LOSCHELDER

Newsletter Datenschutzrecht

Februar 2022

Sehr geehrte Damen und Herren,

wir starten mit unserem Datenschutz-Newsletter in das neue Jahr und haben gleich eine ganze Menge zu berichten: In den ersten Wochen des Jahres haben sich die Themen überschlagen, gerade für Online-Angebote jagte eine Neuigkeit die nächste.

In unserem ersten Beitrag ordnen wir die neuesten Vorgaben für die Gestaltung von Websites und Apps in den Gesamtkontext ein. Beitrag 2 widmet sich dem datenschutzrechtlichen Schadensersatz: Die zunehmende Anzahl an Gerichtsverfahren führen zwar zu erhöhten Risiken für Unternehmen, tragen aber auch zur Rechtssicherheit bei, weil Gerichte über spezielle Rechtsfragen entscheiden. Ähnliches gilt auch für unser Thema im dritten Beitrag: Das neue Papier des EDSA zu den Auskunftsrechten mag nur auf den ersten Blick die Rechtssicherheit erhöhen, steckt aber bei genauem Hinsehen voller Tücken für die zur Auskunft verpflichteten Unternehmen. Mittlerweile schon fast ein alter Hut ist die Erkenntnis, dass auch die datenschutzkonforme Gestaltung des Drittstaatentransfers voller Tücken bleibt. Nun helfen neue behördliche Veröffentlichungen bei der Einschätzung der nationalen Rechtslage in den USA, Russland, Indien und China, die wir in Beitrag 4 darstellen. Unser Newsletter schließt wie gehabt mit einem Überblick über berichtenswerte Bußgelder der letzten Wochen.

Zudem noch ein werblicher Hinweis in eigener Sache: Am 13.01.2022 ist unser neuer Praxisleitfaden **„Digitale Angebote“** im Beck-Verlag erschienen (https://tinyurl.com/4sepsn8u). Das Werk führt Anwender durch die maßgeblichen Rechtsvorschriften von der Idee bis zum Vertrieb und ist damit eine wesentliche Hilfestellung für alle Rechtsfragen rund um Apps, Cloud-Services, Softwareangebote, Plattformen uvm..

Inhalt

Neue Anforderungen an Websites, Cookies & Co.: Ein turbulenter Jahresstart

Für Websites, Apps und andere Online-Angebote kamen die Einschläge zum Jahresbeginn beinahe im Minutentakt: Die neue Orientierungshilfe Telemedien 2021 der Datenschutzkonferenz macht eine Überprüfung der Consent Management Tools und Datenschutzerklärung erforderlich. Dies gilt umso mehr, als die Datenschutzaufsichtsbehörde in Belgien den derzeitigen Markstandard für die Werbevermarktung am 02.02.2022 für DSGVO-widrig erklärt hat. Ein ähnliches Schicksal ist Google Analytics in Österreich widerfahren, so dass das Tool nun womöglich zum Compliance Risiko wird. Und schließlich: 100 Euro Schadensersatz wegen des Einsatzes von Google Fonts könnten sich potenzieren … der Cookiebot darf dafür zunächst weiter genutzt werden.

Strenge Maßstäbe der Datenschutzaufsichtsbehörden:

Für Betreiber von Online-Angeboten wie Websites, Plattformen und Apps wird es nicht langweilig: Wieder sind neue Anforderungen zu beachten und umzusetzen. Anlass hierfür ist zum einen die Umbenennung des Facebook-Konzerns. Zum anderen bringt eine neue Orientierungshilfe der Datenschutzaufsichtsbehörden „Schwung" in die Diskussion um die Anwendung des seit dem 01.12.2021 geltenden TTDSG.

1. Neuer Namen, neue Datenschutzerklärung

Der Facebook-Konzern heißt nun Meta. Konkret hat die in der EU aktive Einheit „Facebook Ireland Limited" ihren Namen ab dem 04.01.2022 in „Meta Platforms Ireland Limited" geändert. Für Unternehmen, die Präsenzen auf Facebook unterhalten oder Facebook-Angebote in ihren eigenen Online-Angeboten eingebunden haben, besteht nun Handlungsbedarf:

In den Datenschutzerklärungen und im CMP bzw. Cookie-Banner muss der den Anbieter ausweisende Unternehmensname jetzt geändert werden. Die Erklärungen sind sonst falsch, es droht ein Verstoß gegen die Informationspflichten.

Zu ändern ist nur der Unternehmensname. Die Plattformen selbst firmieren weiterhin unter „Facebook", „Instagram" oder „WhatsApp". Dies gilt ganz ungeachtet dessen, zu welchen Neuerungen das Metaversum wohl führen mag.

2. Was die Aufsichtsbehörden fordern

Deutlich herausfordernder ist die Umsetzung der neuen „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“, die von der Datenschutzkonferenz (DSK) kurz vor Weihnachten veröffentlicht wurde, kurz die „OH Telemedien 2021“. Darin formulieren die Aufsichtsbehörden, wie Online-Angebote nach ihrer Rechtsauffassung gestaltet sein müssen, um dem neuen Telekommunikation-Telemedien-Datenschutzgesetz, kurz TTDSG, und der DSGVO zu genügen.

Das Ergebnis vorab: Einiges ist überzeugend, vieles aber auch durchaus streitbar. Unternehmen sind gut beraten, die Punkte nun genau zu prüfen und ihre bestehenden Risikoabwägungen zu überdenken. Keinesfalls sollte die OH Telemedien 2021 unbeachtet bleiben. Sie ist allerdings nicht verbindlich – Behörden können abweichen, Gerichte müssen das Rechtsverständnis vollumfassend und selbständig überprüfen. Eine Pflicht zur Umsetzung besteht angesichts dessen nicht, für die Risikoabwägung ist die OH Telemedien 2021 aber höchst relevant, da in ihr vorgezeichnet wird, wie sich Aufsichtsbehörden positionieren dürften.

Relevant ist die Orientierungshilfe für alle Unternehmen, die Websites und andere Online-Angebote betreiben und über diese Angebote auf Endnutzergeräte zugreifen und / oder personenbezogene Daten verarbeiten. Dies ist etwa dann der Fall, wenn (über eingebundene Dienste) Cookies gesetzt werden, Einträge im Local Storage erfolgen oder auch wenn Geräteinformationen wie IDs, MAC Adressen oder andere Informationen etwa über einen JavaScriptCode ausgelesen werden.

All diese Unternehmen sollten sich nun mit folgenden Punkten beschäftigen:

- **Anpassung der Datenschutzerklärung und ggf. des Cookie Banners:** Überall dort, wo Tools auf Endgeräte zugreifen, ist § 25 TTDSG als Rechtsgrundlage neu anzugeben. Dies betrifft die Datenschutzerklärung und ggf. auch die verwendete Consent Management Plattform („Cookie Banner“ – „CMP“), wenn dort Normen angegeben sein sollten. Für alle weiteren Verarbeitungsschritte bleibt eine DSGVO-Erlaubnis erforderlich, falls personenbezogene Daten verarbeitet werden.

