LOSCHELDER

Newsletter Datenschutzrecht
Oktober 2024

Sehr geehrte Damen und Herren,

der Herbst ist da – und bringt mal wieder einige neue EuGH-Entscheidungen zum Datenschutz. In diesem Newsletter bereiten wir für Sie diese neue Rechtsprechung kurz und bündig auf.

Den EuGH beschäftigte zunächst die Frage, ob ein rein wirtschaftliches Interesse ein „berechtigtes Interesse" zur Verarbeitung personenbezogener Daten sein kann. Die Antwort: Ja, solange – wie üblich – dabei die Interessen der betroffenen Personen nicht überwiegen. In einem weiteren Verfahren stellte der EuGH klar, dass die DSGVO es nicht ausschließt, dass Mitbewerber wegen Datenschutzverstößen nach nationalem Wettbewerbsrecht Zivilklage erheben. Immer wieder Gegenstand von EuGH-Urteilen ist Meta's Facebook, dieses Mal geht es um die Datennutzung durch soziale Netzwerke zu Werbezwecken. Die Datennutzung wird jetzt weiter beschränkt, sowohl zeitlich als auch hinsichtlich der Art der verwendbaren Daten. Zum Thema Sanktionen bei DSGVO-Verstößen entschied der EuGH, dass Aufsichtsbehörden nicht zur Verhängung von Bußgeldern verpflichtet sind. Ihnen steht ein Spielraum hinsichtlich der Entscheidung zu, überhaupt eine Aufsichtsmaßnahme zu ergreifen und ein Bußgeld zu verhängen.

Nicht vom EuGH, aber dennoch datenschutzrechtlich interessant ist ein Urteil des OLG Hamm über eine Datenpanne in einem ehemaligen Corona-Impfzentrum. Darin werden die Anforderungen an organisatorische Sicherheitsmaßnahmen sowie an einen immateriellen Schaden konkretisiert. Damit wird die Reihe bereits ergangener Urteile zum immateriellen Schadensersatz fortgeführt.

Webinar-Ankündigung:

Neben datenschutzrechtlichen Neuerungen begleiten wir auch die weiteren Digitalisierungsakte der EU. Mit Blick auf die im August 2024 in Kraft getretene KI-Verordnung ergeben sich zahlreiche neue Fragen. Allen voran: Wer wird wozu verpflichtet, gerade jenseits der großen KI-Entwickler? Die Verordnung ist für alle Unternehmen relevant, die KI-Anwendungen intern betreiben. Und dank der weiten KI-Definition in der KI-Verordnung steckt künstliche Intelligenz in verdammt vielen digitalen Anwendungen! Wir beleuchten in unserem Lunch@Loschelder-Webinar, welche Pflichten die KI-Verordnung für die „Old Economy" und all jene

Unternehmen bringt, die nicht wie Mistral, Aleph Alpha oder OpenAI in vorderster Reihe der KI-Entwickler stehen.

Welche Pflichten bringt die KI-Verordnung für die Unternehmen?

Dienstag, den 19. November 2024 - 12.00 bis 12.45 Uhr

Ihre Referentin: Dr. Kristina Schreiber

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.

Inhalt

EuGH: Auch rein wirtschaftliches Interesse von Unternehmen kann „berechtigtes Interesse“ sein

Das „berechtigte Interesse“ i.S.v. Art. 6 Abs 1 UAbs. 1 lit. f DSGVO ist weit auszulegen. Dies hat der EuGH nun bestätigt. Im Fall des niederländischen Tennisverbands entschied das Gericht, dass auch rein wirtschaftliche Interessen „berechtigte Interessen“ sein können. Für die Praxis ist das von großer Bedeutung.

Der Fall

Im Jahr 2018 legte der niederländische Tennisverband KNLTB gegenüber zwei Sponsoren, darunter dem größten Anbieter von Glücks- und Kasinospielen in den Niederlanden, personenbezogene Daten seiner Mitglieder offen. Für die Bereitstellung der betreffenden personenbezogenen Daten erhielt der KNLTB von seinen Sponsoren ein Entgelt. Der KNLTB stellte die Namen, Anschriften und Wohnorte seiner Mitglieder für den postalischen Versand eines Werbebriefs bereit. Außerdem legte der KNLTB Geburtsdaten, Festnetznummern, Mobiltelefonnummern und E-Mail-Adressen seiner Mitglieder sowie die Namen der Tennisclubs offen, denen diese Mitglieder angehörten. Zweck dieser Bereitstellung war eine Telefonwerbemaßnahme. Auf Beschwerden einiger Mitglieder stellte die niederländische Aufsichtsbehörde fest, dass für die Weitergabe der personenbezogenen Daten keine Rechtsgrundlage bestanden habe. Ein berechtigtes Interesse i.S.v. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO des Tennisverbands habe nicht vorgelegen. Der niederländische Tennisverband klagte gegen diese Entscheidung und das zuständige Bezirksgericht Amsterdam legte dem EuGH die Frage vor, ob auch rein wirtschaftliche Interessen ein „berechtigtes Interesse“ i.S.v. Art. 6 Abs. 1 UAbs. 1lit. f DSGVO darstellen.

