Sehr geehrte Damen und Herren,
liebe Kund:innen,

heute erhalten Sie die Februar-Ausgabe der Beratungsinformation. Aus der Beratungspraxis, Rechtsprechung und der Welt der Aufsichtsbehörden haben wir Ihnen wieder einen Strauß von Themen zusammengestellt.

Wir geben Ihnen unsere Einschätzung zum Einsatz von WhatsApp an die Hand, ein Dauerthema in der Beratung. Auch der Umgang mit Betroffenenrechten und hier insbesondere mit Auskunftsersuchen ist Gegenstand der täglichen Beratungspraxis. Einen neuen Aspekt, das „missbräuchliche“ Auskunftsersuchen, haben wir Ihnen in dieser Ausgabe aufbereitet.

Der Anstieg der verhängten Bußgelder im Jahr 2020 sowie anstehende Gerichtsentscheidungen zeigen den Trend in der Datenschutzpraxis für 2021 auf.

Mit einem Artikel in einem Randthema des Datenschutzes, den Pflichtangaben im Impressum von Webseiten, schließt diese Ausgabe ab.

Wo auch immer Sie diese Information erreicht, im Büro oder zu Hause im Homeoffice, ich wünsche eine interessante Lektüre und alles Gute!

Ihr

Asmus Eggert

Inhalt

Nutzung von WhatsApp im Unternehmen – Ein Dauerbrenner

Für den Austausch von Neuigkeiten in der Familie, für den virtuellen Stammtisch, für die wöchentliche Verabredung zur Joggingrunde oder das Teilen von Neuigkeiten im Fanclub nutzen inzwischen viele Menschen WhatsApp als Instant-Messaging-Dienst. WhatsApp ist im familiären Kreis

de facto der Kommunikationsstandard, auch wenn Messenger-Apps wie Signal und Threema mittlerweile viel Aufmerksamkeit erhalten.

Der Wunsch den Einsatz von WhatsApp auch im beruflichen Kontext unter Kollegen und im Austausch mit Kunden zu nutzen, liegt daher nahe. Freilich geht es hier um den Austausch von personenbezogenen Daten. Daher werden wir zu diesem Thema als Datenschutzbeauftragte regelmäßig um Rat gefragt.

Praxishinweis: Es ist erst einmal zu unterscheiden, ob die Nutzung vom privaten Smartphone der Beschäftigten erfolgt oder von einem dienstlich bereitgestellten Gerät.

1. Geschäftliche Nutzung auf privaten Smartphones:
   Im privaten Bereich ist die Nutzung von WhatsApp grundsätzlich kein Verstoß gegen die DSGVO, da die rein private Nutzung von WhatsApp unter Freunden bzw. in der Familie nicht unter den Anwendungsbereich der Datenschutzgrundverordnung (DSGVO) fällt. Erfolgt allerdings eine Nutzung der privaten Smartphones im Unternehmenskontext, ist der Anwendungsbereich der DSGVO eröffnet und es bestehen prinzipiell die gleichen Probleme wie bei der Nutzung von WhatsApp auf geschäftlichen Smartphones (siehe unten). Allerdings ist aus Datenschutzgründen die Nutzung privater Smartphones im Unternehmenskontext nicht zu empfehlen. Die Sicherheit von Unternehmensdaten und insbesondere personenbezogener Daten kann schlicht nicht gewährleistet werden (keine Sicherstellung der Nutzung aktueller Betriebssystemversionen, freie Installation von Apps, usw.).

