LOSCHELDER

Newsletter Datenschutzrecht

März 2021

Sehr geehrte Damen und Herren,

Sie haben sicherlich gelesen, dass Mitte März Teile eines Rechenzentrums des größten europäischen Cloud-Service-Anbieters OVH abgebrannt sind. Dieser ganz physische Datenverlust dürfte für viele betroffene Unternehmen zu enormen Schäden führen. Achten Sie einmal bei Durchsicht des nächsten AV-Vertrages darauf, ob der Feuerschutz bei den TOM erwähnt ist.

Ansonsten haben wir eine Zeit der sehr praxisrelevanten Gerichtsentscheidungen: Ein weiteres hohes DSGVO-Bußgeld hatte vor Gericht keinen Bestand, das Bundesverfassungsgericht entschied zu Schadensersatz bei Bagatelldatenschutzverstößen, Google will Cookies verbannen und ein Oberverwaltungsgericht bestätigte die Relevanz des UWG für die DSGVO-Auslegung. Viel Stoff für unseren März-Newsletter, ergänzt um erstaunliche Schlaglichter in unserer Rubrik „Zu guter Letzt“ (etwa neue Aktionen der Datenschutzkonferenz in Sachen „US-Transfer“ nach Schrems II). Wir freuen uns über Ihr Interesse und wünschen viel Spaß beim Lesen!

Auch würden wir uns freuen, Sie zu unserem Lunch@Loschelder-Webinar zum **neuen digitalen Vertragsrecht am 14.04.2021 (12 Uhr)** begrüßen zu dürfen – weitere Informationen dazu finden Sie unter https://loschelder.de/de/webinare.html, melden Sie sich gerne (kostenfrei) an unter webinare@loschelder.de.

Inhalt

DSGVO-Bußgelder auf dem Prüfstand: LG Berlin kippt Millionenbußgeld gegen Deutsche Wohnen

Gegen die Deutsche Wohnen SE wurde im Oktober 2019 ein Bußgeldbescheid über 14,5 Millionen Euro erlassen. Das LG Berlin hob den Bescheid nunmehr mit Beschluss vom 18. Februar 2021 vollständig auf und stellte das Verfahren ein. In dem Beschluss heißt es wörtlich: „Der Bußgeldbescheid der Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 30. Oktober 2019 leidet unter derart gravierenden Mängeln, dass er nicht Grundlage des Verfahrens sein kann." Was dahintersteckt, fassen wir in unserem aktuellen Newsletter zusammen.

Der Bußgeldbescheid, der dem Verfahren vor dem LG Berlin zugrunde lag, wurde von der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BInBDI) erlassen. Der Vorwurf: Die Deutsche Wohnen SE habe jahrelang personenbezogene Mieterdaten in einem Archivsystem gespeichert, das keine Möglichkeit zur Löschung nicht (mehr) erforderlicher personenbezogener Daten vorsah. Nach der Berichterstattung handelte es sich bei den unrechtmäßig gespeicherten Daten z.B. um Gehaltsbescheinigungen, Selbstauskunftsformulare, Auszüge aus Arbeits- und Ausbildungsverträgen, Steuer-, Sozial- und Krankenversicherungsdaten sowie Kontoauszüge.

Die Deutsche Wohnen SE legte Einspruch gegen den Bußgeldbescheid ein. Das LG Berlin stellte das Bußgeldverfahren daraufhin mit Beschluss vom 18.02.2021 ohne Hauptverhandlung ein (Az.: (526 OWi LG) 2021 Js-OWi 1/20 (1/20)) und führte zur Begründung u.a. aus: *„Der Bußgeldbescheid der Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 30. Oktober 2019 leidet unter derart gravierenden Mängeln, dass er nicht Grundlage des Verfahrens sein kann."*

Diese gravierenden Mängel sah das LG Berlin in zwei Umständen: Das Bußgeld könne nicht in der von der BlnBDI gewählten Form gegen eine juristische Person verhängt werden, zudem fehle die Angabe des konkreten Schuldvorwurfs. Während der erste Vorwurf so eindeutig nicht durchgreift – die Frage ist höchst umstritten –, ist der zweite Aspekt erstaunlich, auch mit Blick auf die über mehrere Jahre hinweg geführten Ermittlungen.

Bußgelder gegen juristische Personen?

