LOSCHELDER

Newsletter Datenschutzrecht

August 2024

Sehr geehrte Damen und Herren,

nach einer kreativen Pause melden wir uns zurück – pünktlich zu sommerlichen Temperaturen mit unserer Übersicht über die aktuell „heißen Themen“ im Datenschutz.

Nicht fehlen darf hier die Zusammenfassung der aktuellen Entwicklungen in Sachen Schadensersatz und Auskunftsrecht. Der Dauerbrenner in der Beratungspraxis und nicht selten der „wunde Punkt“ im operativen Geschäftsablauf. Wir werfen sodann einen Blick auf die anstehenden Änderungen im BDSG: Braucht Ihr Unternehmen künftig noch einen Datenschutzbeauftragten? Abschließend blicken wir auf die neue Digitalregulierung, heute ganz konkret auf die Anfang August in Kraft getretene KI-Verordnung.

Nicht weniger spannend sind die Entwicklungen im IT-Sicherheitsrecht: Nach zähem Ringen hat das Kabinett den Regierungsentwurf für die Umsetzung der NIS2-Richtlinie verabschiedet, der Entwurf zum – Achtung, Zungenbrecher – NIS2UmsuCG. Mit dem Regierungsentwurf kann (und sollte) nun jedes Unternehmen mit 50 Mitarbeitenden oder einem Jahresumsatz von 10 Mio. Euro in die Betroffenheitsanalyse gehen: Viele Unternehmen werden erstmalig vom IT-Sicherheitsrecht adressiert. Wir erwarten, dass das Gesetz im Frühjahr 2025 verabschiedet werden wird und dann zeitnah in Kraft tritt. Noch verbleibt also ein gutes halbes Jahr zur Umsetzung. Für erstmalig adressierte Unternehmen wird die Zeit schon beinahe eng.

Wir geben Ihnen daher in unserem nächsten Lunch@Loschelder-Webinar einen Überblick, welche Unternehmen von dem neuen IT-Sicherheitsrecht adressiert werden und was es bei Betroffenheit zu tun gibt. Wir freuen uns sehr über Ihr Interesse und Ihre Anmeldungen zu unserem Webinar (Anmeldung unter webinare@loschelder.de, die Teilnahme ist kostenfrei).

Kommt jetzt die Cybersecurity-Pflicht für alle? Wen betrifft das neue IT-Sicherheitsrecht? Und was muss getan werden?

Donnerstag, den 19. September 2024 - 12.00 bis 12.45 Uhr

Ihre Referenten: Dr. Kristina Schreiber / Dennis Pethke, LL.M. (Stellenbosch)

Alle Webinare bieten wir kostenfrei an und freuen uns über Ihre Anmeldung unter webinare@loschelder.de. Das Webinar findet über Teams statt, der Einladungslink wird rechtzeitig vor der Veranstaltung bereitgestellt.

Selbstverständlich unterstützen wir Sie bei Bedarf auch, wie viele andere unserer Mandanten, bei einer umfassenden Betroffenheitsanalyse mit gutachterlicher Einschätzung oder auch lediglich telefonischem Brainstorming – ganz, wie Sie dies wünschen!

Wir freuen uns über Ihr Interesse!

Inhalt

Schadensersatzanspruch bei DSGVO-Verstoß: EuGH-Linie festigt sich

Der EuGH hat bereits mehrfach zu den Voraussetzungen des Schadensersatzanspruchs nach Art. 82 DSGVO und insbesondere den Voraussetzungen für einen immateriellen Schadensersatz entschieden. Mit den letzten Urteilen hierzu festigt sich die bisherige Linie zunehmend. Wir werfen dafür einen besonderen Blick auf seine Urteile aus April und Juni 2024. Im Ergebnis: Immaterieller Schadensersatz hängt nicht davon ab, dass gestohlene Daten tatsächlich zum Identitätsbetrug verwendet wurden, es ist auch keine besondere Erheblichkeit des Schadens erforderlich. Der eingetretene Schaden muss aber vom Betroffenen konkret nachgewiesen werden.

Ausgangsverfahren 1: Juris

Das Landgericht (LG) Saarbrücken legte dem EuGH im Wege des Vorabentscheidungsverfahrens mehrere Fragen zu den Voraussetzungen und der Berechnung des Schadensersatzanspruchs nach Art. 82 DSGVO vor (Rs. C-741/21).

In dem Ausgangsverfahren vor dem LG Saarbrücken machte der Kläger, ein niedergelassener Rechtsanwalt, gegen die juris GmbH einen Anspruch auf Schadensersatz aus Art. 82 DSGVO geltend. Der Kläger war Kunde der juris GmbH, die eine juristische Datenbank betreibt. Nachdem der Kläger erfahren hatte, dass die juris GmbH seine personenbezogenen Daten auch für Zwecke der Direktwerbung nutzte, widerrief er seine Einwilligungen zum Erhalt von Informationen per E-Mail und Telefon und widersprach jeglicher Verarbeitung dieser Daten mit Ausnahme des Versands von Newslettern, die er weiterhin beziehen wollte. Dennoch erhielt der Kläger mehrfach Werbeschreiben, in denen er namentlich angeschrieben wurde, an seine Geschäftsadresse. Auch nachdem er die juris GmbH daraufhin auf seinen Widerspruch und die Rechtswidrigkeit der Verarbeitung seiner Daten hingewiesen und Schadensersatz gefordert hatte, erhielt er im Anschluss ein weiteres Werbeschreiben. Er erklärte daraufhin noch einmal seinen Widerspruch. Jedes dieser Werbeschreiben enthielt dabei einen persönlichen Code, der zu einer Bestellmaske auf der Website der juris GmbH führte, die Angaben zur Person des Klägers enthielt.

