus dem Produkt oder Dienst gewonnen werden können. Daraus kann sich die Notwendigkeit ergeben, Datenlizenzverträge abzuschließen.

Schließlich regelt der Data Act auch das Recht der Nutzer, die Weitergabe ihrer Daten an Dritte zu verlangen (Art. 5 Data Act). In diesem Fall ist der Dateninhaber verpflichtet, die entsprechenden Daten auf Wunsch des Nutzers bereitzustellen.

Das Verhältnis zwischen Datenschutz und Datenzugänglichmachung

Die Pflicht zur Zugänglichmachung nach dem Data Act steht im Widerspruch zum Datenminimierungsgrundsatz der DSGVO. Hier fordert der HmbBfDI eine klare Trennung zwischen personenbezogenen und nicht-personenbezogenen Daten. Gerade bei Mischdatensätzen ist genau zu prüfen, unter welche Kategorie die Daten fallen, da bei personenbezogenen Daten der Schutz der DSGVO Vorrang hat. Die pauschale Annahme „im Zweifel personenbezogen" gilt nicht mehr. Bei der Bereitstellung personenbezogener Daten ist zu unterscheiden, ob der Anspruchsteller und die betroffene Person identisch sind oder nicht. Denn eine Bereitstellung personenbezogener Daten darf nur mit einer Rechtsgrundlage erfolgen. Im ersten Fall kann regelmäßig auf Art. 6 DSGVO abgestellt werden, wobei es bei besonderen personenbezogenen Daten (z. B. Gesundheitsdaten) einer expliziten Einwilligung bedarf. Wenn jedoch ein Dritter betroffen ist, wie etwa bei einem gemeinsam genutzten Auto, wird es komplexer. Die Handreichung schlägt als Rechtsgrundlage ein überwiegendes berechtigtes Interesse, die Pflicht zur Erfüllung eines Vertrags oder bereits bei Vertragsschluss eine Einwilligung einzuholen, die einen etwaigen Bereitstellungsanspruch trägt, vor.

Umsetzungspflichten für Unternehmen

Die Handreichung listet konkrete Maßnahmen für Unternehmen zur Umsetzung der Anforderungen auf:

- Prüfung des Anwendungsbereichs anhand gesetzlicher Kriterien;
- Erstellung einer Übersicht über vorhandene Datensätze/ Verarbeitungsverzeichnisse;
- Klärung des Personenbezugs einzelner Datensätze;
- Kennzeichnung schutzwürdiger Geschäftsgeheimnisse;
- Einrichtung technischer Schnittstellen zur Datenausgabe;
- Anpassung bestehender Verträge an neue Vorgaben;
- Vereinheitlichung von Transparenzpflichten gemäß DSGVO-Vorgaben.

Aufsichtsbehörde

Zuletzt befasst sich der HmbBfDI mit der Durchsetzung des Data Acts und der zuständigen Aufsichtsbehörde. Laut dem Referentenentwurf der alten Bundesregierung vom 5. Februar 2025 soll die Bundesnetzagentur (BNetzA) für nicht-personenbezogene Daten und die Beauftragte für Datenschutz und Informationsfreiheit (BfDI) für personenbezogene Daten zuständig sein (zweigeteilte Aufsicht). Der HmbBfDI sieht hier jedoch einen Verstoß gegen Art. 37 Abs. 3 Data Act und seine eigene Zuständigkeit. Nach Art. 37 Abs. 3 Data Act ist die für personenbezogene Daten zuständige Behörde auch für den Data Act zuständig. Sollte bis Mitte September kein entsprechendes Umsetzungsgesetz vorliegen, werden die für die jeweiligen Datenschutzbeauftragten der Länder kraft Unionsrechts zuständig.

Die Aufgaben und Befugnisse der neuen Aufsichtsbehörde umfassen insbesondere Untersuchungs-, Abhilfe-, Beratungs- und Genehmigungsbefugnisse. Auch eine Bußgeldbefugnis ist vorgesehen.

Auswirkungen des Data Act auf SaaS-Anwendungen und andere Cloud-Dienste

Im Bereich der Cloud-Dienste richtet sich der Data Act in erster Linie an Anbieter sogenannter „Datenverarbeitungsdienste". Darunter versteht der Data Act digitale Dienstleistungen, die es Kunden ermöglichen, über ein Netzwerk flexibel und bedarfsgerecht auf einen gemeinsamen Pool an konfigurierbaren, skalierbaren und elastischen Rechenressourcen zuzugreifen (Art. 2 Nr. 8 Data Act). Zu diesen Diensten zählen insbesondere die Modelle wie Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS). Kurzum: ein Großteil der heute gängigen cloudbasierten Geschäftsmodelle.

Der Data Act verpflichtet die Anbieter dazu, technische und organisatorische Maßnahmen zu ergreifen, die einen einfachen Anbieterwechsel („Cloud Switching", Kapitel VI des Data Acts) ermöglichen. Dadurch sollen Lock-in-Effekte gezielt abgebaut werden. Ziel des Data Acts ist es, Nutzerinnen und Nutzern von SaaS-Diensten mehr Kontrolle über ihre Daten zu geben und ihnen einen einfacheren und selbstbestimmteren Anbieterwechsel zu ermöglichen.

Entsprechende Vertragsklauseln müssen den Anforderungen des Art. 25 Abs. 2 Data Act entsprechen und die entsprechenden Informationspflichten gegenüber den Kunden erfüllen. Verträge müssen künftig so gestaltet sein, dass ein Wechsel ohne unfaire Verzögerungen und Hürden möglich ist. Dazu zählen beispielsweise unangemessene Kündigungsfristen – maximal zwei Monate –, lange Vertragslaufzeiten oder Wechselentgelte. Gemäß Art. 41 Data Act ist die Kommission verpflichtet, vor dem 12. September 2025 entsprechende Mustervertragsklauseln vorzulegen.