„Berechtigtes Interesse“ muss nicht gesetzlich geregelt und kann rein wirtschaftlich sein

Hierauf antwortet der EuGH zunächst mit der Feststellung, dass der Begriff des „berechtigten Interesses“ i.S.v. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO nicht auf gesetzlich verankerte und bestimmte Interessen beschränkt ist (EuGH, Urteil vom 04.10.2024 – C-621/22). Dies ergebe sich aus Erwägungsgrund 47 der DSGVO. Das „berechtigte Interesse“ müsse allerdings rechtmäßig sein. Sodann führt der EuGH aus, dass auch ein wirtschaftliches Interesse ein „berechtigtes

Interesse“ darstellen könne, sofern es nicht gesetzeswidrig ist. In diesem Fall müsse der Verantwortliche aber allen anderen ihm obliegenden Pflichten aus der DSGVO nachkommen, damit die Wahrnehmung dieses Interesses eine Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO rechtfertigen kann.

Strenge Anforderungen an Erforderlichkeit und Interessenabwägung

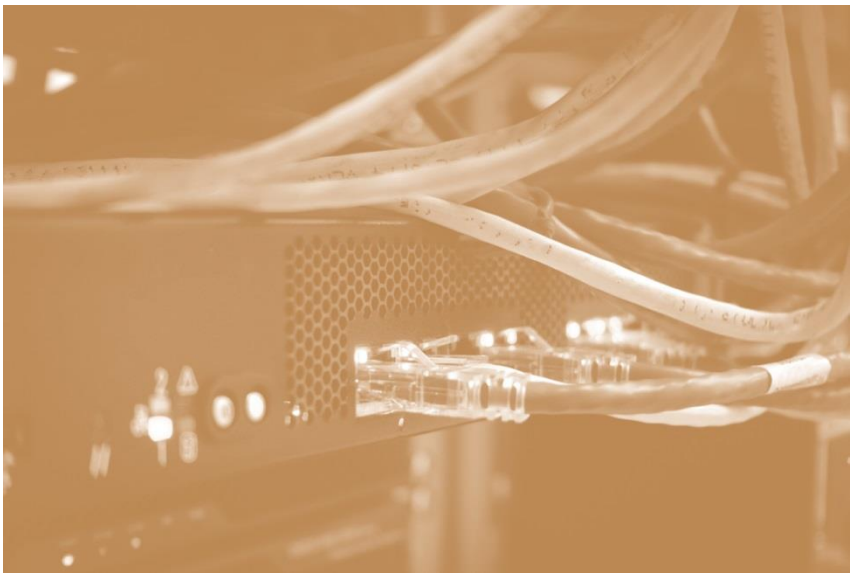
Zugleich betont der EuGH jedoch, dass an die zweite und dritte Stufe der Rechtmäßigkeitsprüfung bei einer Datenverarbeitung aufgrund eines „berechtigten Interesses“ (namentlich Erforderlichkeit und Interessenabwägung) hohe Anforderungen zu stellen sind. Insbesondere sei für den niederländischen Tennisverband im vorliegenden Fall als milderes Mittel in Betracht gekommen, seine Mitglieder im Voraus zu informieren und sie zu fragen, ob sie möchten, dass ihre Daten für Werbe- oder Marketingzwecke an Dritte weitergegeben werden. Im Rahmen der Interessenabwägung sei zudem zu berücksichtigen, ob die Mitglieder zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten zum Zweck des Beitritts zu einem Tennisverein vernünftigerweise absehen konnten, dass diese Daten gegen Entgelt für Werbe- und Marketingzwecke gegenüber Dritten, im vorliegenden Fall Sponsoren des KNLTB, offengelegt werden. Auch der Umstand, an wen die Daten übermittelt werden, sei zu berücksichtigen. So würden durch die Übermittlung an Anbieter von Glücks- und Kasinospielen Mitglieder der Gefahr der Entwicklung einer Spielsucht ausgesetzt.

„Berechtigtes Interesse“ als Türöffner – Feintuning über Stufen 2 und 3

Das Urteil zeigt, dass das „berechtigte Interesse“ als Türöffner für die Rechtmäßigkeitsprüfung einer Datenverarbeitung zu verstehen und als solcher weit auszulegen ist. Dass auch rein wirtschaftliche Interessen dem Anwendungsbereich von Art. 6 Abs. 1 lit. f DSGVO unterfallen, stellt für Unternehmen eine begrüßenswerte Entwicklung dar. Die eigentliche Rechtmäßigkeitsprüfung erfolgt indes auf zweiter und dritter Stufe der Erforderlichkeit bzw. Interessenabwägung. Und die hieran zu stellenden Anforderungen sind durchaus hoch, wie der EuGH im vorliegenden Fall noch einmal unterstrichen hat.

