LOSCHELDER

Newsletter Datenschutzrecht

März 2022

Sehr geehrte Damen und Herren,

es zeigt sich Licht am Ende des Tunnels: Die EU-Kommission und die USA haben einen Durchbruch erzielt und sich laut diverser Pressemitteilungen auf ein neues Abkommen geeinigt, um den Datentransfer in die USA rechtskonform zu gestalten. Details sind noch unbekannt und die kritischen Stimmen sind selbstverständlich auch zu hören. Für die Praxis ist dies eine überaus erfreuliche Nachricht, da damit ein Ende der permanenten Risikohinweise absehbar wird. Sobald das Abkommen in Kraft und die EU-Kommission daraufhin einen Angemessenheitsbeschluss erlassen hat, ist die Nutzung von US-Diensten wieder DSGVO-konform möglich (wenn auch ggf. nur bis zu einer weiteren EuGH-Entscheidung…). Wir halten Sie auf dem Laufenden.

Zunehmend sehen sich Unternehmen weitreichenden Auskunftsansprüchen und Schadensersatzansprüchen Betroffener ausgesetzt. Immer wieder stellt sich in diesem Zusammenhang die Frage, ob derartige Ansprüche auch unmittelbar gegen die Organe eines Unternehmens gerichtet sein können. Das KG Berlin hat dazu nun den EuGH angerufen, das OLG Dresden hat in einer höchst streitbaren Entscheidung eine persönliche Haftung von Geschäftsführern als unmittelbar DSGVO-Verantwortliche angenommen. So fragwürdig diese Entscheidung ist, sie ist in der Welt (und rechtskräftig). Rund um diese höchst praxisrelevanten Entscheidungen drehen sich unsere Beiträge 1 bis 3.

Der vierte Beitrag widmet sich der DSGVO-konformen Werbung: Die Aufsichtsbehörden haben zu diesem Themenkomplex eine neue Orientierungshilfe veröffentlicht. Geschlossen wird unser Newsletter, wie üblich, mit einem Blick auf besonders interessante Bußgelder der letzten Wochen.

Wir freuen uns über Ihr Interesse an unserem Newsletter!

Schließlich: Sie können der **Verwendung Ihrer Daten für diesen Newsletter-Versand jederzeit widersprechen,** indem Sie den Newsletter abbestellen. Bitte scrollen Sie dazu ans Ende dieser E-Mail.

Inhalt

Jetzt entscheidet der EuGH: Wer zahlt das Bußgeld – Geschäftsführung oder Unternehmen?

Das Kammergericht (KG) Berlin hat dem EuGH zwei hoch umstrittene Fragen zur Haftung von Unternehmen und Leitungsorganen für DSGVO-Verstöße vorgelegt: Der EuGH soll darüber entscheiden, ob sich ein Bußgeldverfahren wegen DSGVO-Verstößen unmittelbar gegen ein Unternehmen richten kann oder – so ist das im deutschen Ordnungswidrigkeitenrecht eigentlich vorgesehen – das Verfahren zunächst gegen ein Leitungsorgan und dann als Annex gegen das Unternehmen geführt wird. Entscheidet der EuGH, dass Unternehmen unmittelbar Betroffene („Angeklagte") eines Bußgeldverfahrens sein können, fragt das Kammergericht weiter, ob für eine Haftung ein bloßer Verstoß ausreicht oder ob das Unternehmen auch schuldhaft gehandelt haben muss. Die Entscheidung wird enorme Auswirkungen auf die interne Compliance und datenschutzrechtliche Risikovorsorge haben. Vor allem deswegen, weil sich hiernach entscheiden wird, welche Fälle überhaupt bußgeldrelevant sind und was die Unternehmensführung überhaupt tun kann, um Bußgelder zu vermeiden oder ob es in Zukunft nur darum geht, deren potenzielle Höhe zu begrenzen.

Im Oktober 2019 wurde ein Bußgelbescheid in Höhe von 14,5 Millionen Euro gegen die Deutsche Wohnen SE erlassen. Darin wurde die Deutsche Wohnen SE mehrerer Datenschutzverstöße beschuldigt. Aufgrund „gravierender Mängel" in dem Bescheid hob das LG Berlin diesen in einem Beschluss vom 18.02.2021 auf und stellte das Verfahren ein. Im März 2021 haben wir in unserem Newsletter ausführlich über diesen Beschluss berichtet. Gegen die Entscheidung des LG Berlin ging die Staatsanwaltschaft vor, sodass das Kammergericht Berlin als nächsthöhere Instanz mit dem Fall befasst wurde. Dieses hat den Fall Ende letzten Jahres dem EuGH vorgelegt und diesen mit der Beantwortung zweier Fragen beauftragt (Beschluss vom 06.12.2021 – 3 Ws 250/21).

Unmittelbare Haftung von Unternehmen für DSGVO-Verstöße?

Es geht um die Frage, ob ein Unternehmen Adressat eines Bußgelbescheides sein kann, ohne dass es dabei auf das konkrete Fehlverhalten seiner Leistungspersonen ankäme. Das ist im deutschen Recht so eigentlich nicht vorgesehen, hier gibt es kein „Unternehmens-Ordnungswidrigkeitenrecht". Nach deutschem Recht bedarf es stets einer Handlung eines Menschen, um eine

Ordnungswidrigkeit zu begehen. Das Unternehmen, für das die natürliche Person gehandelt hat, haftet dann als Annex, also nicht ohne die zuvor festgestellte Ordnungswidrigkeit der Leistungsperson.

