LOSCHELDER

Newsletter Datenschutzrecht
November 2024

Sehr geehrte Damen und Herren,

umso lauter die Siegesrufe nach einer BGH-Entscheidung, umso genauer schauen wir hin: Der BGH hat am 18. November sein Urteil im sog. Scraping-Komplex verkündet, in dem es um immateriellen Schadensersatz wegen eines DSGVO-Verstoßes geht. Die Klägervertreter feiern sich seither, bisweilen mit bizarr anmutenden Siegesposen. Auch Beklagtenvertreter sehen das Urteil in Punkten positiv. Beide Seiten liegen (mindestens) in einem Punkt aus unserer Sicht richtig: Die Entscheidung verdient einige Aufmerksamkeit. Wir erklären Ihnen, wo die große Bedeutung der Entscheidung des BGH für eine Vielzahl von Verfahren zum Schadensersatzanspruch nach Art. 82 DSGVO liegt und welche Fragen offen bleiben.

Intensiv möchten wir diese Entscheidung und ihre praktischen Auswirkungen auch in unserem letzten Lunch@Loschelder Webinar in diesem Jahr diskutieren:

BGH-Urteil zum Facebook-Datenleck - Tasche auf bei jeder Datenpanne?

Das Urteil des Bundesgerichtshofs vom 18. November 2024 zum sog. Scraping hat eine riesen Welle ausgelöst. Das mediale Echo zu dieser Entscheidung hallte unisono: Schadensersatzklagen von Verbrauchern sind nun ein Elfmeter ohne Torwart. Doch sind Unternehmen nun wirklich bei **jeder** Datenpanne zum Schadensersatz verpflichtet?! Wir meinen: So einfach ist das bei Weitem nicht!

Gemeinsam blicken wir genau auf die Voraussetzungen des immateriellen Schadensersatzes nach Art. 82 DSGVO und erläutern wie Unternehmen sich zeitlich vor und nach einem (potentiellen) Datenschutzverstoß aufstellen können.

Wann: Donnerstag, den 12. Dezember 2024, 12:00 bis 12:45 Uhr
Referenten: Rebecca Moßner / Dennis Pethke, LL.M. (Stellenbosch)

Alle Webinare bieten wir für Unternehmensvertreter und unsere Mandanten 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.

Wir freuen uns über Ihr Interesse und Ihre Anmeldung!

In unserem heutigen Newsletter stecken indes noch mehr spannende Themen. Auch die letzte Plenartagung des Europäischen Datenschutzausschusses (EDSA) hatte es noch einmal in sich: Der

Ausschuss verabschiedete gleich vier Dokumente. Allen voran Leitlinien zur Datenverarbeitung wegen berechtigter Interessen des Verantwortlichen. Wann und unter welchen Voraussetzungen der Rechtfertigungsgrund für eine Datenverarbeitung gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO greift, wird bereits seit Einführung der DSGVO stark diskutiert. Die nun vorgelegten Leitlinien dürften insbesondere für Unternehmen mehr Rechtssicherheit bringen. Die Leitlinien werden noch bis zum 20. November 2024 öffentlich konsultiert. Daneben hat der Ausschuss in einer Stellungnahme die Pflichten von Verantwortlichen bei der Beauftragung von Auftragsverarbeitern und Unterauftragsverarbeitern konkretisiert. Im Zentrum steht die Auswahl- und Überwachungsverantwortung gem. Art. 28 Abs. 1 DSGVO. Passend hierzu entwickelte das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) eine „Abgrenzungshilfe“ zu der Frage, wann eine Auftragsverarbeitung vorliegt und wann nicht.

Der EDSA veröffentlichte zudem eine Erklärung zur geplanten DSGVO-Durchsetzungsverordnung, welche die Zusammenarbeit von verschiedenen nationalen Datenschutzbehörden bei grenzüberschreitenden Datenschutzfällen vereinfachen soll. Schließlich gab der Ausschuss einen Ausblick in die Zukunft und stellte sein Arbeitsprogramm 2024/2025 vor.

Zu guter Letzt werfen wir einen Blick auf die Aktivitäten der EU-Datenschutzbehörden in den letzten Wochen. Diese haben wieder teils erhebliche Bußgelder verhängt. Allen voran: Eine Rekordstrafe von 310 Millionen Euro gegen das Business-Netzwerk LinkedIn.

Wir bedanken uns für Ihr Interesse!

Inhalt

Neue EDSA-Leitlinien zur Datenverarbeitung wegen berechtigter Interessen des Verantwortlichen

Die Wahrung berechtigter Interessen des Verantwortlichen wird oftmals als Rechtfertigung für die Verarbeitung personenbezogener Daten herangezogen. Ob die Voraussetzungen nun vorliegen oder nicht, ist allerdings oft streitig: Eine Interessenabwägung zwischen den Interessen an der Verarbeitung und den gegenläufigen Betroffeneninteressen ist naturgemäß keine objektive Entscheidung. In der Praxis helfen hier nun Leitlinien des Europäischen Datenschutzausschusses zur Datenverarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO. Darin werden insbesondere die Vorgaben der Norm erläutert: Wann liegt ein berechtigtes Interesse vor? Wann ist die Datenverarbeitung erforderlich? Und wie müssen die Interessen der Betroffenen berücksichtigt werden?

