LOSCHELDER

Newsletter Datenschutzrecht
Dezember 2023

Sehr geehrte Damen und Herren,

zum Jahresendspurt ist unser Newsletter noch einmal prall gefüllt: In den letzten Tagen hat der EuGH eine ganze Reihe von Entscheidungen zu in der Praxis höchst relevanten Datenschutzfragen verkündet. Konkret geht es um Bußgelder, Schadensersatzansprüche, Kopien und das SCHUFA-Scoring.

Aufgrund der hohen Praxisrelevanz der neuen EuGH-Entscheidungen und der neuen gesetzgeberischen Entwicklungen im Datenrecht werden wir das neue Jahr unseren Lunch@Loschelder-Webinaren beginnen. Damit können Sie sich gleich zum Jahresstart *up to date* bringen für ein optimiertes Compliance-Niveau in Ihrem Unternehmen.

Wir freuen uns sehr über Ihr Interesse und Ihre Anmeldungen zu den folgenden Webinaren (Anmeldung unter webinare@loschelder.de, die Teilnahme ist kostenfrei und findet über Teams statt. Der Einladungslink wird rechtzeitig vor der Veranstaltung bereitgestellt.):

Bußgelder nach DSGVO-Verstoß: Droht eine Ausweitung?

Wann ein Bußgeld nach einem DSGVO-Verstoß gegen welche Einheit – das Unternehmen oder die Leitungsorgane – verhängt werden darf, war Gegenstand der aktuellen EuGH-Entscheidung in der Rechtssache Deutsche Wohnen. Das Urteil hat enorme Auswirkungen auf die Compliance-Strukturen im Unternehmen. Wir besprechen mit Ihnen, was zu tun ist, um das eigene Unternehmen bestmöglich vor Bußgeldern zu schützen.

Mittwoch, den 24. Januar 2024 - 12.00 bis 12.45 Uhr
Ihre Referenten: Dr. Simon Kohm und Philipp Schoel

Schadensersatzrisiken nach DSGVO-Verstoß: Uferlose Haftung?

Kommen nach den neuen EuGH-Entscheidungen vom 14.12.2023 jetzt die Massenklagen? Wann ist ein Schadensersatzanspruch nach DSGVO-Verstoß begründet? Und wie können sich Unternehmen auch in Sachen Informations- und Datensicherheit entlasten, wenn es zu einem Hacker-Angriff gekommen ist? Wir besprechen mit Ihnen die Folgen der EuGH-Urteile in Sachen C-340/21 und C-456/22 und zeigen auf, wie sich Ihr Unternehmen aufstellen sollte, um Schadensersatzrisiken zu minimieren.

Mittwoch, den 31. Januar 2024 - 12.00 bis 12.45 Uhr
Ihre Referenten: Dr. Kristina Schreiber und Dennis Pethke, LL.M.

Das neue Datenrecht: Der Data Act

Kurz vor Jahresende hat auch der Rat den Data Act bestätigt: Dieser wird zeitnah in Kraft treten. Damit beginnt der Countdown, um vernetzte Produkte und Datenverarbeitungsdienste rechtskonform zu gestalten. Aber was ist zu tun? Und wie können sich Unternehmen möglichst rechtssicher aufstellen und den Data Act womöglich sogar für neue Geschäftsmodelle nutzen? Überhaupt: Wer ist von den neuen Regelungen betroffen? Wir geben Ihnen einen ersten Einblick in die wichtigsten Weichenstellungen des Data Act: Verpflichtete und Berechtigte, betroffene Produkte, Risiken und Gestaltungschancen.

Mittwoch, den 28. Februar 2024 - 12.00 bis 12.45 Uhr
Ihre Referenten: Dr. Patrick Pommerening und Dr. Kristina Schreiber

Schließlich: Wir bedanken uns herzlich für Ihr Interesse an unserem Newsletter auch in diesem Jahr 2023 und freuen uns sehr, wenn Sie uns auch im kommenden Jahr 2024 wieder mit Interesse begleiten.
Wir wünschen Ihnen besinnliche Weihnachtsfeiertage und einen guten Start in das neue Jahr 2024!

Inhalt

Bußgeldrisiken: Wann und wem drohen sie?

Bußgelder wegen eines DSGVO-Verstoßes können den Unternehmen unmittelbar auferlegt werden, nicht nur den Leitungsorganen. Allerdings: Bußgelder setzen einen schuldhaften Verstoß gegen die DSGVO voraus. Gerade das Urteil in der Rechtssache Deutsche Wohnen war mit Spannung erwartet worden. Wo es Klärung bringt und wo neue Fragen, erläutern wir in unserem Beitrag.

Am 05.12.2023 entschied der EuGH in dem von vielen intensiv beobachteten Verfahren „Deutsche Wohnen“: Ein deutsches Vorabentscheidungsverfahren, in dem eines der frühen hohen Bußgelder (14,5 Mio. Euro) auf dem Prüfstand steht. Ein richtungsweisendes Verfahren für die künftige Bußgeldhaftung und damit auch die Anforderungen an das Datenschutzmanagement und die Aufstellung der Leitungsebene zur Vermeidung von Bußgeldern.