Das LG Berlin hat den Bußgeldbescheid als rechtswidrig angesehen, weil er die Deutsche Wohnen SE als Betroffene des Verfahrens ausweist und ihr gegenüber das Bußgeld verhängt. Das Gericht steht auf dem Standpunkt, dass Bußgelder gegen Unternehmen nur verhängt werden können, wenn Leitungspersonen oder gesetzlichen Vertretern/-innen eine konkrete Handlung nachgewiesen werden kann, die den Bußgeldtatbestand verwirklicht. Daher hätte ein Vertreter/ein Organ als Betroffener im Bußgeldbescheid genannt werden müssen. Diese Sichtweise entspricht dem althergebrachten Schuldprinzip des deutschen Ordnungswidrigkeitenrechts (§ 30 Abs. 1 OWiG). Umstritten ist aber, ob dieses nationale Schuldprinzip auch auf Bußgelder nach der europäischen DSGVO Anwendung findet.

Dagegen spricht, dass Art. 83 Abs. 4-6 DSGVO ausdrücklich Geldbußen „gegen Unternehmen" vorsieht. Der Wortlaut der Normen sieht keine Einschränkungen vor, nach denen für die Verhängung einer Geldbuße die schuldhafte Handlung eines Vertreters/Organs erforderlich wäre. Im Grundsatz haften die Unternehmen also nach Art. 83 Abs. 4-6 DSGVO für jeden Verstoß, der in ihrem Verantwortungsbereich begangen wurde. Bisher wurde indes noch nicht höchstrichterlich oder vor EU-Gerichten geklärt, ob die DSGVO hier den deutschen Vorschriften vorgeht. Die deutschen Datenschutzbehörden (vgl. Entschließung der Datenschutzkonferenz vom 03.04.2019) und das LG Bonn, Urteil vom 11.11.2020, Az. 29 OWi 1/20 – „1&1", sind von einer solchen Überlagerung ausgegangen. Dagegen hat sich jetzt das LG Berlin positioniert. Es erscheint gut möglich, dass diese Frage letztlich vom EuGH zu entscheiden sein wird.

Für die Praxis hat das Thema enorme Relevanz – im Kern steht zunächst in Rede, ob Organe und Leitungspersonen unmittelbar persönlich wegen DSGVO-Verstößen in Anspruch genommen werden, oder aber ausschließlich die dahinterstehende juristische Person. Auch für die Organisation der internen Compliance und Risikoprävention ist entscheidend, ob maßgeblich auf das schuldhafte Fehlverhalten einer Leistungsperson im Unternehmen angeknüpft werden muss. Denn durch eine sachgerechte Risikoverteilung und ein funktionierendes Compliance Management System kann dem wirksam begegnet werden, vor allem beim Fehlverhalten einzelner Mitarbeiter auf Arbeitsebene.

Weitere Mängel

Das LG Berlin hat noch auf weitere Mängel erkannt: Der Tatvorwurf sei nicht hinreichend bestimmt, es fehlten die „Angabe von Tatzeit und -ort sowie des Organmitglieds, das schuldhaft […] die Einrichtung eines den datenschutzrechtlichen Anforderungen genügenden EDV-Systems unterlassen […] haben soll". Inwiefern diese Mängel allein darauf beruhen, dass der BlnBDI von der Haftung des Unternehmens selbst ausgegangen ist, bleibt nach Lektüre des Beschlusses offen – konkrete Angaben jedenfalls sind von Behörden auch in Ordnungswidrigkeitenverfahren stets zum Nachweis des Vorwurfs anzuführen.

Folgen des Beschlusses

Sollte sich das LG Berlin mit seiner Auffassung durchsetzen, hätte das zur Folge, dass die Datenschutzbehörden – wie es die Kartellbehörden bei Kartellverstößen tun - bei ihren Ermittlungen auch Verantwortlichkeiten innerhalb der beschuldigten Unternehmen nachvollziehen und prüfen müssten. Nur, wenn sie dabei eine schuldhafte Handlung einer Leitungsperson nachweisen können, würde diese Person und das Unternehmen für einen Datenschutzverstoß haften. Da auch Aufsichtspflichtverletzungen und Unterlassungen haftungsbegründend sind, wird zwar in der Regel auch ein Organ oder gesetzlicher Vertreter für den Datenschutzverstoß verantwortlich sein, in jedem Fall zwingend ist das aber nicht. So könnte ein Unternehmen etwa nicht für die Taten eines schuldlos handelnden Organs/Vertreters verantwortlich gemacht werden.