Der Europäische Datenschutzausschuss (EDSA) hat am 08.10.2024 Leitlinien zur Verarbeitung personenbezogener Daten aufgrund Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO veröffentlicht (Guidelines 1/2024). Der EDSA ist ein Gremium der EU, welches sich aus Vertretern der europäischen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten zusammensetzt. Ziel des Ausschusses ist die einheitliche Anwendung der Datenschutzvorschriften der EU durch die Mitgliedstaaten. Dazu werden regelmäßig Leitlinien oder Empfehlungen veröffentlicht, die vor allem bei der Anwendung und Auslegung der DSGVO helfen sollen.

In den neuesten Leitlinien befasst sich der EDSA im Detail mit den Kriterien aus Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO. Nach dieser Vorschrift ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung **berechtigter Interessen** des Verantwortlichen oder eines Dritten **erforderlich** ist, sofern nicht die **Interessen der von der Datenverarbeitung betroffenen Person** überwiegen. Die Norm kann schnell als Ausweichtatbestand angesehen werden, für den Fall, dass alle weiteren Rechtfertigungsgründe des Art. 6 DSGVO nicht greifen. Die Vorgaben an diese Erlaubnisgrundlage erscheinen wenig konkret und leicht zu begründen. Dem widerspricht der EDSA nun in seinen Leitlinien eindeutig und betont, dass hiermit gerade nicht jede Verarbeitung personenbezogener Daten gerechtfertigt werden soll. Vielmehr muss Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO restriktiv ausgelegt und kritisch beurteilt werden, ob die erforderlichen

Vorgaben auch wirklich vorliegen. Der EDSA teilt diese Prüfung in drei Schritte auf:

1. Die Verfolgung berechtigter Interessen

Allgemein können zwar verschiedenste Interessen als Begründung für eine Datenverarbeitung in Betracht kommen – dazu berechtigen jedoch nicht alle. Nur, wenn das Interesse an der Datenverarbeitung (1.) **rechtmäßig** ist, d.h. nicht gegen EU- oder nationales Recht verstößt, (2.) **klar und präzise bestimmt** ist und (3.) **tatsächlich und gegenwärtig** besteht, kommt es als berechtigtes Interesse im Rahmen von Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO in Betracht. So kann z.B. eine Datenspeicherung aufgrund möglicherweise in der Zukunft entstehender Interessen an diesen Daten nicht nach Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO gerechtfertigt sein.

An sich bleibt der EDSA hier noch vage, da eine vollständige Erfassung aller berechtigten Interessen gar nicht möglich wäre. Orientierungspunkte und Beispiele geben die Leitlinien dennoch (Rn. 18). Eingeschränkt wird die Beurteilung der rechtmäßigen Datenverarbeitung durch die weiteren Prüfungsschritte.

2. Beurteilung der Erforderlichkeit der Datenverarbeitung

Eine Verarbeitung personenbezogener Daten muss **mehr als lediglich nützlich** zur Wahrung der berechtigten Interessen sein. Bei der Bewertung der Erforderlichkeit müssen die Prinzipien des Datenschutzrechts mit einbezogen werden, insbesondere der Grundsatz der „Datenminimierung". Danach dürfen personenbezogene Daten nur verarbeitet werden, wenn sie angemessen, erheblich und auf das für den Zweck notwendige Maß beschränkt sind. Sobald es passende alternative Maßnahmen gibt, die gleichermaßen zum Erreichen der verfolgten Interessen geeignet sind, ist eine Datenverarbeitung nicht mehr von Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO gedeckt.

3. Abwägung der entgegenstehenden Interessen der betroffenen Person

Kernstück ist die Interessenabwägung. Dazu müssen zum einen die **Interessen, Rechte und Freiheiten** der betroffenen

Person benannt werden. Außerdem muss erörtert werden, welche **Auswirkungen** die Art und der Umfang der Datenverarbeitung auf die Rechte der betroffenen Person hat. Auch, ob die Person mit einer Verarbeitung ihrer Daten **rechnen konnte**, wird mit einbezogen. All diese Aspekte sind schließlich in einer **Gesamtabwägung** den berechtigten Interessen des Verantwortlichen an der Verarbeitung gegenüberzustellen. Sollten die Interessen der betroffenen Person das Verarbeitungsinteresse überwiegen, könnte der Verantwortliche noch Maßnahmen treffen, die ggf. das Gleichgewicht beider Seiten wiederherstellen. Überwiegen trotzdem die Interessen der betroffenen Person, darf die Datenverarbeitung nicht auf Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO gestützt werden.

