Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

die wohlverdiente Urlaubszeit steht bei uns allen vor der Tür. Im Bereich des Datenschutzrechts gibt es allerdings einige Themen auf die wir Sie noch vor der Urlaubspause hinweisen möchten.

Vor den deutschen Gerichten landen nämlich immer häufiger Schadensersatzklagen im Bereich des Datenschutzrechts und immer mehr Gerichte bejahen Schadensersatzansprüche in Folge einer Verletzung von Pflichten nach der DSGVO.

Zunächst möchten wir Ihnen in diesem Zusammenhang die Entscheidung des Arbeitsgerichts Neuruppin vorstellen. Hier ging es um einen ausgeschiedenen Mitarbeiter, dessen Daten trotz Ausscheidens weiter auf der Unternehmens-Webseite verfügbar waren. Ein weiterer Fall wurde vor dem LG Köln verhandelt. Nachdem bereits das LG München I die Firma Broker Scalable Capital auf Klage eines Kunden zu Schadenersatz verurteilt hatte, klagte nun beim LG Köln ein weiterer Kunde auf Schadenersatz nach Art. 82 DSGVO wegen der Verletzung von Sorgfaltspflichten im Bereich technisch-organisatorischer Maßnahmen. Das OLG Frankfurt a.M. hatte wiederum über einen Sachverhalt zu entscheiden, bei dem eine Bank Kontoabschlüsse eines Kunden an Dritte versendet und zusätzlich eine falsche SCHUFA-Meldung abgegeben hatte.

Neben den Entscheidungen zum Schadenersatz möchten wir Ihnen eine interessante Entscheidung des LG Berlin nicht vorenthalten. Hier entschied das Gericht, dass die bloße Wohnadresse ohne einen Namensbezug nicht unter den Schutz der DSGVO falle. Bis dato wurde das von vielen Gerichten anders entschieden.

Im Bereich Social Media gibt es einen aktuellen Beschluss der Datenschutzkonferenz (DSK) zur Datenschutzkonformität von Facebook-Fanpages und zum Schluss stellen wir Ihnen die wichtigsten Aussagen des European Data Protection Board (EDPB) in seiner Guideline zum Thema Auskunftsrecht vor.

Ich wünsche Ihnen einen erholsamen Sommer!

Ihr Asmus Eggert

Inhalt

ArbG Neuruppin: 1000 EUR DSGVO-Schadensersatz für Mitarbeiter

Im vorliegenden Fall beim AG Neuruppin (ArbG Neuruppin, Urt. v. 14.12.2021 - Az.: 2 Ca 554/21) hatte der ehemalige Mitarbeiter das Unternehmen bereits zur Löschung seines Namens von der Unternehmenswebseite aufgefordert, doch sein Name erschien weiterhin auf der Webseite. Infolgedessen forderte der Kläger eine Geldentschädigung iHv. 5.000 EUR für die unerlaubte Nutzung seines Namens. Das Unternehmen entrichtete jedoch lediglich 150 EUR, weshalb der Kläger vor Gericht zog.

Das Gericht sprach dem Kläger letztlich keine 5.000 EUR zu, aber insgesamt 1.000 EUR (inkl. der bereits gezahlten 150 EUR) zu. Das Vorliegen einer Datenschutzverletzung bejahte das Gericht.

Arbeitgeber sind nach Beendigung des Arbeitsverhältnisses dazu verpflichtet unverzüglich die Daten ihrer ehemaligen Mitarbeiter von Ihrer Unternehmenswebseite zu löschen. Dies ergibt sich nicht nur aufgrund der bestehenden datenschutzrechtlichen Pflichten, sondern stellt auch eine allgemeine Nebenpflicht aus dem Arbeitsverhältnis i.S.v. § 241 Abs. 2 BGB dar. Vorliegend waren die Daten des Mitarbeiters sogar noch mehrere Monate später verfügbar.

Praxishinweis: Unternehmen müssen mit entsprechenden arbeitsgerichtlichen Urteilen bei Datenschutzverstößen rechnen und sollten der Gefahr von Schadensersatzzahlungen durch einen entsprechenden Prozess beim Ausscheiden von Mitarbeitern zuvorkommen.