Anbieter sind bereits in der Entwicklungsphase verpflichtet eine entsprechende Schnittstelle zur Datenausgabe einzuplanen und die Systeme so zu gestalten, dass ein späterer Datenzugang technisch möglich ist. Die Systeme müssen interoperabel gestaltet werden und entsprechende Schnittstellen bereitstellen.

Fazit und Ausblick

Der Data Act bringt eine Vielzahl von Rechten und Pflichten mit sich. Ähnlich wie die DSGVO sieht der Data Act bei Verstößen Bußgelder von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes vor. Damit ist er genauso ernst zu nehmen wie die DSGVO.

Für die betroffenen Unternehmen sind die Vorgaben des Data Act hinsichtlich der erforderlichen vertraglichen und technischen Strukturen bis zum 12. September 2025 umzusetzen. Herausforderungen ergeben sich im Rahmen der Vertragsgestaltung vor allem im Hinblick auf die aktive Unterstützung der Kunden beim Anbieterwechsel. Auf technischer Ebene werden für viele Anbieter hinsichtlich Datenportabilität und Interoperabilität Anpassungen erforderlich sein. Mit Blick auf die fortschreitende Umsetzungsfrist empfiehlt es sich, diese Umstrukturierungen möglichst zeitnah anzugehen. Zudem sollten Unternehmen ihre bestehenden Verträge auf Vereinbarkeit mit dem Data Act prüfen. Dies gilt insbesondere für Klauseln, die einen Anbieterwechsel erschweren können. Zur Erleichterung der Umsetzung wird die Europäische Kommission noch vor Geltung des Data Acts unverbindliche Standardvertragsklauseln bereitstellen, die als wertvolle Orientierung für die Vertragsgestaltung dienen können.

Gleichzeitig sollten die geforderten technischen Anforderungen, wie offene Schnittstellen, maschinenlesbare Datenformate und strukturierte Exportfunktionen bereitgestellt werden.

Eine Cloud für Europa: Was bedeutet die Einführung der Microsoft EU Data Boundary für europäische Kunden von Microsoft-Diensten wie Azure, Dynamics 365 und Microsoft 365?

Hintergrund: Warum eine EU Data Boundary?

Mit der fortschreitenden Digitalisierung und dem verstärkten Einsatz von Cloud-Diensten stehen Unternehmen in Europa vor der Herausforderung, die strengen Vorgaben der Datenschutz-Grundverordnung (DSGVO) einzuhalten. Insbesondere die Frage, wo und wie personenbezogene Daten gespeichert und verarbeitet werden, ist für viele Organisationen von zentraler Bedeutung. Vor diesem Hintergrund hat Microsoft das sogenannte Programm „EU Data Boundary“ (zu Deutsch: „EU-Datengrenze“) ins Leben gerufen. Ziel dieser Initiative ist es, personenbezogene Daten von Kunden aus der Europäischen Union (EU) und der Europäischen Freihandelszone (EFTA) ausschließlich innerhalb dieser Regionen zu speichern und zu verarbeiten. Damit möchte Microsoft nicht nur die gesetzlichen Anforderungen erfüllen, sondern auch das Vertrauen europäischer Kunden in seine Cloud-Dienste stärken.

Das Programm gilt für zentrale Microsoft-Cloud-Dienste wie Azure, Microsoft 365 und Dynamics 365 und umfasst nicht nur klassische Kundendaten, sondern auch Telemetrie- und Diagnosedaten, pseudonymisierte Informationen sowie CRM-Daten. Damit soll ein umfassender Schutz für verschiedenste Datenkategorien gewährleistet werden.

Die Entwicklung der Microsoft EU Data Boundary

Die Einführung der EU Data Boundary erfolgt in drei aufeinanderfolgenden Phasen:

- **Phase 1:** Seit dem 1. Januar 2023 werden personenbezogene Kundendaten der genannten Cloud-Dienste ausschließlich in Rechenzentren innerhalb der EU/EFTA gespeichert.

- **Phase 2:** Im Januar 2024 wurde der Geltungsbereich auf Verarbeitungsvorgänge ausgeweitet. Das bedeutet, dass nun auch Analyseprozesse oder maschinelles Lernen – soweit technisch möglich – ausschließlich innerhalb Europas stattfinden.
- **Phase 3:** Seit Februar 2025 werden der technische Support sowie andere unterstützende Dienstleistungen aus der EU/EFTA heraus erbracht. Der Zugriff auf Kundendaten erfolgt dann nur noch durch Personal mit Sitz in Europa, es sei denn, der Kunde hat ausdrücklich zugestimmt oder zwingende rechtliche Gründe machen einen Zugriff von außerhalb erforderlich.

Keine absolute europäische Datensouveränität

Microsoft teilt in einem Blogbeitrag zum Abschluss der Entwicklung mit, dass sich aus der EU Data Boundary für europäische Unternehmen zahlreiche Vorteile ergeben sollen: Die Speicherung und Verarbeitung innerhalb Europas soll die Kontrolle über eigene Daten erheblich stärken und das Risiko ungewollter Übertragungen in Drittländer reduzieren. Die europäische Datenspeicherung soll zudem die Einhaltung der strengen europäischen Datenschutzanforderungen erleichtern und für mehr Transparenz sorgen. Zu beachten ist jedoch, dass einige Anwendungen und Dienste individuell konfiguriert werden müssen, damit die Datenverarbeitung und -speicherung innerhalb der EU/EFTA stattfindet.