2. Nutzung von WhatsApp auf geschäftlichem Smartphone:
   Grundsätzlich ist auf einem geschäftlichen Smartphone das Speichern und Nutzen der geschäftlichen Kontakte, soweit dabei die allgemeinen Datenschutzanforderungen (Rechtgrundlage, Information des Betroffenen, Löschregeln etc.) eingehalten werden, erst einmal unkritisch. Für den Einsatz von WhatsApp müssen darüber hinaus aber folgende datenschutzrechtliche Themen bedacht werden:
   A. **Upload des gesamten Telefonbuchs auf Server in den USA**
      Problem: Alle im Telefonbuch gespeicherten Kontakte des WhatsApp-Nutzers werden zum Abgleich auf Server in die USA übermittelt, und zwar unabhängig davon, ob der jeweilige Telefonbuchkontakt ebenfalls WhatsApp nutzt oder nicht. WhatsApp führt auf seiner Webseite hierzu aus:
      Wenn einer oder mehrere deiner Kontakte WhatsApp noch nicht verwenden, verwalten wir diese Informationen für dich in einer Form, in der sichergestellt ist, dass solche Kontakte nicht identifiziert werden können. Wir speichern diese Telefonnummern nicht und verarbeiten sie nur für kurze Zeit, um kryptografische Hash-Werte zu erstellen, mit denen wir effizienter eine Verbindung zwischen dir und diesen Kontakten herstellen können, wenn diese WhatsApp beitreten.
   B. **Verarbeitung von Metadaten auf Servern in den USA**
      Problem: WhatsApp-Chats sind grundsätzlich Ende-zu-Ende verschlüsselt (AES-256-Standard) und ein Zugriff auf die Inhalte des Chats ist für WhatsApp damit nicht möglich. Allerdings werden von WhatsApp unverschlüsselte Metadaten zu den jeweiligen Chats, insbesondere Nutzungs- und Protokollinformationen, Geräte- und Verbindungsdaten sowie Standort-Informationen (Geräte-ID, Rufnummer, Profildaten, Profilbild oder die dort angegebenen Informationen, Beginn und Ende eines Chats sowie Teilnehmer, deren Standort und

Häufigkeit von Chats) in den USA verarbeitet. Bei diesen Metadaten handelt es sich um personenbezogene Daten, für die die Vorgaben der DSGVO einzuhalten sind.

C. **Unverschlüsselte Backups in der Cloud**
Problem: WhatsApp verschlüsselt Cloud-Backups (inklusive der Chats) nicht. D.h. wird die Backup-Funktion von WhatsApp verwendet, wird das Backup unverschlüsselt beim jeweiligen Cloud-Anbieter (z.B. bei Apple Geräten in der Apple Cloud) abgelegt.

D. **Weitergabe der Daten an Dritte, insbesondere Facebook-Unternehmen**
Problem: Es ist bisher unklar, ob und welche Daten genau WhatsApp an Dritte und insbesondere Facebook bzw. Facebook-Unternehmen weitergibt.

Leider lassen sich die aufgezählten Probleme nicht einfach so beheben, weil Sie z.B. in der Funktionalität des Dienstes begründet sind. Es sind vielmehr die jeweiligen Risiken zu ermitteln und zu bewerten. Auf Basis der Risikobewertung muss bzw. kann dann entschieden werden, ob der Einsatz erfolgen soll oder nicht. Die Risikobewertung ist zu dokumentieren.

Unsere Zusammenfassung: Der Einsatz ist nicht zu empfehlen. Wir haben das Thema für unsere Kunden ausführlich aufbereitet. Dieses Dokument können Sie als Kunde unter folgendem Link downloaden: https://www.sofortdatenschutz.de/exklusiver-downloadbereich/

Hinweis: Sollte man sich für die geschäftliche Nutzung von WhatsApp entscheidet, ist gemäß WhatsApp AGB die Einwilligung von WhatsApp einzuholen.

Angesichts der genannten Probleme stellt sich die Frage nach alternativen Messengerdienste. Hier finden Sie z.B. eine Liste inkl. Bewertung der Verbraucherzentrale (https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055).

Missbräuchlich motivierte Geltendmachung von Betroffenenrechten

In unsrer Beratungspraxis stellen wir vermehrt fest, dass die Geltendmachung von Betroffenenrechten gem. Art. 15 DSGVO bis Art. 22 DSGVO durch Betroffene teilweise missbräuchliche Züge annimmt. Es lässt sich in einigen dieser Fällen das folgende Muster erkennen: Es wird eine Drohkulisse aufgebaut, um den Verantwortlichen zur außergerichtlichen Zahlung eines immateriellen Schadensersatzes in vierstelliger Höhe an den Betroffenen sowie der Erstattung der angeblich entstandenen Rechtsanwaltskosten zu bewegen.

Folgende zwei Szenarien sind festzustellen:

1. **Anfrage über ein Kontaktformular**
Bei diesem Szenario meldet sich eine Person über das auf der Webseite des Unternehmens geschaltete Kontaktformular und bittet um Rückruf. Versucht das Unternehmen dann im Nachgang die entsprechende Person unter der angegebenen Rufnummer zu erreichen, wird der Anruf nicht angenommen. Ein paar Wochen später meldet sich die Person wieder. Diesmal wird gefragt, welche Daten das Unternehmen gespeichert hat und es wird die Löschung der Daten verlangt.