Die DSGVO sieht dagegen in Art. 83 vor, dass „*ein Verantwortlicher*" für Verstöße haftet. Verantwortlich kann auch (und ist in der Regel) ein Unternehmen sein. Außerdem genießt die DSGVO als europarechtliche Verordnung grundsätzlich Vorrang vor mitgliedstaatlichem Recht, wobei allerdings umstritten ist, wie weit dieser Vorrang im Einzelfall und insbesondere im Fall von Bußgeldverfahren geht, deren konkrete Verfahrensregeln die DSGVO nicht vorsieht. Bei diesen ist hochumstritten, ob sich das nationale Recht durchsetzt und daher eine natürliche Person Betroffene eines Verfahrens sein muss oder ob auch ein Unternehmen selbst Betroffener sein kann. Mit dieser Frage ist nunmehr der EuGH befasst. Der Ausgang ist hier – soweit erkennbar – völlig offen. Das Kammergericht Berlin scheint mit einer unmittelbaren Haftung der Unternehmen zu sympathisieren, wenn man als Kriterium dafür gelten lässt, dass Argumente für diese Position erheblich mehr Raum in dem Vorlagebeschluss einnehmen als Gegenargumente. Urteilt der EuGH entsprechend, würde das auf den ersten Blick die Leitungsorgane von Unternehmen begünstigen, die dann nicht mehr Betroffene eines Bußgeldverfahrens werden könnten. Gleichzeitig muss man damit rechnen, dass in diesem Fall die potenziell bebußbaren Datenschutzverstöße massiv zunehmen, weil es nicht mehr auf das Fehlverhalten einzelner Personen ankommt, sondern auf den objektiven Verstoß im Unternehmen (dazu gleich). Und dafür haften Geschäftsführer und Vorstände wiederum zivilrechtlich und persönlich.

Haftung von Unternehmen nur für schuldhafte Verstöße?

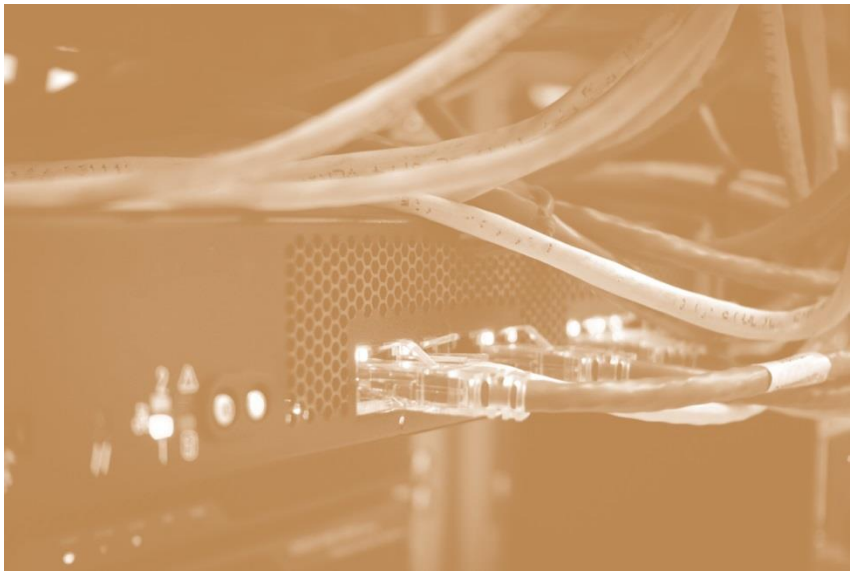
Außerdem müsste der EuGH sich einer weiteren Auslegungsfrage stellen, die das KG Berlin für den Fall gestellt hat, dass Unternehmen unmittelbar Betroffene in einem Bußgeldverfahren sein können: ist schuldhaftes Verhalten des Unternehmens erforderlich oder haftet das Unternehmen für jeden objektiv vorliegenden Verstoß? Nach dem deutschen Ordnungswidrigkeitenrecht haften Unternehmen zwar für jeden Verstoß ihrer leitenden Angestellten oder Organe, aber ein Verstoß liegt immer nur vor, wenn die Organe vorsätzlich

oder fahrlässig gehandelt haben. Daher haftet ein Unternehmen prinzipiell nur für schuldhafte Verstöße.

Nach der Konzeption der Bußgeldtatbestände der DSGVO bestehen allerdings keine Anhaltspunkte dafür, dass ein Verstoß schuldhaft sein muss. Eine entsprechende Entscheidung des EuGH wäre höchst überraschend. Davon scheint auch das Kammergericht auszugehen, das in dem Vorlagebeschluss eine Entscheidung des EuGH zitiert, nach der (allerdings im Kartellrecht) jeder objektiv vorliegende Verstoß ausreicht, um ein Bußgeld gegen ein Unternehmen zu verhängen. Aller Voraussicht nach ist ein Verschulden daher, wenn der EuGH entscheidet, dass ein Unternehmen unmittelbar Betroffener eines Bußgeldverfahrens sein kann, nicht Voraussetzung für die Verhängung einer Geldbuße. Auch ein noch so sorgfältig handelndes Unternehmen könnte dann im Falle eines Verstoßes seine Sorgfalt nur noch bei der Entscheidung zur Höhe des Bußgeldes, nicht aber zum „ob", anführen.

Praxis

Die Entscheidung des EuGH wird die unternehmensinterne Compliance maßgeblich beeinflussen. Entscheidet der EuGH, dass für ein Unternehmensbußgeld kein Fehlverhalten einer Leistungsperson notwendig ist, wächst die potenzielle Zahl von Bußgeldfällen im Unternehmen drastisch. Nun kann auch jedes Fehlverhalten auf der Arbeitsebene relevant sein, auch wenn kein Organisationsverschulden vorliegt. Wenn zudem noch kein Verschulden notwendig ist, summieren sich die potenziellen Fälle noch weiter auf. Unternehmen können demnach nur versuchen, möglichst intensiv zu schulen und zu sensibilisieren. Bußgeldfälle kann man gleichwohl durch gute Compliance verhüten, indem man den Behörden aufzeigt, alles Erforderliche getan zu haben, sodass die Behörde schon kein Verfahren einleitet oder zumindest das Bußgeld niedrig ansetzt. Bei alldem ist es also auch in Irrglaube, dass eine fehlende Mangerhaftung hier für Entlastung der Leitungspersonen führt: Wegen der potenziell höheren Zahl der Fälle bleibt gleichwohl das Risiko der zivilrechtlichen Regresshaftung gegenüber dem Unternehmen.