Dass der EDSA sich nun zu den Vorgaben des Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO geäußert hat, ist sehr zu begrüßen. Die Norm ist äußerst praxisrelevant, ihre Anwendung aber auch immer wieder mit Bewertungsunsicherheiten verbunden. Zwar bleiben die Leitlinien ziemlich generell, da eine konkrete Aussage zu einem Tatbestand, der eine Interessenabwägung und damit die Betrachtung jedes konkreten Einzelfalles voraussetzt, nicht möglich ist. Dennoch bringen sie mehr Rechtssicherheit durch diverse Fallbeispiele und Anwendungshinweise. Wer personenbezogene Daten aufgrund (vermeintlich) berechtigter Interessen verarbeitet, sollte in jedem Fall genau prüfen und zwingend auch dokumentieren, ob und weshalb die beschriebenen Vorgaben auch wirklich erfüllt sind.

EDSA konkretisiert Pflichten bei der Auftragsverarbeitung

In einer kürzlich veröffentlichten Stellungnahme hat der EDSA die Pflichten von Verantwortlichen bei der Beauftragung von Auftragsverarbeitern und Unterauftragsverarbeitern konkretisiert. Gefordert wird ein gutes Vertragsmanagement.

Verantwortliche müssen jederzeit Informationen über Identität aller Auftrags- und Unterauftragsverarbeiter bereithalten

Der Europäische Datenschutzausschuss (EDSA) kommt in seiner Stellungnahme vom 07.10.2024 zu dem Schluss, dass Verantwortliche Informationen über die Identität (d.h. Name, Adresse, Kontaktperson) aller Auftrags- und Unterauftragsverarbeiter jederzeit bereithalten sollten, damit sie ihre Verpflichtungen gemäß Art. 28 DSGVO erfüllen können. Das gilt unabhängig von dem Risiko, das mit einer Verarbeitungstätigkeit verbunden ist. Zu diesem Zweck soll der jeweilige Auftragsverarbeiter dem Verantwortlichen proaktiv Informationen zur Verfügung stellen und sie jederzeit auf dem neusten Stand halten.

Konkretisierung der Auswahl- und Überwachungsverantwortung des Verantwortlichen

Gemäß Art. 28 Abs. 1 DSGVO darf der Verantwortliche nur mit (Unter-)Auftragsverarbeitern zusammenarbeiten, die „hinreichende Garantien" für eine ordnungsgemäße Datenverarbeitung bieten. Den Verantwortlichen trifft also eine Auswahl- und Überwachungsverantwortung. Diese hat der EDSA nunmehr dahingehend konkretisiert, dass der Verantwortliche insbesondere sicherzustellen hat, dass das Schutzniveau für Betroffenenrechte durch die Einbindung des Auftragsverarbeiters nicht gesenkt wird. Die Auswahl- und Überwachungsverantwortung soll zudem unabhängig von dem Risiko gelten, das für die Rechte und Freiheiten der betroffenen Personen besteht. Sie bleibt ferner auch bei Beauftragung eines Unterauftragsverarbeiters bestehen. So hat der Verantwortliche auch die vom Erstverarbeiter erhaltenen Informationen über den Unterauftragsverarbeiter kritisch zu überprüfen, insbesondere bei Verarbeitungen, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen bergen. Die DSGVO verpflichtet ihn laut EDSA aber nicht dazu, systematisch die Unterverarbeitungsverträge anzufordern, um zu prüfen, ob die im ursprünglichen Vertrag vorgesehenen Datenschutzverpflichtungen in der Verarbeitungskette weitergegeben worden sind.

Auswahl- und Überwachungsverantwortung des Verantwortlichen auch bei Drittlandsübermittlungen

Der EDSA hat zudem klargestellt, dass auch bei Übermittlungen von personenbezogenen Daten außerhalb des Europäischen Wirtschaftsraums, zusätzlich zu den sich aus Art. 44 DSGVO ergebenden Pflichten, die Auswahl- und Überwachungs-verantwortung des Verantwortlichen gem. Art. 28 Abs. 1 DSGVO eingreift. Der Verantwortliche sollte auch in diesem Zusammenhang Informationen darüber bereithalten können, welche Datenübermittlungen stattfinden und auf welche Rechtsgrundlagen sie sich stützen. Den Auftragsverarbeiter trifft wiederum die Pflicht dem Verantwortlichen die hierfür relevante Dokumentation der Übermittlungssachverhalte zur Verfügung zu stellen.

EDSA-Empfehlung für Vertragsgestaltung

Der EDSA befasst sich in der Stellungnahme auch mit der Gestaltung von Verträgen zwischen Verantwortlichen und

Auftragsverarbeitern. Ein grundlegendes Element sei die Verpflichtung des Auftragsverarbeiters, personenbezogene Daten nur auf dokumentierte Weisung des für die Verarbeitung Verantwortlichen zu verarbeiten, „sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist“ (Art. 28 Abs. 3 lit. a) DSGVO). Die Aufnahme einer entsprechenden Klausel, die dieser Ausnahme Rechnung trägt, in Auftragsverarbeitungsverträge sei „sehr empfehlenswert“. Der EDSA betont in diesem Zusammenhang zudem, dass die Formulierung als solche jedoch nicht ausreiche, um im Falle einer Drittslandsübermittlung die Einhaltung der Voraussetzungen des Art. 28 Abs. 3 lit. a) i. V. m. Art. 44 ff. DSGVO zu gewährleisten.