Der Fall

Die Immobiliengesellschaft Deutsche Wohnen verarbeitet personenbezogene Daten der Mieter von Wohn- und Gewerbeeinheiten. Im Sommer 2017 wies die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnDI) DW darauf hin, dass Mieterdaten gespeichert würden, für die nicht nachvollzogen werden könne, ob die Speicherung erforderlich sei und ob nicht mehr erforderliche Daten gelöscht würden.

Im März 2019 prüfte die BlnDI die DW erneut. DW teilte mit, dass das beanstandete Archivsystem bereits außer Betrieb gesetzt worden sei und die Migration der Daten auf ein neues Speichersystem unmittelbar bevorstehe. Die BlnDI sah aufgrund der Zeitverzögerungen und aus ihrer Sicht nach wie vor bestehenden Unzulänglichkeiten einen wegen den Hinweisen aus 2017 *vorsätzlichen* Verstoß gegen die DSGVO. Vorgeworfen wird DW eine zu lange Speicherung von personenbezogenen Daten, deren Verarbeitung nicht (mehr) erforderlich sein. Die Aufsichtsbehörde setzte eine Geldbuße in Höhe von ca. 14,5 Mio. Euro fest.

In ihrem Bußgeldbescheid rechnete die BlnDI den Verstoß keinem Leitungsorgan der DW zu und wies auch kein konkretes, individuelles Verschulden nach. Nach deutschem Ordnungswidrigkeitenrecht ist dies gem. § 30 OWiG indes grundsätzlich erforderlich. Ob dies indes auch für Bußgelder nach

der DSGVO gilt, ist seit Inkrafttreten der DSGVO höchst umstritten (neben dem hier gegenständlichen Berliner Verfahren etwa auch im 1&1-Verfahren: LG Bonn, Urteil vom 11.11.2020 – 29 OWi 1/20).

Die EuGH-Entscheidung

Der EuGH hat nun entschieden: Die DSGVO geht dem deutschen Ordnungswidrigkeitenrecht vor (Rs. C-807/21). Für die Verhängung eines Bußgelds nach Art. 83 DSGVO ist es nicht erforderlich, eine natürliche Person aus dem Kreis der Leitungspersonen zu identifizieren, der der konkrete DSGVO-Verstoß zuzurechnen oder der ein konkretes Verschulden vorzuwerfen ist.

Aus der EuGH-Entscheidung ergeben sich damit drei zentrale Aussagen:

1. Bußgelder können **gegen Unternehmen** verhängt werden, ohne dass der DSGVO-Verstoß einer konkreten (Leitungs-) Person zuzurechnen ist.

2. Bußgelder setzen **Verschulden** voraus. Unklar bleibt aber, auf wessen Verschulden es ankommt und wie dieses nachzuweisen ist. Der EuGH verlangt nur ein Verschulden des „Verantwortlichen", also letztlich des Unternehmens selbst(?).

3. Bußgelder werden anhand der **Umsätze der gesamten Unternehmensgruppe** ermittelt, konkret der aus dem Kartellrecht bekannten „wirtschaftlich tätigen Einheit". Damit kommt es regelmäßig auf die Umsätze aller verbundenen Unternehmen an.

Im Einzelnen:

Bußgelder gegen Unternehmen

Die Durchsetzung der DSGVO darf durch nationales Recht nicht beschränkt werden. Der EuGH erteilt daher zusätzlichen Anforderungen an die Verhängung von Bußgeldern, die sich aus dem deutschen Ordnungswidrigkeitenrecht ergeben könnten, eine Absage.

Die DSGVO unterscheide in ihrem Bußgeldregime nicht zwischen natürlichen und juristischen Personen. Ein Bußgeld werde gegen „den Verantwortlichen", also die datenverarbeitende Stelle verhängt. In der Regel ist das das Unternehmen selbst.

Daraus folgt, dass die Daten verarbeitenden Unternehmen nicht nur für Verstöße haften, die von ihren Leitungsorganen begangen werden. Sie haften für alle Verstöße, die von irgendeiner Person begangen werden, *„die im Rahmen der unternehmerischen Tätigkeit und im Namen dieser juristischen Personen handelt“* (Rn. 44). Damit genügt für die Haftung der DSGVO-Verstoß eines jeden Mitarbeitenden, ungeachtet des jeweiligen Aufgaben- und Verantwortungsbereiches. Mehr noch: Die Person, die den Verstoß gegangen hat, muss nicht identifiziert werden (Rn. 46).

Zu diskutieren wird nun sein, inwiefern eine Haftung auch dann in Betracht kommt, wenn Mitarbeitende außerhalb des vorgegebenen Rahmens agieren. Im Fall eines „echten Exzesses“ wird es letztlich wohl nur dann zu einer Haftung kommen können, wenn die Compliance-Struktur unzureichend war und damit ein Organisationsverschulden im Raum steht.

Bußgelder nur bei Verschulden

Begrenzend gilt aber auch weiterhin, dass Bußgelder ein Verschulden voraussetzen. Sie können also nur dann auferlegt werden, wenn der DSGVO-Verstoß vorsätzlich oder fahrlässig begangen wurde.