Der Kläger machte in dem Ausgangsverfahren den Ersatz seines materiellen Schadens, der ihm durch die Rechtsverfolgung entstanden ist, sowie seines immateriellen Schadens geltend. Das LG Saarbrücken hielt es für seine Entscheidungsfindung für erforderlich, dem EuGH Fragen zu den Voraussetzungen des Schadensersatzanspruchs, zur Zurechnung von Handlungen unterstellter Personen sowie zur Schadensberechnung zu stellen.

Voraussetzungen des Schadensersatzes nach Art. 82 DSGVO bei immateriellen Schäden

In seiner ersten Frage wollte das LG Saarbrücken wissen, ob der Begriff des immateriellen Schadens im Hinblick auf Erwägungsgrund 85 und 146 Satz 3 DSGVO in dem Sinne zu verstehen ist, dass er jede Beeinträchtigung der geschützten Rechtsposition erfasst, unabhängig von deren sonstigen Auswirkungen und deren Erheblichkeit.

Nach dem die juris GmbH die Zulässigkeit der Frage zunächst gerügt hat, stellte der EuGH zunächst fest, dass es allein Sache des vorlegenden Gerichts ist, die Erforderlichkeit einer Vorabentscheidung für den Erlass seines Urteils zu beurteilen. Dies gilt auch für die Erheblichkeit der Fragen, die es dem Gerichtshof vorlegt, wobei eine Vermutung für die Entscheidungserheblichkeit gilt. Der EuGH ist somit grundsätzlich gehalten über die ihm vorgelegten Fragen zu entscheiden. Etwas Anderes gilt nur, wenn die erbetene Auslegung offensichtlich in keinem Zusammenhang mit den Gegebenheiten oder dem Gegenstand des Ausgangsrechtsstreits steht, das Problem hypothetischer Natur ist oder der EuGH nicht über die tatsächlichen und rechtlichen Angaben verfügt, die für eine zweckdienliche Beantwortung der Fragen erforderlich sind. All dies war vorliegend jedoch nicht der Fall.

Bezüglich der ersten Frage führte der EuGH sodann aus, dass der bloße Verstoß gegen die DSGVO nicht ausreicht, um einen Schadensersatzanspruch zu begründen. Es ist vielmehr erforderlich, dass der Kläger, der auf Grundlage von Art. 82 Abs. 1 DSGVO den Ersatz eines immateriellen Schadens verlangt, nicht nur den bloßen Verstoß gegen die Bestimmungen der DSGVO nachweist, sondern auch, dass ihm durch diesen Verstoß ein Schaden entstanden ist. Allerdings darf der Ersatz eines nachgewiesenen immateriellen Schadens nicht davon abhängig gemacht werden, dass der Schaden einen gewissen Schweregrad erreicht hat. Der EuGH weist auch

darauf hin, dass Erwägungsgrund Nr. 85 der DSGVO ausdrücklich den „Verlust der Kontrolle“ zu den Schäden zählt, die durch eine Verletzung personenbezogener Daten verursacht werden können. Der EuGH knüpft damit an seine bisherige Rechtsprechung zum immateriellen Schadensersatz an (siehe dazu hier). Es ist somit erforderlich, aber auch ausreichend, dass die betroffene Person den Nachweis erbringt, dass sie tatsächlich einen solchen Schaden – so geringfügig er auch sein mag – erlitten hat.

Verantwortlicher trägt Beweislast für Exkulpation

Mit seiner zweiten Frage möchte das LG Saarbrücken wissen, ob es für eine Befreiung des Verantwortlichen von seiner Haftung nach Art. 82 Abs. 3 DSGVO ausreicht, dass er geltend macht, dass der in Rede stehende Schaden durch ein Fehlverhalten einer ihm im Sinne von Art. 29 DSGVO unterstellten Person verursacht wurde.

Der EuGH hat dies verneint. Für eine Befreiung genügt es nicht, wenn der Verantwortliche nachweist, dass er den ihm im Sinne von Art. 29 dieser Verordnung unterstellten Personen Weisungen erteilt hat, welche nicht befolgt wurden damit zum Eintritt des in Rede stehenden Schadens beigetragen wurde. Die Haftungsbefreiung nach Art. 82 Abs. 3 DSGVO kann dem Verantwortlichen nur zugutekommen, wenn er nachweist, dass es keinerlei Kausalzusammenhang zwischen der etwaigen Verletzung der ihm nach der DSGVO obliegenden Pflichten und dem der betroffenen Person entstandenen Schaden gibt.