Neue EDSA-Leitlinien

Das berechtigte Interesse als Erlaubnisgrundlage ist derzeit auch Gegenstand neuer EDSA-Leitlinien 1/2024, die noch bis Ende November konsultiert werden.



EuGH: Wettbewerbsrechtliche Klage bei DSGVO-Verstoß möglich und weiter Begriff „Gesundheitsdaten“

Eine Klage gegen einen Mitbewerber wegen eines DSGVO-Verstoßes, der als unlautere Geschäftspraktik geltend gemacht wird, ist möglich. Das entschied der EuGH in einem kürzlich ergangenen Urteil. Dabei ging es um den DSGVO-widrigen Vertrieb von Arzneimitteln über eine Online-Plattform. Im Ausgangsfall wurde durch den Verkäufer beim Bestellprozess keine datenschutzrechtliche Einwilligung in die Verarbeitung von Gesundheitsdaten von den Kunden eingeholt. Der EuGH musste sich deshalb auch mit der Frage auseinandersetzen, ob die beim Bestellvorgang eingegebenen Kundendaten Gesundheitsdaten im Sinne der DSGVO darstellen.

Die Möglichkeit, nach nationalen wettbewerbsrechtlichen Vorschriften gegen Datenschutzverstöße eines Mitbewerbers zu klagen, wird nicht durch die DSGVO ausgeschlossen. Zu diesem Schluss kam der EuGH in seinem Urteil vom 4. Oktober 2024 zur Rechtssache C-21/23; die Frage war zuvor umstritten.

Der Fall

Sowohl Kläger als auch Beklagter im Ausgangsverfahren waren Betreiber von Apotheken. Der Beklagte vertreibt Arzneimittel in seiner Apotheke sowie online über Amazon. Bei der Bestellung der Medikamente müssen die Kunden ihre Daten wie Namen, Lieferadresse und Informationen zur Individualisierung des Arzneimittels angeben. Dabei holte der Beklagte keine datenschutzrechtliche Einwilligung in die Verarbeitung von Gesundheitsdaten ein. Der Kläger beantragte deshalb vor dem Landgericht Dessau-Roßlau, zu verbieten, dass der Beklagte weiterhin online Arzneimittel verkauft, ohne dabei eine entsprechende datenschutzrechtliche Einwilligung der Kunden einzuholen. Es handele sich hierbei um eine unlautere Handlung, die nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) unzulässig sei.

Zivilrechtliche Klage eines Mitbewerbers zulässig

Dem EuGH wurde hierzu zum einen die Frage vorgelegt, ob es für Mitbewerber (hier den anderen Apothekenbetreiber) überhaupt möglich ist, vor nationalen Zivilgerichten gegen DSGVO-Verstöße vorzugehen. In der DSGVO selbst sind nämlich Rechtsbehelfe bei DSGVO-Verstößen vorgesehen. Danach ist es grundsätzlich Sache der betroffenen Personen – in diesem Fall der Kunden – Verstöße gegen den Schutz der sie betreffenden personenbezogenen Daten geltend zu machen. Möglich sind z.B. die Beschwerde bei einer Aufsichtsbehörde oder gerichtliche Rechtsbehelfe gegen den Verantwortlichen.

Nach Ansicht des EuGH schließt die DSGVO eine zivilgerichtliche Geltendmachung von DSGVO-Verstößen durch Mitbewerber jedoch nicht aus. Der DSGVO-Verstoß kann wettbewerbsrechtlich als unlautere Geschäftspraktik im Sinne des UWG geltend gemacht werden. Dass nicht ausschließlich betroffene Personen zu datenschutzrechtlichen Klagen befugt sind, trage dazu bei, die Rechte betroffener Personen in Bezug auf ihre Daten zu stärken und das in der EU angestrebte hohe Schutzniveau personenbezogener Daten zu gewährleisten. Durch diese Möglichkeit können insgesamt mehr Datenschutzverstöße geltend gemacht werden, was auch zu einer besonders wirksamen Erhaltung dieses hohen Datenschutzniveaus beiträgt.

Welche Folgen dies wettbewerbsrechtlich hat, haben unsere Kollegen aus dem gewerblichen Rechtsschutz im Blick und etwa hier bereits zusammengefasst (dort von Dr. Stefan Maaßen). Relevanz wird die Entscheidung für Unternehmen haben, die mehr als 250 Mitarbeiter beschäftigen: Diese können kostenpflichtig wegen jedes kleinen Datenschutzverstoßes abgemahnt werden.