Ob ein Verhalten derart vorwerfbar ist, kann nach deutscher Rechtstradition regelmäßig nur mit Blick auf das Verhalten konkreter natürlicher Personen bewertet werden: Gab es die „Absicht“, gegen die DSGVO zu verstoßen, wurde der Verstoß zumindest billigend in Kauf genommen oder haben die handelnden Personen die im Verkehr erforderliche Sorgfalt außer Acht gelassen?

Dieser Ansatz passt aber nicht zu dem vom EuGH angenommenen Vorgehen: Für ein DSGVO-Bußgeld ist es nicht erforderlich, einen Datenschutzverstoß einer identifizierten Person zuzurechnen, so dass es womöglich auch nicht auf das Verschulden einer einzelnen Person ankommen kann.

Die EuGH-Entscheidung ist an diesem Punkt vage:

> *„Aus dem Wortlaut von Art. 83 Abs. 2 DSGVO ergibt sich somit, dass nur Verstöße gegen die Bestimmungen der DSGVO, die der Verantwortliche schuldhaft, d. h. vorsätzlich oder fahrlässig, begeht, zur Verhängung einer Geldbuße gegen ihn nach diesem Artikel führen können.“* (Rn. 68)

Der „Verantwortliche“ ist, wie oben erläutert, das Unternehmen. Diesem muss also ein Verschulden vorgeworfen werden. Wie das in Einklang zu bringen ist mit der EuGH-Aussage, dass ein DSGVO-Verstoß keiner identifizierten Person zugerechnet werden muss, bleibt offen. Wie genau dieser Maßstab in der Anwendungspraxis nun umgesetzt wird, muss nun konkretisiert werden. Sicher ist: Ohne Verschulden darf es kein Bußgeld geben.

Dieses Verschulden muss von der Datenschutzaufsichtsbehörde *nachgewiesen* werden (Rn. 75). Allerdings ist es dafür ausreichend, *„wenn er [der Verantwortliche] sich über die Rechtswidrigkeit seines Verhaltens nicht im Unklaren sein konnte, gleichviel, ob ihm dabei bewusst war, dass es gegen die Vorschriften der DSGVO verstößt“* (Rn. 76). Dies öffnet dem Ansatz über ein Organisationsverschulden – also dem Vorwurf, dass eine unzureichende Datenschutzorganisation im Unternehmen den Verstoß „ermöglicht“ hat – Tür und Tor. Hier gibt es noch viel zu diskutieren; einiges spricht allerdings schon nach den ersten Analysen der Entscheidung dafür, dass das Bußgeldrisiko damit steigt.

Umsätze der gesamten Unternehmensgruppe

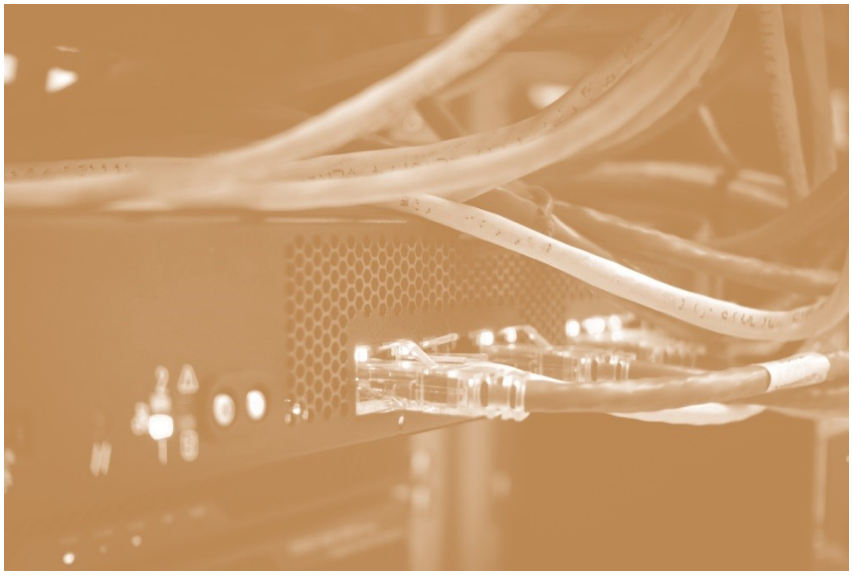
Schließlich hat der EuGH die Befürchtungen bestätigt, dass der für die Bußgeldbemessung relevante Umsatz anhand der gesamten Gruppenumsätze zu berechnen ist: Erwägungsgrund 150 verweist auf das aus dem Kartellrecht bekannte Prinzip, auf die wirtschaftliche Einheit abzustellen. Dies gilt nun bestätigt auch für die DSGVO: Für die Bußgeldbemessung sind die Umsätze von allen verbundenen Unternehmen, also in der Regel dem „Konzern“ bzw. der „Gruppe“, zusammen zu rechnen (Rn. 53 ff.).

Ausblick: Datenschutz-Compliance

Bußgeldrisiken können nach der EuGH-Entscheidung vor allem durch ein effektives Datenschutz-Compliancemanagement vermieden werden. Hierauf sollten Unternehmen ein verstärktes Augenmerk legen.