Höhe des Schadensersatzanspruchs hängt vom Schaden ab

Mit seiner dritten und vierten Frage, die der EuGH zusammen prüft, möchte das LG Saarbrücken zum einen wissen, ob bei der Bemessung des immateriellen Schadenersatzes eine Orientierung an den in Art. 83 DSGVO, insbesondere Art. 83 Abs. 2 und Abs. 5 DSGVO, genannten Zumessungskriterien erlaubt bzw. geboten ist. Zum anderen soll der EuGH beantworten, ob zu berücksichtigen ist, dass die Person, die Schadenersatz verlangt, von mehreren Verstößen gegen die Verordnung betroffen ist, die sich auf denselben Verarbeitungsvorgang beziehen.

Beide Fragen verneinte der EuGH. Die in Art. 83 DSGVO vorgesehenen Kriterien für die Festsetzung des Betrags von Geldbußen sind nicht entsprechend anzuwenden. Zu

berücksichtigen ist auch nicht, dass die Person, die Schadenersatz verlangt, von mehreren Verstößen gegen die Verordnung betroffen ist, die sich auf denselben Verarbeitungsvorgang beziehen. Der EuGH stellte fest, dass die DSGVO selbst keine Bestimmungen zur Bemessung des Schadensersatzanspruchs enthält und insofern von den nationalen Gerichten grundsätzlich die innerstaatlichen Vorschriften anzuwenden sind, sofern diese die unionsrechtlichen Grundsätze der Äquivalenz und Effektivität beachten. In diesem Zusammenhang hebt der EuGH hervor, dass der Schadensersatz nach Art. 82 DSGVO, anders als die Bußgeldbestimmungen nach Art. 83 DSGVO, keine Straf- sondern eine Ausgleichsfunktion hat. Daraus hat der EuGH abgeleitet, dass die Schwere des Verstoßes gegen die DSGVO, durch den der jeweilige Schaden entstanden ist, sich nicht auf die Höhe des Schadenersatzes auswirken kann. Deshalb kann auch der Umstand, dass der Verantwortliche mehrere Verstöße gegenüber derselben betroffenen Person begangen hat, nicht als relevantes Kriterium für die Bemessung des dieser Person gemäß Art. 82 dieser Verordnung zu gewährenden Schadenersatzes herangezogen werden.

Ausgangsfall 2: Scalable

Der immaterielle Schadensersatz nach der DSGVO ist beim EuGH ein beliebtes Thema: In einem weiteren Vorabentscheidungsverfahren beschäftigte er sich erneut mit den Voraussetzungen des Art. 82 DSGVO (verb. Rs. C-182/22 und C-189/22). Konkret wurde in diesen Scalable-Verfahren gefragt, ob ein Identitätsdiebstahl i.S.d. Erwägungsgrund 75 DSGVO vorliegt, wenn Straftäter über Daten verfügen, die den Betroffenen identifizieren oder ob ein Anspruch auf Schadensersatz erst begründet ist, wenn sich Straftäter tatsächlich als die betroffene Person ausgegeben haben.

Es geht bei den durch das AG München vorgelegten Fragen um zwei weitgehend vergleichbare Klagen gegen das Unternehmen Scalable Capital GmbH („Scalable“). Die beiden Kläger haben bei einer von der Scalable betriebenen Trading-App ein Nutzerkonto angelegt und zur Identifizierung personenbezogene Daten wie Name, Geburtsdaten sowie digitale Kopien ihrer Personalausweise hinterlegt. Diese Daten konnten von unbekannten Straftätern gestohlen werden. Das AG München war der Auffassung, dass den Klägern grundsätzlich ein Schadensersatz nach Art. 82 DSGVO zusteht. Um die Höhe des zu gewährenden

Schadensersatzanspruchs zu bestimmen, hat das AG München das Verfahren ausgesetzt und dem EuGH Fragen zur Auslegung von Art. 82 DSGVO vorgelegt. Die Schlussanträge des Generalanwalts Collins zu diesem Verfahren haben wir bereits in unserem Newsletter aus November 2023 vorgestellt. Der EuGH schließt sich den Schlussanträgen an und bestätigt:

- Der Begriff „Identitätsdiebstahl" ist nur dann erfüllt, wenn ein Dritter die Identität einer Person, die von einem Diebstahl personenbezogener Daten betroffen ist, tatsächlich angenommen hat.

- Der Ersatz eines immateriellen Schadens, der durch den Datendiebstahl verursacht wurde, darf allerdings nicht auf die Fälle beschränkt werden, in denen nachgewiesen wird, dass der Datendiebstahl zu einem Identitätsdiebstahl oder -betrug geführt hat. Der Betroffene muss mithin den vollen Schadensbeweis führen.

Fazit

Die Rechtsprechungslinie des EuGH festigt sich zunehmend. Ein DSGVO-Verstoß kann zu einem zu ersetzenden immateriellen Schaden führen, der für einen Ersatzanspruch auch nicht erheblich sein muss. Exkulpieren können sich Verantwortliche nur, wenn sie nachweisen, dass sie keinerlei Verschulden trifft. Allerdings ist dieser Schaden vom Betroffenen konkret und detailliert nachzuweisen, ihn trifft die volle Beweislast dafür. Allgemein behauptete „Sorgen" oder „Ängste" reichen nicht.