Darüber hinaus führt die Auslegung des LG Berlin potentiell zu einer unterschiedlichen Anwendung der DSGVO in den verschiedenen Mitgliedstaaten. Wenn etwa nach deutschem Recht Unternehmen nur für Verstöße verantwortlich sind, die von ihren Vertretern/Organen begangen wurden, würde das zu einer anderen Anwendung der DSGVO in Deutschland als in anderen Staaten führen. Diese könnten wiederum andere Umstände zur Voraussetzung einer Haftung von Unternehmen machen.

Und jetzt?

Ob sich das LG Berlin mit seiner Auffassung durchsetzen kann, bleibt abzuwarten. Die Staatsanwaltschaft ist gegen den Beschluss mit der sofortigen Beschwerde vorgegangen, sodass das Kammergericht Berlin als Nächstes über den Fall zu entscheiden

hat. Für die Deutsche Wohnen SE ist schon der Beschluss des LG Berlin ein Zwischenerfolg. Selbst wenn das KG Berlin zu einem abweichenden Ergebnis kommen sollte, muss sie bis zum rechtskräftigen Abschluss des Verfahrens das beträchtliche Bußgeld nicht zahlen. Ob auch bei rechtskräftiger Aufhebung noch ein Bußgeld gegen ein Organ / eine Leitungsperson verhängt werden könnte, ist vertieft zu betrachten: Niemand darf für eine Tat zweimal bestraft werden, allerdings könnte es sich hier um zwei unterschiedlich Personen (Unternehmen vs. Organ) handeln.

Schadensersatz bei Bagatelldatenschutzverstößen?

Nur wenige Verfassungsbeschwerden werden vom Bundesverfassungsgericht auch tatsächlich zur Entscheidung angenommen. Dieser Fall hat es geschafft: Gibt es auch bei Bagatelldatenschutzverstößen einen Anspruch auf (immateriellen) Schadensersatz in Geld?

Ein Kläger hatte eine einzelne Werbeemail erhalten. Er war der Auffassung, dass die Verwendung seiner Daten zu Werbezwecken nicht rechtmäßig gewesen sei und verklagte deshalb den Versender der E-Mail vor dem Amtsgericht Goslar nicht nur auf Unterlassung, sondern auch auf Zahlung eines Schmerzensgelds von 500 Euro (Art. 82 Abs. 1 DSGVO). Das Amtsgericht wies die Klage ab: Für ein Schmerzensgeld wegen Persönlichkeitsrechtsverletzung sei eine schwerwiegende Beeinträchtigung erforderlich. Dafür könne bei

einer einzigen unrechtmäßigen Werbeemail nicht ausgegangen werden.

Entscheidung des AG Goslar

In der Sache hatte das AG Goslar die Frage unter Heranziehung der Grundsätze der BGH-Rechtsprechung für Entschädigungsansprüche aufgrund von Verletzungen des allgemeinen Persönlichkeitsrechts entschieden (dazu BGH, Urteil vom 14.02.1958, Az. I ZR 151/56, NJW 1958, 827). Danach führt ein Eingriff in das allgemeine Persönlichkeitsrecht einer Person zu einer billigen Entschädigung in Geld, wenn ein schwerwiegender Eingriff vorliegt und dieser nicht anders wiedergutzumachen ist als durch eine Entschädigungszahlung.

Von dieser BGH-Rechtsprechung zu unterscheiden ist der Anspruch auf Ersatz immaterieller Schäden wegen Datenschutzverstößen aus Art. 82 Abs. 1 DSGVO. Nach dieser Norm hat jede Person, der aufgrund eines Datenschutzverstoßes ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen. Eine Erheblichkeitsschwelle ist in der Norm im Wortlaut nicht angelegt, wird aber unter Juristen immer wieder gefordert.

Der Kläger gab sich mit dieser Entscheidung nicht zufrieden und beklagte den Entzug des gesetzlichen Richters beim Bundesverfassungsgericht: Eine Ablehnung von Schadensersatzansprüchen nach Art. 82 Abs. 1 DSGVO bei Bagatellverstößen könne angesichts der gebotenen Auslegung von Europarecht nicht ohne Einschaltung des EuGH entschieden werden. Das Bundesverfassungsgericht bestätigte dies in seinem am 14.01.2021 entschiedenen Fall (Az.: 1 BvR 2853/19) und verwies das Verfahren an das AG Goslar zurück: Das Amtsgericht habe Art. 101 Abs. 1 Satz 2 GG verletzt, indem es von einem Vorabentscheidungsersuchen zum EuGH absah. Das AG Goslar wird die Frage nach einem Schmerzensgeld mithin im weiteren Verfahren dem EuGH vorlegen müssen.