2. **Newsletter-Abonnement**
Eine Person abonniert einen Newsletter auf der Webseite des Unternehmens. Kurz darauf wird das Unternehmen kontaktiert und um Auskunft über gespeicherte Daten gebeten und ebenfalls wieder Datenlöschung gefordert.

Die Reaktionen der betroffenen Unternehmen gleichen sich häufig:

- Die personenbezogenen Daten werden direkt gelöscht, dem Auskunftsersuchen wird nicht entsprochen.

- Es wird beauskunftet, dass keine personenbezogenen Betroffenendaten verarbeitet werden, obwohl zumindest die Rufnummer/E-Mail-Adresse des Betroffenen vorliegt.
- Es wird nicht reagiert.

Zeitlich nachgelagert meldet sich bei den Unternehmen dann ein Rechtsanwalt, welcher namens und im Auftrag seiner Mandantschaft wegen mutmaßlicher Verletzung der Betroffenenrechte (unvollständige Auskunft, falsche Auskunft, vorschnelle Löschung - keine Auskunft) immateriellen Schadensersatz in vierstelliger Höhe (meist zwischen 1.500 € - 2.500 €) geltend macht und darüber hinaus die Vergütung für seine anwaltliche Tätigkeit einfordert (zw. 500 € - 600 €). Weiterer Druck wird auf die Unternehmen durch Androhung eines mit angeblich zwangsläufig weitaus höheren Kosten verbundenen gerichtlichen Verfahrens aufgebaut.

Grundsätzlich ist es korrekt, dass jeder Verstoß gegen die DSGVO zu einem Anspruch auf Ersatz des materiellen und/oder immateriellen Schadens führen kann. Voraussetzung für einen solchen Schadensersatzanspruch nach Art. 82 DSGVO ist, dass

- ein Schaden entstanden ist,
- der Anspruchsgegner hierfür kausal geworden ist sowie
- schuldhaft gehandelt hat.

Die Darlegungs- und Beweislast für die haftungsbegründenden Voraussetzungen trägt der Anspruchsteller nach allgemeinen zivilprozessualen Grundsätzen. Eine Beweislastumkehr ist allerdings in Art. 82 Abs. 3 DSGVO bezüglich des Verschuldens vorgesehen. Das Unternehmen kann sich danach von der Schadenersatzpflicht nur befreien, wenn es nachweist, dass es „in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“.

Dies wiederum ist dem datenschutzrechtlich Verantwortlichen (Art. 4 Nr. 7 DSGVO) in der Regel nur möglich, wenn er die von ihm getroffenen Maßnahmen zur Bearbeitung von sog. Betroffenenbegehren im erforderlichen Umfang dokumentiert (vgl. Art. 5 Abs. 2 und 24 DSGVO).

Seit Inkrafttreten der DSGVO haben sich diverse Gerichte mit immateriellen Schadensansprüchen befasst. Die ergangene Rechtsprechung hierzu ist jedoch bislang uneinheitlich.

Vor diesem Hintergrund empfehlen wir, bei der Bearbeitung von Betroffenenanfragen größte Sorgfalt walten zu lassen. Der Verantwortliche hat gem. Art. 12 Abs. 3 S. 1 DSGVO einen Monat nach Eingang des Antrags Zeit, um die betroffene Person über die aufgrund des Betroffenenbegehrens ergriffenen Maßnahmen zu unterrichten. Ist der Aufwand zur Abhilfe des Betroffenenbegehrens überschaubar, muss der Verantwortliche innerhalb der 1-Monats-Frist die geforderten Informationen gem. Art. 15 DSGVO zur Verfügung stellen oder auch die Wahrnehmung der Betroffenenrechte gem. Art. 16 f. DSGVO ermöglichen.

Sollte die Bearbeitung des Betroffenenbegehrens innerhalb dieser Frist nicht möglich sein, besteht - bei Vorliegen der Voraussetzungen des Art. 12 Abs. 3 S. 2 DSGVO - die Möglichkeit, die 1-Monats-Frist um weitere zwei Monate zu verlängern. Der Verantwortliche muss dazu die betroffene Person über die Fristverlängerung und die Gründe für die Verzögerung gem. Art. 12 Abs. 3 S. 3 DSGVO unterrichten. Ein möglicher Grund kann insbesondere eine sehr hohe Anzahl an gleichzeitigen zu bearbeitenden Betroffenenbegehren sein.