Neues zum Auskunftsrecht – Bedeutung für die Praxis

Das datenschutzrechtliche Auskunftsrecht ist eines der wichtigsten Betroffenenrechte in der DSGVO. Es wird häufig geltend gemacht und immer wieder diskutiert. Der Bundesgerichtshof (BGH) legte jetzt in neuen Entscheidungen Anforderungen an die Bestimmtheit eines Auskunftsantrags fest. Außerdem äußerte er sich zum Umfang herauszugebender Kopien. Für die Praxis sind dies wichtige Entscheidungen, um im Einzelfall rechtssicher durch die Bearbeitung von Auskunftsersuchen zu navigieren.

Wieder einmal war der datenschutzrechtliche Anspruch auf Auskunft und Kopie Gegenstand von höchstrichterlichen Entscheidungen. In mehreren BGH-Urteilen wurden die Voraussetzungen und Grenzen des Art. 15 DSGVO jetzt weiter konkretisiert. Das ist auch notwendig, denn diese Rechte werden immer häufiger geltend gemacht, doch es besteht nach wie vor keine abschließende Klarheit über Anforderungen und Umfang.

Zur Bestimmtheit des Auskunftsantrags

Wer einen Auskunftsanspruch gem. Art. 15 DSGVO klageweise geltend machen will, muss zunächst einen entsprechenden Klageantrag stellen, der bestimmt genug ist. Mit der Frage, wann diese Bestimmtheit gegeben ist, beschäftigte der BGH sich in seinem Urteil vom 05.03.2024 (Rs. VI ZR 330/21). Die Klägerin verlangte die Herausgabe von Kopien aller personenbezogenen Daten, die sich im

Besitz der Beklagten, einer Finanzberaterin, befanden. Insbesondere wollte sie Telefonnotizen, Aktenvermerke, Gesprächsprotokolle, E-Mails, Briefe und Zeichnungsunterlagen für Kapitalanlagen aus der Zeit der Geschäftsbeziehung erhalten.

Der BGH stellte in diesem Verfahren zunächst klar, dass ein Klageantrag grundsätzlich bestimmt genug ist, wenn der geltend gemachte Anspruch konkret bezeichnet ist. Wie konkret die Bezeichnung sein muss, hängt wiederum von den Umständen des Einzelfalls und von einer Abwägung der gegenüberstehenden Interessen des Beklagten (Rechtsklarheit und Verteidigungsmöglichkeit) und des Klägers (wirksamer Rechtsschutz) ab. Bei einem Antrag auf Herausgabe von Kopien personenbezogener Daten nach Art. 15 Abs. 3 DSGVO ist der Antrag nach Ansicht des BGH bestimmt genug, wenn „sämtliche Dokumente, welche sich im Besitz [der Beklagten] befänden" verlangt werden. Der Kläger muss dabei nicht konkretisieren, welche Daten und Dokumente er genau verlangt. Das ist meist überhaupt nicht möglich und zudem ist es gerade das Ziel des Klägers, die ihn betreffenden personenbezogenen Daten vollständig in Erfahrung zu bringen. Es reicht somit aus, lediglich die gewünschten Kategorien von Dokumenten oder Daten, die Informationen über den Kläger enthalten, zu beantragen (BGH, Urteil vom 05.03.2024 – VI ZR 330/21 Rn. 11).

Zum Umfang von Auskunfts- und Kopierecht nach Art. 15 Abs. 1 und 3 DSGVO

Der Verantwortliche hat zum einen Auskunft darüber zu erteilen, ob überhaupt personenbezogene Daten des Antragstellers bei ihm verarbeitet werden (oder nicht). Werden Daten verarbeitet, hat die betroffene Person das Recht auf Auskunft darüber, welche Daten verarbeitet werden sowie über weitere Informationen, wie Verarbeitungszwecke, Kategorien und Empfänger der jeweiligen personenbezogenen Daten oder die Dauer einer etwaigen Datenspeicherung.

Mit dem Auskunftsrecht einher geht das Recht der betroffenen Person auf Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Das Kopierecht gewährt dabei kein anderes Recht als das Auskunftsrecht aus Abs. 1, sondern stellt letztlich eine Ergänzung dar: Die Auskünfte, die nach Abs. 1 geschuldet sind, sind der betroffenen Person in Form von Kopien zur Verfügung zu stellen

(EuGH, Urteil vom 04.05.2023 – C-487/21). Über den genauen Umfang dieses Kopierechtes wurde schon vielfach diskutiert (wir berichteten hier und hier) und auch die neuesten BGH-Urteile behandeln diese Thematik.

Grundsätzlich bezieht sich das Auskunfts- und damit auch das Kopierecht ausschließlich auf die personenbezogenen Daten, die Gegenstand der Verarbeitung beim Verantwortlichen sind, und nicht auf ganze Dokumente. Die Auskunft muss aber insofern vollständig erteilt werden und alle verarbeiteten Daten mit Bezug zur betroffenen Person beinhalten, als dies für die Überprüfung der Richtigkeit der Auskunft nach Art. 15 Abs. 1 DSGVO und die Nachvollziehbarkeit notwendig ist. Was dies konkret in jedem Einzelfall bedeutet, ist allerdings nach wie vor diskutabel.