Welche Bedeutung der EuGH-Entscheidung für die Unternehmenspraxis im Einzelnen zukommen, diskutieren wir mit Ihnen im Rahmen unseres Lunch@Loschelder-Webinars am 24.01.2024. Wir freuen uns über Ihre Anmeldung unter

webinare@loschelder.de (Teilnahme kostenfrei, weitere Informationen auch zeitnah hier).



Uferlose Schadensersatzrisiken nach neuen EuGH-Entscheidungen?

Der EuGH hat in zwei Entscheidungen die Anforderungen an einen immateriellen Schadensersatz nach DSGVO-Verstoß konkretisiert. Hoch praxisrelevant sind dabei gerade die Anforderungen an Schadensersatzforderungen gegen die Opfer eines Hackerangriffs: Müssen Unternehmen auch dann noch Schadensersatz an betroffene Personen zahlen? In der Praxis wird bereits befürchtet, dass nun die Massenklagen anrollen. Aber ist das wirklich so? Eine genaue Betrachtung der beiden Urteile lohnt sich!

Kommt es nach einem schuldhaften DSGVO-Verstoß zu einem Vermögensschaden, liegen Schadensersatzansprüche auf der Hand. Was aber ist, wenn es an einem materiellen Schaden fehlt, die Betroffenen allerdings immaterielle Schäden beklagen? Wie intensiv muss die Beeinträchtigung sein, um einen Ausgleich in Geld zu erhalten – und wie ist die Beeinträchtigung nachzuweisen?

Insbesondere: Was gilt nach einem Hackerangriff, wenn Daten der Betroffenen unbefugt eingesehen, wurden? Muss das Opfer des Hackerangriffs wegen des Vorfalls an sich Schadensersatz leisten?

Der EuGH hat sich dieser Fragen angenommen. Im ersten Fall ging es um die bloße Befürchtung eines Datenmissbrauchs nach einem Hackerangriff (Rs. C-340/21), im zweiten Fall um die Namensnennung in öffentlichen Dokumenten (Rs. C-456/22).

Angst vor Datenmissbrauch und die Anforderungen an die Datensicherheit

Der Fall

Hacker haben auf das Computersystem der bulgarischen Behörde NAP zugegriffen. Laut Medienberichten wurde dabei personenbezogene Steuer- und Sozialversicherungsdaten von mehreren Millionen Personen abgegriffen und im Internet veröffentlicht. Die Klägerin des Ausgangsverfahrens verlangte daraufhin von der NAP Schadensersatz aus Art. 82 DSGVO, wozu der EuGH im Rahmen eines Vorabentscheidungsverfahrens angerufen wurde. Zu den Schlussanträgen in diesem Verfahren berichteten wir in unserem Newsletter aus Mai 2023.

Die EuGH-Entscheidung

Die EuGH-Entscheidung erging am 14.12.2023 (Rs. C-340/21). Die für die Praxis wichtigsten Aussagen des EuGH betreffen die Anforderungen an die **angemessene Datensicherheit** und den **immateriellen Schadensnachweis**:

1. Ein (erfolgreicher) Hackerangriff alleine belegt nicht, dass das angegriffene Unternehmen keine ausreichenden technischen und organisatorischen Schutzmaßnahmen ergriffen hatte.

   Auch im neuen IT-Sicherheitsrecht, das bislang im Entwurf vorliegt, werden folgerichtig lediglich Risikomanagementmaßnahmen verlangt, die die Auswirkungen von Cyber-Attacken geringhalten. Vermieden werden können diese bisweilen selbst bei optimaler IT-Sicherheit nicht.

2. Allerdings trägt das angegriffene Unternehmen auch im Rahmen einer Schadensersatzklage die **Beweislast für angemessene Sicherheitsmaßnahmen**. Dieses muss sich entlasten und nicht der Kläger eine unzureichende Sicherheit nachweisen.

3. Ein immaterieller Schaden i.S.d. Art. 82 Abs. 1 DSGVO kann auch schon dann vorliegen, wenn die betroffene Person infolge eines Verstoßes gegen die DSGVO **die Befürchtung hat**, dass ihre personenbezogenen Daten durch Dritte missbräuchlich verwendet werden könnten. Der Datenmissbrauch muss (noch) nicht stattgefunden haben. Allerdings muss die betroffene Person ihre **Befürchtung nachweisen**.

Voraussetzungen des immateriellen Schadensersatzes

Der Fall

Die Gemeinde Ummendorf hatte auf ihrer Internetseite für einen Zeitraum von drei Tagen ohne Einwilligung der Kläger deren Namen sowie Anschrift im Zusammenhang mit der Tagesordnung einer Gemeinderatssitzung sowie eines Gerichtsurteils veröffentlicht. Die Kläger machten wegen der unzulässigen Offenlegung ihrer Daten immateriellen Schadensersatz geltend.