- **Wirksamkeit der benötigten Einwilligungen checken:** Für eine Vielzahl von Tools wird eine Einwilligung benötigt – nach den Regelungen in § 25 TTDSG immer dann, wenn der Endgerätezugriff oder das Auslesen von Informationen aus dem Endgerät nicht unbedingt erforderlich ist, um den vom Nutzer angefragten Dienst zu erbringen. Die OH TMG 2021 bringt zu diesem Thema eine Reihe von Rechtsansichten, die von Unternehmen zu beachten sind ():

  Einwilligung auch für Analysedienste? Ob auch Analysedienste einer Einwilligung bedürfen oder aber unbedingt erforderlich im Sinne des Gesetzes sind, ist umstritten. Aufsichtsbehörden anderer EU-Mitgliedstaaten billigen aktuell den Einsatz auch ohne Einwilligung, die deutschen Aufsichtsbehörden sind hier zurückhaltender und haben insbesondere für Google Analytics bereits ausdrücklich Einwilligungen gefordert. Die OH TMG 2021 bestätigt dies: Wer Analysedienste ohne Einwilligung nutzen will, sollte dies sehr genau prüfen. Im Einzelfall kann dies aber nach wie vor zulässig sein. Abhängig ist dies von dem konkreten Zuschnitt des Tools, welche Daten wofür verwendet werden und wo der Einsatz erfolgt.

  Jedenfalls finden sich im OH Telemedien 2021 hinreichend Anhaltspunkte für ein enges, strenges Verständnis der „unbedingten Erforderlichkeit". Die Aufsichtsbehörden werden mithin bei einer Vielzahl von Tools von einer Einwilligungsbedürftigkeit ausgehen.

  Eine wirtschaftliche Erforderlichkeit sei, so die ausdrückliche Aussage, unerheblich – wirtschaftliche Erwägungen könnten keinen Verzicht auf eine Einwilligung tragen. Ob dies auch vor einem Gericht so bestätigt würde, ist diskussionswürdig, insbesondere, wenn der entsprechende Dienst ansonsten nicht angeboten würde.

  Ein Klick für alle Tools? Eine Bündelung von Einwilligungen ist zulässig. Die weit verbreitete Grundstruktur der CMPs, die auf 1. Ebene ein „alle akzeptieren" vorsehen, ist damit auch nach Ansicht der Aufsichtsbehörden möglich. Das setzt aber voraus, dass schon vor dem Klick ein Überblick gegeben wird, was die abgefragte Einwilligung alles umfasst. In der Praxis bedeutet dies, dass der Text auf 1. Ebene sehr genau gefasst

sein muss, um in kurzer Form einen vollständigen und klaren Überblick übermitteln zu können.

„Alle ablehnen“ Button auf 1. Ebene des CMP? Nach den bisherigen Verlautbarungen nicht überraschend fordern die Aufsichtsbehörden, dass die Einwilligung nicht einfacher gestaltet sein darf als ihre Ablehnung. Nutzer müssen die Online-Angebote daher auch ohne eine Aktion (ohne „Klick“) besuchen können oder aber der Klick auf „alle ablehnen“ müsste genauso einfach sein, wie der Klick auf „alle akzeptieren“ (siehe hierzu auch die Entscheidung der französischen Aufsichtsbehörde in unserer Rubrik „Zu guter Letzt"). Diskutiert wurde dies zuletzt etwa auch unter dem Schlagwort „Nudging“: Die Aufsichtsbehörden kritisierten auch die farblich ansprechendere Gestaltung eines Buttons „Alle akzeptieren“, der Nutzer dazu verleite, auf diesen – und nicht den „Ablehnen-Button“ – zu klicken.

Vollständige Informationen im CMP? Eine Einwilligung kann nur dann wirksam eingeholt werden, wenn der Nutzer zuvor über alle relevanten Umstände informiert wird und seine Entscheidung damit auch tatsächlich freiwillig treffen kann. Ein besonderes Augenmerk richten die Aufsichtsbehörden hier auf die Information, wer Daten erhebt und an wen sie weitergegeben werden sowie die Angabe der Dauer.

Keine Blanko-Einwilligung und Neuabfrage bei Änderungen: Sichergestellt sein muss, dass die abgegebene Einwilligung stets die tatsächlichen Verarbeitungsprozesse abbildet. Ändern sich diese, muss von allen Nutzern eine neue Einwilligung eingeholt werden.

Einfacher Widerruf: Der Widerruf der Einwilligung muss genau so einfach möglich sein, wie ihre Erteilung. Wird die Einwilligung durch einen Klick im CMP abgefragt, muss auch der Widerruf mit einem Klick möglich sein (und nicht etwa eine E-Mail des Nutzers erfordern). In der Praxis ist dies regelmäßig durch entsprechende „Klick-Optionen“ im CMP abbildbar, auf die etwa in der Datenschutzerklärung im Rahmen der Erläuterung der Widerrufsmöglichkeiten ergänzend verlinkt werden kann.

Mehr dazu finden Sie auf unserem Blog „Digitalisierung & Recht“:

- zur Gestaltung von CMP und Datenschutzklärung hier https://digitalisierungsrecht.eu/neue-vorgaben-fuer-online-angebote-unternehmen-sollten-datenschutzerklaerung-und-cmp-jetzt-updaten/

- und zur Frage, welche Tools nun der Einwilligung bedürfen, hier https://digitalisierungsrecht.eu/einwilligungspflicht-fuer-online-tools-der-standpunkt-der-behoerden/

Die OH Telemedien 2021 wird aktuell von den Datenschutzaufsichtsbehörden konsultiert, Stellungnahmen sind noch möglich: https://datenschutz-hamburg.de/pages/dsk-konsultationsverfahren/

Belgische DPA: Consent Management Plattformstandard für Online-Werbung verstößt gegen die DSGVO

Einen erheblichen Umbruch könnte eine aktuelle Entscheidung der belgischen Datenschutzaufsichtsbehörde für die Online-Werbewelt bedeuten: Websites, die umfangreiche Werbeeinbindungen nutzen und Werbende, die online zielgerichtet werben möchten, platzieren ihre Werbung bzw. verkaufen die Werbeplätze auf ihrer Website über Echtzeit-Bietverfahren in Sekundenschnelle.

Eine solche Technik ist in der Praxis nur umsetzbar, wenn benötigte Einwilligungen und Informationen (nach Datenschutzrecht und ePrivacy-Recht) automatisiert und stets aktuell eingeholt bzw. ausgegeben werden können. Der hierfür bislang weit verbreitete technische Standard ist das sog. **TCF (Transparency and Consent Framework) des IAB**.

