LOSCHELDER

Newsletter Datenschutzrecht

Februar 2023

Sehr geehrte Damen und Herren,

das Evergreen des Datenschutzrechts, das Auskunftsrecht, beschäftigt uns in diesem Monat erneut: Der Generalanwalt beim EuGH hat zuletzt eine sehr pragmatische Position zum „Recht auf Kopie“ eingenommen. Für die Praxis kann dies einen Kompromiss darstellen, der den Ressourcenaufwand im Unternehmen begrenzt hält und gleichzeitig eine effektive Information der Betroffenen absichert.

Auch ein Evergreen ist die rechtskonforme Gestaltung von Websites: Wie Cookie-Banner und Datenschutzerklärungen aussehen sollen, hat jetzt (auch) der Europäische Datenschutzausschuss näher beleuchtet. Er ist, so viel sei vorweggenommen, praxisnäher unterwegs als manche Aussagen der deutschen Aufsichtsbehörden.

Bemerkenswert ist sodann auch eine weitere Gerichtsentscheidung: Der BGH hat dem EuGH hoch praxisrelevante Fragen zur Personenbeziehbarkeit von Daten vorgelegt, konkret zu Bestelldaten von Arzneimitteln.

Schließlich widmen wir uns einem wichtigen Grundsatzthema, das gerade am Beispiel von Microsoft erneut praktisch relevant wurde: Wann und in welchem Umfang dürfen Datenschutzaufsichtsbehörden öffentliche Aussagen zur Datenschutzkonformität von digitalen Produkten treffen? Wie können sich Unternehmen vor unzutreffenden oder unberechtigten und ggf. auch geschäftsschädigenden öffentlichen Äußerungen schützen?

Wir freuen uns über Ihr Interesse!

Inhalt

Das Recht auf Kopie personenbezogener Daten: Zur Reichweite des Auskunftsrechts

Websites: Neues zur Gestaltung von Cookie-Bannern

BGH legt EuGH Fragen zu Bestelldaten von Medikamenten vor

Risiko Datenschutzaufsichtsbehörden: Welche öffentlichen Äußerungen sind zulässig?

Zu guter Letzt

Das Recht auf Kopie personenbezogener Daten: Zur Reichweite des Auskunftsrechts

Der Auskunftsanspruch nach Artikel 15 DSGVO umfasst unter anderem ein Recht auf Kopie dieser Daten. Doch was ist unter einer solchen Kopie zu verstehen und welche Informationen muss sie beinhalten, um diesem Anspruch zu genügen? Zu diesen Fragen hat der Generalanwalt beim EuGH nun Stellung genommen mit für die Praxis bedeutsamen Hinweisen.

Das Auskunftsrecht aus Art. 15 DSGVO ist einer der wichtigsten und praktisch besonders relevanten Ansprüche im Datenschutzrecht. Verlangt die betroffene Person Auskunft, geht damit nach Art. 15 Abs. 3 DSGVO ein Recht auf „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind" einher. Der Umfang dieser „Kopie" ist seit jeher umstritten.

Diese Fragen sind Gegenstand eines laufenden Vorabentscheidungsverfahrens am EuGH, welches mehr Rechtssicherheit verspricht. In dem zugrundeliegenden Sachverhalt aus Österreich ging es darum, ob der Auskunftsanspruch verletzt wird, wenn der Betroffene lediglich eine Zusammenfassung seiner personenbezogenen Daten in Form einer Übersicht oder Tabelle und keine vollständigen Dokumentkopien oder Datenbankauszüge erhält. Hierzu hat der Generalanwalt Giovanni Pitruzzella am 15.12.2022 seine Schlussanträge veröffentlicht. Die wichtigsten Aussagen aus diesen lauten:

1. Eine „Kopie" im Sinne des Art. 15 Abs. 3 DSGVO ist die originalgetreue Wiedergabe der angeforderten personenbezogenen Daten. Diese muss der betroffenen Person eine umfassende Kenntnis ihrer personenbezogenen Daten, die Gegenstand der Verarbeitung sind, vermitteln, sodass sie die Richtigkeit und die Ordnungsgemäßheit der Verarbeitung überprüfen kann.