In zwei Fällen, die es bis zum BGH schafften, forderten Versicherungsnehmer die Herausgabe von Kopien von ganzen Schreiben und Erklärungen, die im Laufe der vertraglichen Beziehung mit dem Versicherer verschickt worden sind. Hieraus ergeben sich wichtige Konkretisierungen für die Praxis:

- Der BGH entschied, dass Kopien von Erklärungen oder Schreiben, die dem Verantwortlichen vorliegen, dann im Ganzen herauszugeben sind, wenn sie von der betroffenen Person selbst verfasst wurden. Ein solches Schreiben stelle insgesamt ein personenbezogenes Datum dar, denn der Personenbezug liegt schon darin, dass die betroffene Person das Schreiben mit dem jeweiligen Inhalt überhaupt verfasst hat.

- Erklärungen des Verantwortlichen (in diesem Fall des Versicherungsunternehmens) einschließlich interner Vermerke, Notizen etc. sind dagegen nur insoweit als Kopie herauszugeben als sie auch wirklich personenbezogene Daten der betroffenen Person enthalten. Hierbei besteht nicht zwangsläufig im gesamten Dokument ein Bezug zur Person des Anspruchstellers, weshalb diese auch nicht notwendigerweise im Gesamten als Kopie herauszugeben sind.

  (BGH, Urteil vom 27.09.2023 – IV ZR 177/22 Rn. 48;
  BGH, Urteil vom 16.04.2024 – VI ZR 223/21 Rn. 13, 18)

Maßgeblich für das Recht auf Kopie ist, dass betroffene Personen ihr Auskunftsrecht wirksam ausüben können müssen. Dafür muss auch eine gewisse Verständlichkeit der herauszugebenden verarbeiteten Daten gewährleistet sein. Es kann daher erforderlich sein, die herauszugebenden Daten in den jeweiligen Kontext zu setzen und diesen dem Anspruchsteller mitzuteilen. Kann die geschuldete Verständlichkeit nur dadurch erreicht werden, dass ein Dokument im Ganzen herausgegeben wird, erstreckt sich der Umfang des Kopierechts dann doch auf das gesamte Dokument und nicht lediglich auf die einzelnen Daten (BGH, Urteil vom 16.04.2024 – VI ZR 223/21 Rn. 19).

Ausblick

Als Merkposten festzuhalten ist aus den jüngsten BGH-Entscheidungen:

1. Es genügt für den Antrag auf Auskunft, wenn allgemein alle Daten und Dokumente verlangt werden, die Informationen über die betroffene Person enthalten.

2. Personenbezogen sind regelmäßig alle Schreiben (einschl. E-Mails), die von der Auskunft verlangenden Person selbst verfasst wurde.

3. Vom Anspruchsgegner, dem Verantwortlichen, erstellte Erklärungen (seien es Schreiben oder interne Vermerke) sind nicht generell personenbezogen, sondern nur in den konkret auf den Anspruchsteller bezogenen Angaben und Informationen.

4. Kopien müssen so bereitgestellt werden, dass der Gesamtkontext als Illustration der Auskunft gem. Art. 15 Abs. 1 DSGVO verständlich wird.

Braucht Ihr Unternehmen künftig noch einen Datenschutzbeauftragten?

Das BDSG soll novelliert werden. Diese Gesetzesänderung könnte dazu führen, dass viele Unternehmen künftig keinen Datenschutzbeauftragten mehr benötigen: Die Schwelle ab der ein solcher Beauftragter unabhängig von der Kerntätigkeit des Unternehmens verpflichtend ist, soll von 20 auf 50 Beschäftigte angehoben werden. Eine Zusammenarbeit mit einem Datenschutzbeauftragten kann jedoch auch bei geringerer Beschäftigtenzahl sinnvoll und wichtig sein. Insbesondere, wenn die Einhaltung datenschutzrechtlicher Vorgaben auf andere Weise nicht sichergestellt werden kann.

Die am 05.07.2024 veröffentlichte „Wachstumsinitiative“ im Zusammenhang mit dem Bundeshaushalt 2025 bringt einen Paukenschlag. Beinahe lapidar heißt es dort als Forderung Nr. 13 c, unter der Überschrift „Anwendung datenschutzrechtlicher Anforderungen reduzieren“:

> *„Erhöhung der Schwelle, ab der Unternehmen einen Datenschutzbeauftragten bestellen müssen von derzeit 20 Mitarbeitenden auf 50 Mitarbeitende.“*

Der Aufschrei in der Datenschutzszene war ungleich lauter: Reduziert es die datenschutzrechtlichen Anforderungen, wenn weniger Unternehmen einen Datenschutzbeauftragten („DSB“) bestellen müssen? Bisher liegt die Schwelle, ab der ein DSB zu

bestellen ist, gem. § 38 Abs. 1 S. 1 Bundesdatenschutzgesetz (BDSG) bei 20 Mitarbeitenden.