Praxishinweis: Betroffene oder vermeintlich Betroffene können Anträge zur Wahrnehmung ihrer Rechte über verschiedenste Kommunikationskanäle geltend machen. Um eine falsche Negativbeauskunftung zu vermeiden, sollten Verantwortliche nicht nur alle Unternehmensbereiche erneut sensibilisieren, sondern auch eine Erhebung über mögliche Datenpools im Unternehmen aus sämtlichen Fachabteilungen erstellen. Mitarbeiter:innen im Kundenservice, im Sekretariat, in der HR-

Abteilung etc., also alle, die über eine öffentliche Kontaktadresse/-nummer verfügen, sollten bei Fragen über gespeicherte Daten direkt den Kontakt zu der mit den Datenschutzthemen beauftragten Person im Unternehmen (betriebliche/externe Datenschutzbeauftragte, DS-Koordinator:innen, DS-Manager:innen etc.) aufnehmen und Rücksprache halten.

Konkret sollten die folgenden Schritte beachtet werden:

- Identifikation der betroffenen Person (ggf. Art. 11. Abs. 2 DSGVO beachten)
- Überprüfung der personenbezogenen Daten in allen Systemen - ggf. sind Newsletter-Abonnenten nicht in der Kunden-/Mitgliederdatenbank zu finden oder es gibt andere Kundenbindungs-/Werbesysteme
- Beachtung aller angesprochenen Betroffenenrechte - nicht die Daten zuerst löschen und dann angeben, dass keine personenbezogenen Daten vorhanden sind
- Beachtung der 1-Monats-Frist, ggf. über Notwendigkeit der Fristverlängerung informieren

Aufsichtsbehörden: 2020 erreichen Bußgelder bisherigen Rekordwert

Im vergangenen Jahr sind sowohl die Anzahl als auch die Höhe der von Aufsichtsbehörden ausgesprochene Bußgelder stark gestiegen. So hatte der Modehändler H&M eine Geldbuße in Höhe von 35 Mio. EUR zu zahlen. Laut einer Umfrage des Handelsblattes wurden im vergangenen Jahr insgesamt 301 Bußgelder ausgesprochen. Im Jahr 2019 waren es hingegen nur 187 Verfahren, die in einem Bußgeld endeten.

Es wird auch berichtet, dass die Aufsichtsbehörden in der Coronakrise Datenschutzverstöße registriert und geahndet haben. Insbesondere sei es infolge der Verlagerung von Arbeitsplätzen ins Homeoffice zu Datenpannen gekommen (Beachten Sie unsere Hinweise in der Beratungsinformation Januar 2021). Vielfach sind die Verstöße auf Mängel bei den technischen und organisatorischen Maßnahmen zurückzuführten. Als Schwerpunktthemen finden sich hier „Videoüberwachung“ und „unsachgemäße Datenentsorgung“.

Aber auch die klassischen Verstöße gegen die Vertraulichkeit (Offenlegung von personenbezogenen Daten in Netzwerken, Versand an falsche Verteiler, Austausch über Messengerdienste etc.) sind weiterhin vielfach festgestellt worden. Diese „Standardfehler“ spiegeln sich auch in der Zahl der Datenpannen, die nach Information der Aufsichtsbehörden auf 26.260 gestiegen sind.

Praxishinweis: Datenschutz ist nicht mit der Schaffung einer Datenschutzorganisation abgeschlossen. Vielmehr muss Datenschutz in die Unternehmenskultur einfließen und in ein funktionierendes und lebendiges Datenschutzmanagement münden. Dazu gehört, dass neben einem regelmäßigen Review der bestehenden Datenschutzorganisation, dass Veränderungen im Unternehmen stets auf deren datenschutzrechtliche Relevanz zu prüfen sind und ggfs. zu Anpassungen führen. Gleichfalls müssen Datenpannen, in denen Mängel offenbar werden, analysiert werden und organisatorische oder personelle Folgen haben. Dazu müssen die Beschäftigten für das Thema genauso sensibilisiert sein, wie das Management.

EuGH: Gericht muss in einem Vorabentscheidungsverfahren das Verhältnis von nationalem Wettbewerbsrecht zur DSGVO klären

Der Gerichtshof der Europäischen Union (EuGH) gab am 26.10.2020 bekannt, dass der Bundesgerichtshof (BGH) ein Vorabentscheidungsersuchen in der Rechtssache Facebook Ireland Ltd. gegen Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. eingereicht hat.