Es bleibt fraglich, ob die Annahme einer Erheblichkeitsschwelle mit Art. 82 Abs. 1 DSGVO in Einklang zu bringen ist – eine unionsrechtlich zu entscheidende Frage.

BVerfG: Vorlagepflichtige Fragen zur Auslegung der DSGVO

Das Bundesverfassungsgericht hat der gegen das Urteil des AG Goslar gerichteten Verfassungsbeschwerde stattgegeben und entschieden, dass das Amtsgericht Goslar eben diese Frage, ob ein Bagatelldatenschutzverstoß einen Schadensersatzanspruch begründet, im Rahmen eines Vorabentscheidungsverfahrens dem EuGH hätte vorlegen müssen. Ein Gericht, gegen dessen Urteil kein Rechtsmittel zulässig ist, darf eine unionsrechtliche Frage nur selbst entscheiden, wenn die Frage bereits geklärt oder so eindeutig ist, dass vernünftigerweise keine Zweifel an ihrer Beantwortung bestehen können. Beides war hier nicht der Fall, daher hat das Amtsgericht Goslar mit seiner Alleinentscheidung das Recht des Klägers auf seinen gesetzlichen Richter aus Art. 101 Abs. 1 S. 2 des Grundgesetzes verletzt. Das Bundesverfassungsgericht hat den Rechtsstreit nunmehr an das Amtsgericht Goslar mit der Maßgabe, die Frage dem Europäischen Gerichtshof vorzulegen und anschließend erneut zu entscheiden, zurückverwiesen.

Ausblick

Legt das Amtsgericht Goslar die Frage dem Europäischen Gerichtshof vor, wird dieser zu entscheiden haben, ob auch für Datenschutzverstöße im Bagatellbereich Entschädigungszahlungen zu leisten sind. Bejaht das Gericht diese Frage, werden Abmahnwellen wegen Datenschutzverstößen wahrscheinlicher. Eine Entscheidung des Europäischen Gerichtshofs ergeht im Durchschnitt nach 15 Monaten, so dass das Verfahren noch einige Zeit in Anspruch nehmen wird.

Gilt das UWG für die Auslegung der DSGVO?

Wann sind Werbeanrufe zulässig? Wird für jede Werbeemail eine Einwilligung benötigt? Diese Fragen werden heute intensiv unter der DSGVO diskutiert, auch angesichts der damit einhergehenden Bußgeldrisiken. Im unlauteren Wettbewerbsrecht sind diese Fragen unter dem UWG schon seit vielen Jahren ein Dauerbrenner, ihre Beantwortung in etlichen Gerichtsentscheidungen konkretisiert. Das OVG Saarland hat sich jüngst mit der in diesem Kontext höchst praxisrelevanten Frage befasst, ob die unter dem UWG entwickelten Grundsätze zu zulässiger Werbeansprache bei der Auslegung der DSGVO herangezogen werden können. Entgegenstehen könnte dem insbesondere, dass die DSGVO dem vorrangig anzuwendenden EU-Recht zuzuordnen ist, während das UWG nationales Recht darstellt.

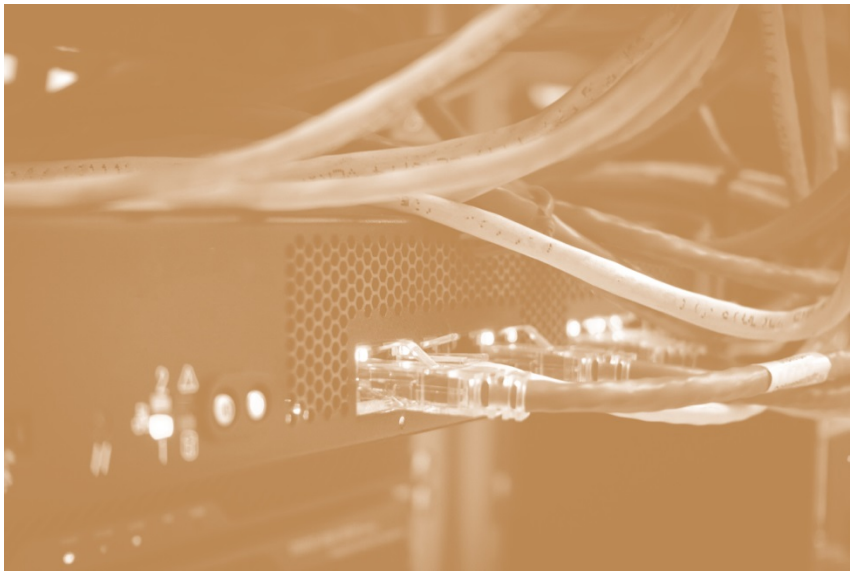
Um das Ergebnis vorweg zu nehmen: Das OVG Saarland sah in den Unterschieden der Normenhierarchie keinen zwingenden Grund, die zum UWG entwickelten Maßstäbe nicht auch für die Auslegung der DSGVO heranzuziehen (Beschluss vom 16.02.2021, Az. 2 A 355/19). Maßgeblich wird dies bei der Prüfung, ob eine konkrete Werbeansprache einer Einwilligung bedarf („Opt-In“) oder aber aufgrund berechtigter Interessen ohne eine solche zulässig ist, solange der Angesprochene widersprechen kann („Opt-Out“).