Was ist Auftragsverarbeitung und was nicht?

Auftragsverarbeitung oder nicht – diese Frage stellt sich häufig, wenn Dienstleister, Schwesterunternehmen oder Lieferanten (auch) personenbezogene Daten verarbeiten. Die Abgrenzung ist dabei nicht immer einfach. Das BayLDA hilft hier mit seiner aktualisierten „Abgrenzungshilfe“.

Die Frage, ob jemand als Auftragsverarbeiter oder als Verantwortlicher einzustufen ist, stellt sich häufig in der Praxis, wenn mehrere Akteure an einer Datenverarbeitung beteiligt sind. Diese Frage stellte sich auch das Bayerische Landesamt für

Datenschutzaufsicht (BayLDA) und entwickelte aufgrund dessen eine „Abgrenzungshilfe“, die in der Praxis überaus hilfreich ist.

Hierbei handelt es sich um die Überarbeitung einer früheren Abgrenzungshilfe des BayLDA zur Auftragsverarbeitung. In der ersten Version wurden – zur Vereinfachung bzw. zum besseren Verständnis – beispielhaft Dienstleistungen genannt, die typischerweise Auftragsverarbeitungen darstellen. Schnell wurde klar, dass so eine pauschalisierte Betrachtung nicht immer zielführend ist, da zwei Dienstleistungen mit derselben Bezeichnung durchaus unterschiedliche Verarbeitungstätigkeiten umfassen können.

Auftragsverarbeitung bedeutet nach der DSGVO, dass jemand – der Auftragsverarbeiter – personenbezogene Daten im Auftrag eines anderen, nämlich des datenschutzrechtlich Verantwortlichen, verarbeitet. Verantwortlich ist derjenige, der über die Zwecke und Mittel der Datenverarbeitung entscheidet. Eine korrekte Einordnung ist notwendig, um den mit der jeweiligen Rolle einhergehenden Pflichten nachkommen zu können und vor allem die Privilegierung der Auftragsverarbeitung in Anspruch nehmen zu können: Wer weisungsabhängig unter Einhaltung der Anforderungen des Art. 28 DSGVO personenbezogene Daten verarbeitet, braucht keine eigene Rechtsgrundlage, sondern partizipiert an der Erlaubnis des Verantwortlichen.

Zur Abgrenzung verweist das BayLDA auf die Leitlinien 7/2020 des Europäischen Datenschutzausschusses (EDSA) zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“. Im Einklang mit diesen Leitlinien stellt das BayLDA zunächst klar, dass nicht jeder Dienstleister, der im Zuge seiner Leistungserbringung personenbezogene Daten verarbeitet, auch gleichzeitig Auftragsverarbeiter ist. Dennoch ist die Art der Dienstleistung ein wichtiges Indiz zur Bestimmung der datenschutzrechtlichen Rolle. Jedenfalls dann, wenn die Dienstleistung ihrem Inhalt nach speziell auf die Verarbeitung personenbezogener Daten abzielt oder eine solche Verarbeitung ein Schlüsselelement der Dienstleistung darstellt, liegt eine Auftragsverarbeitung vor – sofern dabei der Dienstleister nicht selbst über die Zwecke und Mittel der Datenverarbeitung entscheidet.

Beispiele für Auftragsverarbeitungen aus den EDSA-Leitlinien sind das Hosting / die Speicherung von personenbezogenen Daten nach

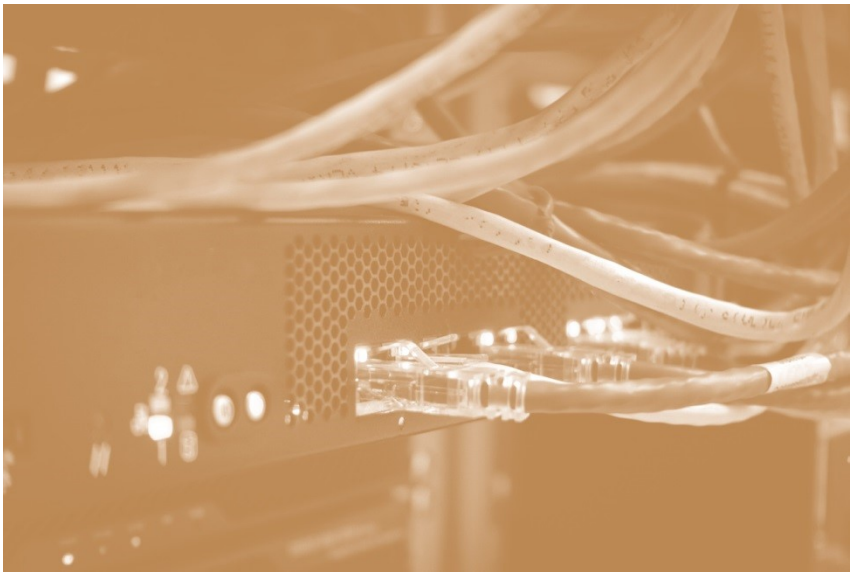
Weisung und Cloud-Dienstleistungen (z.B. Messaging, Videokonferenzen, Kalenderverwaltung).