Trotz der Einführung der Microsoft EU Data Boundary bleibt ein Restrisiko für europäische Unternehmen bestehen. Insbesondere auf Grundlage des Clarifying Lawful Overseas Use of Data Act („CLOUD Act“) bleibt es amerikanischen Behörden weiterhin erlaubt, auf Daten zuzugreifen, die US-amerikanische IT-Dienstleister verwaltet werden - selbst wenn diese Daten außerhalb der USA gespeichert sind. Hinzu kommt, dass der Foreign Intelligence Surveillance Act (FISA) die gezielte Überwachung von Personen außerhalb der USA erlaubt, solange sie keine US-Bürger sind. Nicht auszuschließen ist, dass dieser auch auf innerhalb der EU gespeicherte Daten anwendbar ist. Microsoft selbst weist darauf hin, dass für globale Sicherheitsoperationen weiterhin Datenübertragungen außerhalb der EU erforderlich sein können, etwa um Cyberangriffe zu erkennen und abzuwehren. Eine absolute Abschottung gegenüber dem Zugriff durch US-Behörden und europäische Datensouveränität ist somit aufgrund der fortbestehenden Geltung amerikanischer Gesetze für US-Unternehmen nicht gewährleistet.

Fortbestehende Datenschutzpflichten nach der DSGVO

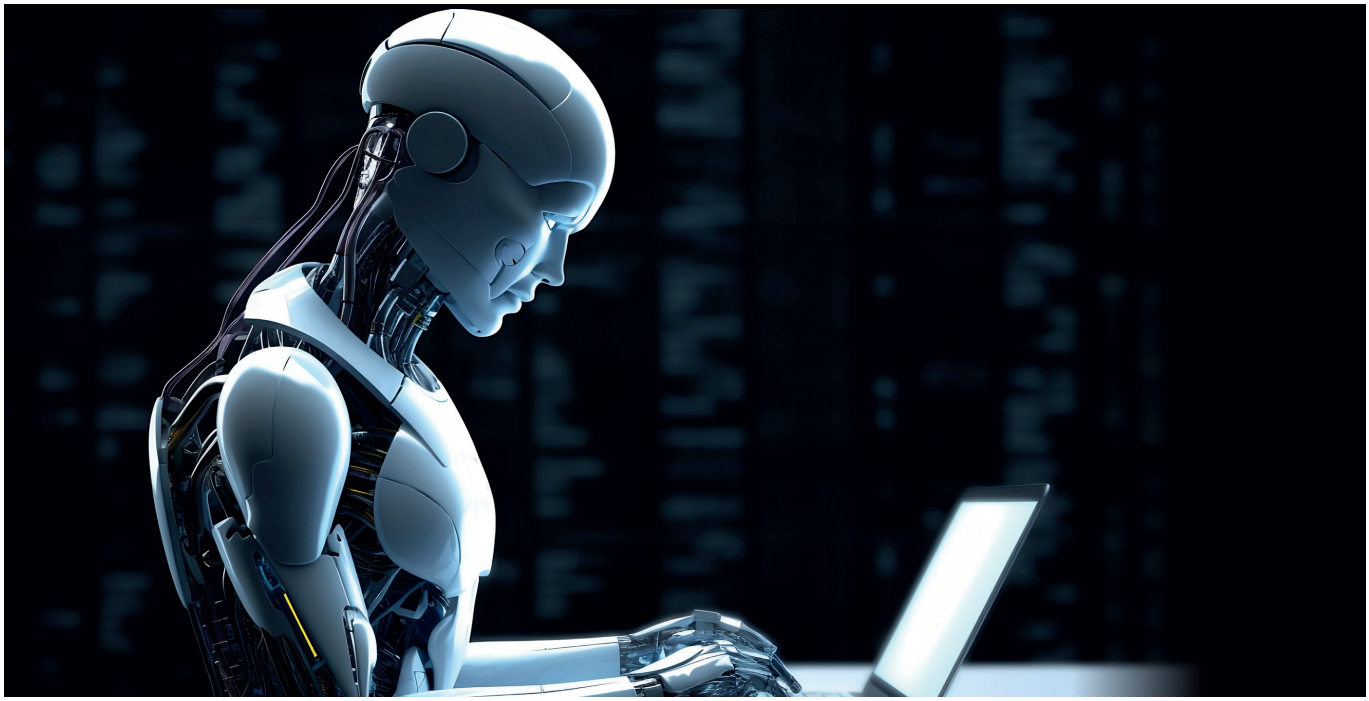
Auch mit der Einführung der Microsoft EU Data Boundary bleiben sämtliche Anforderungen der DSGVO für Unternehmen weiterhin bestehen. Die Nutzung der EU Data Boundary entbindet die Kunden nicht von ihrer eigenen Verantwortung für eine sichere Konfiguration ihrer Cloud-Dienste, um ihren Verpflichtungen aus der DSGVO nachzukommen und ihre eigenen Datenflüsse zu kontrollieren. Fehlerhafte Einstellungen können dazu führen, dass Daten dennoch außerhalb des vorgesehenen Gebiets verarbeitet werden. Microsofts EU Data Boundary ersetzt keine sorgfältige datenschutzrechtliche Analyse im Unternehmen. Die Verantwortung für die Rechtmäßigkeit der Verarbeitung, die Wahrung der Betroffenenrechte sowie die Erfüllung von Dokumentations- und Informationspflichten verbleibt grundsätzlich beim Kunden als Verantwortlichen. Der EU Data Boundary stellt somit keine Freistellung oder Haftungsübernahme durch Microsoft dar, sondern ist als zusätzliche Schutzmaßnahme Microsofts im Rahmen des bestehenden europäischen Datenschutzsystems zu verstehen, um den eigenen Verpflichtungen nachzukommen und sich als datenschutzkonformer Anbieter auf dem Markt zu etablieren.

Dazu gehört auch, dass Unternehmen ihre Datenschutzerklärungen gegebenenfalls anpassen müssen, um über die neue Datenverarbeitung innerhalb der EU/EFTA sowie über verbleibende Ausnahmen transparent zu informieren. Auch die interne Datenschutzdokumentation – insbesondere das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO – sollte aktualisiert werden, um neue Datenflüsse korrekt abzubilden.