Die belgische Datenschutzaufsichtsbehörde hat nun entschieden, dass dieses TCF in einer Vielzahl von Punkten gegen die DSGVO verstößt (Entscheidung vom 02.02.2022). Die Aufsichtsbehörde hat ein Bußgeld von 250.000 Euro ausgesprochen und eine Reihe von Maßnahmen verlangt, bis hin zur Datenlöschung. Derzeit ist noch nicht absehbar, wie dies in der Praxis umgesetzt wird. Das IAB jedenfalls hat am 11.02.2022 erwartungsgemäß verkündet, die Entscheidung einer gerichtlichen Überprüfung zuzuführen.

Darf Google Analytics noch verwendet werden?

Google Analytics verstößt gegen die DSGVO, die Nutzung dieses Tools ist rechtswidrig: Dies hat die Datenschutzaufsichtsbehörde in Österreich unlängst entschieden. Auch die französische Datenschutzaufsicht CNIL hat jüngst die Verwendung von Google Analytics untersagt. Ist Google Analytics damit jetzt ein Compliance-Risiko und die Abschaltung dringend anzuraten?

Die Entscheidung ist die erste öffentlich bekannt gewordene Entscheidung in einem der 101 von NOYB (der von dem Aktivisten Max Schrems initiierten NGO, die sich der Durchsetzung des Datenschutzes verschrieben hat) in der ganzen EU eingeleiteten Beschwerdeverfahren. Auch in Deutschland sind Verfahren anhängig.

NOYB kritisiert im Wesentlichen, dass beim Einsatz von Google Analytics personenbezogene Daten ohne hinreichende Schutzmaßnahmen von EU-Websitebesuchern in die USA übermittelt werden. Die Datenschutzaufsichtsbehörde hat dies im entschiedenen Fall bestätigt.

Bedeutet dies, dass Unternehmen nun auf den Einsatz von Google Analytics verzichten müssen?

Sicher ist: Google Analytics sollte nur nach umfassender Risikoanalyse eingesetzt werden und nur mit individueller Konfiguration.

Dafür ist entscheidend:

Die Entscheidung der Datenschutzaufsichtsbehörde in Österreich, die den Einsatz von Google Analytics als DSGVO-widrig eingeordnet hat, ist nicht ohne weiteres verallgemeinerbar. Google bietet diverse Konfigurationsmöglichkeiten für Google Analytics an und hat das Produkt seit dem für die Entscheidung maßgeblichen Zeitpunkt (14.08.2020) weiterentwickelt. Zudem hat der Websitebetreiber es in der Hand, einige Stellschrauben zu verändern:

- **Konfiguration:** Die Ausgangskonfiguration von Google Analytics ist regelmäßig datenschutzunfreundlich. Hier liegt es am Webseitenbetreiber, diese datenschutzfreundlich anzupassen. In dem Fall, der in Österreich entschieden wurde, war dies allenfalls bedingt geschehen: **Die Funktion „IP-**

Anonymisierung“ war nicht aktiviert, dafür aber die Vergabe einer einzigartigen Kennnummer (UID). Auch die Pressemitteilung aus Frankreich deutet an, dass im dort zu entscheidenden Fall umfangreichere personenbezogene Daten erhoben wurden.

- **Opt In oder Opt Out:** Es liegt in der Hand des Websitebetreibers, ob er Google Analytics als „Opt Out“ (Widerspruchslösung) oder nur nach Einwilligung („Opt In“) eines jeden einzelnen Nutzers aktiviert. Eine Aktivierung ohne Einwilligung begegnet deutlich weitergehenden rechtlichen Bedenken, die aus unserer subjektiven Sicht inzwischen überwiegende Zahl der Websites setzt Google Analytics nur nach Einwilligung ein. Hier liegt ein weiterer entscheidender Unterschied zur Entscheidung aus Österreich: **Dort war Google Analytics ohne Einwilligung aktiviert.**

- **Standardvertragsklauseln 2021**: Seit Juni 2021 gibt es zudem neue Standardvertragsklauseln, die den Drittstaatentransfer absichern können. Die Datenschutzaufsichtsbehörde in Österreich hat diese (völlig zutreffen) nicht geprüft, sondern zu den am 14.08.2020 geltenden und vereinbarten Standardvertragsklauseln 2010 entschieden. Die Entscheidung in Österreich stellt fest, dass diese Standardvertragsklauseln 2010 nicht ausreichen, um ein angemessenes Schutzniveau für den Drittstaatentransfer zu schaffen. Für die Entscheidung aus Frankreich ist dies noch nicht bekannt – da auch diese einen Websitebesuch im August 2020 zu prüfen hatte, spricht indes viel dafür, dass auch dort noch die alten Klauseln Prüfgegenstand waren.

Nach alledem zeigt die Entscheidung aus Österreich letztlich nur, mit welcher erheblichen Rechtsunsicherheit und welchen Risiken der Betrieb von Online-Angeboten derzeit belegt ist. In diesem Zusammenhang ist denn auch interessant, dass die Aufsichtsbehörde in Österreich ausschließlich einen DSGVO-Verstoß festgestellt hat. Sie hat kein Bußgeld ausgesprochen.

Für die Praxis raten wir den Einsatz von Analysetools sehr genau zu untersuchen und eine ausgewogene und umfassende Risikoentscheidung zu treffen – und diese weitere Entwicklung zu monitoren. Auch in Deutschland werden die ersten Entscheidungen zu Google Analytics kommen, auf EU-Ebene wurde bereits über

einen „Muster-Bescheid“ diskutiert, mit dem die NOYB-Beschwerden beschieden werden könnten, bislang allerdings ohne Einigung (dazu TOP 4 hier).

Mehr dazu finden Sie hier: https://digitalisierungsrecht.eu/darf-google-analytics-noch-verwendet-werden/

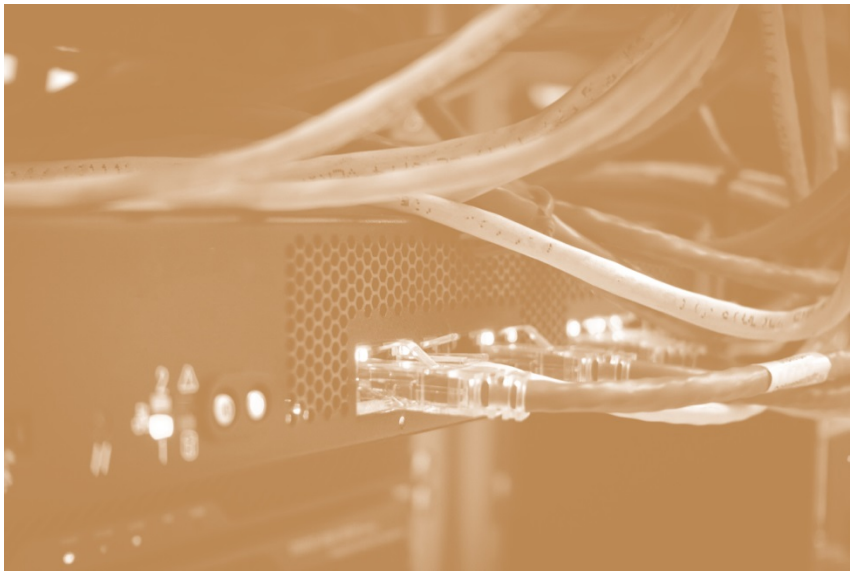
Google Fonts und Cookiebot: Die IP-Adresse als personenbezogenes Datum

Die Einbindung des Consent Management Tools „Cookiebot“ war Gegenstand eines Verfahrens des Einstweiligen Rechtsschutzes in Hessen. Ende 2021 untersagte das VG Wiesbaden den Einsatz des Cookiebot auf der betroffenen Website vorläufig, da mit der Darstellung des Cookiebot die Übermittlung der IP-Adresse des Websitebesuchers in die USA einherging. Wir haben darüber in unserem letzten Newsletter in 2021 berichtet (hier). Ein kleines Erdbeben für viele Unternehmen.