Auch wenn die Haupttätigkeit des Dienstleisters nicht in der Verarbeitung personenbezogener Daten liegt, kann dieser Auftragsverarbeiter sein. Das ist der Fall, wenn seine Leistungen einen „systematischen, umfangreichen Zugang zu personenbezogenen Daten unvermeidlich mit sich bringen". Beispielhaft hierfür ist der Fall, dass ein IT-Dienstleister allgemein zum Support von IT-Systemen beauftragt ist, dabei aber ein *systematischer* Zugang zu personenbezogenen Daten faktisch möglich ist. Eine rein zufällige Möglichkeit des Datenzugriffs reicht jedoch noch nicht für eine Auftragsverarbeitung aus.

Darüber hinaus betont das BayLDA, dass je nach Einzelfall eine Auftragsverarbeitung auch dann in Betracht kommt, wenn der vorrangige Gegenstand einer Dienstleistung nicht auf die Verarbeitung personenbezogener Daten abzielt. Voraussetzung ist, dass der Auftraggeber, der Empfänger der Dienstleistung, die Entscheidung über Zwecke und Mittel der Verarbeitung trifft. Auch nur dieser ist dann Verantwortlicher der Datenverarbeitung. Das Konzept der sog. Funktionsübertragung, wonach in solchen Fällen der Dienstleister verantwortlich und eine Auftragsverarbeitung ausgeschlossen war, gibt es seit Einführung der DSGVO nicht mehr.

Ein Beispiel für solche Fälle ist die Kundenbetreuung im Call-Center: Hier benötigt der Dienstleiter gezwungenermaßen Zugang zu den Kundendaten des Auftraggebers. Der Dienstleister ist Auftragsverarbeiter, obwohl die Datenverarbeitung nicht Hauptgegenstand seiner Dienstleistung ist.

Wer am Ende die Entscheidung über die Verarbeitungszwecke und –mittel trifft und wer personenbezogene Daten im Auftrag verarbeitet, bleibt stets eine einzelfallabhängige Prüfung. Die reine Beurteilung anhand des Schwerpunktes der Dienstleistung reicht jedenfalls nicht für die Bewertung der Verantwortlichkeit aus. Die EDSA-Leitlinien liefern weitere spannende Beispiele, die bei der Abgrenzung hilfreich sein können.



Noch mehr vom EDSA zur DSGVO-Durchsetzungsverordnung und seinem Arbeitsprogramm

Neben den Leitlinien zum berechtigten Interesse und der Stellungnahme zur Auftragsverarbeitung verabschiedete der EDSA außerdem eine Erklärung zur geplanten Festlegung zusätzlicher Verfahrensvorschriften für die Durchsetzung der DSGVO. Zudem beschloss der Ausschuss sein Arbeitsprogramm für 2024/2025.

Bereits im April 2023 berichteten wir über die Gesetzesinitiative der Europäischen Kommission für eine DSGVO-Durchsetzungsverordnung. Ziel dieser Verordnung ist es, die Zusammenarbeit zwischen verschiedenen nationalen Datenschutzbehörden bei der Durchsetzung der DSGVO in grenzüberschreitenden Fällen zu verbessern. Verfahrensvorschriften sollen dazu beitragen, Meinungsverschiedenheiten zwischen Behörden zu klären, die Zusammenarbeit und die Durchsetzung der datenschutzrechtlichen Vorschriften zu vereinfachen.

Nachdem das Europäische Parlament und der Rat an dem Vorschlag der Europäischen Kommission Änderungen vorgenommen hatten (u.a. Einführung konkreter Fristen bei der Zusammenarbeit, Modifikation der Regelungen über eine außergerichtliche Einigung, Einführung einer gemeinsamen Fallakte) hat der Europäische Datenschutzausschuss (EDSA) hierzu nun eine Erklärung abgegeben.

Der EDSA begrüßt die Änderungen. Er weist gleichzeitig darauf hin, dass die Einführung neuer Verfahrensschritte und zusätzlicher Aufgaben für Aufsichtsbehörden auch einen Bedarf an zusätzlichen Ressourcen mit sich bringen und gibt im Hinblick darauf Empfehlungen ab. So sei beispielsweise für eine außergerichtliche Einigung eine Rechtsgrundlage und ein harmonisiertes Verfahren notwendig. Zudem müssten Fristen so ausgestaltet werden, dass sie auch realistisch eingehalten werden können. Die Einführung einer gemeinsamen Fallakte erfordere zudem noch weitere technische Lösungsansätze, da die verschiedenen nationalen Dokumentenverwaltungs- und Kommunikationssysteme nicht ohne Weiteres miteinander kompatibel seien.

