LOSCHELDER

Newsletter Datenschutzrecht
Dezember 2019

Sehr geehrte Damen und Herren,

es weihnachtet sehr und auch wir haben daher im Dezember-Newsletter kleine Datenschutzpakete geschnürt, mit interessanten bis kuriosen Entwicklungen.

Für das neue Jahr möchten wir Sie dann auch nochmals auf unsere anstehenden Veranstaltungen im Januar und Februar hinweisen, bei denen wir Sie sehr gerne begrüßen würden. Im Januar werden wir moderne Marken- und Vertriebsformen, Tracking- und Analysetools sowie aktuelle EU-Vorgaben für Plattformen näher beleuchten. Im Februar geht es dann um ein modernes, digitales Compliance- und Krisenmanagement mit den diversen Chancen und Risiken, die durch die digitale Transformation entstehen:

Digitaler Vertrieb: 22.01.2020, 16.00 Uhr – 18.00 Uhr

Compliance & Krisenmanagement: 12.02.2020, 16.00 Uhr – 18.00 Uhr

In diesen Veranstaltungen beleuchten wir aktuelle Entwicklungen und zentrale Rechtsfragen rund um die digitale Transformation – praxisnah und im unmittelbaren Gespräch mit Ihnen. Weitere Informationen dazu und die **Möglichkeit zur Anmeldung** finden Sie auf unserer Homepage.

Inhalt

Aktuelle Entwicklungen rund um Websites und Bußgelder

Messenger-Apps auf mobilen Dienstgeräten

Für den Dienstwagen bedarf es keiner Führerscheinkopie

Gesundheitsdaten im Fokus der Aufsichtsbehörden

Der Umfang von Auskunftsansprüchen

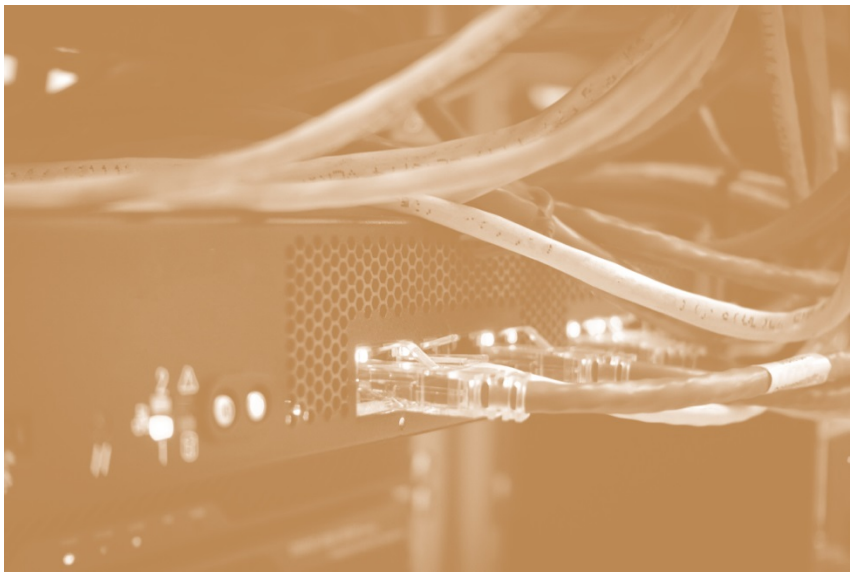
Aktuelle Entwicklungen rund um Websites und Bußgelder

Aus den Aufsichtsbehörden gibt es Neuigkeiten zur datenschutzkonformen Websitegestaltung (Stichwort: Cookies). Und auch Bußgelder sind im letzten Monat wieder in teils erstaunlicher Höhe verhängt worden.