2. Art. 15 Abs. 3 DSGVO verleiht der betroffenen Person (nur) das Recht auf eine Kopie der konkreten personenbezogenen Daten, die auch schon Gegenstand des Auskunftsanspruchs aus Absatz 1 sind. Mit anderen Worten braucht eine Kopie nicht mehr enthalten als eine anderweitige Auskunft über die konkreten, nach Art. 15 Abs. 1 DSGVO beauskunfteten Daten.

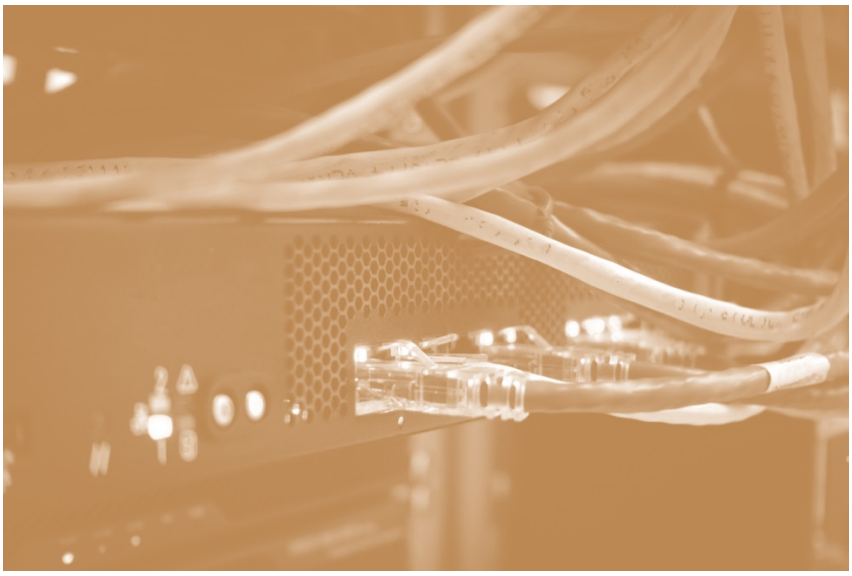
3. Im Einzelfall kann es dabei erforderlich sein, ganze Dokumente oder Datenbankauszüge zur Verfügung zu stellen, um die volle Verständlichkeit der angeforderten Daten zu gewährleisten. Dies folgt u.a. aus dem Transparenzgrundsatz, wonach sichergestellt sein muss, dass die betroffene Person in die Lage versetzt wird, die Informationen vollständig zu verstehen und ihre Betroffenenrechte geltend zu machen. Immer ist das aber nicht erforderlich!

4. Im Falle eines elektronischen Antrags sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen (Art. 15 Abs. 3 Satz 3 DSGVO). Der Begriff „Informationen" bezieht sich hierbei ausschließlich auf die Daten, die Gegenstand der Kopie und des konkreten Auskunftsantrags sind.

Auskunftsansprüche haben eine enorme praktische Bedeutung. Gerade die Zusammenstellung der Kopien nach Art. 15 Abs. 3 DSGVO kann dabei enorme Ressourcen im Unternehmen beanspruchen und ist dem Umfang nach oftmals hoch umstritten. Auf nationaler Ebene entschied etwa das Bundesverwaltungsgericht jüngst, dass Examenskandidaten ein Recht auf Kopie der vollständigen Prüfungsarbeiten haben (siehe dazu unseren Newsletter vom Dezember 2022).

Das EuGH-Verfahren zeigt deutlich, dass es auf den Einzelfall ankommt, wie umfangreich die Kopien tatsächlich sein müssen: Übermittelt werden muss nur, was die Auskunft nach Art. 15 Abs. 1 DSGVO illustriert und für ihr Verständnis erforderlich ist. Das sind nicht notwendigerweise ganze Datenbankkopien, sondern meist nur einzelne Auszüge. Eine solche Auslegung bringt die Interessen beider Seiten in einen angemessenen Ausgleich. Nicht zuletzt hängt dies auch vom Antrag und Verhalten des Antragstellers ab.

Das bevorstehende Urteil durch den EuGH wird hier für die Praxis mehr Klarheit bringen. Statistisch betrachtet folgt der EuGH meistens den Schlussanträgen der Generalanwälte. Wir werden berichten.