Der EDSA hat auf seiner letzten Plenartagung am 08.10.2024 zudem sein Arbeitsprogramm 2024/2025 beschlossen. Es handelt sich um das erste von zwei Arbeitsprogrammen, mit denen die im April 2024 beschlossene Strategie des EDSA für 2024 bis 2027 umgesetzt werden soll. Unter anderem will der Ausschuss zur Erfüllung seiner Hauptaufgabe, die Auslegung der DSGVO in den einzelnen Mitgliedstaaten zu harmonisieren, weitere Leitlinien bereitstellen und die Entwicklung von Compliance-Maßnahmen unterstützen. Auch die Kooperation der Mitglieder des EDSA soll verstärkt und eine Zusammenarbeit mit anderen Regulierungsbehörden gefördert werden. Schließlich will sich der EDSA für einen globalen Dialog über Datenschutz einsetzen.

Leitentscheidung des BGH im Scraping-Komplex

Eine aktuelle Entscheidung des BGH zum immateriellen Schadensersatz nach DSGVO-Verstoß sorgt derzeit für Aufregung: Am 18. November 2024 entschied der BGH in einer Leitentscheidung im sog. Scraping-Komplex. Seither feiern sich Klägervertreter medial, da der Schadensnachweis vereinfacht und auch mit Textbausteinen möglich sei. Beklagtenvertreter verweisen auf einen Scheinsieg angesichts der niedrigen Summen, die der BGH als berechtigt ansieht. Auch wenn die Urteilsgründe noch nicht vorliegen, ordnen wir Ihnen die Entscheidung nachfolgend in den Kontext der bisherigen Rechtsprechung zum immateriellen Schadensersatz nach Art. 82 DSGVO und bewerten die Auswirkungen auf Ihr Unternehmen.

Der Kontrollverlust über personenbezogene Daten und der aufgrund dessen erlittene Ärger im Zusammenhang mit einem Scraping-Vorfall genügen, um einen Schadensersatzanspruch nach Art. 82 DSGVO zu begründen. Dies entschied der BGH am 18.11.2024 zum sog. Scraping-Komplex.

Besondere Bedeutung erlangt dieses Verfahren in vielerlei Hinsicht. Von dem für Datenschutz zuständigen VI. Zivilsenat des BGH wurde es mit Beschluss vom 31.10.2024 zu dem ersten Leitentscheidungsverfahren i.S.d. neuen § 552b ZPO erklärt. Die Vorschrift ermöglicht es dem BGH, ein anhängiges Revisionsverfahren zum Leitentscheidungsverfahren zu erklären, wenn die zu klärenden Fragen – wie in diesem Fall – für eine Vielzahl von Verfahren von Bedeutung sind. Vor deutschen Gerichten sind aktuell noch weitere tausende Klagen zu ähnlichen Sachverhalten anhängig. Durch die Entscheidung des BGH können andere Gerichte ihre Verfahren nun danach ausrichten und schneller zu Ergebnissen kommen.

Worum es in dem Verfahren ging

Facebook ermöglicht es, in Abhängigkeit von den Suchbarkeits-Einstellungen des jeweiligen Nutzers, dessen Facebook-Profil mithilfe seiner Telefonnummer zu finden. Diese Funktion nutzen unbekannte Dritte im April 2021 aus. Sie gaben in großem Umfang Ziffernfolgen ein und ordneten Telefonnummern unzähligen Nutzerkonten zu, um im Anschluss die zu diesen Nutzerkonten vorhandenen öffentlichen Daten abzugreifen (sog. Scraping). Auf diese Weise konnten sie Daten von rund 533 Millionen Nutzern aus 106 Ländern erlangen. Insbesondere wurde auf Daten wie Nutzer-

IDs, Namen, Geschlechter, Arbeitsstätten und Geschlecht zugegriffen. Diese Daten wurden von ihnen daraufhin öffentlich im Internet verbreitet.

Zu den Betroffenen des Scrapings zählte auch der Kläger. Er machte deshalb der beklagten Facebook-Betreiberin Meta gegenüber geltend, dass die Sicherheitsmaßnahmen auf Facebook unzureichend seien, da das Ausnutzen des Kontakt-Suche-Tools nicht im Vorhinein verhindert worden sei. Aufgrund des Datendiebstahls habe er großen Ärger empfunden. Dies begründe einen immateriellen Schaden und damit einen Anspruch auf Entschädigung nach der DSGVO.