Kommt jetzt die persönliche Haftung von Geschäftsführern für DSGVO-Verstöße?

Nach einem Urteil des Oberlandesgerichts (OLG) Dresden ist der Geschäftsführer einer GmbH persönlich verantwortlich für einen im Unternehmen begangenen DSGVO-Verstoß. Damit treffen den Geschäftsführer persönlich alle DSGVO-Pflichten, inklusive der Bußgeldrisiken. Das Urteil ist rechtskräftig.

Das Gericht hatte den Geschäftsführer neben der Gesellschaft ohne nähere Begründung als datenschutzrechtlichen Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO angesehen und ihn und die Gesellschaft zu einer Schadensersatzzahlung in Höhe von 5.000 Euro verurteilt. Die Entscheidung überzeugt nicht, im Gegenteil: Sie ist mehr als fragwürdig. Aber: Die Entscheidung ist rechtskräftig und damit in der Praxis zumindest zu beachten. Sie erhöht damit das persönliche Haftungsrisiko von Geschäftsführern und anderen Leitungsorganen.

Verantwortlichkeit des Geschäftsführers?

Im Urteil des OLG Dresden (Urteil vom 30.11.2021, Az. 4 U 1158/21) befasste sich das Gericht mit der Haftung einer GmbH und der Haftung des Geschäftsführers wegen eines Datenschutzverstoßes. Der Geschäftsführer hatte rechtswidrig personenbezogene Daten des Klägers durch einen von ihm beauftragten Detektiv verarbeiten lassen.

Den daraufhin dem Kläger zugesprochenen Schadensersatzanspruch stützte das Gericht auf Art. 82 DSGVO. Danach steht Personen, die einen Schaden durch einen Datenschutzrechtsverstoß erlitten haben, ein Anspruch auf Schadensersatz gegen den Verantwortlichen oder den Auftragsverarbeiter zu. Das OLG erkannte jeweils auf einen selbstständigen Verstoß der GmbH und des Geschäftsführers.

Dabei stellte es nicht nur die Verantwortlichkeit der Gesellschaft, sondern – entgegen der bisherigen Rechtspraxis und aller überzeugender Argumente – auch die des Geschäftsführers fest. Die datenschutzrechtliche Verantwortlichkeit wird bejaht, wenn eine natürliche oder juristische Person allein oder gemeinsam über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden kann. Verantwortlich kann demnach zwar auch eine natürliche Person sein; ist diese aber für eine rechtliche Einheit wie eine GmbH tätig, trifft diese nach bisher ganz herrschender Meinung die Verantwortlichkeit. Das OLG Dresden hat dagegen festgestellt, dies gelte nicht für den Geschäftsführer. Eine Begründung bleibt das Gericht dabei schuldig, in dem Urteil findet sich nicht mehr als die bloße Feststellung.

Ordnungswidrigkeiten: Leitungsorgane als Adressaten

Bekannt ist die Diskussion um die Haftung von Geschäftsführung und anderen Leitungsorganen aus anderem Zusammenhang: Das Ordnungswidrigkeitenrecht sieht dies regelmäßig vor, dann aber nicht als datenschutzrechtliche Verantwortlichkeit, sondern als für das Unternehmen und dessen Organisation verantwortliche Person. Der Hintergrund: Ordnungswidrigkeiten oder Straftaten können im rein deutschen Recht nur durch Menschen, nicht aber durch Unternehmen begangen werden. Für ein Unternehmensbußgeld ist immer eine Anknüpfung an das Verhalten einer Leistungsperson notwendig.

Im letzten Jahr beschäftigte sich das LG Berlin in seinem Beschluss zur Deutsche Wohnen SE mittelbar mit der Frage der Verantwortlichkeit von Leitungsorganen für Datenschutzverstöße (wir berichteten in unserem Newsletter vom März 2021). Dabei setzte sich das Gericht mit der Frage auseinander, ob juristische Personen bei Verstößen gegen die DSGVO unmittelbar haften und die juristische Person daher auch Betroffene eines Bußgeldverfahrens

sein kann oder aber das Verfahren nach den üblichen Vorgaben des deutschen Ordnungswidrigkeitenrechts gegen ein Leitungsorgan gerichtet ist (und gegen die juristische Person nur nachrangig, wegen des Verstoßes des Leitungsorgans, ein Bußgeld verhängt werden kann). Richtet sich das Verfahren wie vom LG Berlin angenommen, gegen das Leitungsorgan, kann das auch zur Verhängung eines Bußgeldes gegen das Leitungsorgan führen. Selbst wenn dies aber nicht der Fall ist, ist das Leitungsorgan zumindest mit dem gegen das Unternehmen verhängten Bußgeld verknüpft, was den meisten Geschäftsführern, Vorständen usw. höchst unangenehm sein dürfte.

Auch die Ansicht des LG Berlin ist umstritten. Derzeit ist der Fall der Deutsche Wohnen SE beim KG Berlin anhängig, das jüngst Fragen zur Auslegung der DSGVO dem EuGH vorgelegt hat. Über den aktuellen Stand berichten wir in unserem ersten Beitrag in diesem Newsletter.

Folgen für die Praxis

So wenig überzeugend das Urteil des OLG Dresden ist, so ist es in der Praxis nun doch existent (und rechtskräftig). Geschäftsführer und andere Leitungsorgane sollten dies im Blick haben – bei der Implementierung und Umsetzung des Datenschutzmanagements im Unternehmen und beim Abschluss der relevanten Versicherungen. Was Gerichte möglicherweise bestärken kann: Wenn Leistungspersonen eigenmächtig, vorsätzlich und vollkommen selbstständig Entscheidungen treffen, die zu Rechtsverstößen führen. Dann liegt ggf. nach Wertung des Gerichts der Fall nicht anders, als wenn ein Einzelkaufmann für sein Unternehmen eine solche Entscheidung trifft. Dogmatisch und rechtlich bleibt es aber dabei, dass die genannte Entscheidung fragwürdig bleibt.