Fazit und Ausblick

Die Einführung der Microsoft EU Data Boundary ist ein bedeutender Schritt für einen verbesserten Datenschutz und eine stärkere Kontrolle über digitale Informationen für europäische Unternehmen und Verbraucher. Sie verdeutlicht, wie internationale Anbieter auf die wachsenden Anforderungen an Datensouveränität und rechtliche Transparenz reagieren und sich den europäischen Standards anpassen. Gleichzeitig zeigt sich, dass technische und organisatorische Maßnahmen stets im Kontext globaler Rechtsrahmen betrachtet werden müssen. Für Unternehmen bleibt es daher unerlässlich, ihre Datenschutzstrategie kontinuierlich weiterzuentwickeln und an neue Entwicklungen anzupassen. Letztlich unterstreicht die Initiative die zentrale Rolle des Datenschutzes als Wettbewerbs- und Vertrauensfaktor im digitalen Zeitalter.

Aktuelle Entwicklungen im Rahmen der datenschutzkonformen Nutzung der Dienste von OpenAI, insbesondere ChatGPT



Eine aktuelle gerichtliche Verfügung in den USA verpflichtet OpenAI dazu, Nutzerdaten weiterhin zu speichern, selbst dann, wenn diese eigentlich gelöscht werden sollten. Diese Anordnung wirft bedeutende Fragen zum Datenschutz, Urheberrecht und der zukünftigen Entwicklung Künstlicher Intelligenz (KI) auf. Auch der Europäische Gerichtshof (EuGH) und das Oberlandesgericht Hamburg setzen sich derzeit im Rahmen laufender Verfahren mit diesen rechtlichen Herausforderungen auseinander.

Hintergrund

Gegenstand des Rechtsstreits vor einem New Yorker Gericht ist eine Klage mehrerer großer Verlagshäuser, darunter die New York Times, gegen OpenAI wegen Urheberrechtsverletzungen im Zusammenhang mit dem Training der OpenAI-KI-Modelle. Das Gericht hat am 13. Mai 2025 einen Beschluss erlassen, der OpenAI dazu verpflichtet, sämtliche ChatGPT-Konversationen vorerst aufzubewahren. Die Kläger argumentieren, dass ChatGPT urheberrechtlich geschützte Inhalte ihrer Artikel in Antworten wiedergebe, sodass Nutzer diese Inhalte lesen können, ohne die Originalquellen zu besuchen. Deshalb sollen nun alle Chatprotokolle – auch vom Nutzer gelöschte – (all Output Log Data) als potenzielle Beweismittel erhalten bleiben.

Wer ist betroffen?

Die gerichtliche Anordnung gilt zwar nur in den USA, betrifft aufgrund der globalen Präsenz von OpenAI auch Nutzer weltweit. Betroffen sind Nutzer der Versionen ChatGPT Free, Plus, Pro und Team sowie API-Kunden ohne spezielle Datenschutzvereinbarungen. Das betrifft auch Nutzer, die einen Auftragsverarbeitungsvertrag (AVV) mit OpenAI Ireland Limited abgeschlossen haben – zumindest solange sie nicht unter eine Zero-Data-Retention-Vereinbarung (ZDR-Vereinbarung) fallen. Nicht betroffen sind Nutzer von ChatGPT Enterprise, Edu oder diejenigen mit einer ZDR-Vereinbarung. Bei letzterem sichert OpenAI zu, Ein- und Ausgaben grundsätzlich nicht zu speichern. Diese Nutzer behalten weiterhin eine automatische Löschpraxis nach 30 Tagen.

Die ZDR-Vereinbarung steht jedoch nur bestimmten Kundengruppen, insbesondere den Enterprise-Kunden, zur Verfügung. Free-, Plus- oder Team-Pläne fallen nicht unter eine ZDR-Vereinbarung (How does Zero Data Retention work? - API - OpenAI Developer Community).

Wie reagiert OpenAI?

OpenAI kündigte an, gegen die Anordnung Berufung einzulegen, da diese gegen die eigenen Datenschutzzusagen und branchenübliche Standards verstoße (How we're responding to The New York Times' data demands in order to protect user privacy | OpenAI).

Laut OpenAI werden die nun aufzubewahrenden Daten in einem separaten, gesicherten System gespeichert, das einem sogenannten „Legal Hold", also einer rechtlichen Aufbewahrungspflicht, unterliegt. Der Zugriff sei streng auf ein kleines, geprüftes Team innerhalb von OpenAI beschränkt und erfolge nur zur Erfüllung rechtlicher Vorgaben. Auf tatsächlicher Ebene bedeutet der „Legal Hold" zunächst:

- Chats bleiben gespeichert, auch wenn Sie sie manuell löschen oder die „temporäre" Chatfunktion nutzen.
- Die Daten sind getrennt abgespeichert, gesichert und nur im Falle gerichtlicher Anforderungen zugänglich.
- Kein öffentlicher Zugriff: Die New York Times oder andere Dritte erhalten die Daten nicht automatisch. Sie müssten hierfür eine gesonderte gerichtliche Herausgabeanordnung vorlegen.
- Unklarer Endzeitpunkt: Solange das Gerichtsverfahren läuft, bleibt der Legal Hold aktiv – ein genaues Ablaufdatum gibt es nicht.

Wichtig ist die Klarstellung von OpenAI, dass diese Änderung keine Auswirkungen auf die Richtlinien zur Verwendung von Daten für das KI-Training haben soll. Nutzer können weiterhin selbst bestimmen, ob ihre Inhalte zur Verbesserung der Modelle genutzt werden dürfen.

Was bedeutet der „Legal Hold" in datenschutzrechtlicher Hinsicht?