In der Praxis besteht für Unternehmen oftmals die Herausforderung, dass die datenschutzrechtlichen Vorschriften sehr wertungsbasiert sind, insbesondere, wenn es um das berechtigte Interesse des Unternehmens und die Abwägung mit den Interessen der Betroffenen geht. Seit Inkrafttreten der DSGVO ist die Orientierung an Grundsätzen des UWG daher *best practice.* Auch etliche andere Stimmen, u.a. die Datenschutzaufsichtsbehörden, hatten sich bereits in diese Richtung positioniert. Für einen Rückgriff auf die zum UWG entwickelten Maßstäbe in dieser Abgrenzungsfrage sprach für das OVG Saarland nun auch, dass beide Materien auf den Missbrauchsschutz abzielen und auch das UWG auf EU-Recht beruht (§ 7 UWG setzt die ePrivacy-Richtlinie 2002/58/EG um). Zudem könne gerade für die Auslegung des Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO als Ausgangspunkt auf konkret gefasste Erlaubnistatbestände aus dem

nationalen Recht abgestellt werden, um dem allgemeinen Erlaubnistatbestand Konturen zu verleihen und Rechtssicherheit herzustellen.

Konkret fehlte im vorliegenden Fall eine nachgewiesene, wirksame Einwilligung des Angesprochenen in ein Direktmarketing via Telefon. Bei der dann erforderlichen Prüfung, ob das Telefonmarketing auch ohne Einwilligung aus hinreichend berechtigten Interessen datenschutzrechtlich zulässig sei, berücksichtigte das Gericht die Wertung des § 7 Abs. 2 Nr. 2 UWG und verneinte danach einen Rückgriff auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Gem. § 7 Abs. 2 Nr. 2 UWG liegt nämlich bei Werbung mit einem Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung stets eine unzumutbare Belästigung vor, ohne dass es auf eine Abwägung ankäme. Dem Einwand, die Wertung des § 7 Abs. 2 Nr. 2 UWG könne bei der Anwendung der DSGVO keine Rolle spielen, da es sich einerseits um nationales Recht handle, andererseits auch zu differenzieren sei zwischen wettbewerbs- und datenschutzrechtlichen Wertungen, verpasste das OVG eine Absage.

Für die Praxis bringt die Entscheidung Rechtssicherheit: Anders, als zur DSGVO, findet sich zum UWG umfangreiche, wenn auch zum Teil fragmentierte Rechtsprechung und Kommentierung. In der Praxis erleichtert das aber die Prüfung ungemein, vor allem bei latent konturlosen Abwägungsfragen.



Google will künftig auf Cookies verzichtet: Bringt dies Ruhe in die Datenschutz- und ePrivacy-Diskussionen?

Spätestens seit der Planet49-Entscheidung zunächst vom EuGH, dann vom BGH, gibt es kaum noch eine Website ohne umfangreiche Consent Management Tools, Nutzer werden umfassend um eine Einwilligung in das Setzen diverser Cookies gebeten. Cookies werden für die unterschiedlichsten Zwecke verwendet – von der Bereitstellung einer Warenkorb- oder LogIn Funktion bis hin zum Ausspielen personalisierter Werbung auch über diverse Websites hinweg. Google hat jüngst angekündigt, in ihrem Chrome-Browser künftig vollständig auf Cookies verzichten zu wollen. Aber beseitigt dies alle rechtlichen Hürden und Bedenken?