LG Köln: Broker Scalable Capital: 1.200 EUR Schadensersatzzahlung

Im Oktober 2020 hatte Scalable Capital seine Kunden darüber informiert, dass es eine Datenschutzpanne gab und unbekannte Dritte bestimmte Informationen der Kunden erbeutet hätten (u.a. Ausweisdaten, Name und Adresse, Wertpapierabrechnungen, steuerliche Daten).

Schon Ende 2021 hatte das LG München I (LG München I, Urt. v. 9.12.2021, 31 O 16606/20) einem Kunden in einem anderen Gerichtsverfahren einen Schadensersatz iHv. 2.500 EUR wegen der Verletzung der Sorgfaltspflichten nach Art. 32 DSGVO zugesprochen. Scalable Capital hatte nämlich viele Jahre nach der Kündigung eines Subdienstleisters die Zugänge zu seinen Daten immer noch nicht geändert, so dass der Subdienstleister weiter Zugriff auf die Daten hatte.

Jetzt hatte ein weiterer Kunde - diesmal vor dem LG Köln - geklagt und das LG Köln (LG Köln, Urt. v. 18.05.2022 - Az.: 28 O 328/21) bejahte ebenfalls einen entsprechenden Anspruch. Die Höhe des Schadensersatz setzte das LG Köln allerdings bei lediglich 1.200,- EUR (das LG München I hatte 2.500,- EUR angenommen) fest und führte hierzu aus:

"Hier war bei der Bemessung der Höhe zu berücksichtigen, dass ein Missbrauch der Daten zu Lasten des Klägers bislang nicht festgestellt wurde, und es daher einstweilen bei einer Gefährdung geblieben ist. Wie vom LG München I a.a.O. zutreffend herausgearbeitet, muss allerdings auch die Absicht des EU-Verordnungsgebers berücksichtigt werden, mit Hilfe des Schadensersatzanspruchs eine abschreckende Wirkung zu erzielen. […] Zu Gunsten der Beklagten fällt […], ins Gewicht, dass der ihr zuzurechnende Datenschutzverstoß nur eine von mehreren Ursachen war, die erst im Zusammenwirken den Schadenseintritt bewirkten. Denn hinzu kam ein weiterer mindestens fahrlässiger Verstoß bei der Fa. (...) sowie nicht zuletzt das vorsätzliche rechtswidrige Vorgehen der Hacker selbst. […] Zu berücksichtigen ist auch, dass die Beklagte dem Kläger vorübergehend das „meine Schufa Plus" Angebot finanzierte."

Praxishinweis: Datenschutzvorfälle sind ein schwieriges Thema und bergen nicht unbeträchtliche Haftungsrisiken. Das Investment in ein entsprechendes Datenschutz- und Informationssicherheits-management ist angesichts steigender Haftungsrisiken, aber auch angesichts der generellen Cybercrime-Bedrohungslage dringend zu empfehlen. Wir unterstützen gern, z.B. auch durch Schwachstellen-Tests ihrer Webseiten und Web-Applikationen.

OLG Frankfurt a.M.: 500 EUR Schadensersatz für Übersendung von Unterlagen an Dritte und falsche SCHUFA-Meldung

Der Kläger forderte vor dem OLG Frankfurt (OLG Frankfurt a.M., Urt. v. 14.04.2022 - Az.: 3 U 21/20) von seiner Bank einen Schadensersatz von mindestens 5.000 EUR. Hintergrund der Forderung war, dass das Finanzinstitut fehlerhaft an einen Dritten Kontoabschlüsse des klägerischen Kontos übersandte und der SCHUFA die Adresse des Dritten als "frühere Wohnung" mitteilte.

Das OLG Frankfurt a.M. sprach dem Kläger aber lediglich eine Summe von 500 EUR zu und führte hinsichtlich der Höhe aus, dass der eingetretene Schaden am unteren Rand möglicher Beeinträchtigungen des Persönlichkeitsrechts des Klägers läge. Die vom Kläger nach außen gedrungenen personenbezogenen Daten beträfen lediglich seine Kontonummer, einen Kontostand aus dem Jahr 2018 sowie Abschlussposten in Höhe von insgesamt 29,28 € und den Umstand, dass er im dritten Quartal einen (Dispositions-)Kredit zu 10,9% in Anspruch genommen hatte. Auch ist nur bekannt, dass lediglich zwei Personen Kenntnis erlangt haben und es sei nicht ersichtlich, dass sich die falsche „frühere Adresse“ des Klägers negativ auf dessen Bonität oder „Score“ bei der Schufa ausgewirkt habe.