Rechtlich steht die unbegrenzte Speicherung von Daten jedoch im direkten Widerspruch zu fundamentalen Prinzipien der europäischen Datenschutz-Grundverordnung (DSGVO). Dazu zählen vorrangig das Recht auf Vergessenwerden (Art. 17 DSGVO) und der Grundsatz der Datenminimierung (Art. 5 DSGVO). Ein US-Gerichtsbeschluss hebelt somit de facto zentrale Datenschutzrechte für europäische Bürger aus. Daher bleibt abzuwarten, wie sich die europäischen Datenschutzaufsichtsbehörden positionieren werden. Bisher haben sich die europäischen (die irische Data Protection Commission (DPC) ist für die europäische Niederlassung OpenAI Ireland Limited zuständig) und die deutschen Aufsichtsbehörden noch nicht geäußert. Seit 2023 laufen bereits Prüfungen der OpenAI Dienste unterschiedlicher Datenschutzaufsichtsbehörden.

Für die betroffenen Unternehmen entsteht dadurch ein neues relevantes Risiko bei der Nutzung von Dritt-Diensten. Die Aufbewahrung und Löschung der eigenen Daten bei Dritten, deren Dienste genutzt werden, ist ein zentraler Punkt bei der Gewährleistung der Datenschutz-Compliance. Unternehmen, die OpenAI-Dienste nutzen, stehen vor dem Problem, dass sie eigene rechtliche und vertragliche Pflichten allenfalls nicht mehr einhalten können. Das Risiko, dass ein Anbieter wie OpenAI aufgrund einer behördlichen oder gerichtlichen Verfügung bestimmte Daten aller Nutzer aufbewahren muss bzw. nicht mehr löschen darf, war bislang allerdings kein gängiger Bestandteil von Risikobeurteilungen. Das wird sich jetzt ändern müssen - nicht nur mit Blick in die USA.

Verfahren in der EU

Auch in der EU wird die Nutzung urheberrechtlich geschützter Inhalte im Rahmen des Trainings Künstlicher Intelligenz derzeit gerichtlich überprüft. In der Rechtssache C-250/25 gegen Google befasst sich der EuGH mit der Frage, ob durch KI erzeugte Texte als öffentliche Wiedergabe im Sinne des Urheberrechts gelten und ob Trainingsprozesse eine Lizenzierungspflicht auslösen. Sollte der EuGH dies bejahen, wären Unternehmen wie Google oder OpenAI künftig verpflichtet, umfassende Lizenzvereinbarungen abzuschließen – ein möglicher Wendepunkt für die europäische KI-Branche.

Das Landgericht Hamburg hat in seinem Urteil vom 27. September 2024 (Az. 310 O 227/23) die Klage eines Fotografen gegen den Verein LAION e.V. abgewiesen. Der Kläger hatte beanstandet, dass der Datensatz LAION-5B ohne seine Zustimmung urheberrechtlich geschützte Fotografien enthalte. Das Verfahren befindet sich derzeit in der Berufungsinstanz vor dem Oberlandesgericht Hamburg; eine mündliche Verhandlung ist für Oktober 2025 angesetzt.

Handlungsempfehlung

Im Ergebnis hat die Anordnung des US-Gerichts auch für einen Großteil der Nutzer in der EU erhebliche Auswirkungen auf die Beurteilung der Datenschutzkonformität der Nutzung der OpenAI-Dienste.

Trotz der angekündigten Berufung gegen die Anordnung muss OpenAI vorerst dem Beschluss Folge leisten. Solange die Anordnung Wirkung entfaltet, sollten betroffene europäische Nutzer sicherstellen, dass keine besonders sensiblen und vertraulichen Informationen sowie personenbezogene Daten von OpenAI unbegrenzt gespeichert werden.

Kurzfristig sollten schlicht keine personenbezogenen Daten, vertraulichen Informationen oder Geschäftsgeheimnisse in ChatGPT eingegeben werden. Soweit noch nicht geschehen, sollte dahingehend die Formulierung unternehmensinterner Verhaltensregeln und Richtlinien für den Umgang und die Nutzung von ChatGPT durch die Mitarbeitenden, umgesetzt werden.

Längerfristig können strategische Überlegungen hinsichtlich sog. Self-Hosting-Lösungen und Open-Source-Modellen angestellt werden. Eine Option kann der Umstieg auf interne KI-Lösungen sein. Statt ChatGPT über die Cloud zu nutzen, können Unternehmen Large Language Models auf eigenen Servern oder in einer privaten Cloud betreiben. Durch ein solches internes Hosting behalten sie die volle Kontrolle über die Daten. Open-Source-Modelle wie LLaMA, GPT-J oder GPT4All haben in letzter Zeit erhebliche Fortschritte gemacht und können daher als Alternative in Betracht kommen. Ihr Vorteil liegt neben Kostenersparnis vor allem in der Datensouveränität. Die Daten bleiben im Unternehmen, was Datenschutzrisiken erheblich reduziert. Allerdings müssen Unternehmen dafür in Expertise und Rechenressourcen investieren, und die Leistungsfähigkeit dieser Modelle kann (noch) hinter dem marktführenden GPT-4 zurückstehen.

Eine Zwischenlösung sind die Enterprise-Angebote von OpenAI mit den beschriebenen vertraglich zugesicherten Datenschutz-Features wie ZDR-Vereinbarungen und Datenverbleib in der EU-Region für europäische Kunden. Für Unternehmen, die auf OpenAI-Dienste setzen, unterstreicht dieser Fall eindrücklich den Wert einer ZDR-Vereinbarung, um die Kontrolle über die eigenen Daten und die der eigenen Kunden zu behalten. Die ZDR-Vereinbarungen gewährleisten, dass die Eingaben und Ausgaben nicht gespeichert werden, die Daten nicht für Modelltraining verwendet werden und die Daten nicht von OpenAI-Mitarbeitern eingesehen werden können.

Zuletzt sind die rechtlichen Entwicklungen im Blick zu halten, um auf neue Entscheidungen reagieren zu können. Auch die Entscheidungen der Datenschutzbehörden könnten neue Auflagen oder Einschränkungen mit sich bringen.