Wir möchten Sie zu Beginn unseres Newsletters auf die Aufforderung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) aufmerksam machen (Pressemitteilung vom 14. November 2019): *Websitebetreiber sollten sich genau damit auseinandersetzen, welche Dritt-Dienste bei ihnen eingebunden sind und diese notfalls deaktivieren, bis sie sichergestellt haben, dass ein datenschutzkonformer Einsatz gewährleistet werden kann*. Er teilt die Ansicht der Landesaufsichtsbehörden, wonach Websitebetreiber, die Nutzerdaten an Dritte wie Google Analytics übermitteln, die diese Daten wiederum für eigene Zwecke nutzen, hierfür einer Einwilligung des Nutzers bedürfen. Wir berichteten in unserem November Newsletter über Bedenken, die Landesaufsichtsbehörden in der Vergangenheit und im Rahmen ihrer koordinierten Pressemitteilungsaktion geäußert haben. Im Adventskalender der Aufsichtsbehörde Rheinland-Pfalz klingt nun an, dass sich diese Bedenken auf solche Tools beziehen, die keine ordnungsgemäße Auftragsverarbeitung gewährleisten. Letztere – vermutlich gehört etwa eTracker dazu – könnten dagegen auch ohne Einwilligung datenschutzkonform nutzbar sein.

Was die aktuelle Bußgeldpraxis angeht, sticht ebenfalls der BfDI heraus. Dieser verhängte ein Bußgeld in Höhe von 9,55 Millionen gegen 1&1 wegen - aus seiner Sicht - unzureichender Authentifizierung von Kunden an der Telefonhotline. Der Telekommunikationsdienstleister hat angekündigt, gegen das Bußgeld vorgehen zu wollen.

Und auch der Einsatz von Messenger-Diensten wurde in der jüngeren Vergangenheit Grundlage für Bußgeldentscheidungen: Die rumänische Aufsichtsbehörde verhängte gegen die Raiffeisen Bank S.A. und die Vreau Credit S.R.L. Bußgelder in Höhe von 150.000 € bzw. 20.000 €. Die Mitarbeiter der Finanzdienstleister hatten Daten des Ausweisdokumentes eines Kunden per WhatsApp ausgetauscht.



Messenger-Apps auf mobilen Dienstgeräten

Die Nutzung von Messenger-Apps wie WhatsApp auf mobilen Dienstgeräten ist ein Dauerbrenner im Datenschutzrecht. Das aktuelle „Whitepaper" der deutschen Datenschutzaufsichtsbehörden (DSK) zu technischen Datenschutzanforderungen an Messenger-Dienste/Applikationen (Apps) im Krankenhausbereich beschäftigt sich mit den datenschutzrechtlichen Anforderungen im Krankenhausbereich. Dem Papier lassen sich aber allgemeine und branchenunabhängige Grundsätze entnehmen. Das Fazit vorab: Die Nutzung von Messenger-Applikationen wie WhatsApp ist datenschutzrechtlich nicht ausgeschlossen, muss aber durch die Unternehmen aktiv gestaltet werden und zahlreiche Anforderungen erfüllen.

Datenschutzrechtlichen Bedenken begegneten Messenger-Apps bereits vor Inkrafttreten der DSGVO. Im März 2017 erging ein (kontroverses) Urteil des Amtsgerichts Bad Hersfeld, wonach das Abrufen der auf dem Endgerät des WhatsApp-Nutzers gespeicherten Rufnummern einer Einwilligung der Nummerninhaber bedürfe. Das datenschutzrechtliche Grundproblem bleibt auch unter der DSGVO bestehen. Durch Messenger-Apps, wie WhatsApp, werden regelmäßig personenbezogene Daten an die gewerblichen Messenger-Betreiber übertragen, obwohl die Personen keine Einwilligung hierzu erteilt haben und womöglich auch sonst in keinem Verhältnis zu dem App-Anbieter stehen; sie nutzen die App also selbst gar nicht aktiv. Dies geschieht regelmäßig dadurch, dass die Messenger-Apps das Telefonbuch des mobilen Endgerätes abgleichen und

dabei sämtliche Telefonbucheinträge an den Messenger-Betreiber übermittelt werden, unabhängig davon, ob mit einer dort vermerkten Person über den Messenger kommuniziert wird oder nicht. Teilweise können App-Nutzer die Datenübertragung auch nicht oder kaum verhindern; beispielsweise im Falle von WhatsApp lässt sich die Synchronisationsfunktion des Adressbuchs nicht in der App deaktivieren (im iPhone nur über „Einstellungen", bei Android über eine gesonderte App). Während nach der alten Rechtslage noch vereinzelt eine Zustimmung aus schlüssigem Verhalten für die Fälle diskutiert wurde, in denen ein Dritter die Messenger-App selber auch installiert hat, ist diese Option unter Geltung der DSGVO u.a. aufgrund der Transparenzanforderungen und des Ausdrücklichkeitserfordernisses (Einwilligung durch „aktives Tun", Erwägungsgrund 32) ausgeschlossen.