Die Bestellung eines DSB ist eine Formsache. Natürlich ist sie mit kommerziellem Aufwand verbunden, unabhängig davon, ob ein interner oder externer DSB bestellt wird. Materiell wachsen oder sinken die datenschutzrechtlichen Anforderungen an ein Unternehmen allerdings nicht mit der Pflicht, einen DSB zu bestellen – oder eben nicht. Ein DSB kontrolliert in der Regel nicht nur, er unterstützt Unternehmen auch bei der Einhaltung datenschutzrechtlicher Vorgaben wie dem BDSG oder der Datenschutzgrundverordnung (DSGVO). Er berät und informiert und hilft so – im Best Case – gerade bei der Anwendung der datenschutzrechtlichen Anforderungen.

Ob das Ziel einer Reduktion der Anforderungen damit mit der Anhebung der Schwelle erreich werden kann, ist mehr als fraglich. Sicher ist indes, dass mehr Unternehmen Gestaltungsspielraum erhalten würden. Denn auch freiwillig kann ein DSB bestellt werden.

Pflichten zur Benennung eines DSB

Das Überschreiten der Schwelle der Beschäftigtenzahl ist nicht der einzige Fall in dem eine Pflicht zur Benennung eines DSB bestehen kann. Im Privatsektor ist „auf jeden Fall" ein DSB zu benennen, wenn zur Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters Datenverarbeitungsvorgänge gehören, bei denen eine umfangreiche Überwachung von betroffenen Personen erforderlich ist. Eine Benennungspflicht besteht auch dann, wenn die Kerntätigkeit in der Verarbeitung besonders sensibler oder strafrechtlich relevanter Daten besteht (Art. 37 Abs. 1 lit. b und c DSGVO).

Darüber hinaus kann Unionsrecht oder nationales Recht vorschreiben, dass auch ein Verantwortlicher, dessen Datenverarbeitung nicht in die vorgenannten Kategorien fällt, einen DSB zu benennen hat (Art. 37 Abs. 4 DSGVO). Eine solche nationale Regelung stellt § 38 BDSG dar. Zum einen liegt eine DSB-Pflicht bei Überschreiten der noch bei 20 liegenden Beschäftigtenzahl vor. Zum anderen, bei der Durchführung von Datenverarbeitungen, die einer Datenschutz-Folgenabschätzung unterliegen. Wird diese Vorschrift tatsächlich wie angekündigt geändert, kommt vielen Unternehmen mehr Gestaltungsspielraum zu bei der Frage, ob sie einen DSB bestellen wollen oder nicht.

DSB auch ohne Verpflichtung sinnvoll

Ob der Verzicht auf einen DSB jedoch für jedes Unternehmen unterhalb der 50-Beschäfigten-Schwelle sinnvoll ist, kann nicht pauschal mit Ja oder Nein beantwortet werden. Daten werden in unterschiedlichem Umfang und auf unterschiedliche Art und Weise von Unternehmen verarbeitet. Dabei sind – selbstverständlich auch ohne Einschaltung eines DSB – die datenschutzrechtlichen Pflichten und Vorgaben zu beachten. Ein Datenschutzkoordinator ist daher in den meisten Fällen ohnehin notwendig. Die DSGVO sieht im Falle der Pflichtverletzung zum Teil hohe Bußgelder vor, welche es zu vermeiden gilt. Zivilrechtliche Schadensersatzklagen nehmen rasant zu. Die Umsetzung des Datenschutzrechts im Unternehmen muss also unabhängig von der Benennung eines DSB organisiert und abgesichert sein.

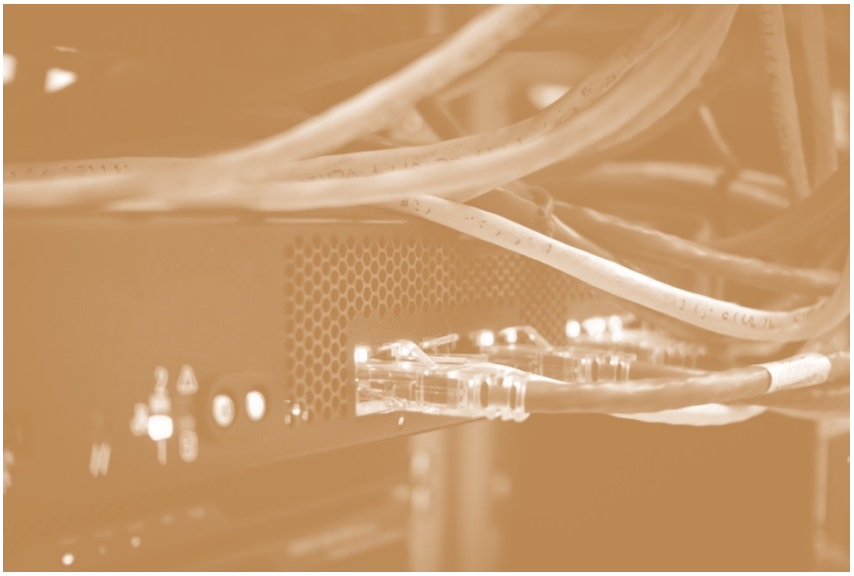
DSB – Ja oder Nein?