Hierfür plant Google, die aktuelle Technologie des Browsers Google Chrome, die das Setzen von Third-Party-Cookies unterstützt, auslaufen zu lassen. Dies teilte ein Konzernsprecher von Google in einem Blogbeitrag mit (hier in englischer Sprache abrufbar). Schon im Januar hatte der Konzern bekannt gegeben, dass sie innerhalb der nächsten zwei Jahre ein Werbesystem für Google-Produkte entwickeln möchten, das ohne sog. Third-Party-Cookies auskommt (hier der Blogbeitrag in englischer Sprache). Mit „Third-Party-Cookies" bezeichnet man Cookies, die nicht vom Website-Betreiber selbst, sondern von Dritten auf einer Website eingesetzt werden. Third-Party-Cookies werden etwa für das Ausspielen personalisierter Werbung verwendet.

Der Google-Konzern möchte mit seiner Entscheidung, künftig das Nutzertracking über Cookies nicht mehr zu unterstützen, nach eigenen Angaben der wachsenden Skepsis gegenüber der Cookie-basierten Werbeindustrie entgegentreten und eine datensparsamere Variante der Onlinewerbung ermöglichen. In diesem Denken ist Google nicht alleine: Laut Medienberichten aus dem Handelsblatt und Netzpolitik.org reagiert Google damit einerseits auf Konkurrenzkonzerne wie Apple und Mozilla (Safari / Firefox), die schon länger Schritte in Richtung datenschutzfreundlicheren Cookie-Einsatz in ihren Browsern getan haben. Andererseits nimmt gerade hinsichtlich der personalisierten Werbung durch Cookies auch der Druck der Datenschützer zu, etwa durch die neue „Tracking Free Ads"-Koalition im Europaparlament, die ein Verbot der verhaltensbasierten Werbung durch sogenannte Tracking-Cookies fordern (dazu Bericht von heise.de).

Browser-Analyse anstelle von Third-Party-Cookies

Dies bedeutet indes nicht, dass Google künftig keine passgenaue Werbung über Chrome ermöglichen würde. Google setzt künftig auf eine neue Technik, „Federated Learning of Cohorts“ („FloC“). Diese basiert nach Angaben des Konzerns in einem Whitepaper (hier auf Englisch abrufbar) auf der Sammlung der von Nutzern aufgerufenen URLs und der Browser-Geschichte. Die datenschutzfreundlichere Neuerung ist, dass keine individuellen Profile mehr erstellt werden sollen. Vielmehr sollen die Informationen in Gruppen – oder eben „Kohorten" – so zusammengestellt werden, dass der einzelne Nutzer nicht mehr identifizierbar ist. Zudem soll die Verarbeitung rein auf dem Rechner des Browsernutzers erfolgen, sodass die Daten nicht verteilt werden. Nutzer sollen nach ihrem Suchverhalten bestimmten Kohorten zugeordnet und interessenbasierte Werbung entsprechend der Kohorte ausgespielt werden. Laut Google kann über diese Methode der Gruppenbildung ähnlich effektiv interessenbasierte Werbung geschaltet werden wie mit Third-Party-Cookies.

Datenschutzbedenken bestehen auch hier

Dass Google durch diese Methode alle Datenschutzbedenken an verhaltensbasierter Werbung aus dem Weg räumt, ist unwahrscheinlich. Etwa weisen laut Netzpolitik.org Beobachter darauf hin, dass die in den Kohorten verarbeiten Daten zumindest für Google nicht anonymisiert sind und deshalb weiterhin die DSGVO-Vorgaben beachtet werden müssten. Auch bei der Zuteilung in Kohorten könnten weiterhin persönliche oder sensible Informationen ausgelesen werden, zudem müsse auf die effektive Anonymisierung der Daten durch die Werbewirtschaft geachtet werden. Überdies wird auch dadurch – und dies eröffnet regelmäßig den Anwendungsbereich des ePrivacy-Rechts – auf das Endgerät der Nutzer zugegriffen.

Große Konsequenzen für die Werbeindustrie

Unabhängig davon wird die Entscheidung von Google erheblichen Einfluss auf die Werbeindustrie haben, die sich momentan auf den Einsatz von Third-Party-Cookies stützt. Zwar bietet Google über die „FloC“ eine vielleicht ähnlich effektive Alternative zu Third-Party-Cookies-basierter Werbeschaltung an, Beobachter prognostizieren aber für Anbieter von Werbung eine größere Abhängigkeit von

Google-Konzern und ihren Datenbeständen. Soll sich nicht auf die weniger ertragsreiche nicht-verhaltensbasierte Werbung verlassen werden, wird wohl auf Googles Datensätze zu den Konditionen des Konzerns zurückgegriffen werden müssen. Der Konzern hat angekündigt, den Browser mit der neuen Werbetracking-Funktion noch im März testweise anzubieten – für Werbende soll im Laufe des zweiten Quartals 2021 die Möglichkeit zum Test bestehen.