Websites: Neues zur Gestaltung von Cookie-Bannern

Der Europäische Datenschutzausschuss (EDSA) hat sich mit der Zulässigkeit und Gestaltung von Cookies und Cookie-Bannern im Lichte der e-Privacy-Richtlinie und der DSGVO beschäftigt. In einem Bericht vom 17. Januar 2023 hat er eine gemeinsame Position zu Cookie-Bannern angenommen. Mit den vertretenen Positionen zaubert der EDSA keine unerwarteten Überraschungen aus dem Datenschutz-Hut, dennoch gilt es für Website-Betreiber bestimmte Punkte zu beachten.

Ausgangspunkt für den EDSA-Bericht bilden die durch den Verein „NOYB – Europäisches Zentrum für digitale Rechte“ eingelegten Beschwerden gegen verschiedene Ausgestaltungen von Cookie-Bannern durch Website-Betreiber in der EU. Auch in Deutschland sind etliche dieser Verfahren anhängig. Sie können als Musterverfahren verstanden werden, deren Ausgang auch für etliche andere Websites von Bedeutung ist.

Der EDSA bemüht sich um eine einheitliche Positionierung der EU-Datenschutzaufsichtsbehörden in diesen Verfahren. Dies ist im nun veröffentlichten Bericht gelungen, auch wenn die dortigen Positionen nicht rechtsverbindlich sind. Sie dienen als Auslegungshilfe. In der Praxis haben sie erfahrungsgemäß richtungsweisende Auswirkungen auf die Behördenentscheidungen.

Die wichtigsten Aussagen im EDSA-Bericht:

1. Kein „Ablehnen"-Button auf dem ersten Layer (aber auf dem zweiten Layer)

   Im Bericht des EDSA heißt es, dass die weit überwiegende Mehrheit der Behörden für eine wirksame Einwilligung das Vorhandensein eines „Ablehnen"-Buttons auf *irgendeinem* Layer des Cookie-Banners für erforderlich halten.

   Die Datenschutzkonferenz (DSK) hatte hier noch mehr gefordert und dahin tendiert, der Button müsse schon auf dem ersten Layer implementiert werden: Denn laut DSK müsse den Nutzenden eine gleichwertige Handlungsoption zur Erteilung und zur Ablehnung der Einwilligung offeriert werden (vgl. Orientierungshilfe Telemedien der DSK; s. zu den DSK-Positionen bereits unseren Newsletter aus Februar 2022).

2. „Pre-ticked boxes" auf dem zweiten Layer

   Vorab angekreuzte Opt-in-Boxen für verschiedene Cookie-Kategorien auf dem zweiten Layer führen auch nach Auffassung des EDSA nicht zu einer wirksamen Einwilligung. Dies entspricht der Position des EuGH im Planet49-Verfahren und ergibt sich auch aus Erwägungsgrund 32 DSGVO sowie Art. 5 Abs. 3 ePrivacy-RL.

3. Irreführende Link-Gestaltung

   Cookie-Banner dürfen nicht so designt sein, dass Websitebesucher den Eindruck haben, sie müssten in die Cookienutzung einwilligen, um Zugang zu den Inhalten der Website zu erlangen. Ebenfalls unzulässig ist ein „Nudging", das Nutzende durch die Gestaltung klar dazu bewegt, einzuwilligen. Insbesondere sollen die folgenden Gestaltungen zu einer Unwirksamkeit der Einwilligung führen

   - Als einzige Alternative zur Einwilligung befindet sich ein (versteckter) Link hinter dem Begriff „Ablehnen", der, ohne ausreichende visuelle Unterstützung, in den Text des Cookie-Banners integriert ist.

- Die einzige Alternative zur Einwilligung bildet ein Link, der außerhalb des Cookie-Banners und ohne ausreichende visuelle Unterstützung platziert ist.

4. Schaltflächen mit irreführender Farbgestaltung oder Kontrastierung

Ebenfalls ein klassischer Fall: Der „Alle akzeptieren"-Button ist im Cookie-Banner durch entsprechende Farbwahl oder höheren Kontrast deutlich hervorgehoben. Der EDSA trifft keine allgemeingültige Aussage, ob dies zulässig ist. Den Verantwortlichen kann vielmehr, so der EDSA überzeugend, kein genereller Standard für die Gestaltung des Cookie-Banners im Hinblick auf Farbe und Kontrast vorgegeben werden. Letztlich ist im Einzelfall zu beurteilen, ob die Gestaltung offensichtlich irreführend ist und dann zur Unwirksamkeit der Einwilligung führt. Jedenfalls irreführend sei es, wenn der Kontrast des Buttons für die einzige Alternative zur Einwilligung so gestaltet ist, dass der Text für die Nutzenden unlesbar ist.