Prozessstrategie: DSGVO-Auskunftsansprüche mitdenken

Der datenschutzrechtliche Auskunftsanspruch ist nahezu allumfassend. Er wird daher auch zunehmend von Prozessparteien genutzt, um die eigene Position in gerichtlichen Streitigkeiten zu verbessern: Kläger begehren etwa Auskunft gegen den (künftigen) Beklagten, um Unterlagen zur Untermauerung von Schadensersatzklagen zu erhalten. Das (künftig) beklagte Unternehmen muss dann oftmals auch interne Schreiben, E-Mails und Vermerke mit Fallbewertungen herausgeben, in denen die Erfolgsaussichten einer „Klage von Herrn Müller" festgehalten sind, womöglich sogar mit Prozesstaktik, Insiderinformationen und Schwachstellen der eigenen Verteidigung. Auch an der Tagesordnung sind Ansprüche der Beklagtenseite, die mehr über die klägerische Prozesstaktik in Erfahrung bringen wollen. Was können Unternehmen also tun, um einer Herausgabepflicht solcher Unterlagen unter Art. 15 DSGVO vorzubeugen und sich in drohenden Rechtsstreitigkeiten nicht selbst zu schwächen?

Weiter Auskunftsanspruch

Viele Unternehmen haben die Erfahrung bereits gemacht: Der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DSGVO ist nahezu allumfassend. Betroffenen, die Auskunft begehren, sind nicht nur Informationen über die Art und Weise der verarbeiteten Daten

mitzuteilen. Sie müssen auch **Kopien** aller vorhandenen personenbezogenen Daten erhalten (wir berichteten etwa hier).

Der **Begriff der personenbezogenen Daten** ist dabei in Art. 4 Nr. 1 DSGVO weit zu verstehen. Erfasst werden alle Informationen die sich auf eine identifizierte oder identifizierbare Person beziehen. Als identifizierbar gilt eine Person dann, wenn die vorhandene Information eine Zuordnung zu der dahinterstehenden natürlichen Person ermöglicht. Die Auskunft ist also nicht nur hinsichtlich einer ausdrücklich namentlichen Nennung zu erteilen, sondern auch dann, wenn die betroffene Person mithilfe von Aktenzeichen oder anderen Referenzdaten ermittelt werden kann.

Der Auskunftsanspruch birgt damit die Gefahr der „**Zweckentfremdung**“: Betroffene können die Herausgabe sämtlicher personenbezogenen Daten nicht nur aus Gründen des Datenschutzes verlangen, sondern auch um Informationen zu erlangen, die der Durchsetzung von außerhalb des Datenschutzrechts liegenden Ansprüchen dienen. Unternehmen sind damit in der misslichen Lage, gegebenenfalls auch solche Daten herausgeben zu müssen, die anschließend in anderem Zusammengang (vor Gericht) gegen sie verwendet werden könnten.

„Pre-trial discovery“ statt Beibringung?

Diese Situation gleicht dem im angelsächsischen Rechtssystem vorhandenen Grundsatz der sogenannten „pre-trial discovery“, wonach die Parteien verpflichtet sind sich gegenseitig die für den Prozess relevanten Informationen zukommen zu lassen. Im deutschen Zivilprozessrecht ist ein solches Verfahren nicht vorgesehen. Nach dem hier maßgeblichen Beibringungsgrundsatz muss jede Partei grundsätzlich selbst die für sie günstigen Tatsachen vorbringen. Gelingt ihr das nicht, verliert sie den Prozess.

Die hiesige Rechtsprechung hat bisher keinen einheitlichen Umgang mit der Geltendmachung des datenschutzrechtlichen Auskunftsanspruchs zur **taktischen „Ausforschung“ des Gegners** etabliert. Das LG Köln hat hierauf bezogene Einwände mit der Begründung für unbeachtlich gehalten, dass der Anspruch aus Art. 15 DSGVO unabhängig von der dahinterstehenden Motivation bestünde.

Keine Auskunft über rechtliche Bewertungen

In einem Urteil des BGH hat der 6. Zivilsenat den Auskunftsanspruch jedoch dahingehend eingeschränkt, dass **interne Bewertungen** einer Versicherung zu den Ansprüchen des Versicherten gegen die Versicherung nicht herauszugeben seien. Konkret bezog der BGH dies auf rechtliche Analysen: Diese könnten zwar personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO enthalten (etwa den Namen eines Anspruchstellers), die auf Grundlage dieser personenbezogenen Daten vorgenommene rechtliche Analyse selbst stelle jedoch keine Information über den Betroffenen dar und sei folglich auch nicht herauszugeben.

Dabei stützt sich der BGH auf ein noch zur Datenschutzrichtlinie, die von der DSGVO abgelöst wurde, ergangenes Urteil des EuGH. In dem der EuGH-Entscheidung zugrundeliegenden Fall verlangte ein Asylbewerber nach Ablehnung einer beantragten Aufenthaltserlaubnis die Einsicht in den Entscheidungsentwurf, der der Ablehnung zugrunde lag. In diesem Entwurf waren Name, Geburtsdatum, Staatsangehörigkeit, Geschlecht, ethnische Zugehörigkeit, Religion und Sprache des Asylbewerbers angeführt. Ferner enthielt der Entwurf Angaben zum Verfahrensverlauf, vorgelegten Unterlagen, rechtlichen Bestimmungen sowie eine rechtliche Beurteilung dieser Angaben. Diese rechtliche Beurteilung stellte nach Ansicht des EuGH kein personenbezogenes Datum (mehr) dar. **Der Entwurf musste nicht herausgegeben werden.** Begründet wurde dies mit dem Schutzzweck der Datenschutzrichtlinie, wonach die Privatsphäre der Betroffenen bei der Verarbeitung personenbezogener Daten geschützt werden solle. Nicht vom Schutzzweck erfasst sei jedoch ein Recht auf Zugang zu solchen internen Dokumenten, die die rechtliche Analyse betragen.