Das im Berufungsverfahren mit der Sache befasste Landgericht Ravensburg war sich unsicher, ob tatsächlich ein immaterieller Schaden entstanden ist. Daher bat das LG Ravensburg den EuGH um Auskunft im Rahmen eines Vorabentscheidungsverfahrens zu der Frage, ob die Annahme eines immateriellen Schades einen spürbaren Nachteil und eine objektiv nachvollziehbare Beeinträchtigung persönlichkeitsbezogener Belange erfordert oder ob bereits der kurzzeitige Verlust des Betroffenen über die Hoheit seiner Daten, der ohne spürbare und nachteilige Konsequenzen für den Betroffenen blieb, für die Annahme eines immateriellen Schadens genügt.

Die EuGH-Entscheidung

Das EuGH-Urteil vom 14.12.2023 in dieser Rechtssache C-456/22 ist weitreichend: Die Veröffentlichung der Daten im Internet sowie der daraus resultierende – kurzzeitige – Verlust der Datenhoheit kann zu einem immateriellen Schaden führen. Auch ein Bagatellschaden begründet einen Schadensersatzanspruch. Allerdings muss der Betroffene nachweisen, dass er tatsächlich einen Schaden erlitten hat, wie gering dieser auch sein mag.

Fazit

Der EuGH knüpft inhaltlich an vergangene Urteilen zum immateriellen Schadensersatz an. Bereits in den Verfahren Österreichische Post und Identitätsdiebstahl Rs. C-182/22 und C-189/2 hatte der EuGH klargestellt, dass zwar auch Bagatellschäden vom immateriellen Schadensersatz umfasst sind, jeder Schaden aber nachgewiesen werden muss. Der bloße DSGVO-Verstoß begründet noch keinen Schadensersatzanspruch (wir berichteten hier). Insofern bleibt der EuGH seiner bisherigen Linie treu.

Insgesamt scheinen die Anforderungen aber zunehmend zu sinken. So kann bereits die begründete **Befürchtung** eines Datenmissbrauchs zu einem Schaden führen. Nach Hackerangriffen sind zudem die Opfer in der **Beweislast**, dass die von ihnen ergriffenen Sicherheitsmaßnahmen angemessen waren, um einen Schadensersatzanspruch abzuwehren.

Dies verdeutlicht, wie wichtig eine ausreichende Informationssicherheit im Unternehmen ist – ganz ungeachtet der aktuellen gesetzgeberischen Entwicklungen zum neuen IT-Sicherheitsrecht und dem Cyber Resilience Act aus der EU.

Welche Bedeutung den EuGH-Entscheidungen für die Unternehmenspraxis im Einzelnen zukommen, diskutieren wir mit Ihnen im Rahmen unseres Lunch@Loschelder-Webinars am 31.01.2024. Wir freuen uns über Ihre Anmeldung unter webinare@loschelder.de (Teilnahme kostenfrei, weitere Informationen auch zeitnah hier).

EuGH: Die erste Kopie geht aufs Haus

Der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DSGVO hält nach wie vor Unternehmen sowie Gerichte auf Trapp. Nun hat der EuGH eine bemerkenswerte Entscheidung getroffen, die sich ausführlich mit den Voraussetzungen des Auskunftsanspruchs befasst und klarstellt, unter welchen Bedingungen dieser durch nationale Rechtsvorschriften eingeschränkt werden kann.

In dem zugrundeliegenden Sachverhalt ging es um einen Patienten, der bei einem Zahnarzt in Behandlung war und, da er einen Behandlungsfehler vermutete, um eine erste Kopie seiner Patientenakte bat. Der Zahnarzt wollte dieser Bitte nur nachkommen, wenn der Patient die Kosten hierfür übernimmt, wie dies im BGB vorgesehen ist (§ 630g Abs. 2 Satz 2 BGB). Nachdem der Patient Klage auf eine unentgeltliche Herausgabe der ersten Kopie der Patientenakte erhob, bekam dieser in der ersten und zweiten Instanz Recht. Der sodann mit der Revision befasste BGH war der Ansicht, dass es bei der Entscheidung darauf ankäme, wie die maßgeblichen Bestimmungen der DSGVO auszulegen seien und legte daher diesbezügliche Fragen dem EuGH zur Vorabentscheidung vor. Dieser hat nunmehr in seinem Urteil vom 26.10.2023 die vorgelegten Fragen beantwortet (Rs. C-307/22). Zu den Schlussanträgen berichteten wir bereits an dieser Stelle.

Voraussetzungen des Anspruchs auf eine kostenfreie Kopie

In einer ersten Frage wollte der BGH wissen, ob der Anspruch auf Herausgabe einer kostenfreien Kopie nach Art. 15 Abs. 3 S. 1 DSGVO auch dann bestehe, wenn der Betroffene die Kopie nicht zur Verfolgung einer der in Erwägungsgrund 63 der DSGVO näher bezeichneten Zwecke, sondern zur Verfolgung eines datenschutzfremden Zwecks herausverlangt (hier: Nachweis Behandlungsfehler).

Der EuGH sieht einen **bedingungslosen Anspruch auf Kopie**: Unternehmen müssen auch dann eine erste unentgeltliche Kopie nach Art. 15 DSGVO herausgeben, wenn das Auskunftsersuchen andere als die in Erwägungsgrund 63 genannten Ziele verfolgt.