5. Berufung auf ein berechtigtes Interesse

Ist nach der ePrivacy-RL und dem deutschen TTDSG eine Einwilligung in das Setzen von Cookies erforderlich, kann eine nachfolgende Verarbeitung laut EDSA nicht im Einklang mit der DSGVO stehen. Der EDSA sieht damit eine „Infizierung" späterer Verarbeitungen, die durchaus streitbar ist. Die Position verdeutlicht aber nochmals, dass in der gesamten Verarbeitungskette auf eine rechtskonforme Vorgehensweise zu achten ist.

6. Fälschlich als „notwendig" deklarierte Cookies

Teilweise kommt es vor, dass Verantwortliche solche Cookies als „notwendig" oder „zwingend erforderlich" bezeichnen, die nach Art. 5 Abs. 3 ePrivacy-RL und der DSGVO eigentlich nicht als solche anzusehen sind. Der EDSA erkennt insoweit an, dass die Einordnung von Cookies als „unbedingt erforderlich" in der Praxis Schwierigkeiten bereitet. Er erwähnt aber auch eine Verpflichtung der Website-Betreiber, eine Liste der eingesetzten Cookies vorzuhalten und deren Notwendigkeit gegenüber den Behörden nachweisen zu

können. Zur Bestimmung, wann ein Cookie als notwendig anzusehen ist, verweist der Report ergänzend auf die Stellungnahme Nr.4/2012 der Artikel-29-Datenschutzgruppe zu den Ausnahmen von Cookie-Einwilligungen. Demnach sollen u.a. solche Cookies als notwendig erachtet werden, die es den Website-Betreibern erlauben, die von den Nutzenden im Hinblick auf einen bestimmten Dienst zum Ausdruck gebrachten Präferenzen (z.B. Spracheinstellungen) beizubehalten.

7. Keine „Widerrufen"-Schaltfläche

Als letzten Punkt hält der Report fest, dass Website-Betreiber einfach zugängliche Lösungen bereithalten müssen, um eine Einwilligung jederzeit zu widerrufen. Als konkrete Möglichkeiten nennt der EDSA den Einsatz eines kleinen „schwebenden" und dauerhaft sichtbaren Symbols oder eines Links der an einer sichtbaren und einheitlichen Stelle platziert ist. Erforderlich sei, dass der Widerruf jederzeit und ebenso einfach wie die Erteilung der Einwilligung möglich ist.

8. Hilfestellung durch Design-Guidelines

Für die praktische Umsetzung eines fairen und verbraucherfreundlichen Cookie-Banner-Consent-Managements hat eine vom BMUV geförderte europäische Stakeholder-Initiative Design-Guidelines sowie ein Muster-Cookie-Banner entwickelt und am 26.01.2023 veröffentlicht. Diese demonstrieren anschaulich, wie die verschiedenen Layer des CMP im Sinne von Autonomie, Fairness und Transparenz gestaltet sein könnten und was es dabei zu beachten gilt. Wie der Name bereits sagt, handelt es sich hierbei nicht um verbindliche Vorgaben, sondern lediglich um Empfehlungen.

BGH legt EuGH Fragen zu Bestelldaten von Medikamenten vor

Der Bundesgerichtshof (BGH) hat dem Europäischen Gerichtshof (EuGH) mit Beschluss vom 12. Januar 2023 eine Frage zur Qualifikation von Arzneimittelbestelldaten vorgelegt: Sind dies auch dann Gesundheitsdaten, wenn aus den übermittelten Daten nicht hervorgeht, für wen ein Arzneimittel bestimmt ist? Das Verfahren ist für die Auslegung des Begriffs der Gesundheitsdaten in Art. 9 DSGVO praktisch hoch relevant und auch für sonstige Fälle, in denen Gesundheitsdaten zur Vertragserfüllung verarbeitet werden.

Dem Vorlagebeschluss (I ZR 223/19, veröffentlicht ist bislang nur die Pressemitteilung) lag die Klage eines Apothekers gegen einen anderen Apotheker zugrunde. Der Beklagte vertreibt sein Sortiment auch im Internet, wofür er eine Versandhandelserlaubnis hat, u.a. über den sog. Amazon Marketplace. Das angebotene Sortiment enthält dabei auch apothekenpflichtige Medikamente.