Ein Unternehmen braucht nach alledem also gesetzlich verpflichtend einen DSB, wenn

- es unter Art. 37 Abs. 1 DSGVO fällt, etwa, weil die Kerntätigkeit risikobehaftete Datenverarbeitungsvorgänge betrifft, beispielsweise bei der Verarbeitung von Gesundheitsdaten oder

- die Beschäftigtenzahl oberhalb der 20- bzw. bald 50-Personen-Schwelle liegt.

In anderen Fällen bleibt die Entscheidung über die Hinzuziehung eines DSB dem Unternehmen selbst überlassen, soweit nicht eine andere gesetzliche Pflicht greift.



Neues zum Einsatz von KI-Modellen

Künstliche Intelligenz (KI) spielt eine immer größere Rolle, was auch zunehmend rechtliche Fragen aufwirft. Mitte Juli wurde die lange diskutierte KI-Verordnung der EU veröffentlicht, die Anfang August in Kraft getreten ist. Sie stellt erstmals einen Rechtsrahmen für den Einsatz von KI-Systemen auf. Die meisten Pflichten werden in zwei Jahren unmittelbar gelten. In einem kürzlich veröffentlichten Diskussionspapier des Hamburgischen Datenschutzbeauftragten wird darüber hinaus das Verhältnis von Datenschutz und Large Language Models (LLMs) erörtert, wie es z.B. ChatGPT zugrunde liegt. Das soll Unternehmen bei der datenschutzkonformen Nutzung von KI-Systemen, die LLMs einsetzen, unterstützen. Wir fassen die wichtigsten Entwicklungen für Sie als Datenschützer in unserem Artikel zusammen.

Hamburger Thesen zum Personenbezug in LLMs

Der Hamburgische Beauftragte für den Datenschutz und die Informationsfreiheit (HmbBfDI) hat sich in einem Diskussionspapier mit dem Verhältnis der DSGVO zu Large Language Models (LLMs) beschäftigt. Ein LLM ist eine Komponente eines KI-Modells, die Sprachen verstehen, verarbeiten und generieren kann. Das bekannteste Beispiel für ein KI-Modell, welche ein LLM beinhaltet, ist ChatGPT. Bei der Nutzung eines LLMs können nicht nur im eigenen Prompt, den der Nutzer eingibt, sondern auch im sog. Output Angaben über natürliche Personen enthalten sein, insbesondere, wenn Nutzer das System explizit danach fragen. Das

warf beim HmbBfDI die Frage auf, ob LLMs personenbezogene Daten speichern und daher quasi „aus sich heraus“ im Output produzieren. Der HmbBfDI sieht dies differenziert:

- **In LLMs werden keine personenbezogenen Daten gespeichert**

  Trainingsdaten für LLMs und auch Inputs (sog. Prompts) können personenbezogene Daten enthalten. Die LLMs selbst speichern nach HmbBfDI aber keine personenbezogenen Daten. Dies bedeutet, dass im System selbst die beim Training verwendeten personenbezogenen Daten nicht mehr als solche vorhanden sind, sie haben lediglich zur Entwicklung der entsprechenden Gewichte und Tokens geführt.

  Wer ein LLM speichert und hostet, verarbeitet daher auch noch keine personenbezogenen Daten i.S.v. Art. 4 Nr. 2 DSGVO. Das LLM ist insofern nur „Tool“, wie eine Software. Personenbezogene Daten werden mit diesem erst und nur dann verarbeitet, wenn es mit solchen trainiert wird oder aber im entsprechenden Input oder Output.

- **Ein LLM kann nicht selbst Gegenstand von Betroffenenrechten sein**

  Mangels Speicherung personenbezogener Daten im LLM, können die Betroffenenrechte der DSGVO auch nicht das LLM selbst zum Gegenstand haben. Sie können sich aber auf Trainingsdaten, Input oder Output eines KI-Systems, das ein LLM beinhaltet, beziehen. Das ist dann auch maßgeblich für die Person, der gegenüber die Betroffenenrechte geltend gemacht werden, ähnlich der bei Software bekannten Differenzierung zwischen Hersteller und Anwender der Software.

- **Training mit personenbezogenen Daten nur im Rahmen der DSGVO**

  LLMs dürfen nur im Rahmen des Datenschutzrechts mit personenbezogenen Daten trainiert werden. Auch die Betroffenenrechte müssen dabei selbstverständlich beachtet werden.

Allerdings wirkt sich ein Datenschutzverstoß beim Training des LLMs nicht auf die Rechtmäßigkeit seines Einsatzes aus, wenn mit dem HmbBfDi davon ausgegangen wird, dass das LLM selber keine personenbezogenen Daten speichert. Einem Unternehmen, welches Daten mit KI-Systemen verarbeitet, wird ein etwaiger Datenschutzverstoß beim Training des integrierten LLMs dann auch nicht zugerechnet. Allein der Entwickler des LLMs ist für das rechtmäßige Training seines Modells verantwortlich. Dies entlastet alle Nutzer von ChatGPT & Co. enorm, die immer wieder datenschutzrechtlichen Bedenken hinsichtlich ihres Trainings ausgesetzt sind.