Dies bedeutet aber nicht, dass nunmehr die Nutzung von Messenger-Apps stets ausgeschlossen ist: Der Einsatz kann vielmehr zulässig sein, wenn bestimmte Schutzvorkehrungen getroffen und unnötige Datenübermittlungen vermieden werden. Dies erfordert es insbesondere, den automatischen Adressbuchabgleich auszuschließen. Die DSK hebt aus den personenbezogenen Daten Dritter nochmal ausdrücklich die Kontaktdaten von Kommunikationsteilnehmern hervor und verlangt für diese eine getrennte Speichermöglichkeit (S. 3. Ziffer I. Nr. 3):

> *„Die Applikation muss über die Möglichkeit verfügen, Kontaktdaten von Kommunikationsteilnehmern in einem eigenen, vom allgemeinen Adressbuch des Smartphones getrennten Speicher abzulegen."*

Die getrennte Speicherung verlangt die DSK aber nicht nur für die Kontaktdaten, sondern für alle Nachrichten und Anhänge. Die App muss über die Möglichkeit verfügen, Nachrichten sowie Dateianhänge, wie Bilder, Videos, Dokumente etc., ausschließlich in einem eigenen, von den allgemeinen Speicherbereichen des Smartphones getrennten Speicher in verschlüsselter Form abzulegen. Diese Trennung kann mit sog. Container-Apps erreicht werden. Neben zahlreichen weiteren Anforderungen an die Messenger-App führt die DSK überdies Sicherheitsmaßnahmen bezüglich der Kommunikation und der Endgeräte auf. So muss beispielsweise die Kommunikation nach dem gegenwärtigen Stand der Technik und der interne Speicher des Geräts verschlüsselt sein. Das Endgerät muss außerdem zugriffsgesichert werden, z.B. durch PINs, Passphrasen oder

biometrische Lösungen, und die aktuelle Betriebssoftware mit allen Sicherheitspatches versorgt sein.

Neben den soeben beispielhaft aufgezählten Anforderungen enthält das Whitepaper noch zahlreiche weitere Muss- und Soll-Vorschriften, die im Einzelfall zu prüfen sind.

Für den Dienstwagen bedarf es keiner Führerscheinkopie

Stellen Unternehmen ihren Mitarbeitern Dienstfahrzeuge zur Verfügung, haben sie die (strafbewehrte) Pflicht, zu prüfen, ob der Fahrer die notwendige Erlaubnis zur Führung des KfZ hat (§ 21 Abs. 1 Nr. 3 Straßenverkehrsgesetz). Um dies nachweisen zu können, werden in vielen Unternehmen die Führerscheine der Mitarbeiter/innen kopiert und zu den Personalakten genommen. Ob dies zulässig ist, hat eine Datenschutzaufsichtsbehörde zuletzt näher betrachtet.

Nach Ansicht des BayLfD verstößt die Kopie von Führerscheinen und die Archivierung von Führerscheinkopien gegen den Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und der Zweckbindung.

Nach der DSGVO dürfen personenbezogene Daten nur in dem Umfang erhoben und gespeichert werden, wie es für die Zweckerfüllung erforderlich sind. Daraus folgert der BayLfD, dass nur die Angaben „aus“ dem Führerschein zu erheben und zu speichern seien,

die für die Erfüllung der Halterpflichten benötigt werden. Hierfür genüge es, wenn z. B. mittels eines Formblattes die zur Prüfung erforderlichen Informationen eingeholt werden, der Führerschein vorgezeigt wird und eine entsprechende Dokumentation des Vorgangs erfolgt. Eine Kopie des Führerscheines sei hierbei nicht notwendig (und etwa auch die Anfertigung von Kopien von Personalausweisen wird in den allermeisten Fällen datenschutzrechtlich kritisch beurteilt, wie das LDI NRW in einer Übersicht aus Juli 2019 darstellt).