Zur Begründung äußerte sich der EuGH im Wesentlichen wie folgt:

1. Nur bei rechtsmissbräuchlicher Ausübung des Auskunftsrechts muss der Betroffene zahlen (Art. 12 DSGVO). Die Verfolgung anderer Ziele begründet noch keinen Rechtsmissbrauch.

2. Das Auskunftsrecht aus Art. 15 DSGVO umfasst nach seinem Absatz 3 auch ein Recht auf kostenfreie Kopie. Dieser Anspruch besteht unabhängig von einer Begründung.

3. Die Erwägungsgründe der DSGVO sind nicht rechtsverbindlich.

Abweichende nationale Regelungen?

Die DSGVO belässt in den ausgewiesenen Bereichen dem nationalen Gesetzgeber Gestaltungsspielräume. Dieser Spielraum kann nach dem EuGH auch durch Normen ausgefüllt werden, die bereits vor Inkrafttreten der DSGVO erlassen wurden. Voraussetzung ist aber auch dann, dass diese Regelungen den Rechten und Pflichten der DSGVO entsprechen, den Wesensgehalt der Grundrechte und Grundfreiheiten achten und verhältnismäßig sind.

Damit stünde eine Entgeltpflicht für die erste Kopie zu beauskunftender Daten nicht im Einklang. § 630g Abs. 2 Satz 2 BGB erfülle diese Voraussetzungen nicht.

Der EuGH weicht hier von den Schlussanträgen ab – dies geschieht selten. Zur Begründung führt der EuGH u.a. an, dass § 630g Abs. 2

Satz 2 BGB nicht dem Schutz der Rechte und Freiheiten anderer Personen diene, sondern lediglich dem wirtschaftlichen Interesse des Verantwortlichen. Zudem stünde die Vorschrift dem Grundsatz der Unentgeltlichkeit der ersten Kopie diametral entgegen und sei daher nicht geeignet, den Anspruch auf eine erste unentgeltliche Kopie einzuschränken.

Fazit

Das Auskunftsrecht aus Art. 15 DSGVO ist denkbar weit, einschließlich des Rechts auf Kopie. Dennoch ist im Einzelnen genau hinzusehen: Das Recht auf Kopie ergänzt den Auskunftsanspruch nach Absatz 1 und steht nicht losgelöst. In Kopie herauszugeben ist nur, was für das Verständnis der Auskunft nach Absatz 1 erforderlich ist, nicht alles, was der Betroffene begehrt. Wir berichteten dazu bereits ausführlich in unserer Mai-Ausgabe.

Gemeinsame Verantwortlichkeit setzt keine Vereinbarung voraus

In einem weiteren Urteil hat der EuGH die Voraussetzungen für eine „gemeinsame Verantwortlichkeit" geschärft. Sind mehrere Akteure derart gemeinsam verantwortlich, müssen sie dazu eine Vereinbarung schließen und die Rollen klar verteilen. In der Praxis ist besonders relevant, dass die Akteure dann auch gemeinsam (gesamtschuldnerisch) haften. Dies führt in vielen Fällen zu dem Bemühen, eine gemeinsame Verantwortlichkeit zu vermeiden, um Haftungsdiffusionen auszuschließen. Wann dies noch möglich ist, erläutern wir im nachfolgenden Beitrag.

Dem Urteil des EuGH vom 05.12.2023 in der Rs. C-683/21 liegt ein litauischer Sachverhalt zugrunde: Das nationale Zentrum für öffentliche Gesundheit beim litauischen Gesundheitsministerium (NZÖG) beauftragte ein IT-Unternehmen mit der Entwicklung einer App zur epidemiologischen Erfassung und Überwachung von Daten von mit Covid-19 infizierten Personen. Wegen Verstößen gegen die DSGVO bei der Verarbeitung personenbezogener Daten in dieser App wurde ein Bußgeld gegen das NZÖG sowie gegen das IT-Unternehmen als gemeinsam Verantwortliche verhängt. Jedoch sahen sich weder das NZÖG noch das IT-Unternehmen als Verantwortlicher i.S.d. DSGVO und somit nicht als richtiger Adressat des Bußgeldbescheids.