Der VGH Hessen hat diese Entscheidung nun revidiert: Der Cookiebot darf vorläufig weiter im Einsatz bleiben, erst das Hauptsacheverfahren wird hier mehr Klarheit schaffen (Beschluss vom 17.01.2021, Az. 10 B 2486/21). Zu den datenschutzrechtlich brisanten Themen hat sich das Gericht indes nicht geäußert. Die Entscheidung des VG Wiesbaden wurde aufgehoben, weil es am Anordnungsgrund, also der Eilbedürftigkeit fehlte.

Die Übermittlung der IP-Adresse an einen Diensteanbieter war auch in einer anderen Entscheidung der springende Punkt: Das LG München sprach einem Websitebesucher einen Schadensersatzanspruch i.H.v. 100 Euro gegen den Betreiber der Seite zu, weil dieser Google Fonts eingesetzt hatte und für die Darstellung der entsprechenden Schriftarten eine Verbindung zu Google aufgebaut wurde. Für die damit einhergehende Übermittlung der IP-Adresse der Websitebesucher sah das Gericht keine Erlaubnisgrundlage: Überwiegende berechtigte Interessen bestünden schon deshalb nicht, weil der Websitebetreiber die Google Fonts-Library auch lokal hätte einbinden können (Urteil vom 20.01.2022, Az. 3 O 17493/20). Die Sprengkraft dieser Entscheidung ist enorm, sie könnte Grundlage für Massenverfahren werden, da ein entsprechender Schadensersatzanspruch dann jedem Websitebesucher zustände, sodass sich der Gesamtschaden für Unternehmen schnell potenzieren kann.

Mehr dazu finden Sie hier: https://digitalisierungsrecht.eu/erste-gerichtsentscheidung-zum-drittstaatentransfer-online-tools-vor-dem-aus/



Schadensersatz nach DSGVO-Verstoß: Klagen bringen auch mehr Rechtssicherheit

Betroffene können im Fall eines DSGVO-Verstoßes zivilrechtlichen Schadensersatz verlangen. Darauf gerichtete Gerichtsverfahren nehmen zu. Eine einheitliche Linie zu den Voraussetzungen einer Haftung kann den gerichtlichen Entscheidungen bislang indes nicht entnommen werden. Dies könnte sich in Zukunft ändern: Aktuell liegen einige Verfahren beim EuGH zur Vorabentscheidung, zu anderen Fragen lassen sich Tendenzen aus den aktuellen Entscheidungen ersehen. Die aus unserer Sicht wichtigsten Aspekte der jüngsten Gerichtsentscheidungen haben wir für Sie zusammengefasst.

Keine Beweislastumkehr für den Datenschutzverstoß und den Schaden

Für Schadensersatzansprüche dürfte in einer Sache weitgehend Einigkeit unter den Gerichten bestehen: Die Betroffenen tragen die Beweislast für das Vorliegen sämtlicher Anspruchsvoraussetzungen – mit Ausnahme des Verschuldens.

Daraus folgt, dass die Betroffene auch einen Datenschutzverstoß erst einmal darzulegen und im Zweifel zu beweisen haben, bevor

Unternehmen Schadensersatz leisten müssen. Das LG München hatte jüngst der klägerischen Argumentation eine Absage erteilt, aus einer durch die DSGVO begründete allgemeine Rechenschaftspflicht (Art 5 Abs. 2 DSGVO) folge stets eine Beweislastumkehr für einen Verstoß gegen datenschutzrechtliche Vorschriften (Urteil vom 09.12.2021, Az. 31 O 16606/20). Die datenschutzrechtlichen Rechenschaftspflichten gelten nur im Verhältnis zu einer Aufsichtsbehörde. Betroffene können sich darauf nicht berufen.

Anders als von den Klägern häufig argumentiert, tragen die Betroffenen auch die Beweislast für das Vorliegen eines Schadens (OLG Brandenburg, Beschluss vom 11.08.2021, Az. 1 U 69/20). Auch diesbezüglich sei eine Beweislastumkehr zulasten der verantwortlichen Unternehmen abzulehnen, wobei in der Praxis Schadenspositionen sicherlich in vielen Fällen geschätzt werden können.

Nachweis der fehlenden „Verantwortlichkeit"?

Das OLG Brandenburg hat zudem bestätigt, dass der Anspruchsgegner „nur" die fehlende sog. Verantwortlichkeit für den entstandenen Schaden nachzuweisen hat, um einer Haftung zu entgehen.

Konkret stand dazu das LG Saarbrücken zum Jahresende vor der Frage, welche Anforderungen an den Nachweis der fehlenden Verantwortlichkeit durch das Unternehmen zu stellen sind. Die maßgebende DSGVO-Vorschrift fordert hier ausdrücklich, dass der Anspruchsgegner in *keinerlei Hinsicht* für den Umstand, der zum Schaden geführt hat, verantwortlich sein darf. Das Gericht weist darauf hin, dass die gesetzliche Formulierung keinen Hinweis auf die Darlegungslast des Verantwortlichen gibt (Beschluss vom 22.11.2021, Az. 5 O 151/19).

Fraglich ist in diesem Kontext, ob bereits die Berufung auf ein weisungswidriges Verhalten eines Mitarbeiters die Verantwortlichkeit entfallen lässt. Das LG Saarbrücken hat diese Frage dem EuGH vorgelegt. Sollte der Verweis auf ein Fehlverhalten des Angestellten der Nachweispflicht Genüge tun, ergäbe sich hieraus eine erhebliche Einschränkung der Schadensersatzpflicht für Verantwortliche.

***Ungutes Gefühl* als Schaden?**

Die Darlegung eines (immateriellen) Schadens dürfte die größte Hürde aus Sicht der Betroffenen darstellen.