Darin habe der BGH dem EuGH insbesondere die Frage vorgelegt, ob die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) ("DSGVO") einer nationalen Regelung entgegensteht, die es Wettbewerbern sowie nach nationalem Recht berechtigten Einrichtungen, Verbänden und Kammern erlaubt, unabhängig von einer Verletzung der Rechte der betroffenen Person und ohne ein Mandat der betroffenen Person wegen unlauterer Geschäftspraktiken, des Verbraucherschutzrechts oder unwirksamer AGB vor den Zivilgerichten Klage zu erheben.

Praxishinweis: Die zentrale Frage ist, ob gegen Datenschutzverstöße unabhängig vom Betroffenen, z.B. durch Verbraucherschutzverbände oder Wettbewerber, insbesondere im Wege der Abmahnung, vorgegangen werden kann. Wird dies zugelassen, ist ein Anstiege der Verfolgung und Sanktion von Datenschutzverstößen zu erwarten.

Webseiten-Impressum – Änderung der Rechtsgrundlage

Fast alle Betreiber von Internetseiten müssen Nutzern bestimmte Angaben über ihre Identität bereitstellen. Der Gesetzgeber hat dies im Telemediengesetz (TMG) geregelt. Er spricht dort von allgemeinen Informationspflichten. Die wesentliche Vorschrift ist § 5 TMG. Unternehmen müssen danach mindestens folgende Angeben machen:

- den Namen (bei natürlichen Personen sind es Vor- und Nachname; bei Unternehmen, also den sogenannten juristischen Personen, der Unternehmensname sowie Name und Vorname des Vertretungsberechtigten),
- bei juristischen Personen außerdem die Rechtsform,
- die Anschrift (Straße, Hausnummer, Postleitzahl und Ort. Nicht ausreichend ist ein Postfach),
- einen Kontakt, unter dem Sie die Person oder das Unternehmen schnell erreichen können – elektronisch als auch nicht elektronisch. In der Regel sind das E-Mail-Adresse und Telefonnummer,
- soweit vorhanden, die Umsatzsteuer- oder Wirtschaftssteuer-Identifikationsnummer,
- ebenfalls, soweit vorhanden, das Handels-, Vereins-, Partnerschafts- oder Genossenschaftsregister mit Registernummer.

Webseiten, die redaktionell-journalistische Inhalte anbieten (also z.B. einen Blog oder vergleichbares) müssen hierfür einen inhaltlich Verantwortlichen benennen. Diese Pflicht ergab sich bisher aus § 55 Abs. 2 Rundfunkstaatsvertrag (RStV). Am 07.11.2020 wurde der Rundfunkstaatsvertrag vom Medienstaatsvertrag (MStV) abgelöst. Hinsichtlich der Informationspflicht im Impressum ändert sich nichts. **Allerdings muss hier die neue Regelung, § 18 Abs. 2 MStV, zitiert werden.**

Praxishinweis: Unternehmen sollten das Impressum regelmäßig auf Aktualität und Richtigkeit prüfen. Oft werden neue Rubriken in der Webseite aufgenommen (z.B. eine Blog-Rubrik, ein Pressebereich), ohne dass das Impressum mit angepasst wird. Wenn es also redaktionell-journalistische Inhalte gibt, ist ein Verantwortlicher gem. § 18 Abs. 2 MStV zu bestimmen und im Impressum auszuweisen.
Ein Verstoß gegen die Informationspflichten im Impressum kann abgemahnt werden.

Impressum

mip Consult GmbH
Wilhelm-Kabus-Straße 9
10829 Berlin
Tel: +49 (0) 30 – 20 88 999 – 00
Fax: +49 (0) 30 – 20 88 999 – 88
Redaktion: Stefan Ax, Asmus Eggert

Internet: www.sofortdatenschutz.de und www.blog.sofortdatenschutz.de
E-Mail: sofortdatenschutz@mip-consult.de

Vertretungsberechtigte Geschäftsführer: Asmus Eggert, Uwe Leider
Registergericht: Amtsgericht Berlin-Charlottenburg
Registernummer: HRB 121869
USt.-Identnr.: DE249276018
Verantwortlich nach § 18 Abs. 2 MStV: Asmus Eggert