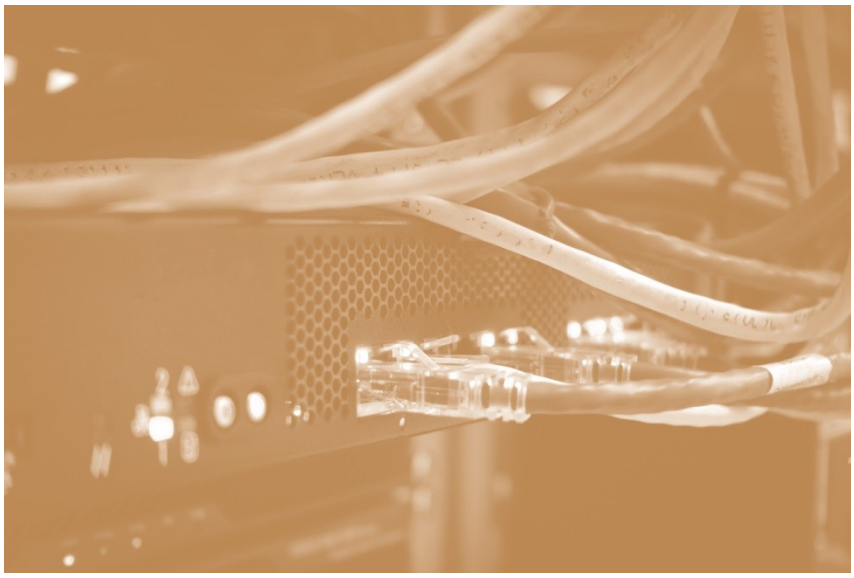
Laut DSGVO ist „verantwortlich", wer über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Davon ausgehend fällt laut EuGH auch eine Einrichtung (hier: das NZÖG) unter diesen Begriff, die ein Unternehmen mit der Erstellung einer App beauftragt und in diesem Zusammenhang an der Entscheidung über die Verarbeitungszwecke und -mittel mitwirkt.

Hierbei kommt es alleine auf die tatsächlichen Umstände an. Eine vorherige Vereinbarung dazu ist nicht erforderlich. Vielmehr kann diese Mitwirkung unabhängig von einer förmlichen Vereinbarung in verschiedenen Formen erfolgen. Aus der Einstufung als gemeinsame Verantwortliche – aber auch erst dann – ergibt sich anschließend die Pflicht, einen Vertrag gem. Art. 26 DSGVO zu schließen und zu vereinbaren, wer welche Pflichten aus der DSGVO erfüllt.

Für die Annahme einer gemeinsamen Verantwortlichkeit war vorliegend für den EuGH entscheidend, dass das NZÖG die Ziele gesetzt hat, die mit der App umgesetzt werden sollten, und damit zugleich die Zwecke der Verarbeitung personenbezogener Daten mitbestimmt hat. Dass NZÖG als Verantwortlicher in der Datenschutzerklärung genannt war, hatte dagegen keinen maßgeblichen Einfluss – dies sei nur dann der Fall, wenn NZÖG dem (stillschweigend) zugestimmt hätte.

Nicht maßgeblich gegen eine gemeinsame Verantwortlichkeit spricht dagegen, dass NZÖG selbst keinen Zugriff auf die personenbezogenen Daten hatte. Dies entspricht der bisherigen Rechtsprechungslinie.

Die Entscheidung hilft in der Praxis enorm: Maßgeblich ist zu untersuchen, wer die Zwecke und Mittel tatsächlich beeinflusst und mitbestimmt. Wenn dies nicht geschieht, wie bisweilen bei den Anwendern großer IT-Produkte, dann spricht das gegen eine gemeinsame Verantwortlichkeit.



Die SCHUFA und der Datenschutz

SCHUFA-Auskünfte und die Grundlagen des Scorings für Bonitätsauskünfte sind datenschutzrechtlich seit jeher höchst umstritten. Angesichts der erheblichen Folgen (falscher) negativer Bonitätsauskünfte für die Betroffenen liegt dies auf der Hand. Schon das BDSG alt enthielt daher Sonderregelungen für das Scoring. Was unter der DSGVO gilt, hat nun der EuGH konkretisiert.

Scoring

Das sog. „Scoring" war Gegenstand eines aktuell vom EuGH entschiedenen Vorabentscheidungsverfahrens (Rs. C-634/21). Dabei handelt es sich um eine Methode, mit deren Hilfe die Wahrscheinlichkeit eines künftigen Verhaltens (bspw. die Rückzahlung eines Kredits) vorhergesagt werden kann. Das „Scoring" wurde nun vom EuGH als eine „automatisierte Entscheidung im Einzelfall" bewertet, die von der DSGVO grundsätzlich verboten ist (Art. 22 DSGVO). Das allerdings unter der Voraussetzung, dass Banken dem „Score-Wert" eine maßgebliche Rolle im Rahmen der Kreditgewährung beimessen, denn nach Art. 22 DSGVO sind automatisierte Entscheidungen nur dann verboten, wenn sie auch rechtlich erheblich sind für die Betroffenen.

Informationen über Restschuldbefreiung dürfen nur begrenzt gespeichert werden

Laut EuGH (verb. Rs. C-26/22, C-64/22) widerspricht es der DSGVO, wenn private Auskunfteien (wie die SCHUFA) Daten über die Erteilung einer Restschuldbefreiung länger speichern als das öffentliche Insolvenzregister. Solche Informationen haben stets negative Auswirkungen auf die Bewertung der Kreditwürdigkeit einer Person und somit existenzielle Bedeutung. In Deutschland ist die Speicherung der Daten für sechs Monate erlaubt, eine längere Speicherung ist rechtswidrig und die Informationen müssen gelöscht werden.

Die Bewertung, ob die parallele Speicherung der Daten bei der SCHUFA während der genannten sechs Monate überhaupt rechtmäßig ist, überlässt der EuGH dem vorlegenden Gericht. Auch dies steht mithin noch zur Debatte.