Praxishinweis: Die Gerichte berücksichtigen durchaus die Umstände eines Falles und korrigieren überzogene Vorstellungen. Wichtig ist daher im Falle eines Falles auch alle entlastenden Umstände sauber aufzuklären und den Gerichten und insbesondere den Aufsichtsbehörden in einem entsprechenden aktiven Dialog mitzuteilen.

LG Berlin: Bloße Wohnadresse ohne Namensbezug unterfällt nicht der DSGVO

Das LG Berlin hat entschieden, dass es sich bei der bloßen Nennung einer Wohnadresse ohne Namensbezug nicht um ein personenbezogenes Datum gem. der DSGVO handelt (LG Berlin, Urt. v. 27.01.2022 - Az.: 26 O 177/21).

Hintergrund war hier ein Scheidungsverfahren zwischen der Klägerin und ihrem Ehemann, bei dessen Verhandlung die beim Amtsgericht zuständige Richterin die exakte Adresse der Klägerin googelte, d.h. sie gab bei Google Maps die Adresse der Klägerin "*XY-.straße (...) Berlin“* ein. Im Beschluss des Amtsgerichts hieß es dann: "(...) bei einer bei Google Maps ersichtlichen Grundfläche des Doppelhauses von über 150 qm [dürfte] die Immobilie der Beteiligten mindestens eine Wohnfläche von 100 qm haben (...)." Die Klägerin wertete das als eine unzulässige Datenverarbeitung. Durch die Nutzung dieser Informationen seien ihre personenbezogenen Daten ohne Ihre Zustimmung in die USA übermittelt worden. Sie verlangte daraufhin Schadensersatz iHv. 2.000 EUR.

Zu Unrecht, wie das LG Berlin auf die entsprechende Beschwerde der Klägerin gegen die Richterin am Amtsgericht urteilte. Denn es handle sich bei den von der Richterin eingegebenen Daten gar nicht um personenbezogene Daten, die dem Schutz der DSGVO unterfallen würden:

"In der bloßen Eingabe einer (puren) Adresse ist noch kein personenbezogenes Datum zu erblicken. Denn die bloße Adresse ohne Bezugnahme auf eine Person – sei es durch namentliche Nennung, sei es

durch die Bezugnahme auf ein diese Adresse betreffendes Eigentums-, Besitz- oder Mietverhältnis o.ä. – stellt keinen hinreichenden Personenbezug dar."

Praxishinweis: Es kommt bei der Beurteilung, ob es sich um personenbezogene Daten handelt, immer auf die konkrete Situation an. Gemäß Art. 4 DSGVO sind „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Wie die isolierte Nutzung einer „Adresse" zu bewerten ist, kann durchaus kontrovers diskutiert werden. Handelt es sich nämlich hinter der Adresse um ein Einfamilienhaus, dann lässt sich damit durchaus ein Personenbezug herstellen. Ob andere Gerichte daher ähnlich urteilen, bleibt abzuwarten. Das Urteil sollte daher mit entsprechender Vorsicht gewertet werden.

DSK Beschluss zu den Zweifeln an der Datenschutz-Konformität von Facebook-Fanpages

Die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, zweifelt die Datenschutz-Konformität von Facebook-Fanpages bereits seit langem an. Die DSK hat nun eine spezielle Taskforce eingerichtet, um die Rechtskonformität solcher Facebook-Fanpages weiter zu untersuchen. Diese Taskforce hat am 18.03.2022 ein Kurzgutachten zum datenschutzkonformen Betrieb solcher Seiten veröffentlicht. Darin wird eine rechtliche Bewertung zum Betrieb von Facebook-Fanpages unter Berücksichtigung des seit 1.12.2021 geltenden Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG) sowie zu den Voraussetzungen einer wirksamen Einwilligung abgegeben. Zudem wird die Vereinbarkeit der Verarbeitung personenbezogener Daten zu Statistiken (sog. Insights) mit der DSGVO näher beleuchtet und das Thema Drittstaatentransfer erörtert. Im Ergebnis heißt es:

„Für die bei Besuch einer Fanpage ausgelöste Speicherung von Informationen in den Endeinrichtungen der Endnutzer:innen und den Zugriff auf Informationen, die bereits in der Endeinrichtungen gespeichert sind, sowie für die Verarbeitungen personenbezogener Daten, die von Seitenbetreibern verantwortet werden, sind ***keine wirksamen Rechtsgrundlagen*** *gegeben. Darüber hinaus werden die* ***Informationspflichten aus Art. 13 DSGVO nicht erfüllt****."*

Die DSK nahm in Ihrem Beschluss vom 23.03.2022 das von der Taskforce Facebook-Fanpages erstellte Kurzgutachten zur Frage der datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages vom 18.03.2022 zur Kenntnis und stimmte der Bewertung zu.

Praxishinweis: Damit rücken alle Stellen, die Facebook-Fanpages betreiben, wieder in den Fokus der Datenschutzbehörden. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hatte entsprechende Kontrollen von Facebook-Fanpages schon Anfang 2022 angekündigt. Aufsichtsbehörden können insbesondere erwirken, dass betriebene Facebook-Fanpages deaktiviert werden, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können. Dem Beschluss der DSK kann entnommen werden, was die Aufsichtsbehörden hier verlangen werden:

- Abschluss einer Vereinbarung nach Art. 26 DSGVO über die gemeinsame Verantwortlichkeit mit Facebook,
- ausreichende Informationen über die gemeinsamen Datenverarbeitungen gegenüber den die Fanpages Nutzenden gemäß Art. 13 DSGVO,
- die Zulässigkeit zur Speicherung von Informationen in der Endeinrichtung des Endnutzers (d.h. insbesondere Cookies) und der Zugriff auf diese Informationen gemäß § 25 TTDSG sowie
- die Zulässigkeit der Übertragung personenbezogener Daten in den Zugriffsbereich von Behörden in Drittstaaten.

Für Details finden Sie den Link zum Kurzgutachten hier: Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages (datenschutzkonferenz-online.de) und zum Beschluss hier: DSK_Beschluss_Facebook_Fanpages.pdf (datenschutzkonferenz-online.de)

European Data Protection Board (EDPB) zum Recht auf Auskunft nach Art. 15 DSGVO

Das Auskunftsrecht ist Gegenstand vieler Fragestellungen in der Praxis. Das European Data Protection Board (EDPB) beschäftigt sich mit diesem Thema in einer 60-seitigen englischsprachigen Guideline. Wir haben im Folgenden die wichtigsten und praxisrelevantesten Punkte zusammengefasst:

- **Umfang des Rechts auf Auskunft**
  Das EDPB legt den Begriff der Kopie weit aus und folgt insofern der Ansicht des Bundesarbeitsgerichts (BAG), das in seinem Urteil vom 27.4.21 (2 AZR 342/20) eine umfassende Auslegung des Rechts auf Kopie statuierte. Kopien sollten durch den Verantwortlichen in dauerhafter Form zur Verfügung gestellt werden und leicht verfügbar sein. Eine Übermittlung per E-Mail ist nicht ausgeschlossen, sofern sämtliche Sicherheitsstandards eingehalten werden.

- **Inhalt des Rechts auf Auskunft**
  Der Antrag eines Betroffenen ist nach Ansicht des EDPB aufgrund der zum Zeitpunkt der Antragstellung erfolgenden Verarbeitung zu beantworten. Konkret bedeutet dies, dass der Verantwortliche dem Betroffenen auch solche Daten, die ggf. unrichtig sind oder unrechtmäßig verarbeitet wurden, zur Verfügung stellen soll. Daten, die z. B. bereits aufgrund von gesetzlichen Aufbewahrungsfristen gelöscht wurden, sind hiervon ausgenommen. Das EDPB begründet das Zurverfügungstellen aller verarbeiteten Daten damit, dass Sinn und Zweck des Auskunftsrechts gerade darin liegen, dass ein Betroffener herausfinden können soll, wenn unrichtige Daten verarbeitet werden. Nach dem EDPB darf sich ein Verantwortlicher auch nicht vorsätzlich der Verpflichtung entziehen, die angeforderten personenbezogenen Daten zur Verfügung zu stellen, indem die personenbezogenen Daten als Reaktion auf einen Antrag auf Auskunft gelöscht oder geändert werden.