Kundendaten sind Gesundheitsdaten

In der zweiten Vorlagefrage befasste sich der EuGH damit, ob es sich überhaupt bei den beim Online-Kauf angegebenen Kundendaten um Gesundheitsdaten im Sinne der DSGVO handelt. Gesundheitsdaten sind alle personenbezogenen Daten, die Rückschlüsse auf den Gesundheitszustand der jeweiligen Person zulassen. Sie gehören zu den besonders geschützten Kategorien von personenbezogenen Daten. Ihre Verarbeitung ist nur unter bestimmten Voraussetzungen gem. Art. 9 Abs. 2 DSGVO zulässig, u.a., wenn eine ausdrückliche Einwilligung in die Datenverarbeitung erteilt wurde.

Die eingegebenen Kundendaten sind unzweifelhaft Gesundheitsdaten, wenn verschreibungspflichtige Medikamente bestellt werden. Die Bestellung eines Medikaments ermöglicht es, einen Zusammenhang zwischen dessen therapeutischen Indikationen und der durch die Angaben identifizierbaren Person herzustellen – wird ein Rezept vorgelegt, ist eindeutig, für welche Person das Medikament bestimmt ist.

Aber ist das auch bei den nicht-verschreibungspflichtigen OTC-Arzneimitteln der Fall? Diese können für jedermann bestimmt sein. Der BGH zweifelte daher in seinem Vorlagebeschluss daran, sie als Gesundheitsdaten qualifizieren (wir berichteten hier). Der EuGH zweifelt nicht: Er ordnet auch diese Daten als Gesundheitsdaten ein. Zwar könne es sein, dass diese nicht für den Kunden selber, sondern für einen Dritten bestellt werden. Laut EuGH kann allerdings auch dabei auf den Gesundheitszustand einer natürlichen Person geschlossen werden – unabhängig davon, ob es sich dabei um den Kunden oder eine andere Person handelt. Die bloße „gewisse Wahrscheinlichkeit“ dafür, dass der Kunde selber die Medikamente benötigt, reicht aus, um die Eigenschaft der Kundendaten als Gesundheitsdaten zu bejahen. Dies liegt auf der Linie der bisherigen Rechtsprechung des EuGH, die Begriffe des Art. 9 DSGVO für den bestmöglichen Schutz äußerst weit auszulegen (siehe dazu auch schon hier).

Für die Praxis bringt diese weite Auslegung enorme Herausforderungen, da in etlichen Fällen von Art. 9er-Daten auszugehen und so auf die zusätzliche Erlaubnis nach Art. 9 Abs. 2 DSGVO abzustellen ist.

EuGH: Neue Beschränkungen für soziale Netzwerke bei Datennutzung zu Werbezwecken

Soziale Netzwerke dürfen nicht alle Daten ihrer Nutzer für Werbewecke verwenden. Außerdem ist eine zeitlich unbegrenzte Verwendung unzulässig. Dies entschied der EuGH in einem Verfahren des österreichischen Datenschutzaktivisten Maximilian Schrems gegen den Facebook-Mutterkonzern Meta. Für Meta ist es derweil nicht der einzige datenschutzrechtliche Verstoß in jüngster Zeit.

Worum es beim EuGH ging

Der österreichische Datenschutzaktivist Maximilian Schrems hatte gegen die Verarbeitung seiner personenbezogenen Daten, insbesondere der Daten zu seiner sexuellen Orientierung, durch den Facebook-Mutterkonzern Meta geklagt. Schrems hatte sich bei einer Podiumsdiskussion zu seiner sexuellen Orientierung geäußert. Meta nutzte diese Informationen für personalisierte Werbung auf seinem Netzwerk Facebook. Das Unternehmen nahm die öffentliche Aussage des Klägers zudem zum Anlass, um weitere Daten über die sexuelle Orientierung des Klägers zu verarbeiten, die die Plattform von Partnerwebsites erhalten hatte. Der Kläger gab an, auf Facebook

Werbung erhalten zu haben, die sich gezielt an homosexuelle Personen richtete, ohne dass er auf seinem Profil eine entsprechende sexuelle Orientierung angegeben habe. Er klagte daraufhin vor den österreichischen Gerichten. Der österreichische Oberste Gerichtshof wandte sich schließlich an den EuGH, um im Wesentlichen zwei Auslegungsfragen betreffend die DSGVO klären zu lassen: Erstens sollte der EuGH klären, ob die DSGVO eine unbegrenzte Analyse und Verarbeitung personenbezogener Daten zu Werbezwecken zulässt. Zweitens wurde die Frage aufgeworfen, ob Facebook die Informationen über die sexuelle Orientierung des Klägers deshalb verarbeiten durfte, weil dieser die entsprechenden Informationen auf der Podiumsdiskussion öffentlich gemacht hat (EuGH, Urteil vom 04.10.2024 – C-446/21).