Die Entscheidung des BGH

Nachdem das Landgericht Bonn (Urteil vom 29.03.2023, Az. 13 O 125/22) dem Kläger zunächst Schadensersatz in Höhe von 250 Euro zusprach, wies das Oberlandesgericht Köln (Urteil vom 07.12.2023, Az. 15 U 67/23) die Klage ab. Das ist nicht verwunderlich. Über den Ersatz eines immateriellen Schadens im Rahmen des Scraping-Komplexes wurde von den Landgerichten und Oberlandesgerichten bisher unterschiedlich geurteilt. Gegen Facebook eingereichte Schadensersatzklagen von Nutzern blieben größtenteils ohne Erfolg.

Anders fällt nun das Urteil des BGH aus. Auch er prüfte auf die Revision des Klägers hin insbesondere, ob die Voraussetzungen für einen Schadensersatzanspruch nach Art. 82 DSGVO vorliegen und entschied: Auch der bloße und kurzzeitige Verlust der Kontrolle über eigene personenbezogene Daten infolge eines Verstoßes gegen die DSGVO kann ein immaterieller Schaden im Sinne der Norm sein. Dafür bedürfe es keiner konkreten missbräuchlichen Verwendung dieser Daten zum Nachteil des Betroffenen und auch sonst müssen keine zusätzlichen spürbaren negativen Folgen vorliegen.

Der BGH verwies das Berufungsgericht für die erneute Verhandlung und Entscheidung darauf, dass die von der Beklagten vorgenommene Voreinstellung der Suchbarkeitseinstellung auf "alle" nicht dem Grundsatz der Datenminimierung entsprochen haben dürfte. Ergänzend dürfte zudem die Frage einer wirksamen Einwilligung des Klägers in die Datenverarbeitung durch die Beklagte zu prüfen sein. Schließlich bestünden keine rechtlichen Bedenken dagegen, den Ausgleich für den bloßen Kontrollverlust

über personenbezogene Daten im vorliegenden Fall in einer Größenordnung von 100 Euro zu bemessen.

Entscheidungen des EuGH

Bereits aus der Pressemitteilung zu dem Urteil geht ausdrücklich hervor, dass der BGH sich für seine Entscheidung auf die für die Auslegung des Art. 82 DSGVO maßgebliche Rechtsprechung des EuGH stützt. Gerade diese geht jedoch mit der Schlussfolgerung, dass aus dem Umstand des bloßen Kontrollverlusts das Vorliegen eines immateriellen Schadens folgt, besonders kritisch um. Im August berichteten wir hier über die Linie des EuGH und insbesondere darüber, dass ein Schaden durch den Betroffenen konkret und detailliert nachzuweisen ist. Allgemein behauptete „Sorgen" oder „Ängste" genügen hierfür noch nicht.

Im Rahmen einer dreistufigen Prüfung muss zur Feststellung des Verstoßes gegen die DSGVO (1) und den hieraus resultierenden negativen Folgen für den Betroffenen (2) auf dritter Ebene der konkrete Nachweis hinzutreten, dass diese negativen Folgen auch einen immateriellen Schaden begründen (3).

Aus früherer Rechtsprechung des EuGH ergibt sich daher auch für den Fall des Scrapings: Der Kontrollverlust über die eigenen personenbezogenen Daten darf nicht bereits mit einem immateriellen Schaden gleichgesetzt werden.

Erst im letzten Monat hat der EuGH erneut klargestellt, „dass ein zeitlich begrenzter Verlust der Kontrolle der betroffenen Person über ihre personenbezogenen Daten […] ausreichen kann, um einen „immateriellen Schaden" zu verursachen, sofern diese Person nachweist, dass sie tatsächlich einen solchen Schaden – so geringfügig er auch sein mag – erlitten hat, ohne dass dieser Begriff des „immateriellen Schadens" den Nachweis zusätzlicher spürbarer negativer Folgen erfordert." (Urteil vom 04.10.2024, Az. C-200/23, Rn. 156)

Wir sind gespannt, ob die schriftliche Urteilsbegründung des BGH über den konkreten Nachweis des Schadens des sich ärgernden Facebook-Nutzers im Scraping-Fall Aufschluss geben wird. Nach der Pressemitteilung wird der Schadensnachweis leichter, als von vielen Instanzgerichten zuletzt gefordert: „*Weder muss insoweit eine konkrete missbräuchliche Verwendung dieser Daten zum Nachteil des Betroffenen*

erfolgt sein noch bedarf es sonstiger zusätzlicher spürbarer negativer Folgen.“ Allerdings sieht der BGH keinen hohen Schadensersatzanspruch, jedenfalls nicht im vierstelligen Bereich, wie gefordert, sondern mein, der „*Ausgleich für den bloßen Kontrollverlust*“ sei „*in einer Größenordnung von 100 € zu bemessen*“.