Der Kläger sah den Vertrieb apothekenpflichtiger, jedoch nicht verschreibungspflichtiger Medikamente über Amazon durch den Beklagten als wettbewerblich unlauter an. Er ging von einem Rechtsbruch aus, da die notwendige datenschutzrechtliche Erlaubnis nicht vorläge. Im Kern ist dafür entscheidend, ob die in Rede stehenden Daten besonders sensitive Daten i.S.d. Art. 9 DSGVO (Gesundheitsdaten) darstellen oder aber nur „normale“

personenbezogene Daten, deren Verarbeitungserlaubnis aus Art. 6 DSGVO folgen kann.

Das OLG Naumburg vertrat in der Berufungsinstanz die Auffassung, dass es sich bei den erfassten Bestelldaten um Gesundheitsdaten i.S.v. Art. 9 Abs. 1 DSGVO handle. Aus den Bestelldaten könnten Rückschlüsse auf die Gesundheit des Bestellers gezogen werden.

Der in der Revisionsinstanz eingeschaltete BGH geht davon aus, dass der Erfolg der Revision von der Auslegung insb. des Art. 9 DSGVO abhängt.

Konkret fragt der BGH den EuGH u.a., „ob es sich bei den Daten, die Kunden des Beklagten bei der Bestellung von zwar apothekenpflichtigen, nicht aber verschreibungspflichtigen Medikamenten auf der Verkaufsplattform einzugeben haben (Name des Kunden, Lieferadresse und für die Individualisierung des bestellten apothekenpflichtigen Medikaments notwendige Informationen), um Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DSGVO sowie Daten über Gesundheit im Sinne von Art. 8 Abs. 1 DSRL handelt“ (Vorlagefrage 2).

Zweifel ergeben sich hier, da es nicht um verschreibungspflichtige Medikamente geht. Dementsprechend könne man aus der Bestellung selbst, so der BGH, nicht ersehen, wem dieses Medikament verschrieben worden sei und wer es demnach einnehmen solle bzw. wolle. Es sei nicht ausgeschlossen, dass der Besteller das Medikament nicht für sich selbst kaufe, sondern für einen Dritten. Ob diese Daten des Bestellers dann Gesundheitsdaten darstellen würden, obwohl nicht mit Sicherheit davon auszugehen ist, dass die durch die Bestelldaten identifizierte oder identifizierbare natürliche Person auch das bestellte Medikament einnehmen wird, hält der BGH für fraglich. Dafür spräche allerdings, dass der EuGH den Begriff der besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO in seiner Rechtsprechung sehr weit auslege.

Die ausstehende Entscheidung des EuGH hierzu ist höchst praxisrelevant: Reicht für die Qualifikation als besonders sensitive Daten schon die Möglichkeit, dass die Informationen etwas über den Gesundheitszustand der betroffenen Person aussagen? Wird dies bejaht, erweitert sich der Anwendungsbereich des Art. 9 DSGVO weiter.

Risiko Datenschutzaufsichtsbehörden: Welche öffentlichen Äußerungen sind zulässig?

Datenschutzaufsichtsbehörden spielen bei der Anwendung und Auslegung des Datenschutzrechts eine entscheidende Rolle. Äußern sich diese kritisch gegenüber der Datenschutzkonformität von (digitalen) Produkten, kann dies das Ende des Produkterfolgs und einen echten wirtschaftlichen Schaden bedeuten: Der Absatz wird gehemmt, die Risiken steigen auch für (potentielle) Investoren enorm. Der Fall Microsoft illustriert dies derzeit deutlich: Die Datenschutzaufsichtsbehörden veröffentlichten vernichtende Einschätzungen, nach denen ein datenschutzkonformer Einsatz von MS365 geradezu unmöglich sei – und dies zunächst sogar ohne vorherige Anhörung von Microsoft. Gäbe es Alternativprodukte am Markt, so wäre MS365 wohl kaum noch genutzt. Aber: War dies zulässig? Was dürfen Datenschutzaufsichtsbehörden in welcher Form öffentlich äußern?