Keine zeitlich unbegrenzte Datenverarbeitung

Für die Beantwortung der ersten Frage verweist der EuGH auf den in der DSGVO festgelegten Grundsatz der „Datenminimierung". Dieser verbiete es, dass sämtliche personenbezogene Daten, die ein Online-Werbeunternehmen erhält, „zeitlich unbegrenzt und ohne Unterscheidung nach ihrer Art für Zwecke der zielgerichteten Werbung aggregiert, analysiert und verarbeitet werden". Die DSGVO selbst gibt hierfür keine konkrete Frist vor. Auch der EuGH stellt eine solche nicht auf. Er führt im Urteil aber aus, dass jedenfalls eine zeitlich unbegrenzte Verarbeitung von personenbezogenen Daten einen schweren Eingriff in die durch die Art. 7 und 8 der Charta der Grundrechte der Europäischen Union gewährleisteten Rechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten darstelle.

Veröffentlichung von sexueller Orientierung rechtfertigt keine Verarbeitung weiterer Daten

In Bezug auf die zweite Frage führt der EuGH zunächst aus, dass Meta solche Informationen über die sexuelle Orientierung ausnahmsweise verarbeiten dürfe, die die betroffene Person von sich aus (etwa im Rahmen einer Podiumsdiskussion) veröffentlicht hat. Dies berechtige Facebook jedoch nicht dazu, weitere Daten über die sexuelle Orientierung zu verarbeiten. Die bei „offensichtlich öffentlich gemachten" Daten eingreifende Ausnahme zum grundsätzlichen Verbot der Verarbeitung von Daten zur sexuellen Orientierung in Art. 9 Abs. 2 lit. e DSGVO sei eng auszulegen und beschränkte sich auf die konkret veröffentliche Information. Auch

stelle die Veröffentlichung keine Einwilligung zur Verarbeitung weiterer Daten über die sexuelle Orientierung gemäß Art. 9 Abs. 2 lit. a DSGVO dar.

Dies ist nicht der einzige Einschlag in Meta's Darenpraxis in der letzten Zeit. Erst kürzlich ist der Facebook-Mutterkonzern Meta von der irischen Datenschutzkommission (DPC) mit einem Bußgeld in Höhe von 91 Millionen Euro belegt worden, da Meta Passwörter von Facebook- und Instagram-Nutzern unverschlüsselt auf eigenen Servern gespeichert hatte. Der vorliegende Fall könnte weitere Bußgelder und umfangreiche Sammelklagen gegen Meta auslösen.

Keine Bußgeldpflicht: EuGH zu Ermessen von Aufsichtsbehörden bei Datenschutzverstößen

Aufsichtsbehörden sind bei Datenschutzverstößen nicht in jedem Fall verpflichtet, ein Bußgeld zu verhängen. Vielmehr steht ihnen bei der Durchsetzung der DSGVO ein Auswahlermessen zu, welche Maßnahmen ergriffen werden. Die DSGVO räumt den Aufsichtsbehörden auch die Möglichkeit ein, auf die Verhängung von Bußgeldern zu verzichten, wie der EuGH in einem Fall des Hessischen Datenschutzbeauftragen nun entschied. Untersagung, Anordnung und andere Maßnahmen können ebenso gewählt werden, wenn sie im konkreten Fall angemessen sind.

Kein Anspruch von Betroffenen auf Verhängung eines Bußgelds

Der Ausgangsfall spielte in einer hessischen Sparkasse: Eine Mitarbeiterin hatte mehrmals unbefugt auf personenbezogene Daten eines Kunden zugegriffen. Die Sparkasse sah davon ab, den Kunden von dem Datenschutzverstoß zu benachrichtigen. Sie ergriff jedoch Disziplinarmaßnahmen gegen die Mitarbeiterin. Diese bestätigte zudem schriftlich, dass sie die personenbezogenen Daten weder kopiert oder gespeichert noch an Dritte übermittelt habe, und sagte zu, dies auch zukünftig nicht zu tun. Zusätzlich meldete die Sparkasse den Vorfall dem Hessischen Datenschutzbeauftragen als zuständiger Aufsichtsbehörde. Hiervon erlangte der Kunde Kenntnis und reichte Beschwerde beim Hessischen Datenschutzbeauftragten ein. Dieser wies die Beschwerde mit der Begründung zurück, dass die Sparkasse nicht ihre Benachrichtigungspflicht gemäß Art. 34 DSGVO verletzt habe. Hiergegen klagte wiederum der Kunde und beantragte, den Hessischen Datenschutzbeauftragen zum Einschreiten gegen die Sparkasse zu verpflichten.