Erste Entscheidungen haben die Geltendmachung von sogenannten *Bagatellschäden* ausgeschlossen, andere Gerichte stellen bisweilen nur sehr geringe Anforderungen und fordern keine Erheblichkeit des Schadens. So ließ das AG Pfaffenhofen kürzlich bereits das *ungute Gefühl* genügen, dass personenbezogene Daten Unbefugten bekannt geworden sind (Urteil vom 09.09.2021, Az. 2 C 133/21). Zugegeben: Die Höhe des zugesprochenen Schadensersatzanspruchs von 300 Euro erscheint auf den ersten Blick überschaubar. Soweit eine Datenpanne aber bei vielen Personen nur ein ungutes Gefühl auslöst, drohen Haftungsrisiken in empfindlicher Höhe.

Die unterschiedlichen Anforderungen an den Schaden haben ihren Ursprung im nationalen Recht. Hiernach setzt ein Anspruch auf Geldentschädigung wegen der Verletzung des Persönlichkeitsrechts nämlich stets voraus, dass es sich um einen schwerwiegenden Eingriff handelt. Ob das Erreichen einer Erheblichkeitsschwelle auch für den europäischen Schadensersatzanspruch aus Art. 82 DSGVO gefordert werden kann, wird der EuGH entscheiden. Mittlerweile haben eine Vielzahl von Gerichten diese Vorlagefrage nach Luxemburg übersandt, auch das BVerfG (wir berichteten hier).

Zurechnung von Fehlverhalten nur durch Leitungspersonal?

Im Zusammenhang mit behördlichen Bußgeldern nach Art. 83 DSGVO liegt nun eine weitere für Unternehmen wichtige Frage beim EuGH: Sind Bußgelder an Leitungspersonen oder das Unternehmen als solches zu richten (wir berichteten dazu hier)? Diese Frage liegt nun beim EuGH (Vorlage des KG Berlin, Beschluss vom 06.12.2021, Az. 3 Ws 250/21). Die Beantwortung durch den EuGH muss daher mit Spannung erwartet werden, hat sie doch ganz erhebliche Auswirkungen auf die unternehmensinterne Compliance.

Auskunftsrechte: Neue Leitlinien und viel Arbeit für Unternehmen

Der Europäische Datenschutzausschuss (EDSA) hat am 28.01.2022 Leitlinien zum Auskunftsrecht veröffentlicht. Das Betroffenenrecht auf Auskunft ist in der Praxis wohl das meist genutzte Instrument aus dem Betroffenen zur Verfügung stehenden Werkzeugkoffer der DSGVO (teils auch zur Verfolgung sachfremder Ziele bzw. rechtsmissbräuchlichen Schikanen). Unternehmen müssen zur Erfüllung von Auskunftsrechten teils ganz erhebliche Ressourcen aufwenden, vor allem bei der Bereitstellung von Datenkopien. Umfang und etwaige Grenzen werden denn auch intensiv diskutiert. Die neuen EDSA-Leitlinien zeigen sich hier extensiv: Das Auskunftsrecht ist umfassend. Unternehmen müssen sich weiterhin auf einen ganz erheblichen Aufwand einstellen. Wir haben die wichtigsten Aspekte zusammengefasst.

Die Leitlinien des Europäischen Datenschutzausschuss (EDSA) thematisieren das Recht auf Auskunft gemäß Art. 15 DSGVO. Ziel des Auskunftsrechts ist es, dem Betroffenen ausreichende, transparente und leicht zugängliche Informationen über die Verarbeitung seiner personenbezogenen Daten zur Verfügung zu stellen. Er soll damit die Rechtmäßigkeit der Verarbeitung und die Richtigkeit der verarbeiteten Daten erkennen und überprüfen können. Da Art. 15 DSGVO das Recht auf Auskunft abstrakt formuliert und Raum für Auslegung und Interpretation lässt,

werden seit Verabschiedung der DSGVO der Umfang und etwaige Grenzen intensiv diskutiert.

Insgesamt vertritt der EDSA nun erwartungsgemäß eine strenge Auslegung zugunsten der Betroffenen. Der Auskunftsanspruch sei weit auszulegen, wodurch nur wenige Fälle verbleiben, in denen Auskunftsersuchen verweigert oder inhaltlich begrenzt werden können.

Schritt 1: Interpretation und Bewertung des Auskunftsersuchens

Betroffene können sich formlos und ohne Angabe von Gründen an den für die Verarbeitung Verantwortlichen wenden und von ihm Auskunft über ihre bei ihm verarbeiteten personenbezogenen Daten verlangen. Nur Anfragen, die an völlig willkürliche und offensichtlich unrichtige Adressen gesendet werden, können unbeachtet bleiben.

Anwendungsbereich des Art. 15 DSGVO

Erreicht den Verantwortlichen ein Auskunftsersuchen muss er zunächst prüfen,

- ob sich das Auskunftsersuchen auf personenbezogene Daten bezieht und

- ob sich es sich bei der Anfrage um ein Auskunftsersuchen i.S.d. Art. 15 DSGVO handelt und sich nicht auf eine andere (speziellere) rechtliche Grundlage (z.B. Zugang zu öffentlichen Dokumenten) oder ein anderes Betroffenenrecht bezieht.

Identifikation des Betroffenen

Der Verantwortliche muss sodann sicherstellen, dass nur dem Berechtigten Daten zur Verfügung gestellt werden. Hat der Verantwortliche Zweifel daran, dass die auskunftsersuchende Person diejenige ist, die sie vorgibt zu sein, muss er zusätzliche Informationen anfordern, um die Identität dieser zu bestätigen. Hat ein Dritter einen Antrag auf Auskunft über personenbezogene Daten gestellt, darf der Verantwortliche, dem Dritten die personenbezogenen Daten nur zur Verfügung stellen, wenn er die Berechtigung des Dritten überprüft hat. In der Praxis sollten keine Informationen an unbekannte E-Mail-Adresse übermittelt werden,

auch telefonisch sollten Auskunftsersuchen regelmäßig nicht beantwortet werden.

Gegenstand des Auskunftsersuchens

Der Verantwortliche muss den Inhalt des Auskunftsersuchens prüfen. Ist er aufgrund eines ungenau formulierten Antrags nicht in der Lage, die personenbezogenen Daten zu ermitteln, muss er den Betroffenen um zusätzliche Informationen bitten. Stellt der Betroffene die angeforderten Informationen nicht zur Verfügung, kann der Verantwortliche die Auskunft verweigern.

Im Zweifel bezieht sich ein Antrag auf alle personenbezogenen Daten des Betroffenen, die beim Verantwortlichen verarbeitet werden. Der Verantwortliche kann den Betroffenen zwar dazu auffordern, sein Auskunftsersuchen zu präzisieren, wenn eine große Menge an Daten verarbeitet wird. Verpflichtet ist der Betroffene dazu aber nicht.