Für Behörden gilt in Deutschland der Grundsatz der Gesetzmäßigkeit der Verwaltung (Art. 20 Abs. 3 GG). Danach haben sie die geltenden Gesetze einzuhalten und dürfen jedenfalls bei Grundrechtseingriffen nicht ohne Ermächtigungsgrundlage tätig werden.

Warnungen als Grundrechtseingriff

Spricht eine Behörde eine Warnung über ein Produkt aus oder gibt eine Einschätzung ab, dass sie ein Produkt für nicht gesetzeskonform hält, kann dies das betroffene Unternehmen fundamental und

nachhaltig treffen und sogar den Ruin bedeuten. Solche Äußerungen können das Marktverhalten erheblich beeinflussen, indem es (potentielle) Kunden und Investoren abschreckt. Dies kann zu schwerwiegenden finanziellen Auswirkungen durch die damit verbundene „Prangerwirkung" führen mit Eingriffen in die Berufsfreiheit und das Eigentumsgrundrecht. In einem aktuell in München entschiedenen Fall etwa hatte ein (zu weitgehender) Rückruf von Produkten durch das Verbraucherschutzministerium die Insolvenz einer Großmetzgerei zur Folge, der daher nun Amtshaftungsansprüche zustehen (OLG München, Urteil vom 31.01.2023, Az. 1 U 1316/21).

Warnungen oder Hinweise zur (fehlenden) Datenschutzkonformität von digitalen Produkten werden auch von Datenschutzaufsichtsbehörden immer wieder veröffentlicht. Prominentes Beispiel sind etwa die Äußerungen der Behörden zur Datenschutzkonformität von MS365, worüber wir zuletzt im Dezember 2022 berichteten. Weitere Beispiele sind etwa Aussagen der Berliner Behörde zu Videokonferenzsystemen oder des HmbBfDI zu E-Scootern. Dabei sind die Datenschutzaufsichtsbehörden zunächst einmal lediglich zur Überwachung und Durchsetzung der DSGVO zuständig (Art. 51 ff. DSGVO). Zwar dürfen sie auch aufklärend oder beratend tätig werden, eine ausdrückliche Erlaubnis zur Warnung der Öffentlichkeit vor Produkten ist jedoch weder der DSGVO noch dem BDSG zu entnehmen. Hinzu kommt, dass die Anbieter und Hersteller mit ihren Produkten nicht unmittelbar von der DSGVO adressiert sind.

Wird durch staatliches Informationshandeln die Markt- und Wettbewerbssituation eines konkreten Unternehmens negativ beeinflusst, liegt darin zugleich ein Eingriff in die durch Art. 12 GG geschützte Berufsfreiheit. Bei existenziellen Auswirkungen kann sogar der Schutzbereich der Eigentumsfreiheit nach Art. 14 GG berührt sein. Produktwarnungen haben bei Interessenten und Investoren oftmals eine abschreckende Wirkung und damit einen Einfluss auf das Auftreten eines Unternehmens am Markt. Wird etwa ein Produkt als nicht datenschutzkonform eingeordnet, werden es Kunden schon aufgrund eigener Bußgeldrisiken nicht einsetzen wollen und können, man denke etwa an ein CRM-System oder eben MS365, gäbe es Alternativprodukte und wären die Warnungen unangreifbar.

Gefahren für die Informationssicherheit

Führt eine Aussage einer Datenschutzaufsichtsbehörde zu einem derartigen Grundrechtseingriff, ist sie nur mit einer Ermächtigungsgrundlage rechtmäßig. Ausdrückliche Befugnisse, öffentliche Warnungen auszusprechen, finden sich z.B. im Marktüberwachungs-, im Arzneimittelgesetz oder u.a. in § 7 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Bei Gefahren für die Sicherheit in der Informationstechnik darf hiernach sogar der Name des konkreten Produkts sowie des Herstellers genannt werden. Diskutiert wurde in diesem Zusammenhang vor allem die BSI-Warnung vor der russischen Virenschutz-Software Kaspersky im Zuge des Ukraine-Krieges. Das Oberverwaltungsgericht NRW entschied, dass die Warnung durch das BSI rechtmäßig war.

Gilt das auch für Datenschutzbehörden?