In diesem Sinne urteilte auch das LG Köln in seinem zu dem vorgenannten Rechtsstreit zwischen Versicherer und Versichertem ergangenen Berufungsurteil mit der saloppen Bemerkung, dass der Auskunftsanspruch *„nicht der vereinfachten Buchführung des Betroffenen [diene]“*. Er solle vielmehr sicherstellen, dass der Betroffene Umfang und Inhalt der personenbezogenen Daten beurteilen kann. Der BGH bestätigte dies in der Sache.

Auch wenn die Hintergründe und Grundlagen der Entscheidung durchaus berechtigter Kritik ausgesetzt sind, ist das Urteil für die

Praxis höchst relevant: Es begrenzt den Auskunftsanspruch höchstrichterlich. Rechtliche Analysen sind nicht herauszugeben, auch dann nicht, wenn sie einzelne Angaben mit Personenbezug enthalten.

Herauszugeben sind allerdings nach dem vom BGH entschiedenen Rechtsstreit interne Vermerke wie Telefon-, Gesprächs- und Bewertungsvermerke zum Versicherungsverhältnis, welche von dem Auskunftsanspruch gegen die Versicherung umfasst sind.

Zu bedenken ist bei alledem, dass Betroffene stets einen hinreichend bestimmten Antrag stellen müssen – ohne einen solchen gibt es ebenfalls gute Gründe, von einer Übermittlung zu umfassender Auskünfte abzusehen (siehe dazu hier). Grundsätzlich kann von dem Betroffenen verlangt werden, dass er sein Auskunftsbegehren präzise formuliert. Nach Erwägungsgrund 63 der DSGVO gilt dies insbesondere, wenn eine große Menge an Informationen über die betroffene Person verarbeitet werden.

Keine Auskunft bei Geheimhaltungsbedürfnis

Ein Auskunftsanspruch ist ferner dann begrenzt, wenn durch eine Auskunftserteilung Rechte Dritter (auch solcher des Unternehmens, das die Auskunft erteilt) verletzen würde (Art. 15 Abs. 4 i.V.m. Erwägungsgrund 63 Satz 5 DSGVO und § 29 Abs. 1 Satz 2 BDSG): Das Auskunftsrecht soll keine „Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums“ beeinträchtigen, geheimhaltungsbedürftige Informationen bleiben geheim.

In der bisherigen Diskussion werden diese Ausnahmen sehr restriktiv gehandhabt, nur wenige Fälle sind sicher anerkannt. Erforderlich ist ein überwiegendes rechtliches, wirtschaftliches oder ideelles Interesse an der Geheimhaltung. Die Verteidigung vor außerhalb des Datenschutzrechts liegenden Leistungsansprüchen wird von der Literatur in diesem Zusammenhang regelmäßig nicht als hinreichender Grund erwähnt. Zumeist fallen hierunter Fälle, in denen bei Erfüllung des Auskunftsanspruches auch personenbezogene Daten Dritter erfasst wären. Im Einzelfall sollte indes genau geprüft werden, ob die Herausgabe bestimmter Informationen nach diesen Vorschriften unterbleiben darf oder sogar muss.

Als dem Auskunftsanspruch entgegenstehende Rechtsvorschriften kommen etwa auch die uns Rechtsanwälte treffenden Geheimhaltungsvorschriften in Betracht (§ 203 StGB oder § 43a Abs. 2 BRAO). Diese sind jedenfalls unmittelbar einschlägig, wenn sich das Auskunftsersuchen gegen den Rechtsanwalt selbst richtet, bei Auskunftsanfragen gegen Unternehmen ggf. unter dem Aspekt privilegierter Anwaltskommunikation. Hierfür spricht, dass die Rechtsordnung solcher Kommunikation einen besonderen Schutz gewährt.

Was tun?

In der Praxis sollten Auskunftsersuchen, die der Vorbereitung oder Verteidigung von bzw. in Prozessen oder anderen, zweckfremden Zielen dienen, genau analysiert werden, gerade auch mit Blick auf die Motivlage des Antragstellers.

Von vornherein kann die Auskunft nach Art. 12 Abs. 5 DSGVO verweigert werden, wenn ein Auskunftsbegehren offensichtlich unbegründet oder missbräuchlich ist (bei exzessiven und häufig gestellten Anträgen). In diesen Fällen muss jedoch das Unternehmen die Tatsachen für die offensichtliche Unbegründetheit oder den exzessiven Charakter des Antrages nachweisen. Die Grenzen sind hoch gesteckt, nur wenige Fälle in der Praxis sind tatsächlich derart unbegründet oder missbräuchlich.

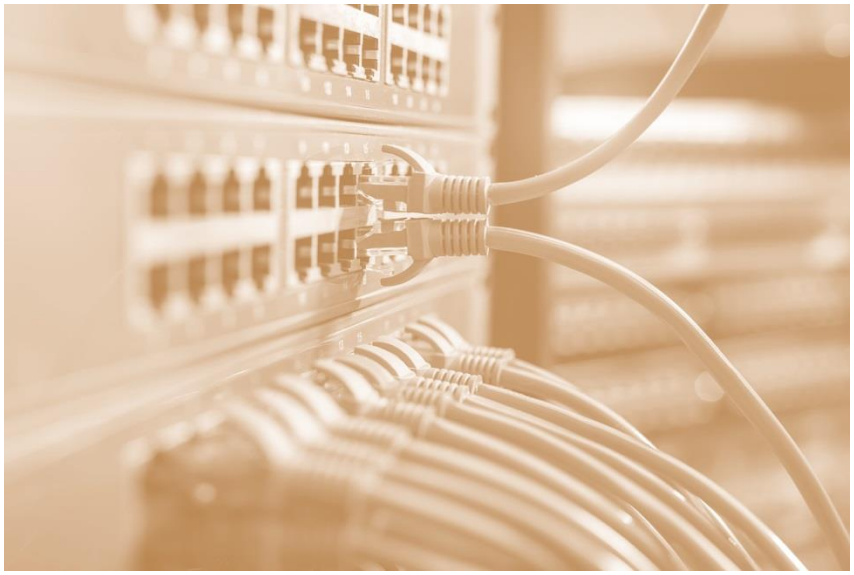
Bedeutsamer sind in der Praxis die weiteren, oben skizzierten Grenzen:

- Ist der Antrag bestimmt genug gestellt oder kann man von dem Antragsteller eine zeitliche, inhaltliche oder sonstige Konkretisierung erwarten?
- Können womöglich einzelne Dokumente als „rechtlichen Analysen“ von der Beauskunftung ausgeklammert werden?
- Besteht ein hinreichend valides Geheimhaltungsinteresse bezogen auf Rechte Dritter oder Betriebs- und Geschäftsgeheimnisse?

Je nach Beantwortung der vorstehenden Fragen sind die zu beauskunftenden Dokumente zu reduzieren (neben der stets zu gebenden allgemeinen Auskunft über die verarbeiteten Daten nach Maßgabe des Katalogs in Art. 15 Abs. 1 DSGVO).

Übrigens: In den Niederlanden verlangte ein Unternehmen von Personen, die ihre Betroffenenrechte aus der DSGVO geltend machten, eine Kopie des Personalausweises zur Identifizierung. Dies aber geht trotz Identifizierungspflicht den Niederländern zu weit: Die niederländische Datenschutzbehörde sah in dem konkreten Vorgehen einen Verstoß gegen Art. 12 Abs. 2 DSGVO und setzte ein Bußgeld in Höhe von 525.000 Euro fest.

Im Kern ging es um die Reichweite der Identifizierungspflicht: Nach Art. 12 Abs. 6 DSGVO müssen Unternehmen sicherstellen, dass die Auskunft, Löschung oder Berichtigung begehrende Person auch die ist, die sie vorgibt zu sein. Danach sind aber nur solche Identifizierungsmaßnahmen zulässig, die auch wirklich erforderlich sind. Im zu entscheidenden Fall war dies nicht mehr der Fall. Die „Ausweispflicht“ führte vielmehr nach Ansicht der Behörde dazu, dass die Ausübung der Betroffenenrechte entgegen Art. 12 Abs. 2 DSGVO erschwert wurde.



DSK: Wann dürfen personenbezogene Daten für Werbezwecke verarbeitet werden?

In einer neuen Orientierungshilfe hat die Datenschutzkonferenz des Bundes und der Länder (DSK) ihre Leitlinien aus dem Jahr 2018 für die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung erneuert. Die wichtigsten Punkte stellen wir Ihnen dar.

Werbemailings, Telefonanrufe und auch die Briefwerbung haben eines gemeinsam: Sie ist besonders effektiv, wenn Personen direkt angesprochen werden. Dann geht mit der Werbung auch stets die Verarbeitung personenbezogener Daten einher. Diese ist bekanntlich nur erlaubt, wenn eine Rechtsgrundlage dies trägt – bei Werbemaßnahmen stellt sich dabei regelmäßig eine Frage: Taugen die berechtigten Interessen als Erlaubnis oder ist doch eine Einwilligung erforderlich?

In ihrer neuen Orientierungshilfe konkretisiert die DSK ihre Sicht auf eben diese Frage und aktualisiert damit ihre Leitlinien aus dem Jahr 2018 für die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung.

Direktwerbung …

Im Ausgangspunkt ist für alles Weitere entscheidend, wann überhaupt von Werbung oder – noch konkreter „Direktwerbung" gesprochen wird. Um dies gleich vorweg zu nehmen: Der Begriff ist denkbar weit. „Werbung" ist nach gefestigter weiter Auffassung auch aus dem Wettbewerbsrecht jede Ansprache Dritter mit dem Zweck der Verkaufsförderung.

Die DSK definiert in ihrer neuen Orientierungshilfe nun erstmals den Begriff der „Direktwerbung": Dies ist Werbung durch unmittelbare Ansprache der Zielperson in unterschiedlichster Form, z.B. postalisch, per E-Mail, Telefon, Fax oder SMS (so auch LG Stuttgart Urt. v. 25.2.2022 – 17 O 807/21 - BeckRS 2022, 4821). Ein bestehendes Kundenverhältnis zwischen den Parteien setzt eine „Direktwerbung" nicht voraus. Auch Neukundenwerbung kann „Direktwerbung" sein.

Der Begriff der „Direktwerbung" ist datenschutzrechtlich wichtig, weil die DSGVO ein berechtigtes Interesse von Unternehmen an solch direkter, gezielter Werbung ausdrücklich als schutzwürdiges

Interesse anerkennt (EG 47 Satz 7 DSGVO). Die neue Orientierungshilfe beschränk sich auf die „klassische“ Direktwerbung und klammert insbesondere Werbung durch Werbetrackingmaßnahmen im Internet aus, die Gegenstand ihrer OH Telemedien sind.

… aus berechtigten Interessen oder mit Einwilligung?

In der Praxis stellt sich für Werbemaßnahmen regelmäßig die Frage, ob diese ohne Einwilligung der betroffenen Personen zulässig sind. Dies ist dann der Fall, wenn berechtigte Interesse der Werbenden im Sinne von Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO bestehen und diese nicht von gegenläufigen Interessen der Betroffenen überwogen werden.