LAG Hessen: Datenschutzverletzung durch Betriebsratsmitglied: Ausschluss wegen Übermittlung von Beschäftigtendaten an privates Postfach

Das Landesarbeitsgericht (LAG) Hessen hat mit Beschluss vom 10. März 2025 (Az.: 16 TaBV 109/24) entschieden, dass ein schwerwiegender Verstoß eines Betriebsratsmitglieds gegen datenschutzrechtliche Pflichten einen Ausschluss aus dem Betriebsrat gemäß § 23 Abs. 1 Betriebsverfassungsgesetz (BetrVG) rechtfertigen kann. Im vorliegenden Fall hat der Vorsitzende des Betriebsrates wiederholt gegen die einschlägigen Bestimmungen der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) verstoßen.

Der Sachverhalt

Der Arbeitgeber, ein Betreiber einer Klinik mit etwa 390 Beschäftigten, stritt mit dem Vorsitzenden des Betriebsrates über dessen Ausschluss aus dem Betriebsrat. Im September 2023 stellte der Arbeitgeber fest, dass im dienstlichen E-Mail-Postfach eine automatische Weiterleitungsregel an das private E-Mail-Postfach des Betriebsratsvorsitzenden eingerichtet war. Daraufhin mahnte der Arbeitgeber den Betriebsratsvorsitzenden ab und sperrte die ihm bekannte private E-Mail-Adresse des Betriebsratsvorsitzenden, so dass dieser an diese keine E-Mails mehr verschicken konnte. Ende Oktober stellte der Arbeitgeber erneut fest, dass eine Weiterleitung an die private E-Mail-Adresse stattgefunden hat. Anfang November versandte der Betriebsratsvorsitzende von seinem privaten E-Mail-Account eine vollständige Personalliste unter dem Betreff „Vergütungsverhandlung 2023 – Berechnungen“ an seinen dienstlichen E-Mail-Account. Am gleichen Tag versandte er die E-Mail nebst Anlagen (nochmals) an die E-Mail-Adresse des Betriebsrats.

Er hatte sich die Datei zuvor von seinem dienstlichen E-Mail-Account an eine andere private E-Mail-Adresse verschickt und diese zu Hause am eigenen PC bearbeitet. Am 08.11.2023 leitete er die Personalliste nochmals von seinem privaten E-Mail-Account an die E-Mail-Adresse des Betriebsrats sowie an seine dienstliche E-Mail-Adresse weiter.

Die Entscheidung des LAG Hessen

Der Arbeitgeber beantragte gemäß § 23 Abs. 1 BetrVG den Ausschluss des Vorsitzenden aus dem Betriebsrat am Arbeitsgericht Wiesbaden. Zur Begründung führte er grobe datenschutzrechtliche Pflichtverletzungen an. Der Betriebsrat sowie dessen Vorsitzender argumentierten, die Weiterleitung sei ausschließlich aus praktischen Gründen erfolgt, um die Datei auf einem größeren Bildschirm bearbeiten zu können; sämtliche Daten seien nach Abschluss der Bearbeitung gelöscht worden. Das Arbeitsgericht Wiesbaden entsprach dem Antrag des Arbeitgebers mit Beschluss vom 23. Mai 2024 und stellte fest, dass das Verhalten des Vorsitzenden eine schwerwiegende Pflichtverletzung darstelle, die den Ausschluss aus dem Gremium rechtfertige. Gegen diese Entscheidung legten sowohl der Betriebsrat als auch dessen Vorsitzender Beschwerde beim LAG Hessen ein.

Vor dem LAG argumentierte der Betriebsratsvorsitzende zusätzlich, dass sein heimischer PC technisch gesichert sei und ein HDMI-Kabel, mit dem er seinen Dienstrechner mit seinem heimischen Monitor verbinden könne, durch die IT-Abteilung des Arbeitgebers nicht zeitnah herangeschafft werden kann – einen entsprechenden Versuch hat er nicht unternommen. Aufgrund der anstehenden Verhandlungen mit dem Arbeitgeber sei ein Warten nicht möglich gewesen.

In seiner Entscheidung hat das LAG Hessen den Ausschluss aus dem Betriebsrat bestätigt und die datenschutzrechtliche Verantwortung des Betriebsrats erneut bekräftigt. Das Gericht stellte klar, dass der Betriebsrat bei der Verarbeitung personenbezogener Daten gemäß § 79a BetrVG uneingeschränkt den Vorgaben der DSGVO und des BDSG unterliegt. Die Frage der Vereinbarung von Unionsrecht und des BDSG ließ es jedoch offen. Die Weiterleitung sensibler Beschäftigtendaten – insbesondere vollständiger Entgeltinformationen – an eine private E-Mail-Adresse wurde vom Gericht als Datenverarbeitung im Sinne von Art. 4 Nr. 2 DSGVO eingeordnet. Für diese Datenübermittlung sowie für die anschließende Bearbeitung außerhalb der gesicherten Infrastruktur des Arbeitgebers fehlte es sowohl an einer Einwilligung der betroffenen Personen als auch an einer anderweitigen Rechtsgrundlage. Insbesondere war die Verarbeitung nicht erforderlich im Sinne von § 26 Abs. 1 BDSG bzw. Art. 6 Abs. 1 DSGVO, da eine Verarbeitung der Daten auf den vom Arbeitgeber bereitgestellten dienstlichen Geräten ohne Weiteres möglich gewesen wäre. Das Verhalten des Betriebsratsvorsitzenden wurde als objektiv gravierende Pflichtverletzung gewertet. Ausschlaggebend war neben der Sensibilität der übermittelten Daten auch die Tatsache, dass der Vorsitzende bereits zuvor wegen desselben datenschutzrechtlichen Verstoßes abgemahnt war und die technische Schutzmaßnahme – die Sperrung der privaten E-Mail-Adresse – durch eine weitere private E-Mail-Adresse umging. Laut LAG sei der Betriebsratsvorsitzende unbelehrbar. Weder die behaupteten technischen Schutzmaßnahmen am privaten PC, noch eine etwaige Dringlichkeit überzeugten das Gericht.