Gespeichert werden dürfen die im Rahmen der Führerscheinkontrolle erhobenen Daten auch nur solange wie sie für die Nachweisführung erforderlich sind (Art. 5 Abs. 1 lit. e DSGVO). Über die Nutzungsdauer der Fahrzeuge durch einen Beschäftigten hinaus käme eine Speicherung nur insoweit in Betracht, als die Speicherung dem Nachweis dient, den Halterpflichten in der Vergangenheit nachgekommen zu sein, mit Blick auf die strafrechtliche Relevanz i.d.R. drei Jahre (§ 78 Abs. 3 Nr. 5 StGB).

Zudem weist der BayLfD auch auf die Informationspflichten des Art. 13 DSGVO hin. Soweit die Betroffenen nicht bereits über die erforderlichen Informationen (z.B. durch einen Arbeitsvertrag) verfügten, seien die Informationen im Zeitpunkt der Erhebung, d.h. im Rahmen der Führerscheinkontrolle, zur Verfügung zu stellen. Sichergestellt werden sollte darüber hinaus nach Ansicht des BayLfD, dass möglichst wenig Personen mit den personenbezogenen Daten in Berührung kommen bzw. die Zugriffsmöglichkeiten so weit wie möglich eingeschränkt werden.

Die Stellungnahme des BayLfD bezieht sich zwar auf öffentliche Dienstherren in Bayern, für die datenschutzrechtliche Besonderheiten gelten (Art. 103 Satz 1 BayBG), die in Bezug genommenen Grundsätze der DSGVO gelten aber auch für private Arbeitgeber.

Gesundheitsdaten im Fokus der Aufsichtsbehörden

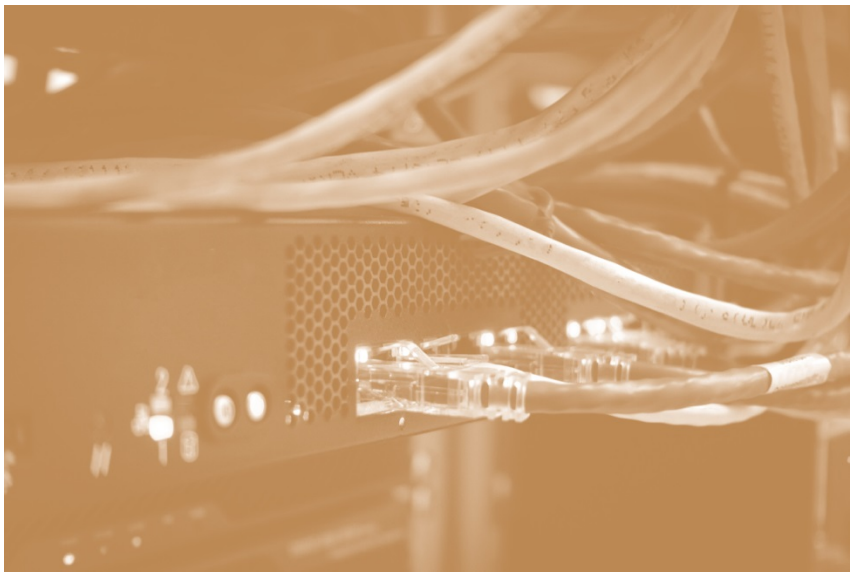
Die Verarbeitung von Gesundheitsdaten bleibt im Fokus der Aufsichtsbehörden. Hintergrund ist der nach ersten aufsichtsbehördlichen Prüfungen bisweilen sorglose Umgang mit dieser besonders schutzwürdigen Kategorie von Daten (Art. 9 Abs. 1 DSGVO); ihre Verarbeitung muss die gesteigerten Anforderungen des Art. 9 DSGVO erfüllen. Einem rheinland-pfälzischen Krankenhaus wurde aufgrund von strukturellen Defiziten bei der Rechnungstellung jüngst ein Bußgeld in Höhe von (wegen Kooperation mit der Aufsichtsbehörde) 105.000 € auferlegt.