Was dies für die Praxis bedeutet, ob die Entscheidung wirklich zu einem Umschwung in der bisherigen Schadensersatzrechtsprechung nach DSGVO-Verstoß spürt und wie sich Unternehmen im Fall von Schadensersatzbegehren nach dieser Entscheidung verhalten können, diskutieren wir mit Ihnen in unserem Lunch@Loschelder Webinar am 12. Dezember 2024: **BGH-Urteil zum Facebook-Datenleck - Tasche auf bei jeder Datenpanne?** Weitere Informationen dazu finden Sie hier; wir freuen uns über Ihre Anmeldung!

Zu guter Letzt

Zu guter Letzt werfen wir einen Blick auf die Aktivitäten der europäischen Datenschutzbehörden in den letzten Wochen. Diese haben wieder teils erhebliche Bußgelder verhängt. Allen voran: Eine Rekordstrafe von 310 Millionen Euro gegen das Business-Netzwerk LinkedIn.

- **310 Millionen Euro Bußgeld gegen LinkedIn**

  Die irische Datenschutzaufsichtsbehörde (DPC) hat gegen das Business-Netzwerk LinkedIn ein Bußgeld in Höhe von 310 Millionen Euro verhängt. Gegenstand der Untersuchung war die Verarbeitung personenbezogener Daten von Nutzern der Plattform durch LinkedIn zum Zwecke der Verhaltensanalyse und der gezielten Werbung. Die DPC stellte gleich drei Verstöße fest: Erstens seien Art. 6 und Art. 5 Abs. 1 lit. a) DSGVO verletzt, da eine Rechtsgrundlage für die Datenverarbeitung durch LinkedIn fehle. Die Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO), auf die sich LinkedIn berufen hat, sei nicht freiwillig und nicht hinreichend informiert erfolgt. Auch ein Berufen auf berechtigte Interessen (Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO) scheide aus, da die Interessen von LinkedIn durch die Interessen und Grundrechte und -freiheiten der betroffenen Nutzer überlagert würden. Zweitens habe LinkedIn gegen die Informationspflichten gemäß Art. 13 und Art. 14 DSGVO verstoßen. Und drittens sei auch der Grundsatz der Fairness verletzt.

- **91 Millionen Euro Bußgeld gegen Facebook-Mutterkonzern Meta**

  Bereits in der Oktober-Ausgabe unseres Newsletters haben wir berichtet, dass der Facebook-Mutterkonzern Meta von der DPC mit einem Bußgeld in Höhe von 91 Millionen Euro belegt worden ist. Hierzu sind nun weitere Details bekannt geworden: Grund für das Bußgeld ist, dass der Meta-Konzern Passwörter von mehreren hundert Millionen Facebook-Nutzern im Klartext gespeichert und nach Kenntnis hiervon gegen seine datenschutzrechtliche Meldepflicht verstoßen hat. Dementsprechend stellte die DPC Verstöße gegen Art. 5 Abs. 1 lit. f) DSGVO und Art. 33 Abs. 1 DSGVO fest. Zwar hatte Meta die betroffenen Nutzer im März 2019 über den

Datenschutzvorfall informiert. Da Meta zu diesem Zeitpunkt jedoch bereits seit zwei Monaten Kenntnis von dem Vorfall hatte, sei die Meldung nicht rechtzeitig gewesen. Diese hätte innerhalb von 72 Stunden erfolgen müssen.

- **Über 3 Millionen Euro Bußgeld gegen schwedisches Unternehmen Apoeket AB**

  Auch kleineren Unternehmen drohen bei Datenschutzverstößen empfindliche Bußgelder. Das zeigt ein Fall aus Schweden. Die dortige Aufsichtsbehörde verhängte gegen das Unternehmen Apoteket AB ein Bußgeld in Höhe von über 3 Millionen Euro wegen eines Verstoßes gegen Art. 32 Abs. 1 DSGVO. Der Grund: Apoteket hatte auf seiner Webseite unbeabsichtigt sog. Meta-Pixel integriert, die Daten der Nutzer sammelten und an Meta weiterleiteten.

- **250.000 Euro Bußgeld für französische Hellseher-Hotline**

  Auch die Hellseher-Branche ist nicht gefeit vor Bußgeldern wegen Datenschutzverstößen. Die französische Datenschutzbehörde belegte das Unternehmen Cosmospace, einen Anbieter für hellseherische Tätigkeiten per Telefon, SMS oder Chat, mit einem Bußgeld in Höhe von 250.000 Euro. Das Unternehmen zeichnete systematisch alle mit Kunden geführten Telefongespräche auf. Dabei wurden oft sensible Informationen wie die Religionszugehörigkeit oder die sexuelle Orientierung preisgegeben. Eine eindeutige Einwilligung der Kunden habe laut französischer Datenschutzbehörde jedoch nicht vorgelegen. Zusätzlich bewahrte das Unternehmen die von seinen Kunden bereitgestellten Daten sechs Jahre lang auf, bevor sie gelöscht wurden. Dies überschreitet den gesetzlich erlaubten Zeitraum von drei Jahren erheblich.

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

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

Rebecca Moßner
+49 221 65065-337
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