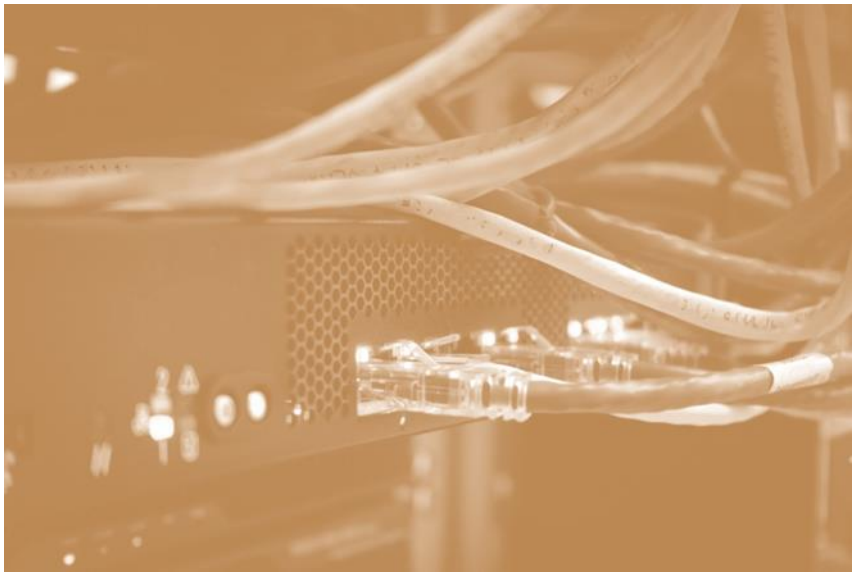
Das VG Wiesbaden legte den Fall dem EuGH vor und wollte von diesem wissen, ob die DSGVO im Fall eines festgestellten Verstoßes gegen Bestimmungen über den Schutz personenbezogener Daten dahin auszulegen sei, dass die Aufsichtsbehörde verpflichtet sei, nach Art. 58 Abs. 2 DSGVO Abhilfemaßnahmen – wie etwa die Verhängung einer Geldbuße – zu ergreifen, oder dahin, dass diese Behörde über ein Ermessen verfüge, das es ihr gestatte, je nach den Umständen vom Erlass solcher Maßnahmen abzusehen.

Der EuGH entschied überzeugend, dass ein Anspruch des Betroffenen auf Verhängung eines Bußgeldes nicht besteht (EuGH, Urteil vom 26. September 2024 - C-768/21). Die DSGVO sei so auszulegen, dass die Aufsichtsbehörde im Fall der Feststellung einer Verletzung des Schutzes personenbezogener Daten nicht verpflichtet ist, eine Geldbuße zu verhängen. Sie müsse nicht einmal notwendigerweise eine Abhilfemaßnahme ergreifen. Entscheidend ist, wie auch sonst im Verwaltungsrecht, welche Maßnahme geeignet, erforderlich und verhältnismäßig ist, um der festgestellten Unzulänglichkeit abzuhelfen und die umfassende Einhaltung der DSGVO zu gewährleisten.

Maßnahmen des Verantwortlichen können Erforderlichkeit des behördlichen Einschreitens entfallen lassen

Der EuGH führt aus, dass die Aufsichtsbehörde bei einem Datenschutzverstoß im Einzelfall ausnahmsweise von einem Einschreiten gegen den Verantwortlichen absehen kann. Dies sei insbesondere dann möglich, wenn der Verantwortliche bereits die erforderlichen Maßnahmen ergriffen hat, damit der Verstoß abgestellt wird und sich nicht wiederholt. Ob im vorliegenden Fall die (Disziplinar-)Maßnahmen der Sparkasse ausreichten, um von der Verhängung eines Bußgeldes absehen zu können, hat nun das VG Wiesbaden zu entscheiden.

Die Grenze ist eindeutig gezogen: Sie liegt in der Gewährleistung eines gleichmäßigen und hohen Schutzniveaus für personenbezogene Daten durch einen klar durchsetzbaren Rechtsrahmen.



Immaterieller Schadensersatz nach DSGVO nach unbefugter Datenweitergabe durch Impfzentrum

Die versehentliche Offenlegung von personenbezogenen Daten durch Mitarbeiter eines Corona-Impfzentrums veranlasste das OLG Hamm dazu, sich mit dem immateriellen Schadensersatz nach der DSGVO zu befassen. In seinem Urteil bestätigte das OLG insbesondere die Abtretbarkeit des Ersatzanspruches nach Art. 82 DSGVO und behandelte die Anforderungen an datenschutzrechtliche Sicherheitsmaßnahmen. Zudem konkretisierte das Gericht, dass ein immaterieller Schaden nicht schon dann gegeben ist, wenn sich lediglich das allgemeine Risiko einer unbefugten Datenweitergabe realisiert.

Was ist passiert?

Das Oberlandesgericht (OLG) Hamm beschäftigte sich vor Kurzem mit einer Datenpanne in einem Corona-Impfzentrum (Urteil vom 24.07.2024 – 11 U 69/23). Die Beklagte im vorliegenden Fall betrieb dieses Impfzentrum während der Covid-19-Pandemie. Aufgrund einer Änderung der Öffnungszeiten mussten 1.200 Impftermine verlegt werden. Die Personen, deren Termine verlegt werden mussten, sollten per E-Mail darüber informiert werden. Es gab zunächst technische Schwierigkeiten beim Versand der Info-Mail. Als sie dann versendet wurden, befanden sich im Anhang versehentlich Excel-Tabellen, die personenbezogene Daten aller – ca. 13.000 – Kunden des Impfzentrums enthielten. Die Empfänger wurden zur unverzüglichen Löschung aufgefordert und die

betroffenen Personen, die Öffentlichkeit sowie die Aufsichtsbehörde wurden über den Vorfall informiert.