Zu guter Letzt

Auch in diesem Monat gibt es wieder einige interessante Entscheidungen ausländischer sowie deutscher Datenschutzbehörden zum Thema Bußgeld. Vor einem solchen sind auch Fußballvereine nicht gefeilt. Besonders interessant für die Praxis sind zudem neue Initiativen der Datenschutzkonferenz zur Umsetzung des EuGH-Urteils von Juli 2020 zum Transfer personenbezogener Daten in die USA sowie – auch mit Blick auf die Datensicherheit – die Sache „Hafnium" und neue Hinweise zum Einsatz von Videokonferenzsystemen.

- **USA-Transfer personenbezogener Daten: Werden die Datenschutzaufsichtsbehörden aktiv?**

Nach dem EuGH-Urteil in Sachen „Schrems II" im Juli 2020 ist der Transfer personenbezogener Daten in die USA mit erheblichen Rechtsunsicherheiten behaftet. Der Zusammenschluss der

deutschen Datenschutzaufsichtsbehörden, die Datenschutzkonferenz (DSK), hat in seiner Sitzung im letzten November, zu der das Protokoll vor wenigen Wochen veröffentlicht wurde, zwei für die Praxis wesentliche Aussagen aufgenommen (TOP 22 des Protokolls):

- *Es sollen (jedenfalls in Hamburg) stichprobenartige Überprüfungen beginnen, in bekannter Vorgehensweise zunächst in Form von „Fragebögen" an verschiedene Unternehmen.*
- *Die DSK will ein Gutachten zur Rechtssituation in den USA beauftragen.*

Gerade Letzteres ist ein für die Praxis hilfreicher Fingerzeig, stellt doch die vom EuGH aufgestellte Prüfpflicht der Rechtssituation im Drittland die Unternehmen vor kaum lösbare Aufgaben. Die Behörden gehen offenbar davon aus, dass die Unternehmen nunmehr Zeit für eine Umsetzung, jedenfalls aber für eine risikoangemessene Behandlung des Themas hatten.

- **„Hafnium" – das Sicherheitsleck bei Microsoft**

Anfang März hat eine Sicherheitslücke in den Exchange-Systemen von Microsoft die IT-Sicherheit in Atem gehalten (siehe etwa hier von Microsoft und hier vom BSI dazu). Nun werden die rechtlichen Folgen diskutiert. Allem voran: Wann besteht für betroffene Unternehmen eine Meldepflicht nach Art. 33 DSGVO? Etwa die Aufsichtsbehörde in Thüringen hat aktuell darauf hingewiesen, dass nach ihrer Ansicht jedenfalls im Fall bereits installierter Schadcodes eine Meldepflicht bestehe. Betroffene Unternehmen sollten in jedem Fall auch eine etwaige Meldepflicht sorgsam prüfen.

- **Neues zum Einsatz von Videokonferenzdiensten und -systemen**

Durch die Kontaktbeschränkungen hat der Einsatz von Videokonferenzsystemen im Berufsalltag deutlich an Bedeutung gewonnen. Von Seiten der Datenschutzaufsichtsbehörden werden viele der gängigen Angebote kritisch gesehen. Für die Praxis hilfreich sind die Handreichungen des BSI zu technischen Mindeststandards, um Vertraulichkeit und Integrität zu wahren. Das Community Draft für Videokonferenzsysteme wurde jüngst aktualisiert. In einer Antwort der Landesregierung NRW auf eine Kleine Anfrage aus dem Kreis der Grünen wurde übrigens jüngst

festgehalten, dass das Einschalten von Kamera und Mikrofon als wirksame Einwilligung gewertet werden könne (Drs. 17/12894).