Möchte ein Unternehmen jedoch selbst das LLM nachtrainieren, sollte darauf geachtet werden, dass personenbezogenen Daten nur unter strenger Einhaltung des Datenschutzrechts dafür verwendet werden.

KI-Verordnung der EU veröffentlicht

Die erste umfassende KI-Risikoregulierung kommt aus der EU: Am 12.07.2024 ist die Verordnung über künstliche Intelligenz (Verordnung (EU) 2024/1689; im Folgenden: „KI-Verordnung“) im Amtsblatt der EU veröffentlicht worden. Die KI-Verordnung ist damit am 01.08.2024 in Kraft, der Großteil ihrer Regelung wird ab dem 02.08.2026 unmittelbar in allen EU-Mitgliedstaaten gelten.

Im Wesentlichen wird damit ein Rechtsrahmen für eine risikogerechte Entwicklung, Inverkehrbringen und Anwendung von KI-Systemen geschaffen, der die Werte der EU schützt und die Grundrechte der Unionsbürger wahrt. Gleichzeitig sollen Innovationen durch den freien Verkehr KI-gestützter Waren und Dienstleistungen in der EU gefördert werden. Dafür werden mit der KI-Verordnung weder das Datenschutzrecht, das Urheberrecht oder das Haftungsrecht geregelt. Vielmehr bringt die KI-Verordnung eine risikoangemessen KI-Governance-Pflicht für alle Entwickler und Anwender von KI-gestützten Systemen.

Die wesentlichen Elemente der KI-Verordnung lassen sich wie folgt zusammenfassen:

- **Risikoklassifizierung von KI-Systemen**

  Inakzeptable KI-Systeme werden verboten. Dies betrifft Anwendungen wir etwa das „Social Scoring“, bei dem Personen auf Grundlage ihres Sozialverhaltens bewertet werden. Ebenso verboten wird die Erstellung von Datenbanken zur Gesichtserkennung durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet.

  Andere Systeme werden als Hochrisiko-KI-Systeme eingestuft, beispielsweise KI in Funkanlagen oder für KI für Personalentscheidungen. Sie unterliegen weitreichenden Risikoüberprüfungen, Dokumentations- und Transparenzpflichten, flankiert durch Anforderungen an eine umfassende KI-Governance im Unternehmen. Bei ihrer Entwicklung und ihrem Einsatz im Unternehmen muss u.a. besonders auf die Qualität der verwendeten Daten, Cybersicherheit und Risikomanagement geachtet werden. Auch Anwender unterfallen weitreichenden Informationspflichten ggü. allen Betroffenen.

  Dagegen fallen KI-Systeme, die nur mit einem mittleren oder geringen Risiko verbunden sind, nur unter wenig strenge Vorgaben der KI-Verordnung. Dies betrifft etwa Kennzeichnungspflichten für Deepfakes und KI, die zur Interaktion mit Menschen genutzt wird (Chatbots & Co.).

- **Einbeziehung von Datenschutzaufsichtsbehörden und Aufsicht**

  Außerdem erhalten Datenschutzaufsichtsbehörden besondere Befugnisse, wie den Zugriff zu Dokumenten, die zur Erfüllung der Aufgaben nach der KI-Verordnung erforderlich sind. Gewisse Anbieter von Hochrisiko-KI-Systemen müssen diese registrieren. Werden bei der Entwicklung und dem Training von KI in sog. Reallaboren personenbezogene Daten verarbeitet, sollen die Datenschutzaufsichtsbehörden ebenfalls einbezogen werden.

  Die Aufsicht über (Hochrisiko-)KI-Systeme wird der EU Kommission und den zuständigen Marktüberwachungsbehörden übertragen. Auf nationaler Ebene müssen die EU-Staaten jeweils einen sog. „Single-Point-

of-Contact“ benennen, der als zentrale Anlaufstelle in Bezug auf KI u.a. Beschwerden und Meldungen entgegennehmen soll.

Erarbeitet wird derzeit auch eine entsprechende Behördenstruktur mit einem AI Office auf EU-Ebene und nationalen Behörden. Einige Unternehmen müssen zudem AI Officer benennen.

KI-Governance-Programme

Verstöße gegen die KI-Verordnung sind mit enormen Bußgeldern belegt. Es ist daher angezeigt, zeitnah eine Betroffenheitsanalyse einzuleiten, wenn KI im Unternehmen entwickelt oder eingesetzt wird. Im ersten Zugriff helfen hierbei AI Act Compliance Checker, die aber oftmals zu pauschal sind, um wirkliche Hilfestellung zu bieten. In diesem Fall sollte intern eine zuständige Stelle geschaffen werden, die die Relevanzprüfung aufnimmt – wir unterstützen dabei gerne mit Workshops bis hin zur Gutachtenerstellung oder – oft sehr effektiv – der Prozessbegleitung insgesamt.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Philipp Schoel
+49(0)221 65065-200
philipp.schoel@loschelder.de

Dennis Pethke, LL.M.
+49(0)221 65065-337
dennis.pethke@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de