Die Klägerin dieses Verfahrens machte den Betroffenen daraufhin ein Angebot: Die Betroffenen sollten von ihr eine Sofortentschädigung erhalten, wenn sie ihr etwaige Schadensersatzansprüche infolge des Vorfalls gegen die Beklagte abtreten. Es kamen einige Abtretungsverträge zustande, auf deren Grundlage die Klägerin immateriellen Schadensersatz aus Art. 82 Abs. 1, 2 DSGVO vom Impfzentrum verlangte.

Abtretbarkeit des Schadensersatzanspruches

Die Beklagte bestritt zunächst die Abtretbarkeit dieser Schadensersatzansprüche. Das OLG entschied jedoch: Ein Schadensersatz nach Art. 82 DSGVO wegen Verletzung des Schutzes personenbezogener Daten ist abtretbar.

Zur Diskussion stand, ob es sich hierbei um einen höchstpersönlichen Anspruch handelt, dessen Abtretung dann gem. § 399 BGB ausgeschlossen wäre. Art. 82 DSGVO bezwecke die Kompensation der Persönlichkeitsrechtsverletzung der betroffenen Person, was auch nur von dieser Person geltend gemacht werden könne.

Das OLG lehnte diese Auffassung jedoch ab, denn der Anspruch ist nicht höchstpersönlich. Es handelt sich bei Art. 82 DSGVO um eine eigenständige Anspruchsgrundlage, die nach allgemeinem Zivilrecht abtretbar ist. Im Vordergrund steht zum einen ein Datenschutzverstoß und nicht etwa die Verletzung des (höchstpersönlichen) Allgemeinen Persönlichkeitsrechts. Und zum anderen die Ausgleichsfunktion des Anspruchs: Er soll den finanziellen Ausgleich des entstandenen (ggf. immateriellen) Schadens sicherstellen. Zudem soll Art. 82 DSGVO zu einem EU-weit gleichmäßigen und hohen Datenschutzniveau beitragen, was eine über den persönlichen Schutz hinausgehende Funktion darstellt. Dass der Schuldner dieses Schadensersatzanspruches – das Impfzentrum – ein schutzwürdiges Interesse daran hat, dass die Person des Gläubigers sich nicht ändert, ist hier auch nicht zu erkennen (Rn. 76).

Unrechtmäßige Datenverarbeitungen und mangelnde Sicherheitsvorkehrungen

Im vorliegenden Fall gab es verschiedene Datenschutzverstöße – allerdings nur bei wenigen von der Datenweitergabe betroffenen Personen. Durch die Versendung der Excel-Tabellen wurde gegen Art. 5 Abs. 1 lit. a und f DSGVO verstoßen, da keine Rechtfertigung für die Weitergabe der Daten vorhanden war. Dabei wurde gleichzeitig gegen Art. 9 Abs. 1 DSGVO verstoßen, da es sich hier unter anderem um Gesundheitsdaten handelte (Rn. 142, 144).

Art. 24 sowie Art. 32 DSGVO wurden ebenfalls verletzt. Es wurden von dem Impfzentrum keine ausreichenden Sicherheitsvorkehrungen getroffen, um die Datenschutzverletzungen zu vermeiden. Es gab zwar generelle Sicherheitsmaßnahmen, wie die Sensibilisierung der Mitarbeiter bzgl. personenbezogener Daten, ein „Vier-Augen-Prinzip" bei der Versendung von E-Mails oder die Anweisung, Dritten keine personenbezogenen Daten offenzulegen. Hier handelte es sich jedoch um eine besondere Situation, in der eine zügige Information der betroffenen Impfwilligen nötig war. Gerade für eine solche Situation, in der es dazu auch noch technische Schwierigkeiten gab, hätte es Anweisungen für die Mitarbeitenden des Impfzentrums geben müssen, wie zu verfahren ist. Zumindest hätten solche Anweisungen in dem Moment vom Leiter der hier zuständigen „Koordinierenden Einheit" eingeholt werden müssen. Er hätte zudem noch einmal die E-Mail vor ihrer Versendung kontrollieren müssen (Rn. 146 ff).

Fahrlässiger DSGVO-Verstoß

Das OLG bewertet die Versendung der Mail samt vollständiger Anhänge als fahrlässig und bejaht deshalb auch das Verschulden der Beklagten. Aber auch schon im Vorhinein wäre es Sache der Beklagten gewesen, „dafür zu sorgen, dass in besonderen Situationen wie der vorliegenden, die im alltäglichen Arbeitsablauf nicht vorkommen und für die es deshalb keine konkreten Weisungen der Beklagten gibt, von ihren Mitarbeitern der Koordinierenden Einheit vor der Verarbeitung der personenbezogenen Daten Anweisungen […] eingeholt werden" (Rn. 154 ff.).