Schritt 2: Beantwortung des Auskunftsersuchens

Bei der Beantwortung des Auskunftsersuchens muss der Verantwortliche

- bestätigten, ob personenbezogene Daten über die betroffene Person verarbeitet werden oder nicht,
- Zugang zu diesen Daten gewähren und
- zusätzliche Informationen über die Verarbeitung, wie den Zweck, die Datenkategorien und Empfänger, Dauer der Verarbeitung, Rechte der betroffenen Personen, ggf. die Herkunft der Daten (Art. 15 Abs. 1 lit. a – h DSGVO) und angemessene Garantien im Falle von Übermittlungen in Drittländer (Art. 15 Abs. 2 DSGVO) bereitstellen.

Der Verantwortliche muss dem Auskunftsersuchenden alle personenbezogenen Daten zugänglich machen, die sich auf seine Person beziehen (Punkt 2) und Gegenstand des Auskunftsersuchens sind (siehe Schritt 1). Nach Ansicht des EDSA sind neben Daten, die nur die betroffene Person selbst betreffen, auch Daten bereitzustellen, die (auch) andere Personen betreffen (z.B. Chatverläufe). Hinsichtlich der zusätzlichen Informationen (Punkt 3) kann der Verantwortliche grundsätzlich auf die Informationen zurückgreifen, die er im Verarbeitungsverzeichnis

(Art. 30 DSGVO) festgehalten hat und in den allgemeinen Datenschutzhinweisen (Art. 13, 14 DSGVO) zur Verfügung stellt. Ggf. müssen diese Informationen jedoch für den konkreten Fall aktualisiert oder angepasst werden; dies ist stets zu überprüfen.

Ermittlung der personenbezogenen Daten

Der Verantwortliche muss die von ihm verarbeiteten personenbezogenen Daten des Betroffenen in allen IT- und Nicht-IT-Systemen suchen, die er zur Ablage von Daten nutzt. Zu verwenden sind dabei geeignete Suchkriterien, die auf den vom Betroffenen bereitgestellten Informationen beruhen und berücksichtigen, wie die Daten in den Systemen strukturiert sind (z.B. auch: Kundennummer, IP-Adresse, Berufsbezeichnung, Familienverhältnisse etc.).

Der Auskunftsanspruch erfasst auch unrichtige Daten sowie möglicherweise unrechtmäßig verarbeitete Daten. Lediglich Daten, die nicht mehr beim Verantwortlichen vorhanden sind, weil sie etwa aufgrund einer Aufbewahrungsregel gelöscht wurden, sind nicht zur Verfügung zu stellen.

Art und Weise der Bereitstellung

Die Auskunft muss in präziser, transparenter, verständlicher und leichter Form unter Verwendung einer klaren und verständlichen Sprache erfolgen (Art. 12 Abs. 1 DSGVO).

Der Verantwortliche muss die Daten dem Betroffenen zudem auch als Kopie bereitstellen (Art. 15 Abs. 3 DSGVO). Das bereitet ob des Umfangs vorhandener Daten in der Regel die größten Schwierigkeiten.

Eine zusammenfassende Darstellung, die dazu führt, dass nicht mehr alle Daten enthalten sind oder Inhalte verändert werden, ist nicht ausreichend. Nur wenn der Betroffene eine andere Art der Bereitstellung wünscht, etwa Zugang vor Ort oder mündliche Übermittlung, kann von der Bereitstellung einer Kopie abgesehen werden.

Zeitraum, innerhalb dem Auskunft zu erteilen ist

Der Antrag muss unverzüglich bearbeitet und beantwortet werden; in jedem Fall ist der Antrag innerhalb eines Monats nach Eingang zu

beantworten (Art. 12 Abs. 1 S. 1 DSGVO). Nur ausnahmsweise kommt eine Verlängerung der Frist um zwei Monate in Betracht.

Schritt 3: Prüfung von Beschränkungen des Auskunftsersuchens

Der EDSA stellt klar, dass der Verantwortliche die Auskunft nicht allgemein mit der Begründung verweigern darf, dass die Auskunft für ihn mit einem **unverhältnismäßigen Aufwand** verbunden ist. Die DSGVO begrenzt den Auskunftsanspruch nur in folgenden Punkten:

- **Keine Beeinträchtigung der Rechte und Freiheiten anderer Personen:** Das Recht auf Erhalt einer Kopie der personenbezogenen Daten ist durch die Rechte und Freiheiten anderer Personen beschränkt. Nach Ansicht des EDSA ist diese Bestimmung weit auszulegen: Rechte und Freiheiten anderer Personen dürfen nicht beeinträchtigt werden. Dem ist durch Schwärzungen Rechnung zu tragen. Der Verantwortliche darf das Ersuchen regelmäßig nicht vollständig ablehnen.

- **Offensichtlich unbegründete und exzessive Anträge:** Bei offensichtlich unbegründeten und exzessiven Anträgen des Betroffenen kann der Verantwortliche Anträge ablehnen oder ein angemessenes Entgelt verlangen. Diese Beschränkung des Auskunftsanspruchs ist nach Ansicht des EDSA eng auszulegen. Aufgrund der geringen Anforderungen an ein Auskunftsersuchen könne nur in den seltensten Fällen von einem offensichtlich unbegründeten Antrag ausgegangen werden. Ob die Häufigkeit der Anträge des Betroffenen als exzessiv einzustufen ist, richte sich nach der Unternehmensbranche in der der Verantwortlich tätig ist: Je häufiger Datenbanken geändert werden, desto häufiger kann ein Betroffener auch Auskunft verlangen, ohne dass dies als übertrieben zu bewerten ist. Denkbar ist auch eine Beschränkung des Auskunftsrechts im Hinblick auf missbräuchliche Anträge, die allein darauf ausgerichtet sind, dem Verantwortlichen zu schaden.

Umgang mit den Leitlinien

Leitlinien des EDSA sind nicht rechtsverbindlich. Sie markieren indes die Position der Datenschutzaufsichtsbehörden. Werden die

Leitlinien eingehalten, ist ein aufsichtsbehördliches Verfahren unwahrscheinlich.

Die Leitlinien bieten denn auch praktische Hilfestellungen, so u.a. ein Flussdiagramm für die Strukturierung der Abläufe im Fall eines Auskunftsersuchens.

Was sollten Unternehmen tun?

Unternehmen sollten Prozessvorgaben implementieren, wie Auskunftsersuchen zu bearbeiten sind. Die jetzt veröffentlichten Leitlinien des EDSA bieten hierfür eine gute Hilfestellung. Klar definierte Prozesse sowie Textvorlagen für verschiedene Situationen ermöglichen die effiziente Bearbeitung.

Zudem sollten die EDSA-Leitlinien „auf Abruf" liegen, wenn ein Auskunftsersuchen zu umfangreich, zweckfremd oder missbräuchlich erscheint. In diesen Fällen lohnt eine vertiefte Prüfung, wie mit diesem umgegangen wird. Gleichzeitig sollen allen Anfragen von Betroffenen im Einzelfall geprüft und bewertet werden auch um die Motivlage und den Gesamtkontext zu berücksichtigen.

Drittstaatentransfer: Helfen neue Gutachten in der Praxis?