- **Deutschland: VfB Stuttgart kassiert DSGVO-Bußgeld in Höhe von 300.000 Euro**

Der Landesbeauftragte für Datenschutz und Informationsfreiheit in Baden-Württemberg (LfDI BW) verhängte ein Bußgeld in Höhe von 300.000 Euro gegen den VfB Stuttgart wegen eines fahrlässigen Datenschutzverstoßes gegen die Rechenschaftspflichten aus Art. 5 Abs. 2 DSGVO. Leitende Mitarbeiter des Vereins verschickten im Vorfeld der Mitgliederversammlung im Juni 2017 Mitgliederdaten an Dritte. Darunter waren personenbezogene Daten wie Festnetz- und Handynummern, E-Mail-Adressen oder Angaben zu Teilnahmen an zurückliegenden Mitgliederversammlungen. Die Vorfälle deckte damals das Sportmagazin Kicker auf. Inwiefern ein DSGVO-Verstoß in der Übermittlung selbst lag, lässt die Pressemitteilung des LfDI BW offen – klar wird aber, dass das Datenschutzmanagement des VfB aus Sicht der Behörde unzureichend war. Der VfB Stuttgart kooperierte umfassend mit dem LfDI BW und verbesserte das Datenschutzmanagement. All dies wirkte sich mildernd auf die Höhe des Bußgeldes aus.

- **Italien: 7 Mio. Euro für unzureichende Datenschutzinformationen bei Facebook**

Die italienische *Kartell*behörde erlegt Facebook eine Geldbuße in Höhe von 7 Mio. Euro auf, weil das Unternehmen einer Abmahnung aus dem Jahr 2018 mit der Aufforderung, eine festgestellte unlautere Geschäftspraxis bei der Verwendung von Nutzerdaten zu beseitigen und eine Richtigstellung zu veröffentlichen, nicht nachgekommen ist. Nach Ansicht der Kartellbehörde verleitete Facebook seine Nutzer irreführend dazu, sich auf ihrer Plattform zu registrieren, indem sie nicht vollständig und präzise bereits bei der Eröffnung eines Nutzerkontos über die kommerzielle Verwendung von Nutzerdaten informierte, sondern die Unentgeltlichkeit des Dienstes betonte. Der Nutzer könne mithilfe der zur Verfügung gestellten Datenschutzinformationen nicht genau unterscheiden, welche der erhobenen Daten Werbezwecken dienten und welche zur Personalisierung des Profils – mit dem Ziel, die Kontaktaufnahme mit anderen Nutzern zu erleichtern – beitragen sollen. Ohne diese Informationen könne der Nutzer nicht selbstbestimmt darüber entscheiden, ob er seine Daten preisgeben will, um die Plattform nutzen zu können. Nach der

Abmahnung habe Facebook zwar die Unentgeltlichkeitsbehauptung bei der Registrierung entfernt, über die gewerblichen Zwecke bei der Verarbeitung der Nutzerdaten habe Facebook jedoch immer noch nicht mit der gebotenen Klarheit informiert.

- **Spanien: 6 Mio. Euro für Datenverarbeitung ohne Rechtsgrundlage und unzureichende Datenschutzinformationen**

Die spanische Datenschutzbehörde verhängte gegen die CAIXABANK ein Bußgeld in Höhe von insgesamt 6 Mio. Euro. Die Behörde ist der Ansicht, dass die Bank ihren Informationspflichten nicht im gebotenen Umfang nachgekommen ist und damit ein Verstoß gegen Art. 13 und 14 DSGVO vorliegt, den sie mit 2 Mio. Euro ahndeten. Weitere 4 Mio. Euro kostetet das Unternehmen ein Verstoß gegen Art. 6 DSGVO: Bestimmte Datenverarbeitungen auf Grundlage von Einwilligungen seien unrechtmäßig, da die eingeholten Einwilligungen nicht die Voraussetzungen einer freiwilligen und informierten Einwilligung erfüllen würden. Auf berechtigten Interessen des Unternehmens beruhende Datenverarbeitungen seien nicht ausreichend gerechtfertigt.

- **Niederlande: Unzureichender Schutz vor unbefugtem Zugriff auf Patientenakten**

Die niederländische Datenschutzbehörde verhängte ein Bußgeld in Höhe von 440.000 Euro gegen das Amsterdamer Krankenhaus OLVG, das keine ausreichenden technischen und organisatorischen Maßnahmen ergriffen hatte, um unbefugten Zugriff auf Krankenakten durch Personal zu verhindern (Art. 32 DSGVO). Patientenakten, die Krankengeschichte, Sozialversicherungsnummer und Kontakt- und Adressaten enthalten, konnten innerhalb des Krankenhaus-Netzwerkes durch einfachen Login eines Mitarbeiters (Benutzername und Passwort) eingesehen werden, es fehlte an einem hinreichenden Benutzerkonzept.

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