Immaterieller Schaden muss über generelles Risiko hinausgehen

Wie bereits vom EuGH betont wurde, genügt der reine DSGVO-Verstoß noch nicht für einen Anspruch auf Schadensersatz. Es muss dazu gesondert festgestellt werden, dass ein (materieller oder immaterieller) Schaden wirklich entstanden ist (Rs. C-687/21). Vorliegend wird der Verlust der Kontrolle über personenbezogene Daten als immaterieller Schaden geltend gemacht. Auch das hat der EuGH bereits als grundsätzlich möglichen immateriellen Schaden anerkannt, solange der Schaden – egal in welcher Höhe – nachgewiesen wird (Rs. C-741/21).

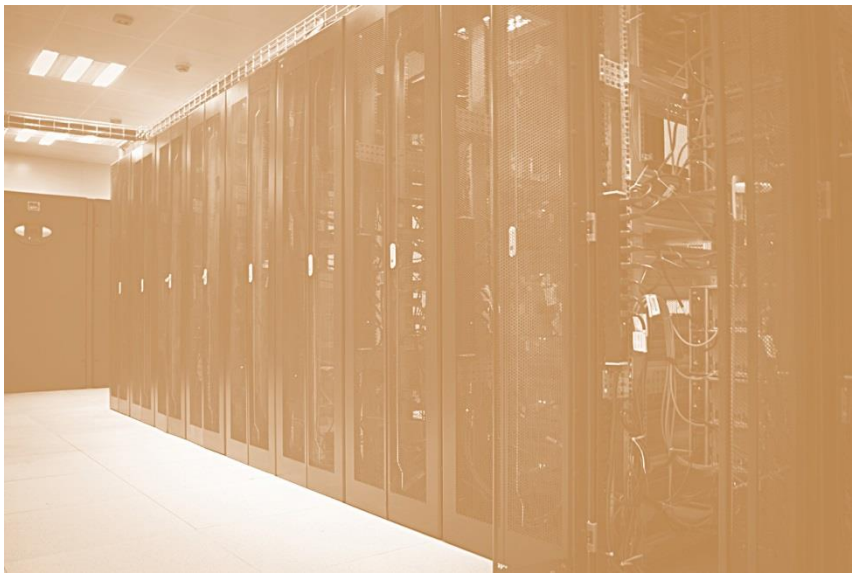
Das OLG schränkt dies nun etwas ein: Bei der Offenlegung oder Zugänglichmachung von Daten verlieren die betroffenen Personen automatisch die Kontrolle über ihre Daten. Das stellt lediglich die „Realisierung des generellen Risikos" dar, die noch nicht für einen Schaden im Sinne von Art. 82 DSGVO ausreichen soll. Notwendig ist darüber hinaus, dass eine „weitergehende Beeinträchtigung des vom Kontrollverlust betroffenen Geschädigten" vorliegt, wobei auch die nachgewiesene Befürchtung einer Datenweitergabe aufgrund des Kontrollverlusts ausreicht. Das bloße Bekanntwerden der offengelegten Daten ist auch nicht für einen Schaden ausreichend, da es sich hierbei ebenfalls um eine unmittelbare Folge des Datenschutzverstoßes handelt (Rn. 168 ff.).

Im vorliegenden Fall wurde lediglich bei zwei der vom Datenschutzverstoß betroffenen Personen ein über den Verstoß hinausgehender Schaden bewiesen. Dieser lag zum einen in wiederholt stattfindenden Spam-Anrufen kurz nach Verbreitung der Daten. Die andere Person erhielt unerwünscht eine auf die Impfung bezogene E-Mail von einer unbekannten Adresse.

Was aus diesem Urteil mitzunehmen ist:

Zum einen ist ein Anspruch aus Art. 82 DSGVO abtretbar. Wichtig für Verantwortliche, die personenbezogene Daten verarbeiten, ist, dass sie auch für Ausnahmefälle Sicherheitsmaßnahmen regeln müssen. Das kann durch organisatorische Maßnahmen geschehen. Außerdem ist der Kontrollverlust über die eigenen personenbezogenen Daten bloß die Realisierung des Risikos ihrer unbefugten Offenlegung. Für den Anspruch aus Art. 82 DSGVO muss ein darüberhinausgehender Schaden, wie z.B. wiederholte Spam-Mails oder -Anrufe, nachgewiesen werden. Das Urteil zeigt

wieder einmal, dass der DSGVO-Schadensersatz ein viel diskutiertes Thema mit noch vielen offenen Fragen ist. Zum Nachlesen zu weiteren vergangenen gerichtlichen Entscheidung hierzu haben wir bereits hier und hier einen Überblick gegeben. Das Urteil des OLG Hamm wird sicherlich nicht das letzte zu diesem Anspruch gewesen sein.



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

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

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

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

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

Rebecca Moßner
+49 221 65065-465
rebecca.mossner@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