Fazit und Ausblick

Diese Entscheidung reiht sich in die zunehmend strengere arbeitsgerichtliche Bewertung datenschutzrechtlicher Verstöße durch Betriebsratsmitglieder ein. Sie verdeutlicht, dass Betriebsratsmitglieder bei der Verarbeitung personenbezogener Daten denselben datenschutzrechtlichen Maßstäben unterliegen wie der Arbeitgeber selbst. Sie stärkt die Position der Arbeitgeber, datenschutzrechtliche Verstöße innerhalb des Betriebsrats konsequent zu sanktionieren, und setzt ein deutliches Signal für die Einhaltung datenschutzrechtlicher Standards im Rahmen der Betriebsratsarbeit.

Betriebsräten ist daher dringend zu empfehlen, sich regelmäßig über ihre datenschutzrechtlichen Pflichten fortzubilden. Unternehmen sollten bei Datenschutzverstößen durch Betriebsratsmitglieder konsequent reagieren und – sofern erforderlich – rechtliche Schritte einleiten, um ihrer eigenen datenschutzrechtlichen Verantwortung nachzukommen. Der Arbeitgeber ist nach § 79a S. 2 BetrVG Verantwortlicher im Sinne der DSGVO und damit verantwortlich für die Einhaltung des Datenschutzes im Unternehmen. Auch wenn der Betriebsrat bei der Verarbeitung personenbezogener Daten eigenständig agiert, bleibt der Arbeitgeber bei einem Datenschutzverstoß Verantwortlicher und ist Adressat von Bußgeldern oder Schadensersatzansprüchen. Um Risiken zu minimieren, sollten Unternehmen ihre Compliance-Strukturen regelmäßig überprüfen und anpassen.

VG Köln: Facebook-Fanpage der Bundesregierung bleibt vorerst erlaubt

Die Öffentlichkeitsarbeit staatlicher Stellen auf Facebook bleibt weiterhin erlaubt – zumindest vorerst. Das Verwaltungsgericht Köln (VG Köln) hat mit Urteil vom 17. Juli 2025 (Az. 13 K 1419/23) entschieden, dass das Presse- und Informationsamt der Bundesregierung (BPA) die Facebook-Seite (sog. „Fanpage“) der Bundesregierung weiter betreiben darf.

Hintergrund

Das BPA betreibt seit 2015 auf der Plattform Facebook, die von der Meta Platforms Ireland Ltd. (Meta) betrieben wird, eine Fanpage, auf der es über die Arbeit der Bundesregierung informiert. Meta platziert sog. „Cookies“, unabhängig davon, ob eine Fanpage oder eine andere Seite auf Facebook aufgerufen wird. Diese Cookies sind erforderlich, um Facebook technisch zu betreiben, dienen aber auch dem Erheben von Daten, um Nutzerverhalten zu analysieren und Nutzern personalisierte Werbung zu zeigen. Über die sog. „Insights“ können Betreiber von Fanpages anonymisierte Statistiken über das Verhalten der Besucher auf ihrer Seite erhalten. Auf Verlangen des BPA deaktivierte Meta diese Funktion der streitgegenständlichen Fanpage. Meta erhebt durch Cookies weiterhin Daten, welche dem BPA nicht mehr zur Verfügung gestellt werden.

Im Februar 2023 untersagte der damalige Bundesbeauftragte für Datenschutz und Informationssicherheit (BfDI) dem BPA den Betrieb der Fanpage auf Facebook und verlangte deren Abschaltung. Neben der Untersagung stellte der BfDI weiter fest, dass das BPA gegen seine Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO und § 25 Abs. 1 TTDSG verstoßen habe sowie ohne Rechtsgrundlage personenbezogene Daten erhoben habe und diese an Meta übermittelte. Der BfDI begründet seine Entscheidung damit, dass der Betrieb einer Facebook-Fanpage nicht datenschutzkonform möglich sei. Wegen der nicht datenschutzkonformen Ausgestaltung Metas Cookie-Banners liege keine wirksame Einwilligung in die Speicherung und das Auslesen bestimmter Cookies vor. Weiter seien Meta und das BPA gemeinsame Verantwortliche in Sinne der Datenschutzgrundverordnung (DSGVO), da sich die Interessen der Betreiber von Fanpages und Meta ergänzen. Neben Meta selbst sei daher auch das BPA als Betreiber der Fanpage verpflichtet, die Einwilligung der Nutzer einzuholen.

Das BPA müsse zudem nachweisen, dass die Grundsätze des Datenschutzes eingehalten werden. Weil es dies nicht getan habe, erfolge der Betrieb der Fanpage ohne Rechtsgrundlage und müsse eingestellt werden.

Gegen diesen Bescheid erhoben das BPA und Meta getrennt Klage beim VG Köln, welches die Verfahren zur gemeinsamen Verhandlung verbunden hat.

Urteil des VG Köln

Der Klage des BPA wurde stattgegeben und der Bescheid aus dem Jahr 2023 aufgehoben. Die Klage von Meta war lediglich in Bezug auf die Untersagungsanordnung zulässig und begründet.

Das VG Köln ist der Ansicht, dass Meta allein verantwortlich ist, eine datenschutzkonforme Ausgestaltung des Cookie-Banners sicherzustellen. Das bedeutet, dass Meta – und nicht die Betreiber einer Fanpage wie das BPA – dafür sorgen müssen, dass Nutzerinnen und Nutzer wirksam in die Verwendung von Cookies einwilligen. Auch ist das BPA und Meta nicht gemeinsame Verantwortliche nach der DSGVO.