- **Einschränkungen des Auskunftsrechts*?***
  Grundsätzlich ist dem Antragssteller nach Ansicht des EDPB allgemein Auskunft zu erteilen und die Auskunft muss alle personenbezogenen Daten des Betroffenen beinhalten.
  Bei großen Datenmengen kann der Verantwortliche sich z. B. mit Selbstbedienungs-instrumenten bedienen. **Er kann auch um Spezifizierung des Antrages bitten** (so auch Erwägungsgrund 63 Satz 7 der DSGVO und das DSK Kurzpapier Nr. 6). Einschränkungen des Auskunftsrechts ergeben sich nach Ansicht des EDPB nur aus der DSGVO. Art. 15 Abs. 4 (Rechte und Freiheiten anderer Personen) DSGVO darf aber zu keiner umfassenden Ablehnung des Antrags führen.

- **Exzessive Anträge**
  Das EDPB äußert sich auch zur Auslegung der Begrifflichkeit des „exzessiven“ Antrags und vertritt hierbei eine enge Auslegung. Nach Auffassung des EDPB sind exzessive Anträge abhängig von dem Bereich, in dem der Verantwortliche tätig ist, z. B. je größer die Änderungsdynamik in der Datenbank des Verantwortlichen ist, desto häufiger kann die betroffene Person Zugang beantragen, ohne dass dies übermäßig ist. Der Verantwortliche sollte dann keine Zugangsverweigerung aussprechen, sondern vielmehr den Betroffenen eine

entsprechende Gebühr zur Deckung seiner entstandenen Verwaltungskosten entrichten lassen. Wann ein Ersuchen als „exzessiv“ zu bewerten ist, benennt das EDPB mehrere Konstellationen. Beispielsweise kann ein Antrag dann „exzessiv“ sein, **wenn eine Person einen Antrag stellt, aber gleichzeitig anbietet, diesen im Gegenzug für irgendeine Form von Vorteil für den Verantwortlichen zurückzuziehen**. Als exzessiv kann ein Antrag auch dann gewertet werden, **wenn ein anderer Zweck verfolgt wird**, z.B. die Störung des Betriebsfriedens oder das Erlangen von Informationen für einen Gerichtsprozess. Zudem fällt hierunter, wenn eine Person systematisch verschiedene Anfragen an den Verantwortlichen als Teil einer Kampagne sendet, z. B. einmal pro Woche, mit der Intention zu stören.

Praxishinweis: In der Gesamtschau bietet die Guideline einen guten Überblick über das Thema Auskunftsrecht. Sie kann in der Praxis als Orientierung dienen. *Es ist aber nicht zu vergessen, dass die letztendliche Ausgestaltung des Umfangs des Auskunftsrechts durch die Gerichte erfolgen wird, namentlich durch den EuGH. Dem EuGH liegen diverse Vorlagen zur Entscheidung vor. D.h. hier werden wir sicher in den kommenden Ausgaben weiter berichten. Den* Link zur Guideline *finden Sie hier*: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf

Impressum

mip Consult GmbH
Wilhelm-Kabus-Straße 9
10829 Berlin
Tel: +49 (0) 30 – 20 88 999 – 00
Fax: +49 (0) 30 – 20 88 999 – 88
Redaktion: Asmus Eggert, Nora Lynn Rodiek

Internet: www.sofortdatenschutz.de und www.blog.sofortdatenschutz.de
E-Mail: sofortdatenschutz@mip-consult.de

Vertretungsberechtigte Geschäftsführer: Asmus Eggert, Uwe Leider
Registergericht: Amtsgericht Berlin-Charlottenburg
Registernummer: HRB 121869
USt.-Identnr.: DE249276018
Verantwortlich nach § 18 Abs. 2 MStV: Asmus Eggert