Ein für Unternehmen immer noch leidiger Dauerbrenner: Um das Datenschutzrisiko beim Datentransfer in Länder außerhalb des EWR zu minimieren, muss bei der Verwendung der Standardvertragsklauseln (SCC) im Einzelfall die Rechtslage im Zielland geprüft werden: Erlaubt das nationale Recht dem Datenimporteur, die Vertragsregeln einzuhalten? Oder bestehen nationale Rechtsvorschriften, die dies ausschließen? Diese notwendige Prüfung und Risikobewertung ist in der Praxis komplex. Die Aufsichtsbehörden haben nun Gutachten veröffentlicht, um die Praxis zu entlasten – sie geben Hinweise zu den USA, China, Indien und Russland.

Seit der EuGH-Entscheidung in Sachen Schrems-II im Juli 2020 besteht in der EU und dem EWR Rechtsunsicherheit, ob und inwiefern personenbezogene Daten datenschutzkonform in Drittstaaten übermittelt werden können. Gerade auf US-Dienstleister können viele Unternehmen nicht verzichten, da alternative EU-Lösungen nicht in der gleichen Praktikabilität flächendeckend verfügbar sind.

Wer Daten in Drittstaaten übermitteln will, muss die nationale Rechtslage im Rahmen eines sog. **Data Transfer Impact Assessment** prüfen: Wie kann ein angemessenes Datenschutzniveau im Zielland gewährleistet werden? Dies umfasst auch die Prüfung, ob nationales Recht mit dem EU-Recht unvereinbare Behördenzugriffe zulässt.

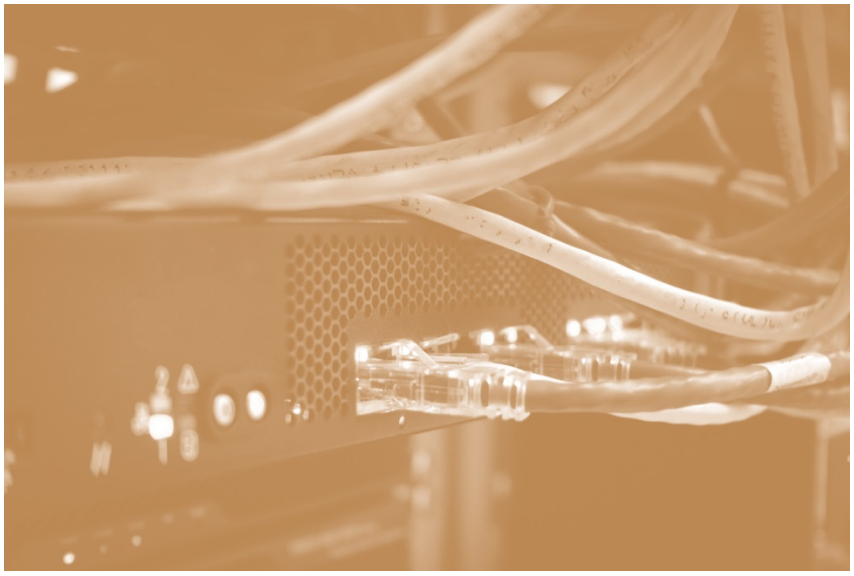
Diese Prüfung stellt die Praxis in den Fällen vor erhebliche Herausforderungen, in denen die Kommission keinen Angemessenheitsbeschluss erlassen hat.

Die von den Datenschutzaufsichtsbehörden in Auftrag gegebenen Rechtsgutachten, die nun veröffentlicht wurden, können hier den Unternehmen als Hilfe dienen:

- **USA**: Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) veröffentlichte am 25.01.2022 ein externes Rechtsgutachten vom 15.11.2021, das den aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse aufbereitet (Originalversion in Englisch, übersetzter Volltext als unverbindliche Arbeitshilfe in Deutsch sowie eine Zusammenfassung der wesentlichen Befunde). Der beauftragte Gutachter, Prof. Stephen I. Vladeck, war bereits

einer der Sachverständigen für Facebook im Rahmen des irischen Gerichtsverfahrens, das im *Schrems-II*-Urteil mündete. Vor diesem Hintergrund nimmt das veröffentlichte Gutachten an verschiedenen Stellen auf die Ausführungen seines Expertenberichts in diesem Fall Bezug.

- **China, Indien und Russland**: Das vom Europäischen Datenschutzausschuss (EDSA) in Auftrag gegeben Expertengutachten, das am 08.11.2021 auf der Website des EDSA veröffentlicht wurde, befasst sich ebenfalls mit der Rechtslage und der Behördenpraxis in Bezug auf den Schutz personenbezogener Daten in Drittstaaten, namentlich China, Indien und Russland.



Zu guter Letzt

Auch in diesem Monat wurden wieder einige Bußgelder aufgrund von Verstößen gegen die Datensicherheit verhängt, u.a. i.H.v. 150 Mio. Euro gegen Google. Hoch praxisrelevant ist zudem ein Verfahren rund um die Verantwortung einer Muttergesellschaft für den Datenschutz durch ihre Tochtergesellschaft.

- **Frankreich**: **150 Mio. Euro für Google und 60 Mio. Euro für Facebook/Meta**

Auf den Websites facebook.com, google.fr und youtube.com war es dem Nutzer möglich, durch einen einzigen Klick die Nutzung von Cookies zu akzeptieren. Gleichzeitig wurde keine Schaltfläche angeboten, die eine gleichwertige Lösung zum Ablehnen der Cookies durch den Internetnutzer ermöglicht hätte. Hierzu waren mehrere Klicks durch den Nutzer der Website notwendig. Dies stellte die französische Datenschutzbehörde nach Untersuchungen fest und sah die Freiheit der Zustimmung durch diese Gestaltung beeinträchtigt. Durch die zusätzlichen Hürden für die Ablehnung von Cookies wurde der Nutzer in seiner Entscheidung zugunsten einer Zustimmung beeinflusst. Dies stellt einen Verstoß gegen Art. 82 des französischen Datenschutzgesetzes dar. Die französische Datenschutzbehörde CNIL verhängte deshalb eine Geldstrafe von 150 Millionen Euro gegen Google, sowie ein Bußgeld in Höhe von 60 Mio. Euro gegen Facebook (nunmehr „Meta“).

Der Ausschuss wies die Unternehmen zusätzlich an, den Internetnutzern innerhalb von drei Monaten ein ebenso einfaches Mittel zur Ablehnung von Cookies zur Verfügung bereitzustellen wie zur Annahme von Cookies, um so die freie Zustimmung zu gewährleisten. Andernfalls müssten die Unternehmen eine Strafe von 100.000 Euro pro Verzugstag zahlen.