Meta ist für Cookie-Banner verantwortlich

Seine rechtliche Beurteilung stützt sich das VG Köln maßgeblich auf die Auslegung des - damals noch geltenden und nun durch den im Wortlaut selben § 25 Telekommunikations-Digitale-Dienste-Datenschutzgesetz (TDDDG) abgelösten - § 25 Abs. 1 S. 1 Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG), der die Speicherung und das Auslesen von Informationen auf Endgeräten regelt.

Der Adressatenkreis dieser Norm wird nach Ansicht der Kammer nicht durch Rückgriff auf die DSGVO, sondern durch Auslegung des TTDSG selbst bestimmt. Zwar ist das BPA Anbieterin eines Telemediums, dies genügt jedoch nicht um Adressat nach § 25 Abs. 1 S. 1 TTDSG zu sein. Hierfür muss neben der Stellung als Anbieter ein Wirkungs- und Ursachenzusammenhang gegeben sein. Dieser bezieht sich – nach dem Ziel des § 25 TTDSG – darauf, Nutzer davor zu schützen, dass Dritte ohne ihr Wissen Informationen auf ihren Geräten speichern oder auslesen (sog. Distanzgefahr). Daher sind der datenschutzrechtliche Verantwortliche nach der DSGVO und die Verpflichtungen aus § 25 Abs. 1 TTDSG nicht zwingend gleich. Verantwortlich für die entsprechende Einwilligung nach § 25 Abs. 1 S. 1 TTDSG ist deshalb die Person oder das Unternehmen, das diesen Zugriff tatsächlich steuern oder verhindern kann. Im Fall der Fanpage bedeute das, dass das BPA zwar die Seite betreibt, aber keinen Einfluss darauf hat, ob und welche Cookies gesetzt werden. Diese werden durch Handlungen des Nutzers ausgelöst – zum Beispiel beim Besuch verschiedener Facebook-Seiten – und nicht direkt durch den Betrieb der Fanpage. Das BPA kann technisch und rechtlich nicht steuern, welche Cookies Meta setzt. Deshalb ist das BPA nicht verantwortlich für die von Meta verwendeten Cookies.

Meta und BPA nicht als gemeinsame Verantwortliche

Die Einleitung des Verfahrens durch den BfDI geht unter anderem auf das Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018 (C-210/16; „Wirtschaftsakademie“) zurück. Demnach sei nicht nur Meta allein für den Datenschutz zuständig, sondern auch die Betreiber einer Fanpages für Datenschutzmängel verantwortlich. Denn durch die Errichtung und den Betrieb einer Fanpage entsteht die Möglichkeit, auf dem Endgerät von Nutzern, die die Fanpage besuchen, Cookies zu platzieren - unabhängig davon, ob diese Person über ein Facebook-Konto verfügt.

Eine gemeinsame Verantwortlichkeit von Meta und dem BPA für die Verarbeitung personenbezogener Daten nach der DSGVO sieht das Gericht nicht, da dies voraussetzt, dass beide Seiten gemeinsam über Zweck und Mittel der Datenverarbeitung entscheiden. Mit Verweis auf die „Wirtschaftsakademie“-Rechtsprechung des EuGH hätte das BPA Parameter oder Filter festlegen müssen, nach denen die Insights bestimmt werden, um eine gemeinsame Verantwortlichkeit anzunehmen. Gerade diese Mitbestimmung an den Mitteln der Verarbeitung ist ein zentrales Kriterium für eine gemeinsame Verantwortlichkeit.

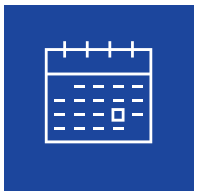
Daran fehlt es hier. Zum Zeitpunkt des Untersagungsbescheids durch den BfDI konnten Betreiber von Fanpages keine eigenen Einstellungen oder Parameter mehr vorgeben, um die Art und Weise der Datenverarbeitung – etwa für die Erstellung von Insights – zu beeinflussen. Diese werden ausschließlich durch Meta vorgenommen. Das BPA habe somit keinen tatsächlichen Einfluss mehr darauf gehabt, wie Meta personenbezogene Daten verarbeitet oder auswertet.

Ausblick

Die Entscheidung stellt klar, wer verantwortlich für die Einwilligung von Cookies ist und erlaubt hierdurch, Behörden, Unternehmen oder andere Institutionen, wenn keine wirtschaftliche Interessen verfolgt werden, eine Fanpage für den Öffentlichkeitsauftritt zu nutzen, ohne für die dort verwendeten Cookies verantwortlich zu sein.

Dass ein Zusammenhang zwischen der Eigenschaft als Anbieter und den Eingriff auf die Endgeräte der Endnutzer durch Cookies als erforderlich gesehen wird, überzeugt. Hierdurch ist nur derjenige verantwortlich, der die Cookies verteilt und deren Funktion bestimmen kann. Gleichzeitig schränkt es nicht die Technologieoffenheit für neue Kommunikationskanäle ein und erlaubt die Verwendung von Social-Media-Plattformen oder anderen modernen Kommunikationskanälen, ohne dass eine (nicht beherrschbare) Verantwortlichkeit bei den Nutzern der Kanäle bleibt. Die jetzige Entscheidung stärkt die Möglichkeit, dass Behörden auch in Zukunft auf wichtigen Plattformen wie Facebook präsent bleiben können. Das ist für eine moderne Öffentlichkeitsarbeit unerlässlich. Es bleibt jedoch abzuwarten, ob die amtierende BfDI Berufung beim Oberverwaltungsgericht NRW einlegt.

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

Bildnachweis

Sutthiphong/Adobe Stock: Seite 3; tippapatt/Adobe Stock: Seite 5; sdecoret/Adobe Stock: Seite 7; BOTAHRY DEX/Adobe Stock: Seite 10; Firn/Adobe Stock: Seite 12; sasun Bughdaryan/Adobe Stock: Seite 15;Getty Images: Seite 17

Haftungsausschluss

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

Luther.

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

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

unyer GLOBAL ADVISORS