Allerdings ist diese Ermächtigungsgrundlage im BSIG für Datenschutzaufsichtsbehörden nicht anwendbar. Ein von der Datenschutzkonferenz (DSK) beauftragter Arbeitskreis setzte sich mit der Frage einer speziellen Rechtsgrundlage für Produktwarnungen durch Datenschutzaufsichtsbehörden auseinander. Dieser sieht in Art. 58 Abs. 3 lit. b DSGVO eine mögliche Ermächtigungsgrundlage. Die Norm befugt die Behörden, sich zu Fragen im Zusammenhang mit dem Schutz personenbezogener Daten im Einklang mit dem Recht der Mitgliedstaaten an die Öffentlichkeit zu wenden. Ob aber eine solche Erlaubnis zur Öffentlichkeitsarbeit auf Grundrechtseingriffe trägt, ist überaus zweifelhaft. Es ist denn auch nach wie vor umstritten, ob Art. 58 DSGVO als Ermächtigungsgrundlage herangezogen werden kann. Gewichtige Gründe sprechen dagegen. Vor allem kümmert sich die DSGVO auch materiell nicht unmittelbar um den Produktdatenschutz.

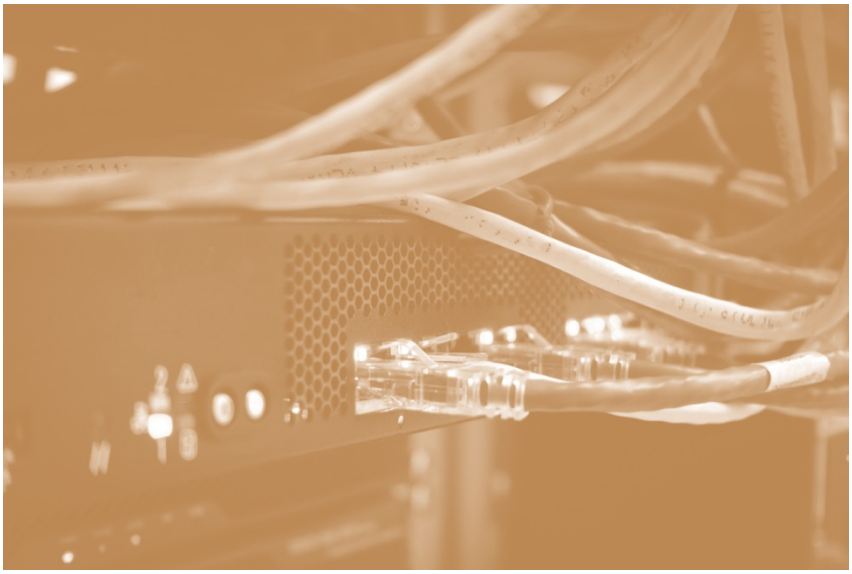
Und selbst wenn die Norm als Ermächtigungsgrundlage tragen kann, so liegt dem ein Verwaltungsverfahren zu Grunde, das nach rechtsstaatlichen Grundsätzen zu führen ist. Dies bedeutet insbesondere, dass der Sachverhalt ausreichend ermittelt und aufgeklärt werden muss – dafür wird in aller Regel eine Anhörung der betroffenen Unternehmen erforderlich sein.

Wird all dem Rechnung getragen, ist zu berücksichtigen, dass für die Öffentlichkeit ein legitimes Interesse an Informationen über die Einhaltung der DSGVO besteht. Allerdings muss dieses mit den Interessen der Unternehmen, insbesondere deren Berufsfreiheit, in Ausgleich gebracht werden. Eine öffentliche Anprangerung darf kein Ersatz für andere – gesetzlich geregelte – Aufsichtsmaßnahmen der Behörde sein. Aussagen dürfen nur im Einklang mit der Bindung der Behörde an Recht und Gesetz (Art. 20 Abs. 3 GG) erfolgen.

Handlungsoptionen für Unternehmen

Werden Anhaltspunkte bekannt, dass eine Datenschutzaufsichtsbehörde ein digitales Produkt prüft und sich womöglich dazu äußern wird, sollten Unternehmen daher unverzüglich mit der Behörde in Kontakt treten und ihre Position darlegen. In jeder behördlichen Kritik über ein Produkt steckt das Risiko negativer Auswirkungen auf dessen Vertrieb. Primäres Ziel sollte daher stets die Verhinderung der Aussage als solche sein. Hier können Unternehmen zur Not vorbeugenden oder einstweiligen Rechtsschutz bei den zuständigen Gerichten beantragen.