- **Finnland**: **Reinigungsunternehmen übermittelt vertrauliche Daten über WhatsApp**

Ein finnisches Reinigungsunternehmen verstieß gegen die DSGVO, indem es WhatsApp nutzte, um seinen Mitarbeitern Informationen über Kunden, einschließlich deren Namen, Adressen, Türcodes oder Schlüsselkastencodes, mitzuteilen. Dem verantwortlichen Unternehmen war es unmöglich, die Nutzung personenbezogener

Daten durch WhatsApp zu überwachen oder anderweitig Beschränkungen für eine mögliche weitere Nutzung festzulegen.

Das Unternehmen teilte der finnischen Datenschutzbehörde gegenüber mit, dass es WhatsApp-Nachrichten von nun an ausschließlich zur Übermittlung von Standortinformationen verwenden würde. Sensiblere Informationen, wie z. B. Türcodes, sollen ausschließlich mündlich an die Mitarbeiter weitergegeben werden und alle ehemaligen Mitarbeiter wurden zur Löschung der früheren Mitteilungen mit personenbezogenen Daten angewiesen. Die finnische Datenschutzbehörde bemängelte jedoch, dass nicht überprüfbar sei, ob und wann die ehemaligen Mitarbeiter dieser Anweisung tatsächlich nachgekommen sind und ob alle Sicherungskopien dieser Daten ebenfalls gelöscht wurden.

Die finnische Datenschutzbehörde erkannte in der Nutzung von WhatsApp durch das Unternehmen einen Verstoß gegen Artikel 5, 25 und 32 DSGVO. Das Unternehmen wurde angewiesen, seine Datenverarbeitungspraktiken mit den Vorgaben der DSGVO in Einklang zu bringen. Es wurde kein Bußgeld verhängt.

- **Finnland: Über 600.000 EUR Bußgeld für Psychotherapiepraxis nach Angriff auf schlecht gesicherte Patientendaten**

Eine Psychotherapiepraxis wurde 2018 und 2019 mindestens zweimal erfolgreich von Hackern angegriffen. Dabei wurde die Patientendatenbank der Praxis kopiert. Sowohl das Unternehmen als auch die Patienten wurden später von den Angreifern erpresst.

Die finnische Datenschutzbehörde stellte fest, dass das Unternehmen die Datenschutzverletzungen nicht rechtzeitig gemeldet hatte und dass die Praxis keine geeigneten Sicherheitsmaßnahmen ergriffen hatte, um die Integrität und Vertraulichkeit der personenbezogenen Daten zu gewährleisten. Zudem sei die in Art. 5 II DSGVO verankerte Rechenschaftspflicht nicht eingehalten worden, da es der Praxis nicht möglich war, nachzuweisen, dass die Grundprinzipien der DSGVO eingehalten wurden. Die finnische Datenschutzbehörde verhängte insgesamt eine Geldbuße in Höhe von 608.000 EUR.

- **Italien: 26,5 Millionen Euro Geldbuße für den italienischen Energiekonzern Enel Energia**

Der italienische Energieversorger Enel Energia hat hartnäckig Nutzer und potenzielle Kunden, die teilweise Maßnahmen zur Verkaufsförderung widersprochen hatten, für Verkaufszwecke angesprochen. Zum Großteil der angerufenen Personen bestand zuvor kein geschäftlicher Kontakt. Zudem wurde auf Auskunftsverlangen und auf Widersprüche von Kunden gegen die Verarbeitung ihrer Daten zu Marketingzwecken verspätet oder gar nicht reagiert. Aufmerksam wurde die italienischen Datenschutzbehörde („Garante"), weil daraufhin hunderte von Beschwerden gegen Enel Energia bei ihr eingingen.

Enel Energia hat gegenüber der Datenschutzbehörde erklärt, dass die unerwünschten Anrufe von außerhalb des Unternehmens und von Geschäftspartnern seines Netzwerks stammten. Die Behörde stellte jedoch fest, dass der Energieversorger nicht über spezifische technische und organisatorische Maßnahmen zur Bekämpfung solcher Vorkommnisse verfüge und verhängte daher ein Bußgeld i.H.v. 26,5 Millionen EUR.

- **Österreich: Datenschutz der Tochtergesellschaft ist Aufgabe der Muttergesellschaft**

Eltern haften für ihre Kinder – so sieht es zumindest die österreichische Datenschutzbehörde (DSB). Dies sei selbst dann der Fall, wenn die Tochtergesellschaft völlig eigenständig arbeite.

Der Lebensmitteleinzelhändler REWE International wurde aufgrund dieser Auffassung zu einer Geldstrafe in Höhe von 8 Millionen EUR verurteilt. Grund dafür war, dass das Kundenbindungs- und Prämienprogramm „jö Bonus Club" Daten von Nutzern ohne deren Zustimmung gesammelt und für Marketingzwecke verwendet hatte. REWE will gegen diese Entscheidung vorgehen, da es der Meinung ist, dass der jö Bonus Club als eigenständige Tochtergesellschaft unabhängig agiere und daher die Geldstrafe hätte erhalten müssen. Zudem habe die Tochtergesellschaft jö keine Kundendaten an die Muttergesellschaft weitergegeben, was aus Sicht von REWE gegen eine Haftbarkeit wegen des Missbrauchs von Kundendaten spricht.

Sofern die Angaben von REWE zutreffen, dürften gute Aussichten auf eine Aufhebung des Bußgeldbescheids bestehen.

Bußgeldbescheide ergehen grundsätzlich gegen den für die Datenverarbeitung Verantwortlichen. Besonders geholfen ist REWE damit allerdings nicht, da zwar gegebenenfalls der jö Bonus Club selbst Adressat des Bußgeldbescheids sein müsste, die Bemessung des Bußgelds aber anhand der Konzernumsätze erfolgt, so dass auch die Umsätze der Mutter herangezogen werden können.

- **Krefeld: Klagezurückweisung wegen fehlendem Interesse am Datenschutz der betroffenen Person**

Das Landgericht Krefeld hat den Antrag einer betroffenen Person auf Auskunft über die von der Krankenversicherung der Person verarbeiteten Daten abgelehnt, da der ein Interesse außerhalb des Datenschutzes verfolge. Die betroffene Person schloss 1976 bei der Beklagten einen Vertrag über eine private Krankenversicherung ab. Während der Vertragslaufzeit erhöhte das Unternehmen wiederholt die Prämien, worüber die betroffene Person informiert wurde. Diese zahlte die erhöhten Prämien zunächst vorbehaltlos, vermutete dann aber später die Unrechtmäßigkeit der Prämienanpassungen. Um eine Prämienrückerstattung zu erwirken, machte sie ein Auskunftsersuchen nach Art 15 DSGVO geltend.

Das Gericht war der Auffassung, dass diese Absicht so weit von dem Auskunftsrecht nach der DSGVO entfernt ist, dass sie nicht schutzwürdig sei und gegen Treu und Glauben verstoße. Zudem betonte das Gericht, dass die betroffene Person die Dokumente mit den angeforderten Informationen unbestritten schon einmal erhalten habe und erst jetzt nicht mehr über sie verfüge.

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