Auch wenn hierfür grundsätzlich eine Einzelfallprüfung erforderlich ist, die u.a. auch die konkrete Ausgestaltung der Werbemaßnahmen in den Blick nimmt, gibt es grundsätzliche Leitplanken. Die DSK hat diese in ihrer neuen Orientierungshilfe mit einigen Beispielen illustriert:

- **Zusendung von Werbung nach Bestellung**

Wird im Nachgang zu einer Bestellung allen Kunden (d.h. ohne Selektion) postalisch Werbung zum Kauf vergleichbarer weiterer Produkte des Verantwortlichen zugesendet, ist dies in der Regel auch ohne Einwilligung zulässig. Das Gleiche gilt, wenn zwar aufgrund eines Selektionskriteriums (z.B. Postleitzahl oder Alphabet) eine Einteilung in Werbegruppen erfolgt, sich daraus aber kein zusätzlicher Erkenntnisgewinn durch Individualisierung ergibt.

Das Interesse der betroffenen Person am Ausschluss der Datenverarbeitung wird hingegen regelmäßig überwiegen, wenn der Verantwortliche automatisierte Selektionsverfahren zur Erstellung detaillierter Profile, Verhaltensprognosen bzw. Analysen, die zu zusätzlichen Erkenntnissen führen, einsetzt (sog. Profiling). Solche Maßnahmen sind nur mit wirksamer Einwilligung zulässig.

- **Kontaktwege: Post, E-Mail oder Telefon**

Im Hinblick auf die Wahl der Kontaktwege folgt die datenschutzrechtliche Interessenabwägung nach wie vor den spezifischen wettbewerbsrechtlichen Vorschriften (§ 7 UWG):

Danach ist die postalische Werbung eher zulässig, während für E-Mails und Telefonanrufe eine Einwilligung benötigt wird.

Ausnahmsweise können auch Werbe-E-Mails ohne Einwilligung verschickt werden, wenn sie unmittelbar bei den betroffenen Personen im Rahmen einer Vertragsbeziehung (Bestandskunden) erhoben wurden und die Vorgaben des § 7 Abs. 3 UWG eingehalten werden.

Telefonanrufe sind dagegen bei Verbrauchern immer nur mit Einwilligung zulässig, im beruflichen Kontext können auch „mutmaßliche Einwilligungen" im UWG-Duktus, datenschutzrechtlich also berechtigte Interessen eine taugliche Grundlage sein. Dafür soll allerdings, so die DSK in ihrer neuen Orientierungshilfe, eine bloße Sachbezogenheit nicht genügen. Es muss vielmehr laut DSK für den Anruf ein konkreter, aus dem Interessenbereich des Anzurufenden herzuleitender Grund vorliegen, z.B. ein geschäftlicher Vorkontakt.

- **Datenerhebung anlässlich von Preisausschreiben, Katalog-/Prospektanforderungen**

Die Verarbeitung von Postadressdaten aus der Durchführung von Preisausschreiben oder Katalog-/Prospektanforderungen zum Zweck der eigenen Direktwerbung ist nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO oftmals zulässig. Notwendig ist dafür aber stets eine Vorab-Information, insbesondere dann, wenn die Daten zunächst nur für die Durchführung des Preisausschreibens erhoben wurden.

- **Verwendung von Daten aus dem Impressum**

Die werbliche Nutzung von Daten, die aus einem Online-Impressum entnommen wurden, ist unzulässig. Zwar handelt es sich um allgemein zugängliche Daten, doch werden diese nicht freiwillig, sondern aufgrund gesetzlicher Verpflichtung veröffentlicht.

- **Beipack-Werbung**

Wird einem Vertragspartner mit vertraglichen Informationen auch eigene oder fremde Werbung postalisch zugesandt, ist dies in den Grenzen von Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO ohne Einwilligung möglich. Bei E-Mail-Werbung sind die Wertungen von § 7 Abs. 3

UWG zu beachten, allerdings gelten dessen Erleichterungen nicht für Fremdwerbung.

- **Freundschafts- und Empfehlungswerbung**

Die Direktwerbung an Postadressen, die Dritten dem werbenden Unternehmen übermitteln (z.B. durch Kundenbefragung oder „Tippgeber"), ist nach Ansicht der DSK regelmäßig unzulässig: Sie verstoße gegen die Grundsätze der fairen und transparenten Verarbeitung personenbezogener Daten. Ob dies in jedem Einzelfall überzeugt, ist indes fraglich und durchaus diskutabel.

Werbewiderspruch

Die Verantwortlichen müssen sicherstellen, dass betroffene Personen ihr Werbewiderspruchsrecht nach Art. 21 Abs. 2 DSGVO auf sämtlichen gegenüber ihnen verwendeten Kommunikationswegen effektiv und einfach geltend machen können. Der Verweis auf vorrangige Kontaktwege ist zwar zulässig, die Betroffenen dürfen aber nicht darauf beschränkt werden.

Wegen häufiger Irritationen bei Betroffenen darüber, dass sie ohne Einwilligung E-Mail-Werbung enthalten, empfiehlt die DSK einen deutlichen Hinweis auf die Möglichkeit von Werbung und das Widerspruchsrecht bereits bei Erhebung der E-Mail-Adresse, sowie die Ermöglichung einer sofortigen Ausübung desselben, z.B. durch eine Checkbox.

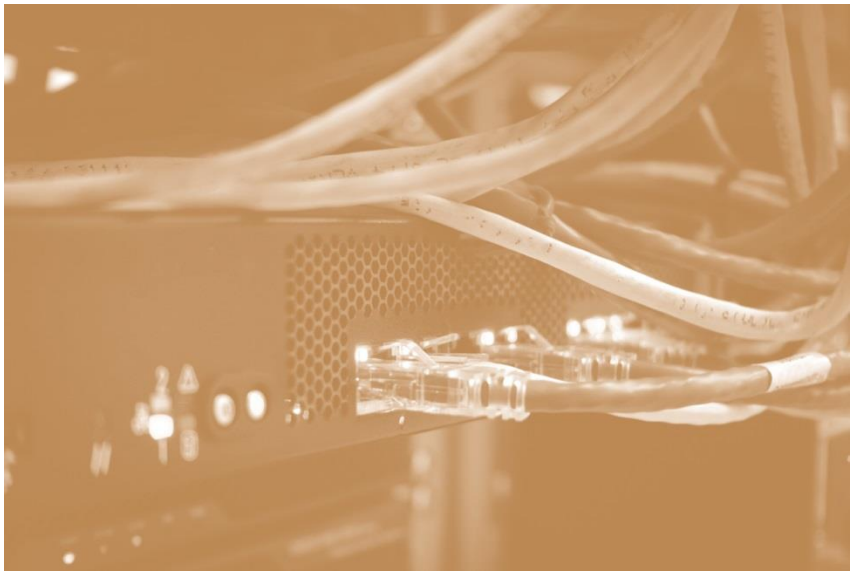
Widerspricht ein Betroffener, sind dessen Daten in einer Werbesperrdatei zu vermerken, um sicherzustellen, dass ihm im Rahmen der nächsten Kampagne nicht erneut Werbung zugeschickt wird.