Ist dies nicht möglich, so sind im Fall fehlerhafter Produktwarnungen Amtshaftungsansprüche denkbar, die geprüft werden sollten. Davor besteht indes nach der aktuellen Entscheidung des OLG München eine Mitwirkungspflicht des Unternehmens, sachliche Fehler im Behördenverfahren aufzudecken und bei der Richtigstellung des Sachverhaltes mitzuwirken. Möglich ist all dies indes nur bei einer Einbeziehung und Anhörung im Verfahren.



Zu guter Letzt

Das Jahr beginnt in Sachen Bußgeldentscheidungen mit Ruhe und dafür gewichtig: Ein erneutes Millionenbußgeld trifft Meta für ihren Messenger-Dienst WhatsApp. In Italien ist ein mit künstlicher Intelligenz gesteuerter ChatBot vorübergehend eingestellt worden.

- **Irland: Meta kassiert für WhatsApp ein Bußgeld von 5,5 Mio. Euro wegen unrechtmäßiger Datenverarbeitung zu Werbezwecken.**

Meta wollte im Rahmen von WhatsApp Nutzer zur Datenweitergabe verpflichten. Da nach Ansicht der Datenschützer hierfür indes eine freiwillige Einwilligung notwendig sei, soll Meta nun ein Millionen-Bußgeld bezahlen (siehe hier die Berichterstattung im Spiegel zum Verfahren). Meta sieht dies anders und führt an, der Vertrag sei ausreichende Erlaubnis zur Datenverarbeitung.

Rund viereinhalb Jahre läuft das Verfahren gegen Meta wegen WhatsApp bereits. Es reiht sich in eine Vielzahl von vorangegangen Verfahren gegen den Großkonzern ein. Über 1 Mrd. Euro Bußgelder wurden wegen diverser Verstöße bereits gegen Meta verhängt.

- **Italien: Anordnung der vorübergehenden Einstellung eines AI-gesteuerten ChatBot**

Die italienische Datenschutzbehörde GPDP ordnete gegen das Unternehmen Luka Inc. die vorübergehende Einstellung eines mit künstlicher Intelligenz gesteuerten ChatBot an. Das US-amerikanische Unternehmen betreibt den ChatBot, mit dem die mentale Gesundheit des Nutzers verbessert werden soll. Der ChatBot verstehe die Gedanken und Gefühle, könne so ein Stressmanagementsystem aufbauen und insgesamt positives Denken bestärken.

Dem ChatBot wird indes vorgeworfen, insbesondere Minderjährige erheblichen mentalen Risiken auszusetzen. Datenschutzrechtlich beanstandete die GPDP nun, dass bei der Erstellung des Nutzeraccounts und auch bei der späteren Nutzung des ChatBot keine Altersabfrage stattfindet. Außerdem beinhaltete die Datenschutzerklärung keine Informationen über die Verarbeitung von Daten Minderjähriger.

Die GPDP stellte zudem fest, dass die Datenverarbeitung durch den ChatBot nicht zur Vertragserfüllung nach Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO erlaubt sei, jedenfalls nicht gegenüber Minderjährigen. Für diese sei es nach italienischem Recht nicht möglich, einen solchen Vertrag wirksam abzuschließen.

- **Finnland: 750.000 Euro Bußgeld wegen ausbleibender Antwort auf Auskunftsersuchen**

Die finnische Datenschutzbehörde leitete eine Untersuchung eines Inkassounternehmens ein, nachdem mehrere Beschwerden zu unbeantworteten Auskunftsersuchen eingegangen sind. Die Untersuchung offenbarte, dass das Unternehmen mehrfach Auskunftsersuchen nicht nachgegangen ist. Grund hierfür war unter anderem, dass das Unternehmen nicht ausreichend mit den Datenschutzgesetzen vertraut war. Das Unternehmen behinderte zudem die Arbeit der Aufsichtsbehörde und verzögerte die Untersuchung. Auch nach mehrfacher Aufforderung verweigerte das Inkassobüro die Kommunikation und wies keine Bereitschaft zur Zusammenarbeit auf. In der Gesamtschau führte dies zu einem Bußgeld in Höhe von 750.000 Euro nebst Verwarnung.

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

Philipp Schoel
+49(0)221 65065-200
philipp.schoel@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