Im letzten Monat hat sich die Datenschutzkonferenz gleich mehrfach zu dem Umgang mit Gesundheitsdaten geäußert:

- In ihrem Whitepaper beschreibt die DSK die technischen Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich (dazu unser Beitrag 2).
- Außerdem veröffentlichte sie eine Entschließung zur Weitergabe von Daten an unbefugte Dritte auf Gesundheitswebseiten und in Gesundheits-Apps und
- eine Entschließung zum Schutz von Patientendaten.

Und auch Wettbewerber können nach einem aktuellen Urteil des OLG Naumburg vom 07. November 2019 die datenschutzkonforme Verarbeitung von Gesundheitsdaten durchsetzen: Nach der Entscheidung kann die rechtswidrige Verarbeitung von Gesundheits-

daten zu Werbezwecken von Wettbewerbern eines Verantwortlichen abgemahnt werden.



Der Umfang von Auskunftsansprüchen

Mit einem datenschutzrechtlichen Auskunftsersuchen eines Betroffenen konfrontiert, stellen sich Unternehmen regelmäßig die Frage, ob und was „in Kopie" herauszugeben ist. Zunehmend verlangen Betroffene – auch zur Vorbereitung von Gerichtsverfahren – Kopien interner Vermerke oder sonstige Aktenstücke. Diese geben die Unternehmen wiederum zurecht ungern heraus: Derartige Unterlagen können Unternehmensinterna und ggf. sogar Betriebs- und Geschäftsgeheimnisse enthalten, es kann sich um strategisch bedeutsame Prozessunterlagen handeln. Aber reicht das „Recht auf Kopie" aus Art. 15 DSGVO wirklich so weit, dass Betroffene diesen Auskunftsanspruch - etwa auch zur Verbesserung ihrer Position in Rechtsstreitigkeiten - einsetzen können?

Die Rechtsprechung ist in diesen Punkten noch in den Anfängen und uneinheitlich (wir berichteten in unserem April und Juni Newsletter). Erfreulich ist, dass sich neben dem OLG Köln nun ein weiteres Gericht - das Amtsgericht München - der engeren Auffassung (AG München, Teilurteil v. 04.09.2019 – 155 C 1510/18) angeschlossen hat: Demnach kann der Betroffene grundsätzlich keine Auskunft über interne Vorgänge, mit dem Betroffenen gewechsel-

ten Schriftverkehr und rechtliche Bewertungen und Analysen über Art. 15 DSGVO verlangen.

In diesem Zusammenhang möchten wir Sie auch auf das im September veröffentlichte Arbeitspapier des bayerischen Landesbeauftragten für Datenschutz (BayLfD) zu offenkundig unbegründeten oder exzessiven Betroffenenanträgen aufmerksam machen. In seinem Arbeitspapier befasst er sich unter anderem mit dem häufigen Phänomen, dass sehr weit gefasste Auskunftsverlangen („alle über mich gespeicherte Daten“) wiederholt gestellt werden; diese sind nach Ansicht des BayLfD zwar nicht per se „exzessiv“ im Sinne von Art. 12 Abs. 5 lit. a DSGVO. Sie sind es aber dann, wenn ersichtlich keine weitere Datenverarbeitung stattgefunden hat. Das Arbeitspapier gibt zwar nur die Meinung einer Aufsichtsbehörde wieder und ist auf die Pflichten öffentlicher Stellen bezogen, die Grundsätze gelten ebenso aber auch für private Verantwortliche. Wenn Sie mit einem solchen Auskunftsersuchen konfrontiert sind oder Ihnen ein Auskunftsersuchen offensichtlich unbegründet oder exzessiv erscheint, lohnt sich daher vor Verweigerung der Auskunft, Verlangen eines Entgelts oder auch einer überobligatorischen Erfüllung des Auskunftsanspruchs eine genauere Prüfung, ggf. beginnend mit dem Arbeitspapier.

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. Lucyne Ghazarian
+49 (0)221 65065-222
lucyne.ghazarian@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