Zu guter Letzt

Zu guter Letzt stellen wir Ihnen in der gebotenen Kürze interessante Urteile deutscher Gerichte vor, die sich zu den Voraussetzungen des Schadensersatzes nach Art. 82 DSGVO äußern. Zudem verlangt die Datenschutzkonferenz eine intensivere Regulierung von Künstlicher Intelligenz (Randnotiz: zu recht, letztlich auch aus Sicht der Entscheider in Brüssel, die sich in letzter Minute politisch im Trilog um die KI-Verordnung einigen konnten).

- **OLG Stuttgart: Kein Schadensersatz für Datenleck bei Facebook in zwei Fällen**

Der 4. Zivilsenat des OLG Stuttgart entschied kürzlich in zwei Fällen über Ansprüche im Zusammenhang mit einem Datenleck bei Facebook. 2018 sei es zu einem Datenabgriff bei Facebook gekommen, bei dem personenbezogene Daten der Kläger ausgelesen und mit deren Handynummern verknüpft wurden. Die Kläger machen gegenüber Meta daher mehrere Verstöße gegen die DSGVO geltend und fordern u.a. immateriellen Schadensersatz, Unterlassung sowie die Feststellung einer künftigen Ersatzpflicht.

Der Senat wies die Klagen überwiegend ab und begründete dies u.a. wie folgt: Die für den Anspruch auf Schadensersatz nach Art. 82 Abs. 1 DSGVO erforderliche spürbare immaterielle Beeinträchtigung der Kläger sei nicht festgestellt worden. Zwar gebe es nach der Rechtsprechung des EuGH diesbezüglich keine Erheblichkeits- oder

Bagatellschwelle, dennoch müsse eine tatsächliche immaterielle Beeinträchtigung festgestellt werden. Bloße Lästigkeit und Unannehmlichkeit sei nicht ausreichend.

- **LAG Düsseldorf: Keine Entschädigung für verspätete und unvollständige Auskunft gem. Art. 15 DSGVO**

Das LAG Düsseldorf lehnte jüngst eine Entschädigung wegen verspäteter und unvollständiger Auskunft ab. Der Kläger war im Jahr 2016 im Kundenservice eines Immobilienunternehmens beschäftigt und machte im Jahr 2020 einen Auskunftsanspruch nach Art. 15 DSGVO gegenüber dem Unternehmen geltend, welchem dieses nachkam. Zwei Jahre später, am 01.10.2022, verlangte der Kläger erneut Auskunft sowie Erhalt einer Kopie nach Art. 15 DSGVO und setzte eine Frist bis zum 16.10.2022. Nachdem das Unternehmen nicht reagierte, erinnerte der Kläger dieses unter erneuter Fristsetzung. Daraufhin folgte ein Schriftwechsel zwischen den Parteien über mehrere Wochen, im Laufe dessen der Kläger wiederholt um weitere und konkrete Auskünfte bat und das Unternehmen diesen zwar teils, aus Sicht des Klägers aber nicht in ausreichendem Maße nachkam. Der Kläger forderte daher Schadensersatz nach Art. 82 Abs. 1 DSGVO in Höhe von mindestens 2.000 Euro wegen Verletzung seines Auskunftsrechts nach Art. 15 DSGVO.

Das LAG wies die Klage – anders, als noch die erste Instanz – ab. Es begründet seine Entscheidung zum einen damit, dass ein Verstoß gegen Art. 15 DSGVO keinen Schadensersatzanspruch nach Art. 82 DSGVO begründe, da es gerade nicht um die von Art. 82 DSGVO vorausgesetzte rechtswidrige Datenverarbeitung ginge. Zum anderen genüge es für einen Schadensersatzanspruch nicht, lediglich einen Verstoß gegen die DSGVO nachzuweisen. Letzteres hat der EuGH jüngst bestätigt, wie wir in diesem Newsletter an anderer Stelle berichten.

- **DSK fordert Regulierung von Künstlicher Intelligenz**

In einer kürzlich veröffentlichten Pressemitteilung fordert die Datenschutzkonferenz (DSK), dass in dem im Gesetzgebungsverfahren befindlichen europäischen Gesetz über künstliche Intelligenz (KI-Verordnung) die Verantwortlichkeiten entlang der gesamten KI-Wertschöpfungskette sachgerecht zugewiesen werden. Dies sei erforderlich, um die Grundrechte

derjenigen zu schützen, deren Daten durch KI verarbeitet werden. Rechtsunsicherheiten hinsichtlich der Verantwortlichkeiten gingen zulasten der Betroffenen. Die Stellungnahme der DSK ist eine Reaktion auf ein Positionspapier der Regierungen der EU-Mitgliedstaaten Frankreich, Italien und Deutschland, welche sich gegen verbindliche Vorgaben für Basismodelle und somit für die Selbstregulierung ohne Sanktionen ausgesprochen haben. Nach langem Ringen konnte vor einer guten Woche eine politische Einigung im Trilog erzielt werden, die dem Vernehmen nach – Texte fehlen noch – einen Kompromiss auch für die Regulierung von Basismodellen gefunden hat.

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