Einwilligung

Selbstverständlich stets alternativ möglich ist eine Werbemaßnahme auf Basis einer wirksamen Einwilligung der angesprochenen Personen. Die DSK weist darauf hin, dass die DSGVO zwar keine spezifischen Vorgaben zur Dauer der Gültigkeit einer Einwilligung enthält, empfiehlt aber bei länger als zwei Jahre ungenutzten Einwilligungen eine Erneuerung der Information oder bestenfalls auch der Einwilligung selbst.

Weitere Pflichten

Jenseits der Frage der Rechtsgrundlage sind selbstverständlich auch die weiteren Pflichten der DSGVO zu beachten, insbesondere die allgemeinen Informations- und Nachweispflichten. Für telefonische Einwilligungen gilt auch im Datenschutzrecht die Nachweispflicht gem. § 7a UWG: Von Verbrauchern eingeholte Einwilligungen müssen für 5 Jahre nach der letzten Verwendung aufbewahrt werden.



Zu guter Letzt

Von Haarfrisuren, Werbeprofilen und Zoom-Meetings: Die Bußgelder der letzten Wochen wurden aufgrund durchaus illustrer Sachverhalte verhängt. Einige davon sind allerdings höchst praxisrelevant: Ausweiskopien als Identitätsnachweis von Personen, die ihre Betroffenenrechte geltend machen, dürfen nur dann verlangt werden, wenn diese dadurch nicht von der Geltendmachung der Betroffenenrechte abgehalten werden. Und ein Cyberangriff kann durchaus zu schmerzhaften Bußgeldern führen, obwohl das betroffene Unternehmen in dem in Griechenland entschiedenen Fall zuvörderst Opfer des Hackerangriffs war.

- **Haarfrisuren, Gesundheitszustand und Hautfarbe von Mietinteressenten: 1,9 Mio. Euro**

Weil sie von rund 9.500 Mietinteressenten Informationen verarbeitete, die für den Abschluss eines Mietverhältnisses nicht erforderlich waren, belegte die LfDI die BREBAU GmbH Anfang März mit einem Bußgeld in Höhe von 1,9 Mio. Euro. Für die Verarbeitung von Informationen wie Haarfrisuren, Körpergeruch und das persönliche Auftreten der Interessenten, Hautfarbe, sexuelle Orientierung oder ethnische Herkunft fehlte jede Rechtsgrundlage. Auch sorgte die BREBAU GmbH nicht für eine hinreichende Transparenz und Information der Mietinteressenten über die Datenverarbeitung. Das Bußgeld blieb trotz der erheblichen Verletzungen deutlich hinter der maximal möglichen Summe zurück, da die BREBAU GmbH laut LfDI umfassend kooperierte.

- **Teure personalisierte Werbung in Spanien: 3 Mio. Euro**

Eine Profiling zu werblichen, kommerziellen Zwecken und ohne Einwilligung der Betroffenen, zudem noch mit von anderen Unternehmen abgefragten Daten, verstößt gegen die DSGVO. Eine Bank in Spanien erhielt dafür ein Bußgeld in Höhe von 3 Mio. Euro von der spanischen Datenschutzbehörde.

Auch der Versuch, Einwilligungen einzuholen, war dabei gescheitert: Die Art und Weise der Profilbildung und Datenverarbeitung war nicht konkret genug dargestellt. Auf der gegebenen Informationsgrundlage konnten keine wirksamen Einwilligungen eingeholt werden.

- **Opfer eines Cyberangriffs und dazu noch ein Millionenbußgeld?**

Nach einem Cyberangriff auf sensible Kundeninformationen von zwei Mobilfunkunternehmen verhängte die griechische Datenschutzbehörde Bußgelder in Höhe von rund 6 bzw. 3,25 Mio. Euro. Die Unternehmen hatten es versäumt, die betroffenen Kunden ordnungsgemäß über den Hackerangriff zu informieren. Zudem traten bei Untersuchungen anlässlich des Vorgangs weitere Mängel im Datenschutzmanagement zu tage, so u.a. unzureichende Anonymisierungsprozesse, insgesamt unzulängliche technisch-organisatorische Maßnahmen und fehlende Verträge über die gemeinsame Verantwortlichkeit bzw. Auftragsverarbeitung.

- **17 Mio. Euro für Facebook nach Datenpannen aufgrund unzureichender technisch-organisatorischer Maßnahmen**

Teuer zu stehen gekommen sind insgesamt 12 Datenpannen dem Meta-Konzern (Facebook): Die irische Aufsichtsbehörde verhängte das Bußgeld, da die Datenpannenserie offenbarte, dass die technisch-organisatorischen Maßnahmen auf der Plattform nicht angemessen ausgestaltet waren.

- **Teures Zoom Meeting für den spanischen Fußballverband (AFE)**

Der spanische Fußballverband hat Aufzeichnung eines Zoom Meetings ohne das Wissen und ohne Zustimmung der Teilnehmer weitergegeben und diese ferner nicht ordnungsgemäß nach Art. 13 DSGVO informiert. Dies ahndete die spanische Datenschutzbehörde mit einem Bußgeld in Höhe von 200.000 Euro.

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

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@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